代数学講義ノート (体とガロア理論)

作成者：石川雅雄

平成 28 年 7 月 22 日

この講義ノートは, 主に Steven Roman の GTM の本 [8] に従って書いてあります. また, 一部は藤崎先生の岩波基礎数学シリーズの中の本 [3] から題材を取ってあります. 講義の目標は, 「体とガロア理論」の基礎を現代的視点から学ぶことです.

目 次

第1章　群と体についての復習

1.1　準備

$\mathbb{N} = \{1, 2, \dots\}$ 自然数の集合, $\mathbb{Z} = \{-2, -1, 0, 1, 2, \dots\}$ 整数の集合, $\mathbb{Q}$ 有理数の集合, $\mathbb{R}$ 実数の集合, $\mathbb{C}$ 複素数の集合.

定義 1.1.1. $(P, \leq)$ が**半順序集合 (partially ordered set, poset)** とは, $x, y \in P$ に二項関係 $x \leq y$ が定義されて

(i) $x \leq x$ (反射律 reflexivity)
(ii) $x \leq y$ かつ $y \leq x \Rightarrow x = y$ (反対称律 anti-symmetry)
(iii) $x \leq y$ かつ $y \leq z \Rightarrow x \leq z$ (推移律 transtivity)

が成り立つこと.

定義 1.1.2. $\emptyset \neq S \subseteq P$ のとき

- a が S の**上界 (upper bound)**（resp. **下界 (lower bound)**）: $^\forall x \in S : x \leq a$ (resp. $x \geq a$)
- a が S の**最大元 (maximum element)**（resp. **最小元 (minimum element)**）: $a \in S$ かつ a は S の上界 (resp. 下界)
- a が S の**極大元 (maximal element)**（resp. **極小元 (minimul element)**）: $a \in S$ かつ $x \gneqq a$ (resp. $x \lneqq a$) を満たす $x \in P$ が存在しない

$S = P$ に最大元 (resp. 最小元) が存在するとき, それを $\widehat{1}_P$ (resp. $\widehat{0}_P$), または, 単に $\widehat{1}$ (resp. $\widehat{0}$) と書く.

例 1.1.3. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ は普通の意味で全順序集合 [1].

定理 1.1.4. $S \subseteq \mathbb{N}$ ならば S に最小限が存在する.

定義 1.1.5. (帰納的集合) 半順序集合 P の任意の全順序部分集合が P に上界を持つとき, P は**帰納的集合**という.

定理 1.1.6. (**Zorn の補題**)　帰納的集合には極大元が存在する.

定義 1.1.7. P が半順序集合, $\{x_\lambda\}_{\lambda\in\Lambda}$ を P の元の族とするとき, $\{x_\lambda\}_{\lambda\in\Lambda}$ の上界 (resp. 下界) 全体の集合に最小限 x_1 (resp. 最大限 x_0) が存在するならば, x_1 を $\{x_\lambda\}_{\lambda\in\Lambda}$ の**上限（結び (join)）** (resp. x_0 を $\{x_\lambda\}_{\lambda\in\Lambda}$ の**下限（交わり (meet)）**) といい, $x_1 = \bigvee_{\lambda\in\Lambda} x_\lambda$ (resp. $x_0 = \bigwedge_{\lambda\in\Lambda} x_\lambda$) と書く. すなわち, x_0, x_1 は

(1) $x_\lambda \leq x_1$ $(^\forall\lambda \in \Lambda)$　　(resp. $x_0 \leq x_\lambda$ $(^\forall\lambda \in \Lambda)$)
(2) $x_\lambda \leq y$ $(^\forall\lambda \in \Lambda) \Longrightarrow x_1 \leq y$　　(resp. $x_0 \leq x_\lambda$ $(^\forall\lambda \in \Lambda) \Longrightarrow y \leq x_0$)

をみたす.

定義 1.1.8. (束)　半順序集合 L の任意の 2 元 x, y に対して $\{x, y\}$ の上限と下限が必ず存在するとき, L は**束 (lattice)** であるという. このとき, $\vee\{x, y\}$, $\wedge\{x, y\}$ をそれぞれ $x \vee y$, $x \wedge y$ と書くことにすると二項演算 $\vee$ (結び, join), $\wedge$ (交わり, meet) は次をみたす.

(i) $(x \vee y) \vee z = x \vee (y \vee z)$,　$(x \wedge y) \wedge z = x \wedge (y \wedge z)$　結合律 (associative raws)
(ii) $x \vee y = y \vee x$,　$x \wedge y = y \wedge x$　可換律 (commutative laws)
(iii) $x \vee x = x \wedge x = x$　(idempotent)
(iv) $x \wedge (x \vee t) = x = x \vee (x \wedge y)$　吸収律 (absorption laws)

[1] さらに, (iv) $x \leq y$ または $x \geq y$ のどちらか一方が成り立つ.

逆に, 集合 L 上に, 上の (i) ∼ (iv) をみたす二項演算 $\vee$, $\wedge$ が定義されているとき

$$s \wedge t = s \Leftrightarrow s \vee t = t \Leftrightarrow s \leq t$$

と定義すると $\leq$ は順序関係である. 二項演算 $\vee$, $\wedge$ が, 順序関係から定義されたものであるときは, この順序関係は元のものと一致する.

さらに, 2 つの元のみではなく, 任意の元の族に対して, その上限と下限が必ず存在するとき, L は**完全束 (complete lattice)** という.

定義 1.1.9. (単位元をもつ半群 (monoid)) 集合 S に二項演算 $(x, y) \mapsto xy$ が定義されて, 次をみたすとき **単位元をもつ半群 (monoid)** という.

(i) (結合法則) $(xy)z = x(yz)$
(ii) (単位元 1 の存在) $^{\exists}1 \in S$ s.t. $^{\forall}x$: $x1 = 1x = x$

この 1 を**単位元**という. さらに

(iv) (交換法則) $xy = yx$

をみたすとき, **可換半群**という.

問題 1.1.10. 単位元は唯一つであることを示せ.

問題 1.1.11. 非結合的な代数系で n 個の元 $x_1, x_2, \ldots, x_n$ のこの順の積に括弧の付け方の総数を C_n とする. 例えば $C_1 = 1$, $C_2 = 1$, $C_3 = 2$, $C_4 = 5, \ldots$ である. C_n は漸化式

$$C_n = \sum_{i=1}^{n} C_i C_{n-i}$$

をみたすことを示せ. $C_{n+1} = \frac{1}{n+1}\binom{2n}{n}$ を**カタラン数**という.

定義 1.1.12. (群) G が単位元をもつ半群のとき

(iii) (逆元の存在) $^{\forall}x \in G$, $^{\exists}y \in G$ s.t. $xy = yx = 1$

をみたすならば, G は **群 (group)** という. このとき y を x の**逆元**といい, x^{-1} と書く. 可換群においては, 演算 xy を和 $x + y$ で書き, **加群**ということも多いこのときは加法の単位元を 0 と書く.

問題 1.1.13. x の逆元 x^{-1} は存在すれば一意であることを示せ.

1.2 基本概念

定義 1.2.1. (環) 集合 $R \neq \emptyset$ に, 2 つの二項演算 (和, 積) が定義されていて, 次をみたすとき, **単位元をもつ可換環 (unitary commutative ring)** という.

(i) 和に関して加群
(ii) 積に関して単位元をもつ可換半群
(iii) 分配法則

$$x(y + z) = xy + xz, \qquad (x + y)z = xz + yz$$

が成り立つ.

$x \in R$ の乗法に関する逆元 x^{-1} が存在するとき, x を単元 (unit) という. R の単元全体の集合を $R^{\times}$ と書く.

定義 1.2.2. R を単位元をもつ可換環, $x \neq 0 \in R$ であるとき, $y \neq 0 \in R$ が存在して $xy = 0$ となるとき, x を**零因子**という. R に零因子が存在しないとき, R を**整域 (integral domain)** という.

問題 1.2.3. $R = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$ は整域であることを示せ.

定義 1.2.4. K が単位元をもつ可換環で, $K^\times = K \setminus \{0\}$ のとき, K は, **体 (field)** という.

定義 1.2.5. (部分環)　R が単位元をもつ可換環, $S \subseteq R$ のとき,

(1) $x, y \in S \Rightarrow x - y \in S$
(2) $x, y \in S \Rightarrow xy \in S$
(3) $1_R \in S$

をみたすならば, S は R の**部分環 (subring)** (R が整域のときは**部分整域**) という. さらに R が体であり

(4) $x \neq 0 \in S \Rightarrow x^{-1} \in S$

をみたすならば, S は R の部分体であるという.

定義 1.2.6. (イデアル)　R が単位元をもつ可換環で, $\mathfrak{a} \subseteq R$ のとき,

(1) $\mathfrak{a}$ は加法群として R の部分群
(2) $^\forall x \in R, ^\forall y \in \mathfrak{a} \Rightarrow xy \in \mathfrak{a}$

をみたすとき $\mathfrak{a}$ を R の**イデアル (ideal)** という.

問題 1.2.7. $\mathbf{0} = \{0\}$ および R 自身は R のイデアルであることを示せ..

定義 1.2.8. (剰余環)　R が単位元をもつ可換環, $\mathfrak{a}$ が R のイデアルのとき

$$R/\mathfrak{a} = \{x + \mathfrak{a} | x \in R\}$$

に $(x + \mathfrak{a}) + (y + \mathfrak{a}) = x + y + \mathfrak{a}$, $(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$ によって二項演算を定義すると, well-defined で, この演算に関して $R/\mathfrak{a}$ は単位元をもつ可換環になる. これを R の $\mathfrak{a}$ による**剰余環**という. ただし

$$x + R = \{x + y | y \in R\}$$

とする.

問題 1.2.9. 上を証明せよ.

例 1.2.10. 整数環 $R = \mathbb{Z}$ において, m の倍数全体の集合 $(m) = m\mathbb{Z} = \{mx | x \in \mathbb{Z}\}$ はイデアルである. $\mathbb{Z}/(m) = \mathbb{Z}/m\mathbb{Z}$ は単位元をもつ可換環で, $\sharp\mathbb{Z}/(m) = m$ である.

問題 1.2.11. $3 + 12\mathbb{Z}$ は $\mathbb{Z}/12\mathbb{Z}$ の零因子であることを示せ.

問題 1.2.12. 次を示せ.

$$\mathbb{Z}/m\mathbb{Z} \text{ が整域} \Leftrightarrow \mathbb{Z}/m\mathbb{Z} \text{ が体} \Leftrightarrow m \text{ は素数}$$

定義 1.2.13. R, R' が単位元をもつ可換環, $f : R \to R'$ が写像のとき,

(1) $f(x + y) = f(x) + f(y)$
(2) $f(xy) = f(x)f(y)$
(3) $f(1_R) = 1_{R'}$ (必ずしも一般的な定義でない)[2]

をみたすとき, **準同型写像 (homomorphism)** という. f が単射 (resp. 全) のとき, **単 (resp. 全) 準同型写像**といい, 全単射のとき, **同型写像**といい, $R \simeq R'$ と書く. 特に, 全単射で $R = R'$ のとき, **自己同型 (automorphism)** という.

補題 1.2.14. R, R' が単位元をもつ可換環, $f : R \to R'$ が準同型写像のとき,

(1) f が全射で S が R の部分環ならば $f(S)$ は R' の部分環である.

[2]普通は (3) は入れないが, ここでは体論をやるので, 議論を簡単にするために入れる.

(2) f が全射で $\mathfrak{a}$ が R のイデアルならば $f(\mathfrak{a})$ は R' のイデアルである.
(3) S' が R' の部分環ならば $f^{-1}(S)$ は R の部分環である.
(4) $\mathfrak{a}'$ が R' のイデアルならば $\mathfrak{a} = f^{-1}(\mathfrak{a}')$ は R のイデアルである. 特に, **核** $\mathfrak{n} = f^{-1}(0)$ は R のイデアルである.

問題 1.2.15. 上を示せ.

問題 1.2.16. 体 K から環 R への準同型写像 $f : K \to R$ は単準同型写像であるか, または $f(x) = 0$ $(^\forall x \in R)$ となることを示せ.

定理 1.2.17. (準同型定理)　f を環 R から環 R' への準同型写像, $\mathfrak{n} = f^{-1}(0)$ を f の核とするとき,

$$\overline{f} : R/\mathfrak{n} \to R', \quad a + \mathfrak{n} \mapsto f(a)$$

によって, $R/\mathfrak{n}$ と R' は同型である.

1.3　イデアルについて

命題 1.3.1. $\mathfrak{a}_\iota$ $(\iota \in I)$ がイデアルの族 (family) のとき, $\bigcap_{\iota \in I} \mathfrak{a}_\iota$ もイデアルである.

問題 1.3.2. 上を示せ.

定義 1.3.3. (生成されるイデアル)　$S \subseteq R$ に対して

$$(S) = \bigcap_{\mathfrak{a} \supset S} \mathfrak{a}$$

は S を含む最小のイデアルである. 特に, $S = \{a_1, \ldots, a_s\}$ のとき, $(\{a_1, \ldots, a_s\})$ を $(a_1, \ldots, a_s)$, と書く. また, $s = 1$ のとき, (a) を**単項イデアル (pricipal ideal)** という.

問題 1.3.4. $(S) = \left\{ \sum_{i=1}^{k} r_i a_i | r_i \in R, a_i \in S, k \in \mathbb{N} \right\}$ を示せ.

定義 1.3.5. (イデアルの和と積)　$\mathfrak{a}_i$ $(i = 1, \ldots, s)$ が有限個のイデアルのとき

$$\left(\bigcup_{i=1}^{s} \mathfrak{a}_i \right) = \{a_1 + \cdots + a_s | a_i \in \mathfrak{a}_i\}$$

を $\mathfrak{a}_1 + \cdots + \mathfrak{a}_s$ または $(\mathfrak{a}_1, \ldots, \mathfrak{a}_s)$ と書く. また,

$$\left(\prod_{i=1}^{s} \mathfrak{a}_i \right) = \left\{ \sum_j \prod_{i=1}^{s} a_j^{(i)} | a_j^{(i)} \in \mathfrak{a}_i \right\}$$

を $\prod_{i=1}^{s} \mathfrak{a}_i$ (または簡単に $\mathfrak{a}_1 \cdots \mathfrak{a}_s$) と書く.

問題 1.3.6. $6\mathbb{Z} + 8\mathbb{Z} = 2\mathbb{Z}$ を示せ.

問題 1.3.7. $(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ を示せ.

命題 1.3.8. R が単位元 1 をもつ可換環で, $\mathfrak{p} \neq R$ がイデアルのとき, 次は同値である.

(1) $R/\mathfrak{p}$ は整域
(2) $a, b \in \mathfrak{p}$ のとき, $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ または $b \in \mathfrak{p}$
(3) R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ または $\mathfrak{b} \subseteq \mathfrak{p}$
(4) R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して, $\mathfrak{a} \not\subseteq \mathfrak{p}$ かつ $\mathfrak{b} \not\subseteq \mathfrak{p} \Rightarrow \mathfrak{a}\mathfrak{b} \not\subseteq \mathfrak{p}$

このいずれかが成り立つとき $\mathfrak{p}$ は**素イデアル (prime ideal)** という.[3]

証明. (1) $\Rightarrow$ (2)
$ab \in \mathfrak{p}$ ならば, $R/\mathfrak{p}$ において $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$ なので, $R/\mathfrak{p}$ が整域であることから $a+\mathfrak{p} = \mathfrak{p}$ または $b+\mathfrak{p} = \mathfrak{p}$ である. すなわち $a \in \mathfrak{p}$ または $b \in \mathfrak{p}$ である.

(2) $\Rightarrow$ (4)
R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して, $\mathfrak{a} \not\subseteq \mathfrak{p}$ かつ $\mathfrak{b} \not\subseteq \mathfrak{p}$ であるとすると $^{\exists}a \in \mathfrak{a} \setminus \mathfrak{p}$, $^{\exists}b \in \mathfrak{b} \setminus \mathfrak{p}$ が存在する. (2) より $ab \notin \mathfrak{p}$ だから $\mathfrak{ab} \not\subseteq \mathfrak{p}$ である.

(4) $\Rightarrow$ (3)
対偶

(3) $\Rightarrow$ (1)
$R/\mathfrak{p}$ の定義より明らか. $\square$

命題 1.3.9. R が単位元 1 をもつ可換環で, $\mathfrak{m} \neq R$ がイデアルのとき, 次は同値である.

(1) $\mathfrak{a}$ がイデアルで, $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R \Rightarrow \mathfrak{a} = \mathfrak{m}$ または $\mathfrak{a} = R$. (すなわち $\mathfrak{m}$ は包含関係に関して極大)
(2) $R/\mathfrak{m}$ は体

このいずれかが成り立つとき $\mathfrak{m}$ は**極大イデアル (maximal ideal)** という

証明. (1) $\Rightarrow$ (2)
$a+\mathfrak{m} \neq \mathfrak{m}$ ならば $a \notin \mathfrak{m}$ なので $\mathfrak{m} \subsetneq (a)+\mathfrak{m}$ となり, $\mathfrak{m}$ が極大イデアルであることより $(a)+\mathfrak{m} = R$ である. すなわち $r \in R$, $m \in \mathfrak{m}$ が存在して $ra+m = 1$ となる. ゆえに $r+\mathfrak{m}$ は $a+\mathfrak{m}$ の逆元である.

(2) $\Rightarrow$ (1)
$\mathfrak{m} \subsetneq \mathfrak{a} \subseteq R$ とすると $^{\exists}x \in \mathfrak{a} \setminus \mathfrak{m}$ が存在する. $R/\mathfrak{m}$ において $x+\mathfrak{m} \neq \mathfrak{m}$ なので $^{\exists}y \in R$ が存在して $(x+\mathfrak{m})(y+\mathfrak{m}) = 1+\mathfrak{m}$ となる. よって $1 \in \mathfrak{a}$ となり $\mathfrak{a} = R$ が示される. $\square$

系 1.3.10. 極大イデアルは素イデアルである.

定理 1.3.11. R が単位元 1 をもつ可換環で, $S \neq \emptyset$ $(0 \notin S)$ が積に関して閉じている R の部分集合 (i.e. $a, b \in S \Rightarrow ab \in S$), $\mathfrak{a}$ が R のイデアル s.t. $\mathfrak{a} \cap S = \emptyset$ とする. このとき, R のイデアルの族

$$\mathscr{I} = \{\mathfrak{b} | \mathfrak{b} \supseteq \mathfrak{a} \text{ かつ } \mathfrak{b} \cap S = \emptyset\}$$

には包含関係で極大元が存在する. $\mathfrak{p}$ を極大元の 1 つを $\mathfrak{p}$ とすれば, $\mathfrak{p}$ は素イデアルである.

証明. $\mathscr{I}$ が帰納的集合であることを示す. $\mathfrak{b}_\iota$ $(\iota \in I)$ が $\mathscr{I}$ の全順序集合であるとき, $\mathfrak{c} = \bigcup_{\iota \in I} \mathfrak{b}_\iota$ とおくと, $\mathfrak{c}$ はイデアルであり, $\mathfrak{c} \in \mathscr{I}$ である.[4] よって, 帰納的集合であることが示された. ゆえに, Zorn の補題より, 極大元 $\mathfrak{p} \in \mathscr{I}$ が存在する. $\mathfrak{p}$ が素イデアルであることを示す. $b \notin \mathfrak{p}$, $c \notin \mathfrak{p}$, $bc \in \mathfrak{p}$ とすると $\mathfrak{p} \subsetneq (b)+\mathfrak{p}$, $\mathfrak{p} \subsetneq (c)+\mathfrak{p}$ だから $((b)+\mathfrak{p}) \cap S \neq \emptyset$, $((c)+\mathfrak{p}) \cap S \neq \emptyset$ であり, $s_1 = r_1 b + p_1$, $s_2 = r_2 c + p_2$ となる $s_1, s_2 \in S$, $r_1, r_2 \in R$, $p_1, p_2 \in \mathfrak{p}$ が存在する. このとき, $S \ni s_1 s_2 = r_1 r_2 bc + r_1 b p_2 + r_2 c p_1 + p_1 p_2 \in \mathfrak{p}$ となり $\mathfrak{p} \cap S = \emptyset$ に矛盾する. $\square$

系 1.3.12. R が単位元 1 をもつ可換環で, $\mathfrak{a} \neq R$ がイデアルのとき, $\mathfrak{a}$ を含む R の極大イデアル $\mathfrak{m}$ が存在する.

証明. 上の定理で $S = \{1\}$ とせよ.

系 1.3.13. R が単位元 1 をもつ可換環ならば R の極大イデアル $\mathfrak{m}$ が存在する.

証明. 上の系で $\mathfrak{a} = \mathbf{0}$ とせよ.

定理 1.3.14. 単位元 1 をもつ可換環 $R \neq \mathbf{0}$ について, 次は同値である.

[3] 定義から R は素イデアルではない.
[4] $\mathfrak{a} \subseteq \mathfrak{c}$ は明らか. $\mathfrak{c} \cap S = \emptyset$ を自分で示せ.

(1) R は体
(2) R のイデアルは $\mathbf{0}$, R 以外に存在しない.

系 1.3.15. 有限個の元からなる整域 R は体である.

証明. $\mathfrak{a} \neq \mathbf{0}$ を R のイデアルとせよ. $0 \neq {}^{\exists}a \in \mathfrak{a}$ を 1 つ取る. $f_a : R \to \mathfrak{a}, x \mapsto xa$ は R から $\mathfrak{a}$ への単射, よって全射でなければならない. すなわち $\mathfrak{a} = R$ である. R のイデアルは $\mathbf{0}$ と R のみである.

1.4 商体

定理 1.4.1. (商体) R が整域のとき, 次をみたす体 F と写像 $f : R \to F$ が存在する.

(1) f は単準同型写像
(2) F の任意の元は $x = f(a)f(b)^{-1}$ の形に書かれる.

また, (F, f), (F', f') がともに (1) (2) をみたせば, 同型写像 $\varphi : F \to F'$ が存在して $f' = \varphi \circ f$ となる.

証明.

$$\overline{F} = \{(a, b) | a, b \in R,\ b \neq 0\}$$

とし, $\overline{F}$ に同値関係 $\sim$ を

$$(a, b) = (c, d) \Leftrightarrow ad = bc$$

で定義する. $F = \overline{F}/\sim$ とおき, F の加法と乗法を

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)},\ \overline{(a, b)(c, d)} = \overline{(ac, bd)}$$

によって定義すると, この二項演算は well-defined で, $0_F = \overline{(0_R, 1_R)}$ が零元で, $1_F = \overline{(1_R, 1_R)}$ が単位元となる. $f : R \to F$ を $f(a) = \overline{(a, 1_R)}$ で定義する.

問題 1.4.2. 上の定理の詳細を述べよ.

定義 1.4.3. R が整域のとき, 上の F を R の**商体 (field of quotients)** という.

以後, R は (単位元をもつ可換環でかつ) 整域とする.

定義 1.4.4. R が整域のとき,

- $a, b \in R$ に対して $b = ac$ $({}^{\exists}c \in R)$ のとき, $a|b$ と書き, b は a の**倍元**, a は b の**約元**という.
- $a \in R$ に対して $x \in R$ が, $x = \epsilon a$ となる単元 ϵ が存在するとき, a と x は**同伴元**といい, $x \approx a$ と書く.[5]
- $a_1, a_2, \ldots, a_n \in R$ $(n \geq 2)$ に対して
  - $d|a_i$ $({}^{\forall}i)$
  - $x|a_i$ $({}^{\forall}i)$ ならば $x|d$

  をみたす $d \in R$ を $a_1, a_2, \ldots, a_n$ の**最大公約元**という. 最大公約元は, 単元を除いて一意に決まる. すなわち, d, d' が共に $a_1, a_2, \ldots, a_n$ の最大公約元ならば $d \approx d'$ である. $a_1, a_2, \ldots, a_n$ の最大公約元が単元のとき $a_1, a_2, \ldots, a_n$ は**互いに疎**という.
- $a_1, a_2, \ldots, a_n \in R$ に対して
  - $a_i|m$ $({}^{\forall}i)$
  - $a_i|x$ $({}^{\forall}i)$ ならば $m|x$

  をみたす m を $a_1, a_2, \ldots, a_n$ の**最小公倍元**という. 最小公倍元も, 単元を除いて一意に決まる.

