平成15年度　学位論文

可解な５次方程式について

兵庫教育大学大学院　学校教育研究科
教科・領域教育専攻　自然系コース
Ｍ０２１７７Ｉ　大迎規宏

目 次

0章　序

本論文のテーマは, 有理数係数の 5 次方程式が可解であるかどうかを判定する D.S.Dummit の方法について考察することである.

方程式とは未知数を含む等式であり, 方程式を解くとは, その等式を満たす未知数の値 (方程式の根) を求めることである. ただし, 本論文では未知数が 1 つの方程式のみを考察の対象とする.

B.C.2000 年頃 (Babylonia) にはすでに, 1 次方程式 $ax+b=0$ はおろか 2 次方程式 $ax^2+bx+c=0$, 3 次方程式 $ax^3+bx^2+cx+d=0$ を計算で解く方法が知られていたといわれる. 2 次方程式 $ax^2+bx+c=0$ の根は

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

である. この根は係数 a, b, c から四則演算とベキ根をとる操作のみを使って表示されている. このときベキ根によって根が表示されるという. 3 次方程式は Cardano(1501-76) により, 4 次方程式はその弟子 Ferrari(1522-65) によって, その根がベキ根によって表示されることが 16 世紀前半に示された. このようにベキ根による根の表示ができるとき, 方程式は可解であるといい, 可解でないとき非可解であるという.

Gauss の代数学の基本定理 (1799) によれば, 複素係数方程式は必ず複素数根を持つ. しかし 5 次方程式の根を「ベキ根によって表示する」という問題は長い間未解決であった. 1824 年, Abel は「一般には, 5 次以上の方程式は非可解である」という結果を発表し, 5 次以上の方程式の根は必ずしもベキ根によって表示することができないことを証明した. ただし $x^5-1=0$ のように有理数体 $\mathbb{Q}$ 上既約でない 5 次方程式は可解である. また既約な 5 次方程式で可解なものも存在する. 例えば $x^5+15x+12=0$ などがその例である.

可解な方程式と非可解な方程式の違いの本質を見抜いたのは Galois (1811-32) であった. 体 F に係数を持つ方程式 $f(x)=0$ に対して $f(x)$ が 1 次式の積に分解する F の拡大体が存在する. そのうち最小な体 E を $f(x)=0$ の分解体という. E の F を固定する自己同型群の元は $f(x)=0$ の根の置換を引き起こす. 拡大 E/F を Galois 拡大, この自己同型群を Galois 群という. Galois は 現在, 群論の基本概念として知られている, 剰余類分解, 正規部分群, 組成列等の概念を最初に用い,「方程式には対応する根の置換群 (Galois 群) が

あり, その構造が 5 次方程式の可解性を決定している」ことを示した. 方程式に Galois 群が対応し, 方程式がベキ根で解けるかどうかが, その Galois 群が可解であるかどうかで判定できるという Galois により得られた成果は, 現在では Galois 理論として知られている. 群論によると, n 次対称群 S_n は $n \leq 4$ のとき可解であるが, $n \geq 5$ のとき可解でない. これが 5 次以上の方程式に根の公式の存在しない理由である. Galois は, 方程式の解法の本質が根の置換のなす群の構造にあることを見抜いたのである.

さて, 5 次方程式の可解性を判定する直接的な方法はないのかという疑問が生じる. Dummit は与えられた 5 次方程式から導かれる 6 次分解式を利用して判定する方法を見出した. S_5 の可解な可移部分群は幸運にも, 巡回群 $\mathbb{Z}_5$, 2 面体群 D_{10}, S_5 の Sylow 5 部分群の正規化群 F_{20} の 3 種類に限られる. Dummit は F_{20} によって固定される元を導入し, その元を有理数体 $\mathbb{Q}$ に添加することで F_{20} の不変体を構成した. さらに, 判定条件「5 次方程式が可解であるための必要十分条件は 6 次分解式がちょうど 1 つの有理数根を持つことである」を導いた. これより, 与えられた 5 次方程式の係数から 6 次式を計算し, それが有理数根を持つかどうか判定すればよいことになる. 本論文では, Dummit の判定法と解法を示した後, 可解な 3 項 5 次方程式に関する B.K. Spearman と K.S. Williams の定理についても考察する.

以下, 論文の構成について述べる.

1 章では, 後章で必要となる群, 環, 体についての基本事項について説明する. §1.1 では正規部分群, 剰余群, 準同型定理, Sylow の定理, 2 面体群などについて説明する. §1.2 ではイデアルによる剰余環, 素体と体の標数, 多項式についての除法の定理, 既約多項式と既約性の判定法などについて説明する. §1.3 では体の拡大と拡大次数, 分解体の存在と一意性などについて説明する.

2 章では対称群, および可解群に関する定理を証明し, S_5 の可解な可移部分群を決定する. §2.1 では対称群, 交代群を定義し, 対称群の生成系を求め, 交代群が 3-cycle で生成されること, 5 次の交代群が単純群であることなどを示す. また, §2.2 では可解群の基本事項について説明する. 最後の §2.3 では $n \geq 5$ のとき S_n が非可解であることを証明し, S_5 の可解な可移部分群の位数が 5, 10, 20 のいずれかになること, 逆にこれらを位数とする部分群が可解な可移部分群であることを証明する.

3 章では Galois 理論について説明する. §3.1 では, 体の拡大の自己同型群, 特に多項式の分解体の自己同型群について考察する. n 次多項式の分解体の自己同型群が n 次対称群の部分群に同型であること, その位数が拡大次数に一致することなどを証明する. §3.2 では, ベキ根拡大を定義し, 方程式がベキ根によって可解であることと, 方程式の分解体がベキ根拡大体に含まれることとが同値であることを示し, 可解な方程式の自己同型群が可解群になることを示す. §3.3 では, 不変体, Galois 拡大, Galois 群などの概念を導入し, Galois 拡

大の中間体と Galois 群の部分群とが一対一に対応する, という Galois の基本定理を証明する. §3.4 では, 方程式がベキ根により可解であることと, その Galois 群が可解群であることとが同値であることを証明する. これより可解な既約 5 次方程式が, S_5 の可解な可移部分群を Galois 群にもつ方程式として特徴づけられる.

4 章では, 本論文のテーマである Dummit による有理数係数既約 5 次方程式の可解性を判定する方法と, 可解な 5 次方程式の解法について述べる. §4.1 では既約 5 次方程式 $f(x)=0$ の 5 個の根の 4 次同次式 θ を導入し, 2 章で示した S_5 の可移部分群に関する結果を基に, θ の 6 個の共役を根に持つ 6 次分解式 $f_{20}(x)$ が 1 つの有理数根を持つことと, $f(x)$ が可解であることとが同値であることを導く. §4.2 では有理数係数の可解な既約 5 次方程式 $f(x)=0$ から定まる Lagrange 分解式と, Lagrange 分解式を 5 乗して得られる式への Galois 群の作用を通して, $f(x)$ の係数と $f_{20}(x)$ の有理数根の有理式として表示できる定数の存在を導く. また, それらの定数を用いて $f(x)$ の根が復元できるしくみを明らかにする. §4.3 では可解な 3 項 5 次方程式に対して, その解法を例示する.

5 章では, 3 項 5 次方程式

$$x^5+ax+b=0$$

が可解であることと, 係数 a,b がある形のパラメータ表示を持つこととが同値である, という Spearman と Williams の定理を証明し, このパラメータ表示を用いて根を求める方法を明らかにする. §5.1 では 3 次方程式の Cardano による解法と同様に

$$x_j=\zeta^j u_1+\zeta^{2j}u_2+\zeta^{3j}u_3+\zeta^{4j}u_4 \quad (j=0,...,4)$$

を根に持つ 5 次方程式が $x^5+ax+b=0$ に一致するための u_1,u_2,u_3,u_4 の満たすべき条件を導き, これを利用して Spearman, Williams の定理を証明する. §5.2 では可解な 3 項 5 次方程式の解法を例示する.

なお, 主たる参考文献は, 群論では [3], Galois 理論では [5] である. また, 田代敏和氏による本学修士論文 [7] においても Galois 理論が扱われているが, そこでの主題は Hermite による楕円関数を用いた 5 次方程式の解法であり, 本論文のテーマである可解な 5 次方程式とは異なることを申し添えておく.

最後に, 本論文作成にあたり, 2 年間ご指導頂いた松山廣先生を始め, ご助言いただいた自然系数学分野の諸先生方, さらにはこのような機会を与えて下さった兵庫県教育委員会, 並びに兵庫県立淡路高等学校長を始めとする諸先生方に, 心より感謝申し上げます.

1章　準備

1章では, 後章で必要となる群, 環, 体についての基本事項について説明する. ただし, 定理の証明は一部を除いて省略し, 参考文献を明記するにとどめた. また, 集合, 写像, 同値関係, 線型代数学についての基本事項は既知とした.

§1.1 では正規部分群, 剰余群, 準同型定理, Sylow の定理, 2面体群などについて説明する. §1.2 ではイデアルによる剰余環, 素体と体の標数, 多項式についての除法の定理, 既約多項式と既約性の判定法などについて説明する. §1.3 では体の拡大と拡大次数, 分解体の存在と一意性などについて説明する.

なお, この論文を通して次の記号を用いる.

$$\begin{aligned}
\mathbb{Z} &= \{0, \pm 1, \pm 2, \pm 3, ...\} \quad \text{整数全体} \\
\mathbb{Q} &= \left\{ \frac{b}{a} \,\middle|\, a, b \in \mathbb{Z},\ a \neq 0 \right\} \quad \text{有理数全体} \\
\mathbb{R} &= \text{実数全体} \\
\mathbb{C} &= \{a + ib \mid a, b \in \mathbb{R}\} \quad \text{複素数全体} \quad (\text{ただし } i \text{ は } i^2 = -1 \text{ を満たす})
\end{aligned}$$

また, 「A ならば B である」ことを「$A \implies B$」と表すことがある.

1.1　群論の基本事項

集合 G の 2 元 a, b に対して G の元を一つ対応させる規則を G 上の演算という. a, b に対応する元を演算記号 $\cdot$ などを用いて $a \cdot b$ などと表し a, b の積と呼ぶ. この論文では, 特に混乱の恐れがない限り, 演算記号 $\cdot$ は省略する.

空でない集合 G に演算 $\cdot$ が定義され, 次の (1)〜(3) を満たすとき G を群という.

(1)　演算は結合法則を満たす. すなわち, 任意の a, b, $c \in G$ に対して $(ab)c = a(bc)$ が成り立つ.

(2)　ある元 $e \in G$ が存在して, 任意の $a \in G$ に対して $ea = ae = a$ を満たす.

(3)　任意の $a \in G$ に対して, ある元 $b \in G$ が存在して $ab = ba = e$ を満たす

定義の条件 (2) を満たす e は一意に定まる. e を G の単位元といい, 以下, 1 と表すことにする. 数字の 1 と異なることに注意されたい.

群 G の元 a に対して条件 (3) を満たす b は一意に定まる. この b を a の逆元といい a^{-1} と表す.

群 G の元 a, b が $ab = ba$ を満たすとき, a, b は可換であるという. 任意の 2 元が可換である群を Abel 群, または可換群という.

G が Abel 群のとき, 演算記号を $+$, 単位元を 0 と表し, 加法群ということがある.

群 G の元の個数 (濃度) を位数といい, $|G|$ と表す. 集合 S の元の個数も同じ記号 $|S|$ で表すことにする. 位数が有限の群を有限群という.

群 G の n 個の元 $a_1, a_2, \cdots, a_n$ のこの順序を変えない演算のしかた (括弧のくくり方) は何通りもあるが, その結果は常に等しい (一般の結合法則). これより a と整数 n に対して, a のベキ a^n が次のように定義される.

$$a^n = \begin{cases} \overbrace{aa\cdots a}^{n\text{個}} & n > 0 \text{ のとき} \\ 1 & n = 0 \text{ のとき} \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{-n\text{個}} & n < 0 \text{ のとき} \end{cases}$$

群 G の元 g に対して $g^m = 1$ となる正の整数 m が存在するとき, そのような m のなかで最小のものを g の位数といい $|g|$ と表す. そのような m が存在しないとき, g の位数は無限であるといい, $|g| = \infty$ と表す.

群 G のすべての元がある元 g のベキとして表されるとき G を巡回群という. このとき, g を G の生成元といい $G = \langle g \rangle$ と表す.

定義 1.1 (部分群) 群 G の 空でない部分集合 H が次の条件を満たすとき, H を G の部分群といい $H \leq G$ と表す.

(1) $a, b \in H$ ならば $ab \in H$ である.

(2) $a \in H$ ならば $a^{-1} \in H$ である.

部分群はそれ自身, 群である.

G の部分群 H と $g \in G$ に対して $gH = \{gh \mid h \in H\}$ を g を含む H の左剰余類, $Hg = \{hg \mid h \in H\}$ を g を含む H の右剰余類という. G は H の左 (右) 剰余類に分割される. ここで $gH = g'H$ となる条件が $g^{-1}g' \in H$ であることを注意しておく.

群 G における部分群 H の左 (右) 剰余類の個数を G の指数といい $[G : H]$ と表す.

定理 1.2 (Lagrange の定理, [3, Theorem 2.11, Corollary 2.12]) G が位数 g の有限群のとき次が成り立つ.

(1) G の部分群 H の位数 h は g を割り切る. 特に $[G:H]=\dfrac{g}{h}$ が成り立つ.

(2) G の元の位数は有限で g を割り切る.

群 G から群 H への写像 $\varphi: G \to H$ が, 任意の $a, b \in G$ に対して $\varphi(ab)=\varphi(a)\varphi(b)$ を満たすとき φ を準同型 (写像) という. 特に φ が全単射のとき φ を同型 (写像) という. 同型 $\varphi: G \to H$ があるとき G と H は同型であるといい $G \simeq H$ と表す. φ が準同型のとき $\varphi(1)=1, \varphi(a^{-1})=\varphi(a)^{-1}$ が成り立つ.

準同型 $\varphi: G \to H$ に対して

$$Ker(\varphi)=\{a \mid a \in G,\ \varphi(a)=1\}, \qquad Im(\varphi)=\{\varphi(a) \mid a \in G\}$$

とおき, $Ker(\varphi)$ を φ の核, $Im(\varphi)$ を φ の像という.

$Ker(\varphi)$ は G の正規部分群, $Im(\varphi)$ は H の部分群である. また φ が単射である条件は $Ker(\varphi)=\{1\}$ となることである.

群 G の元 $x, y \in G$ に対して $y=gxg^{-1}$ となる G の元 g が存在するとき, x と y は共役であるという. G の部分群 H, K に対しても, $K=gHg^{-1}=\{ghg^{-1} \mid h \in H\}$ となる $g \in G$ が存在するとき, H と K は共役であるという. G の元 g による共役をとる写像

$$G \ni x \longmapsto gxg^{-1} \in G$$

は G の自己同型 (G から G への同型) である. 従って共役な部分群は互いに同型である.

定義 1.3 (正規部分群) 群 G の部分群 H が, 任意の $g \in G$ に対して

$$gHg^{-1}=\{ghg^{-1} \mid h \in H\}=H$$

を満たすとき, H を G の正規部分群といい $H \trianglelefteq G$ と表す.

任意の群において, それ自身と $\{1\}$ は正規部分群である. Abel 群の部分群はすべて正規部分群であり, 指数 2 の部分群も正規部分群である.

$H \trianglelefteq G$ のとき, 任意の $g \in G$ に対して $gH=Hg$ が成り立つ.

定理 1.4 (剰余群) $H \trianglelefteq G$ のとき H の剰余類全体を G/H とおき，G/H に演算を

$$(gH)(g'H) = gg'H$$

と定義すると G/H は群になる．これを G の H による剰余群という．

G/H の単位元は $1H = H$ であり，gH の逆元は $g^{-1}H$ である．また G が有限群のとき $|G/H| = |G|/|H|$ である．

以下, 単位元のみからなる群 $\{1\}$ を単に 1 と表すことがある．

定義 1.5 群 $G \neq 1$ の正規部分群が 1 と G 自身のみであるとき G を単純群という．

定理 1.6 (準同型定理, [3, Theorem 2.24]) $\varphi : G \to H$ が準同型のとき次が成り立つ．

$$G/Ker(\varphi) \simeq Im(\varphi)$$

定理 1.7 ([3, Theorem 2.20]) 群 G の部分群 H, K に対して

$$|H \cap K||HK| = |H||K|$$

が成り立つ．ただし $HK = \{hk \mid h \in H, k \in K\}$ である．

定義 1.8 (群の直積) H, K を群とする．直積集合 $H \times K$ の 2 元 $(h,k),(h',k') \in H \times K$ に対して演算を次のように定義すると $H \times K$ は群となる．この群を H と K の直積という．

$$(h,k)(h',k') = (hh',kk')$$

定理 1.9 ([3, Theorem 2.29]) H, K が群 G の正規部分群であり，$HK = G$, $H \cap K = \{1\}$ を満たすならば $G \simeq H \times K$ が成り立つ．

整数 a が整数 b を割り切るとき, すなわち $b = ac$ を満たす整数 c が存在するとき，$a \mid b$ と表すことにする．正の整数 n と整数 a, b に対して，$n \mid a - b$ が成り立つとき，$a \equiv b \pmod{n}$ と表し，a と b は n を法として合同であるという．

G を位数が $p^n m$ の有限群とする．ただし p は素数, $p \nmid m$ とする．G に位数が p^n の部分群 P が存在するとき，P を G の Sylow p 部分群という．なお, 位数が素数 p のベキである有限群を p 群という．Sylow p 部分群は p 群である．

定理 1.10 (Sylow の定理, [3, pp.78-79]) G を有限群, p を $|G|$ の素因数とする. このとき次が成り立つ.

(1) G に Sylow p 部分群が存在し, それらは互いに共役である.

(2) G の任意の p 部分群 H に対して, H を含む Sylow p 部分群が存在する.

(3) G の Sylow p 部分群の個数を r とすると $r \equiv 1 \pmod{p}$ が成り立つ.

群 G の Sylow p 部分群がただ 1 つのとき, それが正規部分群であることは上の定理の (1) から明らかであろう.

また Sylow p 部分群の元の位数が p のべきであることから次の系が導かれる.

系 1.11 (Cauchy の定理, [5, 付録 B, 系 G.14]) p が群 G の位数の素因数ならば G は位数 p の元を含む.

群 G の部分集合 S に対して S を含む G の部分群すべての共通部分はまた G の部分群となる ([3, Theorem 2.5]). これを S で生成された部分群といい $\langle S \rangle$ と表す. G の元 a に対して $\langle a \rangle$ の位数は元 a の位数に一致する.

位数が素数 p である群 G の部分群の位数は Lagrange の定理より 1 または p である. ゆえに G の元 $a \neq 1$ に対して $\langle a \rangle = G$ となる. すなわち素数位数の群は巡回群である.

定義 1.12 (2 面体群) 次の条件を満たす 2 つの元 a, b で生成される群を 2 面体群といい, D_{2n} と表す.

$$|a| = n \ \ (n \geq 2), \quad |b| = 2, \quad bab = a^{-1}$$

D_{2n} の位数は $2n$ である. 次は可解な 5 次方程式の Galois 群を考察する際に必要となる定理である.

定理 1.13 ([3, Theorems 4.19-20]) 位数 $2p$ (p は素数) の群は巡回群か 2 面体群である. また q が $q < p$ かつ $q \nmid p-1$ なる素数とすると, 位数 pq の群はすべて巡回群である.

1.2 環と体の基本事項

集合 R に 2 つの演算, 加法 $+$ と乗法 $\cdot$ が定義され, 次の (1)〜(4) を満たすとき R を可換環という.

(1) R は $+$ について加法群である.

(2) 任意の $a, b \in R$ に対して $ab = ba$ が成り立つ.

(3) 任意の $a, b, c \in R$ に対して $(ab)c = a(bc)$ が成り立つ.

(4) ある元 1 が存在して, 任意の $a \in R$ に対して $a1 = a$ が成り立つ.

(5) 任意の $a, b, c \in R$ に対して $a(b + c) = ab + ac$ が成り立つ.

可換環 R において加法の零元 0 と乗法の単位元 1 は一意に定まる.

以下, 本論文では $1 \neq 0$ と仮定し, 可換環を単に環と呼ぶことにする.

環 R の部分集合 S が次の条件を満たすとき R の部分環であるという.

- $1 \in S$
- $a, b \in S$ ならば $a - b \in S$ かつ $ab \in S$ が成り立つ.

部分環はそれ自身環である. また環 R の任意の元 a に対して $a0 = 0a = 0$ が成り立つことを注意しておく.

定義 1.14 環 R の 0 でない 2 元の積が常に 0 でないとき R を整域という.

環 R が整域になるための条件は簡約法則

$$ra = rb, \quad r \neq 0 \quad \Longrightarrow \quad a = b$$

が成り立つことである.

環 R の元 a に対して $ab = 1$ となる元 $b \in R$ が存在するとき a を単元という. また, このとき $b = a^{-1}$ と表し, b を a の逆元という.

定義 1.15 0 でない元がすべて単元であるような環を体という.

体 R の部分環で, それ自身体であるものを R の部分体という. 体 E の部分体からなる集合 $\{F_i\}_{i \in I}$ に対して, 共通部分 $\cap_{i \in I} F_i$ はまた E の部分体となる. 体 E の部分体 B, C を含む E の部分体すべての共通部分を B, C の合成体といい $B \vee C$ と表す.

体の 0 でない元はすべて単元であるから, 任意の 2 元の積は 0 になり得ない. 従って体は常に整域である.

任意の整域 R に対して, R を部分環として含む体 $\bar{R}$ で, $\bar{R}$ の任意の元は, R のある 2 元 a, $b(\neq 0)$ によって ab^{-1} と表すことができるものが存在する. $\bar{R}$ を R の商体という. 整域の商体は同型を除いて一意である ([4, 1 章, 定理 1.2]).

定義 1.16 (環準同型) 環 R から環 S への写像 $\varphi : R \to S$ で次の条件を満たすものを環準同型 (写像) という. ただし r, r' は R の任意の元を表す.

$$\varphi(r+r') = \varphi(r) + \varphi(r'), \quad \varphi(rr') = \varphi(r)\varphi(r'), \quad \varphi(1) = 1$$

環準同型 φ が全単射のとき環同型 (写像) といい, このとき R と S は (環) 同型であるという.

イデアル

定義 1.17 環 R の空でない部分集合 I が次の条件を満たすとき R のイデアルであるという.

(1) $a, b \in I$ ならば $a - b \in I$ である.

(2) $r \in R$, $a \in I$ ならば $ra \in I$ である.

環 R の元 $a_1, ..., a_n$ に対して

$$I = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R,\ i = 1, ..., n\}$$

とおくと I は R のイデアルである. このような I を $\{a_1, ..., a_n\}$ で生成されるイデアルといい $I = (a_1, ..., a_n)$ と表す.

環 R のイデアル I は加法群 R の部分群であることから剰余群 R/I が存在する. ここで R/I の 2 元 $r + I$, $r' + I$ の積を $(r + I)(r' + I) = rr' + I$ と定義すれば, この定義は well-defined である. すなわち $r + I = s + I$, $r' + I = s' + I$ のとき $r - s, r' - s' \in I$ であるから $rr' - ss' = r(r' - s') + s'(r - s) \in I$ となり, $rr' + I = ss' + I$ が成り立つからである. この積により R/I が環となることは容易に確かめることができる ([5, 5 章, 定理 11]).

定義 1.18 (剰余環) R/I を環 R のイデアル I による剰余環という.

正の整数 n の倍数からなる集合 $n\mathbb{Z}$ は環 $\mathbb{Z}$ のイデアルである. 一方, p.7 で定めた関係 $\equiv \pmod{n}$ は $\mathbb{Z}$ 上の同値関係であり, このときの同値類は n を法とする剰余類と呼ばれ, 剰余環 $\mathbb{Z}/n\mathbb{Z}$ の元に一致する. 以下, 剰余環 $\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}_n$ と表す. 特に素数を法とする剰余環を $\mathbb{Z}_p$ と表すことがある. なお $\mathbb{Z}_n$ でその加法群を表すこともある. 加法群 $\mathbb{Z}_n$ は位数 n の巡回群であることを注意しておく.

剰余環 $\mathbb{Z}/n\mathbb{Z}$ の元 $\bar{a}$ が単元である条件は $(a, n) = 1$, すなわち a と n が互いに素であることである. これより次の定理が得られる.

定理 1.19 ([5, 3章, 定理8]) $\mathbb{Z}_n$ が体であることと，n が素数であることとは同値である．

定義 1.20 (素イデアル) 環 R の イデアル $I(\neq R)$ が条件「$ab \in I$ ならば $a \in I$ または, $b \in I$」を満たすとき, I を素イデアルという．

I が環 R の素イデアルであることと, 剰余環 R/I が整域であることは同値である ([5, 7章, 定理25]).

体 F の部分体すべての共通部分を F の素体という．素体自身も部分体である．体の素体は $\mathbb{Q}$ か $\mathbb{Z}_p$ に同型である．([5, 7章, 定理31]).

定義 1.21 体 F の素体が $\mathbb{Q}$ に同型のとき F の標数は 0 であるといい, 体 F の素体が $\mathbb{Z}_p$ に同型のとき F の標数は p であるという．

体の標数は 0 か素数である．以下標数 p という場合 p は素数であるとする．

F の標数が p のとき $\underbrace{1+\cdots+1}_{p\text{個}}=0$ が成り立つ．これより次が導かれる ([5, 7章, 定理32]).

(1) 任意の $a \in F$ に対して $pa=\underbrace{a+\cdots+a}_{p\text{個}}=0$ である．

(2) 任意の $a, b \in F$ に対して $(a+b)^{p^k}=a^{p^k}+b^{p^k}$ が成り立つ．ただし k は正の整数．

多項式環

環 R に対して, 次の形の式 $f(x)$ を x を変数とする R 係数多項式という．ただし $a_0, \ldots, a_n \in R$ とする．

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

ここで a_kx^k を k 次の項, a_k を k 次の係数という．

R 係数多項式全体のなす集合を $R[x]$ とおくと, $R[x]$ は通常の加法, 乗法により環となる ([5, pp.12-13]). $R[x]$ を R 上の多項式環という．さらに, 環 $R[x]$ 上の y を変数とする多項式環を $R[x,y]$ と表して2変数多項式環という．同様に n 変数多項式環 $R[x_1, \ldots, x_n]$ が定義される．

さて $R[x] \ni f(x) \neq 0$ において $a_k \neq 0$ となる最大の整数 k を $f(x)$ の次数といい $\partial(f)=k$ と表す．このとき a_k を最高次係数という．なお a_0 を定数項と呼ぶ．また, 最高次係数が 1 の多項式をモニック多項式という．

以下 $f(\alpha)=0$ を満たす α を方程式 $f(x)=0$ の根, または単に $f(x)$ の根という.

さて, R が整域のとき 0 でない多項式 f, g に対して $\partial(fg)=\partial(f)+\partial(g)$ が成り立つ. これより次の定理が得られる.

定理 1.22 ([5, 3 章, 問題 13]) R が整域であれば, $R[x]$ も整域である.

同様に n 変数多項式環 $R[x_1,...,x_n]$ も整域である. 体 F 上の n 変数多項式環 $F[x_1,...,x_n]$ の商体を n 変数有理関数体といい $F(x_1,...,x_n)$ と表す.

定理 1.23 (除法の定理, [5, 3 章, 問題 17]) R は整域とする. R 係数多項式 $f(x)$ と R 係数モニック多項式 $g(x)$ に対して

$$f(x)=g(x)q(x)+r(x), \qquad r(x)=0 \ \text{ または } \ \partial(r)<\partial(g)$$

を満たす R 係数多項式 $q(x)$, $r(x)$ が存在する.

$q(x)$ を $f(x)$ を $g(x)$ で割った商, $r(x)$ を $f(x)$ を $g(x)$ で割った余りという.

$f(x)$ を $g(x)$ で割った余りが 0 のとき $g(x)$ は $f(x)$ を割り切るといい $g(x)\mid f(x)$ と表す. またこのとき $g(x)$ を $f(x)$ の因子 (約数) という.

なお, 上の定理は R が体のときには $g(x)$ がモニックでなくとも成り立つことを注意しておく.

次数が 1 以上, $\partial(f)-1$ 以下の因子を持つ多項式 $f(x)$ を可約 (多項式) という.

次数が 1 以上の多項式で可約でないものを既約 (多項式) という.

R が整域のとき, $f(x),g(x)\in R[x]$ のモニックな共通因子 $d(x)$ で次の条件を満たすものを $f(x),g(x)$ の最大公約多項式といい $d(x)=(f(x),g(x))$ と表す.

- $f(x),g(x)$ の任意の共通因子 $c(x)$ に対して $c(x)\mid d(x)$

$(f(x),g(x))=1$ のとき, $f(x)$ と $g(x)$ は互いに素であるという.

最大公約多項式が整数の場合と同様にユークリッドの互除法で求められることから次の定理を得る.

定理 1.24 ([5, 6 章, 系 18]) F を体 E の部分体, $f(x),g(x)\in F[x]\subseteq E[x]$ とする. このとき $E[x]$ における $f(x)$ と $g(x)$ の最大公約多項式は $F[x]$ における $f(x)$ と $g(x)$ の最大公約多項式と一致する.

F が体, $f(x)\in F[x]$ のとき, $a\in F$ が $f(x)$ の根であるための必要十分条件は, $x-a$ が $f(x)$ を割り切ることである ([5, 6 章, 系 21]). これより次の定理が導かれる.

定理 1.25 ([5, 6章, 定理22]) F は体とする. $f(x) \in F[x]$ の次数が $n(\geq 0)$ のとき $f(x)$ は F 内に高々 n 個の根を持つ.