[5] $x \approx a \Leftrightarrow a|x$ かつ $x|a$.

命題 1.4.5. $a, x \in R$ に対して, 次は同値

(i) $x|a$ ならば $x = \epsilon$ または $x = \epsilon a$ (ただし ϵ は単元) と書ける
(ii) $x|a \Leftrightarrow x$ は単元か, または $x \approx a$
(iii) $(a) \subseteq (x) \subseteq R \Rightarrow (x) = (a)$ または $(x) = R$

証明. 易しいので省略. □

定義 1.4.6. R が整域のとき,

- $a \in R$ が, $x \notin R^\times$, かつ $x|a$ ならば $x = \epsilon$ または $x = \epsilon a$ (ただし ϵ は単元) をみたすとき, a は**既約元 (irreducible element)** という.
- $p \notin R^\times$ が $p|ab \Rightarrow p|a$ または $p|b$ をみたすとき, p を R の**素元**という.[6]

命題 1.4.7. 整域 R において, 素元は既約元である.

証明. $p \in R$ が素元であり, $p = ab$ と書けたとすると $ab \in (p)$ なので, $a \in (p)$ または $b \in (p)$ である. たとえば $a \in (p)$ のときは, $p|a$ であり, $p = ab$ より $a|p$ だから $a \approx p$ となり, p は既約元である. $b \in (p)$ のときも同様. □

1.5 素元分解整域 (UFD)

定義 1.5.1. 整域 R において, R の単元でない元 a $(a \neq 0)$ はすべて有限個の素元の積 $a = p_1 p_2 \cdots p_r$ と書けるとき, **素元分解整域** または **一意分解整域 (Unique Factorization Domain)** という.

定理 1.5.2. 素元分解整域において, 素元への分解は順序と単を除いて一意的である. すなわち, $a \in R$ が $a = p_1 \cdots p_r = q_1 \cdots q_s$ と 2 通りの方法で素元の積に分解したとすると, $r = s$ であり, 適当に順番を付け替えることによって $p_1 \approx q_1, \ldots, p_r \approx q_r$ となる.

証明. r に関する数学的帰納法で証明する. $r = 1$ のとき, $p_1 = q_1 \cdots q_s$ とすると, $q_1 \cdots q_s \in (p_1)$ だから $q_1 \in (p_1)$ としてよい. このとき, $p_1 \approx q_1$ であり, $q_2 \cdots q_s$ は単元だから $s = 1$ でなければならない. $r > 1$ のとき, $p_1 \cdots p_r = q_1 \cdots q_s$ だから $q_1 \cdots q_s \in (p_1)$ であり, 今と同じ議論により, $p_1 \approx q_1$ としてよい. $q_1 = \epsilon_1 p_1$ (ϵ_1 は単元) とおくと $p_1 \cdots p_r = \epsilon_1 p_1 \cdots q_s$ より $p_2 \cdots p_r = \epsilon_1 q_2 \cdots q_s$ となり, 帰納法の仮定より $r - 1 = s - 1$ で, 適当に番号を付け替えて $p_2 \approx q_2, \ldots, p_r \approx q_r$ とできる. □

命題 1.5.3. 素元分解整域において, 既約元は素元である. (よって, 既約元であることと素元であることは同値)

証明. 素元分解を考えると明らかである. □

問題 1.5.4. $R = \mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$ を考える. $w = x + y\sqrt{-5} \in R$ に対して, $\overline{w} = x - y\sqrt{-5}$, $N(w) = w\overline{w} = x^2 + 5\,y^2 \in \mathbb{Z}$ と定義すると $N(w_1 w_2) = N(w_1)N(w_2)$ である.

(i) $2, 3, 1 \pm \sqrt{-5}$ は R の素元であることを示せ.
(ii) (2) は R の素イデアルでないことを示せ.
(iii) $(2, 1 + \sqrt{-5})$ は単項イデアルでないことを示せ.
(iv) R は UFD でないことを示せ. $(6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ を使え).

1.6 単項イデアル整域 (PID)

定義 1.6.1. 整域 R において, すべてのイデアルが単項イデアルであるとき, **単項イデアル整域 (Principal Integral Domain)** という.

補題 1.6.2. 単項イデアル整域において, 既約元は素元である. (よって, 既約元であることと素元であることは同値)

[6] 命題 1.3.8 より (p) が素イデアルであると同値

証明. 単項イデアル整域においては, 命題 1.4.5 より p が既約元 $\Leftrightarrow$ (p) が極大イデアル $\Rightarrow$ (p) が素イデアル $\Leftrightarrow$ p は素元 $\square$

同様に, 次も, すぐわかる.

命題 1.6.3. R が単項イデアル整域のとき, $p \in R$ に対して, 次は同値.

(i) (p) は素イデアル
(ii) (p) は極大イデアル

定理 1.6.4. 単項イデアル整域 R は素元分解整域である.

証明. (背理法) $a \neq 0 \in R$ が単元でないとし, 素元の積として表せないと仮定する. したがって, a は既約元でないから $a = a_1 a_1'$ (a_1, a_1' は単元でない) と分解され, a_1, a_1' のうち, どちらか 1 つは既約元でない. たとえば, a_1 が既約元でないならば, $a_1 = a_2 a_2'$ (a_2, a_2' は単元でない) と分解され, a_2, a_2' のうち, どちらか 1 つ, 例えば a_2 が既約元でない. これを繰り返していくことにより, 増大するイデアルの無限列

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \subsetneq R$$

が得られる. このとき $\bigcup_i (a_i)$ はイデアルである.[7] R は単項イデアル整域だから $\bigcup_i (a_i) = (b)$ となる $b \in R$ が存在する. このとき, $^{\exists} i_0$ が存在して $b \in (a_{i_0})$ となるので,

$$(a_{i_0}) = (a_{i_0+1}) = (a_{i_0+2}) = \cdots$$

となり, 矛盾する. $\square$

命題 1.6.5. 単項イデアル整域 R の元 a, b について次は同値.

(i) a と b は互いに素.
(ii) $^{\exists} x, y \in R$ s.t. $ax + by = 1$.

証明. (i) $\Rightarrow$ (ii)
$(a, b) = (c)$ となる $c \in R$ が存在するが $c|a$ かつ $c|b$ なので c は単元でなければならない.
(ii) $\Rightarrow$ (i)
c を a, b の公約元とすると, $c|a$, $c|b$ より $c|1 = ax + by$ だから c は単元である. $\square$

例 1.6.6. X, Y を変数として, $R = \mathbb{Z}[X, Y]$ は UFD である. (後出) $I = (X, Y) \subsetneq R$ は単項イデアルではないことを示せ. よって, R は PID ではない.

1.7 ユークリッド整域

定義 1.7.1. 整域 R の 0 でない各元 a に非負整数 $v(a) \geq 0$ が対応し, 次の条件をみたすとき, **Euclid 整域 (Euclidian Domain)** という.

(1) $^{\forall} a, b \in R$ s.t. $a \neq 0$, $^{\exists} q, r$ such that $b = aq + r$ で, $r = 0$ または $v(r) < v(a)$
(2) $a \neq 0$, $b \neq 0$ に対して $v(a) \leq v(ab)$.

定理 1.7.2. Euclid 整域 R は単項イデアル整域である.

証明. $\mathfrak{a} \neq 0$ を R のイデアルとする.

$$S = \{v(x) | x \in \mathfrak{a} \text{ かつ } x \neq 0\}$$

は $\mathbb{N}$ の空でない部分集合なので最小値 $v(a)$ が存在する. このとき $\mathfrak{a} = (a)$ であることを示す. 実際, $x \in \mathfrak{a}$ として $x = aq + r$ と表すと $r = 0$ または $r \neq 0$ かつ $v(r) < v(a)$ であるが, もし後者だとすると $r = x - qa \in \mathfrak{a}$ となり, $v(a)$ の最小性に矛盾する. $\square$

表 1.8.1: $\varphi(n)$ の値

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

1.8 Möbius 関数について

定義 1.8.1. $n \in \mathbb{N}$ のとき, $1, 2, \ldots, n$ の中で n と互いに素であるものの個数を $\varphi(n)$ と書き, **Euler のファイ関数**という.

命題 1.8.2. 自然数 $n \in \mathbb{N}$ に対して

$$\sum_{d|n} \varphi(d) = n$$

が成り立つ.

例 1.8.3. $n = 12$ のとき

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$

が成り立つ.

問題 1.8.4. 命題 1.8.2 を示せ.

問題 1.8.5. $n = \prod_{i=1}^{r} p_i^{e_i}$ を n の素因数分解とすれば

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

を示せ. 例えば, $\varphi(18) = \varphi(2 \cdot 3^2) = 6$ である.

定義 1.8.6. (Möbius 関数) $n \in \mathbb{N}$ に対して $\mu(n)$ を次のように定義する. $\mu(1) = 1$ であり, $n > 1$ のとき, $n = \prod_{i=1}^{r} p_i^{e_i}$ を n の素因数分解とすれば

$$\mu(n) = \begin{cases} (-1)^r & e_1 = \cdots = e_r = 1, \\ 0 & \text{otherwise.} \end{cases}$$

$\mu(n)$ を n の **Möbius 関数**という.

表 1.8.2: $\mu(n)$ の値

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

問題 1.8.7. $n \in \mathbb{Z}$, $n > 1$ ならば

$$\sum_{d|n} \mu(d) = 0$$

を示せ.

証明. n の素因数分解を $n = p_1^{e_1} \cdots p_r^{e_r}$ $(r \geq 1)$ とすると

$$\sum_{d|n} \mu(d) = \sum_{0 \leq x_1 \leq e_1, \ldots, 0 \leq x_r \leq e_r} \mu(p_1^{x_1} \cdots p_r^{x_r}) = \sum_{0 \leq x_1 \leq 1, \ldots, 0 \leq x_r \leq 1} (-1)^{x_1 + \cdots + x_r} = \sum_{x=0}^{r} (-1)^r \binom{r}{x} = (1-1)^r = 0$$

ここで, 最後の和は $x_1 + \cdots + x_r = x$ とおいた. □

[7] これを示せ.

例 1.8.8. $n = 12$ のとき

$$\mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) = 1 - 1 - 1 + 0 + 1 + 0 = 0$$

が成り立つ.

定理 1.8.9. (逆転公式) f を $\mathbb{N}$ 上の任意の関数とし, 自然数 $n \in \mathbb{N}$ に対して

$$\sum_{d|n} f(d) = g(n)$$

とすれば

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = f(n)$$

が成り立つ.

証明.

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} f(d') = \sum_{d'|d|n} \mu\left(\frac{n}{d}\right) f(d') = \sum_{d'|n} f(d') \sum_{t|\frac{n}{d'}} \mu(t)$$

ここで,

$$\sum_{t|a} \mu(t) = \begin{cases} 1 & a = 1, \\ 0 & a > 1. \end{cases}$$

を使えば, 証明が終わる.

系 1.8.10. 自然数 $n \in \mathbb{N}$ に対して

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) d = f(n)$$

が成り立つ.

例 1.8.11. $n = 12$ のとき

$$\mu(12) \cdot 1 + \mu(6) \cdot 2 + \mu(4) \cdot 3 + \mu(3) \cdot 4 + \mu(2) \cdot 6 + \mu(1) \cdot 12 = 0 \cdot 1 + 1 \cdot 2 + 0 \cdot 3 - 1 \cdot 4 - 1 \cdot 6 + 1 \cdot 12 = 4$$

が成り立つ.

第2章　多項式環

定義 2.0.1. R を単位元をもつ可換環とするとき, R の元を係数とする n 変数 $X_1, \dots, X_n$ の多項式

$$f(X) = f(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} X^{i_1} \cdots X^{i_n}$$

全体のなす環を $R[X_1, \dots, X_n]$ と書き, R 上の n **変数多項式環**という. 特に $aX^{i_1} \cdots X^{i_n}$ の形の多項式を**単項式**といい, $i_1 + \cdots + i_n$ を, この単項式の**次数**という. 多項式 f に現れる各単項式の中で次数が最大のものを, $f(X)$ の**次数**といい, $\deg f$ と書く. $\deg 0 = -\infty$ とする.

例 2.0.2. $f(X, Y) = 2\,X^3 + X^2Y + X^2 + 2\,Y \in \mathbb{Z}[X, Y]$ は 3 次多項式, $g(X) = X^2 + \frac{1}{2}\,X + \frac{2}{3} \in \mathbb{Q}[X]$ は 2 次多項式.

この節では, 実際は R を整域と仮定することが多い. $\deg f \geq 1$ である多項式 $f \in R[X_1, \dots, X_n]$ について,

$$f = gh, \qquad 1 \leq \deg g, \deg h < f$$

となる $g, h \in R[X_1, \dots, X_n]$ が存在するとき, f は**次数可約 (degreewise reducible)** であるという. $f \in R[X_1, \dots, X_n]$ が $\deg f \geq 1$, かつ可約でないとき, **次数既約 (degreewise irreducible)** という.

例 2.0.3. $h(X) = 2\,X^3 + 2\,X^2 + 2\,X + 2 \in \mathbb{Z}[X]$ は次数可約, $g(X) = X^2 + \frac{1}{2}\,X + \frac{2}{3} \in \mathbb{Q}[X]$ は次数既約.

命題 2.0.4. $f \in R[X_1, \dots, X_n]$ が単元 $\Leftrightarrow$ f は R の単元

証明. $\Leftarrow$　$f \in R[X_1, \dots, X_n]$ が単元ならば $\deg f = 0$ である.
$\Rightarrow$　明らか □

例 2.0.5. $\mathbb{Z}[X_1, \dots, X_n]$ の単元は ± 1 のみである.

注意 2.0.6. F が体ならば, 『$f \in F[X]$ が次数既約 $\Leftrightarrow$ f は $F[X]$ の既約元』であるが, 一般には, R が整域のとき, $f \in R[X]$ が次数既約と $R[X]$ の元として既約であることは違う. 例えば $f(X) = 6(X^2 + X + 1) \in \mathbb{Z}[X]$ は, より次数の小さな多項式の積に書けないので次数既約であるが, $f(X)$ は $\mathbb{Z}[X]$ の素元 2, 3, $X^2 + X + 1$ の積に書けるので $\mathbb{Z}[X]$ の既約元ではない. $\mathbb{Q}[X]$ で考えれば 6 は単元なので既約元である.

2.1　1 変数多項式環

$R[X]$ を R 上の 1 変数多項式環とする. $f \in R[X]$ は

$$f = a_0 + a_1X + \cdots + a_mX^m = \sum_{i=0}^{m} a_iX^i \qquad (a_i \in R,\ a_m \neq 0)$$

と書けて, m を**次数 (degree)**, a_m を**最高次の係数 (leading coefficient)** という. $a_m = 1$ のとき**モニック (monic)** な多項式という. また, 上の f に対して, $\sum_{i=1}^{m} ia_iX^{i-1}$ で定義される多項式を f' と書き, f の**導関数 (derivative)** とよぶ.

例 2.1.1. $h(X) = 2\,X^3 + 2\,X^2 + 2\,X + 2 \in \mathbb{Z}[X]$ は 3 次多項式で, 最高次の係数が 2 なので monic でなく, $h'(X) = 6\,X^2 + 4\,X + 2 \in \mathbb{Z}[X]$ である.

命題 2.1.2. R が整域 $\Rightarrow$ $R[X]$ も整域, $f, g \in R[X]$ に対して, $\deg(fg) = \deg f + \deg g$

証明. $f = \sum_{i=0}^{m} a_iX^i$, $g = \sum_{j=0}^{n} b_jX^j$ とすると $fg = \sum_{i=0}^{m} \sum_{j=0}^{n} a_ib_jX^{i+j}$ で $a_mb_n \neq 0$ である.

系 2.1.3. R が整域 $\Rightarrow R[X_1,\dots,x_n]$ も整域, $f,g\in R[X]$ に対して, $\deg(fg)=\deg f+\deg g$

証明. $R[X_1,\dots,x_n]=R[X_1][X_2]\cdots[X_n]$ を使え.

定義 2.1.4. R が整域のとき, $R[X_1,\dots,x_n]$ の商体を

$$R(X_1,\dots,X_n)=\left\{\frac{f(X_1,\dots,X_n)}{g(X_1,\dots,X_n)}\,|\,f(X_1,\dots,X_n),g(X_1,\dots,X_n)\in R[X_1,\dots,X_n],\,g(X_1,\dots,X_n)\neq 0\right\}$$

と書く.

定理 2.1.5. R が整域, $f,g\in R[X]$ で g の最高次の係数が R の単元ならば

$$f=gq+r,\qquad r=0 \text{ または } \deg f<\deg g$$

となる $q,r\in R[X]$ が一意的に存在する.

証明. まず, 存在を示す. $f=\sum_{i=0}^m a_iX^i$, $g=\sum_{j=0}^n b_jX^j$ とすると, $\deg f<\deg g$ のときは明らかである. $\deg f=\deg g$ のときは, 多項式の割算をやれば, q, r が求められる.

次に一意性をいう. $f=gq_1+r_1=gq_2+r_2$, $\deg r_1,\deg r_2<\deg g$ とすると $g(q_1-q_2)=r_2-r_1$ である. $q_1-q_2\neq 0$ ならば $\deg g(q_1-q_2)\geq\deg g>\deg r_2-r_1$ となり矛盾である. よって $q_1=q_2$, $r_1=r_2$.

系 2.1.6. R が整域 のとき, $f\in R[X]$, $a\in R$ に対して,

$$f(X)=(X-a)q(X)+f(a),$$

となる $q(X)\in R[X]$ が一意的に存在する. 特に,

$$X-a|f(X)\quad\Leftrightarrow\quad f(a)=0$$

証明. 上の定理で $g(X)=X-a$ とすると

$$f(X)=(X-a)q(X)+r$$

である. $X=a$ を代入すると $r=f(a)$. 残りは明らか.

系 2.1.7. 整域 R 上の m 次多項式, $f(X)\in R[X]$ は m 個より多くの根を持たない.

証明. m に関する数学的帰納法.

(i) $m=1$ のときは, 明らか.

(ii) $m>2$ とし, $m-1$ まで正しいとする. m 次多項式, $f(X)\in R[X]$ が根 a を持つとすると $f(X)=(X-a)f_1(X)$ と書ける. ここで, $f_1(X)$ は $m-1$ 次式だから, 高々 $m-1$ 個の根しかもたない. よって, $f(X)$ は高々 m 個の根しかもたない.

残りは明らか.

系 2.1.8. 整域 R 上の次多項式, $f(X)\in R[X]$ が無限に多くの相異なる R の元 a に対し, $f(a)=0$ ならば $f(X)=0$ である.

定義 2.1.9. $f\in R[X]$, $a\in R$ のとき,

$$(X-a)^k|f(X)\qquad\text{かつ}\qquad(X-a)^{k+1}\not|f(X)$$

ならば, a は $f(X)$ の k **重根**, k を $f(X)$ の根 a の**重複度**という. 少なくとも 2 重根となっているとき, 単に, **重根**という.

命題 2.1.10. R が整域のとき, $a\in R$ が $f(X)\in R[X]$ の k 重根 $(k\geq 2)$ ならば, a は $f'(X)$ の少なくとも $k-1$ 重根である.

$$a\in R \text{ が } f(X) \text{ の重根} \Leftrightarrow f(a)=f'(a)=0.$$

証明. 仮定より, $f(X)=(X-a)^kg(X)$, $g(a)\neq 0$ である. このとき,

$$f'(X)=k(X-a)^{k-1}g(X)+(x-a)kg'(X)=(X-a)^{k-1}\{kg(X)+(X-a)g'(X)\}$$

なので $(X-a)^{k-1}|f(X)$ である.

2.2 体の上の 1 変数多項式環

命題 2.2.1. 体 F 上の 1 変数多項式環 $F[X]$ は Euclid 整域である.

証明. 定理 2.1.5 を使え.

系 2.2.2. 体 F 上の 1 変数多項式環 $F[X]$ は PID である.

証明. 定理 1.7.2 を使え.

命題 2.2.3. 体 F 上の 1 変数多項式 $f(X), g(X) \in F[X]$ について, 次は同値.

(i) $f(X), g(X)$ は定数以外に公約元をもたない.
(ii) $f(X)u(X) + g(X)v(X) = 1$ となる $u(X), v(X) \in F[X]$ が存在する.

命題 2.2.4. 体 F 上の 1 変数多項式 $p(X) \in F[X]$ について, 次はすべて同値.

(i) $p(X)$ は $F[X]$ の次数既約
(ii) $p(X)$ は $F[X]$ の素元
(iii) $(p(X))$ は $F[X]$ の素イデアル
(iv) $(p(X))$ は $F[X]$ の極大イデアル

2.3 UFD 上の 1 変数多項式環

この節では, R は UFD とする. また, F を R の商体とする.

定義 2.3.1. $f(X) \in R[X]$ の全ての係数の最大公約元が単元であるとき, $f(X)$ は**原始多項式 (primitive polynomial)** という.

例 2.3.2. $h(X) = 2\,X^3+2\,X^2+2\,X+2 \in \mathbb{Z}[X]$ は全ての係数が 2 で割れるので primitive でないが, $k(X) = 6\,X^2+3\,X+4 \in \mathbb{Z}[X]$ は primitive である.

補題 2.3.3. $p \in R$ が R の素元であるならば p は $R[X]$ の素元, i.e.,
$f(X), g(X) \in R[X]$ について $p \not| f(X)$ かつ $p \not| g(X) \Rightarrow p \not| f(X)g(X)$.

証明. $f(X) = a_0 + a_1X + \cdots + a_mX^m$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$ $(a_m, b_n \neq 0)$ とする. $f(X), g(X)$ の最初に p で割れない係数を, それぞれ a_j, b_k とすると, 積 $f(X)g(X)$ の X^{j+k} の係数は

$$c_{j+k} = a_{j+k}b_0 + \cdots + a_{j+1}b_{k-1} + a_jb_k + a_{j-1}b_{k+1} + \cdots + a_0b_{j+k}$$

である. $p \not| a_kb_k$ で, 他の項は全て p で割れるので, $p \not| c_{j+k}$ であるから $p \not| f(X)g(X)$. □

定理 2.3.4. (Gauss's Lemma) $f(X), g(X) \in R[X]$ が原始多項式ならば, その積 $f(X)g(X)$ も原始多項式である.

証明. もし, $f(X)g(X)$ が原始多項式でないならば, $p|f(X)g(X)$ となる素元 $p \in R$ が存在する. 補題 2.3.3 より $p|f(X)$ または $p|g(X)$ となり, $f(X), g(X)$ が原始多項式であることに反する. □

例 2.3.5. $f(X) = 2\,X^2 + 3\,X + 3$, $g(X) = 2\,X^2 + 5\,X + 2 \in \mathbb{Z}[X]$ は原始多項式であり, その積

$$f(X)g(X) = 4\,x^4 + 16\,x^3 + 25\,x^2 + 21\,x + 6 \in \mathbb{Z}[X]$$

も原始多項式である.

定義 2.3.6. 商体の元 $a, b \in F$ に対して, $b = a\epsilon$ となる R の単元 $\epsilon \in R^\times$ が存在するとき, $a \approx b$ と書き [1], a と b は同伴元という.

[1] $approx$ は同値関係

例 2.3.7. $R=\mathbb{Z}$ のとき, その商体は $F=\mathbb{Q}$ で, $\mathbb{Z}^\times=\{\pm1\}$ なので, $\frac{2}{3}$ と同伴な元は $\pm\frac{2}{3}$ である. また, $R=\mathbb{Z}[i]$ $(i=\sqrt{-1})$ のとき, その商体は $F=\mathbb{Q}[i]$ であり, $\mathbb{Z}^\times=\{\pm1,\pm i\}$ なので, $\frac{2}{3}$ と同伴な元は $\pm\frac{2}{3}$, $\pm\frac{2}{3}\,i$ である.

命題 2.3.8. $f(X)\in F[X]$ ならば $f(X)=cg(X)$ となる $c\in F$ と原始多項式 $g(X)\in R[X]$ が存在する. c は同伴元を除いて一意的であり, これを $c=c(f)$ と書き $f(X)$ の**コンテント (content)** という.