多項式の既約性の判定

ここでは $\mathbb{Q}$ 係数多項式が既約かどうか判定する方法について述べる.

補題 1.26 $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ とする. $\frac{r}{s}$ が $f(x)$ の有理数根で $(r, s) = 1$ のとき $r \mid a_0$, $s \mid a_n$ が成り立つ.

Proof 式 $f(\frac{r}{s}) = 0$ を考察すればよい (詳細略). ∎

$\sigma : R \to \bar{R}$ が環準同型であれば

$$\sigma^* : R[x] \ni \sum r_i x^i \mapsto \sum \sigma(r_i) x^i \in \bar{R}[x]$$

で定まる写像 $\sigma^* : R[x] \to \bar{R}[x]$ も環準同型である.

定理 1.27 ([5, 8章, 定理34]) R を整域, F を体とする. $\sigma : R \to F$ を環準同型とし, $\sigma^* : R[x] \ni \sum r_i x^i \mapsto \sum \sigma(r_i) x^i \in F[x]$ を対応する環準同型, $p(x)$ を R 係数モニック多項式とする. $\sigma^*(p(x))$ が $F[x]$ で既約のとき $p(x)$ は $R[x]$ で既約である.

この定理は $\mathbb{Z}$ 係数多項式の既約性の判定に有効である. 例えば $f(x) = x^3 - 7x - 1 \in \mathbb{Z}[x]$ に対して $\sigma : \mathbb{Z} \to \mathbb{Z}_2$ を自然な環準同型として, 定理 1.27 を適用する. $\sigma^*(f(x)) = x^3 + x + 1$ は, $\mathbb{Z}_2$ 内に根を持たないので $\mathbb{Z}_2$ 上既約である. ゆえに $f(x)$ は $\mathbb{Z}$ 上既約であると判定できる. このとき $f(x)$ は $\mathbb{Q}$ 上で考えても既約である ([5, 8章, 定理39]).

定理 1.28 (Eisenstein の判定法,[5, 8章, 定理40]) $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ に対して

$$p \nmid a_n, \qquad p \mid a_i \ (i = 0, \ldots, n-1), \qquad p^2 \nmid a_0$$

を満たす素数 p が存在すれば $f(x)$ は $\mathbb{Q}$ 上既約である.

系 1.29 p が素数のとき $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ は $\mathbb{Q}$ 上既約である.

Proof

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

が成り立つ. ここで

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

であるから $1 \leq k \leq p-1$ のとき $(p, k!) = 1$ より $\binom{p}{k}$ は p の倍数である. 従って Eisenstein の判定法より $\Phi_p(x+1)$ は $\mathbb{Q}$ 上既約となり, このとき $\Phi_p(x)$ も $\mathbb{Q}$ 上既約である. ∎

$\Phi_p(x)$ を p 次円周等分多項式という.

1.3 体の拡大と分解体

この節において F, E は体であるとする.

定義 1.30 (体の拡大) F が体 E の部分体のとき E を F の拡大体であるといい E/F と表す. E/F を単に (体の) 拡大ということがある. また $F \subseteq B \subseteq E$ となる体 B を拡大 E/F の中間体という.

体の拡大 E/F が与えられたとき, F の元 c による加法群 E の元 α のスカラー倍を, E における積 $c\alpha \in E$ で定義すると, E は F 上のベクトル空間となる.

定義 1.31 (拡大次数) 体の拡大 E/F に対して E を F 上のベクトル空間と見なしたときの次元を拡大 E/F の (拡大) 次数といい $[E : F]$ と表す. $[E : F]$ が有限のとき E/F を有限次拡大という.

$[E : F] = n$ のとき, E を F の n 次拡大ということがある.

補題 1.32 ([5, 10 章, 補題 49]) $E/B, B/F$ が有限次拡大のとき E/F も有限次拡大であり, 次式が成り立つ.

$$[E : F] = [E : B][B : F]$$

F 係数多項式 $f(x)$ が $F[x]$ において 1 次式の積として表されるとき $f(x)$ は F で分解するという.

補題 1.33 ([5, 7 章, 系 29]) $p(x) \in F[x]$ が既約のとき剰余環 $F[x]/(p)$ は $p(x)$ の根を含む F の拡大体である.

$p(x)$ を n 次既約多項式, 体 $E = F[x]/(p)$ に含まれる $p(x)$ の根を α とおけば, E は F の n 次拡大であり, E を F 上のベクトル空間と見たときの基底として $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ を選ぶことができる ([5, 10 章, 定理 45]).

定理 1.34 ([5, 7章, 定理30]) 1次以上の多項式 $f(x) \in F[x]$ に対して $f(x)$ が分解するような F の拡大体 E が存在する.

拡大 E/F と $\alpha_1, ..., \alpha_n \in E$ に対して F と $\alpha_1, ..., \alpha_n$ を含む E の部分体すべての共通部分を $F(\alpha_1, ..., \alpha_n)$ で表し, F に $\alpha_1, ..., \alpha_n$ を添加した体という.

特に, E が1つの元 α を F に添加して得られるとき, すなわち, $E = F(\alpha)$ であるとき E/F を単純拡大という.

F の拡大体 E の元 α が $F[x]$ の, ある0でない多項式の根であるとき α は F 上代数的であるという. α が F 上代数的でないとき F 上超越的であるという.

E の任意の元が F 上代数的であるような拡大 E/F を代数拡大という.

定理 1.35 ([5, 10章, 定理46]) 有限次拡大は代数拡大である.

定理 1.36 (最小多項式, [5, 10章, 定理47]) F の拡大体 E の元 α が F 上代数的であるとき, α を根にもつ F 係数モニック多項式で最小次数のもの $p(x)$ が一意に存在し, 次が成り立つ. $p(x)$ を α の F 上の最小多項式という.

(1) $p(x)$ は既約である.

(2) α を根にもつ任意の $f(x) \in F[x]$ に対して $p \mid f$ が成り立つ.

(3) $F[x]/(p)$ から $F(\alpha)$ への同型写像 φ で F の元をすべて固定し, $\varphi(x + (p)) = \alpha$ を満たすものが存在する.

(4) $[F(\alpha) : F] = \partial(p)$ である.

上の(3)の φ のように F の2つの拡大体の間の同型写像で F の元を固定するものを F 同型という.

定義 1.37 (分解体) $f(x) \in F[x]$ が分解する最小の F の拡大体を $f(x)$ の分解体という.

最小の拡大体という表現はこの時点では適当でなく, 極小の拡大体というべきである. しかし後で述べるように $f(x)$ が分解する極小の拡大体はすべて F 同型となり, 同型の意味で最小ということができる.

例えば $\omega(\neq 1)$ を1の3乗根とすると $x^3 - 1 \in \mathbb{Q}[x]$ は $\mathbb{C}$ で分解するが, 分解体は, $\mathbb{Q}(\omega)$ である.

定理1.34より任意の F 係数多項式 $f(x)$ を分解する F の拡大体 K が存在する. $\alpha_1, ..., \alpha_n$ を K における $f(x)$ の根とすると $E = F(\alpha_1, ..., \alpha_n)$ は $f(x)$ を分解する極小の F の拡大体である. すなわち E の 真部分体では $f(x)$ は分解しない.

定理 1.38 ([5, 10章, 定理48]) 任意の F 係数多項式に対して F 上の分解体が存在する.

以下, 分解体の一意性について述べる.

補題 1.39 ([5, 10章, 補題50]) $\sigma^* : F[x] \ni \sum r_i x^i \mapsto \sum \sigma(r_i)x^i \in \bar{F}[x]$ を体同型 $\sigma : F \to \bar{F}$ から導かれる環同型とする. $p(x) \in F[x]$ が F 上既約のとき, $p^*(x) = \sigma^*(p(x)) \in \bar{F}[x]$ も $\bar{F}$ 上既約となる. また β を $p(x)$ の根, β^* を $p^*(x)$ の根とすると, σ を拡張する同型 $\hat{\sigma} : F(\beta) \to \bar{F}(\beta^*)$ で $\hat{\sigma}(\beta) = \beta^*$ となるものが唯一つ存在する.

Proof $\sigma^* : F[x] \to \bar{F}[x]$ が環同型であることから, 定理1.27を $(\sigma^*)^{-1}$ に適用すれば $p^*(x)$ の既約であることが導かれる. 一方, 環同型 $\sigma^* : F[x] \to \bar{F}[x]$ によって, イデアル $(p(x))$ はイデアル $(p^*(x))$ に移る. 従って σ^* から体の同型 $\psi : F[x]/(p) \to \bar{F}[x]/(p^*)$ が誘導される. ψ は

$$\psi(c + (p)) = \sigma(c) + (p^*), \qquad \psi(x + (p)) = x + (p^*)$$

を満たす. ここで定理 1.36,(3) の同型に注意すれば

$$F(\beta) \longmapsto F[x]/(p) \xrightarrow{\psi} \bar{F}[x]/(p^*) \longmapsto \bar{F}(\beta^*)$$

を合成した同型 $\hat{\sigma}$ が得られ, 補題の条件を満たす. σ の拡張で $\hat{\sigma}(\beta) = \beta^*$ となるものが唯一つであることは明らかである. ∎

定理 1.40 ([5, 10章, 定理51]) $\sigma : F \to \bar{F}$ を体同型, $\sigma^* : F[x] \to \bar{F}[x]$ を σ から導かれる環同型とする. $f(x) \in F[x]$ の F 上の分解体を E, $f^*(x) = \sigma^*(f(x)) \in \bar{F}[x]$ の $\bar{F}$ 上の分解体を $\bar{E}$ とすれば次が成り立つ.

(1) σ を拡張する同型 $\tilde{\sigma} : E \to \bar{E}$ が存在する.

(2) $f(x)$ の根が互いに異なるとき, $[E : F]$ 個の σ の拡張 $\tilde{\sigma}$ が存在する.

Proof (1) $[E : F]$ についての帰納法で証明する. $[E : F] = 1$, すなわち $E = F$ のとき $f(x)$ は $F[x]$ において1次因子の積になる. このとき $f^*(x)$ も $\bar{F}[x]$ において1次因子の積となるから $\bar{E} = \bar{F}$ となる. 従って $\tilde{\sigma} = \sigma$ とすればよい.

$[E : F] > 1$ のとき, $f(x)$ の2次以上の既約因子 $p(x)$ を選び, $p(x)$ の1つの根を $\beta (\in E)$ とする. $p^*(x) \in \bar{F}[x]$ を $p(x)$ に対応する既約多項式として, $\beta^* \in \bar{E}$ を $p^*(x)$ の根とす

る. 補題 1.39 より σ を拡張する同型 $\hat{\sigma}: F(\beta) \to \bar{F}(\beta^*)$ で, $\hat{\sigma}(\beta) = \beta^*$ となるものが存在する. E は $F(\beta)$ 上の $f(x)$ の分解体で $\bar{E}$ は $\bar{F}(\beta^*)$ 上の $f^*(x)$ の分解体である. また $[E:F] = [E:F(\beta)][F(\beta):F]$ であるが $[F(\beta):F] \geq 2$ より $[E:F] > [E:F(\beta)]$ である. 従って帰納法の仮定より $\hat{\sigma}$ の拡張 $\tilde{\sigma}: E \to \bar{E}$ が存在するが, $\hat{\sigma}$ は σ の拡張であったから $\tilde{\sigma}$ は σ の拡張である.

(2) ここでも $[E:F]$ についての帰納法を用いる. $[E:F] = 1$, すなわち $E = F$ のとき, σ の拡張は σ の 1 個のみであるから, この場合は成り立つ.

$[E:F] > 1$ のとき, $f(x)$ は次数が 2 以上の既約因子 $p(x)$ をもつ. ここで $\partial(p) = d$ とおき, $p(x)$ の 1 つの根を β とする. $\tilde{\sigma}$ が σ の E への任意の拡張であれば, $\tilde{\sigma}(\beta) = \beta^*$ は $p^*(x)$ の根になる. $f^*(x)$ の根はすべて異なるので, $p^*(x)$ は $\bar{E}$ にちょうど d 個の根をもつ. 補題 1.39 より σ の $F(\beta)$ への拡張 $\hat{\sigma}$ が d 個存在する. E は $F(\beta)$ 上の $f(x)$ の分解体で, $\bar{E}$ は $\bar{F}(\beta^*)$ 上の $f^*(x)$ の分解体である. また $[E:F(\beta)] = [E:F]/d$ であるから, 帰納法の仮定より d 個のおのおのの拡張 $\hat{\sigma}$ に対して, ちょうど $[E:F(\beta)] = [E:F]/d$ 通りの E への拡張が存在する. 従って σ の E への拡張は $[E:F]$ 個存在する.

逆に σ の任意の拡張 $\tau: E \to \bar{E}$ を $F(\beta)$ に制限すれば上述の d 個のいずれかになる. 従って τ はこれを E に拡張したものであるから上の $[E:F]$ 個のいずれかに一致する. ゆえに σ の拡張はちょうど $[E:F]$ 個ある. ∎

系 1.41 任意の F 係数多項式 $f(x)$ に対して, その分解体は互いに F 同型である.

Proof $\bar{F} = F$, σ を F の恒等写像として定理 1.40 を適用すればよい. ∎

定義 1.42 $f(x) \in F[x]$ が $(x-\alpha)^2$ を因子にもつとき, $f(x)$ は重根をもつという. 重根をもたないとき, $f(x)$ は F 上分離的であるという.

F 係数既約多項式 $p(x)$ の導関数 $p'(x)$ が 0 でないとする. このとき $\partial(p') < \partial(p)$ が成り立つ. また p の既約性から p と p' は 1 次以上の共通因子を持たない. ゆえに $p(x)$ は分離的である. これより F の標数が 0 のとき F 係数既約多項式はすべて分離的であることがわかる.

2章　S_5 の可解な可移部分群

方程式の Galois 群は根の置換群と見なすことができる．Abel により証明された一般 5 次方程式の非可解性は 5 次対称群 S_5 の非可解性に由来する．また，本論文のテーマである可解な 5 次方程式の Galois 群は S_5 の可解な可移部分群となる．この章では後章で必要となる対称群，および可解群に関する定理を証明し，S_5 の可解な可移部分群を決定する．§2.1 では対称群，交代群を定義し，対称群の生成系を求め，交代群が 3-cycle で生成されること，5 次の交代群が単純群であることなどを示す．また，§2.2 では可解群の基本事項について説明する．最後の §2.3 では $n \geq 5$ のとき S_n が非可解であることを証明し，S_5 の可解な可移部分群の位数が 5, 10, 20 のいずれかになること，逆にこれらを位数とする部分群が可解な可移部分群であることを証明する．

2.1　対称群と交代群

集合 X からそれ自身への全単射を X 上の置換といい，X 上の置換全体のなす集合を S_X と表す．S_X の 2 元 σ, τ の積 $\sigma\tau$ を $x \in X$ に対して $\sigma\tau(x) = \sigma(\tau(x))$ により定まる置換と定義すれば，S_X はこの積に関して群となる．S_X を X 上の対称群という．S_X の単位元は恒等写像 1 である．

X が n 個の元からなる有限集合のとき，$X = \{1, ..., n\}$ としてよい．このとき S_X を n 次対称群といい S_n と表す．$|S_n| = n!$ である．

S_n の元 σ を

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

と表す．このとき

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

である．

S_n の元 σ が，相異なる m 個の文字 $a_1, ..., a_m$ に対して置換 $\begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$ を引き起

こし, 他の文字をすべて固定するとき, 長さ m の巡回置換, または単に m-cycle といい, $\sigma = (a_1, \ldots, a_m)$ と表す. 特に 2-cycle を互換という.

次の補題は容易に導くことができる (証明略).

補題 2.1 (1) $\sigma = (a_1, \ldots, a_m)$ の位数は m である.

(2) $\sigma \in S_n$, $\tau = (a_1, \ldots, a_m)$ のとき $\sigma\tau\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_m))$ である.

(3) $(a_1, a_2, \ldots, a_m) = (a_1, a_m) \cdots (a_1, a_3)(a_1, a_2)$ である.

cycle は上の補題の (3) より互換の積として表される. 一方, 任意の置換は互いに共通文字を含まない cycle の積に分解される. 例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 6 & 7 & 5 \end{pmatrix} = (1,2,3)(4)(5,6,7) = (1,2,3)(5,6,7)$$

である. 従って任意の置換は互換の積として表される. ここで置換を互換の積として表す仕方は何通りもあるが, 現れる互換の個数の偶奇性は一定である. 偶数個の互換の積として表される置換を偶置換, 奇数個の互換の積として表される置換を奇置換という ([3, pp.6-9]).

なお, 上のように置換を互いに共通文字を含まない cycle の積に分解することを cycle 分解という. 補題 2.1, (3) より次の補題が得られる.

補題 2.2 S_n は互換により生成される.

系 2.3 (1) S_n は $(1,2)$, $(1,3)$,...,$(1,n)$ により生成される.

(2) S_n は $(1,2)$, $(2,3)$, ..., $(n-1,n)$ により生成される.

(3) S_n は $(1,2)$, $(1,\ldots,n)$ により生成される.

(4) S_n は $(1,2)$, $(2,\ldots,n)$ により生成される.

Proof (1) $i \neq j$ がともに 1 と異なるとき, 互換 (i,j) が $(i,j) = (1,i)(1,j)(1,i)$ と表されることから, 任意の置換が $(1,2)$, $(1,3)$,...,$(1,n)$ の積として表される. 従って任意の置換が $\langle (1,2), (1,3), \ldots, (1,n) \rangle$ に含まれるので, $S_n = \langle (1,2), (1,3), \ldots, (1,n) \rangle$ が成り立つ.

(2) $1, i, j$ が互いに異なるとき $(1,j) = (i,j)(1,i)(i,j)$ であるから

$$(1,3) = (2,3)(1,2)(2,3),\ (1,4) = (3,4)(1,3)(3,4),\ \ldots,\ (1,n) = (n-1,n)(1,n-1)(n-1,n)$$

が成り立つ. 従って $(1,i)$ $(2 \leq i \leq n)$ はすべて $(1,2)$, $(2,3)$, ..., $(n-1,n)$ の積として表

される. ゆえに

$$S_n = \langle (1,2),(1,3),...,(1,n) \rangle \subseteq \langle (1,2),(2,3),...,(n-1,n) \rangle$$

となるので $S_n = \langle (1,2),(2,3),...,(n-1,n) \rangle$ が成り立つ.

(3) $\sigma = (1,2), \tau = (1,2,\ldots,n)$ とおくと

$$\tau\sigma\tau^{-1} = (2,3),\ \tau^2\sigma\tau^{-2} = (3,4),\ .....,\ \tau^{n-2}\sigma\tau^{-(n-2)} = (n-1,n)$$

となることから

$$S_n = \langle (1,2),(2,3),...,(n-1,n) \rangle \subseteq \langle \sigma, \tau \rangle$$

を得る. よって $S_n = \langle \sigma, \tau \rangle$ が成り立つ.

(4) $\sigma = (1,2), \rho = (2,3,\ldots,n)$ とおくと

$$\rho\sigma\rho^{-1} = (1,3),\ \rho^2\sigma\rho^{-2} = (1,4),\ .....,\ \rho^{n-2}\sigma\rho^{-(n-2)} = (1,n)$$

が成り立つ. 従って

$$S_n = \langle (1,2),(2,3),...,(n-1,n) \rangle \subseteq \langle \sigma, \rho \rangle$$

より $S_n = \langle \sigma, \rho \rangle$ が得られる. ∎

補題 2.4 p を素数とする. S_p の部分群 H が 1 つの互換と 1 つの p -cycle を含めば, $H = S_p$ である.

Proof 一般性を失うことなく H に含まれる互換を $\sigma = (1,i)$, p -cycle を $\tau = (1,j_2,...,j_p)$ としてよい. $\tau, \tau^2, ..., \tau^{p-1}$ の中に $(1,i,k_3,\ldots,k_p)$ なる形のものが現れるから $\sigma = (1,2)$, $\tau = (1,2,\ldots,p)$ としてよい. このとき, 系 2.3 より $H = S_p$ が成り立つ. ∎

S_n の偶置換全体のなす集合を A_n とおき n 次交代群という. 偶置換と偶置換の積が偶置換であることから A_n は S_n の部分群である. σ が偶置換のとき $\varphi(\sigma) = 1$, 奇置換のとき $\varphi(\sigma) = -1$ と $\varphi : S_n \to \{\pm 1\}$ を定義すれば φ は準同型である. ここで $Ker(\varphi) = A_n$ であるから $A_n \trianglelefteq S_n$ である. また $n \geq 2$ のとき $Im(\varphi) = \{\pm 1\}$ となるから $S_n/A_n \simeq \{\pm 1\}$ が成り立つ. これより $[S_n : A_n] = 2$, すなわち $|A_n| = \frac{n!}{2}$ が得られる.

補題 2.5 $n \geq 3$ のとき A_n は 3 -cycle により生成される.

Proof A_n の任意の元は偶数個の互換の積で表される. 互換 2 つの積が 1 でないときは

$(i,j)(k,l)$ か $(i,j)(j,k)$ のいずれかである. ただし, i, j, k, l は互いに異なるとする. ここで

$$(i,j)(k,l) = (i,j,k)(j,k,l), \qquad (i,j)(j,k) = (i,j,k)$$

が成り立つことから A_n の任意の元は 3 -cycle の積として表される. ゆえに A_n は 3 -cycle で生成される. ∎

群の集合への作用

群 G の元 g と 集合 X の元 x に対して X の元 $g(x)$ が定まり, 次の条件を満たすとき, X を G-set という. またこのとき G は X に作用するという.

(1) 任意の $g, h \in G$ と任意の $x \in X$ に対して $h((g(x))) = (hg)(x)$.

(2) 任意の $x \in X$ に対して $1(x) = x$.

G-set X の元 x に対して

$$\mathcal{O}(x) = \{g(x) \mid g \in G\}$$

を x を含む G-軌道という. また

$$G_x = \{g \in G \mid g(x) = x\}$$

は G の部分群になる. G_x を x の固定群という.

$X = \mathcal{O}(x)$ となる $x \in X$ が存在するとき, X を可移な G-set という. またこのとき G は X に可移に作用するという. X が可移な G-set であることと, X の任意の 2 元 x, y に対して $g(x) = y$ となる $g \in G$ が存在することとは同値である.

群 G の集合 G への作用を, 群 G の元 g と集合 G の元 x に対して, g による共役をとる操作 $g(x) = gxg^{-1}$ と定めれば, これは群 G の集合 G への作用となる. このときの $x \in G$ を含む軌道を x を含む共役類という. また x の固定群

$$\{g \in G \mid x = gxg^{-1}\}$$

を x の中心化群といい $C_G(x)$ と表す.

同様に G は G の部分群全体のなす集合に共役をとる操作で作用する. このときの H の固定群

$$\{g \in G \mid gHg^{-1} = H\}$$

を H の正規化群といい $N_G(H)$ と表す.

定理 2.6 ([5, 付録 B, 定理 G.10]) 有限群 G が集合 X に作用しているとする. このとき $x \in X$ に対して

$$|\mathcal{O}(x)| = [G : G_x] = \frac{|G|}{|G_x|}$$

が成り立つ. 特に $|X| = n$ で, G が可移に作用しているときは $|G| = n|G_x|$ が成り立つ.

定理 2.6 から有限群 G がそれ自身に共役により作用する場合に, 定理 2.6 を適用すると

$$x \text{ を含む共役類の元の個数} = [G : C_G(x)]$$

が成り立つ. また G が部分群全体の集合に共役で作用する場合に適用すると

$$H \text{ に共役な部分群の個数} = [G : N_G(H)]$$

が成り立つ.

可移群

対称群 S_X の部分群を X 上の置換群という. X 上の置換群 G は自然に X に作用する. この作用が可移であるとき G を X 上の可移群という.

S_n の元 σ が生成する巡回部分群 $\langle\sigma\rangle$ が X 上の可移群であることと, σ が n -cycle であることとは同値である. また定理 2.6 より S_n の可移部分群の位数は n の倍数である.

定理 2.7 S_n の可移部分群 G が $(n-1)$-*cycle* と互換を含めば $G = S_n$ である.

Proof S_n の可移部分群 G に含まれる $(n-1)$-cycle を $\sigma = (2, 3, \ldots, n)$, 互換を $\tau = (i, j)$ として一般性を失わない. G の可移性より $\rho(i) = 1$ となる $\rho \in G$ が存在する. このとき $\delta = \rho\tau\rho^{-1} = (1, k)$ が G に含まれる. このとき G は $\sigma^l\delta\sigma^{-l} \in G$, $(l = 1, 2, ..., n-1)$ の形の元を含むことから互換 $(1,2)$, $(1,3)$, ...,$(1,n)$ をすべて含む. 従って, 系 2.3 より $G = S_n$ である. ∎

A_5 の単純性

補題 2.8 すべての 3 -cycle は A_5 で共役である.

Proof S_5 に 3 -cycle は $5 \times 4 \times 3/3 = 20$ 個存在する. 補題 2.1 (2) より, S_5 の 3 -cycle 全体は 1 つの共役類をなす. $\sigma = (1, 2, 3)$ とおくと $[S_5 : C_{S_5}(\sigma)] = 20$ より $|C_{S_5}(\sigma)| = 6$ で

ある. ここで

$$C_{S_5}(\sigma) = \{1, \sigma, \sigma^2, (4,5), (4,5)\sigma, (4,5)\sigma^2\}$$

であることから $|C_{A_5}(\sigma)| = 3$ である. 従って $[A_5 : C_{A_5}(\sigma)] = 20$ となり, A_5 における σ を含む共役類は 20 個の元を含む. すなわち S_5 の共役類に一致する. ゆえにすべての 3 -cycle は A_5 において互いに共役である. ∎

定理 2.9 A_5 は単純群である.

Proof $H \neq 1$ を A_5 の正規部分群とする. H の元の A_5 における共役はすべて H の元であることを注意しておく. H の元 $\sigma \neq 1$ を任意に選ぶ. 適当に共役を選び直すと, σ の cycle 分解は $(1,2,3)$, $(1,2)(3,4)$, $(1,2,3,4,5)$, $(1,2,3,5,4)$ のいずれかとなる. $\sigma = (1,2,3)$ のときは補題 2.8 より H にすべての 3 -cycle が含まれ, 補題 2.5 より $H = A_5$ が得られる.

$\sigma = (1,2)(3,4)$ のとき, $\tau = (1,2)(3,5)$ とおくと

$$\tau\sigma\tau^{-1} = (1,2)(4,5) \in H \quad \text{より} \quad (\tau\sigma\tau^{-1})\sigma = (3,5,4) \in H$$

となることから $H = A_5$ が得られる.

$\sigma = (1,2,3,4,5)$ のとき $\tau = (1,3,2)$ に対して $\tau\sigma\tau^{-1} = (3,1,2,4,5) \in H$ となる. これより $(\tau\sigma\tau^{-1})\sigma^{-1} = (1,3,4) \in H$ が得られ, $A_5 = H$ が成り立つ.

$\sigma = (1,2,3,5,4)$ のときも $\tau = (1,3,2)$ に対して $(\tau\sigma\tau^{-1})\sigma^{-1} = (1,3,5) \in H$ となり, $A_5 = H$ が得られる.

以上から A_5 の正規部分群は 1 または A_5 自身であることが示されたので, A_5 は単純群である. ∎

A_n は $n \geq 5$ のとき常に単純群であることが知られている ([3, Chapter 3, Theorem 3.11]).

系 2.10 S_5 の正規部分群は 1, A_5, S_5 のみである.

Proof $H \neq 1$ を S_5 の正規部分群とすると $H \cap A_5 \trianglelefteq A_5$ が成り立つ. 定理 2.9 より A_5 が単純群であることから, $H \cap A_5 = 1$ または $H \cap A_5 = A_5$ が成り立つ.

$H \cap A_5 = A_5$ のとき, $A_5 \leq H$ となり $H = A_5$ または $H = S_5$ を得る.

$H \cap A_5 = 1$ のときは $h \notin A_5$ となる $h \in H$ が存在するので $HA_5 = S_5$ が成り立つ. ここで定理 1.7 より

$$|H| = \frac{|HA_5| \cdot |H \cap A_5|}{|A_5|} = \frac{|S_5|}{|A_5|} = 2$$

が成り立つ. ゆえに h は位数が 2 の奇置換であるから互換である. 適当に共役を選び $h = (1,2)$ としてよい. このとき $k = (1,2,3)$ に対して $khk^{-1}h = (1,3,2) \in H$ となり

$|H| = 2$ に矛盾が生じる. ゆえに $H \cap A_5 = 1$ は起こりえない. 以上より $H \neq 1$ が A_5 または S_5 であることが示された. ∎

2.2 可解群

群 G の部分群列

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$$

で $G_{i-1} \trianglerighteq G_i$ $(1 \leq i \leq n)$ を満たすものを G の正規列という.

G の2元 x, y に対して, $[x,y] = xyx^{-1}y^{-1}$ とおき, x と y の交換子という. また G の交換子すべてで生成された部分群を G の交換子群といい G' と表す.

$$G' = \left\langle [x,y] \,\middle|\, x, y \in G \right\rangle \quad \text{である.}$$

任意の $g \in G$ に対して $g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$ より $gG'g^{-1} \subseteq G'$ が成り立つ. ゆえに G' は G の正規部分群である.

補題 2.11 G の部分群 H について次は同値である.

(1) H は G' を含む.

(2) H は G の正規部分群であり, 剰余群 G/H は *Abel* 群である.

Proof (1)⇒(2) $h \in H$, $g \in G$ に対して $ghg^{-1} = (ghg^{-1}h^{-1})h$ が成り立つ. 仮定より $ghg^{-1}h^{-1} \in H$ であるから $ghg^{-1} \in H$ を得る. ゆえに $H \trianglelefteq G$ である. また $[y^{-1}, x^{-1}] = y^{-1}x^{-1}yx \in G' \subseteq H$ に注意すれば

$$(xH)(yH) = (xy)H = (xy\,[y^{-1}, x^{-1}])H = (yx)H = (yH)(xH)$$

が成り立つ. よって G/H はAbel群である.

(2)⇒(1) 剰余群 G/H がAbel群であることから, 任意の $x, y \in G$ に対して

$$(xy)H = (xH)(yH) = (yH)(xH) = (yx)H \quad \Longrightarrow \quad x^{-1}y^{-1}xy \in H$$

が成り立つ. 従って H は任意の交換子を含むので $G' \subseteq H$ が得られる. ∎

$G^{(0)} = G$, $G^{(1)} = G'$, $G^{(i+1)} = (G^{(i)})'$ $(i \geq 0)$ と定めて得られる G の部分群の列は, 上の補題より正規列

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots\cdots$$

をなす. これを G の交換子群列という. 交換子群列の剰余群 $G^{(i)}/G^{(i+1)}$ $(i \geq 0)$ は Abel 群である.

定理 2.12 群 G について次の 2 条件は同値である.

(1) G の正規列 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$ で G_{i-1}/G_i $(1 \leq i \leq n)$ がすべて *Abel* 群であるものが存在する.

(2) $G^{(t)} = \{1\}$ となる番号 t が存在する.

Proof (2)⇒(1) $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(t)} = 1$ は (1) の条件を満たす正規列である.

(1)⇒(2) $G_i \geq G^{(i)}$ が成り立つことを i についての帰納法で証明する. G/G_1 は Abel 群であるから補題 2.11 より $G_1 \geq G^{(1)}$ となり $i = 1$ のときは成り立つ. $i \geq 2$ として $i-1$ のときは成り立つと仮定すると, $G_{i-1} \geq G^{(i-1)}$ である. ここで $(G_{i-1})' \geq (G^{(i-1)})' = G^{(i)}$ であるが, G_{i-1}/G_i が Abel 群であるから $G_i \geq (G_{i-1})' \geq G^{(i)}$ が成り立つ. 従って i の場合も成り立つことが示された. ∎

定義 2.13 (可解群) 定理 2.12 の条件を満たす群 G を可解群という. またこのとき G は可解であるという.

定義より Abel 群は可解である.

系 2.14 可解群の部分群, 剰余群はそれぞれ可解群である.

Proof H を可解群 G の部分群とすると $H^{(i)} \leq G^{(i)}$ $(i \geq 0)$ が成り立つ. G が可解群であるから $G^{(t)} = 1$ となる番号 t が存在する. このとき $H^{(t)} \leq G^{(t)} = 1$ となるので H も可解群である.

可解群 G の正規部分群を N, $\varphi : G \to G/N$ を自然な準同型として, $G/N = \bar{G}$ とおく. $\bar{G}$ の交換子は $G'N/N$ に含まれるので $(\bar{G})' \leq G'N/N$ が成り立つ. 同様に

$$(\bar{G})^{(2)} \leq G^{(2)}N/N,\ (\bar{G})^{(3)} \leq G^{(3)}N/N,\ \ldots,(\bar{G})^{(t)} \leq G^{(t)}N/N = N$$

が成り立つので $\bar{G}$ も可解である. ∎

定理 2.15 N を群 G の正規部分群とする. このとき G が可解である条件は N, G/N がともに可解であることである.

Proof G が可解のときは系 2.14 より N, G/N は可解である. 逆に N, G/N が可解であるとすると, 定義より正規列

$$G/N \trianglerighteq G_1/N \trianglerighteq \cdots\cdots \trianglerighteq G_n/N = 1, \qquad N \trianglerighteq N_1 \trianglerighteq \cdots\cdots \trianglerighteq N_m = 1$$

で剰余群が Abel 群であるものが存在する. このとき正規列

$$G \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = N \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_m = 1$$

の剰余群が Abel 群となるので G は可解である. ∎

補題 2.16 有限 *Abel* 群 $G \neq 1$ は素数指数の正規部分群を含む.

Proof $|G|$ の素因数の個数 k についての帰納法で証明する. $k = 1$ のときは 1 が素数指数の部分群である. $k > 1$ として $k-1$ のときは成り立つと仮定する. $|G|$ を割り切る素数 p を 1 つ選ぶと, Cauchy の定理より位数 p の元 g が存在し, $H = \langle g \rangle$ は G の真の正規部分群になる. 従って剰余群 G/H には帰納法の仮定から素数指数の部分群 M/H が存在する. このとき M は G の素数指数の部分群である. ∎

定理 2.17 有限群 $G \neq 1$ が可解となるための条件は, G の正規列

$$G = N_0 \trianglerighteq N_1 \trianglerighteq \cdots\cdots \trianglerighteq N_m = 1$$

で, 剰余群 N_{i-1}/N_i $(1 \leq i \leq m)$ が素数位数の巡回群となるものが存在することである.

Proof G に定理の条件を満たす正規列が存在すれば, 定義より G は可解である.

逆に有限群 $G(\neq 1)$ が可解群であるとして, 定理の条件を満たす正規列が存在することを G の位数に関する帰納法で証明する. G が素数位数のときは明らかに成り立つ. G の位数が合成数とすると, 可解群の定義から G の正規列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots\cdots \trianglerighteq G_n = 1$$

で, 剰余群 G_{i-1}/G_i $(1 \leq i \leq n)$ が Abel 群であるものが存在する. ここで $G \gneq G_1$ であるとしてよい. 補題 2.16 より G/G_1 の部分群 N_1/G_1 で指数が素数のものが存在する. N_1 に帰納法の仮定を適用すれば, 正規列

$$N_1 \trianglerighteq N_2 \trianglerighteq \cdots\cdots \trianglerighteq N_m = 1$$

で剰余群 N_{i-1}/N_i $(1 \leq i \leq m)$ が素数位数の巡回群であるものが存在する. このとき正規列

$$G = N_0 \trianglerighteq N_1 \trianglerighteq \cdots\cdots \trianglerighteq N_m = 1$$

は定理の条件を満たす G の正規列である. ∎

定理より次の系が得られる.

系 2.18 可解群は素数指数の正規部分群を含む.

定理 2.19 2 面体群は可解である.

Proof G を次の条件を満たす元 a,b で生成される位数 $2n$ の 2 面体群とする.

$$|a| = n \ \ (n \geq 2), \quad |b| = 2, \quad bab = a^{-1}$$

このとき $N = \langle a \rangle$ は指数 2 の正規部分群であり, 正規列 $G \trianglerighteq N \trianglerighteq 1$ の剰余群は巡回群となる. ゆえに G は可解である. ∎

p 群の可解性

群 G に対して

$$Z(G) = \{g \in G \mid \text{任意の } x \in G \text{ に対して } gx = xg\}$$

を G の中心という. $Z(G)$ は G の可換な正規部分群である. また $g \in Z(G)$ に対して $xgx^{-1} = g$ が任意の $x \in G$ について成り立つから, g の共役は g のみである.

補題 2.20 $G \neq 1$ が p 群のとき $Z(G) \neq 1$ である.

Proof $G = Z(G) \cup C_1 \cup \cdots \cup C_n$ を G の共役類への分割とする. ここで C_i $(1 \leq i \leq n)$ は元の個数が 1 より大きい共役類とする. p.22 で示したように, $x_i \in C_i$ とすると $|C_i| = [G : C_G(x_i)]$ が成り立つ. 従って

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)]$$

が得られる. ここで Lagrange の定理より各 i に対して $[G : C_G(x_i)]$ は p の倍数である. 従って p は, $|Z(G)|$ を割り切ることになり, $Z(G) \neq 1$ が導かれる. ∎

定理 2.21 p 群は可解である.

Proof p 群 G の位数に関する帰納法で示す. $G = 1$ のときは明らかに可解である. 次に $|G| > 1$ とすると, 補題 2.20 より $Z(G) \neq 1$ である. $Z(G) = G$ ならば G は Abel 群であるから可解である. $Z(G) \neq G$ とすると 剰余群 $G/Z(G)$ は帰納法の仮定より可解である. $Z(G)$ も可解であるから, 定理 2.15 より G は可解である. 以上で定理が証明された. ∎

2.3 S_5 の可解な可移部分群

定理 2.22 S_n は $1 \leq n \leq 4$ のとき可解, $n \geq 5$ のとき可解でない.

Proof $m < n$ のとき S_m は S_n の部分群に同型である. 従って S_n が可解のとき S_m も可解である. ゆえに S_4 が可解であり, S_5 が非可解であることを示せばよい. ここで

$$V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

とおくと $V \trianglelefteq S_4$ であり, 正規列 $S_4 \rhd A_4 \rhd V \rhd 1$ において, 剰余群 S_4/A_4, A_4/V, $V/1$ の位数は, それぞれ 2, 3, 4 となる. 従って剰余群はすべて Abel 群である. ゆえに S_4 は可解である. 次に S_5 が可解であると仮定すると, その部分群 A_5 も可解となる. A_5 は単純群であるから正規列は $A_5 \rhd 1$ のみであり, 剰余群 $A_5/1 \simeq A_5$ が Abel 群でないことから矛盾が生じる. ゆえに S_5 は可解でない. ∎

上の証明中, A_5 の非可解であることが示されていることに注意されたい.

補題 2.23 H を群 G の指数 n の部分群とすれば $Ker(\varphi) \leq H$ となる準同型 $\varphi : G \to S_n$ が存在する.

Proof $\mathcal{H}$ を G における H の (左) 剰余類全体のなす集合とする. G の元 a に対して

$$\varphi_a : \mathcal{H} \ni gH \longmapsto agH \in \mathcal{H}$$

と定義すれば φ_a は $\mathcal{H}$ 上の置換を引き起こす. 従って写像

$$\varphi : G \ni a \longmapsto \varphi_a \in S_{\mathcal{H}}$$

が定まる. $a, b \in G$ に対して

$$\varphi_{ab}(gH) = (ab)gH = a(bg)H = \varphi_a(bgH) = \varphi_a(\varphi_b(gH)) = \varphi_a\varphi_b(gH)$$

より $\varphi_{ab} = \varphi_a\varphi_b$, すなわち $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つから φ は準同型である. また $a \in Ker(\varphi)$ とすると, 任意の gH に対して $agH = gH$, 特に $aH = H$ が成り立つことから $a \in H$ が得られる. ゆえに $Ker(\varphi) \leq H$ である. 以上で $Ker(\varphi) \leq H$ となる準同型 $\varphi : G \to S_{\mathcal{H}}$ の存在が示された. 一方 $|\mathcal{H}| = n$ より $S_{\mathcal{H}}$ は S_n と同一視できるので, 定理の主張が導かれる. ∎

補題 2.24 指数が 4 以下の可解部分群をもつ群は可解である.

Proof 群 G に指数 $k(\leq 4)$ の可解な部分群 H があるとする. このとき補題 2.23 より $Ker(\varphi) \leq H$ となる準同型 $\varphi : G \to S_k$ が存在する. G の正規列 $G \trianglerighteq Ker(\varphi) \trianglerighteq 1$ において $Ker(\varphi)$ は可解群 H の部分群であるから可解, $G/Ker(\varphi)$ は S_k の部分群に同型であるから定理 2.22 より可解である. ゆえに定理 2.15 より G は可解である. ∎

補題 2.25 S_5 は位数 30, 40 の部分群をもたない.

Proof H を位数 30 の S_5 の部分群とする. このとき $[S_5 : H] = 4$ となるから, 補題 2.23 より $Ker(\varphi) \leq H$ となる準同型 $\varphi : S_5 \to S_4$ が存在する. ここで $Ker(\varphi)$ は S_5 の正規部分群で, 系 2.10 よりその位数は, 1, 60, 120 のいずれかである. 一方 $|H| = 30$ であるから $Ker(\varphi) = 1$ となる. 従って φ が S_5 から S_4 への単射となり, 矛盾が生じる. $|H| = 40$ と仮定しても同様である. ∎

補題 2.26 位数 24 以下の群は可解である.

Proof 定理 2.21 より, 位数が素数のベキである群は可解である. 位数 $2p$ (p は素数) の群は定理 1.13 より 2 面体群であるか巡回群である. 従って定理 2.19 より可解である. また位数が $q < p$ かつ $q \nmid p - 1$ を満たす 2 つの素数の積 pq である群は定理 1.13 より巡回群となり, 可解である. 残りの 24 以下の自然数は 12, 18, 20, 21, 24 である.

$|G| = 12$ のときは Sylow 2 部分群の指数が 3 となる. $|G| = 18$ のときは Sylow 3 部分群の指数が 2 となる. $|G| = 20$ のときは Sylow 5 部分群の指数が 4 となる. $|G| = 21$ のときは Sylow 7 部分群の指数が 3 となる. $|G| = 24$ のときは Sylow 2 部分群の指数が 3 となる. いずれの場合も補題 2.24 より可解となる. ∎

一般に位数が 60 より小さい群は可解であることが知られている.

定理 2.27 S_5 の部分群 H が可解であるための条件は H の位数が 24 以下になることである.

Proof 位数 24 以下の群が可解であることは補題 2.26 で示した. 次に H を位数が 24 より大きい S_5 の部分群とする. H の位数は 120 の約数で 24 より大きいので, $|H| = 30$, 40, 60, 120 のいずれかが成り立つ. S_5 に位数 30, 40 の部分群は存在しない. また位数 60 の部分群は A_5, 位数 120 の部分群は S_5 自身であるが, これらは可解でない. よって S_5 の可解な部分群の位数は 24 以下である. ∎

定理 2.6 より S_5 の可移部分群の位数は 5 の倍数である. これより次の系が得られる.

系 2.28 S_5 の可移部分群が可解である条件は位数が 20 以下となることである.

S_5 の部分群 F_{20}, F_{10}, F_5 を

$$F_{20} = \langle (1,2,3,4,5), (2,3,5,4) \rangle, \quad F_{10} = \langle (1,2,3,4,5), (2,5)(3,4) \rangle, \quad F_5 = \langle (1,2,3,4,5) \rangle$$

とおく. F_5 は S_5 および F_{20} の Sylow 5 部分群である. p.22 で述べたように, F_{20} における F_5 の共役の個数は $[F_{20} : N_{F_{20}}(F_5)]$ に一致する. これは $[F_{20} : F_5] = 4$ の約数であり, Sylow の定理 (定理 1.10) より 5 を法として 1 に合同であるから 1 となる. 従って F_5 は F_{20} の正規部分群である.

同様に考えて, S_5 における F_5 の共役の個数は $[S_5 : F_{20}] = 6$ の約数で, 5 を法として 1 に合同であるから 1 または 6 となる. 1 でないことは容易に確かめられるので, 6 である. これより S_5 における F_5 の正規化群が F_{20} であることがわかる. ゆえに F_{20} に同型な S_5 の部分群は, ある Sylow 5 部分群の正規化群となり, Sylow の定理より, すべて互いに共役である. また F_{10} に同型な群は位数 10 の 2 面体群であり, Sylow 5 部分群の正規化群に含まれるので, F_{20} の部分群 F_{10} に共役である.

F_{20} には正規列

$$F_{20} \trianglerighteq F_5 \trianglerighteq 1$$

が存在し, その剰余群は巡回群である. ゆえに F_{20} は可解であり, その部分群 F_{10}, F_5 も可解である. これらの群は 4 章で再び登場する.

定理 2.29 S_5 の可解な可移部分群 G は F_{20}, F_{10}, F_5 のいずれかに共役である.

Proof F_{20}, F_{10}, F_5 は 5-cycle を含むので可移である. また可解であることも上で示した. ゆえに F_{20}, F_{10}, F_5 は S_5 の可解な可移部分群である.

逆に, G を S_5 の可解な可移部分群とすると, G の位数は 5 の倍数 (定理 2.6) かつ 120 の約数である. また系 2.28 より G の位数は 24 以下である. 従って 5, 10, 15, 20 のいずれかである.

$|G| = 5$ のとき, G は S_5 の Sylow 5 部分群であるから F_5 に共役である.

$|G| = 10$ のとき, 定理 1.13 より G は 2 面体群 D_{10} か巡回群 $\mathbb{Z}_{10}$ に同型である. S_5 は位数 10 の置換を含まないので $G \simeq D_{10} \simeq F_{10}$ が成り立つ. ゆえに G は F_{10} に共役である.

$|G| = 15$ と仮定すると, 定理 1.13 より G は巡回群 $\mathbb{Z}_{15}$ に同型となる. これは S_5 が位数 15 の置換を持たないことに矛盾する.

$|G| = 20$ のとき, G の Sylow 5 部分群 P は G の正規部分群である. ゆえに G は Sylow 5 部分群の正規化群に一致する. 従って F_{20} に共役である. ∎

3章 Galois 理論

この章では Galois 理論について説明する. 方程式に Galois 群が対応し, 方程式がベキ根で解けるかどうかが, その Galois 群が可解であるかどうかで判定できるという Galois により得られた成果は, 現在では Galois 理論として知られている. n 次対称群は $n \leq 4$ のとき可解であるが, $n \geq 5$ のとき可解でないことが, 5 次以上の方程式に根の公式の存在しない理由である. 方程式の解法の本質が根の置換のなす群の構造にあることを見抜いた Galois の天才は, 今日の様々に脚色された文脈からも, 強く感じることができる.

§3.1 では, 体の拡大の自己同型群, 特に多項式の分解体の自己同型群について考察する. n 次多項式の分解体の自己同型群が n 次対称群の部分群に同型であること, その位数が拡大次数に一致することなどを証明する. §3.2 では, ベキ根拡大を定義し, 方程式がベキ根によって可解であることと, 方程式の分解体がベキ根拡大体に含まれることとが同値であることを示し, 可解な方程式の自己同型群が可解群になることを示す. §3.3 では, 不変体, Galois 拡大, Galois 群などの概念を導入し, Galois 拡大の中間体と Galois 群の部分群とが一対一に対応する, という Galois の基本定理を証明する. §3.4 では, 方程式がベキ根により可解であることと, その Galois 群が可解群であることとが同値であることを証明する. これより可解な既約 5 次方程式が, S_5 の可解な可移部分群を Galois 群にもつ方程式として特徴づけられる.

以下, 特に断らない限り, 体の標数は 0 であるとする. この仮定は既約多項式がすべて分離的であることを保証するためのものであり, 既約多項式が分離的である場合には, 標数が 0 でなくとも, この章で導かれた定理が成立することに注意されたい.

3.1 体の拡大の自己同型

体 E から E への同型を E の自己同型という. E の自己同型全体の集合は写像の合成を演算として群をなす. これを $Aut(E)$ と表し, E の自己同型群という. また拡大 E/F に

対して E の F (自己) 同型全体を $Aut(E/F)$ と表す. $Aut(E/F)$ は $Aut(E)$ の部分群である.

補題 3.1 E/F を体の拡大, $f(x)$ を F 係数多項式, $\sigma \in Aut(E/F)$ とする. このとき $f(x)$ の根 α に対して $\sigma(\alpha)$ もまた $f(x)$ の根である.

Proof $f(x) = c_0 + c_1x + \cdots + c_nx^n$ とする. このとき $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$ が成り立つことから

$$0 = \sigma(c_0 + c_1\alpha + \cdots + c_n\alpha^n) = c_0 + c_1\sigma(\alpha) + \cdots + c_n\sigma(\alpha)^n$$

が得られる. 従って $\sigma(\alpha)$ は $f(x)$ の根である. ∎

定理 3.2 F 係数 n 次多項式 $f(x)$ の分解体を E とすれば $Aut(E/F)$ は S_n の部分群に同型である.

Proof $X = \{\alpha_1, ..., \alpha_n\} \subseteq E$ を $f(x)$ の根全体のなす集合とする. 補題 3.1 より $\sigma \in Aut(E/F)$ に対して $\sigma(X) = X$ が成り立つ. 従って σ を X に制限する写像

$$\varphi : Aut(E/F) \ni \sigma \longmapsto \sigma|_X \in S_X$$

が定まる. φ は準同型であり, $\varphi(\sigma) = \sigma|_X = 1$ とすると σ は $\alpha_1, ..., \alpha_n$ を固定する. 一方 σ は F の各元を固定し $E = F(\alpha_1, ..., \alpha_n)$ であることから E の恒等写像となる. ゆえに $Ker(\varphi) = 1$ となるので, φ は単射である. よって $Aut(E/F)$ は S_X ($\simeq S_n$) の部分群に同型である. ∎

以下 $Aut(E/F)$ を方程式 $f(x) = 0$ の Galois 群, または, 方程式 $f(x) = 0$ の自己同型群, あるいは単に $f(x)$ の Galois 群という. 系 1.41 より, 方程式の Galois 群は分解体の選び方によらない.

定理 3.2 により, 4 次方程式の Galois 群を S_4 の部分群, 5 次方程式の Galois 群を S_5 の部分群と見なすことができる. 特にその位数は, それぞれ 24, 120 の約数である.

$\mathbb{C}$ は $f(x) = x^2 + 1 \in \mathbb{R}[x]$ の分解体である. 定理 3.2 より $|Aut(\mathbb{C}/\mathbb{R})| \leq 2$ が成り立つ. 一方 $Aut(\mathbb{C}/\mathbb{R})$ には恒等写像と複素共役をとる写像

$$\mathbb{C} \ni z = a + bi \longmapsto \bar{z} = a - bi \in \mathbb{C}$$

が存在する. ゆえに $|Aut(\mathbb{C}/\mathbb{R})| = 2$ である.

定理 3.3 E が F 係数多項式 $f(x)$ の分解体のとき $|Aut(E/F)| = [E : F]$ が成り立つ.

Proof　定理 1.40 において, $\sigma : F \to F$ を恒等写像, $\bar{E} = E$ とすればちょうど $[E : F]$ 個の E の F 自己同型が存在する. ∎

E を F 係数 n 次既約多項式 $f(x)$ の分解体, $\alpha \in E$ を $f(x)$ の根の 1 つとすれば, 定理 1.32, 定理 1.36 より

$$|Aut(E/F)| = [E : F] = [E : F(\alpha)]\,[F(\alpha) : F] = n\,[E : F(\alpha)]$$

が得られる. 従って $f(x)$ の Galois 群 $Aut(E/F)$ の位数は n の倍数である.

$g(x) = x^3 - 2 \in \mathbb{Q}[x]$ の実数根を α, 複素数 ω を 1 の原始 3 乗根とする. このとき $E = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega)$ は $g(x)$ の分解体である. $g(x)$ は $\mathbb{Q}$ 上既約であるから $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ である. $\alpha \in \mathbb{R}$ より $\mathbb{Q}(\alpha) \neq E$ となるので

$$|Aut(E/\mathbb{Q})| = [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] > 3$$

が成り立つ. 一方 $Aut(E/\mathbb{Q})$ は S_3 の部分群であるから $Aut(E/\mathbb{Q}) \simeq S_3$ が得られる.

補題 3.4 拡大 E/F の中間体 B が F 係数多項式 $f(x)$ の分解体であるとする. このとき $\sigma \in Aut(E/F)$ に対して $\sigma|_B \in Aut(B/F)$ が成り立つ.

Proof　$\sigma(B) = B$ を示せばよい. $f(x)$ の根を α_1,..., α_n とすれば $B = F(\alpha_1, ..., \alpha_n)$ である. σ は F 同型であるから, 補題 3.1 より, α_1,..., α_n の置換を引き起こす. ゆえに

$$\sigma(B) = \sigma(F(\alpha_1, ..., \alpha_n)) = F(\sigma(\alpha_1), ..., \sigma(\alpha_n)) = B$$

が成り立つ. ∎

定理 3.5 拡大 E/F の中間体を B とし, E, B がそれぞれ F 係数多項式 $g(x)$, $f(x)$ の分解体であるとする. このとき

$$Aut(E/B) \trianglelefteq Aut(E/F), \qquad Aut(E/F)/Aut(E/B) \simeq Aut(B/F)$$

が成り立つ.

Proof　補題 3.4 より写像 $\psi : Aut(E/F) \ni \sigma \mapsto \sigma|_B \in Aut(B/F)$ が定義でき, 準同型であることも容易に確かめることができる. ここで $Ker(\psi) = Aut(E/B)$ が成り立つので $Aut(E/B) \trianglelefteq Aut(E/F)$ が得られる. 一方, 定理 1.40 より $Aut(B/F)$ の任意の元 τ に対して τ の拡張である E の自己同型 $\tilde{\tau}$ が存在する. このとき $\tau = \tilde{\tau}|_B = \psi(\tilde{\tau})$ となるので ψ は全射である. 従って準同型定理より $Aut(E/F)/Aut(E/B) \simeq Aut(B/F)$ が成り立つ. ∎

定理 3.6 F 係数多項式 $f(x)$ の分解体を E とし, $G = Aut(E/F)$ とおく. このとき次は同値である.

(1) $f(x)$ は F 上既約である.

(2) G は $f(x)$ の根全体のなす集合に可移に作用する.

Proof $f(x)$ の根全体のなす集合を X とする. G が X 上の置換群と見なせることを注意しておく.

(1)⇒(2) $f(x)$ が F 上既約であると仮定する. 定理1.36 より $F(\alpha_i) \simeq F[x]/(f)$ となるので $F(\alpha_i)$ はすべて互いに F 同型である. 従って任意の i に対して $\sigma : F(\alpha_1) \to F(\alpha_i)$ となる F 同型 σ が存在する. 定理1.40 より σ は E の自己同型 $\hat{\sigma}$ に拡張できる. $\hat{\sigma} \in G$ より G は X 上可移である.

(2)⇒(1) G が X 上可移であり, $F[x]$ で $f(x) = g(x)h(x)$ $(\partial(g) \geq 1,\ \partial(h) \geq 1)$ と分解できたと仮定する. E は $f(x)$ の分解体であるから $E[x]$ で

$$g(x) = c\prod(x - \alpha_i), \qquad h(x) = d\prod(x - \beta_j)$$

と 1 次式の積に分解する. ただし $c, d \in F$ である. $f(x)$ は分離的であるから α_i, β_j は互いに異なる. 仮定より G が X 上可移群であるから $\sigma(\alpha_i) = \beta_j$ となる $\sigma \in G$ が存在する. これは補題 3.1 に矛盾する. 従って $f(x)$ は $F[x]$ で 1 次以上の 2 つの式の積に分解できない, すなわち既約である. ∎

3.2 ベキ根拡大

体 F の乗法群 $F^\sharp = F - \{0\}$ の有限部分群は巡回群である ([5, 12 章, 定理 62]). 従って 1 の n 乗根全体は巡回群をなす. F の標数は 0 であると仮定しているので 1 の n 乗根は n 個存在する.

定義 3.7 体 F における 1 の n 乗根全体のなす群の生成元を 1 の原始 n 乗根という.

以下 1 の (原始) n 乗根を, 単に (原始) n 乗根という.
環 R の単元全体のなす集合を $U(R)$ と表すことにすると

$$U(\mathbb{Z}_n) = \{\bar{i} \in \mathbb{Z}_n \mid (i, n) = 1\}$$

である. 特に p が素数のとき $U(\mathbb{Z}_p) = \mathbb{Z}_p^\sharp$ である.

定理 3.8 E は F の拡大体で $E=F(\zeta)$ となる 1 の 原始 n 乗根 ζ が存在するとする. このとき $Aut(E/F)$ は $U(\mathbb{Z}_n)$ の部分群と同型である. 特に $Aut(E/F)$ は $Abel$ 群である.

Proof $\sigma \in Aut(E/F)$ とすると σ は 1 の原始 n 乗根を 1 の原始 n 乗根に移すので, $\sigma(\zeta)=\zeta^i$ となる, n と互いに素な i が n を法として一意に定まる. これより写像 ψ を

$$\psi : Aut(E/F) \ni \sigma \longmapsto \bar{i} \in U(\mathbb{Z}_n)$$

と定義することができる. σ, τ が $\psi(\sigma)=\bar{i}, \psi(\tau)=\bar{j}$ であるとき

$$\sigma\tau(\zeta)=\sigma(\zeta^j)=\zeta^{ji}=\zeta^{ij}$$

となる. 従って

$$\psi(\sigma\tau)=\overline{ij}=\bar{i}\cdot\bar{j}=\psi(\sigma)\psi(\tau)$$

が成り立つので ψ は準同型である. ここで $\tau \in Ker(\psi)$ とすると $\psi(\tau)=\bar{1}$ となるので $\tau(\zeta)=\zeta$ が成り立つ. $E=F(\zeta)$ であるから τ は恒等写像である. ゆえに $Ker(\psi)=1$ が得られた. よって ψ は単射であるので, $Aut(E/F)$ は $U(\mathbb{Z}_n)$ の部分群に同型である. ∎

p が素数のとき, 系 1.29 より $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ は $\mathbb{Q}$ 上既約である. ζ を原始 p 乗根とすると, $\mathbb{Q}(\zeta)$ は $\Phi_p(x)$ の分解体である. 従って定理 3.3 より $|Aut(\mathbb{Q}(\zeta)/\mathbb{Q})|=[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$ が成り立つ. 一方, 定理 3.8 より $Aut(\mathbb{Q}(\zeta)/\mathbb{Q})$ は $U(\mathbb{Z}_p)$ の部分群に同型である. ここで $|U(\mathbb{Z}_p)|=|\mathbb{Z}_p^\sharp|=p-1$ より $Aut(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq \mathbb{Z}_p^\sharp$ が得られる.