証明. $f(X)=\dfrac{a_0}{b_0}+\dfrac{a_1}{b_1}X+\cdots+\dfrac{a_m}{b_m}X^m$ とするとき, $b_0,b_1,\ldots,b_m$ の最小公倍元を B とおくと

$$f(X)=\frac{1}{B}\left(a_0\cdot\frac{B}{b_0}+a_1\cdot\frac{B}{b_1}X+\cdots+a_m\cdot\frac{B}{b_m}X^m\right)$$

と書けて, $a_i\cdot\dfrac{B}{b_i}\in R$ の R での最大公約元を $A\in R$ とすると,

$$f(X)=\frac{A}{B}\,(c_0+c_1X+\cdots+c_mX^m)$$

という形になる. ここで, $c=\frac{A}{B}$, $f_0(X)=c_0+c_1X+\cdots+c_mX^m$ とおくと, 作り方から $f_0(X)\in R[X]$ は原始的である.

もし, $f(X)=cf_0(X)=c'f_0'(X)$ $(f_0(X),f_0'(X)\in R[X]$ は原始的$)$ と書けたとすると, $c=\dfrac{a}{b}$, $c'=\dfrac{a'}{b'}$ とおくと $ab'f_0(X)=a'bf_0'(X)\in R[X]$ となる. 両辺の係数の最大公約元を考えると, $f_0(X),f_0'(X)$ が原始的であることより $ab'\approx a'b$ でなければならない. すなわち $ab'=a'b\epsilon$ となる単元 $\epsilon\in R^\times$ が存在する. よって, $c'=c\epsilon$ かつ $f_0(X)=\epsilon f_0'(X)$ となる. □

例 2.3.9. $R=\mathbb{Z}$ のとき, その商体は $F=\mathbb{Q}$ で, $g(X)=X^2+\frac{1}{2}\,X+\frac{2}{3}\in\mathbb{Q}[X]$ の場合は. $c(g)=\frac{1}{6}$, と primitive な多項式 $k(X)=6\,X^2+3\,X+4\in\mathbb{Z}[X]$ を使って, $g(X)=c(g)\,k(X)$ と分解する.

命題 2.3.10. 次は明らか

- $f\in F[X]$ に対して, $f\in R[X]\Leftrightarrow c(f)\in R$
- $f\in R[X]$ に対して, f が原始多項式 $\Leftrightarrow c(f)\approx1$
- $f,g\in F[X]$ に対して, $c(fg)=c(f)c(g)$.[2] □

補題 2.3.11. $f(X),g(X)\in R[X]$ で, $g(X)$ が原始多項式のとき, $f(X)=g(X)h(X)$ となる $h(X)\in F[X]$ が存在すれば $h(X)\in R[X]$.

証明. $f(X)=g(X)h(X)$ より $R\ni c(f)=c(g)c(h)=c(h)$ だから, 命題 2.3.10 より $h(X)\in R[X]$. □

補題 2.3.12. $f(X)\in R[X]$ が, $f(X)=g(X)h(X)$ となる $g(X),h(X)\in F[X]$ が存在したとすれば

$$f(X)=g_1(X)h_1(X),\quad \deg g=\deg g_1,\quad \deg h=\deg h_1$$

となる $g_1(X),h_1(X)\in R[X]$ が存在する.

証明. $g(X)=c(g)g_0(X)$, $h(X)=c(h)h_0(X)$ $(g_0,h_0\in R[X]$ は原始多項式$)$ とすると $f(X)=c(g)c(h)g_0(X)h_0(X)$ で, 定理 2.3.4 より, $g_0(X)h_0(X)$ は原始的で, 命題 2.3.10 より $c(g)c(h)\in R$ でなければならない. よって, 例えば, $g_1(X)=g_0(X)\in R[X]$, $h_1(X)=c(g)c(h)h_0(X)\in R[X]$ とおけばよい. □

定理 2.3.13. $f(X)\in R[X]$ が, $R[X]$ において次数既約ならば $F[X]$ において既約である.

定理 2.3.14. 素元分解整域 R 上の多項式環 $R[X]$ の元 $f(X)$ について, 次は同値

(1) $f(X)$ は $R[X]$ の素元である
(2) f は R の素元 $(\deg f=0)$, または, f は原始的かつ次数既約 $(\deg f\geq1)$.

証明. (1) ⇒ (2)
$f(X)\in R[X]$ が素元のとき, 命題 2.3.8 より $f(X)=c(f)f_0(X)$ $(f_0(X)\in R[X]$ は原始多項式$)$ とすれば, $f(X)|c(f)f_0(X)$ より $f(X)|c(f)$ または $f(X)|f_0(X)$ である. 前者の場合は $f(X)\approx c(f)$ は R の素元, 後者の場合は $f(X)\approx f_0(A)$ で $c(f)\approx1$ でなければならない.

(2) ⇒ (1)
明らか. □

[2]定理 2.3.4 を使え.

定理 2.3.15. 素元分解整域 R 上の多項式環 $R[X]$ は素元分解整域である.

証明. $f(X) \in R[X]$ のとき, 命題 2.3.8 より $f(X) = c(f)f_0(X)$ ($c(f) \in R$, $f_0(X) \in R[X]$ は原始多項式) と書ける. $c(f)$ は R の素元の積で $c(f) = p_1 \cdots p_r$ と書ける. また, R の商体 F 上の多項式環 $F[X]$ は素元分解整域だから, $F[X]$ の中で $f_0(X) = g_1(X) \cdots g_s(X)$ ($g_i(X) \in F[X]$) と書ける. 補題 2.3.12 より, $h_1, \ldots, h_s \in R[X]$ が存在し,

$$f_0(X) = h_1(X) \cdots h_s(X), \deg g_i = \deg g_i$$

となる. このとき, f_0 が原始多項式だから $1 \approx c(h_1) \cdots c(h_s)$ となり, h_i も原始多項式で $F[X]$ で次数既約だから $R[X]$ でも次数既約である. したがって, 定理 2.3.14 より, $f(X) = p_1 \cdots p_r h_1(X) \cdots h_s(X)$ は f の素元分解を与える. □

系 2.3.16. 素元分解整域 R 上の多項式環 $R[X_1, \ldots, X_n]$ は素元分解整域である.

証明. $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ を使え. □

定理 2.3.17. (Eisenstein)　R は整域, $p \in R$ が素元のとき, $f(X) = a_0 + a_1X + \cdots + a_mX^m$ が

$$p \not| a_m,\ p|a_i\ (i = 0, \ldots, m-1),\ p^2 \not| a_0$$

ならば $f(X)$ は $R[X]$ において次数既約である.

証明. もし, $f(X) = g(X)h(X)$ と分解されたとして, $g(X) = b_0 + b_1X + \cdots + b_rX^r$, $h(X) = c_0 + c_1X + \cdots + c_sX^s$ とすると, $a_0 = b_0c_0$ で

$$p|a_0,\ p^2 \not| a_0$$

より, b_0, c_0 のどちらか一方が p の倍元である. 例えば

$$p|b_0,\ p \not| c_0$$

とすると

$$p|a_1 = b_1c_0 + b_0c_1,\ p|b_0,\ p \not| c_0 \Rightarrow p|b_1$$

である. さらに

$$p|a_2 = b_2c_0 + b_1c_1 + b_0c_2,\ p|b_0,\ p|b_1,\ p \not| c_0 \Rightarrow p|b_2$$

である. これを繰り返していくと $p|b_i$ ($i = 1, \ldots, m-1$) がわかる. もし, $r < m$ ならば $p|a_m = b_rc_s$ となり $p \not| a_m$ に反するので, $r = m$, $s = 0$ でなければならない. □

定理 2.3.18. $f \in R[X]$, $c \in$ のとき,

$$f(X) \text{ は次数既約} \Leftrightarrow f(X + c) \text{ は次数既約}$$

問題 2.3.19. $X^2 - 6$ は $\mathbb{Q}$ 上既約であることを示せ. ($\sqrt{6}$ が無理数であることを使ってはいけない.)

解答. $p = 2$ として Eisenstein's Irreducibility Criterion を使え. □

問題 2.3.20. p が素数のとき, $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ は $\mathbb{Q}$ 上既約であることを示せ.

解答. $f(X) = \dfrac{X^p - 1}{X - 1}$ より

$$f(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$$

に Eisenstein's Irreducibility Criterion を使え. □

問題 2.3.21. $F(X) = X^4 + 1$ は $\mathbb{Q}$ 上既約であることを示せ.

解答. $f(X+1) = X^4 + 4\,X^3 + 6\,X^2 + 4\,X + 2$ に $p = 2$ として Eisenstein's Irreducibility Criterion を使え. □

問題 2.3.22. $f(X) = X^6 + X^3 + 1$ は $\mathbb{Q}$ 上既約であることを示せ.

解答. $f(X+1) = x^6 + 6\,x^5 + 15\,x^4 + 21\,x^3 + 18\,x^2 + 9\,x + 3$ に $p = 3$ として Eisenstein's Irreducibility Criterion を使え. □

問題 2.3.23. $X^3 - X - 1$ は $\mathbb{Q}$ 上既約であることを示せ.

解答. $\mathbb{Z}[X]$ において $f(X) = (X + b_1X + b_0)(X + c_0)$ と 2 次式と 1 次式の積に分解したとすると $b_0c_0 = -1$ なので $c_0 = \pm 1$ でなければならない. ところが $f(\pm 1) \neq 0$. □

R, S が整域, $\sigma : R \to F$ を環準同型写像とする. $a \in R$ に対して $\sigma(a)$ を a^σ と書く. また $f(X) = \sum_{i=1}^{m} a_i X^i \in R[X]$ に対して $\sum_{i=1}^{m} a_i^\sigma X^i \in S[X]$ を $f^\sigma(X)$ と書く. また, ここから F は R の商体ではない.

定理 2.3.24. R が整域, F が体で, $\sigma : R \to F$ を環準同型写像とする. このとき, $f(X) \in R[X]$ が次の 2 条件をみたせば, R 上次数既約である.

(1) $\deg f^\sigma = \deg f$.
(2) $\deg f^\sigma$ は F 上次数既約である.

証明. $f(X)$ が次数可約であるとすると

$$f(X) = g(X)h(X), \qquad 0 < \deg g, \deg h < \deg f$$

となる $g, h \in R[X]$ が存在する. このとき, $f^\sigma(X) = g^\sigma(X)h^\sigma(X)$ となり, 次数はあがらないので $\deg g^\sigma, \deg h^\sigma < \deg f = \deg f^\sigma$ となる. よって $f^\sigma(X)$ も次数可約である.

系 2.3.25. R が単項イデアル整域 (PID),

$$f(X) = a_0 + a_1X + \cdots + a_mX^m \in R[X]$$

を多項式, $p \in R$ を $p \nmid a_m$ である素元であるとき $\pi_p : R \to R/(p)$ を射影とする. $f^{\pi_p}(X)$ が $R/(p)$ 上次数既約であれば, $f(X)$ は R 上次数既約である.

例 2.3.26. $f(X) = X^3 + 6\,X^2 + 5\,X + 1 \in \mathbb{Z}[X]$ が $\mathbb{Z}$ 上既約であることを示したいとき, $p = 3$ をとると $g(X) = f^{\pi_3}(X) = X^3 + 2\,X + 1 \in \mathbb{F}_3[X]$ である. $g(X)$ は 3 次式なので, 可約だとすると必ず 1 次の因子があるが, $X = 0, 1, 2$ を代入しても 0 にはならないので既約である.

第3章　体の拡大

3.1　部分体, 拡大体

定義 3.1.1. E が体, 部分集合 $F \subseteq E$ が

(1) F は E の部分環.
(2) $x \in F \Rightarrow x^{-1} \in F$

F は E の**部分体 (subfield)**, E は F の**拡大体 (extension field)** という. また, **体の拡大を** E/F と表す. さらに, $F \subseteq M \subseteq E$ で, F が M の部分体, M が E の部分体のとき, M を拡大 E/F の**中間体 (intermediate field)** といい, $E/M/F$ と書く. さらに, 各 E_{i+1}/E_i が体の拡大になっているとき

$$E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots \subseteq E_n$$

を**体の拡大列 (tower)** という.

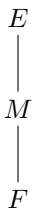

図 3.1.1: 体の拡大 $E/M/F$

定義 3.1.2. F が体 L の部分体, S は L の部分集合のとき

$$F(S) = \bigcap \{M \mid L/M/F \text{ は中間体 s.t. } M \supset S\}$$

は S を含む最小の F の拡大体 で, F 上 S で**生成**される体, または, F に S を**添加**した体という. 特に,S が有限集合 $S = \{a_1, \ldots, a_n\}$ のとき, $F(S)$ を $F(a_1, \ldots, a_n)$ と書き, $F(S)$ は F 上**有限生成であるという**. さらに, 1 個の元を添加して得られるとき, $F(a)$ を F の**単拡大** (または**単純拡大 (simple extension)**) という.

例 3.1.3. $F = \mathbb{Q}$, $E = \mathbb{C}$ として, $\mathbb{Q}\left(\sqrt{2}\right)$ は $F = \mathbb{Q}$ の単拡大である.

定義 3.1.4. L/F を体の拡大とする. E_λ $(\lambda \in \Lambda)$ が L の部分体の族のとき, $\bigcup_{\lambda\in\Lambda} E_\lambda$ を含む最小の体 $F\left(\bigcup_{\lambda\in\Lambda} E_\lambda\right)$ を, $\bigvee_{\lambda\in\Lambda} E_\lambda$ と書き, E_λ $(\lambda \in \Lambda)$ の**合成体 (composite)** という. 特に, E, F が L の部分体のとき, $E \vee F$ を EF と書く. L/F の中間体全体の集合は, 結び $\bigvee_{\lambda\in\Lambda} E_\lambda$ と交わり $\bigcap_{\lambda\in\Lambda} E_\lambda$ によって, 完全束である.

例 3.1.5. $F = \mathbb{Q}$, $L = \mathbb{C}$ として, $E_1 = \mathbb{Q}\left(\sqrt{2}\right)$, $E_2 = \mathbb{Q}\left(\sqrt{3}\right)$ は L/F の中間体であり, $E_1 \vee E_2 = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, $E_1 \wedge E_2 = E_1 \cap E_2 = \mathbb{Q}$ である. $E_1 \vee E_2 \supsetneq E_1 \cup E_2$ であることに注意せよ. 例えば $\sqrt{6} \notin E_1 \cup E_2$.

命題 3.1.6. E/F 体の拡大とする.

(1) $S_1, S_2 \subseteq E$ 部分集合のとき

$$F(S_1 \cup S_2) = F(S_1)(S_2)$$

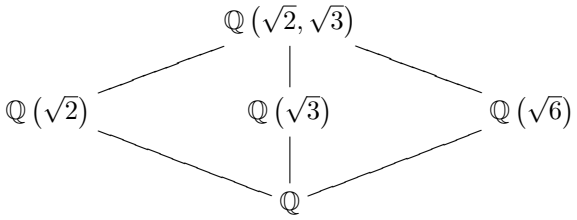

図 3.1.2: 体の拡大 $E/M/F$

(2) $\{S_\lambda\}_{\lambda\in\Lambda}$ を S の有限部分集合全体の族とすると

$$F(S)=\bigcup_{\lambda\in\Lambda}F(S_\lambda)$$

である.

証明. (1) $F(S_1\cup S_2)\supseteq F(S_1)$ かつ $F(S_1\cup S_2)\supseteq S_2$ より $F(S_1\cup S_2)\supseteq F(S_1)(S_2)$ である. また, 逆に $F\subseteq F(S_1)(S_2)$ かつ $S_1\cup S_2\subseteq F(S_1)(S_2)$ より $F(S_1\cup S_2)\subseteq F(S_1)(S_2)$ となる.

(2) $S_\lambda\subseteq S$ より $\bigcup_{\lambda\in\Lambda}F(S_\lambda)\subseteq F(S)$ である. また, $\bigcup_{\lambda\in\Lambda}F(S_\lambda)$ は体である. なぜなら, $\alpha,\beta\in\bigcup_{\lambda\in\Lambda}F(S_\lambda)$ ならば $^\exists\lambda\in\Lambda$ s.t. $\alpha,\beta\in F(S_\lambda)$ となり, このとき $\alpha\pm\beta,\alpha\beta,\alpha^{-1}\in F(S_\lambda)$ となる. よって $\bigcup_{\lambda\in\Lambda}F(S_\lambda)\supseteq F(S)$ である.

例 3.1.7. 例えば $Q\left(\sqrt{2},\sqrt{3}\right)=Q\left(\sqrt{2}\right)\left(\sqrt{3}\right)$ である.

命題 3.1.8. E/F 体の拡大, $S\subseteq E$ 部分集合のとき

$$F(S)=\left\{\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)}\,\middle|\,n\in\mathbb{N},\ f,g\in F[X_1,\ldots,X_n],\ a_1,\ldots,a_n\in S,\ g(a_1,\ldots,a_n)\neq 0\right\}$$

証明. まず, 右辺の集合を

$$F\langle S\rangle=\left\{\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)}\,\middle|\,n\in\mathbb{N},\ f,g\in F[X_1,\ldots,X_n],\ a_1,\ldots,a_n\in S,\ g(a_1,\ldots,a_n)\neq 0\right\}$$

とおく. また, $F\langle S\rangle$ が E の部分体であることを示すのは易しくて, $F\langle S\rangle$ は S を含む体だから, $F(S)$ の最小性より, $F\langle S\rangle\subseteq F(S)$ となる. したがって $F(S)=F\langle S\rangle$ である.

問題 3.1.9. 上の証明の中で $F\langle S\rangle$ が E の部分体であることを示せ.

例 3.1.10. $Q\left(\sqrt{2}\right)$ において, 任意の元は, $x,y,z,w\in\mathbb{Z}$ として

$$\frac{x+y\sqrt{2}}{z+w\sqrt{2}}=\frac{(x+y\sqrt{2})(z-w\sqrt{2})}{z^2-2w^2}=\frac{xz-2yw}{z^2-2w^2}+\frac{-xw+yz}{z^2-2w^2}w\sqrt{2}$$

の形をしているので

$$Q\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\right\}$$

である.

定義 3.1.11. (Lang) 体の拡大のクラス Cl が次の 3 条件をみたすならば **distinguished class** という.

(1) (Tower Property) 任意の拡大列 $F\subseteq K\subseteq E$ について

$$K/F\in\mathrm{Cl}\ \text{かつ}\ E/K\in\mathrm{Cl}\Leftrightarrow E/F\in\mathrm{Cl}$$

(2) (Lifting Property) 任意の拡大 $F\subseteq E$, $F\subseteq K$ について

$$K/F\in\mathrm{Cl}\Rightarrow EK/K\in\mathrm{Cl}$$

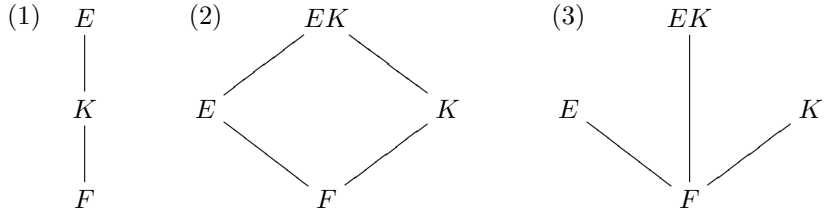

図 3.1.3: Tower Property, Lifting Property, Closure under finite composites

(3) (Closure under finite composites) 任意の拡大 $F \subseteq E$, $F \subseteq K$ について

$$K/F \in \mathrm{Cl} \text{ かつ } K/F \in \mathrm{Cl} \Rightarrow EK/F \in \mathrm{Cl}$$

補題 3.1.12. $F \subseteq K \subseteq E$ が拡大列, E/F が有限生成ならば K/F も有限生成である.

証明. 超越拡大の話のところまで証明を先延ばしする. (時間があればやる.)

定理 3.1.13. 有限生成拡大は distinguished class である.

証明. (1) (Tower Property) $K = F(\alpha_1, \ldots, \alpha_m)$, $E = K(\beta_1, \ldots, \beta_n)$ とすると, 命題 3.1.6 より

$$K = F(\alpha_1, \ldots, \alpha_m)(\beta_1, \ldots, \beta_n) = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$$

は有限生成である. 逆に, E/F が有限生成であるとき, $E = F(\alpha_1, \ldots, \alpha_m)$ とすると, $E = K(\alpha_1, \ldots, \alpha_m)$ なので, E/K は有限生成である. K/F が有限生成であることは, 補題 3.1.12 による.

(2) (Lifting Property) $K = F(\alpha_1, \ldots, \alpha_m)$ ならば $S = \{\alpha_1, \ldots, \alpha_m\}$ とおくと命題 3.1.6 より

$$EK = K(E) = F(S)(E) = F(E)(S) = E(S) = E(\alpha_1, \ldots, \alpha_m)$$

は有限生成である.

(3) (Closure under finite composites) $K = F(\alpha_1, \ldots, \alpha_m)$, $E = F(\beta_1, \ldots, \beta_n)$ とすると,

$$EK = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$$

は有限生成である.

定義 3.1.14. F が体 E の部分体のとき, E を F 上のベクトル空間と考えて, 有限次元であるか, 無限次元であるかにしたがって, E を F の**有限次拡大体**, または**無限次拡大体**といい, ベクトル空間としての次元を $[E;F]$ と書き, 拡大 E/F の**次数**という.

例 3.1.15. 上のことより $1, \sqrt{2}$ は $Q\left(\sqrt{2}\right)$ の $\mathbb{Q}$ 上の基底であり, $\left[Q\left(\sqrt{2}\right);\mathbb{Q}\right] = 2$ である.

定理 3.1.16. $F \subseteq K \subseteq E$ が部分体で $\{\omega_\alpha\}_{\alpha\in A}$ が拡大 K/F の基底, $\{\eta_\beta\}_{\beta\in B}$ が拡大 E/K の基底であるとき, $\{\omega_\alpha\eta_\beta\}_{\alpha\in A,\,\beta\in B}$ は拡大 E/F の基底である. よって $[E;F] = [E;K]\,[K;F]$ となる.

証明. $\{\omega_\alpha\eta_\beta\}_{\alpha\in A,\,\beta\in B}$ が F 上 E を生成することと線型独立であることを示せばよい. 例えば, 生成することは, $\xi \in E$ は, K-線型結合として

$$\xi = \sum_{\beta\in B} \mu_\beta\eta_\beta$$

と書ける. ここで $\mu_\beta \in K$ は $\mu_\beta = \sum_{\alpha\in A} \lambda_{\alpha.\beta}\omega_\alpha$ $(\lambda_{\alpha.\beta} \in F)$ と書けるので,

$$\xi = \sum_{\alpha\in A}\sum_{\beta\in B} \lambda_{\alpha.\beta}\omega_\alpha\eta_\beta$$

と書ける. 線型独立性も同様.

例 3.1.17. $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ であり, $1, \sqrt{2}$ は $Q\left(\sqrt{2}\right)/\mathbb{Q}$ の基底で, $1, \sqrt{3}$ は $Q\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ の基底なので $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ は $Q\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$ の基底である. ゆえに $\left[Q\left(\sqrt{2},\sqrt{3}\right);\mathbb{Q}\right] = 4$.

3.2 素体

この講義では $0 \neq 1$ と仮定している. F が体のとき, ある自然数 $^{\exists}n \in \mathbb{N}$ $(n \geq 2)$ に対して

$$n \cdot 1 = \overbrace{1 + 1 + \cdots + 1}^{n \text{ 個}} = 0$$

となるならば, そのような自然数 n の中で最小のものを p とおき, F の**標数 (characteristic)** といい, $\mathrm{ch}(F) = p$ と書く. このような自然数 n が存在しないとき, F の標数は 0 といい, $\mathrm{ch}(F) = 0$ と書く.

命題 3.2.1. F は体で $\mathrm{ch}(F) = p$ とおく.

(1) $p > 0$ のとき, p は素数である.
(2) $p > 0$ のとき F は $\mathbb{F}_p := \mathbb{Z}/(p)$ と同型な体を部分体にもつ.
(3) $p = 0$ のとき F は $\mathbb{Q}$ と同型な体を部分体にもつ.

このとき, $\mathbb{F}_p$ や $\mathbb{Q}$ を**素体 (prime field)** とよぶ. 素体は, 自分自身以外に部分体をもたない.