定理 3.9 体 F は 1 の原始 n 乗根を含み, E は $f(x)=x^n-c \in F[x]$ の分解体であるとする. このとき, 単射準同型 $\psi : Aut(E/F) \to \mathbb{Z}_n$ が存在する. ここで $f(x)$ が既約であることと, ψ が全射であることとは同値である.

Proof F に含まれる 1 の原始 n 乗根を ζ とする. E が $f(x)$ の分解体であることから $f(\alpha)=0$ を満たす $\alpha \in E$ が存在する. このとき $\alpha^n=c$ に注意すれば $f(x)$ の根は $\alpha, \alpha\zeta,$ ..., $\alpha\zeta^{n-1}$ の n 個である. $\zeta \in F$ であるから $E=F(\alpha)$ が成り立つ.

$G=Aut(E/F)$ とおく. $\sigma \in G$ に対して $\sigma(\alpha)$ も $f(x)$ の根であるから $\sigma(\alpha)=\alpha\zeta^i$ と表すことができる. ここで i は n を法として一意に定まるので, 写像

$$\psi : G \ni \sigma \longmapsto \bar{i} \in \mathbb{Z}_n$$

が定義できる. $\sigma, \tau \in G$ が $\psi(\sigma) = \bar{i}$, $\psi(\tau) = \bar{j}$ を満たすとすると

$$\sigma\tau(\alpha) = \sigma(\alpha\zeta^j) = \alpha\zeta^i\zeta^j = \alpha\zeta^{i+j}$$

となる. 従って

$$\psi(\sigma\tau) = \overline{i+j} = \bar{i} + \bar{j} = \psi(\sigma) + \psi(\tau)$$

となるので ψ は準同型である. 次に $\tau \in Ker(\psi)$ とすると $\psi(\tau) = 0$ であるから $\tau(\alpha) = \alpha$ が成り立つ. 従って τ は恒等写像である. よって $Ker(\psi) = 1$ となるので ψ は単射である.

ψ が全射になるための条件は, 任意の i に対して, $\sigma(\alpha) = \alpha\zeta^i$ となる $\sigma \in G$ が存在することであるが, これは G が $f(x)$ の根全体のなす集合に可移に作用することを意味する. 一方, 定理 3.6 より G が $f(x)$ の根全体のなす集合に可移に作用することと, $f(x)$ が F 上既約であることとは同値であるから, 定理の主張が導かれる. ∎

定義 3.10 体 F の拡大体 E に $E = F(\alpha)$, $\alpha^m \in F$ を満たす元 α が存在するとき, 拡大 E/F を m 型純拡大という. 各々の拡大 B_{i+1}/B_i が純拡大である拡大列

$$B_0 \subseteq B_1 \subseteq \cdots\cdots \subseteq B_t$$

をベキ根拡大列という. 拡大 E/F に対して

$$F = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_t = E$$

を満たすベキ根拡大列が存在するとき, E/F をベキ根拡大という. またこのとき E を F のベキ根拡大体という.

ベキ根拡大が有限次拡大であることに注意されたい.

定義 3.11 $f(x) \in F[x]$ の分解体を E とする. E を含む F のベキ根拡大が存在するとき, 方程式 $f(x) = 0$ は F 上でベキ根によって可解であるという.

以下 $f(x) = 0$ がベキ根によって可解であることを, 単に方程式 $f(x) = 0$ が可解である, あるいは, $f(x)$ が可解である, などということにする.

定義より, 方程式 $f(x) = 0$ が F 上可解であるとは, そのすべての根が F のあるベキ根拡大 B に含まれることである. B の元は F の元から四則演算とベキ根をとる操作を有限回繰り返して得られる. 従って $f(x) = 0$ の根はすべて, F の元に四則演算, 根号を用いた形で表示されることになる.

p が素数, $n = p^m$ で, $F(\alpha)/F$ が n 型純拡大であるとき, 次のような p 型純拡大の列に細分できる.

$$F \subseteq F(\alpha^{p^{m-1}}) \subseteq \cdots\cdots \subseteq F(\alpha^p) \subseteq F(\alpha)$$

同様に一般の n 型純拡大も素数型純拡大の列に細分できる.

補題 3.12 B/F が有限次拡大のとき, B の拡大体 E で, ある $f(x) \in F[x]$ の F 上の分解体であるものが存在する.

Proof B/F は有限次拡大であるから代数拡大である. 従って $B = F(\alpha_1, ..., \alpha_n)$ と表すことができる. ここで各 α_i の F 上の最小多項式を $p_i(x)$, $f(x) = p_1(x) \cdots p_n(x)$ とおけば, $f(x)$ の F 上の分解体 E は B を含む. ∎

B, F, E, α_1,...,α_n, $p_1(x)$,...,$p_n(x)$ を補題 3.12 の証明中で定めたものとする. $p_k(x)$ の根を

$$\alpha_k = \alpha_k^{(1)}, \alpha_k^{(2)}, ..., \alpha_k^{(t_k)}$$

とおく. このとき

$$E = F(\alpha_1^{(1)}, ..., \alpha_1^{(t_1)}, ..., \alpha_n^{(1)}, ..., \alpha_n^{(t_n)})$$

である. 一方 $B = F(\alpha_1, ..., \alpha_n)$ であり, $Aut(E/F)$ は $p_k(x)$ の根のなす集合の上に可移に作用するから E は $\sigma(B)$ $(\sigma \in Aut(E/F))$ の合成体である. 従って $\sigma(B)$ $(\sigma \in Aut(E/F))$ から適当に $B_1, ..., B_r$ を選べば $E = B_1 \vee \cdots\cdots \vee B_r$ と表すことができる. ここで B/F がベキ根拡大であると仮定すると B_k/F はすべてベキ根拡大である. F に順次ベキ根を添加して B_k が得られることから, $B_1 \vee \cdots \vee B_{k-1}$ に順次ベキ根を添加して $B_1 \vee \cdots \vee B_{k-1} \vee B_k$ が得られる. 従って, 拡大

$$(B_1 \vee \cdots \vee B_{k-1} \vee B_k)/(B_1 \vee \cdots \vee B_{k-1})$$

はベキ根拡大となる. ゆえに E/F もベキ根拡大である. 以上から次の補題が得られる.

補題 3.13 ベキ根拡大 B/F に対して, B の拡大体 E で, ある $f(x) \in F[x]$ の F 上の分解体であり, F のベキ根拡大体であるものが存在する.

補題 3.14 可解な F 係数多項式 $f(x)$ の分解体を E とする．このとき，各々の拡大 R_i/R_{i-1} が素数 p_i 型純拡大であるようなベキ根拡大列

$$F = R_0 \subseteq R_1 \subseteq \cdots\cdots \subseteq R_t$$

で，$E \subseteq R_t$，かつ R_t がある F 係数多項式の F 上の分解体であるようなものが存在する．また，すべての i に対して F が 1 の原始 p_i 乗根を含むならば $Aut(E/F)$ は可解である．

Proof $f(x)$ が可解ならば，$E \subseteq B_s$ となる F のベキ根拡大体が存在する．このとき，補題 3.13 により，B_s の拡大体で，ある F 係数多項式の F 上の分解体であり，F のベキ根拡大体であるような K が存在する．ここで拡大 K/F を各々が素数型純拡大であるベキ根拡大列に細分したものを

$$F = R_0 \subseteq R_1 \subseteq \cdots\cdots \subseteq R_t$$

とすればよい．

R_i/R_{i-1} が p_i 型純拡大で，F が 1 の原始 p_i 乗根を含むとする．このとき R_i は $x^{p_i} - c_i \in R_{i-1}[x]$ なる形の多項式の R_{i-1} 上の分解体である．$Aut(R_t/R_k) = G_k$ とおくと $Aut(R_t/F)$ の部分群列

$$Aut(R_t/F) = G_0 \geq G_1 \geq \cdots \geq G_t = \{1\}$$

が得られる．定理 3.5 より $G_k \trianglerighteq G_{k+1}$ が成り立つので，上の列は正規列である．また

$$G_k/G_{k+1} = Aut(R_t/R_k)/Aut(R_t/R_{k+1}) \simeq Aut(R_{k+1}/R_k)$$

が成り立つので，定理 3.9 より剰余群はすべて巡回群である．ゆえに $Aut(R_t/F)$ は可解である．従って定理 3.5 を拡大列 $F \subseteq E \subseteq R_t$ に適用すれば

$$Aut(E/F) \simeq Aut(R_t/F)/Aut(R_t/E)$$

となるから $Aut(E/F)$ も可解である． ∎

定理 3.15 可解な多項式の *Galois* 群は可解である．

Proof 可解な $f(x) \in F[x]$ の F 上の分解体を E として $Aut(E/F)$ が可解であることを示せばよい．補題 3.14 より $E \subseteq R_t$ となるベキ根拡大

$$F = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_t \tag{3.1}$$

で, 各 R_i/R_{i-1} は素数 p_i 型純拡大であり, R_t はある F 係数多項式 $h(x)$ の F 上の分解体となるものが存在する. m を p_i $(i=1,...,t)$ の最小公倍数として, R' を R_t 上の x^m-1 の分解体とする. R' は 1 の原始 m 乗根 ζ を含むので $R'=R_t(\zeta)$ である. ζ を添加することにより得られる拡大列

$$F=R_0\subseteq R_0(\zeta)\subseteq R_1(\zeta)\subseteq\cdots\subseteq R_t(\zeta)=R' \tag{3.2}$$

において $F(\zeta)/F$ は m' 型, $R_i(\zeta)/R_{i-1}(\zeta)$ は p_i' 型の純拡大である. ただし m' は m の約数, p_i' は 1 または p_i である.

拡大列 $F\subseteq F(\zeta)\subseteq R'$ において R', $F(\zeta)$ はそれぞれ $(x^m-1)h(x)$, x^m-1 の F 上の分解体である. 従って定理 3.5 を適用すれば $Aut(R'/F(\zeta))\trianglelefteq Aut(R'/F)$ であり

$$Aut(R'/F)/Aut(R'/F(\zeta))\simeq Aut(F(\zeta)/F)$$

が成り立つ. 定理 3.8 より $Aut(F(\zeta)/F)$ は Abel 群である. また拡大列

$$F(\zeta)=R_0(\zeta)\subseteq R_1(\zeta)\subseteq\cdots\cdots\subseteq R_t(\zeta)=R'$$

は補題 3.14 の仮定を満たす. 従って $Aut(R'/F(\zeta))$ は可解である. よって定理 2.15 より $Aut(R'/F)$ も可解である. これより拡大列 $F\subseteq E\subseteq R'$ に定理 3.5 を適用して $Aut(E/F)$ の可解性が得られる. ∎

3.3 Galois の基本定理

定義 3.16 (指標) 群 G の体 E における指標とは準同型 $\sigma:G\to E^{\sharp}$ のことをいう.

定義 3.17 群 G の体 E における指標 $\{\sigma_1,...,\sigma_n\}$ が独立であるとは, E の元 $a_1,...,a_n$ で, 任意の $x\in G$ に対して $\sum a_i\sigma_i(x)=0$ となるものが $a_1=\cdots=a_n=0$ に限るときにいう.

補題 3.18 群 G の体 E における相異なる指標 $\{\sigma_1,...,\sigma_n\}$ は独立である.

Proof n についての帰納法で示す. $n=1$ のとき, $\sigma_1(x)\neq 0$ であるから $a_1\sigma_1(x)=0$ ならば $a_1=0$ となる. 従って $\{\sigma_1\}$ は独立である.

$n > 1$ として $n-1$ 個の指標は独立であると仮定する. すべては 0 でない E の元の組 $(a_1, ..., a_n)$ が存在して, 任意の $x \in G$ に対して

$$a_1\sigma_1(x) + \cdots\cdots + a_n\sigma_n(x) = 0 \tag{3.3}$$

が成立すると仮定する. $a_i = 0$ とすると $a_i\sigma_i(x) = 0$ であるから $\sum_{k\neq i} a_k\sigma_k(x) = 0$ が成り立つ. 従って帰納法の仮定から $a_k = 0$ が得られ矛盾が生じる. よってすべての i に対して $a_i \neq 0$ と仮定してよい.

a_n^{-1} をかけて $a_n = 1$ としておく. $\sigma_n \neq \sigma_1$ より $\sigma_n(y) \neq \sigma_1(y)$ となる $y \in G$ が存在する. ここで (3.3) において x を yx に置き換えれば

$$a_1\sigma_1(y)\sigma_1(x) + \cdots + a_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(y)\sigma_n(x) = 0 \tag{3.4}$$

を得る. 次に $\sigma_n(y)^{-1}$ をかけると

$$a_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x) + \cdots + a_{n-1}\sigma_n(y)^{-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(x) = 0 \tag{3.5}$$

を得る. $a_n = 1$ に注意して, (3.3) からこの式を引けば

$$a_1[1 - \sigma_n(y)^{-1}\sigma_1(y)]\sigma_1(x) + \cdots + a_{n-1}[1 - \sigma_n(y)^{-1}\sigma_{n-1}(y)]\sigma_{n-1}(x) = 0 \tag{3.6}$$

が得られる. 帰納法の仮定よりこの式の係数はすべて 0 である. 従って $a_1 \neq 0$ より $1 - \sigma_n(y)^{-1}\sigma_1(y) = 0$ となり, $\sigma_n(y) = \sigma_1(y)$ が得られ, 矛盾が生じる. 以上で n の場合も証明された. ∎

系 3.19 体 E の相異なる自己同型の集合 $\{\sigma_1, ..., \sigma_n\}$ は独立である.

Proof $\tau \in Aut(E)$ に対して, $\sigma = \tau|_{E^\sharp}$ とおくと σ は $E^\sharp$ の E における指標である. よって補題 3.18 を適用すれば, 独立であることが導かれる. ∎

定義 3.20 (不変体) $G \subseteq Aut(E)$ に対して

$$E^G = \{\alpha \in E \mid \text{任意の } \sigma \in G \text{ に対して} \sigma(\alpha) = \alpha\}$$

とおき, E^G を G の不変体という.

E^G が E の部分体であることは容易にわかる. また $Aut(E)$ の部分集合 H, G が $H \subseteq G$ を満たせば $E^G \subseteq E^H$ が成り立つ.

補題 3.21 $G=\{\sigma_1,...,\sigma_n\}$ が E の自己同型からなる集合のとき $[E:E^G]\geq n$ が成り立つ.

Proof $[E:E^G]=r<n$ と仮定して矛盾を導く. $\{\alpha_1,...,\alpha_r\}$ を E の E^G 上の基底とする. $x_1,...,x_n$ を未知数とする連立一次方程式

$$\begin{aligned}\sigma_1(\alpha_1)x_1+\cdots+\sigma_n(\alpha_1)x_n &= 0\\ \sigma_1(\alpha_2)x_1+\cdots+\sigma_n(\alpha_2)x_n &= 0\\ &\vdots\\ \sigma_1(\alpha_r)x_1+\cdots+\sigma_n(\alpha_r)x_n &= 0\end{aligned}$$

は $r<n$ より自明でない解 $(d_1,...,d_n)$ をもつ. さて, 任意の $\beta\in E$ に対して $\beta=\sum b_i\alpha_i$ となる $b_i\in E^G$ が存在する. 上の連立方程式に $x_1=d_1,...,x_n=d_n$ を代入し, i 番目の式に b_i をかけると, $b_i\in E^G$ より $b_i=\sigma_j(b_i)$ となることに注意すれば

$$\sigma_1(b_i\alpha_i)d_1+\cdots+\sigma_n(b_i\alpha_i)d_n=0$$

が得られる. これらをすべて加えれば

$$\sigma_1(\beta)d_1+\cdots+\sigma_n(\beta)d_n=0$$

を得る. β は E の任意の元であり, $(d_1,...,d_n)\neq(0,...,0)$ であるから, 上式は指標 $\{\sigma_1,...,\sigma_n\}$ の独立性に矛盾する. ∎

定理 3.22 $G=\{\sigma_1,...,\sigma_n\}$ が E の自己同型群 $Aut(E)$ の部分群のとき $[E:E^G]=n$ が成り立つ.

Proof 補題 3.21 より $[E:E^G]>n$ と仮定して矛盾を導けばよい. $\{\theta_1,...,\theta_{n+1}\}$ を E^G 上 1 次独立な E の元とする. 連立一次方程式

$$\begin{aligned}\sigma_1(\theta_1)x_1+\cdots+\sigma_1(\theta_{n+1})x_{n+1} &= 0\\ &\vdots\\ \sigma_n(\theta_1)x_1+\cdots+\sigma_n(\theta_{n+1})x_{n+1} &= 0\end{aligned}$$

は自明でない解 $(a_1,...,a_{n+1})$ をもつ. 0 でない a_i の個数 r が最小の解を選び, 適当に番号付けして $a_1,...,a_r$ が 0 でないようにする. $r=1$ とすれば $\sigma_1(\theta_1)a_1=0$ より $a_1=0$ となり矛盾が生じる. 従って $r\neq1$ である. 必要ならばすべての式を $1/a_r$ 倍することによ

り $a_r = 1$ と仮定してよい. ここで, すべての i について $a_i \in E^G$ と仮定すると σ_i が恒等写像のとき

$$\theta_1 a_1 + \cdots + \theta_r a_r = 0$$

となり $\{\theta_1, ..., \theta_{n+1}\}$ が E^G 上 1 次独立であったことに矛盾する. 従って, ある i に対して $a_i \notin E^G$ が成り立つ. 再び番号を改めて $a_1 \notin E^G$ とする. このとき $\sigma_k(a_1) \neq a_1$ となる $\sigma_k \in G$ が存在する. 元の連立方程式の j 番目の式に σ_k を作用させれば

$$\sigma_k\sigma_j(\theta_1)\sigma_k(a_1) + \cdots + \sigma_k\sigma_j(\theta_{r-1})\sigma_k(a_{r-1}) + \sigma_k\sigma_j(\theta_r) = 0 \tag{3.7}$$

を得る. G は群であるから $\sigma_k\sigma_j = \sigma_i$ となる番号 i があるので

$$\sigma_i(\theta_1)\sigma_k(a_1) + \cdots + \sigma_i(\theta_{r-1})\sigma_k(a_{r-1}) + \sigma_i(\theta_r) = 0 \tag{3.8}$$

と表すことができる. 元の i 番目の式に解 $(a_1, ..., a_{n+1})$ を代入した式と (3.8) との差をとれば i 番目が

$$\sigma_i(\theta_1)[a_1 - \sigma_k(a_1)] + \cdots + \sigma_i(\theta_{r-1})[a_{r-1} - \sigma_k(a_{r-1})] = 0$$

である n 個の式が導かれ, $a_1 - \sigma_k(a_1) \neq 0$ より元の連立一次方程式の自明でない解で, 0 でない成分が r 個より少ないものが存在することになり, 矛盾が生じる. ∎

系 3.23 *$Aut(E)$ の有限部分群 G, H が $E^G = E^H$ を満たせば $G = H$ が成り立つ.*

Proof $|G| = n$ とする. $\sigma \notin G$ の不変体が E^G を含むとすると E^G は $G \cup \{\sigma\}$ の $n+1$ 個の元で固定される. 補題 3.21 より $[E : E^G] \geq n+1$ となるが, これは, 定理 3.22 より $[E : E^G] = |G| = n$ となることに矛盾する. よって E^G を不変体に含む $Aut(E)$ の元は G の元に限る. 同様に E^H を不変体に含む $Aut(E)$ の元は H の元に限るが, 仮定より $E^G = E^H$ であることから $G = H$ が得られる. ∎

Galois 拡大

$F = \mathbb{Q}$, α を $f(x) = x^3 - 2$ の実根として $E = F(\alpha)$, $Aut(E/F) = G$ とする. $\sigma \in G$ に対して $\sigma(\alpha)$ は $f(x)$ の根であるが E は実数体に含まれるので $\sigma(\alpha) = \alpha$ となる. 従って σ は E の恒等写像となり, $G = Aut(E/F) = 1$ を得る. ゆえに $E^G = E \neq F$ となり, 一般に $F = E^G$ が成り立つとは限らない.

定理 3.24 E/F を有限次拡大, $G = Aut(E/F)$ とする. このとき次の 3 条件は同値である.

(1) $F = E^G$

(2) 任意の $\alpha \in E$ の F 上の最小多項式は E で分解する.

(3) E はある F 係数多項式の分解体である.

Proof (1)⇒(2) $\alpha \in E$ を任意に選び, その F 上の最小多項式を $p(x)$ とする.

$$\{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1, ..., \alpha_n\}$$

とおくと G は $\{\alpha_1, ..., \alpha_n\}$ の置換を引き起こすので, それらの対称式である $q(x) = \prod(x-\alpha_i)$ の係数を固定する. $E^G = F$ より $q(x)$ は F 係数となる. 従って定理 1.36 より $q(x)$ は $p(x)$ の倍数である. ゆえに $p(x)$ の根はすべて E に含まれる.

(2)⇒(3) E/F は有限次拡大であるから E の F 上の基底を $\{\beta_1, ..., \beta_n\}$ とすれば $E = F(\beta_1, ..., \beta_n)$ である. ここで β_i の F 上の最小多項式を $p_i(x)$ とすると, 仮定より $p_i(x)$ の根はすべて E に含まれる. 従って E は $f(x) = p_1(x) \cdots p_n(x)$ の分解体である.

(3)⇒(1) E はある多項式の分解体であるから定理 3.3 より $|G| = [E : F]$ が成り立つ. また補題 3.21 より $|G| \leq [E : E^G]$ となるので G は有限群である. 従って定理 3.22 より $|G| = [E : E^G]$ を得る. ゆえに $[E : E^G] = [E : F]$ かつ $F \subseteq E^G$ であるから $F = E^G$ が成り立つ. ∎

定義 3.25 (Galois 拡大) 有限次拡大 E/F が定理 3.24 の 3 条件のいずれかを満たすとき, E/F を *Galois* 拡大という. またこのとき E/F の自己同型群を *Galois* 群といい, $Gal(E/F)$ と表す.

以下, 特に断らない限り, 体の拡大は有限次拡大であるとする.

p.33 で述べたように $x^3 - 2$ の $\mathbb{Q}$ 上の分解体は $E = \mathbb{Q}(\alpha, \omega)$ であるから $E/\mathbb{Q}$ は Galois 拡大である. また $g(x) = x^3 - 3x^2 + 3x - 3$ は Eisenstein の判定法より $\mathbb{Q}$ 上既約である. $g(x)$ は E 上で

$$g(x) = (x-1)^3 - \alpha^3 = (x - 1 - \alpha)\left((x-1)^2 + \alpha(x-1) + \alpha^2\right)$$

と分解できるから $\beta = \alpha + 1 \in E$ を根に持つ. $E/\mathbb{Q}$ は Galois 拡大であるから, 定理 3.24 より $g(x)$ は E で分解する. このとき他の 2 根は $1 + \alpha\omega$, $1 + \alpha\omega^2$ である.

Galois 拡大の定義より $G = Aut(E/F)$ の不変体 E^G に対して E/E^G は Galois 拡大である.

E/F が Galois 拡大ならば, 任意の中間体 B に対して E/B も Galois 拡大である. なぜならば, E はある多項式 $f(x) \in F[x]$ の F 上の分解体であるが, $f(x) \in B[x]$ より $f(x)$ の B 上の分解体と見なせるからである.

2 次拡大 E/F は Galois 拡大である. なぜならば, $\alpha \in E$ の最小多項式を $x^2+bx+c \in F[x]$ とすると, $E = F(\alpha)$ で, 他方の解が $-b-\alpha$ となり, E が x^2+bx+c の分解体となるからである.

E, L, F はある体の部分体で, $F \subseteq E \cap L$ であるとする. E/F, L/F がともに Galois 拡大のとき, 合成体 $E \vee L$ も F の Galois 拡大である. なぜならば, E を $f(x) \in F[x]$ の分解体, L を $g(x) \in F[x]$ の分解体とすれば, $E \vee L$ は $f(x)g(x) \in F[x]$ の分解体になるからである.

Galois 拡大 E/F の中間体 M, N に対して $Gal(E/F)$ の元 σ が存在して $\sigma(M) = N$ となるとき N を M の共役 (体) という. また M と N は互いに共役であるという.

定理 3.26 *Galois* 拡大 E/F の中間体 B に対して次の 3 条件は同値である.

(1) B の共役は B のみである.

(2) 任意の $\sigma \in Gal(E/F)$ に対して $\sigma(B) = B$ が成り立つ.

(3) B/F は *Galois* 拡大である.

Proof (1)⇒(2) 共役の定義より明らかである.

(2)⇒(3) $\beta \in B$ を任意に選び, その F 上の最小多項式を $p(x)$ とする. E/F は Galois 拡大であるから $p(x)$ は E で分解する. β' を $p(x)$ の根とすれば, 補題 1.39 より同型 $\tau : F(\beta) \to F(\beta')$ $(\tau(\beta) = \beta')$ が存在し, 定理 1.40 より $Gal(E/F)$ の元 σ に拡張される. 仮定より $\sigma(B) = B$ であるから $\beta' = \sigma(\beta) \in \sigma(B) = B$ が成り立つ. これより B は $p(x)$ の根をすべて含むことになるので $p(x)$ は B で分解する. ゆえに B/F は Galois 拡大である.

(3)⇒(1) B/F が Galois 拡大であるとすると, B はある F 係数多項式 $f(x)$ の分解体である. $f(x)$ の根を $\alpha_1, ..., \alpha_n$ とおけば $B = F(\alpha_1, ..., \alpha_n)$ となる. $\delta \in Gal(E/F)$ は $\alpha_1, ..., \alpha_n$ を置換するので $\delta(B) = \delta(F(\alpha_1, ..., \alpha_n)) = F(\delta(\alpha_1), ..., \delta(\alpha_n)) = B$ が成り立つ. δ は任意に選ぶことができるから B の共役は B のみである. ∎

体 F 上の n 変数有理関数体を $E = F(x_1,..., x_n)$ とおく. このとき S_n の元 σ は

$$\sigma^*(f(x_1, ..., x_n)) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$$

と定めることにより, E の F 自己同型 σ^* を引き起こす.

$$S_n \ni \sigma \mapsto \sigma^* \in Aut(E/F)$$

が単射準同型であることは容易に確かめられる. 従って σ と σ^* を同一視して, $S_n \leq Aut(E/F)$ と見なすことにする. なお任意の $\sigma \in S_n$ に対して $\sigma(f) = f$ となる $f \in E$ を (有理) 対称式という. 特に

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k} \qquad (k = 1, 2, ..., n) \tag{3.9}$$

を基本対称式という. さて

$$g(t) = (t - x_1) \cdots (t - x_n) = t^n - s_1 t^{n-1} + \cdots + (-1)^{n-1} s_{n-1} t + (-1)^n s_n$$

とおくと $g(t)$ は $L = F(s_1, ..., s_n)$ 上の多項式で, E で $g(t) = \prod(t - x_k)$ と分解する. $E = L(x_1, ..., x_n)$ であるから E は L 係数多項式 $g(t)$ の L 上の分解体である. ゆえに E/L は Galois 拡大である.

一方, S_n の任意の元は L の各元を固定するので $S_n \leq Gal(E/L)$ が成り立つ. E は n 次多項式 $g(t)$ の L 上の分解体であるから, 定理 3.2 より $Gal(E/L)$ は S_n の部分群と見なせる. ゆえに位数を比較して $Gal(E/L) \simeq S_n$ を得る. このとき, 定理 3.24 より $L = E^{S_n}$ が成り立つ. これより S_n の各元で固定される有理式は $L = F(s_1, ..., s_n)$ の元に限ること, すなわち, 有理対称式は基本対称式の有理式として表されること, がわかる.

定理 3.27 有理対称式は基本対称式の有理式として表される.

ここでは証明しないが, 対称多項式は基本対称式の多項式として表される. 証明については, 例えば [6, 2 章, 定理 2.59, 命題 2.60] などを参照されたい.

定理 3.28 対称多項式は基本対称式の多項式として 一意に表される.

Galois の基本定理

以下, 群 G の部分群 H, K で生成された部分群を $H \vee K$ と表すことにする.

定理 3.29 (Galois の基本定理) E/F を *Galois* 拡大, その *Galois* 群を $G = Gal(E/F)$ とする. また G の部分群全体のなす集合を $\mathcal{S}(G)$, E/F の中間体全体のなす集合を $\mathcal{M}(E/F)$ とする. このとき次が成り立つ.

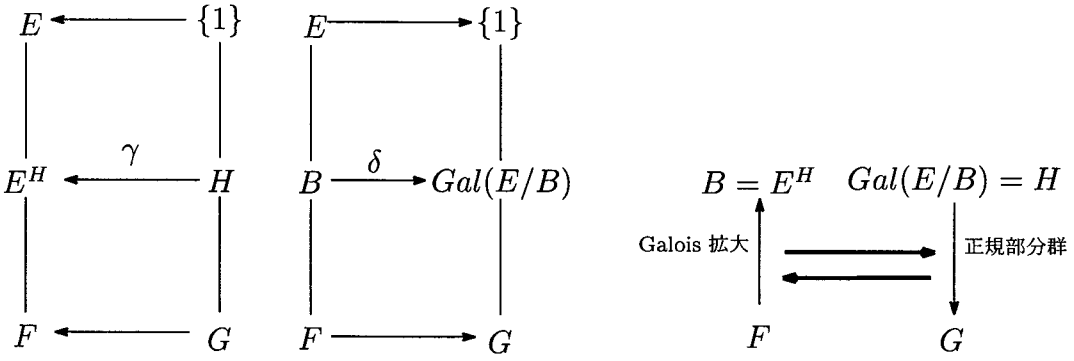
(1) $\gamma : \mathcal{S}(G) \ni H \mapsto E^H \in \mathcal{M}(E/F)$ は全単射で, 包含関係を逆転する. γ の逆写像は $\delta : \mathcal{M}(E/F) \ni B \mapsto Gal(E/B) \in \mathcal{S}(G)$ であり, δ も包含関係を逆転する.