証明. (1) $p > 0$ のとき, $p = ab$ $a, b > 1$ と分解したとすると, $(a \cdot 1)(b \cdot 1) = a(b \cdot 1) = ab \cdot 1 = n \cdot 1 = 0$ なので, $a \cdot 1$ または $b \cdot 1 = 0$ となり, p の最小性に反するので p は素数でなければならない.
(2) $p > 0$ のとき, 準同型写像 $\varphi : \mathbb{Z} \to F$ を $n \mapsto n \cdot 1$ によって定義すると, $\mathrm{Ker}\,\varphi = (p)$ なので, $\varphi(\mathbb{Z}) \simeq \mathbb{Z}/(p) = \mathbb{F}_p$.
(3) $p = 0$ のとき, 準同型写像 $\varphi : \mathbb{Z} \to F$ を $n \mapsto n \cdot 1$ は, は一意的に単準同型写像 $\overline{\varphi} : \mathbb{Q} \to F$ に拡張される.
□

例 3.2.2. $\mathbb{F}_2 = \{0, 1\}$ は標数 2 の有限体で, 表 3.2.1 の演算表をもつ.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

表 3.2.1: $\mathbb{F}_2$ の演算表

例 3.2.3. $\mathbb{F}_3 = \{0, 1, 2\}$ は標数 3 の有限体で, 表 3.2.2 の演算表をもつ.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

表 3.2.2: $\mathbb{F}_3$ の演算表

命題 3.2.4. $\mathrm{ch}(F) = p > 0$ のとき, $x, y \in F$, $n \in \mathbb{Z}$ $(n \geq 0)$ に対して

(1) $(x + y)^{p^n} = x^{p^n} + y^{p^n}$, $(xy)^{p^n} = x^{p^n} y^{p^n}$.
(2) $\varphi : F \to F$, $x \mapsto x^{p^n}$ は中への同型.

証明. (1) 第 1 式は $p | m$, $0 < r < m$ のとき, $p | \binom{m}{r}$ という式に帰着する.
(2) (1) を使うと φ は準同型写像で, $\varphi(x) = x^{p^n} = 0$ とすると $x = 0$ なので単射である.
□

例 3.2.5. 例えば, $p = 2$, $n = 2$ のとき, $p^n = 4$ で

$$\binom{4}{0} = 1, \quad \binom{4}{1} = 4, \quad \binom{4}{2} = 6, \quad \binom{4}{3} = 4, \quad \binom{4}{4} = 1$$

だから, 二項定理より $\mathbb{F}_2$ においては

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 = x^4 + y^4$$

である.

3.3 単純拡大

定義 3.3.1. F が体 E の部分体のとき, $\alpha \in E$ に対して, $f(\alpha) = 0$ となる 0 でない多項式 $f(X) \in F[X]$ が存在するとき, F 上**代数的 (algebraic)** という. α が代数的でないとき, **超越的 (transcendental)** という.

例 3.3.2. $\mathbb{Q}$ 上代数的な複素数を**代数的数**という. また, $\mathbb{Q}$ 上超越的な複素数を**超越数**という. $\sqrt{2}, \sqrt[3]{2}$ などは代数的数, e, π などは 超越数であることが知られている. e^π は超越数であることがわかっているが, π^e が超越数であるかどうかは未解決である. $e+\pi$, $e\pi$ なども未解決らしい.

定理 3.3.3. E/F 体の拡大, $\alpha \in E$ のとき

(i) α が F 上超越的ならば, $F(\alpha) \simeq F(X)$, すなわち $F(\alpha)$ は多項式環 $F[X]$ の商体 $F(X)$ と同型.

(ii) α が F 上代数的ならば, $f_0(\alpha) = 0$ となる 0 でない monic な F 上既約多項式 $f_0(X) \in F[X]$ が一意的に定まる. このとき $F(\alpha) \simeq F[X]/(f(X))$ となる. また, このとき

$$F(\alpha) = \{f(\alpha) \,|\, f \in F[X]\}$$

であり, $\deg f_0 = n$ とすると, $F(\alpha)$ は F 上 n 次拡大である.

証明. (1) α が F 上超越的のとき, 準同型写像 $\phi : F(X) \to F(\alpha)$ が $X \mapsto \alpha$ によって一意的に定まり, $F(X) \simeq F(\alpha)$ であることを形式的に示すのは難しくない.

(2) α が F 上代数的のとき, 準同型写像 $\varphi : F[X] \to F(\alpha)$ が $X \mapsto \alpha$ によって一意的に定まる. このとき, $\mathfrak{m} = \operatorname{Ker}\varphi = \varphi^{-1}(0)$ は 1 変数多項式環 $F[X]$ の素イデアルである. なぜなら, もし $f, g \in F[X]$ が $fg \in \mathfrak{m}$ ならば $f(\alpha)g(\alpha) = 0$ なので $f(\alpha) = 0$ または $g(\alpha) = 0$ となり, $f \in \mathfrak{m}$ かまたは $g \in \mathfrak{m}$ である. $F[X]$ は単項イデアル整域なので, 命題 1.6.3 より $\mathfrak{m}$ は極大イデアルである. よって $\mathfrak{m} = (f_0(X))$ となる monic な既約多項式 $f_0(X) \in F[X]$ が存在する. 定理 1.2.17 より

$$F[X]/(f_0(X)) \simeq F(\alpha)$$

となる. $\deg f_0 = n$ とすると, $F[X]/(f_0(X))$ の元は

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + \mathfrak{m}$$

という形をしており, 任意の元は $1+\mathfrak{m}, X+\mathfrak{m}, \ldots, X^{n-1}+\mathfrak{m}$ の一次結合として一意的に書けるので $1+\mathfrak{m}, X+\mathfrak{m}, \ldots, X^{n-1}+\mathfrak{m}$ が F 上の基底である. よって, $1, \alpha, \ldots, \alpha^{n-1}$ は $F(\alpha)$ の F 上のベクトル空間としての基底であり, $F(\alpha); F] = n$, $F(\alpha) = \{f(\alpha) \,|\, f \in F[X]\}$ が成り立つ.

系 3.3.4. E/F 体の拡大, $\alpha \in E$ のとき, 次は同値

(1) α が F 上代数的

(2) $F(\alpha)/F$ は有限次拡大

証明. (1) $\Rightarrow$ (2)　定理 3.3.3 (ii)

(2) $\Rightarrow$ (1) もし, α が F 上超越的であるとすると, 定理 3.3.3 (i) より $[F(\alpha); F] = \infty$ となる.

定義 3.3.5. E/F 体の拡大, $\alpha \in E$ が代数的のとき α に対して一意的に定まる monic な既約多項式 $f_0(X)$ を α の F 上の**最小多項式 (minimal polynomial)** という.

系 3.3.6. E/F 体の拡大, $\alpha \in E$ が代数的のとき, $f(X) \in F[X]$ について次は同値

(1) $f(X) \in F[X]$ は α の F 上の最小多項式
(2) $f(X) \in F[X]$ は $f(\alpha) = 0$ となる monic な多項式で,

$$g(X) \in F[X],\, g(\alpha) = 0 \Rightarrow f(X) | g(X)$$

をみたす.
(3) $f(X) \in F[X]$ は, $g(\alpha) = 0$ となる monic な多項式 $g(X) \in F[X]$ の中で次数が最小のものである.

証明. (1) $\Rightarrow$ (2)　定理 3.3.3 (ii) の証明より $g(X) \in F[X],\, g(\alpha) = 0 \Rightarrow g(X) \in (f(X)) \Rightarrow f(X) | g(X)$
(2) $\Rightarrow$ (1)　$f_0(X) \in F[X]$ を最小多項式とする. 定理 3.3.3 (ii) の証明より $f_0(X) | f(X)$ であり, 仮定より $f(X) | f_0(X)$ だから $f(X) \approx f_0(X)$ となる. monic なので $f(X) = f_0(X)$ でなければならない.
(2) $\Leftrightarrow$ (3)　明らか.

例 3.3.7. $F = \mathbb{Q}$, $E = \mathbb{C}$ とする. $\alpha = \sqrt{2} \in E$ は $F = \mathbb{Q}$ 上代数的で $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ が最小多項式である.

$$\mathbb{Q}\left(\sqrt{2}\right) \simeq \mathbb{Q}[X]/(X^2 - 2)$$

は 2 次拡大である. Eisenstein の判定法により, $X^2 - 2$ は $\mathbb{Q}[X]$ の既約多項式で, $\mathfrak{m} = (X^2 - 2)$ は, $\mathbb{Q}[X]$ の極大イデアルであり,

$$\pm X + \mathfrak{m}$$

$f(X) = 0$ の根である. $\left(\sqrt{2}\right)^2 = 2 \in \mathbb{Q}$ なので

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{ a + b\sqrt{2} \,|\, a, b \in \mathbb{Q} \right\}$$

なので, 基底は 1, $\sqrt{2}$ をもつ $\mathbb{Q}$ 上のベクトル空間で, 基底の間の積の演算表は表 3.3.1 のようになる. $\mathbb{Q}\left(\sqrt{2}\right)$ の中で $f(X) =$

$\cdot$	1	$\sqrt{2}$
1	1	$\sqrt{2}$
$\sqrt{2}$	$\sqrt{2}$	2

表 3.3.1: $\mathbb{Q}\left(\sqrt{2}\right)$ の基底の間の積

$X^2 - 2 = \left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)$ と因数分解する.

例 3.3.8. 同様にして

$$\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \,|\, a, b, c \in \mathbb{Q} \right\} \simeq \mathbb{Q}[X]/(X^3 - 2)$$

は $\mathbb{Q}$ の 3 次拡大である. 基底は 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ をもつ $\mathbb{Q}$ 上のベクトル空間で, 基底の間の積の演算表は表 3.3.2 のようになる. $\mathbb{Q}\left(\sqrt[3]{2}\right)$ の中で $f(X) = X^3 - 2 = \left(X - \sqrt[3]{2}\right)\left(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}\right)$ と因数分解する.

$\cdot$	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$
1	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{4}$	2
$\sqrt[3]{4}$	$\sqrt[3]{4}$	2	$2\sqrt[3]{2}$

表 3.3.2: 基底の間の積

例 3.3.9. $n > 1$ が自然数, p が素数のとき, $f(X) = x^n - p \in \mathbb{Z}[X]$ は定理 2.3.17 より既約多項式である.

$$\mathbb{Q}\left(\sqrt[n]{p}\right) \simeq \mathbb{Q}[X]/(X^n - p)$$

で, $\left[\mathbb{Q}\left(\sqrt[n]{p}\right); \mathbb{Q}\right] = n$ である.

例 3.3.10. $F=\mathbb{Q}$, $E=\mathbb{C}$ とする. 例えば, $f(X)=X^4-X-1\in\mathbb{Q}[X]$ は, $\mathbb{Q}$ 上の既約多項式 [1] で, その $\mathbb{C}$ における根の 1 つを α とすれば $K=\mathbb{Q}(\alpha)$ は F の 4 次拡大で.

$$\mathbb{Q}(\alpha)=\left\{a+b\alpha+c\alpha^2+d\alpha^3\,|\,a,b,c,d\in\mathbb{Q}\right\}\simeq\mathbb{Q}[X]/(X^4-X-1)$$

なので 1, α, α^2, α^4 が $\mathbb{Q}$ 上の基底である. $\alpha^4=\alpha+1$ の関係式があるので, 基底の間の積の演算表は表 3.3.3 のようになる. $\mathbb{Q}(\alpha)$ の中で $f(X)$ は $f(X)=X^4-X-1=(X-\alpha)\left(X^3+\alpha X^2+\alpha^2X+\alpha^3-1\right)$ と因数分解する.

$\cdot$	1	α	α^2	α^3
1	1	α	α^2	α^3
α	α	α^2	α^3	$\alpha+1$
α^2	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$
α^3	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$

表 3.3.3: $\mathbb{Q}(\alpha)$ における基底の間の積 (α は X^4-X-1 の根)

例 3.3.11. $F=\mathbb{F}_2$ とする. 例えば, $f(X)=X^2+X+1\in\mathbb{F}_2[X]$ は, $\mathbb{F}_2$ 上の既約多項式で, その根の 1 つを β とすれば $K=\mathbb{F}_2(\beta)$ は F の 2 次拡大で.

$$\mathbb{F}_2(\beta)=\{a+b\beta\,|\,a,b\in\mathbb{F}_2\}\simeq\mathbb{F}_2[X]/(X^2+X+1)$$

なので 1, β が $\mathbb{F}_2$ 上の基底である. $a,b=0,1$ なので, K の元は全部で $2^2=4$ 個ある. $\beta^2=1+\beta$ の関係式があるので, 演算表は表 3.3.4 のようになる. $K=\mathbb{F}_2(\beta)$ で $f(X)$ は一次式の積に因数分解して

$+$	0	1	β	$1+\beta$
0	0	1	β	$1+\beta$
1	1	0	$1+\beta$	β
β	β	$1+\beta$	0	1
$1+\beta$	$1+\beta$	β	1	0

$\cdot$	0	1	β	$1+\beta$
0	0	0	0	0
1	0	1	β	$1+\beta$
β	0	β	$1+\beta$	1
$1+\beta$	0	$1+\beta$	1	β

表 3.3.4: $\mathbb{F}_2(\beta)$ における元の間の和と積 (β は X^2+X+1 の根)

$$f(X)=(X-\beta)(X-\beta-1)=(X-\beta)(X-\beta^2)$$

となる.

問題 3.3.12. $F=\mathbb{F}_2$ とする. 既約多項式 $f(X)=X^3+X^2+1\in\mathbb{F}_2[X]$ の根の 1 つを γ とする. 例 3.3.11 と同様に演算表を作れ.

略解. $K=\mathbb{F}_2(\gamma)$ は F の 3 次拡大で.

$$\mathbb{F}_2(\gamma)=\left\{a+b\gamma+c\gamma^2\,|\,a,b,c\in\mathbb{F}_2\right\}\simeq\mathbb{F}_2[X]/(X^3-X^2-1)$$

なので 1, γ, γ^2 が $\mathbb{F}_2$ 上の基底である. 実際には, 上の $a,b,c=0,1$ なので, K は全部で $2^3=8$ 個の元からなる. $\gamma^3=1+\gamma^2$ の関係式があるので, 基底の間の積の演算表は表 3.3.5 のようになる. $K=\mathbb{F}_2(\gamma)$ で $f(X)$ は因数分解して

$$f(X)=(X-\gamma)(X-\gamma^2)(X-\gamma^2-\gamma-1)=(X-\gamma)(X-\gamma^2)(X-\gamma^4)$$

となる.

[1] $\sigma:\mathbb{Z}\to\mathbb{Z}/(2)$ による像 $f^\sigma(X)=X^4+X+1\in\mathbb{Z}/(2)[2]$ は $\mathbb{F}_2[X]$ で既約多項式なので $f(X)\in\mathbb{Z}[X]$ は既約多項式である.

$\cdot$	0	1	γ	γ^2	$1+\gamma$	$1+\gamma^2$	$\gamma+\gamma^2$	$1+\gamma+\gamma^2$
0	0	0	0	0	0	0	0	0
1	0	1	γ	γ^2	$1+\gamma$	$1+\gamma^2$	$\gamma+\gamma^2$	$1+\gamma+\gamma^2$
γ	0	γ	γ^2	$1+\gamma^2$	$\gamma+\gamma^2$	$1+\gamma+\gamma^2$	1	$1+\gamma$
γ^2	0	γ^2	$1+\gamma^2$	$1+\gamma+\gamma^2$	1	$1+\gamma$	γ	$\gamma+\gamma^2$
$1+\gamma$	0	$1+\gamma$	$\gamma+\gamma^2$	1	$1+\gamma^2$	γ	$1+\gamma+\gamma^2$	γ^2
$1+\gamma^2$	0	$1+\gamma^2$	$1+\gamma+\gamma^2$	1	γ	γ^2	γ^2	$1+\gamma$
$\gamma+\gamma^2$	0	$\gamma+\gamma^2$	1	γ	$1+\gamma+\gamma^2$	γ^2	$1+\gamma$	$1+\gamma^2$
$1+\gamma+\gamma^2$	0	$1+\gamma+\gamma^2$	$1+\gamma$	$\gamma+\gamma^2$	γ^2	1	$1+\gamma^2$	γ

表 3.3.5: $\mathbb{F}_2(\gamma)$ の元の積 (γ は X^3+X^2+1 の根)

例 3.3.13. $\alpha=\sqrt{2}+\sqrt{3}\in E=\mathbb{Q}(\sqrt{2},\sqrt{3})$ とおくと $\mathbb{Q}(\alpha)\subseteq E$ である. $(1,\sqrt{2},\sqrt{3},\sqrt{6})$ は E の $\mathbb{Q}$ 上のベクトル空間としての基底なので, 線形写像 $F_\alpha : E\to E$, $x\mapsto \alpha x$ の基底 $(1,\sqrt{2},\sqrt{3},\sqrt{6})$ に関する表現行列を求めると

$$A=\begin{pmatrix}0&2&3&0\\1&0&0&3\\1&0&0&2\\0&1&1&0\end{pmatrix}$$

となる. A の固有多項式は $\gamma_A(x)=x^4-10x^2+1$ となるので,

$$\alpha^4-10\alpha^2+1=0$$

である. $f(X)=X^4-10\,X^2+1\in\mathbb{Z}[X]$ は Z 上既約なので, $\mathbb{Q}$ 上既約であり α の $\mathbb{Q}$ 上の最小多項式である. よって $[\mathbb{Q}(\alpha);\mathbb{Q}]=4$ となるので $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\alpha)$ がわかる.

3.3.1 単純超越拡大

もし, t が F 上超越的ならば, 定理 3.3.3 (i) より $F(t)$ は t の有理関数全体のなす体で

$$F(t)=\left\{\frac{f(t)}{g(t)}\,\middle|\, f(X),g(X)\in F[X],\, g\neq 0\right\}$$

である.

$F\subseteq F(t)$ が超越拡大とする. このとき, 任意の元 $s\in F(t)\setminus F$ は t の定数でない有理関数なので

$$s=\frac{f(t)}{g(t)}\in F(t)$$

と書ける. ここで, $f(t)$ と $g(t)$ は互いに素としてよい. このとき

$$p(X)=g(X)s-f(X)\in F(s)[X]$$

とおくと, t は $p(X)$ の根なので, t は $F(s)$ 上代数的で, かつ有限生成である. よって, 系 3.3.4 より, $F(t)$ は $F(s)$ 上, 有限次拡大であるもし, 仮に $F\subseteq F(s)$ が代数拡大と仮定して矛盾を導く. このとき, 系 3.3.4 より $F(s)/F$ は有限次拡大である. よって, 定理 3.1.16 より $F(t)/F$ も有限次拡大となり系 3.3.4 より t は F 上代数的でなければならないことになり矛盾する. よって, $F\subseteq F(s)$ は超越拡大である.

次に $p(X)$ が $F(S)$ 上既約であることを示す. s は F 上超越的であるので, 定理 3.3.3 (i) より $F(s)\simeq F(Y)$ である. ここで Y は独立変数とする. よって $F(s)[X]\simeq F(Y)[Y]$ なので

$$h(Y,X)=g(X)Y-F(X)\in F(Y)[X]$$

が有理関数体 $F(Y)$ 上既約であることを示せばよい. これは, $p(Y,X)=g(X)Y-f(X)$ が $F(Y)$ 上既約であるとから示すことができる. なぜなら, もし

$$P(Y,X)=a(X)\{b(X)Y+c(X)\}$$

と因数分解したとすると, $f(X)$ と $g(X)$ が互いに素であることより. $a(X)$ は単元でなければならないからである.

定理 3.3.14. 1) t が F 上超越的であるとし, 体の拡大 $F\subseteq F(t)$ を考える.

$$s=\frac{f(t)}{g(t)}\in F(t)$$

を, 任意の $F(t)\setminus F$ の元とする. ここで, $f(t)$ と $g(t)$ は互いに素とする. このとき, 拡大列

$$F\subseteq F(s)\subseteq F(t)$$

において, 左の拡大は超越的で, また, 右の拡大は代数的であり,

$$[F(t):F(s)]=\max(\deg f,\deg g)$$

である.

2) t が F 上超越的ならば, $F(t)$ は $F\subseteq F(t)$ の F 以外の如何なる中間体上代数的である.

証明. 1) 既に示した.

(2) もし $F\subseteq K\subseteq F(t)$ かつ $K\neq F$ とすると s
$inK\setminus F$ を取る. このとき, 拡大列 $F\subseteq F(S)\subseteq K\subseteq F(t)$ において, 1) より $F(t)/F(S)$ は代数的かつ単純拡大だから系 3.3.4 より有限次拡大であり, $F(t)/K$ も有限次拡大なので, 代数拡大である.

3.4 代数拡大 (Algebraic Extnsions)

定義 3.4.1. $F\subseteq E$ 部分体のとき, E の任意の元が F 上代数的であるとき, E は F の**代数 (的) 拡大 (algebraic extnsion)** という. E は F の代数的拡大でないとき, **超越拡大 (transcedental extension)** という.

命題 3.4.2. 有限次拡大は代数拡大である.

証明. E/F が有限次拡大で $[E:F]=n$ とすると任意の $\alpha\in E$ に対して $1,\alpha,\alpha^2,\ldots,\alpha^n$ は F 上線形従属なので

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0$$

となる全てが 0 ではない係数 $a_0,a_1,\ldots,a_n\in F$ が存在する. □

命題 3.4.3. 体の拡大 E/F について, 次は同値である.

(1) E/F は有限次拡大
(2) E/F は有限生成な代数拡大
(3) E/F は有限個の代数的な元によって生成される

また, この条件が成り立つとき, E の F 上代数的な生成元を $S=\{\alpha_1,\ldots,\alpha_n\}$ とすると

$$E=\{f(\alpha_1,\ldots,\alpha_n)\,|\,f(X_1,\ldots,X_n)\in F[X_1,\ldots,X_n]\,\}$$

となる.

証明. (1) ⇒ (2) 命題 3.4.2 より代数拡大で, 基底が生成するので有限生成.

(2) ⇒ (3) 明らか

(3) ⇒ (1) $E=F(\alpha_1,\ldots,\alpha_n)=F(\alpha_1)\ldots(\alpha_n)$ とすると, 系 3.3.4 より $F(\alpha_1)/F$ は有限次拡大で, α_2 は F 上代数的だから $F(\alpha_1)$ 上も代数的であり, $F(\alpha_1,\alpha_2)/F(\alpha_1)$ も有限次拡大である. これを繰り返すと, 定理 3.1.16 より E/F は有限次拡大である.

後半は, 定理 3.3.3 (ii) と n に関する数学的帰納法. □

例 3.4.4. $F=\mathbb{Q}$, $E=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ とすると, $\sqrt{2}$, $\sqrt{3}$ はいずれも $\mathbb{Q}$ 上代数的だから E/F は有限次代数拡大である. $\alpha=\sqrt{2}$, $\beta=\sqrt{3}$ とおくと, $\alpha^2=2\in\mathbb{Q}$, $\beta^2=3\in\mathbb{Q}$ なので

$$E=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\{\,f(\alpha,\beta)\,|\,f(X,Y)\in\mathbb{Q}[X,Y]\,\}=\{\,a+b\alpha+c\beta+d\alpha\beta\,|\,a,b,c,d\in\mathbb{Q}\,\}=\{\,a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\,|\,a,b,c,d\in\mathbb{Q}\,\}$$

である. 一方で, $\gamma=\sqrt{2}+\sqrt{3}$ とおくと, $\gamma^4-10\,\gamma^2+1=0$ で $E=\mathbb{Q}(\gamma)$ なので

$$E=\mathbb{Q}\,(\gamma)=\{\,f(\gamma)\,|\,f(X)\in\mathbb{Q}[X]\,\}=\{\,a+b\gamma+c\gamma^2+d\gamma^3\,|\,a,b,c,d\in\mathbb{Q}\,\}$$

とも書ける.