(2) $E^{Gal(E/B)} = B, \quad Gal(E/E^H) = H$

(3)
$$E^{H \vee K} = E^H \cap E^K, \quad Gal(E/B \vee C) = Gal(E/B) \cap Gal(E/C),$$
$$E^{H \cap K} = E^H \vee E^K, \quad Gal(E/B \cap C) = Gal(E/B) \vee Gal(E/C)$$

(4) $[B : F] = [G : Gal(E/B)], \quad [G : H] = [E^H : F]$

(5) B/F が *Galois* 拡大であるための条件は $Gal(E/B)$ が G の正規部分群であることである.



Proof (1) 系 3.23 より γ は単射である. また p.40 で注意したように γ は包含関係を逆転する. 次に, 任意の $B \in \mathcal{M}(E/F)$ に対して $H = \delta(B)$ とおくと $H = Gal(E/B)$ であるから $B = E^H$, すなわち $\gamma(H) = B$ が成り立つ. 従って γ が全射であること, および $\gamma\delta$ が $\mathcal{M}(E/F)$ の恒等写像であることが示された.

$$\mathcal{M}(E/F) \xrightarrow{\delta} \mathcal{S}(G) \xrightarrow{\gamma} \mathcal{M}(E/F)$$

ゆえに δ は γ の逆写像である. δ が包含関係を逆転することも γ の逆写像であることから明らかである.

(2) $\gamma\delta, \delta\gamma$ が恒等写像であることより明らかである.

(3) $H, K \in \mathcal{S}(G)$ に対して $E^{H \vee K} \supseteq E^H \cap E^K$ は明らかに成り立つ. また $E^{H \vee K} \subseteq E^H$ かつ $E^{H \vee K} \subseteq E^K$ が成り立つから $E^{H \vee K} \subseteq E^H \cap E^K$ が得られる. 従って $E^{H \vee K} = E^H \cap E^K$

が成り立つ. 他の等式についても同様にして導くことができる.

(4) $B \in \mathcal{M}(E/F)$ に対して $[E:F] = [E:B][B:F]$ より

$$[B:F] = \frac{[E:F]}{[E:B]} = \frac{|G|}{|Gal(E/B)|} = [G : Gal(E/B)]$$

が成り立つ. ここで $B = E^H$ とおけば

$$[E^H : F] = [G : Gal(E/E^H)] = [G:H]$$

が得られる.

(5) B/F が Galois 拡大のとき, 定理3.5 より $Gal(E/B)$ は G の正規部分群である. 逆に $H = Gal(E/B)$ が G の正規部分群であると仮定すると $\sigma \in G$ に対して $\sigma H \sigma^{-1}$ の不変体が $\sigma(B)$ であることから $\sigma H \sigma^{-1} = H$ より $\sigma(B) = B$ が得られる. 従って B の共役が B のみとなり, 定理3.26 より B/F は Galois 拡大である. ∎

ここで, 有限体の Galois 群が巡回群であることを示すことにする. 有限体の場合は標数 0 の場合と同様に, 既約多項式がすべて分離的となり, これまでに得られた結果が適用できる.

位数 q の有限体 F は $\mathbb{Z}_p$ 係数多項式 $x^q - x$ の根全体に一致する ([5, 7章, 定理33の証明]). 一方 F の乗法群 $F^\sharp = F - \{0\}$ は巡回群であるから, F は $\mathbb{Z}_p$ に 1 の原始 $q-1$ 乗根を添加した拡大体である.

定義 3.30 F が標数 p の有限体のとき, $F = \mathbb{Z}_p(\alpha)$ となる F の元 α を F の原始元という.

有限体 F の位数 q は素数 p のべき, $q = p^n$ である. また位数が同じ有限体は系1.41 より互いに同型である. これより, 位数 p^n の有限体を $GF(p^n)$ と表し, Galois 体という. $GF(p^n)$ は $GF(p)$ 係数多項式 $x^q - x$ の分解体であるから, 拡大 $GF(p^n)/GF(p)$ は Galois 拡大である.

定理 3.31 $Gal(GF(p^n)/GF(p)) \simeq \mathbb{Z}_n$ が成り立つ. またその生成元は $\sigma : u \mapsto u^p$ である.

Proof $q = p^n$, $g(x) = x^q - x \in GF(p)[x]$ とおく. $g'(x) = qx^{q-1} - 1 \neq 0$ であるから $g(x)$ は分離多項式である. 従って定理3.3 より $|Gal(GF(p^n)/GF(p))| = [GF(p^n) : GF(p)] = n$ が成り立つ.

$K = GF(p^n)$, $G = Gal(GF(p^n)/GF(p))$ とおけば標数 p の体の演算 (p.11) より $\sigma : K \ni u \mapsto u^p \in K$ は G の元である. ここで $j < n$ のとき $\sigma^j \neq 1$ が成り立つ. なぜならば, 仮に $j(<n)$ で $\sigma^j = 1$ となったとすると, 任意の K の元 u に対して $u^{p^j} = u$ が成り立つこと

になり, 定理1.25に矛盾するからである. ゆえに σ の位数は n となり, $G = \langle\sigma\rangle$ が得られる. よって G は位数 n の巡回群である. ∎

Galois 拡大 E/F の Galois 群 $Gal(E/F)$ は有限群であるから, 部分群は有限個である. 従って Galois の基本定理より E/F の中間体も有限個である. これより次の系が得られる.

系 3.32 *Galois* 拡大 E/F の中間体は有限個である.

定理 3.33 有限次拡大 E/F が単純拡大であるための条件はその中間体が有限個であることである.

Proof $E = F(\alpha)$, α の F 上の最小多項式を $p(x)$ とする. E/F の中間体を B とし, $q(x)$ を α の B 上の最小多項式, B' を F と $q(x)$ の係数から生成される B の部分体とする. $q(x)$ は B' 上でも既約であるから $E = B(\alpha) = B'(\alpha)$ となり

$$[E : B] = [B(\alpha) : B] = \partial(q) = [B'(\alpha) : B'] = [E : B']$$

が成り立つ. 従って $B = B'$ となり, B は $q(x)$ の係数から一意に定まる. $q(x)$ は $p(x)$ のモニックな因子であり, $p(x)$ のモニックな因子は有限個であるから, 拡大 E/F の中間体は有限個である.

逆に, 拡大 E/F の中間体が有限個であると仮定する. F が有限体のときは原始元を添加すればよいので, F は無限体であるとする. E/F が有限次拡大であるから $E = F(\alpha_1, ..., \alpha_n)$ とおくことができる. ここで $F(\alpha, \beta)$ $(\alpha, \beta \in E)$ と表される拡大が単純拡大であることを示せば, 任意の n について $F(\alpha_1, ..., \alpha_n)$ が単純拡大であることが導かれる. $\beta \neq 0$ としてよいので, $F(\alpha, \beta)$ に含まれる $\gamma_t = \alpha + t\beta$, $t \in F$ なる形の元は, F が無限体であることから, 無限に存在する. 一方, 中間体は有限個であるから F の異なる2元 s, t に対して $F(\gamma_s) = F(\gamma_t)$ となるものが存在する. 従って $F(\gamma_s) = F(\gamma_t)$ は $\gamma_s - \gamma_t = (s - t)\beta$ を含む. $s \neq t$ であるから $\beta \in F(\gamma_t)$ が得られる. また $\alpha = \gamma_t - t\beta \in F(\gamma_t)$ となるので $F(\alpha, \beta) \subseteq F(\gamma_t)$ が成り立つ. よって $F(\alpha, \beta) = F(\gamma_t)$ が示された. ∎

系3.32, 定理3.33から次の系を得る.

系 3.34 *Galois* 拡大は単純拡大である.

系 3.35 F 係数多項式 $f(x)$ が $F[x]$ で $f(x)=g(x)h(x)$ と分解されたとする. E を $f(x)$ の F 上の分解体, $B\subseteq E$ を $g(x)$ の F 上の分解体, $C\subseteq E$ を $h(x)$ の F 上の分解体とする. ここで $B\cap C=F$ ならば

$$Gal(E/F)\simeq Gal(B/F)\times Gal(C/F)$$

が成り立つ.

Proof B/F, C/F は Galois 拡大であるから $Gal(E/B)$, $Gal(E/C)$ はともに $Gal(E/F)$ の正規部分群である. 仮定より $B\vee C=E$, $B\cap C=F$ であるから, Galois の基本定理より

$$Gal(E/B)\cap Gal(E/C)=Gal(E/B\vee C)=Gal(E/E)=1,$$

$$Gal(E/B)\vee Gal(E/C)=Gal(E/B\cap C)=Gal(E/F)$$

が導かれる. 従って定理 1.9 より

$$Gal(E/F)\simeq Gal(E/B)\times Gal(E/C) \tag{3.10}$$

が成り立つ. これより $Gal(E/F)/Gal(E/B)\simeq Gal(E/C)$ となるが, 定理 3.5 (p.33) より $Gal(E/F)/Gal(E/B)\simeq Gal(B/F)$ が成り立つ. ゆえに $Gal(E/C)\simeq Gal(B/F)$ が導かれる. 同様に $Gal(E/B)\simeq Gal(C/F)$ が導かれるので

$$Gal(E/F)\simeq Gal(B/F)\times Gal(C/F)$$

が示された. ∎

3.4 多項式の可解性

この節では定理 3.15 の逆を証明し, 方程式がベキ根により可解であることと, その Galois 群が可解群であることとが同値であることの証明を完成する.

定理 3.36 ある体の部分体 K,E,L,F が, $F\subseteq E\cap L$, E/F は *Galois* 拡大, $K=E\vee L$ を満たすとする. このとき K/L は *Galois* 拡大で

$$Gal(K/L)\simeq Gal(E/E\cap L)$$

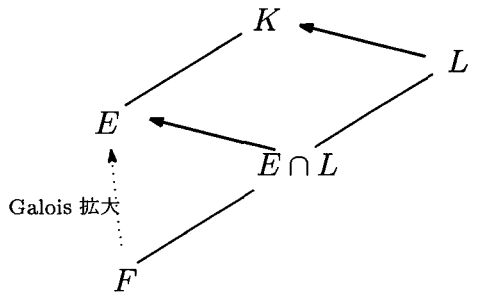
が成り立つ.

Proof E/F は Galois 拡大であるから, E はある F 係数多項式 $f(x)$ の分解体である. $f(x)$ の根を $\alpha_1, ..., \alpha_n$ とすれば $E = F(\alpha_1, ..., \alpha_n)$ となる. このとき $K = E \vee L = L(\alpha_1, ..., \alpha_n)$ であるから K は L 係数多項式 $f(x)$ の L 上の分解体である. 従って K/L は Galois 拡大である.

$\sigma \in Gal(K/L)$ の E への制限 $\sigma|_E$ は $Gal(E/E \cap L)$ の元となるから準同型写像

$$\varphi : Gal(K/L) \ni \sigma \mapsto \sigma|_E \in Gal(E/E \cap L)$$

が定義できる. $\sigma|_E$ が恒等写像のとき, σ は E と L の元をすべて固定するので K の恒等写像になる. 従って $Ker(\varphi) = 1$ より φ は単射である.



$E/E \cap L$ は Galois 拡大であるから単純拡大となり, ある E の元 β によって $E = (E \cap L)(\beta)$ と表される. β の L 上の最小多項式を $g(x)$, $E \cap L$ 上の最小多項式を $h(x)$ とすると $g(x)$ は $h(x)$ を割り切る. 一方 $E/E \cap L$ が Galois 拡大であることより $h(x)$ の根はすべて E の元である. 従って $g(x)$ の根もすべて E の元であるから $g(x)$ は $E \cap L$ 係数である. これより $h(x)$ は $g(x)$ を割り切ることになるので $g(x) = h(x)$ を得る. ゆえに

$$|Gal(K/L)| = \partial(g) = \partial(h) = |Gal(E/E \cap L)|$$

が成り立ち, φ の同型であることが示された. ∎

ノルム

定義 3.37 E/F が *Galois* 拡大のとき, $\alpha \in E^\sharp$ に対して

$$N_{E/F}(\alpha) = \prod_{\sigma \in Gal(E/F)} \sigma(\alpha)$$

と定め, α のノルムという. また $N_{E/F}$ をノルム (写像) という.

ノルム $N_{E/F}(\alpha)$ について次が成り立つ (証明略).

- $\alpha \in E^\sharp$ のとき $N_{E/F}(\alpha) \in F^\sharp$ である.

- $\alpha, \beta \in E^\sharp$ のとき $N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)N_{E/F}(\beta)$ が成り立つ. 従って $N_{E/F} : E^\sharp \mapsto F^\sharp$ は準同型である.
- $[E : F] = n$, $a \in F^\sharp$ のとき $N_{E/F}(a) = a^n$ である.
- $\sigma \in Gal(E/F)$, $\alpha \in E^\sharp$ ならば $N_{E/F}(\sigma(\alpha)) = N_{E/F}(\alpha)$ である.

次は Hilbert の定理 90 として知られている.

補題 3.38 *E/F は Galois 拡大で, その Galois 群 G は σ を生成元とする位数 n の巡回群であるとする. このとき $N_{E/F}(\alpha) = 1$ となる条件は*

$$\alpha = \beta\sigma(\beta)^{-1}$$

となる $\beta \in E^\sharp$ が存在することである.

Proof $\alpha = \beta\sigma(\beta)^{-1}$ となる $\beta \in E^\sharp$ が存在するとすれば

$$N_{E/F}(\alpha) = N_{E/F}(\beta\sigma(\beta)^{-1}) = N_{E/F}(\beta)N_{E/F}(\sigma(\beta))^{-1} = N_{E/F}(\beta)N_{E/F}(\beta)^{-1} = 1$$

が成り立つ. 逆に $N_{E/F}(\alpha) = 1$ と仮定する. ここで

$$\begin{aligned}
\delta_0 &= \alpha \\
\delta_1 &= \alpha\sigma(\alpha) \\
\delta_2 &= \alpha\sigma(\alpha)\sigma^2(\alpha) \\
&\vdots \\
\delta_{n-1} &= \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = N_{E/F}(\alpha) = 1
\end{aligned}$$

とおくと, すべての i $(0 \le i \le n-2)$ に対して

$$\alpha\sigma(\delta_i) = \delta_{i+1} \tag{3.11}$$

が成り立つ. ただし $\delta_n = \delta_0$ とする. 一方, 指標 $\{1, \sigma, ..., \sigma^{n-1}\}$ は独立であるから

$$\delta_0\gamma + \delta_1\sigma(\gamma) + \cdots + \delta_{n-2}\sigma^{n-2}(\gamma) + \delta_{n-1}\sigma^{n-1}(\gamma) \neq 0 \tag{3.12}$$

を満たす E の元 γ が存在する. (3.12) の左辺を β とおき, 両辺に σ を作用させ, $\delta_{n-1}=1$ に注意して (3.11) を適用すると

$$\begin{aligned}\sigma(\beta) &= \sigma(\delta_0)\sigma(\gamma)+\sigma(\delta_1)\sigma^2(\gamma)+\cdots+\sigma(\delta_{n-2})\sigma^{n-1}(\gamma)+\sigma^n(\gamma)\\ &= \alpha^{-1}[\delta_1\sigma(\gamma)+\delta_2\sigma^2(\gamma)+\cdots+\delta_{n-1}\sigma^{n-1}(\gamma)]+\sigma^n(\gamma)\end{aligned}$$

が得られる. 個の最終項が $\sigma^n(\gamma)=\gamma=\alpha^{-1}\alpha\gamma=\alpha^{-1}\delta_0\gamma$ であることから

$$\sigma(\beta)=\alpha^{-1}\big(\delta_1\sigma(\gamma)+\delta_2\sigma^2(\gamma)+\cdots+\delta_{n-1}\sigma^{n-1}(\gamma)+\delta_0\gamma\big)=\alpha^{-1}\beta$$

が得られる. ∎

系 3.39 *p を素数, E/F を p 次の Galois 拡大, F は 1 の原始 p 乗根を含むとする. このとき $\beta^p\in F$ を満たす E の元 β が存在して $E=F(\beta)$ となる. 特に E/F は p 型純拡大である.*

Proof $G=Gal(E/F)$ の位数が p であることから p.8 で述べたように $G=Gal(E/F)$ は位数 p の巡回群である. $G=\langle\sigma\rangle$ とおく.

F に含まれる 1 の原始 p 乗根を ζ とすると $N_{E/F}(\zeta)=1$ が成り立つ. 従って補題 3.38 より $\zeta=\beta\sigma(\beta)^{-1}$ となる E の元 β が存在する. $\zeta\neq 1$ より $\beta\notin F$ であることから $F(\beta)\neq F$ となる. Galois の基本定理より E/F の中間体は E, F のみであるから $E=F(\beta)$ が成り立つ. さて $\sigma(\beta)=\beta\zeta^{-1}$ となるから

$$\sigma(\beta^p)=\sigma(\beta)^p=(\beta\zeta^{-1})^p=\beta^p$$

が得られ, $\beta^p\in E^G=F$ が導かれる. ∎

定理 3.40 *Galois 拡大 E/F の Galois 群 $G=Gal(E/F)$ が可解になるための条件は E が F のあるベキ根拡大体に含まれることである. 特に多項式 $f(x)\in F[x]$ の Galois 群が可解になるための条件は $f(x)$ が可解になることである.*

Proof Galois 拡大 E/F はある F 係数多項式の分解体であるから, E が F のあるベキ根拡大体に含まれるならば, その多項式は可解となり, 定理 3.15 より, その Galois 群 G は可解である.

逆に G が可解であると仮定する. 系 2.18 より G に素数指数の正規部分群 H が存在する. その指数を p とおく. まず 1 の原始 p 乗根 ζ が F に含まれる場合を指数 $[E:F]$ に関する帰納法により示す.

$[E:F]=1$ のときは $E=F$ より明らかである. $[E:F]>1$ とする. E/E^H は Galois 拡大で $H=Gal(E/E^H)$ は 可解群である. $[E:E^H]<[E:F]$ であるから帰納法の仮定によりベキ根拡大列

$$E^H \subseteq R_1 \subseteq \cdots\cdots \subseteq R_m \qquad (E \subseteq R_m)$$

が存在する. 一方 H が G の正規部分群であることから, E^H/F は p 次 Galois 拡大である. $\zeta \in F$ より, 系 3.39 を適用できるので E^H/F は p 型純拡大である. よってベキ根拡大列

$$F \subseteq E^H \subseteq R_1 \subseteq \cdots\cdots \subseteq R_m \qquad (E \subseteq R_m)$$

が存在する.

一般の場合には $|G|=n$ として, 1 の原始 n 乗根 ω を E に添加した体を $E^*=E(\omega)$ とおく. $F^*=F(\omega)$ とすれば $E^*=E\vee F^*$ である. E/F が Galois 拡大であるから定理 3.36 より E^*/F^* も Galois 拡大で, $Gal(E^*/F^*) \simeq Gal(E/E\cap F^*)$ が成り立つ. ここで $G^*=Gal(E^*/F^*)$ とおけば G^* は可解群 G の部分群に同型であるから可解群である. $\omega \in F^*$ より, G の任意の素因数 p に対して, F^* が 1 の原始 p 乗根を含むので, 上の結果が適用できて, ベキ根拡大列

$$F^* \subseteq R_1^* \subseteq \cdots\cdots \subseteq R_n^*=R^* \qquad (E \subseteq E^* \subseteq R^*)$$

が得られる. このとき $F^*=F(\omega)$ よりベキ根拡大列

$$F \subseteq F^* \subseteq \cdots\cdots \subseteq R^* \qquad (E \subseteq R^*)$$

が存在する. 以上で E が F のあるベキ根拡大体に含まれることが示された. ∎

系 3.41 4 次以下の方程式は可解である.

Proof 4 次以下の方程式の Galois 群は S_4 の部分群である. 定理 2.22 より S_4, および, その部分群はすべて可解である. ゆえに 4 次以下の方程式は可解である. ∎

5 次方程式の Galois 群は S_5 の部分群である. 定理 2.22 より S_5 は可解でないが, 補題 2.26 より, 位数 24 以下の部分群は可解である. 従って位数 24 以下の S_5 の部分群を Galois 群にもつ 5 次方程式は可解である.

系 3.42 既約 5 次方程式が可解となるための条件は, その *Galois* 群が F_{20}, F_{10}, F_5 のいずれかと同型になることである.

Proof 定理 3.40 と定理 2.29 より直ちに得られる. ∎

4章　可解な5次方程式・その1

4章では, 本論文のテーマである D.S. Dummit [1] による有理数係数既約 5 次方程式の可解性を判定する方法と, 可解な 5 次方程式の解法について述べる. §4.1 では既約 5 次方程式 $f(x)=0$ の 5 個の根の 4 次同次式 θ を導入し, 2 章で示した S_5 の可移部分群に関する結果を基に, θ の 6 個の共役を根に持つ 6 次分解式 $f_{20}(x)$ が 1 つの有理数根を持つことと, $f(x)$ が可解であることとが同値であることを導く. §4.2 では有理数係数の可解な既約 5 次方程式 $f(x)=0$ から定まる Lagrange 分解式と, Lagrange 分解式を 5 乗して得られる式への Galois 群の作用を通して, $f(x)$ の係数と $f_{20}(x)$ の有理数根の有理式として表示できる定数の存在を導く. また, それらの定数を用いて $f(x)$ の根が復元できるしくみを明らかにする. §4.3 では可解な 3 項 5 次方程式に対して, その解法を例示する.

4.1　可解性の判定方法

以下, 複素 (変) 数 $x_1,...,x_5$ を根とする 5 次方程式を

$$f(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=0$$

とおき, これを展開した式を

$$f(x)=x^5-s_1x^4+s_2x^3-s_3x^2+s_4x-s_5=0 \tag{4.1}$$

とする. $s_1,...,s_5$ は $x_1,...,x_5$ の基本対称式である. ここで

$$\begin{aligned}\theta \;=\; & x_1^2x_2x_5+x_1^2x_3x_4+x_2^2x_1x_3+x_2^2x_4x_5+x_3^2x_1x_5 \\ & +x_3^2x_2x_4+x_4^2x_1x_2+x_4^2x_3x_5+x_5^2x_1x_4+x_5^2x_2x_3\end{aligned} \tag{4.2}$$

とおく．さて p.30 で定義した S_5 の置換 $\sigma=(1,2,3,4,5)$, $\tau=(2,3,5,4)$ と S_5 の部分群

$$F_{20}=\langle\,\sigma,\,\tau\,\rangle,\qquad F_{10}=\langle\,\sigma,\,\tau^2\,\rangle,\qquad F_5=\langle\,\sigma\,\rangle$$

を想起されたい．S_5 の置換は p.45 で定めた方法で θ に作用する．σ,τ は θ を固定するので，$F_{20}=\langle\sigma,\tau\rangle$ の任意の元が θ を固定する．一方 $[S_5:F_{20}]=6$ より S_5 は F_{20} の 6 個の剰余類に分解できる．θ と同じ S_5-軌道に属する元を θ の共役と呼ぶことにすれば，F_{20} が θ の固定部分群に一致するのは θ の共役がちょうど 6 個あるときに限る．$\theta_1=\theta$ とし，θ_1 に $(1,2,3)$ を作用させたものを $(1,2,3)\theta_1$ と表すことにすれば

$$\begin{aligned}
\theta_2 &= (1\ 2\ 3)\theta_1\\
&= x_1^2x_2x_5+x_1^2x_3x_4+x_2^2x_1x_4+x_2^2x_3x_5+x_3^2x_1x_2\\
&\quad +x_3^2x_4x_5+x_4^2x_1x_5+x_4^2x_2x_3+x_5^2x_1x_3+x_5^2x_2x_4\\
\theta_3 &= (1\ 3\ 2)\theta_1\\
&= x_1^2x_2x_3+x_1^2x_4x_5+x_2^2x_1x_4+x_2^2x_3x_5+x_3^2x_1x_5\\
&\quad +x_3^2x_2x_4+x_4^2x_1x_3+x_4^2x_2x_5+x_5^2x_1x_2+x_5^2x_3x_4\\
\theta_4 &= (1\ 2)\theta_1\\
&= x_1^2x_2x_3+x_1^2x_4x_5+x_2^2x_1x_5+x_2^2x_3x_4+x_3^2x_1x_4\\
&\quad +x_3^2x_2x_5+x_4^2x_1x_2+x_4^2x_3x_5+x_5^2x_1x_3+x_5^2x_2x_4\\
\theta_5 &= (2\ 3)\theta_1\\
&= x_1^2x_2x_4+x_1^2x_3x_5+x_2^2x_1x_5+x_2^2x_3x_4+x_3^2x_1x_2\\
&\quad +x_3^2x_4x_5+x_4^2x_1x_3+x_4^2x_2x_5+x_5^2x_1x_4+x_5^2x_2x_3\\
\theta_6 &= (1\ 3)\theta_1\\
&= x_1^2x_2x_4+x_1^2x_3x_5+x_2^2x_1x_3+x_2^2x_4x_5+x_3^2x_1x_4\\
&\quad +x_3^2x_2x_5+x_4^2x_1x_5+x_4^2x_2x_3+x_5^2x_1x_2+x_5^2x_3x_4
\end{aligned}\tag{4.3}$$

と θ の共役が 6 個現れる．従って θ の固定群は F_{20} である．また $\{\theta_1,...,\theta_6\}$ が θ を含む S_5-軌道であるから θ_1,..., θ_6 の対称式は S_5 の元により固定される．ゆえに θ_1,.., θ_6 の対称式は x_1,...,x_5 の対称式で表される．ここで θ_1,...,θ_6 を根にもつ 6 次多項式を

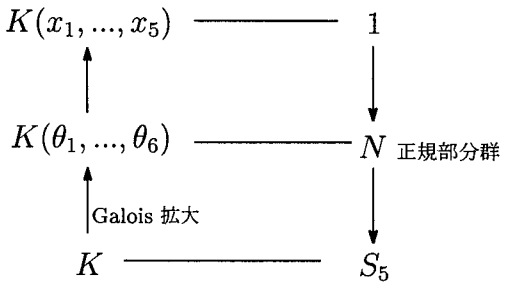
$$f_{20}(x)=(x-\theta_1)\cdots(x-\theta_6)$$

と定めると，その係数は，x_1,...,x_5 の対称式で表され，さらに (4.1) の係数 $s_1,...,s_5$ で表される．以下 $f_{20}(x)$ を (4.1) の 6 次分解式ということにする．

補題 4.1 $K=\mathbb{Q}(s_1,...,s_5)$ とおけば $K(x_1,...,x_5)=K(\theta_1,...,\theta_6)$ が成り立つ.

Proof まず $x_1,...,x_5$ を変数と見なして証明する. このとき $\theta_1,...,\theta_6$ はすべて互いに異なることを注意しておく. $K(x_1,...,x_5)$, $K(\theta_1,...,\theta_6)$ はそれぞれ (4.1), $f_{20}(x)$ の分解体であるから, $K(x_1,...,x_5)/K$, $K(\theta_1,...,\theta_6)/K$ はともに Galois 拡大である. K が 基本対称式 s_1,...,s_5 の有理関数体であるから p.45 で述べたように $Gal(K(x_1,...,x_5)/K)\simeq S_5$ が成り立つ. このとき $Gal(K(x_1,...,x_5)/K)$ が $\theta_1,...,\theta_6$ に可移に作用するので $f_{20}(x)$ は K 上既約な 6 次多項式である. Galois の基本定理より $K(\theta_1,...,\theta_6)$ に対応する S_5 の正規部分群 N が存在する. $[K(\theta_1):K]=6$ より $N\neq S_5$ である. $N\neq 1$ とすると系 2.10 より $N=A_5$ となるが, このとき $[K(\theta_1,...,\theta_6):K]=2$ となり矛盾が生じる. ゆえに $N=1$, すなわち $K(x_1,...,x_5)=K(\theta_1,...,\theta_6)$ が成り立つ.

上の結果より $x_1,...,x_5$ は $\theta_1,...,\theta_6$, $s_1,...,s_5$, および $\mathbb{Q}$ の元に四則演算を施した形で表される. この式は恒等式であり, $x_1,...,x_5$ が一般の複素数値であっても成り立つ. ゆえに $x_1,...,x_5$ が複素数の場合も $K(x_1,...,x_5)=K(\theta_1,...,\theta_6)$ が成り立つ. ∎



定理 4.2 $\mathbb{Q}$ 係数既約 5 次方程式が可解になる条件は, その 6 次分解式 $f_{20}(x)$ がちょうど 1 つの有理数根をもつことである.

Proof $\mathbb{Q}$ 係数既約 5 次方程式 $f(x)=0$ が可解であるとする. このとき, $f(x)$ の Galois 群 G は F_{20}, F_{10}, F_5 のいずれかに共役である. 従ってある θ_i を固定する. ゆえに $\theta_i\in\mathbb{Q}$ が得られる. 次に $f_{20}(x)$ の有理数根が θ_i のみであることを示す. ここで $i=1$ としても一般性を失わない. このとき G は 5 -cycle $\sigma=(1,2,3,4,5)$ を含む. $\theta_i, i\neq 1$ は σ によって

$$\theta_2 \overset{\sigma}{\mapsto} \theta_6 \overset{\sigma}{\mapsto} \theta_3 \overset{\sigma}{\mapsto} \theta_4 \overset{\sigma}{\mapsto} \theta_5 \overset{\sigma}{\mapsto} \theta_2$$

と置換される. ここで θ_2,...,θ_6 のある 2 つが等しいとき, 例えば, $\theta_2=\theta_6$ のときは

$$\theta_2=\theta_6=\sigma(\theta_2)=\sigma(\theta_6)=\theta_3$$

となり, すべて等しくなる. これは補題 4.1 より $K(x_1,...,x_5)=K(\theta_1,...,\theta_6)$ であることに矛盾する. ゆえに θ_2,...,θ_6 は互いに異なり, $\mathbb{Q}$ に含まれない. よって $f_{20}(x)$ は 1 次式と既

約5次式に分解され, 有理数根は θ_1 のみである.