命題 3.4.5. L/F を体の拡大, $S\subseteq L$ は (必ずしも有限でない) 部分集合で, S の元はすべて F 上代数的とする. このとき, $K=F(S)$ は F の代数拡大体であり, $K=F(S)$ の元は S の元の有限変数の F-係数の多項式値で表される. すなわち

$$K=\{\,f(\alpha_1,\ldots,\alpha_r)\,|\,\alpha_1,\ldots,\alpha_r\in S,\,f(X_1,\ldots,X_r)\in F[X_1,\ldots,X_r],\,r\geq 1\,\}$$

証明. $\alpha\in F(S)$ ならば命題 3.1.6 (2) より, 有限部分集合 $T=\{\alpha_1,\ldots,\alpha_r\}\subseteq S$ が存在して $\alpha\in F(T)$ となる. $\alpha_1,\ldots,\alpha_r$ は F 上代数的なので, 命題 3.4.3 より $F(T)/F$ は代数拡大で α は F 上代数的である.

後半は, 命題 3.4.3 の後半より明らかである. □

補題 3.4.6. E/F は有限次拡大で, K/F は体の拡大であるとする. このとき, EK/K 有限次拡大で

$$[EK:K]\leq[E:F]$$

が成り立つ.

証明. $\alpha_1,\ldots,\alpha_n$ を E/F の基底とすると, $E=F(\alpha_1,\ldots,\alpha_n)$ なので, 命題 3.1.6 より $EK=K(E)=K(\alpha_1,\ldots,\alpha_n)$ である. 命題 3.4.3 より $\alpha_1,\ldots,\alpha_n$ は F 上代数的だから, K 上も代数的で, 命題 3.4.3 より EK/K は有限次拡大である. これで前半は示された.

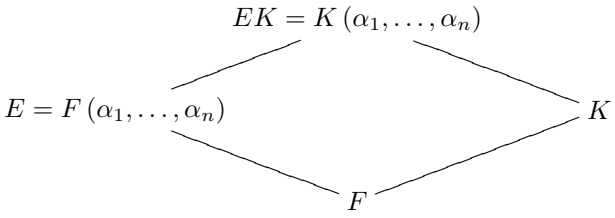

図 3.4.1: 有限次拡大の Lifting Property

最後に, $[EK:K]\leq[E:F]$ を示す. $EK=K(\alpha_1,\ldots,\alpha_n)$ だから, 命題 3.4.3 後半より EK の元は $\alpha_1,\ldots,\alpha_n$ の K 係数の多項式である. すなわち $\alpha_1^{i_1}\cdots\alpha_n^{i_n}$ の形の単項式の K-線形結合である. $\alpha_1,\ldots,\alpha_n$ を E/F の基底であったので, $\alpha_1^{i_1}\cdots\alpha_n^{i_n}\in E$ は $\alpha_1,\ldots,\alpha_n$ の F-線形結合として書けるので EK の任意の元は $\alpha_1,\ldots,\alpha_n$ の K-線形結合として書ける. よって, $[EK:K]\leq n$ である.

例 3.4.7. ω を $\omega^2+\omega+1$ の根として, $F=\mathbb{Q}$, $E=\mathbb{Q}(\sqrt[3]{2},\omega)$ とする. このとき, $[E:F]=6$ を示せ.

問題 3.4.8. $F=\mathbb{Q}$, $E=\mathbb{Q}(\sqrt[3]{2},\omega)$, $K=\mathbb{C}$ とする. ただし, ω は $\omega^2+\omega+1$ の根とするこのとき, $EK=K=\mathbb{C}$ なので, $[EK:K]=1<6=[E:F]$ となる.

例 3.4.9. $F=\mathbb{Q}$, $E=\mathbb{Q}(\sqrt[3]{2},\omega)$, $K=\mathbb{Q}(\omega)$ とする. ただし, ω は $\omega^2+\omega+1$ の根とするこのとき, $EK=E=\mathbb{Q}(\sqrt[3]{2},\omega)$ なので, $[EK:K]=3<6=[E:F]$ となる.

定理 3.4.10. 有限次拡大は distinguished class である.

証明. (1) (Tower Property) 定理 3.1.16 より明らかである.

(2) (Lifting Property) 補題 3.4.6 より成り立つ.

(3) (Closure under finite composites) $[E:F],[K:F]<\infty$ のとき, 定理 3.1.16, 補題 3.4.6 より

$$[EK:F]=[EK:K][K:F]\leq[E:F][K:F]<\infty$$

は有限次拡大である.

定義 3.4.11. $F\subseteq E$ が部分体のとき, A を E の F 上代数的な元全体の集合とすると, A は体である. A を E **の中の** F **の代数的閉包 (algebraic closure)** という. F の E 中での代数的閉包 A が F となるとき, F は E **の中で代数的に閉じている**という. F の E の中での代数的閉包 A は E の中で代数的に閉じている.

証明. $\alpha,\beta\in E$ ならば命題 3.4.3 より $F(\alpha,\beta)$ は代数拡大だから $\alpha\pm\beta,\alpha\beta,\alpha^{-1}\in F(\alpha,\beta)$ は F 上代数的である. よって, $\alpha\pm\beta,\alpha\beta,\alpha^{-1}\in E$ であり, A は体である.

最後に, A が E の中で代数的に閉じていることを示す. $\alpha\in E$ が A 上代数的ならば, α の A 上の最小多項式を

$$f(X)=a_0+a_1X+\cdots+a_nX^n\in A[X]$$

とすると, 命題 3.4.3 より $F(\alpha_1,\ldots,\alpha_n)/F$ は有限次拡大で, $F(\alpha_1,\ldots,\alpha_n,\alpha)/F(\alpha_1,\ldots,\alpha_n)$ も有限次拡大であるので, 定理 3.4.10 より $F(\alpha_1,\ldots,\alpha_n,\alpha)/F$ も有限次拡大となり, 再び, 命題 3.4.3 より α は F 上代数的となることがわかるので, $\alpha\in A$ である. □

次は上の証明からすぐにわかる.

系 3.4.12. $F\subseteq E$ が部分体のとき, $\alpha,\beta\in E$ が F 上代数的な元ならば, $\alpha\pm\beta$, $\alpha\beta$, α^{-1} 等も F 上代数的である.

定理 3.4.13. 代数拡大は distinguished class である. さらに, 任意の F 上の代数拡大体の族 $\{E_\lambda\}_{\lambda\in\Lambda}$ に対して $\bigvee_{\lambda\in\Lambda}E_\lambda$ は F 上代数拡大である

証明. (1) (Tower Property) $F\subseteq K\subseteq E$ とする. K/F, E/K が代数拡大とすると, 任意の $\alpha\in E$ に対して

$$f(X)=a_0+a_1X+\cdots+a_nX^n\in K[X]$$

を α の K 上の最小多項式とすると $a_0,a_1,\ldots,a_n$ は F 上代数的だから, 命題 3.4.3 により, $M=F(a_0,a_1,\ldots,a_n)$ は F の有限次拡大で, 定理 3.3.3 より $M(\alpha)/M$ も有限次拡大だから, 定理 3.4.10 より $M(\alpha)/F$ も有限次拡大で命題 3.4.3 より α は F 上代数的である. 逆に, E/F が代数拡大ならば, K/F, E/K が代数拡大であることは明らかである.

(2) (Lifting Property) E/F が代数拡大で, K/F が拡大ならば, 命題 3.1.6 (2) より

$$EK=K(E)=\bigcup\{K(S)\,|\,S\subseteq E\text{ 有限部分集合 }\}$$

だから $\alpha\in EK$ に対して, E の有限部分集合 $S=\{\alpha_1,\ldots,\alpha_n\}$ が存在して $\alpha\in K(\alpha_1,\ldots,\alpha_n)$ となる. ここで $\alpha_1,\ldots,\alpha_n\in E$ は F 上代数的だから, K 上も代数的で, 命題 3.4.3 より $K(\alpha_1,\ldots,\alpha_n)$ は K 上有限次拡大で代数拡大でもあるので α は K 上代数的である.

(3) (Closure under finite composites) F,E_λ はすべて拡大体 L の部分体とし, F の L の中での代数的閉包を A とする. 任意の F 上の代数拡大体の族 $\{E_\lambda\}_{\lambda\in\Lambda}$ に対して, 代数的閉包の定義より $E_\lambda\subseteq A$ である. 系 3.4.12 より A は体であるから $\bigvee_{\lambda\in\Lambda}E_\lambda\subseteq A$ となる. よって, $\bigvee_{\lambda\in\Lambda}E_\lambda$ は F 上代数拡大である.

3.5 代数的閉体・代数的閉包

定義 3.5.1. 体 F が

任意の定数ではない多項式 $f(X)\in F[X]$ は必ず F で一次式の積に分解する.

をみたすとき, F は**代数的に閉じている (algebraically closed)**, または**代数的閉体**という.

補題 3.5.2. 体 F について次の条件は同値である.

(1) F は代数的閉体.
(2) 任意の多項式 $f(X) \in F[X]$ は必ず F で少なくとも 1 つ根をもつ.
(3) $F[X]$ における既約多項式は 1 次式のみである.
(4) F の代数拡大体は F のみである.

証明. (2) $\Rightarrow$ (1)　系 2.1.6 を使え.

(1) $\Rightarrow$ (3)　明らか

(3) $\Rightarrow$ (4)　定理 3.3.3 より, α が F 上代数的ならば, α の最小多項式は 1 次式になる.

(4) $\Rightarrow$ (2)　定理 2.3.15 より, 定数でない多項式 $f(X) \in F[X]$ は既約多項式の積 $f(X) = p_1(X) \cdots p_r(X)$ に分解する. もし, 1 次式でない既約多項式 $p_i(X)$ があれば, 定理 3.3.3 より, F の代数拡大 $F[X]/(p_i(X))$ が存在するので矛盾する.

また, F が代数的閉体ならば, F の代数拡大は F 自身しかないことに注意せよ.

定義 3.5.3. $F \subseteq \Omega$ が体の列のとき

(i) Ω は代数的閉体
(ii) Ω/F は代数拡大

をみたすとき, Ω を F の**代数的閉包 (algebraically closure)** といい, $\Omega = \overline{F}$ と書く.

例 3.5.4. 例えば, 代数学の基本定理により $\mathbb{C}$ は $\mathbb{Q}$ の代数的に閉じた拡大体であるが, $\mathbb{C}/\mathbb{Q}$ は代数拡大ではない. $\mathbb{C}$ は π や e 等の $\mathbb{Q}$ 上代数的でない数を含むからである. 定理 3.5.6 は, 任意の体にそれを含む代数的閉体が存在することを保証している.

定理 3.5.5. 体の拡大 L/F において, F の L における代数的閉包を A とする. L が代数的閉体ならば, A は F の代数的閉包である.

証明. A は F の代数拡大体であるから, A が代数的閉体であることを示せばよい. $g(X) \in A[X]$ を定数でない任意の多項式とすれば, L は代数的閉体であるから, $g(X) = 0$ の根 $\alpha \in L$ が存在する. L の元 α は A に関して代数的であり, A は L の中で代数的に閉じているから $\alpha \in A$. それゆえ定数でない $A[X]$ の多項式は根をもつから, 補題 3.5.2 により A は代数的閉体である. □

定理 3.5.6. F が体のとき, F の代数的閉包 Ω が存在する.

証明. (E. Artin)　$F[X]$ における定数でないすべての多項式の作る族を $\{f_\lambda(X) | \lambda \in \Lambda\}$ とする. 添え字の集合 λ の各元 λ に不定元 X_λ を対応させて, $\{X_\lambda\}_{\lambda\in\Lambda}$ を変数とする F 上の多項式環, i.e. $\{X_\lambda\}_{\lambda\in\Lambda}$ の有限部分集合を変数とする多項式全体の集合を $R = F[\dots, X_\lambda, \dots]$ とする. R の各元は $\{X_\lambda\}_{\lambda\in\Lambda}$ の中の有限個の変数の多項式である.

いま, $f_\lambda(X_\lambda)$ $(\lambda \in \Lambda)$ 全体により生成される R のイデアルを $\mathfrak{a}$ とする. もし, $\mathfrak{a} = R$ であると仮定すると $1 \in \mathfrak{a}$ だから

$$1 = \sum_{k=1}^{N} u_k(\dots, X_\lambda, \dots) f_{\lambda_k}(X_{\lambda_k})$$

と表される. このとき, F の代数拡大 L で f_{λ_k} $(k = 1, \dots, N)$ が解を持つものが存在する. L では $0 = 1$ となり, 矛盾である. よって, $\mathfrak{a} \subsetneq R$ である.

ゆえに, 系 1.3.12 により $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq R$ となる極大イデアル $\mathfrak{m}$ が存在する. $F_1 := R/\mathfrak{m}$ と F_1 は $\{X_\lambda + \mathfrak{m}\}_{\lambda\in\Lambda}$ で生成され, $X_\lambda + \mathfrak{m}$ は $f_\lambda(X_\lambda) = 0$ をみたすから F_1/F は代数拡大である. 同様にして, 帰納的に, 次のような体の拡大列 $F = F_0 \subseteq F_1 \subseteq \cdots$ をつくることができる.

(1) F_{i+1}/F_i は代数拡大.
(2) $F_i[X]$ における定数でない多項式はすべて F_{i+1} において根をもつ.

$\Omega = \bigcup_{i=1}^{\infty} F_i$ とすると, 任意の多項式 $f(X) \in \Omega[X]$ に対して, $^\exists i \in \mathbb{N}$ が存在して $f(X)$ のすべての係数は F_i に含まれるとできる. このとき, $f(X)$ は F_{i+1} に根をもつので, 必ず Ω で少なくとも 1 つ根をもつ. よって補題 3.5.2 より Ω は代数的閉体である.

最後に, Ω/F が代数拡大であることを示す. $^\forall\alpha\in\Omega$ に対して $^\exists i\in\mathbb{N}$ が存在して $\alpha\in F_i$ となる. Tower Property より F_i/F は代数拡大なので α は F 上代数的である. □

補題 3.5.7. 体の拡大 $F\subseteq E$ について次の条件は同値である.

(1) E は F の代数的閉包.
(2) E は F の代数拡大の中で極大である. i.e., E/F は代数拡大で, もし K/E が代数拡大ならば $K=E$.
(3) E は F を含む代数的閉体の中で極小である. i.e., E は代数的閉体で $E\supset F$, かつ $F\subsetneq K\subsetneq E$ かつ K が代数的閉体であるような K は存在しない.

3.6 埋込みとその延長

$\sigma:F\to E$ が写像のとき, 次の記法を使う.

(1) 部分集合 $S\subseteq F$ に対して, σ の S への制限を $\sigma|_S$ と書く.
(2) $a\in F$ のとき, 像 $\sigma(a)$ を a^σ と書く. また, 部分集合 $S\subseteq F$ に対して, 像 $\sigma(S)$ を C^σ と書く.
(3) 多項式 $f(X)=\sum a_iX^i\in F[X]$ に対して, σ による像である多項式 $\sum a_i^\sigma X^i\in F^\sigma[X]$ を $f^\sigma(X)$ と書く.

体 F のイデアルは 0 と F 自身しかないので体 F から環 R への零写像でない写像 $\sigma:F\to R$ は <u>必ず単射</u> であり単射準同型なので, 今後, **埋込み (embedding)** とよぶことにする.

例 3.6.1. F が素体, L が任意の体ならば埋込み $\sigma:F\to L$ は $\sigma(1)=1$ より恒等写像しかない.

例 3.6.2. $F=L=\mathbb{Q}(\sqrt{2})$ ならば埋込み $\sigma:F\to L$ は $\sigma_1:\sqrt{2}\mapsto\sqrt{2}$ となるものと $\sigma_2:\sqrt{2}\mapsto-\sqrt{2}$ となるものの 2 つある.

例 3.6.3. $F=\mathbb{Q}(\sqrt{2})$, $L=\mathbb{Q}(\sqrt{3})$ ならば埋込み $\sigma:F\to L$ は存在しない.

問題 3.6.4. $F=\mathbb{Q}(\sqrt{2})$, $L=\mathbb{Q}(\sqrt{3})$ のとき埋込み $\sigma:F\to L$ が存在して $\sigma\left(\sqrt{2}\right)=a+b\sqrt{3}$ $(a,b\in\mathbb{Q})$ であるとすると矛盾することを示せ. (よって埋め込みはない.)

定義 3.6.5. E/F が体の拡大, L が体で $\sigma:F\to L$ を F の L への埋込みとする. 埋込み $\overline{\sigma}:E\to L$ が $\overline{\sigma}|_F=\sigma$ をみたすとき, σ の**延長 (extension)** という. 特に, $F\subseteq L$ で, 恒等写像 $F\to F$ の E への延長をの F **上の埋込み (embedding over F)**, または, **F-埋込み (F-embedding)** という. F の L への埋込み全体の集合, $\sigma:F\to L$ の E への延長全体の集合, F-埋込み全体の集合をそれぞれ $\hom(F,L)$, $\hom_\sigma(E,L)$, $\hom_F(E,L)$ と書く.

例 3.6.6. $F=\mathbb{Q}$, $E=\mathbb{Q}(\sqrt{2})$, $L=\mathbb{C}$ として, 恒等写像 $\sigma:\mathbb{Q}\to\mathbb{C}$ は埋め込みであり, $\overline{\sigma}:\sqrt{2}\mapsto-\sqrt{2}$ は σ の延長なので, $\overline{\sigma}\in\hom_\sigma(\mathbb{Q}(\sqrt{2}),\mathbb{C})=\hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}),\mathbb{C})$ と書く.

例 3.6.7. $F=\mathbb{Q}\left(\sqrt{2}\right)$, $E=\mathbb{Q}(\sqrt[4]{2},i)$, $L=\mathbb{C}$ とすると, E/F は 4 次の拡大である. 埋め込み $\sigma:\mathbb{Q}\to\mathbb{C}$ を $\sigma\left(\sqrt{2}\right)=-\sqrt{2}$ とする. $\tau,\varphi:E\to\mathbb{C}$ を $\tau:\sqrt[4]{2}\mapsto-\sqrt[4]{2},i\mapsto-i$, $\varphi:\sqrt[4]{2}\mapsto\sqrt[4]{2}i,i\mapsto i$ によって決める. このとき, $\tau\left(\sqrt{2}\right)=\sqrt{2}$, $\varphi\left(\sqrt{2}\right)=-\sqrt{2}$ なので φ は σ の延長であるが, τ は σ の延長ではない. $\varphi\in\hom_\sigma(\mathbb{Q}(\sqrt[4]{2},i),\mathbb{C})$, $\tau\in\hom_{\mathbb{Q}\left(\sqrt{2}\right)}(\mathbb{Q}(\sqrt[4]{2},i),\mathbb{C})$ と書く.

補題 3.6.8. (1) (埋込みによる既約性や根の対応) $\sigma:F\to L$ が埋め込みで $f(X)\in F[X]$ のとき

$$f(X)=p(X)q(X)\Longleftrightarrow f^\sigma(X)=p^\sigma(X)q^\sigma(X)$$

また, $\alpha\in F$ が $f(X)$ の根 $\Longleftrightarrow\alpha^\sigma\in F^\sigma$ が $f^\sigma(X)$ の根.

(2) (埋込みよる束構造の代数的閉包の対応) $\sigma:K\to L$ が埋め込みで $\{E_\lambda\}_{\lambda\in\Lambda}$ が K の部分体の族のとき,

$$\left(\bigcap_{\lambda\in\Lambda}E_\lambda\right)^\sigma=\bigcap_{\lambda\in\Lambda}E_\lambda^\sigma\ \text{かつ}\ \left(\bigvee_{\lambda\in\Lambda}E_\lambda\right)^\sigma=\bigvee_{\lambda\in\Lambda}E_\lambda^\sigma$$

(3) (埋込みよる添加体の対応 adjoining) $\sigma:K\to L$ が埋め込みで $F\subseteq K$ は部分体, $S\subseteq K$ は部分集合のとき.

$$F(S)^\sigma=F^\sigma(S^\sigma)$$

(4) (埋込みよる代数拡大の対応 algebraic)　$\sigma : F \to L$ が埋め込みで E/F が代数拡大, $\overline{\sigma} : E \to L$ が σ の延長のとき $E^{\overline{\sigma}}/F^{\sigma}$ も代数拡大.

(5) (埋込みによる代数的閉包の対応)　$\sigma : F \to L$ が埋め込みで F が F の代数的閉包, $\overline{\sigma} : E \to L$ が σ の延長のとき $E^{\overline{\sigma}}$ は F^{σ} の代数的閉包.

補題 3.6.9. E/F が拡大, $\alpha \in E$ は F 上代数的で, その最小多項式を $f(X) \in F[X]$ とする. L が代数的閉体で, $\sigma : F \to L$ が埋込みであるとする. このとき, 次が成り立つ.

(1) β が $f^{\sigma}(X)$ の根ならば, σ の延長 $\overline{\sigma}$ で $\alpha^{\overline{\sigma}} = \beta$ となるものが存在する.

(2) σ の $F(\alpha)$ への延長 $\overline{\sigma}$ は必ず (1) の形である.

(3) σ の $F(\alpha)$ への延長の個数は, $f(X)$ の F の代数的閉包 $\overline{F}$ の中の根の個数に等しい. (よって, $\hom_{\sigma}(F(\alpha), L)$ の cardinality は α とその最小多項式にのみに依存し, σ や L に依存しない.)

証明. α の最小多項式を $f(X)$ の次数を n とすると, 定理 3.3.3 (ii) より $F(\alpha)$ の元は $1, \alpha, \ldots, \alpha^{n-1}$ の F-線型結合

$$\gamma = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

という形で書かれる. $\overline{\sigma}|_F = \sigma$ であるとすると

$$\gamma^{\overline{\sigma}} = a_0^{\sigma} + a_1^{\sigma}\beta + \cdots + a_n^{\sigma}\beta^n$$

でなければならないが, 逆に, これは埋込み $\overline{\sigma} : F(\alpha) \to L$ を定義する. したがって $\gamma^{\overline{\sigma}}$ は $\alpha^{\overline{\sigma}} = \beta$ で決まる. (2), (3) は明らかである. □

例 3.6.10. $F = \mathbb{Q}$ とする. $\sigma : \mathbb{Q} \to \mathbb{C}$ は恒等写像しかない. $\alpha = \sqrt{2}$ とすると σ の $E = \mathbb{Q}(\sqrt{2})$ への延長は $\overline{\sigma}_1 : \sqrt{2} \mapsto \sqrt{2}$ と $\overline{\sigma}_2 : \sqrt{2} \mapsto -\sqrt{2}$ の 2 つである. これは $f^{\sigma}(X) = f(X) = X^2 - 1$ の $\mathbb{C}$ における根の個数である.

例 3.6.11. $F = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\sqrt[4]{2})$ とする. $\sigma : F = \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ として $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ となるものを取る. $\alpha = \sqrt[4]{2}$ の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式は $f(X) = X^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ であり, その像は $f^{\sigma}(X) = X^2 + \sqrt{2} \in \mathbb{C}[X]$ である. $L = \mathbb{C}$ は代数的閉体なので, $f^{\sigma}(X)$ の根 $\pm\sqrt[4]{2}i$ が存在する. よって, σ の $E = \mathbb{Q}(\sqrt[4]{2})$ への延長は $\overline{\sigma}_1 : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{C}$, $\sqrt[4]{2} \mapsto \sqrt[4]{2}i$ と $\overline{\sigma}_2 : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{C}$, $\sqrt[4]{2} \mapsto -\sqrt[4]{2}i$ の 2 つである.

定理 3.6.12. E/F が代数拡大, L が代数的閉体のとき, 次が成り立つ.

(1) 任意の埋込み $\sigma : F \to L$ は, 埋込み $\overline{\sigma} : E \to L$ に延長される.

(2) さらに, $\alpha \in E$, $f(X) \in F[X]$ をその最小多項式とする. β が $f^{\sigma}(X)$ の根のとき, (1) の延長 $\overline{\sigma}$ で $\alpha^{\overline{\sigma}} = \beta$ となるものが存在する.