逆に $f_{20}(x)$ が有理数根 θ_k をもつと仮定する. $f(x)$ が既約であるからGalois群 G は5-cycle ρ を含む. 補題4.1より $K(x_1,...,x_5)=K(\theta_1,...,\theta_6)$ であるから $f_{20}(x)$ は1次式と既約5次式に分解され ρ は θ_k のみを固定する. θ_k を固定する5-cycleは ρ のべきのみであるから $\langle\rho\rangle \trianglelefteq G$ を得る. 従って G は S_5 におけるSylow 5部分群の正規化群に含まれる. ゆえに G は F_{20}, F_{10}, F_5 のいずれかに共役である. ∎

定義 4.3 (判別式) $\mathbb{Q}$ 係数 n 次方程式 $g(x)=0$ の根 α_1, ..., α_n に対して

$$\Delta_g=\prod_{i<j}(\alpha_i-\alpha_j), \qquad D_g=\Delta_g^2$$

とおき, D_g を $g(x)$ の判別式という.

Δ_g, D_g を Δ, D と略記することがある.

$\mathbb{Q}$ 係数 n 次方程式 $g(x)=0$ の根を α_1, ..., α_n とし, $g(x)$ のGalois群を $G=Gal(E/\mathbb{Q})$ とおく. このとき G の元 σ によって根 α_1, ..., α_n が置換されるので $\sigma(\Delta_g)=\pm\Delta_g$ が成り立つ. 従って $D_g=\Delta_g^2$ は G の不変体 $E^G=\mathbb{Q}$ の元である.

補題 4.4 $\mathbb{Q}$ 係数方程式 $g(x)=0$ の分解体を E, $\Delta=\Delta_g$, *Galois* 群を $G=Gal(E/\mathbb{Q})$, $H=G\cap A_n$ とおく. このとき $E^H=\mathbb{Q}(\Delta)$ が成り立つ. 従って Δ が $\mathbb{Q}$ に含まれる条件は $G\leq A_n$ となることである.

Proof 偶置換は Δ を不変にするので $\mathbb{Q}(\Delta)\subseteq E^H$ が成り立つ. 一方, 定理1.7とGaloisの基本定理より

$$[E^H:\mathbb{Q}]=[G:H]=\frac{|G|}{|H|}=\frac{|GA_n|}{|A_n|}\leq\frac{|S_n|}{|A_n|}=2$$

が成り立つ. $[G:H]=2$ のとき $[E^H:\mathbb{Q}]=2$, かつ G は奇置換 ρ を含む. $\rho(\Delta)\neq\Delta$ より $\Delta\notin E^G=\mathbb{Q}$ となる. 従って $[\mathbb{Q}(\Delta):\mathbb{Q}]\geq 2$ となるので $\mathbb{Q}(\Delta)=E^H$ が成り立つ. $[G:H]=1$ のときも $G=H$ であることから, $\mathbb{Q}(\Delta)\subseteq E^H=E^G=\mathbb{Q}$ となり, $\mathbb{Q}(\Delta)=E^H$ を得る. 特に Δ が $\mathbb{Q}$ に含まれる条件は $E^H=\mathbb{Q}(\Delta)=\mathbb{Q}$, すなわち $G=H$ が成り立つことである. これは明らかに $G\leq A_n$ と同値である. ∎

補題 4.5 $\mathbb{Q}$ 係数既約5次方程式 $f(x)=0$ の判別式を $D=\Delta^2$ とする. $f(x)$ が可解ならば $D>0$ である.

Proof $f(x)$ の分解体を E, Galois群を G とする. 仮定より G は F_{20}, F_{10}, F_5 のいずれかに共役である. G が F_{10} または F_5 に共役であるときは $G\leq A_5$ が成り立つ. 従って補題4.4より $\Delta\in\mathbb{Q}$ となるので $D=\Delta^2>0$ となる.

G が F_{20} に共役のとき, $G = F_{20}$ として一般性を失わない. G の指数 2 の部分群は, F_{10} のみであるので, Galois の基本定理より E に含まれる $\mathbb{Q}$ の 2 次拡大は唯一つで, $G \not\leq A_5$ より $\mathbb{Q}(\Delta)$ に一致する. また F_5 は G の指数 4 の正規部分群であるから, F_5 に対応する $\mathbb{Q}$ の 4 次 Galois 拡大体 L が存在する. $\mathbb{Q}(\Delta) \subseteq L$ に注意されたい. ここで複素共役を L に作用させると, その不変体 K は $[L:K] \leq 2$ を満たすので $\mathbb{Q}(\Delta)$ を含む. 従って $\Delta \in \mathbb{R}$ より $D = \Delta^2 > 0$ が成り立つ. ∎

5 次方程式

$$x^5 + px^3 + qx^2 + rx + s = 0 \tag{4.4}$$

の 6 次分解式は

$$\begin{aligned}
f_{20}(x) \;=\;& x^6 + 8rx^5 + (2pq^2 - 6p^2r + 40r^2 - 50qs)x^4 \\
&+ (-2q^4 + 21pq^2r - 40p^2r^2 + 160r^3 - 15p^2qs - 400qrs + 125ps^2)x^3 \\
&+ (p^2q^4 - 6p^3q^2r - 8q^4r + 9p^4r^2 + 76pq^2r^2 - 136p^2r^3 + 400r^4 \\
&- 50pq^3s + 90p^2qrs - 1400qr^2s + 625q^2s^2 + 500prs^2)x^2 \\
&+ (-2pq^6 + 19p^2q^4r - 51p^3q^2r^2 + 3q^4r^2 + 32p^4r^3 + 76pq^2r^3 \\
&- 256p^2r^4 + 512r^5 - 31p^3q^3s - 58q^5s + 117p^4qrs + 105pq^3rs \\
&+ 260p^2qr^2s - 2400qr^3s - 108p^5s^2 - 325p^2q^2s^2 + 525p^3rs^2 \\
&+ 2750q^2rs^2 - 500pr^2s^2 + 625pqs^3 - 3125s^4)x \\
&+ (q^8 - 13pq^6r + p^5q^2r^2 + 65p^2q^4r^2 - 4p^6r^3 - 128p^3q^2r^3 + 17q^4r^3 \\
&+ 48p^4r^4 - 16pq^2r^4 - 192p^2r^5 + 256r^6 - 4p^5q^3s - 12p^2q^5s \\
&+ 18p^6qrs + 12p^3q^3rs - 124q^5rs + 196p^4qr^2s + 590pq^3r^2s \\
&- 160p^2qr^3s - 1600qr^4s - 27p^7s^2 - 150p^4q^2s^2 - 125pq^4s^2 \\
&- 99p^5rs^2 - 725p^2q^2rs^2 + 1200p^3r^2s^2 + 3250q^2r^2s^2 \\
&- 2000pr^3s^2 - 1250pqrs^3 + 3125p^2s^4 - 9375rs^4)
\end{aligned} \tag{4.5}$$

となる (計算は Mathematica による). 特に 3 項式 $x^5 + ax + b = 0$ の場合

$$\begin{aligned}
f_{20}(x) \;=\;& x^6 + 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^2 \\
&+ (512a^5 - 3125b^4)x + (256a^6 - 9375ab^4)
\end{aligned} \tag{4.6}$$

となる. また (4.4) の判別式 D は

$$\begin{aligned} D &= -4p^3q^2r^2 - 27q^4r^2 + 16p^4r^3 + 144pq^2r^3 - 128p^2r^4 + 256r^5 + 16p^3q^3s \\ &\quad + 108q^5s - 72p^4qrs - 630pq^3rs + 560p^2qr^2s - 1600qr^3s + 108p^5s^2 \\ &\quad + 825p^2q^2s^2 - 900p^3rs^2 + 2250q^2rs^2 + 2000pr^2s^2 - 3750pqs^3 + 3125s^4 \end{aligned} \tag{4.7}$$

である. 特に $x^5 + ax + b = 0$ の場合は

$$D = 256a^5 + 3125b^4 \tag{4.8}$$

となる. 以上から$\mathbb{Q}$ 係数既約 5 次方程式が与えられたとき, その 6 次分解式と判別式を上の式から計算可能である. 補題 1.26 を適用し, 有限個の有理数根の候補を 6 次分解式に代入することにより, 6 次分解式が有理数根をもつかどうか判定できる. 有理数根をもてば与えられた方程式は可解である. また, そのとき判別式 D は正となり, その実平方根 $\pm\Delta$ から拡大体 $\mathbb{Q}(\Delta)$ が得られる. これらの事実は後節で用いられる.

4.2 可解な5次方程式の解法

複素 (変) 数 $x_1, ..., x_5$ を根とする 5 次方程式を

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) \\ &= x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5 = 0 \end{aligned}$$

とおき, $E = \mathbb{Q}(x_1, ..., x_5)$, $F = \mathbb{Q}(s_1, ..., s_5)$ とする. E/F は Galois 拡大で $Gal(E/F) \simeq S_5$ である. ここで $y_i = x_i - \frac{s_1}{5}$ $(i = 1, ..., 5)$,

$$f^*(x) = (x - y_1)(x - y_2)(x - y_3)(x - y_4)(x - y_5)$$

とおくと, $f^*(x)$ は F 係数多項式で E は F 上の $f^*(x)$ の分解体である. 従って $f(x)$ と $f^*(x)$ の Galois 群は一致して $Gal(E/F)$ であり, F 係数方程式 $f(x) = 0$ を解くことと, F 係数方程式 $f^*(x) = 0$ を解くこととは同値である. 以上から $y_i, f^*(x)$ を改めて $x_i, f(x)$ とおき, その解法を考察することにする. なお $s_1 = x_1 + \cdots + x_5 = 0$, すなわち $f(x)$ の x^4 の係数は 0 であることを注意しておく.

さて, 1 の原始 5 乗根を 1 つ選び ζ とおく. $E(\zeta)$ は F 上の多項式 $f(x)(x^5 - 1)$ の分解体である. 従って $E(\zeta)/F$ は Galois 拡大である. 一方, p.35 で述べたように, $\mathbb{Q}(\zeta)/\mathbb{Q}$ は

Galois 拡大で $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ は位数 4 の巡回群である. また ζ の $\mathbb{Q}$ 上の最小多項式は

$$h_0(x) = x^4 + x^3 + x^2 + x + 1$$

である. 今, $h_0(x)$ が E 上で $h_0(x) = h_1(x)h_2(x)$ と 1 次以上の多項式の積に分解できたと仮定する. $h_1(x), h_2(x)$ はモニックであるとしてよい. $h_1(x), h_2(x)$ の係数は $\mathbb{Q}$ の 4 次拡大 $\mathbb{Q}(\zeta)$ の元であるから定理 1.35 より $\mathbb{Q}$ 上代数的である. 一方 $\mathbb{Q}$ 上の有理関数体 $E = \mathbb{Q}(x_1, ..., x_5)$ の元で $\mathbb{Q}$ 上代数的であるものは $\mathbb{Q}$ の元に限る (cf. [4, 2 章, 例 2.10]). 従って $h_0(x) = h_1(x)h_2(x)$ は $\mathbb{Q}$ 上での分解となるが, これは $h_0(x)$ が $\mathbb{Q}$ 上既約であることに矛盾する. 従って $h_0(x)$ は E 上で 1 次以上の多項式の積に分解できない. すなわち $h_0(x)$ は ζ の E 上の最小多項式である. これより $[E(\zeta) : E] = 4$ が成り立ち, $1, \zeta, \zeta^2, \zeta^3$ は E 上 1 次独立であることがわかる.

θ を前節と同様

$$\begin{aligned}\theta \;=\; & x_1^2x_2x_5 + x_1^2x_3x_4 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_5 \\ & + x_3^2x_2x_4 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_4 + x_5^2x_2x_3\end{aligned}$$

とおくと $K = F(\theta)$ は F_{20} の不変体である. 方程式 $f(x) = 0$ が可解ならば, その Galois 群は $F_{20} = \langle \sigma, \tau \rangle$ の部分群と見なせるので $K = F(\theta)$ は不変体に含まれる.

$E(\zeta) = E \vee K(\zeta)$ は明らかであるが, $E \cap K(\zeta) = K$ が成り立つ. なぜならば, $K \subseteq E \cap K(\zeta)$ は自明であるので, $E \cap K(\zeta)$ の任意の元を β とすると

$$\beta = \alpha_0 + \alpha_1\zeta + \alpha_2\zeta^2 + \alpha_3\zeta^3 \quad (\alpha_i \in K)$$

とおくことができ

$$\alpha_0 - \beta + \alpha_1\zeta + \alpha_2\zeta^2 + \alpha_3\zeta^3 = 0$$

となるが, $1, \zeta, \zeta^2, \zeta^3$ が E 上 1 次独立であることから $\beta = \alpha_0$, $\alpha_1 = \alpha_2 = \alpha_3 = 0$ が得られるからである. 系 3.35 より, E が K 上の $f(x)$ の分解体, $K(\zeta)$ が K 上の $x^5 - 1$ の分解体であることに注意すれば

$$Gal(E(\zeta)/K) \simeq Gal(E/K) \times Gal(K(\zeta)/K) \simeq F_{20} \times \mathbb{Z}_5^\sharp$$

が成り立つ. ここで $Gal(E(\zeta)/E)$ の元 ω で $\omega(\zeta) = \zeta^3$ を満たすものを選び, σ, τ を $Gal(E(\zeta)/K(\zeta))$ の元と見なせば

$$Gal(E(\zeta)/K) = F_{20} \times \langle \omega \rangle$$

が成り立つ.

次に Lagrange 分解式 r_1, r_2, r_3, r_4 を定義する.

$$\begin{aligned} r_1 &= x_1 + x_2\zeta + x_3\zeta^2 + x_4\zeta^3 + x_5\zeta^4 \\ r_2 &= x_1 + x_2\zeta^2 + x_3\zeta^4 + x_4\zeta + x_5\zeta^3 \\ r_3 &= x_1 + x_2\zeta^3 + x_3\zeta + x_4\zeta^4 + x_5\zeta^2 \\ r_4 &= x_1 + x_2\zeta^4 + x_3\zeta^3 + x_4\zeta^2 + x_5\zeta \end{aligned} \tag{4.9}$$

$x_1 + \cdots + x_5 = 0$ に注意すれば

$$\begin{aligned} x_1 &= \frac{1}{5}(r_1 + r_2 + r_3 + r_4) \\ x_2 &= \frac{1}{5}(\zeta^4 r_1 + \zeta^3 r_2 + \zeta^2 r_3 + \zeta r_4) \\ x_3 &= \frac{1}{5}(\zeta^3 r_1 + \zeta r_2 + \zeta^4 r_3 + \zeta^2 r_4) \\ x_4 &= \frac{1}{5}(\zeta^2 r_1 + \zeta^4 r_2 + \zeta r_3 + \zeta^3 r_4) \\ x_5 &= \frac{1}{5}(\zeta r_1 + \zeta^2 r_2 + \zeta^3 r_3 + \zeta^4 r_4) \end{aligned} \tag{4.10}$$

が導かれる. 従って $f(x) = 0$ を解くためには r_1, r_2, r_3, r_4 を求めればよい. r_1, r_2, r_3, r_4 をそれぞれ5乗したものを R_1, R_2, R_3, R_4 とすれば

$$\begin{aligned} R_1 &= r_1^5 = l_0 + l_1\zeta + l_2\zeta^2 + l_3\zeta^3 + l_4\zeta^4 \\ R_2 &= r_2^5 = l_0 + l_3\zeta + l_1\zeta^2 + l_4\zeta^3 + l_2\zeta^4 \\ R_3 &= r_3^5 = l_0 + l_2\zeta + l_4\zeta^2 + l_1\zeta^3 + l_3\zeta^4 \\ R_4 &= r_4^5 = l_0 + l_4\zeta + l_3\zeta^2 + l_2\zeta^3 + l_1\zeta^4 \end{aligned} \tag{4.11}$$

とおくことができる. ただし l_0, l_1, l_2, l_3, l_4 は

$$\begin{aligned} l_0 = {} & x_1^5 + x_2^5 + 20x_1x_2^3x_3 + 30x_1^2x_2x_3^2 + x_3^5 + 30x_1^2x_2^2x_4 + 20x_1^3x_3x_4 + 20x_2x_3^3x_4 \\ & + 30x_2^2x_3x_4^2 + 30x_1x_3^2x_4^2 + 20x_1x_2x_4^3 + x_4^5 + 20x_1^3x_2x_5 + 30x_2^2x_3^2x_5 + x_5^5 \\ & + 20x_1x_3^3x_5 + 20x_2^3x_4x_5 + 120x_1x_2x_3x_4x_5 + 30x_1^2x_4^2x_5 + 20x_3x_4^3x_5 \\ & + 30x_1x_2^2x_5^2 + 30x_1^2x_3x_5^2 + 30x_3^2x_4x_5^2 + 30x_2x_4^2x_5^2 + 20x_2x_3x_5^3 + 20x_1x_4x_5^3 \end{aligned} \tag{4.12}$$

$$\begin{aligned} l_1 \;=\; & 5x_1^4x_2 + 5x_2^4x_3 + 30x_1x_2^2x_3^2 + 10x_1^2x_3^3 + 20x_1x_2^3x_4 + 60x_1^2x_2x_3x_4 + 5x_3^4x_4 \\ & + 10x_1^3x_4^2 + 30x_2x_3^2x_4^2 + 10x_2^2x_4^3 + 20x_1x_3x_4^3 + 30x_1^2x_2^2x_5 + 20x_1^3x_3x_5 + 10x_2^3x_5^2 \\ & + 20x_2x_3^3x_5 + 60x_2^2x_3x_4x_5 + 60x_1x_3^2x_4x_5 + 60x_1x_2x_4^2x_5 + 5x_4^4x_5 \\ & + 60x_1x_2x_3x_5^2 + 30x_1^2x_4x_5^2 + 30x_3x_4^2x_5^2 + 10x_3^2x_5^3 + 20x_2x_4x_5^3 + 5x_1x_5^4 \end{aligned} \tag{4.13}$$

$$\begin{aligned} l_2 \;=\; & 10x_1^3x_2^2 + 5x_1^4x_3 + 10x_2^3x_3^2 + 20x_1x_2x_3^3 + 5x_2^4x_4 + 60x_1x_2^2x_3x_4 + 30x_1^2x_3^2x_4 \\ & + 30x_1^2x_2x_4^2 + 10x_3^3x_4^2 + 20x_2x_3x_4^3 + 5x_1x_4^4 + 20x_1x_2^3x_5 + 60x_1^2x_2x_3x_5 + 30x_2^2x_3x_5^2 \\ & + 5x_3^4x_5 + 20x_1^3x_4x_5 + 60x_2x_3^2x_4x_5 + 30x_2^2x_4^2x_5 + 60x_1x_3x_4^2x_5 \\ & + 30x_1x_3^2x_5^2 + 60x_1x_2x_4x_5^2 + 10x_4^3x_5^2 + 10x_1^2x_5^3 + 20x_3x_4x_5^3 + 5x_2x_5^4 \end{aligned} \tag{4.14}$$

$$\begin{aligned} l_3 \;=\; & 10x_1^2x_2^3 + 20x_1^3x_2x_3 + 10x_2^2x_3^3 + 5x_1x_3^4 + 5x_1^4x_4 + 20x_2^3x_3x_4 + 60x_1x_2x_3^2x_4 \\ & + 30x_1x_2^2x_4^2 + 30x_1^2x_3x_4^2 + 10x_3^2x_4^3 + 5x_2x_4^4 + 5x_2^4x_5 + 60x_1x_2^2x_3x_5 + 10x_1^3x_5^2 \\ & + 30x_1^2x_3^2x_5 + 60x_1^2x_2x_4x_5 + 20x_3^3x_4x_5 + 60x_2x_3x_4^2x_5 + 20x_1x_4^3x_5 \\ & + 30x_2x_3^2x_5^2 + 30x_2^2x_4x_5^2 + 60x_1x_3x_4x_5^2 + 20x_1x_2x_5^3 + 10x_4^2x_5^3 + 5x_3x_5^4 \end{aligned} \tag{4.15}$$

$$\begin{aligned} l_4 \;=\; & 5x_1x_2^4 + 30x_1^2x_2^2x_3 + 10x_1^3x_3^2 + 5x_2x_3^4 + 20x_1^3x_2x_4 + 30x_2^2x_3^2x_4 + 20x_1x_3^3x_4 + 10x_3^3x_5^2 \\ & + 10x_2^3x_4^2 + 60x_1x_2x_3x_4^2 + 10x_1^2x_4^3 + 5x_3x_4^4 + 5x_1^4x_5 + 20x_2^3x_3x_5 + 60x_1x_2x_3^2x_5 \\ & + 60x_1x_2^2x_4x_5 + 60x_1^2x_3x_4x_5 + 30x_3^2x_4^2x_5 + 20x_2x_4^3x_5 + 30x_1^2x_2x_5^2 \\ & + 60x_2x_3x_4x_5^2 + 30x_1x_4^2x_5^2 + 10x_2^2x_5^3 + 20x_1x_3x_5^3 + 5x_4x_5^4 \end{aligned} \tag{4.16}$$

であり

$$l_0 + l_1 + l_2 + l_3 + l_4 = (x_1 + x_2 + x_3 + x_4 + x_5)^5 = 0 \tag{4.17}$$

が成り立つ. 次に l_1, l_2, l_3, l_4 について考察していく.

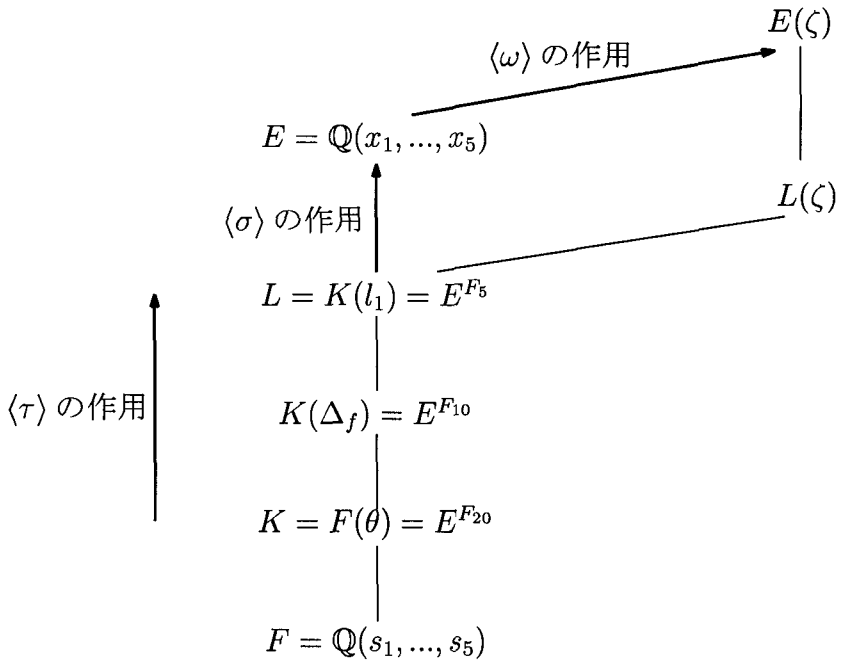
σ は r_1, r_2, r_3, r_4 に対して

$$r_1 \overset{\sigma}{\mapsto} r_1\zeta^4, \qquad r_2 \overset{\sigma}{\mapsto} r_2\zeta^3, \qquad r_3 \overset{\sigma}{\mapsto} r_3\zeta^2, \qquad r_4 \overset{\sigma}{\mapsto} r_4\zeta$$

と作用するので R_1, R_2, R_3, R_4 を固定する. 従って l_1, l_2, l_3, l_4 も固定する. 同様に τ は

$$r_1 \overset{\tau}{\mapsto} r_3 \overset{\tau}{\mapsto} r_4 \overset{\tau}{\mapsto} r_2 \overset{\tau}{\mapsto} r_1, \qquad\qquad l_1 \overset{\tau}{\mapsto} l_2 \overset{\tau}{\mapsto} l_4 \overset{\tau}{\mapsto} l_3 \overset{\tau}{\mapsto} l_1$$

と作用する.



ω の r_1, r_2, r_3, r_4 への作用は, τ の作用と一致する.

$$r_1 \overset{\omega}{\mapsto} r_3 \overset{\omega}{\mapsto} r_4 \overset{\omega}{\mapsto} r_2 \overset{\omega}{\mapsto} r_1$$

ただし ω は $l_0, ..., l_4$ を固定する.

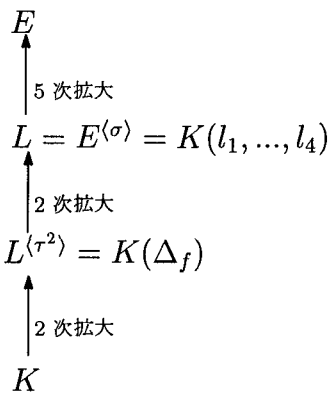
l_0 は σ, τ によって固定される E の元であるから $K = E^{F_{20}}$ に含まれる.

l_1, l_2, l_3, l_4 は σ によって固定され, τ によって置換されるので

$$h(x) = (x - l_1)(x - l_2)(x - l_3)(x - l_4)$$

は K 係数既約 4 次式である.

$L = K(l_1)$ とおくと, 上述のことから $[L : K] = 4$ である. また l_1 は σ で固定されるので $L \subseteq E^{\langle\sigma\rangle}$ が成り立つ. $[E : E^{\langle\sigma\rangle}] = 5$ より $[E^{\langle\sigma\rangle} : K] = 4$ となるので $L = E^{\langle\sigma\rangle}$ を得る. $l_2, l_3, l_4 \in E^{\langle\sigma\rangle}$ であるから $L = K(l_1) = K(l_1, l_2, l_3, l_4)$ が成り立つ. 従って L は $h(x)$ の分解体である.



さて τ の作用から $l_1+l_4,\ l_1l_4,\ l_2+l_3,\ l_2l_3$ は $L^{\langle\tau^2\rangle}=E^{\langle\sigma,\tau^2\rangle}$ に含まれる. $[L^{\langle\tau^2\rangle}:K]=2$ より $L^{\langle\tau^2\rangle}=K(\Delta_f)$ が成り立つ. よって $l_1+l_4,\ l_1l_4,\ l_2+l_3,\ l_2l_3$ は $K(\Delta_f)$ に含まれる. これより

$$l_1+l_4=-T_1-T_2\Delta_f,\quad l_1l_4=T_3+T_4\Delta_f\quad (T_1,T_2,T_3,T_4\in K)$$

とおくことができ, 両辺に τ を作用させると

$$l_2+l_3=-T_1+T_2\Delta_f,\qquad l_2l_3=T_3-T_4\Delta_f$$

が得られる. 以上より $h(x)$ は $K(\Delta_f)[x]$ で

$$\begin{aligned} h(x) &= \big(x^2-(l_1+l_4)x+l_1l_4\big)\big(x^2-(l_2+l_3)x+l_2l_3\big)\\ &= \big(x^2+(T_1+T_2\Delta_f)x+(T_3+T_4\Delta_f)\big)\big(x^2+(T_1-T_2\Delta_f)x+(T_3-T_4\Delta_f)\big) \end{aligned}\quad (4.18)$$

と2つの2次式に分解される.

これより T_1, T_2, T_3, T_4 がわかれば, すなわち各 T_i を $f(x)$ の係数と θ で表示できれば, 2つの2次式から l_1,l_2,l_3,l_4 を, l_1 と l_4 のペア, および l_2 と l_3 のペアとして求めることができる. さらに R_1, R_2, R_3, R_4 が (順序を無視して) 得られるので, それらの5乗根 r_1, r_2, r_3, r_4 から x_1, x_2, x_3, x_4, x_5 が得られることになる (後述).