証明. 集合

$$\mathscr{E} = \{\, (K, \tau) \mid F \subseteq K \subseteq E \text{ 中間体}, \tau : K \to L \text{ s.t. } \tau|_F = \sigma \text{ かつ } \alpha^{\tau} = \beta \,\}$$

上に次のような半順序を定義する. $(K_1, \tau_1), (K_2, \tau_2) \in \mathscr{E}$ に対して

$$(K_1, \tau_1) \leq (K_2, \tau_2) \Leftrightarrow K_1 \subseteq K_2 \text{ かつ } \tau_2|_{K_1} = \tau_1$$

とする. このとき, $\mathscr{E}$ が帰納的順序集合であることを示す. $\{(K_1, \tau_1)\}_{\lambda \in \Lambda}$ が $\mathscr{E}$ の全順序部分集合のとき $K = \bigcup_{\lambda \in \Lambda} K_{\lambda}$ とおき, $\tau : K \to L$ を $\alpha \in K$ に対して $\alpha \in K_{\lambda}$ となる $^{\exists}\lambda \in \Lambda$ をとり $\alpha^{\tau} = \alpha^{\tau_{\lambda}}$ によって定義する. このとき, τ は well-defined で, $(K, \tau) \in \mathscr{E}$, (K, τ) は上界になる. Zorn の補題により $\mathscr{E}$ に極大元 (K, τ) が存在する. このとき, もし, $K = E$ でないとすると, $^{\exists}\alpha \in E \setminus K$. このとき, 補題 3.6.9 により, τ は $K(\alpha) \to L$ に延長されるので矛盾である. □

系 3.6.13. $\sigma : F \to F'$ を体 F から体 F' の上への同型写像, Ω, Ω' をそれぞれ F, F' の代数的閉包とすれば, σ は Ω から Ω' の上への同型写像に拡張される.

3.7 正規拡大と多項式族の最小分解体

定義 3.7.1. $\mathscr{F} = \{f_\lambda(X)\}_{\lambda\in\Lambda}$ を $F[X]$ の多項式の族とする. $\mathscr{F}$ の**最小分解体 (splitting filed)** とは, F の拡大体 E で,

(1) $\mathscr{F}$ の任意の多項式 $f_\lambda(X)$ は $E[X]$ で一次式の積に分解する.
(2) E は $\mathscr{F}$ の多項式のすべての根から F 上生成される

の条件をみたすもののことである.

例 3.7.2. $\mathbb{Q}(\sqrt{2})$ は $\mathscr{F} = \{X^2-2\}$ の $\mathbb{Q}$ 上の最小分解体である. なぜなら X^2-2 の根は $\pm\sqrt{2}$ だからである.

例 3.7.3. $\mathbb{Q}(\sqrt[3]{2})$ は $\mathscr{F} = \{X^3-2\}$ の $\mathbb{Q}$ 上の最小分解体ではないが, $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ は最小分解体である. なぜなら X^3-2 の根は $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ だからである. ここで, $\omega = \frac{-1+\sqrt{3}i}{2}$ は 1 の原始 3 乗根である.

定理 3.7.4. $\mathscr{F} = \{f_\lambda(X)\}_{\lambda\in\Lambda}$ を $F[X]$ の多項式の族とする. 次が成り立つ.

(1) F の任意の代数的閉包 $\overline{F}$ の中で, $\mathscr{F}$ の最小分解体 A が存在する.
(2) $F \subseteq A_1 \subseteq K_1$, $F \subseteq A_2 \subseteq K_2$ がいずれも代数拡大列で, A_1 は K_1 の中での $\mathscr{F}$ の最小分解体, A_2 は K_2 の中での $\mathscr{F}$ の最小分解体のとき, 任意の F-埋込み $\sigma : K_1 \to K_2$ に対して $\sigma(A_1) = A_2$ である.
(3) $\mathscr{F}$ の任意の 2 つの最小分解体は F-同型である.

証明. (1) 代数的閉包 $\overline{F}$ の中では $f_\lambda(X)$ ($^\forall\lambda \in \Lambda$) は 1 次式の積に分解するので, その根全体の集合を R として, $A = F(R)$ とすればよい.

(2) A_1 (resp. A_2) の中での $\mathscr{F}$ の根全体の集合を R_1 (resp. R_2) とすると, $\alpha \in R_1 \Leftrightarrow \alpha^\sigma \in R_2$ なので $R_2 = R_1^\sigma$ である. $A_1 = F(R_1)$, $A_2 = F(R_2)$ より $A_1^\sigma = A_2$ である.

(3) A_1, A_2 が $\mathscr{F}$ の最小分解体のとき, A_2 の代数的閉包を $L = \overline{A_2}$ とおくと, $\sigma := F \to F \subseteq A_2$ (恒等写像) は定理 3.6.12 より, $\overline{\sigma} : A_1 \to L$ に延長される. このとき, (2) より $\overline{\sigma}(A_1) = A_2$ である.

□

例 3.7.5. 定理 3.7.4 (2) は S_1, S_2 が最小分解体でなければ成り立たない. 例えば $F = \mathbb{Q}$, $A_1 = \mathbb{Q}(\sqrt[3]{2})$, $A_2 = \mathbb{Q}(\sqrt[3]{2}\omega)$, $K_1 = K_2 = \mathbb{C}$ とする. $\sigma : \mathbb{C} \to \mathbb{C}$ として, 恒等写像をとれば $\sigma(A_1) \neq A_2$ である.

$f : A \to A$ が写像で, 部分集合 $S \subseteq A$ が $f(S) \subseteq S$ をみたすとき, S は f によって不変 (または, f-不変) という.

定理 3.7.6. $F \subseteq K \subseteq \overline{F}$ が拡大列で, $\overline{F}$ が F の代数的閉包であるとき, 次は同値である.

(1) K は $F[X]$ のある多項式の族 $\mathscr{F} = \{f_\lambda(X)\}_{\lambda\in\Lambda}$ の最小分解体である.
(2) K は任意の F-埋込み $\sigma \in \hom_F(K, \overline{F})$ によって不変である.
(3) 任意の既約多項式 $f(X) \in F[X]$ が K で根をもてば $f(X)$ は K で一次式の積に分解する.

証明. (1) ⇒ (2) 定理 3.7.4 (2)

(2) ⇒ (3) 既約多項式 $f(X) \in F[X]$ が K の中で根をもてば, $f(X)$ の任意の根 $\beta \in \overline{F}$ に対して, 定理 3.6.12 より F-埋込み $\sigma : K \to \overline{F}$ が存在して, $\sigma(\alpha) = \beta$ とできる. このとき, 仮定より $\beta \in \sigma(K) = K$ となる. よって, $f(X)$ は 1 次式の積に分解する.

(3) ⇒ (1) $\alpha \in K$ の最小多項式を $f_\alpha(X)$ と書くと K は $\mathscr{F} = \{f_\alpha(X)\}_{\alpha\in K}$ の最小分解体である. □

定義 3.7.7. 体 F の代数拡大体 E が, 定理 3.7.6 のどれか 1 つの条件 (したがって全て) をみたすとき, **正規拡大 (normal extension)**, または F **上正規**といい, $F \lhd E$ と書く.

系 3.7.8. $F \subseteq K \subseteq \overline{F}$ が拡大列で, $\overline{F}$ が F の代数的閉包であるとき, 次は同値である.

(1) K/F は有限次正規拡大である.
(2) K は有限個の F 上の既約多項式の最小分解体である.

証明. (1) ⇒ (2)　K/F は有限次正規拡大ならば, 命題 3.4.3 より有限生成な代数拡大であり $K = F(\alpha_1, \ldots, \alpha_n)$ ($\alpha_1, \ldots, \alpha_n$ は代数的) とし, $\alpha_1, \ldots, \alpha_n$ の F 上の最小多項式を $f_1(X), \ldots, f_n(X) \in F[X]$ とすると, 定理 3.7.6 より, $f_1(X), \ldots, f_n(X)$ は K で一次式の積に分解するので $\{f_1(X), \ldots, f_n(X)\}$ の最小分解体である.

(2) ⇒ (1)　K は有限個の F 上の既約多項式 $\{f_1(X), \ldots, f_n(X)\}$ の最小分解体ならば, 定理 3.7.6 より, K/F は正規拡大であり, $f_1(X), \ldots, f_n(X)$ の根は有限個なので, 命題 3.4.3 より有限生成な代数拡大で有限次拡大となる. □

例 3.7.9. $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ は正規拡大, $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ も正規拡大である. なぜなら, $\mathbb{Q}\left(\sqrt{2}\right) \simeq \mathbb{Q}[X]/(X^2-2)$ で, 既約多項式 $X^2 - 2 \in \mathbb{Q}[X]$ の根は $\pm\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$ であり, $\mathbb{Q}\left(\sqrt[4]{2}\right) \simeq \mathbb{Q}\left(\sqrt{2}\right)[X]/\left(X^2 - \sqrt{2}\right)$ で, 既約多項式 $X^2 - \sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$ の根は $\pm\sqrt[4]{2} \in \mathbb{Q}\left(\sqrt[4]{2}\right)$ だからである. しかし, $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ は正規拡大ではない. なぜなら $X^4 - 2 \in \mathbb{Q}[X]$ の根は $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$ だからである. よって, 正規拡大について Tower Property が成り立たない. よって, distinguishe class ではない.

しかし, 次が成り立つ.

定理 3.7.10. 正規拡大について次が成り立つ.

(1) 体の拡大列 $F \subseteq K \subseteq E$ に対して, $F \lhd E$ ならば $K \lhd E$ である.
(2) (Lifting Property) $F \lhd E$ が正規拡大で, $F \subseteq E$ が体の拡大のとき, $K \lhd EK$ も正規拡大である.
(3) $\{E_\lambda\}_{\lambda\in\Lambda}$ が体の族で, すべての $F \lhd E_\lambda$ が正規拡大ならば, $F \lhd \bigvee_{\lambda\in\Lambda} E_\lambda$, $F \lhd \bigcap_{\lambda\in\Lambda} E_\lambda$, も正規拡大である.

証明. (1) 多項式の族の F 上の分解体は, K 上の分解体でもある.

(2) E が多項式族 $\mathscr{F}$ の最小分解体で, $\mathscr{F}$ の根全体の集合を R とすると $E = F(R)$ である. このとき, 命題 3.1.6 より,

$$EK = E(K) = F(R)(K) = F(K)(R) = K(R)$$

なので, EK は $\mathscr{F}$ の K 上の最小分解体である.

(3) $\sigma : \bigvee_{\lambda\in\Lambda} E_\lambda \to \overline{F}$ を任意の埋込みとすると, その制限 $\sigma|_{E_\lambda} : E_\lambda \to \overline{F}$ も埋込みなので, $\sigma(E_\lambda) = E_\lambda$ である. よって

$$\sigma\left(\bigvee_{\lambda\in\Lambda} E_\lambda\right) = \bigvee_{\lambda\in\Lambda} \sigma\left(E_\lambda\right) = \bigvee_{\lambda\in\Lambda} E_\lambda$$

となり, 定理 3.7.6 により, $\bigvee_{\lambda\in\Lambda} E_\lambda/F$ は正規拡大である. 同様にして, $\sigma : \bigcap_{\lambda\in\Lambda} E_\lambda \to \overline{F}$ に対して $\sigma(E_\lambda) = E_\lambda$ より

$$\sigma\left(\bigcap_{\lambda\in\Lambda} E_\lambda\right) = \bigcap_{\lambda\in\Lambda} \sigma\left(E_\lambda\right) = \bigcap_{\lambda\in\Lambda} E_\lambda$$

であり, 定理 3.7.6 により, $\bigcap_{\lambda\in\Lambda} E_\lambda/F$ は正規拡大である.

□

3.8　正規閉包

定義 3.8.1. $\overline{F}$ は F の代数的閉包で, $F \subseteq E \subseteq \overline{F}$ が中間体とする. このとき, $E \subseteq K \subseteq \overline{F}$ となる K で, K/F が正規拡大となる K の中で最小のものを E の F 上の**正規閉包 (normal closure)** といい, $\mathrm{nc}(E/F)$ と書く.

定理 3.8.2. $\overline{F}$ は F の代数的閉包で, $F \subseteq E \subseteq \overline{F}$ が中間体とする. ($\overline{F}/F$ は代数拡大なので E/F も代数拡大である.) このとき, 次が成り立つ.

(1) E の F 上の正規閉包は存在し,

$$N = \bigcap\{\, K \mid E \subseteq K \subseteq \overline{F} \text{ かつ } F \lhd K \,\}$$

に等しい.

(2) $\mathrm{nc}(E/F)$ は

$$\mathrm{nc}(E/F) = \bigvee_{\sigma\in\mathrm{hom}_F(E,\overline{F})} E^\sigma$$

によって与えられる.

(3) $\alpha \in E$ の F 上の最小多項式を $f_\alpha(X) \in F[X]$ と書くと, $\mathrm{nc}(E/F)$ は F 上の既約多項式の族

$$\mathscr{F} = \{f_\alpha(X)\}_{\alpha\in E}$$

の最小分解体である.

(4) $\overline{F}$ の部分集合 S によって, $E = F(S)$ と書けたならば $\alpha \in S$ の F 上の最小多項式を $f_\alpha(X) \in F[X]$ と書くと, $\mathrm{nc}(E/F)$ は F 上の既約多項式の族

$$\mathscr{F} = \{f_\alpha(X)\}_{\alpha\in S}$$

の最小分解体である.

(5) E/F が有限次拡大ならば, $\mathrm{nc}(E/F)/F$ も有限次拡大である.

証明. (1) 容易なので省略.

(2) $N = \mathrm{nc}(E/F)$, $M = \bigvee_{\sigma\in\mathrm{hom}_F(E,\overline{F})} E^\sigma$ とおく. $E \subseteq N \subseteq \overline{F}$ であり, $\overline{F}/F$ は代数拡大なので, 任意の $\sigma \in \mathrm{hom}_F(E,\overline{F})$ に対して, 定理 3.6.12 より σ は $\overline{\sigma} : \overline{F} \to \overline{F}$ に延長される. N/F は正規拡大だから, 定理 3.7.6 より $N^\sigma = N$ であり, $E^\sigma \subseteq N^\sigma = N$ となる. よって $M \subseteq N$ となる.

逆を示すために, M/F が正規拡大であることを示す. 任意の $\tau \in \mathrm{hom}_F(M,\overline{F})$ に対して, σ が $\mathrm{hom}_F(M,\overline{F})$ の元全体を動くとき, $\tau\sigma$ も $\mathrm{hom}_F(M,\overline{F})$ の元全体を動くので

$$\tau(M) = \tau\left(\bigvee_{\sigma\in\mathrm{hom}_F(E,\overline{F})} \sigma(E)\right) = \bigvee_{\sigma\in\mathrm{hom}_F(E,\overline{F})} \tau(\sigma(E)) = M$$

となるので, 定理 3.7.6 より M/E は正規拡大である. $F \subseteq M \subseteq \overline{F}$ は明らかなので, N が最小の正規拡大であることより $N \subseteq M$ をえる.

(3)(4) は易しいので自分で.

(5) $N = \mathrm{nc}(E/F)$ とおく. E/F が有限次拡大ならば, 命題 3.4.3 より, E は F 上, 有限個の代数的な元 $\alpha_1, \ldots, \alpha_n$ によって生成される. これらの最小多項式を $f_1(X), \ldots, f_n(X) \in F[X]$ とすると N は, (4) よりこれらの根全体で生成されるので, 命題 3.4.3 より, N/F は有限次元である.

□

3.9 埋込みと分離性

3.10 多項式の分離性・非分離性

定理 3.10.1. F を体, $f(X), g(X) \in F[X]$ とする. K を $f(X), g(X)$ の係数をすべて含む最小の体とする. (よって $K \subseteq F$) このとき, 次が成り立つ.

(1) $f(X), g(X)$ の $F[X]$ における monic な最小公倍式 $d(X)$ は F に依存しない. すなわち, $d(X) \in K[X]$ である.

(2) $a(X), b(X) \in K[X]$ が存在して

$$a(X)f(X) + b(X)g(X) = d(X)$$

となる.

証明. $K[X]$ は PID なので, $K[X]$ の中で $(f(X), g(X))_K = (d_0(X))_K$ となる monic な多項式 $d_0(X) \in K[X]$ が存在する, すなわち, $a(X), b(X) \in K[X]$ が存在して

$$a(X)f(X) + b(X)g(X) = d_0(X)$$

となる. $K \subseteq F$ だから $d_0(X) \in (f(X), g(X))_F$ であり, $f(X), g(X)$ の $F[X]$ における monic な最大公約式を $d_1(X)$ とすると, $d_0(X) \in (f(X), g(X))_F = (d_1(X))_F$ なので

$$d_1(X)|_F d_0(X)$$

である. 一方, $f(X), g(X) \in (d_0(X))_K$ なので $d_0(X)|_K f(X)$ かつ $d_0(X)|_K g(X)$ だから $d_0(X)$ は $F[X]$ の中でも $f(X), g(X)$ の公約式であり, $d_0(X)$ が $f(X), g(X)$ の最大公約式であることより

$$d_0(X)|_F d_1(X)$$

となる. 両方とも monic なので $d_0(X) = d_1(X)$. □

定義 3.10.2. F が体で, $f(X) \in F[X]$ が既約多項式とする.[2] $f(X) \in F[X]$ が**分離的 (separable)** とは F のどんな拡大体上でも $f(X)$ が重根をもたないことである. 分離的でないとき, **非分離的 (inspeparable)** という.

定理 3.10.3. F を体, $f(X) \in F[X]$ とする. このとき, 次は同値.

(1) $f(X)$ は分離的
(2) $f(X)$ と $f'(X)$ は $F[X]$ において互いに素
(3) $f'(X) \neq 0$

証明. $f(X)$ の分解体 $\overline{F}[X]$ の中で

$$f(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_r)^{e_r} \in \overline{F}[X]$$

と書くと, $\overline{F}[X]$ の中では (1) ⇔ (2) は明らかで, 定理 3.10.1 より $F[X]$ の中でも (1) ⇔ (2) となる.

(2) ⇒ (3) は明らかなので, (2) ⇐ (3) を示す. $f(X)$ は既約なので, $f(X)$ と $f'(X)$ の $F[X]$ における最大公約式 $d(X)$ は 1 かまたは $f(X)$ である. $\deg f'(X) < \deg f(X)$ なので $d(X) \neq f(X)$ とすると $f'(X) \neq 0$ である. このとき $d(X) = 1$ となり, $f(X)$ と $f'(X)$ は互いに素である. □

系 3.10.4. $\mathrm{ch}\, F = 0$ である体 F 上の任意の既約多項式 $f(X) \in F[X]$ は分離的である.

よって, この subsection の中では以後 $\mathrm{ch}(F) = p \neq 0$ と仮定する.

系 3.10.5. F を $\mathrm{ch}(F) = p \neq 0$ である体とし, $f(X) \in F[X]$ は既約多項式とする. このとき, $f(X)$ が非分離的であることと

$$f(X) = g\left(X^{p^d}\right)$$

となる整数 $d > 0$ と定数でない多項式 $g(X) \in F[X]$ が存在することは同値である. また, 整数 d は $g(X)$ が分離的になるように選ぶことができ, そのときの d を $f(X)$ の**非分離指数 (radical exponent)** といい, $f(X)$ の分解体での根はすべて重複度 p^d になる.

証明. $f(X) = a_0 + a_1 X + \cdots + a_m X^m$ が非分離的であるとすると $f'(X) = 0$ より $p \nmid i$ のとき $a_i = 0$ だから

$$f(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \cdots + a_{pl} X^{pl} = q(X^p)$$

の形をしている. ここで, $q(X) = a_0 + a_p X + a_{2p} X^2 + \cdots + a_{pl} X^l$ である. もし, $q(X)$ が分離的ならば, 主張が成り立つ. もし, 非分離的ならば同じ議論を繰り返して $f(X) = g(X^{p^d})$ という形で $g'(X) \neq 0$ とできる. $g(X)$ の分解体では

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_k)$$

という形に書け, $g'(X) \neq 0$ より重根を持たない. $f(X)$ の分解体では

$$f(X) = (X^{p^d} - \alpha_1) \cdots (X^{p^d} - \alpha_k) = (X^{p^d} - \beta_1^{p^d}) \cdots (X^{p^d} - \beta_k^{p^d}) = (X - \beta_1)^{p^d} \cdots (X - \beta_k)^{p^d}$$

と書けるので, 根の重複度はすべて p^d である. □

系 3.10.6. 有限体 F 上の任意の既約多項式は分離的である.

[2] 体上の多項式環なので, 次数既約と同値

証明. F が有限体ならば, 標数は $p>0$ で, 素体 $\mathbb{F}_p$ 上の有限次拡大だから, その拡大次数を n とすると F は $q=p^n$ 個の元からなる. その乗法群 $F^\times$ の位数は $q-1$ なので, $F\ni\alpha\neq 0$ ならば $\alpha^{q-1}=1$ である. 両辺に α を掛けると $\alpha^q=\alpha$ となり, この式は任意の $\alpha\in F$ について成り立つ.

$f(X)$ が非分離的とすると, 系 3.10.5 により

$$f(X)=g(X^p)=a_0+a_1X^p+\cdots+a_mX^{pm}$$

と書ける. $a_i=b_i^p$ $(i=1,\ldots,m)$ とすると

$$f(X)=b_0^p+b_1^pX^p+\cdots+b_m^pX^{pm}=(b_0+b_1X+\cdots+b_mX^m)^p$$

となり, $f(X)$ が既約であることに矛盾する. □

3.11 拡大の個数と分離次数

S が F の部分集合, n が自然数のとき, $\{\,s^n\,|\,s\in S\,\}$ を S^n と書く.

補題 3.11.1. $\mathrm{ch}(F)=p\neq 0$, E/F は代数拡大で, $S\subseteq E$ は部分集合とする.

(1) $F(S)=F(S^{p^k})$ がある 1 つの自然数 $k\geq 1$ に対して成立することは, すべての自然数 $k\geq 1$ に対して成立するための必要十分条件である.
(2) $F=F^{p^k}$ がある 1 つの自然数 $k\geq 1$ に対して成立することは, すべての自然数 $k\geq 1$ に対して成立するための必要十分条件である.

証明. (1) ある 1 つの自然数 $k_0\geq 1$ に対して $F(S)=F(S^{p^{k_0}})$ が成立したとする. このとき,

$$F(S)=F(S^{p^{k_0}})\subseteq F(S^p)\subseteq F(S)$$

となるので $F(S)=F(S^p)$ となる. すべての自然数 $k\geq 1$ に対して, $S^{p^k}\subseteq F(S)$ なので $F(S^{p^k})\subseteq F(S)$ である. 逆を k に関する帰納法で示す. $k=1$ のとき正しい. k のとき, $F(S)\subseteq F(S^{p^k})$ が成り立つと仮定する. 任意の $\alpha\in F(S)=F(S^p)$ は, 命題 3.4.5 により S^p の多項式で書けるので S^p の単項式の F-線型結合であり, 各単項式は有限個の S^p の元を使って

$$s_1^{pi_1}\cdots s_k^{pi_k}$$

の形をしている. さらに, $s_1,\ldots,s_k\in S$ は帰納法の仮定より $F(S^{p^k})$ の元なので, 命題 3.4.5 により S^{p^k} の元の多項式で書ける. 上の各 s_j を S^{p^k} の単項式の F-線型結合で書いて代入すると, 上の単項式は $F(S^{p^{k+1}})$ の単項式の F-線型結合で書けることがわかる.

(2) $F=F^{p^{k_0}}$ がある 1 つの自然数 $k_0\geq 1$ に対して成立すれば,

$$F=F^{p^{k_0}}\subseteq F^p\subseteq F$$

より $F^p=F$ である. このとき, すべての自然数 $k\geq 1$ に対して

$$F^{p^k}=(F^p)^{p^k}=F^{p^{k+1}}$$

が成立する.

□

次の定理は, 補題 3.6.9 (3) の代数拡大への拡張である.

定理 3.11.2. E/F は代数拡大, L が代数的閉体で $\sigma:F\to L$ を埋込みとする. このとき, $\hom_\sigma(E,L)$ の濃度は E/F にのみ依存し, L や σ に依存しない. すなわち, L' も代数的閉体で $\tau:F\to L'$ も埋込みのとき, 濃度として

$$|\hom_\sigma(E,L)|=|\hom_\tau(E,L')|$$

となる.