T_1, T_2, T_3, T_4 の計算

$K=F(\theta)$ は $[K:F]=6$ を満たすので K の元は

$$k=\alpha_0+\alpha_1\theta+\alpha_2\theta^2+\alpha_3\theta^3+\alpha_4\theta^4+\alpha_5\theta^5$$

と一意的に表すことができる. ここで, $\alpha_i\ \ (i=0,...,5)$ は $F=\mathbb{Q}(s_1,...,s_5)$ の元, すなわち, x_1,..., x_5 の対称式である. $\theta=\theta_1$ として, S_5 を F_{20} による剰余類分解し, p.55 の式 (4.3) と同様に, その代表元を $k=T_i$ に作用させると, 等式

$$\begin{aligned} k &= \alpha_0+\alpha_1\theta_1+\alpha_2\theta_1^2+\alpha_3\theta_1^3+\alpha_4\theta_1^4+\alpha_5\theta_1^5\\ (1\ 2\ 3)k &= \alpha_0+\alpha_1\theta_2+\alpha_2\theta_2^2+\alpha_3\theta_2^3+\alpha_4\theta_2^4+\alpha_5\theta_2^5\\ (1\ 3\ 2)k &= \alpha_0+\alpha_1\theta_3+\alpha_2\theta_3^2+\alpha_3\theta_3^3+\alpha_4\theta_3^4+\alpha_5\theta_3^5\\ (1\ 2)k &= \alpha_0+\alpha_1\theta_4+\alpha_2\theta_4^2+\alpha_3\theta_4^3+\alpha_4\theta_4^4+\alpha_5\theta_4^5\\ (2\ 3)k &= \alpha_0+\alpha_1\theta_5+\alpha_2\theta_5^2+\alpha_3\theta_5^3+\alpha_4\theta_5^4+\alpha_5\theta_5^5\\ (1\ 3)k &= \alpha_0+\alpha_1\theta_6+\alpha_2\theta_6^2+\alpha_3\theta_6^3+\alpha_4\theta_6^4+\alpha_5\theta_6^5 \end{aligned}$$

を得る. これを α_j を未知数とする連立方程式と見て, Cramer の公式で解き, α_i $(i=0,...,6)$ を求めることができる. α_i は有理式として得られるが, その分母は Vandermonde の行列式である.

$$A=\begin{bmatrix} 1 & \theta_1 & \theta_1^2 & \theta_1^3 & \theta_1^4 & \theta_1^5 \\ 1 & \theta_2 & \theta_2^2 & \theta_2^3 & \theta_2^4 & \theta_2^5 \\ 1 & \theta_3 & \theta_3^2 & \theta_3^3 & \theta_3^4 & \theta_3^5 \\ 1 & \theta_4 & \theta_4^2 & \theta_4^3 & \theta_4^4 & \theta_4^5 \\ 1 & \theta_5 & \theta_5^2 & \theta_5^3 & \theta_5^4 & \theta_5^5 \\ 1 & \theta_6 & \theta_6^2 & \theta_6^3 & \theta_6^4 & \theta_6^5 \end{bmatrix}, \qquad |A|=-\prod_{i<j}^{6}(\theta_i-\theta_j)=\Delta_f^3 C$$

ここで C は x_1,..., x_5 の対称式である. 理論的には, このようにして T_1, T_2, T_3, T_4 を $f(x)$ の係数と θ から計算することが可能であるが, 実際に求めるには (Mathematica を用いても) 困難であるため, ここでは 3 項式 $x^5+ax+b=0$ の場合の結果をあげるにとどめる.

$$\begin{aligned} T_1 &= (512a^5-15625b^4+768a^4\theta+416a^3\theta^2+112a^2\theta^3+24a\theta^4+4\theta^5)/(50b^3) \\ T_2 &= (3840a^5-78125b^4+4480a^4\theta+2480a^3\theta^2+760a^2\theta^3 \\ &\quad +140a\theta^4+30\theta^5)/(512a^5b+6250b^5) \\ T_3 &= (-18880a^5+781250b^4-34240a^4\theta-21260a^3\theta^2-5980a^2\theta^3 \\ &\quad -1255a\theta^4-240\theta^5)/(2b^2) \\ T_4 &= (68800a^5+25000a^4\theta+11500a^3\theta^2+3250a^2\theta^3 \\ &\quad +375a\theta^4+100\theta^5)/(512a^5+6250b^4) \end{aligned} \tag{4.19}$$

l_1, l_2, l_3, l_4 と R_1, R_2, R_3, R_4

可解な 5 次方程式 $f(x)=0$ が与えられれば, その係数から, 判別式 D_f, 6 次分解式 $f_{20}(x)$ とその有理数根 θ, T_i, および 4 次多項式 $h(x)$ は計算できる. 判別式 D_f の平方根 Δ_f は $\pm\Delta_f$ のいずれか特定できないので, 1 つを選び Δ_f' とする. このとき $h(x)$ は (4.18) のように 2 つの 2 次式に分解でき, これらの根 l_1', l_2', l_3', l_4' がペア $\{l_1', l_4'\}$, $\{l_2', l_3'\}$ として得られる. このとき $\{l_1, l_4\}=\{l_1', l_4'\}$, $\{l_2, l_3\}=\{l_2', l_3'\}$ であるか, または $\{l_1, l_4\}=\{l_2', l_3'\}$, $\{l_2, l_3\}=\{l_1', l_4'\}$ であるかのいずれかが成り立つ. このように, 2 つのペア $\{l_1', l_4'\}$, $\{l_2', l_3'\}$ のいずれに l_1 が含まれているか, また, ペア $\{l_1', l_4'\}$ に l_1 が含まれていることがわかっても, それが l_1', l_4' のいずれであるかは決定できない. 以下 l_1', l_2', l_3', l_4' を (4.11) に代入して得

られる, 仮の R_1, R_2, R_3, R_4 を R'_1, R'_2, R'_3, R'_4 とおくことにする.

補題 4.6 $(l_1 - l_4)(l_2 - l_3) = c\Delta_f$ を満たす K の元 c が存在する.

Proof 補題4.4より $L^{\langle\tau^2\rangle} = K(\Delta_f)$ が成り立つ. $\lambda = (l_1 - l_4)(l_2 - l_3)$ とおけば λ は τ^2 によって固定されるから $K(\Delta_f)$ の元である. 従って適当な K の元 s, t により $\lambda = s + t\Delta_f$ と表すことができる. τ を作用させると

$$\tau(\lambda) = \tau\big((l_1 - l_4)(l_2 - l_3)\big) = (l_2 - l_3)(l_4 - l_1) = -\lambda = -s - t\Delta_f,$$

$$\tau(\lambda) = \tau(s + t\Delta_f) = \tau(s) + \tau(t)\tau(\Delta_f) = s + t(-\Delta_f)$$

となるので $s = 0$ を得る. よって $\lambda = t\Delta_f$ $(t \in K)$ と表される. ∎

K の元 c は T_i と同様に $f(x) = 0$ の係数と6次分解式の有理数根 θ で表すことができる. 実際 $x^5 + ax + b = 0$ の場合は次のようになる.

$$\begin{aligned} c \;=\; & (-1036800a^5 + 48828125b^4 - 2280000a^4\theta - 1291500a^3\theta^2 \\ & - 399500a^2\theta^3 - 76625a\theta^4 - 16100\theta^5)/(256a^5 + 3125b^4) \end{aligned} \tag{4.20}$$

さて, 仮に $\Delta'_f = \Delta_f$ であったと仮定すると, $\{l'_1, l'_4\} = \{l_1, l_4\}$, $\{l'_2, l'_3\} = \{l_2, l_3\}$ であるが, 補題4.6より

$$(l'_1, l'_2, l'_3, l'_4) = (l_1, l_2, l_3, l_4) \quad \text{または} \quad (l'_1, l'_2, l'_3, l'_4) = (l_4, l_3, l_2, l_1)$$

が成り立つ. これらを(4.11)に代入すると, $(l'_1, l'_2, l'_3, l'_4) = (l_1, l_2, l_3, l_4)$ のときは (R'_1, R'_2, R'_3, R'_4) (R_1, R_2, R_3, R_4), $(l'_1, l'_2, l'_3, l'_4) = (l_4, l_3, l_2, l_1)$ のときは $(R'_1, R'_2, R'_3, R'_4) = (R_4, R_3, R_2, R_1)$ が成り立つ. $\Delta'_f = -\Delta_f$ のときも同様に判定でき, その結果をまとめると次のようになる.

(1) $\Delta'_f = \Delta_f$

- $(l'_1, l'_2, l'_3, l'_4) = (l_1, l_2, l_3, l_4)$, $(R'_1, R'_2, R'_3, R'_4) = (R_1, R_2, R_3, R_4)$
- $(l'_1, l'_2, l'_3, l'_4) = (l_4, l_3, l_2, l_1)$, $(R'_1, R'_2, R'_3, R'_4) = (R_4, R_3, R_2, R_1)$

(2) $\Delta'_f = -\Delta_f$

- $(l'_1, l'_2, l'_3, l'_4) = (l_2, l_4, l_1, l_3)$, $(R'_1, R'_2, R'_3, R'_4) = (R_3, R_1, R_4, R_2)$
- $(l'_1, l'_2, l'_3, l'_4) = (l_3, l_1, l_4, l_2)$, $(R'_1, R'_2, R'_3, R'_4) = (R_2, R_4, R_1, R_3)$

r_1, r_2, r_3, r_4 の決定

ここでは Lagrange 分解式 r_1, r_2, r_3, r_4 を求める方法について述べる. $R_i = r_i^5$ のみでは, r_i を $r_i, r_i\zeta, r_i\zeta^2, r_i\zeta^3, r_i\zeta^4$ のいずれか特定できないのであるが, 仮に r_1' を1つ選べば, 残りの r_2', r_3', r_4' は一意に決定される. まずこの事実を証明する.

補題 4.7 積 r_1r_4, r_2r_3 は体 $K(\sqrt{5}\Delta_f)$ に含まれる.

Proof　p.60 で述べたように ζ の E 上の最小多項式は $h_0(x) = x^4+x^3+x^2+x+1$ である. 従って E の部分体 K 上の最小多項式も $h_0(x)$ である. これより $[K(\zeta):K]=4$ であり, $Gal(K(\zeta)/K)$ は位数 4 の巡回群 $\langle\omega\rangle$ に一致する. $\langle\omega\rangle$ の指数 2 の部分群はただ1つであるから, Galois の基本定理より $K(\zeta)/K$ の中間体で K の 2 次拡大体であるものはただ1つである. 一方

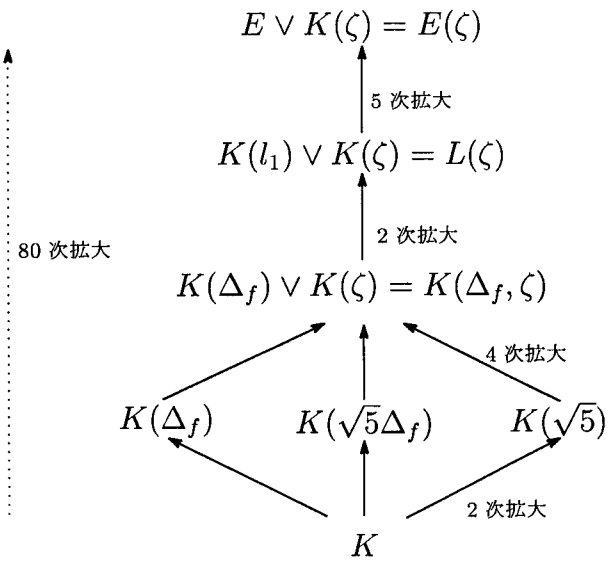
$$h_0(x) = x^4+x^3+x^2+x+1 = \left(x^2+\frac{1+\sqrt{5}}{2}x+1\right)\left(x^2+\frac{1-\sqrt{5}}{2}x+1\right)$$

と分解できるので $\sqrt{5} \in K(\zeta)$ を得る. 従って $K(\zeta)/K$ の中間体で K の 2 次拡大体であるものは $K(\sqrt{5})$ のみである.

r_1r_4, r_2r_3 は $E(\zeta)$ の自己同型 σ, τ^2, $\tau\omega^{-1}$ によって固定される. $Gal(E(\zeta)/K) = F_{20}\times\langle\omega\rangle$ の指数 2 の部分群は

$F_{10}\times\langle\omega\rangle$, $F_{20}\times\langle\omega^2\rangle$, $\langle\sigma,\tau^2,\tau\omega^{-1}\rangle$

の3つであり, それらに対応する K の 2 次拡大体は $K(\Delta_f)$, $K(\sqrt{5})$, $K(\sqrt{5}\Delta_f)$ である. よって $r_1r_4, r_2r_3 \in K(\sqrt{5}\Delta_f)$ が成り立つ. ∎



補題4.5より $\sqrt{5}\Delta_f$ は実数である. 従って $K(\sqrt{5}\Delta_f)$ は $\mathbb{R}$ に含まれるので r_1r_4, r_2r_3 も実数である. これより, 仮に r_1' として $r_1\zeta$ を選んだ場合, $r_1'r_4'$ が実数であるという条件より, r_4' として $r_4\zeta^4$ を選ぶことになる. r_1' として他のものを選んだ場合も, $r_1'r_4'$ が実数であるという条件より, r_4' の選び方は一意となる. r_2' から r_3' の選び方が一意に定まることも同様である.

2元 $r_1r_2^2+r_4r_3^2$ と $r_3r_1^2+r_2r_4^2$ は σ, τ^2, $\tau\omega^{-1}$ によって固定される. 従って $r_1r_2^2+r_4r_3^2$, $r_3r_1^2+r_2r_4^2$ は $K(\sqrt{5}\Delta_f)$ に含まれる. ゆえに適当な K の元 u, v を用いて

$$r_1r_2^2+r_4r_3^2=u+v\sqrt{5}\Delta_f$$

と表される. これに τ を作用させると

$$r_3r_1^2+r_2r_4^2=u-v\sqrt{5}\Delta_f$$

が得られる. $f(x)=x^5+ax+b$ の場合 u,v は次のように与えられる.

$$\begin{aligned} u &= 0 \\ v &= (-2048a^7+25000a^2b^4-3072a^6\theta-6250ab^4\theta-1664a^5\theta^2-3125b^4\theta^2 \\ &\quad -448a^4\theta^3-96a^3\theta^4-16a^2\theta^5)/(32000a^5b^3+390625b^7) \end{aligned} \tag{4.21}$$

補題 4.8 r_1' を1つ選ぶと, r_2', r_3', r_4' の選び方は一意に定まる.

Proof 上で述べたことから, 適当な $u,v\in K$ が存在して r_1, r_2, r_3, r_4 は次式を満たす.

$$r_1r_2^2+r_4r_3^2=u+v\sqrt{5}\Delta_f,\qquad r_3r_1^2+r_2r_4^2=u-v\sqrt{5}\Delta_f \tag{4.22}$$

仮に r_1' を1つ選んだとする. このとき r_4' は一意に定まる. r_2' は(4.22)を満たすような R_2' の5乗根を選ぶのであるが, 今, その選び方が2通りあったとして, それらを r_2', $\varepsilon r_2'$ とする. ただし ε は1の原始5乗根である. r_2 として r_2' を選ぶと r_3' は一意に定まり, r_2 として $\varepsilon r_2'$ を選んだときは r_3 として $\bar{\varepsilon}r_3'$ が選ばれる. ここで $\bar{\varepsilon}$ は ε の複素共役である. これらの選び方から

$$\begin{cases} r_1'(r_2')^2+r_4'(r_3')^2 = u+v\sqrt{5}\Delta_f \\ r_3'(r_1')^2+r_2'(r_4')^2 = u-v\sqrt{5}\Delta_f \end{cases} \qquad \begin{cases} r_1'(\varepsilon r_2')^2+r_4'(\bar{\varepsilon}r_3')^2 = u+v\sqrt{5}\Delta_f \\ (\bar{\varepsilon}r_3')(r_1')^2+(\varepsilon r_2')(r_4')^2 = u-v\sqrt{5}\Delta_f \end{cases}$$

が成り立つ. 従って

$$\begin{aligned} r_1'(r_2')^2+r_4'(r_3')^2 &= r_1'(\varepsilon r_2')^2+r_4'(\bar{\varepsilon}r_3')^2 \\ r_3'(r_1')^2+r_2'(r_4')^2 &= (\bar{\varepsilon}r_3')(r_1')^2+(\varepsilon r_2')(r_4')^2 \end{aligned}$$

より

$$\frac{r_1'(r_2')^2}{r_4'(r_3')^2} = -\frac{1-\bar{\varepsilon}^2}{1-\varepsilon^2} = -\frac{\varepsilon^2-1}{\varepsilon^2-\varepsilon^4} = \frac{1}{\varepsilon^2} \tag{4.23}$$

$$\frac{r_3'(r_1')^2}{r_2'(r_4')^2} = -\frac{1-\varepsilon}{1-\bar{\varepsilon}} = -\frac{\varepsilon-\varepsilon^2}{\varepsilon-1} = \varepsilon \tag{4.24}$$

が得られる. (4.23) と (4.24) から ε を消去すれば $(r_1')^5 = (r_4')^5$ となるので $r_4' = \zeta^i r_1'$ と表される. $\tau^2(r_1') = r_4' = \zeta^i r_1'$ であることから

$$r_1' = \tau^4(r_1') = \tau^2(r_4') = \zeta^i \tau^2(r_1') = \zeta^{2i} r_1'$$

となるので $\zeta^{2i} = 1$ より $\zeta^i = 1$ を得る. これより $r_1' = r_4'$ となり, (4.24) に代入すると $r_3' = \varepsilon r_2'$ が得られる. このとき $\tau^2(r_2') = r_3'$ であることから

$$r_2' = \tau^4(r_2') = \tau^2(r_3') = \varepsilon \tau^2(r_2') = \varepsilon^2 r_2'$$

となり ε が 1 の原始 5 乗根であることに矛盾する. よって (4.22) を満たすような R_2' の 5 乗根 r_2' はただ一つである. ∎

可解な 5 次方程式の解法の手順

ここでは有理数係数既約 5 次方程式

$$f(x) = x^5 + px^3 + qx^2 + rx + s = 0$$

が可解な Galois 群 G をもつものとして, その解法の手順を述べる.

(1) $f(x)$ の係数から次のものを計算する.

- $f(x)$ の判別式 $D_f = \Delta_f^2$
- 6 次分解式 $f_{20}(x)$ とその有理数根 θ

特に D_f と θ は有理数である.

(2) D_f の平方根を 1 つ選び Δ とおく. $\Delta = \Delta_f$ または $\Delta = -\Delta_f$ である.

(3) $f(x)$ の係数と θ を用いて有理数 T_1, T_2, T_3, T_4 を計算する.

(4) 次の2次式の根のペア $\{l'_1, l'_4\}$, $\{l'_2, l'_3\}$ を求め, $l'_0 = -l'_1 - l'_2 - l'_3 - l'_4$ とおく.

$$x^2 + (T_1 + T_2\Delta)x + (T_3 + T_4\Delta), \quad x^2 + (T_1 - T_2\Delta)x + (T_3 - T_4\Delta) \tag{4.25}$$

ただし l'_1, l'_2, l'_3, l'_4 は条件

$$(l'_1 - l'_4)(l'_2 - l'_3) = c\Delta \tag{4.26}$$

を満たすように定める. なお c は $f(x)$ の係数と θ を用いて計算できる有理数である.

(5) (4.11) を用いて R'_1, R'_2, R'_3, R'_4 を計算する.

(6) R'_1 の5乗根 r'_1 を1つ選び, 補題4.7と(4.22)から一意に定まる r'_2, r'_3, r'_4 を計算する.

(7) (4.10) を用いて $x'_1, x'_2, x'_3, x'_4, x'_5$ を求める.

ここで, 上の手順で得られた $x'_1, x'_2, x'_3, x'_4, x'_5$ が実際 $f(x)$ の根であることを確かめておくことにする. 手順(2)での Δ の選び方, 手順(4)での l'_1, l'_2, l'_3, l'_4 の定め方, および, それから得られる R'_1, R'_2, R'_3, R'_4 については, 次の4通りのいずれかであった.

(i) $\Delta = \Delta_f$, $(l'_1, l'_2, l'_3, l'_4) = (l_1, l_2, l_3, l_4)$, $(R'_1, R'_2, R'_3, R'_4) = (R_1, R_2, R_3, R_4)$

(ii) $\Delta = \Delta_f$, $(l'_1, l'_2, l'_3, l'_4) = (l_4, l_3, l_2, l_1)$, $(R'_1, R'_2, R'_3, R'_4) = (R_4, R_3, R_2, R_1)$

(iii) $\Delta = -\Delta_f$, $(l'_1, l'_2, l'_3, l'_4) = (l_2, l_4, l_1, l_3)$, $(R'_1, R'_2, R'_3, R'_4) = (R_3, R_1, R_4, R_2)$

(iv) $\Delta = -\Delta_f$, $(l'_1, l'_2, l'_3, l'_4) = (l_3, l_1, l_4, l_2)$, $(R'_1, R'_2, R'_3, R'_4) = (R_2, R_4, R_1, R_3)$

(i) の場合

この場合 r'_1 は $r_1, r_1\zeta, r_1\zeta^2, r_1\zeta^3, r_1\zeta^4$ のいずれかである.

- $r'_1 = r_1$ のときは $(r'_1, r'_2, r'_3, r'_4) = (r_1, r_2, r_3, r_4)$ となるので

$$(x'_1, x'_2, x'_3, x'_4, x'_5) = (x_1, x_2, x_3, x_4, x_5)$$

が成り立つ.

- $r'_1 = r_1\zeta$ のときは $(r'_1, r'_2, r'_3, r'_4) = (r_1\zeta, r_2\zeta^2, r_3\zeta^3, r_4\zeta^4)$ となるので

$$(x'_1, x'_2, x'_3, x'_4, x'_5) = (x_5, x_1, x_2, x_3, x_4)$$

が成り立つ.

- $r_1' = r_1\zeta^2$ のときは $(r_1', r_2', r_3', r_4') = (r_1\zeta^2, r_2\zeta^4, r_3\zeta, r_4\zeta^3)$ となるので

$$(x_1', x_2', x_3', x_4', x_5') = (x_4, x_5, x_1, x_2, x_3)$$

が成り立つ.

- $r_1' = r_1\zeta^3$ のときは $(r_1', r_2', r_3', r_4') = (r_1\zeta^3, r_2\zeta, r_3\zeta^4, r_4\zeta^2)$ となるので

$$(x_1', x_2', x_3', x_4', x_5') = (x_3, x_4, x_5, x_1, x_2)$$

が成り立つ.

- $r_1' = r_1\zeta^4$ のときは $(r_1', r_2', r_3', r_4') = (r_1\zeta^4, r_2\zeta^3, r_3\zeta^2, r_4\zeta)$ となるので

$$(x_1', x_2', x_3', x_4', x_5') = (x_2, x_3, x_4, x_5, x_1)$$

が成り立つ.

(ii)～(iv) についても, (i) の場合と同様にすればよい.

(ii) の場合

- $(r_1', r_2', r_3', r_4') = (r_4, r_3, r_2, r_1)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_1, x_5, x_4, x_3, x_2)$
- $(r_1', r_2', r_3', r_4') = (r_4\zeta, r_3\zeta^2, r_2\zeta^3, r_1\zeta^4)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_2, x_1, x_5, x_4, x_3)$
- $(r_1', r_2', r_3', r_4') = (r_4\zeta^2, r_3\zeta^4, r_2\zeta, r_1\zeta^3)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_3, x_2, x_1, x_5, x_4)$
- $(r_1', r_2', r_3', r_4') = (r_4\zeta^3, r_3\zeta, r_2\zeta^4, r_1\zeta^2)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_4, x_3, x_2, x_1, x_5)$
- $(r_1', r_2', r_3', r_4') = (r_4\zeta^4, r_3\zeta^3, r_2\zeta^2, r_1\zeta)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_5, x_4, x_3, x_2, x_1)$

(iii) の場合

- $(r_1', r_2', r_3', r_4') = (r_3, r_1, r_4, r_2)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_1, x_3, x_5, x_2, x_4)$
- $(r_1', r_2', r_3', r_4') = (r_3\zeta, r_1\zeta^2, r_4\zeta^3, r_2\zeta^4)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_4, x_1, x_3, x_5, x_2)$
- $(r_1', r_2', r_3', r_4') = (r_3\zeta^2, r_1\zeta^4, r_4\zeta, r_2\zeta^3)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_2, x_4, x_1, x_3, x_5)$

- $(r_1', r_2', r_3', r_4') = (r_3\zeta^3, r_1\zeta, r_4\zeta^4, r_2\zeta^2)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_5, x_2, x_4, x_1, x_3)$
- $(r_1', r_2', r_3', r_4') = (r_3\zeta^4, r_1\zeta^3, r_4\zeta^2, r_2\zeta)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_3, x_5, x_2, x_4, x_1)$

(iv) の場合

- $(r_1', r_2', r_3', r_4') = (r_2, r_4, r_1, r_3)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_1, x_4, x_2, x_5, x_3)$
- $(r_1', r_2', r_3', r_4') = (r_2\zeta, r_4\zeta^2, r_1\zeta^3, r_3\zeta^4)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_3, x_1, x_4, x_2, x_5)$
- $(r_1', r_2', r_3', r_4') = (r_2\zeta^2, r_4\zeta^4, r_1\zeta, r_3\zeta^3)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_5, x_3, x_1, x_4, x_2)$
- $(r_1', r_2', r_3', r_4') = (r_2\zeta^3, r_4\zeta, r_1\zeta^4, r_3\zeta^2)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_2, x_5, x_3, x_1, x_4)$
- $(r_1', r_2', r_3', r_4') = (r_2\zeta^4, r_4\zeta^3, r_1\zeta^2, r_3\zeta)$ から $(x_1', x_2', x_3', x_4', x_5') = (x_4, x_2, x_5, x_3, x_1)$

このように, いずれの場合も順序を無視すれば $f(x)$ の根がすべて得られることがわかる.

最後に, 次節で必要となる次の定理を証明しておく.

定理 4.9 (5次方程式の Galois 群) 有理数係数既約 5 次方程式

$$f(x) = x^5 + px^3 + qx^2 + rx + s = 0$$

が可解な *Galois* 群 G をもつとき, 次が成り立つ.

(1) Δ_f が有理数でないとき $G \simeq F_{20}$ である.

(2) Δ_f が 有理数で, 次の2つの 2 次式が $\mathbb{Q}$ 上既約のとき $G \simeq F_{10}$ であり, $\mathbb{Q}$ 上可約のとき $G \simeq F_5$ である.

$$x^2 + (T_1 + T_2\Delta_f)x + (T_3 + T_4\Delta_f), \qquad x^2 + (T_1 - T_2\Delta_f)x + (T_3 - T_4\Delta_f)$$

Proof $f(x)$ の $\mathbb{Q}$ 上の分解体を E とする. G は F_{20} の部分群に共役である. 以下, 簡単のため G は F_{20} の部分群であるとする.

Δ_f が有理数でないとき, 補題 4.4 より G は奇置換を含む. F_{20} に含まれる奇置換は 4-cycle のみであるから $G = F_{20}$ が成り立つ.

Δ_f が有理数のとき, T_1, T_2, T_3, T_4 が $f(x)$ の係数と θ を用いて計算できる有理数であるから, 次の2式は有理数係数である.

$$x^2 + (T_1 + T_2\Delta_f)x + (T_3 + T_4\Delta_f), \qquad x^2 + (T_1 - T_2\Delta_f)x + (T_3 - T_4\Delta_f)$$

一方, 補題4.4より G は A_5 の部分群である. ゆえに, $G = F_{10}$ か $G = F_5$ が成り立つ. ここで2次式の1つが $\mathbb{Q}$ 上可約ならば l_1, l_2, l_3, l_4 の1つ l_k が有理数となり, $l_1, l_2, l_3, l_4 \in \mathbb{Q}(l_k)$ より l_1, l_2, l_3, l_4 すべてが有理数となる. 従って2つの2次式は共に $\mathbb{Q}$ 上可約である. このとき p.63 の図式からわかるように $[E : \mathbb{Q}(l_1)] = 5$ であり, $\mathbb{Q}(l_1) = \mathbb{Q}$ であるから $G = F_5$ が成り立つ.

2つの2次式が共に $\mathbb{Q}$ 上既約であるときは $[\mathbb{Q}(l_1) : \mathbb{Q}] = 2$ となる. 従って $[E : \mathbb{Q}] = 10$ となるので $G = F_{10}$ が成り立つ. ∎

4.3 5次方程式の解法例1

例 1 $f(x) = x^5 + 15x + 12 = 0$

- Eisenstein の判定法より $f(x)$ は $\mathbb{Q}$ 上既約であり, 6次分解式は

$$f_{20}(x) = x^6 + 120x^5 + 9000x^4 + 540000x^3 + 20250000x^2 + 324000000x$$

となる. これは有理数根 $\theta = 0$ を持つので, 定理4.2より $f(x) = 0$ は可解である.

- 判別式は $D_f = 2^{10} \cdot 3^4 \cdot 5^5$ であるから, その平方根 $\pm 7200\sqrt{5}$ は有理数でない. 従って, 定理4.9より $f(x)$ の Galois 群は F_{20} に同型である.

- D_f の平方根 $\Delta = 7200\sqrt{5}$, を1つ選び固定する. また1の原始5乗根

$$\zeta = e^{\frac{2}{5}\pi i} = \frac{1}{4}(\sqrt{5} - 1 + i\sqrt{10 + 2\sqrt{5}})$$

を固定する.

- (4.19), (4.20), (4.21) より

$$T_1 = 750,\ T_2 = \frac{5}{24},\ T_3 = 6468750,\ T_4 = \frac{3225}{32},\ c = \frac{3475}{4},\ v = -\frac{1}{240}$$

が得られる.

- 補題4.6を満たすように次の2つの2次方程式

$$x^2 + (750 + 1500\sqrt{5})x + 6468750 + 725625\sqrt{5} = 0$$

$$x^2 + (750 - 1500\sqrt{5})x + 6468750 - 725625\sqrt{5} = 0$$

の根 l_1, l_2, l_3, l_4 を次のように定める.

$$\begin{aligned} l_1 &= -375 - 750\sqrt{5} + 75i\sqrt{625 + 29\sqrt{5}} \\ l_4 &= -375 - 750\sqrt{5} - 75i\sqrt{625 + 29\sqrt{5}} \\ l_2 &= -375 + 750\sqrt{5} - 75i\sqrt{625 - 29\sqrt{5}} \\ l_3 &= -375 + 750\sqrt{5} + 75i\sqrt{625 - 29\sqrt{5}} \end{aligned}$$

このとき $l_0 = 1500$ となり, (4.11) より

$$R_1 = -75(25 + 7\sqrt{10}) < 0 \qquad R_2 = 225(25 - 8\sqrt{10}) < 0$$
$$R_3 = 225(25 + 8\sqrt{10}) > 0 \qquad R_4 = 75(-25 + 7\sqrt{10}) < 0$$

が得られる.