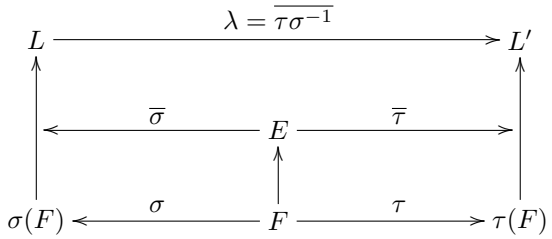

図 3.11.1: 体の拡大 $E/M/F$

証明. E/F は代数拡大なので, $\sigma(F)$, $\tau(F)$ は, それぞれの代数的閉包に含まれるので, L, L' はそれぞれ $\sigma(F)$, $\tau(F)$ の代数的閉包と仮定してよい. このとき, 定理 3.6.12 により $\tau\sigma^{-1} : F^{\sigma} \to F^{\tau}$ は $\lambda = \overline{\tau\sigma^{-1}} : L \to L'$ に延長される. 系 3.6.13 より代数的閉包は同型を除いて一意であるから, $\lambda(L) = L'$ で λ は同型写像である. 任意の $\overline{\sigma} \in \hom_{\sigma}(E, L)$ に対して, $\lambda\overline{\sigma} : E \to L'$ は $\hom_{\tau}(E, L')$ の元であり, 逆に, 任意の $\overline{\tau} \in \hom_{\tau}(E, L')$ に対して, $\lambda^{-1}\overline{\tau} : E \to L$ は $\hom_{\sigma}(E, L)$ の元であるので,

$$|\hom_{\sigma}(E, L) = |\hom_{\tau}(E, L')|$$

となる. □

定義 3.11.3. E/F は代数拡大とする. L が代数的閉体で, $\sigma : F \to L$ を埋込みとするとき $\hom_{\sigma}(E, L)$ の濃度を E の F 上の **分離次数 (separable degree)** といい, $[E : F]_s$ と書く.

定義 3.11.4. $\alpha \in E$ が体 F 上代数的のとき, α の F 上の最小多項式を $f(X) \in F[X]$ とする. $f(X)$ が分離的であるとき, α は**分離的 (separable)** という. また, $f(X)$ が非分離的であるとき, α は**非分離的 (inseparable)** といい, $f(X)$ の非分離指数を α の**非分離指数 (radical exponent)** という.

定理 3.11.5. E/F が代数拡大で, $\alpha \in E$ の F 上の最小多項式を $f(X) \in F[X]$ とする. L が代数的閉体で $\sigma : F \to L$ は埋込みとする. このとき, 次が成り立つ.

(1) α が分離的ならば

$$[F(\alpha) : F]_s = [F(\alpha) : F]$$

(2) α が非分離的ならば, α の非分離指数を d とすると

$$[F(\alpha) : F]_s = \frac{1}{p^d}[F(\alpha) : F]$$

いずれの場合も $|\hom_{\sigma}(F(\alpha), L)|$ は $[F(\alpha) : F]$ の約数である.

証明. $[F(\alpha) : F] = \deg f$ と系 3.10.5 より明らか. □

定理 3.11.6. $F \subseteq K \subseteq E$ が代数拡大ならば, 濃度として

$$[E : F]_s = [E : K]_s[K : F]_s$$

が成り立つ.

証明. $\sigma : F \to \overline{E}$ を埋込みとする. σ の K への延長 $\overline{\sigma} \in \hom_{\sigma}(K, \overline{E})$ の濃度は $[K : F]_s$ であり, それぞれの $\overline{\sigma}$ の $\tau : E \to \overline{E}$ への延長は定理 3.11.2 により $\overline{\sigma}$ に依存せずに濃度が $[E : K]_s$ あり, これらは全て異なるので $[E : F]_s \geq [E : K]_s[K : F]_s$ である. 逆に, $\tau \in \hom_{\sigma}(E, \overline{E})$ が与えられたとき, $\tau|_K : K \to \overline{E}$ は $\hom_{\sigma}(K, \overline{E})$ の元であり, 逆に τ は $\tau|_K$ の延長であるので, $[E : F]_s \leq [E : K]_s[K : F]_s$ である. よって, 等号が成り立つ. □

定義 3.11.7. 代数拡大 E/F が**分離的 (separable)** とは全ての $\alpha \in E$ が F 上分離的であることである. 分離的でないときは, **非分離的 (inseparable)** という.

定理 3.11.8. (単拡大と分離性)　E/F は代数拡大で, $\mathrm{ch}(F) = p \neq 0$ とする. このとき, 次の 4 条件は同値である.

(1) α は F 上分離的である.
(2) $[F(\alpha):F]_s = [F(\alpha):F]$
(3) $F(\alpha)/F$ は分離拡大である.
(4) ある自然数 $k \geq 1$ に対して

$$F(\alpha) = F(\alpha^{p^k})$$

となる. (よって, 補題 3.11.1 より, 任意の自然数 $k \geq 1$ に対して成り立つ.)

もし, α が F 上非分離的ならば α の F 上の非分離的指数を d とすると

$$[F(\alpha):F]_s = \frac{1}{p^d}[F(\alpha):F]$$

である.

証明. 定理 3.11.5 より (1) $\Leftrightarrow$ (2) である.

(1) $\Rightarrow$ (3) を示す. $\beta \in F(\alpha)$ ならば $F \subseteq F(\beta) \subseteq F(\alpha)$ は代数拡大である. 定理 3.11.6 により, $[F(\alpha):F]_s = [F(\alpha):F(\beta)]_s[F(\beta):F]_s$, 定理 3.1.16 により, $[F(\alpha):F] = [F(\alpha):F(\beta)][F(\beta):F]$, (2) より $[F(\alpha):F]_s = [F(\alpha):F]$, 定理 3.11.5 により, $[F(\beta):F]_s \leq [F(\beta):F]$ だから $[F(\beta):F]_s = [F(\beta):F]$ でなければならない. よって, β は F 上分離的である.

(3) $\Rightarrow$ (1) は明らかである.

(1) $\Rightarrow$ (4) を示す. $F \subseteq K \subseteq F(\alpha)$ のとき, α の F 上の最小多項式を $f(X)$, K 上の最小多項式を $g(X)$ とすると, $f(X) \in K[X]$, $f(\alpha) = 0$ より, 系 3.3.6 により $g(X)|f(X)$ である. 任意の自然数 $k \geq 1$ に対して

$$F \subseteq F(\alpha^{p^k}) \subseteq F(\alpha)$$

であり, α は

$$F(\alpha^{p^k})[X] \ni X^{p^k} - \alpha^{p^k} = (X-\alpha)^{p^k}$$

を満たすので, α の $F(\alpha^{p^k})$ 上の最小多項式 $f(X)$ は $(X-\alpha)^{p^k}$ を割り切る. α は $F(\alpha^{p^k})$ 上分離的だから, $f(X) = X - \alpha$ となり, $\alpha \in F(\alpha^{p^k})$ ゆえに $F(\alpha^{p^k}) = F(\alpha)$ である.

(4) $\Rightarrow$ (1) を示す. 補題 3.11.1 より, 任意の自然数 $k \geq 1$ に対して, $F(\alpha^{p^k}) = F(\alpha)$ が成り立つ. 特に, d を α の非分離指数とすると, 系 3.10.5 により α^{p^d} は F 上分離的であり, 既に示した (1) $\Rightarrow$ (3) より, $F(\alpha^{p^d}) = F(\alpha)$ は分離拡大なので, 定義より α は分離的である.

α の F 上の最小多項式を $f(X)$ とすると, 系 3.10.5 により $f(X) = g\left(X^{p^d}\right)$ と書けて, $g(X)$ は分離多項式である. 補題 3.6.9 (3) より $[F(\alpha):F]_s$ は $f(X)$ の異なる根の個数だから $[F(\alpha):F]_s = \deg g$ である. $f(X)$ の形より

$$[F(\alpha):F] = \deg f = p^d \deg g = p^d[F(\alpha):F]_s$$

を得る. □

有限次拡大について, 次のような同様の定理が成り立つことは驚くべきことである.

定理 3.11.9. (有限次拡大と分離性) E/F は有限次拡大で, $\mathrm{ch}(F) = p \neq 0$ とする. このとき, 次の 4 条件は同値である.

1) E/F は分離拡大である.
2) $[E:F]_s = [E:F]$
3) F 上分離的な有限個の元 $\alpha_1, \ldots, \alpha_n \in E$ が存在して $E = F(\alpha_1, \ldots, \alpha_n)$ となる.
4) 有限部分集合 $S \subseteq E$ によって $E = F(S)$ と書けるならば, ある自然数 $k \geq 1$ が存在して

$$E = F(S^{p^k})$$

となる. (よって, 補題 3.11.1 より, 任意の自然数 $k \geq 1$ に対して成り立つ.)

もし, E/F が非分離拡大ならば

$$[E:F]_s = \frac{1}{p^e}[E:F]$$

となる自然数 $e \geq 1$ が存在する.

証明. 1) ⇒ 3)　E/F は有限次拡大なので, 命題 3.4.3 より, S の有限部分集合 $S_0 = \{\alpha_1, \ldots, \alpha_n\}$ によって $E = F(S_0)$ となっている. E/F が分離拡大なので, $\alpha_1, \ldots, \alpha_n$ は F 上分離的である.

3) ⇒ 2)　命題 3.4.3 より, F 上分離的な有限個の元 $\alpha_1, \ldots, \alpha_n \in E$ が存在して $E = F(\alpha_1, \ldots, \alpha_n)$ であるとする. このとき

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \ldots, \alpha_n) = E$$

という拡大列を考えると, 各 α_i は $F(\alpha_1, \ldots, \alpha_{i-1})$ 上分離的である. なぜなら, α_i は F 上分離的だからその拡大体の上でも分離的である.[3] よって, 定理 3.11.8 により,

$$[F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})]_s = [F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})]$$

が $i = 1, \ldots, n$ に対して成り立つ. 定理 3.1.16, 定理 3.11.6 により

$$[E : F]_s = [E : F]$$

となる.

2) ⇒ 1)　任意の $\beta \in E$ に対して, 拡大列

$$F \subseteq F(\beta) \subseteq E$$

を考えると, 定理 3.1.16, 定理 3.11.6 により

$$[E : F] = [E : F(\beta)][F(\beta) : F], \qquad [E : F]_s = [E : F(\beta)]_s[F(\beta) : F]_s$$

なので, もし, $[F(\beta) : F]_s < [F(\beta) : F]$ ならば $[E : F]_s = [E : F]$ とはならない. よって $[F(\beta) : F]_s = [F(\beta) : F]$ であり, 定理 3.11.8 より β は F 上分離的である.

1) ⇒ 4)　E の有限部分集合 S があって, $E = F(S)$ としよう. 任意の $\alpha \in S$ は F 上分離的なので, 定理 3.11.8 より

$$F(\alpha) = F(\alpha^{p^d}) \subseteq F(S^{p^k})$$

が任意の自然数 $k \geq 1$ に対して成り立つ. よって

$$F(S) = F(\alpha_1, \ldots, \alpha_n) \subseteq F(S^{p^k})$$

である. 逆の包含関係 $F(S^{p^k}) \subseteq F(S)$ は自明である.

4) ⇒ 1)　逆に, $F(S^{p^k}) = F(S)$ がある自然数 k について成り立てば, 補題 3.11.1 より, 任意の自然数 $k \geq 1$ に対して成り立つ. ここで, k を S に含まれる有限個の元の非分離指数 d の中の最大のものになるようにとるとすべての $\alpha \in S$ に対して α^{p^k} はすべて分離的である.[4] よって $F(S^{p^k})$ は分離的な元によって生成されるから F 上分離的である. □

定理 3.11.10. (代数拡大と分離性)　E/F は代数拡大で, $\mathrm{ch}(F) = p \neq 0$ とする. このとき, 次が成り立つ.

(1) E/F は分離拡大であるための必要十分条件は分離的な元の集合 S によって $E = F(S)$ と書かれる.
(2) E/F が分離的で $E = F(S)$ とすると, 任意の自然数 $k \geq 1$ に対して $E = F(S^{p^k})$ が成り立つ.

証明. (1) を示す.　E/F が分離拡大ならば E が F 上分離的な元で生成されることは自明である. 逆に, F 上分離的な元の集合 S が存在して $E = F(S)$ としよう. 任意の $\beta \in E$ に対して, 命題 3.1.6 (2) により, S の有限部分集合 S が存在して $\beta \in F(S_0)$ となる. よって, 命題 3.4.3 により, $F(S_0)/F$ は有限次拡大であり, 定理 3.11.9 により, 分離拡大である. よって, β は F 上分離的である. ゆえに E/F は分離拡大である.

次に (2) を示す.　任意の $\alpha \in S$ と任意の自然数 $k \geq 1$ に対して定理 3.11.8 (4) により

$$F(\alpha) = F(\alpha^{p^k}) \subseteq F(S^{p^k})$$

なので, $F(S) \subseteq F(S^{p^k})$ となる. 逆の包含関係は自明なので, $F(S) = F(S^{p^k})$ である. □

[3] $F \subseteq K \subseteq E$ とし, $\alpha \in E$ が F 上分離的であるとすると, α の F 上の最小多項式 $f(X)$ は重根を持たない. α の K 上の最小多項式を $g(X)$ とすると $f(X) \in K[X]$ で $f(\alpha) = 0$ だから, 系 3.3.6 より $g(X) | f(X)$ である. よって $g(X)$ も重根を持たない.

[4] β が F 上分離的ならば, 任意の自然数 $k \geq 1$ に対して β^{p^k} も F 上分離的である. なぜなら, β が F 上分離的ならば, 定理 3.11.8 (3) により $F(\beta)/F$ は分離拡大で, $\beta^{p^k} \in F(\beta)$ は F 上分離的である.

3.12 分離拡大は distinguished

定理 3.12.1. (分離拡大は distinguished)

(1) 分離拡大は distinguished class である.
(2) 分離拡大体の任意の合成体 (composite) は分離拡大体である.
(3) E/F が分離拡大ならば, その正規閉包 $\mathrm{nc}(E/F)$ は F 上の分離拡大である.

証明. (1) Tower property について, もし, 拡大列 $F \subseteq K \subseteq E$ において, E/F が分離拡大ならば, K/F が分離拡大であることは明らかである. E/K が分離拡大であることを示すために, $\alpha \in E$ の F 上の最小多項式を $f(X) \in F[X]$, K 上の最小多項式を $g(X) \in K[X]$ とおけば

$$g(X)|f(X)$$

なので, $f(X)$ が分離的ならば $g(X)$ も分離的である.

逆に, K/F, E/K がいずれも分離拡大ならば, $\alpha \in E$ の K 上の最小多項式を $g(X) \in K[X]$ とすると $g(X)$ の係数全体の集合を S とおくと $g(X)$ は分離的なので, $F(S,\alpha)/F(S)$ は分離拡大である. 同様に, $F(S)/F$ も分離拡大である命題 3.4.3 より $F(S,\alpha)/F(S)$, $F(S)/F$ はいずれも有限次拡大だから, 定理 3.11.6, 定理 3.11.9, 定理 3.1.16 により

$$[F(S,\alpha):F]_s = [F(S,\alpha):F(S)]_s[F(S):F]_s = [F(S,\alpha):F(S)][F(S):F] = [F(S,\alpha):F]$$

となり, α は F 上分離的である.

Lifting property については, E/F が分離拡大で K/F が拡大のとき, $\alpha \in E$ は F 上分離的なので, K 上も分離的である. よって, 定理 3.11.10 により $EK = K(E)$ は K 上分離的である.

(2) E_λ/F が分離拡大のとき, $\bigvee_\lambda E_\lambda$ は $\bigcup_\lambda E_\lambda$ で生成されるので, 定理 3.11.10 1) より分離拡大である.
(3) 最後に $\mathrm{nc}(E/F)$ は E の元の F 上の最小多項式全体の最小分解体である. これらは, 分離的多項式なので, $\mathrm{nc}(E/F)$ は F 上分離的な元全体から生成され, 定理 3.11.10 1) より分離拡大である.

□

3.13 完全体

定義 3.13.1. 体 F 上の任意の既約多項式が分離的であるとき, F を**完全体 (perfect)** という.

命題 3.13.2. F が完全体 $\Leftrightarrow$ F の任意の代数拡大は分離的.

証明. ($\Rightarrow$) 任意の F の代数拡大 $\alpha \in E$ はの元は F 上代数的で, その最小多項式 $f(X) \in F[X]$ は既約多項式なので仮定より分離的である. よって, 定理 3.11.10 より, E/F は分離拡大である.

($\Leftarrow$) $f(X) \in F[X]$ が既約多項式ならば, $f(X)$ の根を α とすると $F(\alpha)/F$ は代数拡大なので仮定より分離拡大である. よって, $f(X)$ は分離的である. □

定理 3.13.3. 標数 0 の体は完全体である. また, 任意の有限体は完全体である.

証明. それぞれ, 系 3.10.4 と系 3.10.6 から明らかである. □

定理 3.13.4. F の標数が $\mathrm{ch}(F) = p \neq 0$ のとき, 次は同値である.

(1) F は完全体である.
(2) ある $k \geq 1$ に対して $F = F^{p^k}$ となる.
(3) ある $k \geq 1$ に対して, フロベニウス写像 (Frobenius map) $\sigma_{p^k} : x \mapsto x^{p^k}$ は F の自己同型である.

もし, 2) かまたは 3) が成り立てば, それは任意の自然数 $k \geq 1$ に対して成り立つ.

証明. 1) ⇒ 2)　F が完全体のとき, 任意の $^\forall\alpha \in F$ に対して, $f(X) = X^p - \alpha \in F[X]$ とおく. $\{f(X)\}$ の最小分解体 E を考え, $\beta \in E$ が $f(X)$ の根であるとすると, $\beta^p = \alpha$ なので $f(X) = X^p - \beta^p = (X-\beta)^p$ である. β の F 上の最小多項式 $g(X)$ は $g(X)|f(X)$ で, $g(X)$ は分離的であるから $g(X) = X - \beta$ でなければならない. すなわち, $\beta \in F$ ということになる. したがって, 任意の $^\forall\alpha \in F$ に対して $^\exists\beta \in F$ が存在して, $\beta^p = \alpha$ となることが示された. すなわち $F \subseteq F^p$ であることが示された. $F^p \subseteq F$ は明らかなので $F = F^p$ である.

2) ⇒ 3)　$F = F^{p^k}$ ならば $\sigma_{p^k} : x \mapsto x^{p^k}$ は全射である. 体から体への準同型写像は常に単射なので同型である.

3) ⇒ 1)　$\sigma_{p^k} : x \mapsto x^{p^k}$ ならば $F = F^{p^k}$ なので, 補題 3.11.1 (2) により, 任意の自然数 m に対して $F = F^{p^m}$ である. もし, 既約多項式 $f(X) \in F[X]$ が非分離的であると仮定すると, 系 3.10.5 より $f(X) = g(X^{q^d})$ となる定数でない分離的多項式 $g(X)$ が存在する. $g(X) = \sum_i a_i X^i$ とすると $^\exists b_i \in F$ が存在して $b_i^{p^d} = a_i$ とできるので,

$$f(X) = \sum_i b_i^{p^d} (X^{q^d})^i = \left(\sum_i b_i X^i \right)^{p^d}$$

となるので $f(X)$ が既約であることに矛盾する. □

命題 3.13.5.　1) F が完全体で E/F が代数拡大ならば E は完全体である.

2) E が完全体で E/F が有限次拡大ならば F は完全体である.

証明. 1) は命題 3.13.2 と定理 3.4.13 による.

2) を証明するために $\mathrm{ch}(F) = p \neq 0$ としよう. E が F の単純拡大のときをまず示す. $E = F(\alpha)$ が完全体とすると, 命題 3.4.2 より α は F 上代数的である. $F(\alpha)$ が完全体なので定理 3.13.4, 補題 3.11.1 により $F(\alpha) = (F(\alpha))^p = F^p(\alpha^p)$ である.[5] α の最小多項式を $f(X) = \sum_i a_i X^i \in F[X]$ とすると

$$0 = \left(\sum_i a_i \alpha^i \right)^p = \sum_i a_i^p \alpha^{pi}$$

なので $[F^p(\alpha^p) : F^p] \leq [F(\alpha) : F]$ である. 拡大列

$$F^p \subseteq F \subseteq F(\alpha) = F^p(\alpha^p)$$

を考えると, 定理 3.1.16 より

$$[F^p(\alpha^p) : F^p] = [F(\alpha) : F][F : F^p]$$

なので $[F : F^p] = 1$, すなわち $F = F^p$ でなければならない. E/F が有限次拡大のときは, 命題 3.4.3 より, E は F 上有限生成だから, この議論を繰り返すことにより $E^p = E$ が証明できる. 定理 3.13.4 により, E は完全体である. □

3.14　純粋非分離拡大

定義 3.14.1. 体 F 上の代数的元 α が**純粋非分離的 (purely inseparable)** であるとは, α の F の最小多項式が根が α 1 つのみであることである. E/F が代数拡大のとき, E の任意の元が F 上純粋非分離的ならば, E/F は**純粋非分離拡大 (purely inseparable extension)** という.

もし, $\alpha \notin F$ が F 上純粋非分離であるとき, α の F 上の最小多項式を $f(X) = (X-\alpha)^n$ (を展開したもの) とする. X^{n-1} の係数は $-n\alpha$ なので, n は $p = \mathrm{ch}(F)$ で割り切れる. ($-n \neq 0$ ならば $-n\alpha \in F$ なので $\alpha \in F$ となり矛盾) n が p で最大 k 回割れるとすると

$$f(X) = (X-\alpha)^{mp^k}$$

---

[5] $F(\alpha)$ の元は F-係数の α の多項式 $\sum_i a_i \alpha^i$ の形をしているので, 標数 p を使うと $(F(\alpha))^p \ni \left(\sum_i a_i \alpha^i \right)^p = \sum_i a_i^p \alpha^{pi} \in F^p(\alpha^p)$ となり, F^p-係数の α^p の多項式であるので $F^p(\alpha^p)$ の元である.

(m と p は互いに素) という形である. 系 3.10.5 より, 分離的多項式 $g(X)$ が存在して $f(X) = g(X^{p^d})$ となる. $f(X)$ の次数は mp^k なので, $g(X)$ の次数を r とすると $rp^d = mp^k$ より $k \geq d$ で $r = mp^{k-d}$ でなければならない. $f(X)$ の根は α のみであるから

$$f(X) = (X-\alpha)^{mp^k} = \{(X-\alpha)^{p^d}\}^{mp^{k-d}} = (X^{p^d} - \alpha^{p^d})^{mp^{k-d}}$$

と書き直すと $g(X) = (X - \alpha^{p^d})^{mp^{k-d}}$ であり, $g(X)$ が分離的であることより, $m = 1$, $k - d = 0$ であることがわかる. したがって, α の最小多項式は

$$f(X) = (X-\alpha)^{p^d} = X^{p^d} - \alpha^{p^d}$$

の形で, d は α の非分離次数である.

例 3.14.2. $\mathrm{ch}(F) = 2$ で t が F 上超越的であるとき, t は $F(t^2)$ 上純粋非分離な元で, その最小多項式は $X^2 - t^2$ である.

例 3.14.3. 次に, 分離的でも, 純粋非分離的でもない例を挙げる. $\mathrm{ch}(F) = p \neq 0$ で, $\alpha \in F$ は 0 でない元とし, t が F 上超越的であるとする. このとき,

$$s = \frac{t^{p^2}}{t^p + \alpha}$$

とおくと, $F(s) \subseteq F(t)$ は代数拡大で, 拡大次数は p^2 である. t は monic な多項式

$$f(X) = X^{p^2} - sX^p - s\alpha$$

をみたす. 定理 3.3.14 1) より, 拡大次数が p^2 なので, 最小多項式でなければならない. $f(X) = g(X^p)$ なので, $f(X)$ は分離的ではない. さらに, もし, t が $F(s)$ 上純粋非分離的であると仮定して矛盾を導く. そのときは

$$f(X) = X^{p^2} - sX^p - s\alpha = (X-t)^{p^2} = X^{p^2} - t^{p^2}$$

とならなければならず, $s = 0$ となり, 矛盾である. したがって t は $F(s)$ 上, 分離的でも純粋非分離的でもない. □

定義 3.14.4. E/F が有限次拡大のとき, 定理 3.11.9 より, $[E:F]_s | [E:F]$ だから

$$[E:F] = [E:F]_s [E:F]_i$$

と書くことができる. $[E:F]_i$ を E の F 上の**非分離次数 (inseparable degree)** という.

分離次数は無限次元拡大に対しても定義されたが, 非分離次数のこの定義は有限次拡大に対してのみである.