- R_1 の5つの5乗根のうち, 実数根を r_1 として選び

$$r_1 = -\sqrt[5]{75(25 + 7\sqrt{10})}$$

と表すことにする. 条件式 (4.22)

$$r_1 r_2^2 + r_4 r_3^2 = -150, \qquad r_3 r_1^2 + r_2 r_4^2 = 150$$

を満たす r_2, r_3, r_4 は実数となり次のように表される.

$$r_2 = -\sqrt[5]{225(-25 + 8\sqrt{10})}, \quad r_3 = \sqrt[5]{225(25 + 8\sqrt{10})}, \quad r_4 = -\sqrt[5]{75(25 - 7\sqrt{10})})$$

- r_1, r_2, r_3, r_4 から (4.10) により5つの根が得られるが, 実数根は

$$x_1 = \frac{1}{5}\left(-\sqrt[5]{75(25 + 7\sqrt{10})} - \sqrt[5]{225(-25 + 8\sqrt{10})} + \sqrt[5]{225(25 + 8\sqrt{10})} - \sqrt[5]{75(25 - 7\sqrt{10})}\right)$$

のみであることが, 次章の定理5.4より導かれる.

例 2 $f(x) = x^5 - 5x + 12 = 0$

- $f(x-2) = x^5 - 10x^4 + 40x^3 - 80x^2 + 75x - 10$ は Eisenstein の判定法より $\mathbb{Q}$ 上既約である. ゆえに $f(x)$ も既約である. 6次分解式

$$f_{20}(x) = x^6 - 40x^5 + 1000x^4 - 20000x^3 + 250000x^2 - 66400000x + 976000000$$

は有理数根 $\theta = 40$ を持つので $f(x) = 0$ は可解である.

- 判別式は, $D_f = 2^{12} \cdot 5^6$ となり, 平方根 ± 8000 は有理数である. 従って定理 4.9 より $f(x)$ の Galois 群は F_{10} か F_5 に同型である.
- D_f の平方根を $\Delta = 8000$ を固定し, 例1と同様1の原始5乗根 $\zeta = e^{\frac{2}{5}\pi i}$ を固定する.
- (4.19), (4.20), (4.21) より

$$T_1 = -1250,\ T_2 = \frac{5}{16},\ T_3 = 5468750,\ T_4 = \frac{4375}{64},\ c = -\frac{5625}{4},\ v = -\frac{1}{160}$$

が得られる.

- l_1, l_2, l_3, l_4 を根とする2次方程式は

$$x^2 + 1250x + 6015625 = 0, \qquad x^2 - 3750x + 4921875 = 0$$

である. 前の方程式から根 l_1, l_4 を選ぶことにし

$$l_1 = -625 + 750i\sqrt{10}$$

とすれば, $c\Delta_f = -11250000$ であることから l_4, l_2, l_3 は次のように定まる.

$$l_4 = -625 - 750i\sqrt{10}, \quad l_2 = 1875 + 375i\sqrt{10}, \quad l_3 = 1875 - 375i\sqrt{10}$$

このとき, $l_0 = -2500$ である. また l_1 が有理数でないことから, $f(x)$ の Galois 群は F_{10} に同型である.

- (4.11) から R_1, R_2, R_3, R_4 は次のようになる.

$$\begin{aligned}
R_1 &= -3125 - 1250\sqrt{5} - 375\sqrt{125 + 55\sqrt{5}} < 0 \\
R_2 &= -3125 + 1250\sqrt{5} - 1875\sqrt{5 + \sqrt{5}} + 750\sqrt{5(5 + \sqrt{5})} < 0 \\
R_3 &= -3125 + 1250\sqrt{5} + 1875\sqrt{5 + \sqrt{5}} - 750\sqrt{5(5 + \sqrt{5})} > 0 \\
R_4 &= -3125 - 1250\sqrt{5} + 375\sqrt{125 + 55\sqrt{5}} < 0
\end{aligned}$$

- r_1 として R_1 の 実5乗根

$$r_1 = -\sqrt[5]{3125 + 1250\sqrt{5} + 375\sqrt{125 + 55\sqrt{5}}}$$

を選ぶ. 条件式

$$r_1r_2^2+r_4r_3^2=-50\sqrt{5},\quad r_3r_1^2+r_2r_4^2=50\sqrt{5}$$

から r_2, r_3, r_4 が一意に定まり, それぞれ実数となる.

$$\begin{aligned}
r_2 &= -\sqrt[5]{3125-1250\sqrt{5}+1875\sqrt{5+\sqrt{5}}-750\sqrt{5(5+\sqrt{5})}}\\
r_3 &= \sqrt[5]{-3125+1250\sqrt{5}+1875\sqrt{5+\sqrt{5}}-750\sqrt{5(5+\sqrt{5})}}\\
r_4 &= -\sqrt[5]{3125+1250\sqrt{5}-375\sqrt{125+55\sqrt{5}}}
\end{aligned}$$

- (4.10) より $f(x)$ の５つの根が得られるが, 実数根は

$$\begin{aligned}
x_1 = &-\sqrt[5]{3125+1250\sqrt{5}+375\sqrt{125+55\sqrt{5}}}\\
&-\sqrt[5]{3125-1250\sqrt{5}+1875\sqrt{5+\sqrt{5}}-750\sqrt{5(5+\sqrt{5})}}\\
&+\sqrt[5]{-3125+1250\sqrt{5}+1875\sqrt{5+\sqrt{5}}-750\sqrt{5(5+\sqrt{5})}}\\
&-\sqrt[5]{3125+1250\sqrt{5}-375\sqrt{125+55\sqrt{5}}}
\end{aligned}$$

のみである.

5章　可解な5次方程式・その2

5章では，3項5次方程式

$$x^5 + ax + b = 0$$

が可解であることと，係数 a, b がある形のパラメータ表示を持つこととが同値である，という B.K. Spearman と K.S. Williams の定理 (cf. [2]) を証明し，このパラメータ表示を用いて根を求める方法を明らかにする．§5.1 では 3 次方程式の Cardano による解法と同様に

$$x_j = \zeta^j u_1 + \zeta^{2j} u_2 + \zeta^{3j} u_3 + \zeta^{4j} u_4 \quad (j = 0, ..., 4)$$

を根に持つ 5 次方程式が $x^5 + ax + b = 0$ に一致するための u_1, u_2, u_3, u_4 の満たすべき条件を導き，これを利用して Spearman, Williams の定理を証明する．§5.2 では可解な 3 項 5 次方程式の解法を例示する．

5.1　Spearman, Williams の定理

Cardano は 3 次方程式を 3 項 3 次方程式 $x^3 + ax + b = 0$ に変形し，等式

$$(x - (u_1 + u_2))\left(x - (\omega u_1 + \omega^2 u_2)\right)\left(x - (\omega^2 u_1 + \omega u_2)\right) = x^3 - 3u_1u_2x - (u_1^3 + u_2^3)$$

を利用して，その根の公式を導いた．ただし ω は 1 の原始 3 乗根，u_1, u_2 は複素変数である．u_1, u_2 が

$$-3u_1u_2 = a, \qquad -(u_1^3 + u_2^3) = b$$

を満たせば，上の式から方程式 $x^3 + ax + b = 0$ の根が得られる．一方

$$u_1^3 u_2^3 = -\frac{a^3}{27}, \qquad u_1^3 + u_2^3 = -b$$

を満たす u_1^3, u_2^3 は2次方程式を解いて求めることができるので, その3乗根を適当に選べばよいことになる.

この考え方を3項5次方程式

$$f(x) = x^5 + ax + b = 0 \tag{5.1}$$

に応用する.

u_1, u_2, u_3, u_4 を複素変数, ζ を1の原始5乗根とする. x の5次式

$$\prod_{j=0}^{4} \left(x - (\zeta^j u_1 + \zeta^{2j} u_2 + \zeta^{3j} u_3 + \zeta^{4j} u_4)\right)$$

を展開し整理すると

$$x^5 - 5Ux^3 - 5Vx^2 + 5Wx + 5(X - Y) - Z$$

となる. ただし

$$\begin{aligned}
U &= u_1u_4 + u_2u_3 \\
V &= u_1u_2^2 + u_2u_4^2 + u_3u_1^2 + u_4u_3^2 \\
W &= u_1^2u_4^2 + u_2^2u_3^2 - u_1^3u_2 - u_2^3u_4 - u_3^3u_1 - u_4^3u_3 - u_1u_2u_3u_4 \\
X &= u_1^3u_3u_4 + u_2^3u_1u_3 + u_3^3u_2u_4 + u_4^3u_1u_2 \\
Y &= u_1u_3^2u_4^2 + u_2u_1^2u_3^2 + u_3u_2^2u_4^2 + u_4u_1^2u_2^2 \\
Z &= u_1^5 + u_2^5 + u_3^5 + u_4^5
\end{aligned}$$

である. 従って, 4つの等式

$$0 = u_1u_4 + u_2u_3 \tag{5.2}$$

$$0 = u_1u_2^2 + u_2u_4^2 + u_3u_1^2 + u_4u_3^2 \tag{5.3}$$

$$a = 5(u_1^2u_4^2 + u_2^2u_3^2 - u_1^3u_2 - u_2^3u_4 - u_3^3u_1 - u_4^3u_3 - u_1u_2u_3u_4) \tag{5.4}$$

$$\begin{aligned}
b = 5\big((u_1^3u_3u_4 + u_2^3u_1u_3 + u_3^3u_2u_4 + u_4^3u_1u_2) - (u_1u_3^2u_4^2 + u_2u_1^2u_3^2 + u_3u_2^2u_4^2 + u_4u_1^2u_2^2)\big) \\
- (u_1^5 + u_2^5 + u_3^5 + u_4^5)
\end{aligned} \tag{5.5}$$

を満たす u_1, u_2, u_3, u_4 が存在すれば (5.1) の根

$$x_j = \zeta^j u_1 + \zeta^{2j} u_2 + \zeta^{3j} u_3 + \zeta^{4j} u_4 \qquad (j = 0, 1, 2, 3, 4) \tag{5.6}$$

が得られる.

補題 5.1 5次方程式 $f(x)=x^5+ax+b=0$ $(a,b\neq 0)$ に対して

$$a=\frac{5e^4(3-4\epsilon c)}{c^2+1},\qquad b=-\frac{4e^5(11\epsilon+2c)}{c^2+1}$$

を満たす有理数 $\epsilon(=\pm 1)$, $c(\geq 0)$, $e(\neq 0)$ が存在するならば $f(x)$ は可解である.

Proof 5次方程式

$$f(x)=x^5+\frac{5e^4(3-4\epsilon c)}{c^2+1}x-\frac{4e^5(11\epsilon+2c)}{c^2+1}=0$$

で $x=ey$ と変換すると

$$e^5\left(y^5+\frac{5(3-4\epsilon c)}{c^2+1}y-\frac{4(11\epsilon+2c)}{c^2+1}\right)=0$$

となる. 従って, 改めて

$$f(x)=x^5+\frac{5(3-4\epsilon c)}{c^2+1}x-\frac{4(11\epsilon+2c)}{c^2+1}=0$$

$$a=\frac{5(3-4\epsilon c)}{c^2+1},\qquad b=-\frac{4(11\epsilon+2c)}{c^2+1}$$

とおき, 4つの等式(5.2), (5.3), (5.4), (5.5) を満たす u_1, u_2, u_3, u_4 が有理数と a,b に四則演算と根号を用いた形で表されることを示せばよい.

$A=c^2+1$ とおくと, A は正の有理数であるから, 実数 v_1, v_2, v_3, v_4 が次のように定義される.

$$\begin{cases} v_1=\sqrt{A}+\sqrt{A-\epsilon\sqrt{A}}, & v_2=-\sqrt{A}-\sqrt{A+\epsilon\sqrt{A}}, \\ v_3=-\sqrt{A}+\sqrt{A+\epsilon\sqrt{A}}, & v_4=\sqrt{A}-\sqrt{A-\epsilon\sqrt{A}}, \end{cases} \tag{5.7}$$

これより

$$\begin{cases} v_1+v_4 &= 2\sqrt{A} \\ v_1v_4 &= \epsilon\sqrt{A} \end{cases} \qquad \begin{cases} v_2+v_3 &= -2\sqrt{A} \\ v_2v_3 &= -\epsilon\sqrt{A} \end{cases}$$

が成り立つ. ここで

$$u_1^5=\frac{v_1^2v_3}{A^2},\qquad u_2^5=\frac{v_3^2v_4}{A^2},\qquad u_3^5=\frac{v_2^2v_1}{A^2},\qquad u_4^5=\frac{v_4^2v_2}{A^2} \tag{5.8}$$

を満たす実数を u_1, u_2, u_3, u_4 とおく. u_1, u_2, u_3, u_4 が有理数と a,b に四則演算と根号を用いた形で表されていることに注意されたい. 以下 u_1, u_2, u_3, u_4 が (5.2), (5.3), (5.4),

(5.5) を満たすことを示す. u_1u_4 は実数で

$$u_1^5u_4^5=\frac{v_1^2v_4^2v_2v_3}{A^4}=\frac{-\epsilon A\sqrt{A}}{A^4}=\left(-\frac{\epsilon}{\sqrt{A}}\right)^5$$

を満たすので

$$u_1u_4=-\frac{\epsilon}{\sqrt{A}}$$

である. 同様にして

$$u_2u_3=\frac{\epsilon}{\sqrt{A}}$$

が得られるので, (5.2) が成り立つ. また

$$u_1^5u_2^{10}=\frac{v_1^2v_3^5v_4^2}{A^6}=\frac{Av_3^5}{A^6}=\left(\frac{v_3}{A}\right)^5$$

より

$$u_1u_2^2=\frac{v_3}{A}$$

を得る. 同様にして

$$u_2u_4^2=\frac{v_4}{A},\qquad u_3u_1^2=\frac{v_1}{A},\qquad u_4u_3^2=\frac{v_2}{A}$$

が得られる. 従って

$$u_1u_2^2+u_2u_4^2+u_3u_1^2+u_4u_3^2=\frac{v_1+v_2+v_3+v_4}{A}=0$$

となり, (5.3) が成り立つ. さらに

$$u_1^{15}u_2^5=\frac{v_1^6v_3^5v_4}{A^8}=\frac{\epsilon\sqrt{A}v_1^5v_3^5}{A^8}=\left(\frac{\epsilon v_1v_3}{A\sqrt{A}}\right)^5$$

より

$$u_1^3u_2=\frac{\epsilon v_1v_3}{A\sqrt{A}}$$

が得られ, 同様にして

$$u_2^3u_4=-\frac{\epsilon v_3v_4}{A\sqrt{A}},\qquad u_3^3u_1=-\frac{\epsilon v_1v_2}{A\sqrt{A}},\qquad u_4^3u_3=\frac{\epsilon v_2v_4}{A\sqrt{A}}$$

を得る. ここで

$$(v_1-v_4)^2=4\sqrt{A}(\sqrt{A}-\epsilon),\qquad (v_2-v_3)^2=4\sqrt{A}(\sqrt{A}+\epsilon),\qquad v_1>v_4,\qquad v_3>v_2$$

に注意すれば

$$
\begin{aligned}
&5(u_1^2u_4^2+u_2^2u_3^2-u_1^3u_2-u_2^3u_4-u_3^3u_1-u_4^3u_3-u_1u_2u_3u_4)\\
&=5\left(\frac{3}{A}+\frac{\epsilon}{A\sqrt{A}}(v_1v_2+v_3v_4-v_1v_3-v_2v_4)\right)\\
&=\frac{5}{A\sqrt{A}}\left(3\sqrt{A}+\epsilon(v_1-v_4)(v_2-v_3)\right)\\
&=\frac{5}{A\sqrt{A}}\left(3\sqrt{A}-4\epsilon\sqrt{A}\sqrt{A-1}\right)\\
&=\frac{5(3-4\epsilon\sqrt{A-1})}{A}\\
&=\frac{5(3-4\epsilon c)}{c^2+1}\ =\ a
\end{aligned}
$$

となり, (5.4) が示された. 最後に, 以上の結果から

$$
\begin{aligned}
&5\left((u_1^3u_3u_4+u_2^3u_1u_3+u_3^3u_2u_4+u_4^3u_1u_2)-(u_1u_3^2u_4^2+u_2u_1^2u_3^2+u_3u_2^2u_4^2+u_4u_1^2u_2^2)\right)\\
&\quad-(u_1^5+u_2^5+u_3^5+u_4^5)\\
&=\frac{10\epsilon}{A\sqrt{A}}(-v_1+v_3+v_2-v_4)-\frac{1}{A^2}\left(v_1^2v_3+v_3^2v_4+v_2^2v_1+v_4^2v_2\right)\\
&=\frac{10\epsilon}{A\sqrt{A}}\left(-2\sqrt{A}-2\sqrt{A}\right)-\frac{1}{A^2}\left(4\epsilon A+8A\sqrt{A-1}\right)\\
&=\frac{-44\epsilon-8\sqrt{A-1}}{A}\\
&=-\frac{4(11\epsilon+2c)}{c^2+1}\ =\ b
\end{aligned}
$$

となり, (5.5) も成り立つ. よって $f(x)$ の根は

$$
x_j=\zeta^j u_1+\zeta^{2j}u_2+\zeta^{3j}u_3+\zeta^{4j}u_4 \qquad (j=0,1,2,3,4)
$$

となり, 有理数と a,b に四則演算と根号を用いた形で表されるので $f(x)$ は可解である. ∎

上の補題の証明の中で方程式 $f(x)=x^5+ax+b=0$ の根を求める方法が明らかにされていることに注意されたい. これは次節で解法を例示するときに用いる.

定理 5.2 5次方程式 $f(x)=x^5+ax+b=0 \quad (a\neq 0, b\neq 0)$ が $\mathbb{Q}$ 上既約であるとする. このとき $f(x)=0$ が可解となる条件は

$$
a=\frac{5e^4(3-4\epsilon c)}{c^2+1}, \qquad b=-\frac{4e^5(11\epsilon+2c)}{c^2+1} \tag{5.9}
$$

となる有理数 $\epsilon(=\pm 1)$, $c(\geq 0)$, $e(\neq 0)$ が存在することである.

Proof 補題5.1より, (5.9)のようなパラメータ表示があれば $f(x)$ は可解である. 従って $f(x)$ が $\mathbb{Q}$ 上既約という仮定のもとで a, b が(5.9)のように表示されることを示せばよい.

$f(x)=0$ が可解のとき6次分解式(4.6)は定理4.2より有理数根 θ をもつ. 従って

$$\begin{aligned}&\theta^6+8a\theta^5+40a^2\theta^4+160a^3\theta^3+400a^4\theta^2+(512a^5-3125b^4)\theta+256a^6-9375ab^4\\&=(\theta+2a)^4(\theta^2+16a^2)-5^5b^4(\theta+3a)=0\end{aligned}\tag{5.10}$$

が成り立つ.

$\theta=-2a$ と仮定すれば $ab=0$ となり, 仮定に反する. $\theta=-3a$ と仮定しても同様である. 従って, 以下 $\theta\neq-2a,-3a$ であるとする. ここで

$$\left|\frac{3\theta-16a}{4(\theta+3a)}\right|=c,\qquad \frac{3\theta-16a}{4(\theta+3a)}=c\epsilon,\qquad \frac{-5b\epsilon}{2(\theta+2a)}=e\tag{5.11}$$

を満たすように c, ϵ, e を定める. 明らかに $c\geq 0$, $\epsilon=\pm1$, $e\neq 0$ である.

このとき

$$\begin{aligned}c^2+1 &= \frac{(3\theta-16a)^2}{16(\theta+3a)^2}+1=\frac{25(\theta^2+16a^2)}{16(\theta+3a)^2}\\3-4\epsilon c &= 3-4\cdot\frac{3\theta-16}{4(\theta+3a)}=\frac{25a}{\theta+3a}\\11\epsilon+2c &= 11\epsilon+2\cdot\frac{3\theta-16a}{4\epsilon(\theta+3a)}=\frac{25(\theta+2a)}{2\epsilon(\theta+3a)}\end{aligned}$$

が成り立つ. ここで(5.10)から

$$\frac{5^5b^4(\theta+3a)}{\theta^2+16a^2}=(\theta+2a)^4$$

が得られるので

$$\begin{aligned}\frac{5e^4(3-4\epsilon c)}{c^2+1} &= 5\cdot\frac{5^4b^4}{2^4(\theta+2a)^4}\cdot\frac{25a}{\theta+3a}\cdot\frac{16(\theta+3a)^2}{25(\theta^2+16a^2)}=a\\\frac{-4e^5(11\epsilon+2c)}{c^2+1} &= 4\cdot\frac{5^5b^5\epsilon}{2^5(\theta+2a)^5}\cdot\frac{25(\theta+2a)}{2\epsilon(\theta+3a)}\cdot\frac{16(\theta+3a)^2}{25(\theta^2+16a^2)}=b\end{aligned}$$

とパラメータ表示できる. 以上で定理が証明された. ∎

補題 5.3 5次方程式 $f(x)=x^5+ax+b=0$ $(a\neq 0, b\neq 0)$ は5実根をもつことはない.

Proof $f(x)=0$ が5実根をもつと仮定すれば, $f'(x)=0$ は4実根をもつことになるが,

$f(x)$ を微分すれば $f'(x)=5x^4+a$ となり，$a>0$ のとき $f'(x)=0$ は4虚根，$a<0$ のときは2実根，2虚根をもつことになり仮定に反する． ∎

定理 5.4 有理数係数既約 5 次方程式 $f(x)=x^5+ax+b=0$ が可解ならば，ちょうど1つの実根をもつ．

Proof $f(x)$ が $\mathbb{Q}$ 上既約であるから $b\neq 0$ である．$a=0$ のとき $f(x)$ はちょうど1つの実根をもつ．従って，以下 $a\neq 0, b\neq 0$ とする．

補題5.3 より $f(x)$ の実根は 1 個，または 3 個である．$f(x)$ が3実根 α,β,γ をもつと仮定し，残りの2虚根を $\delta,\bar{\delta}$ とすると

$$\begin{aligned}\Delta_f &= (\alpha-\beta)(\alpha-\gamma)(\alpha-\delta)(\alpha-\bar{\delta})(\beta-\gamma)(\beta-\delta)(\beta-\bar{\delta})(\gamma-\delta)(\gamma-\bar{\delta})(\delta-\bar{\delta})\\ &= (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\,|\alpha-\delta|^2\,|\beta-\delta|^2\,|\gamma-\delta|^2\,(\delta-\bar{\delta})\end{aligned}$$

となる．ここで $\delta-\bar{\delta}$ は ci という形の虚数であり，これ以外の因子は実数であるから，$D_f=\Delta_f^2<0$ となる．これは補題4.5より，$D_f>0$ が成り立つことに矛盾する．よって $f(x)$ の実根はちょうど1個である． ∎

一般に $\mathbb{Q}$ 係数既約奇素数次方程式が可解のとき，その根はすべて実数か，1根のみ実数かのいずれかであることが知られている ([4, 3章, 定理3.69, 系]).

定理5.4 より，可解かつ既約な $\mathbb{Q}$ 係数 3 項 5 次方程式 $f(x)=0$ の Galois 群を G とすれば，G は2つの互換の積を含む．従って $G\simeq F_{20}$，または $G\simeq F_{10}$ が成り立つ．

また定理5.2 より (5.9) を満たす有理数 ϵ, c, e を用いると，判別式 D_f は

$$D_f=256a^5+3125b^4=\frac{4^4\cdot 5^5\cdot e^{20}}{A^5}\left(4\epsilon c^3-84c^2-37\epsilon c-122\right)^2$$

と表される．ただし $A=c^2+1$ であり，有理数 ϵ, c, e は (5.11) から計算できる．これより $\sqrt{D_f}$ が有理数であることと，$\sqrt{5A}$ が有理数であることとは同値である．従って，以上のことと定理4.9から次の定理が得られる．

定理 5.5 $\mathbb{Q}$ 係数既約 5 次方程式 $f(x)=x^5+ax+b=0$ の *Galois* 群 G が可解であるとき，次が成り立つ．

(1) $\sqrt{5A}$ が有理数のとき $G\simeq F_{10}$

(2) $\sqrt{5A}$ が有理数でないとき $G\simeq F_{20}$

ただし c は (5.11) で定まる有理数，$A=c^2+1$ である．

5.2 5次方程式の解法例2

例 3 $f(x)=x^5+330x-4170=0$

Eisenstein の判定法より $f(x)$ は $\mathbb{Q}$ 上既約である. 6 次分解式は

$$\begin{aligned} f_{20}(x) &= x^6+2640x^5+4356000x^4+5749920000x^3+4743684000000x^2 \\ &\quad -942914527909650000x-935138461630873500000 \end{aligned}$$

となり, 有理数根 $\theta=3510$ を持つので, 定理 4.2 より $f(x)$ は可解である. また (5.11) より

$$\epsilon=1, \qquad c=\frac{7}{24}, \qquad e=\frac{5}{2}$$

を得る. このとき

$$A=\left(\frac{7}{24}\right)^2+1=\frac{625}{576}, \qquad 5A=\frac{5^5}{2^6\cdot 3^2}$$

となり, $\sqrt{5A}$ は有理数でない. ゆえに, 定理 5.5 より $f(x)$ の Galois 群は F_{20} に同型である.

(5.7) に従って

$$\begin{aligned} v_1&=\sqrt{\tfrac{625}{576}}+\sqrt{\tfrac{625}{576}-\sqrt{\tfrac{625}{576}}} & v_2&=-\sqrt{\tfrac{625}{576}}-\sqrt{\tfrac{625}{576}+\sqrt{\tfrac{625}{576}}} \\ v_3&=-\sqrt{\tfrac{625}{576}}+\sqrt{\tfrac{625}{576}+\sqrt{\tfrac{625}{576}}} & v_4&=\sqrt{\tfrac{625}{576}}-\sqrt{\tfrac{625}{576}-\sqrt{\tfrac{625}{576}}} \end{aligned}$$

とおくと, (5.8) より

$$u_1^5=\frac{1728}{3125}, \qquad u_2^5=\frac{384}{3125}, \qquad u_3^5=\frac{20736}{3125}, \qquad u_4^5=-\frac{4608}{3125}$$

となり, u_1, u_2, u_3, u_4 は実数であるから

$$u_1=\frac{2}{5}\cdot\sqrt[5]{54}, \qquad u_2=\frac{2}{5}\cdot\sqrt[5]{12}, \qquad u_3=\frac{2}{5}\cdot\sqrt[5]{648}, \qquad u_4=-\frac{2}{5}\cdot\sqrt[5]{144}$$

が得られる. 従って $\zeta=e^{\frac{2\pi i}{5}}$ を用いて, $f(x)$ の根が

$$x_j=\sqrt[5]{54}\zeta^j+\sqrt[5]{12}\zeta^{2j}+\sqrt[5]{648}\zeta^{3j}-\sqrt[5]{144}\zeta^{4j} \qquad (j=0,1,2,3,4)$$

と表される.

例 4 $f(x)=x^5+4x=0$

$\epsilon=-1$, $c=\frac{11}{2}$, $e=1$ とおけば $a=4$, $b=0$ となり, $f(x)=x^5+4x$ となる. これより

$f(x)$ の根 $0, \pm 1 \pm i$ が得られる.

一方 $f(x)$ は既約でないが, 補題5.1は $f(x)$ が既約でない場合も成り立つので

$$A = \left(\frac{11}{2}\right)^2 + 1 = \frac{125}{4}$$

と (5.7) より

$$v_1 = \tfrac{1}{2}(5\sqrt{5} + \sqrt{5}\cdot\sqrt{25+2\sqrt{5}}) \qquad v_2 = \tfrac{1}{2}(-5\sqrt{5} - \sqrt{5}\cdot\sqrt{25-2\sqrt{5}})$$
$$v_3 = \tfrac{1}{2}(-5\sqrt{5} + \sqrt{5}\cdot\sqrt{25-2\sqrt{5}}) \qquad v_4 = \tfrac{1}{2}(5\sqrt{5} - \sqrt{5}\cdot\sqrt{25+2\sqrt{5}})$$

とおき

$$u_1 = \tfrac{1}{5}(-\sqrt{5} - \sqrt{5-2\sqrt{5}}) \qquad u_2 = \tfrac{1}{5}(\sqrt{5} - \sqrt{5+2\sqrt{5}})$$
$$u_3 = \tfrac{1}{5}(\sqrt{5} + \sqrt{5+2\sqrt{5}}) \qquad u_4 = \tfrac{1}{5}(-\sqrt{5} + \sqrt{5-2\sqrt{5}})$$

を求め

$$\zeta = e^{\frac{2}{5}\pi i} = \frac{1}{4}(\sqrt{5} - 1 + i\sqrt{10+2\sqrt{5}})$$

と u_1, u_2, u_3, u_4 から

$$x_0 = 0, \qquad x_1 = -1 - i, \qquad x_2 = 1 + i, \qquad x_3 = 1 - i, \qquad x_4 = -1 + i$$

を導くこともできる.

以上からわかるように, 3項5次方程式に対する Spearman, Williams の解法は, より明快であるということができる.

References

[1] D.S. Dummit, *Solving solvable quintics*, Math. Comp. 57 (1991), 387-401.

[2] B.K. Spearman and K.S. Williams, *Characterization of solvable quintics*, Amer. Math. Monthly 101 (1994), 986-992.

[3] J.Rotman, An introduction to the theory of groups, Springer, 1995.

[4] 藤崎 源二郎, 体とガロア理論, 岩波, 1991.

[5] J. ロットマン (関口 次郎・訳), ガロア理論, シュプリンガー・フェアラーク東京, 2000.

[6] 酒井 文雄, 環と体の理論, 共立出版, 1997.

[7] 田代敏和, ガロア群と代数方程式について, 兵庫教育大学修士論文, 1989.