定理 3.14.5. $F \subseteq E$ が有限次拡大で $\mathrm{ch}(F) = p \neq 0$ とする.

1) $F \subseteq K \subseteq E$ のとき $[E:F]_i = [E:K]_i [K:F]_i$ である.
2) E/F が分離拡大である必要十分条件は $[E:F]_i = 1$ である.
3) $\alpha \in E$ の非分離指数を d とすると $[F(\alpha):F]_i = p^d$ である.
4) $\alpha \in E$ が純粋非分離元であるための必要十分条件は $[F(\alpha):F]_s = 1$, すなわち $[F(\alpha):F]_i = [F(\alpha):F]$ である.
5) $[F(\alpha):F]_i$ は p の冪である.

証明. 1) 定理 3.1.16 定理 3.11.6, 定義 3.14.4 より明らか.
2) 定理 3.11.9
3) 定理 3.11.5 (2)
4) $\alpha \in E$ が純粋非分離元であるための必要十分条件は α の F 上の最小多項式 $f(X)$ の根がただ 1 つであることであり. これは $|\hom_F(F(\alpha), \overline{F})| = 1$ であることと同値である.
5) 定理 3.11.9
□

定理 3.14.6. $\mathrm{ch}(F) = p \neq 0$ で, α が F 上代数的な元, α の非分離指数を d, 最小多項式を $f(X)$ とする. このとき, 次の 3 条件は同値である.

1) $\alpha \in E$ が純粋非分離元である.

2) $F(\alpha)/F$ が純粋非分離拡大である.

3) ある $k \geq 0$ が存在して $\alpha^{p^k} \in F$ である.

さらに, このとき, d は $\alpha^{p^k} \in F$ とない る最小の非負整数である.

証明. 1) が成り立つとすると, 任意の $\beta \in F(\alpha)$ に対して, 拡大列 $F \subseteq F(\beta) \subseteq F(\alpha)$ において, 定理 3.14.5 4) より $[F(\alpha) : F]_i = [F(\alpha) : F]$ が成り立つ. このとき, 定理 3.1.16, 定理 3.14.5 1) より $[F(\beta) : F]_i = [F(\beta) : F]$ でなければならない. よって, 定理 3.14.5 4) より β は純粋非分離である. 逆に 2) から 1) は trivial である.

1) が成り立つとき, 仮定より $f(X) = X^{p^d} - \alpha^{p^d}$ なので, $\alpha^{p^d} \in F$ でなければならない. 逆に, 3) が成り立てば, $g(X) = X^{p^d} - \alpha^{p^d}$ とおくと, $g(\alpha) = 0$ なので

$$f(X) | g(X)$$

であり, $f(X)$ の根は α だけなので, $f(X)$ は純粋非分離的である. □

定理 3.14.6 3) より $F(\alpha^{p^d}) = F$ である. これは, α が 分離的のとき, 任意の自然数 k に対して $F(\alpha^{p^k}) = F(\alpha)$ であることと対照的である. (補題 3.11.1, 定理 3.11.8 (4) 参照)

定理 3.14.7. E/F が代数拡大のとき, 次の 3 条件は同値である.

1) E は純粋非分離元で生成される. (このとき, E は F 上**純粋非分離生成 (purely inseparably generated)** という.)

2) $[E : F]_s = 1$ (このとき, E は F 上**次数純粋非分離 (degreewise purely inseparable)** という.)

3) E/F は純粋非分離拡大である.

証明. 1) $\Rightarrow$ 2)　$E = F(I)$, I は F 上純粋非分離的元の集合であるとする. L を代数的閉体として, 埋込み $\sigma : K \to L$ は I の元上の値で完全に決まる. しかし, $\alpha \in I$ に対して, その最小多項式を $f(X)$ とすると, α^σ は $f(X)$ の根でなければならない. $f(X)$ の根は α のみであるから $\alpha^\sigma = \alpha$ となり σ は恒等写像でなければならない. よって $[E : F]_s = 1$ である.

2) $\Rightarrow$ 3)　任意の $\alpha \in E$ に対して, α を α の最小多項式として, β を $\overline{F}$ における $f(X)$ の根とすると, 定理 3.6.12 より恒等写像 $\iota : F \to \overline{F}$ は $\alpha^\sigma = \beta$ となる $\sigma : E \to \overline{F}$ に延長される. ところが $[E : F]_s = 1$ より σ は E 上の恒等写像となり, $\beta = \alpha$ で $f(X)$ は 1 つの根しかもたないので, α は F 上純粋非分離的である. 3) $\Rightarrow$ 1)　は自明である. □

定理 3.14.8. 純粋非分離拡大は distinguished class である. さらに, 純粋非分離拡大体の任意の合成体も純粋非分離拡大体である.

証明. $F \subseteq K \subseteq E$ を拡大列とする. 定理 3.14.7 より, 純粋非分離性は次数で決まるので, $[E : F]_s = 1$ である必要十分条件は $[E : K]_s = 1$ かつ $[K : F]_s = 1$ が成り立つことであるから, tower property は明らかである. 次に Lifting property を証明する. E/F が純粋非分離拡大で K/F が拡大とする. このとき, E の元はすべて F 上純粋非分離的であるので, K 上も純粋非分離的である. $EK = K(E)$ は K 上 E の元で生成されるので, 定理 3.14.7 3) より EK/K は純粋非分離拡大である. 任意の合成体に関しても同様である. E_λ/F が純粋非分離拡大ならば E_λ の元はすべて F 上純粋非分離的であり, $\bigvee E_\lambda$ は F 上 $\bigcup E_\lambda$ で生成されるので, 定理 3.14.7 3) より F 上純粋非分離拡大である. □

3.15　有限体

定理 3.15.1. 有限体 $\mathbb{F}_q$ 上の n 次の monic な既約多項式の個数は

$$\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

で与えられる.

この式を使って既約多項式の個数の最初の方を計算すると次の表のようになる. 例えば, $\mathbb{F}_2$ 上の 2 次の既約多項式は

$$X^2 + X + 1$$

3 次の既約多項式は

$$X^3 + X + 1, \qquad X^3 + X^2 + 1$$

表 3.15.1: $\mathbb{F}_q$ 上の既約多項式の個数

n	2	3	4	5	6	7	8	9	10
$q=2$	1	2	3	6	9	18	30	56	99
$q=3$	3	8	18	48	116	312	810	2184	5880
$q=4$	6	20	60	204	670	2340	8160	29120	104754
$q=5$	10	40	150	624	2580	11160	48750	217000	976248

4 次の既約多項式は

$$X^4+X+1, \qquad X^4+X^3+1, \qquad X^4+X^3+X^2+X+1$$

5 次の既約多項式は

$$X^5+X^2+1, \qquad X^5+X^3+X^2+X+1, \qquad X^5+X^4+X^3+X^2+1$$
$$X^5+X^3+1, \qquad X^5+X^4+X^2+X+1, \qquad X^5+X^4+X^3+X+1$$

6 次の既約多項式は

$$X^6+X+1, \qquad X^6+X^3+1, \qquad X^6+X^5+1$$
$$X^6+X^4+X^2+X+1, \qquad X^6+X^5+X^2+X+1, \qquad X^6+X^4+X^3+X+1$$
$$X^6+X^5+X^4+X+1, \qquad X^6+X^5+X^3+X^2+1, \qquad X^6+X^5+X^4+X^2+1$$

である. また, $\mathbb{F}_3$ 上の 2 次の既約多項式は

$$X^2+1, \qquad X^2+X-1, \qquad X^2-X-1$$

3 次の既約多項式は

$$X^3-X+1, \qquad X^3-X-1, \qquad X^3+X^2-1, \qquad X^3+X^2+X-1,$$
$$X^3+X^2-X+1, \qquad X^3-X^2+1, \qquad X^3-X^2+X+1, \qquad X^3-X^2-X-1$$

4 次の既約多項式は

$$X^4+X-1, \qquad X^4-X-1, \qquad X^4+X^2-1, \qquad X^4-X^2-1, \qquad X^4+X^3-1, \qquad X^4-X^3-1,$$
$$X^4+X^2+X+1, \qquad X^4+X^2-X+1, \qquad X^4+X^3-X+1,$$
$$X^4-X^3+X+1, \qquad X^4+X^3+X^2+1, \qquad X^4-X^3+X^2+1,$$
$$X^4+X^3+X^2+X+1, \qquad X^4+X^3+X^2-X-1, \qquad X^4+X^3-X^2-X-1,$$
$$X^4-X^3+X^2+X-1, \qquad X^4-X^3-X^2+X-1, \qquad X^4-X^3+X^2-X+1$$

である.

第4章　ガロア理論

4.1　ガロアの短い生涯の簡単な紹介

エヴァリストガロアの生涯は, 控えめに言っても, 非常に短く, かつ非常に輝かしいものでした。もちろん, それは今日, 彼の天才的な発見, しかもそれは彼の人生のわずか数年の短い期間に行われたという伝説のためだけではありません.

ガロアは, 1811 年 10 月 25 日にパリの近くに生まれました。あきらかに, ガロアは, 幼い頃からたいへん頭の良い生徒として認識されていましたが, 多少, 変わった性癖と反抗的な傾向をもっていたようです. 1828 年, 17 歳のとき, ガロアは名門エコール・ポリテクニークの入学試験を受験しましたが, 試験に合格しなかったので, 彼は Louis-le-Grand 王立学校で学び続け, そこで高等数学を学ぶことになりました. 彼の数学教師は彼の天才的な面を発見し, 彼に最初の論文を執筆・発表するよう促しました. その最初の論文は 1829 年 4 月 1 日に出版されます.

この頃からガロアにとって不幸な悪い事が続くようになりました。ガロアが王立科学アカデミーに送った論文の 1 つがコーシーに回されますが, コーシーはそれを紛失してしまいます. （どうやら, コーシーは論文をよく紛失したようです. 彼は, あのアーベルによる論文も紛失したことがあります.）1829 年 4 月 2 日には, ガロアの父が自殺を試みます. その年, ガロアは再びエコール・ポリテクニークを入るべく受験しましたが, このような混乱した状況下で再び失敗してしまいました. そこで彼は, エコール・ポリテクニークよりもはるかに低いレベルであると考えられていたエコール・ノルマルに入学しました. エコール・ノルマルに在学中に, ガロアは彼の研究成果をまとめた論文を書き, 科学アカデミーの数学大賞 (the Grand Prize in Mathematics of the Academy of Sciences) に応募しました. 彼の論文は検討のためにフーリエの手に渡りましたが, それを家に持って帰ったフーリエがその直後に死亡したため, その論文は永久に失われたようです. ガロアは非常に強力で反政府的な政治的意見を持っていました. 1831 年 7 月 14 日に, 彼は政治的なデモ中に逮捕され, 禁固 6 ヶ月を宣告されます. 1832 年 5 月には, ガロアは, 若い女性との短い恋愛関係がありました. 彼は 5 月 14 日に恋愛関係に終止符を打ち, これが後のガロアが命を落とす決闘の原因であったと考えられています. ガロアは 1832 年 5 月 31 日に決闘に敗れて死亡しました.

リウヴィルは 1843 年 9 月 4 日に王立科学アカデミーにおいて, 1831 年のガロアのメモアールの論文の中の定理で, ガロアが素数次数の代数方程式の冪根による可解性について言及し, それが正しく, かつ非常に深い結果だと述べました. しかし, ガロアのその論文が掲載されたのは 1846 年になってのことでした. 1850 年代になって, やっとガロアのすべての仕事が出版され, あまたの数学者の知るところとなりました. そして, それは, ベッチ, クロネッカー, デデキント, ケーリー, エルミート, ジョルダン等々の名立たる数学者達による, この分野のその後の大きな発展の契機になりました. 過去の歴史はこれくらいにして, 現代の視点からガロア理論について学ぶことにしましょう.[1]

[1]Evariste Galois life was, to say the least, very short and very controversial. Of course, it would not be the subject of such legend today were it not for his remarkable discoveries, which spanned only a few short years.

Galois was born on October 25, 1811, near Paris. Apparently, Galois was recognized at an early age as a brilliant student with some bizarre and rebellious tendencies. In 1828, at the age of 17, Galois attempted to enter the prestigious Ecole Polytechnique, but failed the entrance exams, so he remained at the royal school of Louis-le-Grand, where he studied advanced mathematics. His teacher urged Galois to publish his first paper, which appeared on April I, 1829.

After this, things started to go very badly for Galois. All article that Galois sent to the Academy of Sciences was given to Cauchy, who lost it. (Apparently, Cauchy had a tendency to lose papers; he had already lost a paper by Abel.) On April 2, 1829, Galois' father committed suicide. Galois once again tried to enter the Ecole Polytechnique, but again failed under some rather controversial circumstances. So he entered the Ecole Normale, considered to be on a much lower level than the Ecole Polytechnique. While at the Ecole Normale, Galois wrote up his research and entered it for the Grand Prize in Mathematics of the Academy of Sciences. The work was given to Fourier for consideration, who took it home, but promptly died, and the manuscript appears now to be lost. Galois possessed very strong political opinions. On July 14, 1831, he was arrested during a political demonstration, and condemned to six months in prison. In May 1832, Galois had a brief love affair with a young woman. He broke off the affair on May 14, and this appears to be the cause of a subsequent duel that proved fatal to Galois. Galois died on May 31,1832. On September 4,1843, Liouville announced to the Academy of Sciences that he had discovered, in the papers of Galois, the theorem, from his 1831 Memoir, that we mentioned earlier concerning the solvability by radicals of a prime degree equation, and referred to it with the words "as precise as it is deep." However, he waited until 1846 to publish Galois' work.

In the 1850s, the complete texts of Galois' work became available to mathematicians, and it initiated a great deal of subsequent work by the likes of Betti, Kronecker, Dedekind, Cayley, Hemiite, Jordan and others. Now it is time that we left the past, and pursued Galois' theory from a modern perspective.

4.2 ガロア系

定義 4.2.1. P と Q を半順序集合とする. 写像 $\pi : P \to Q$ と $\omega : Q \to P$ の組 (π, ω) で, 次の 2 条件を満たすものを**ガロア系 (Galois connection)** という.

1) (順序逆準同型 (order-reversing または antitone)) $p, q \in P$, $r, s \in Q$ のとき

$$p \leq q \Rightarrow p^\pi \geq q^\pi \text{ かつ } r \leq s \Rightarrow r^\omega \geq s^\omega$$

2) (拡大的 extensive) $p \in P$, $r \in Q$ のとき

$$p \leq p^{\pi\omega} \text{ かつ } r \leq r^{\omega\pi}$$

定義 4.2.2. P を半順序集合とする. 写像 $\mathrm{cl} : P \to P$ が, 次の 3 条件を満たすとき**閉包作用 (closure operation)** という. 以下, $p, q \in P$ とする.

1) (拡大的 extensive) $p \leq \mathrm{cl}(p)$
2) (idempotemt) $\mathrm{cl}(\mathrm{cl}(p)) = \mathrm{cl}(p)$
3) (Isotone) $p \leq q \Longrightarrow \mathrm{cl}(p) \leq \mathrm{cl}(q)$

$p \in P$ が $\mathrm{cl}(p) = p$ を満たすとき p は**閉じている (closed)** といい, P の中の閉じている元全体を $\mathrm{Cl}(P)$ と書く.

命題 4.2.3. (π, ω) が (P, Q) 上のガロア系であるとする. このとき

$$p \to p^{\pi\omega} \qquad q \to q^{\omega\pi}$$

は, それぞれ P, Q 上の閉包作用であり, $p^{\pi\omega} = \mathrm{cl}(p)$, $q^{\omega\pi} = \mathrm{cl}(q)$ と書くことにする. さらに

1) $p^{\pi\omega\pi} = p^\pi$, すなわち $\mathrm{cl}(p^\pi) = \mathrm{cl}(p)^\pi = p^\pi$
2) $q^{\omega\pi\omega} = q^\omega$, すなわち $\mathrm{cl}(q^\omega) = \mathrm{cl}(q)^\omega = q^\omega$

が成り立つ.

証明. $p \leq p^{\pi\omega}$ の両辺に π を作用させると

$$p^\pi \geq (p^{\pi\omega})^\pi = p^{\pi\omega\pi} = (p^\pi)^{\omega\pi} \geq p^\pi$$

なので, $p^\pi = p^{\pi\omega\pi}$ である. 同様に, $q^\omega = q^{\omega\pi\omega}$ も示せる, あとは明らか. □

命題 4.2.4. 写像 $\pi : P \to \mathrm{Cl}(Q)$ と $\omega : Q \to \mathrm{Cl}(P)$ は全射であり, その制限 $\pi : \mathrm{Cl}(P) \to \mathrm{Cl}(Q)$ と $\omega : \mathrm{Cl}(Q) \to \mathrm{Cl}(P)$ は順序逆同型 (order-reversing bijection) である.

証明. 明らか. □

命題 4.2.5. P, Q が束で, (π, ω) が (P, Q) 上のガロア系であるとする.

1) P が完全束ならば $\mathrm{Cl}(P)$ も完全束である. Q についても同様.
2) P, Q に**ドモルガンの法則 (De Morgan's, Law)** が成り立つ. すなわち $p, q \in P$, $r, s \in Q$ に対して

$$(p \wedge q)^\pi = p^\pi \vee q^\pi \qquad (p \vee q)^\pi = p^\pi \wedge q^\pi$$

かつ

$$(r \wedge s)^\omega = r^\omega \vee s^\omega \qquad (r \vee s)^\omega = r^\omega \wedge s^\omega$$

が成り立つ.

証明. 1) は

$$\bigwedge_\lambda p_\lambda = \max\{x \in P \mid x \leq p_\lambda \text{ for } {}^\forall\lambda\}, \quad \bigvee_\lambda p_\lambda = \min\{x \in P \mid x \geq p_\lambda \text{ for } {}^\forall\lambda\}$$

を使う. 2) は

$$p \wedge q = \max\{x \in P \mid x \leq p \text{ かつ } x \leq q\}, \quad p \vee q = \min\{x \in P \mid x \geq p \text{ かつ } x \geq q\}$$

を使う. 形式的なので自分で. □

cl が拡大的であることから, P の最大元 1_P は閉じていることがわかる. (もし, 最大元が存在すればの話で, 完全束のときは必ず存在するが一般の半順序集合では存在するとは限らない.) なぜなら $1_P \leq \mathrm{cl}(1_P) \leq 1_P$ だから $\mathrm{cl}(1_P) = 1_P$ である.

さらに, もし 0_Q が存在すれば $1_P = 0_Q^\omega$ である. なぜなら, $1_P = \mathrm{cl}(1_P) = 1_P^{\pi\omega}$ であるが $1_P^\pi \geq 0_Q$ なので $1_P^{\pi\omega} \leq 0_Q^\omega \leq 1_P$ だから $1_P^{\pi\omega} = 1_P$ より $1_P = 0_Q^\omega$ である.

一方, 最小元が存在しても, それは閉じているとは限らない. 例えば, もし 1_P が存在するならば Q の closed な元で最小なものは 1_P^π である.[2] よって Q の最小元が closed であることと $0_Q = 1_P^\pi$ は同値である.

問題 4.2.6. X と Y を空でない集合とし, $P = \mathscr{P}(X)$ と $Q = \mathscr{P}(Y)$ を P と Q の部分集合全体の集合とする. $R \subseteq X \times Y$ を X と Y の間の関係とする.[3] このとき

$$S \in \mathscr{P}(X) \mapsto S^\pi = \{y \in Y \mid (x,y) \in R \text{ for } {}^\forall x \in S\} \in \mathscr{P}(Y)$$

かつ

$$T \in \mathscr{P}(Y) \mapsto T^\omega = \{x \in X \mid (x,y) \in R \text{ for } {}^\forall y \in T\} \in \mathscr{P}(X)$$

と定義すると (π, ω) は $(\mathscr{P}(X), \mathscr{P}(Y))$ 上のガロア系であることを示せ.

定義 4.2.7. (P,Q) 上のガロア系 (π,ω) が**次数付けられている (indexed)** とは

a) $p \leq q$ である $p,q \in P$ に対して, q の p 上の**次数 (degeee または index)** と呼ばれる $(q:p)_P \in \mathbb{Z}_{>0} \cup \infty$ が決まる
b) $r \leq s$ である $r,s \in Q$ に対して, s の r 上の**次数 (degeee または index)** と呼ばれる $(s:r)_Q \in \mathbb{Z}_{>0} \cup \infty$ が決まる

そして, 次の 3 条件をみたすことである. これ以降, 同じことの繰り返しをやめるために P,Q を省略して $(q:p)$ のように書くことにする.

1) (Degree is multiplicative) $s_1, s_2, s_3 \in P$ または $s_1, s_2, s_3 \in Q$ のとき

$$s_1 \leq s_2 \leq s_3 \Longrightarrow (s_3 : s_1) = (s_3 : s_2)(s_2 : s_1)$$

2) (π and ω are degree-non-increasing) $p,q \in P$ のとき

$$p \leq q \Longrightarrow (p^\pi : q^\pi) \leq (q:p)$$

また $r,s \in P$ のとき

$$r \leq s \Longrightarrow (r^\omega : s^\omega) \leq (s:r)$$

3) (Equality by degree) $s,t \in P$ または $s,t \in Q$ で $s \geq t$ のとき

$$(s:t) = 1 \Longleftrightarrow s = t$$

$(s:t) < \infty$ のとき s は t の**有限次拡大 (finite extension)** であるという. P に最大元と最小元が存在するとき, $\mathrm{index}(P) = (1_P : 0_P)$ を P の**次数 (index)** という. Q についても同様である.

以後, $(q:p)$ と書くときは, 暗黙に $p \leq q$ であると仮定する.

命題 4.2.8. (π,ω) が (P,Q) 上の次数付きガロア系であるとする. このとき, 次が成り立つ.

1) (Degree-preserving on closed elements) $p,q \in \mathrm{Cl}(P)$ かつ $p \leq q$ ならば $(q:p) = (p^\pi : q^\pi)$ である. Q についても同様.
2) (Finite extensions of closed elements are closed) $p \in \mathrm{Cl}(P)$ かつ $(q:p) < \infty$ ならば $q \in \mathrm{Cl}(P)$ である. 特に, 0_P が閉じていて $(1_P : 0_P)$ が有限ならば P の任意の元は閉じている. Q についても同様.

証明. 1) は

$$(q:p) \geq (p^\pi : q^\pi) \geq (q^{\pi\omega} : p^{\pi\omega}) = (\mathrm{cl}(q) : \mathrm{cl}(p)) = (q:p)$$

より等号が成り立つ. 2) は $p \in \mathrm{Cl}(P)$ かつ $(q:p) < \infty$ ならば

$$(q:p) \geq (p^\pi : q^\pi) \geq (q^{\pi\omega} : p^{\pi\omega}) = (\mathrm{cl}(q) : p) = (\mathrm{cl}(q) : q)(q:p)$$

より $(\mathrm{cl}(q) : q) = 1$ なので q は閉じている. □

[2] $1_P^{\pi\omega\pi} = 1_P^\pi$ より 1_P^π は閉じている. $q \in Q$ が閉じていたら $q^\omega \leq 1_P$ だから $q = q^{\omega\pi} \geq 1_P^\pi$ である.
[3] 集合 A と集合 B の直積 $A \times B$ の部分集合 R を**関係**と呼ぶ.

命題 4.2.9. (π,ω) が (P,Q) 上の次数付きガロア系であるとする. $p,q\in P$ のとき, もし

1) $(q:\mathrm{cl}(p))<\infty$ かつ $(q:p)=(p^\pi:q^\pi)$
2) $\mathrm{cl}(p)\leq q$ かつ $(q:p)=(p^\pi:q^\pi)<\infty$

のいずれかが成り立てば p は閉じている. 特に, この命題で $q=1_P$ とおくと, もし

$$(1_P:p)=(p^\pi:0_Q)<\infty$$

ならば p は閉じている.

証明. もし 1) が成り立つならば条件 $(q:\mathrm{cl}(p))<\infty$ から, 命題 4.2.8 2) より q は closed で, 命題 4.2.3 1) により $\mathrm{cl}(p)^\pi=p^\pi$ なので, 命題 4.2.8 1) より

$$\infty>(q:\mathrm{cl}(p))=(p^\pi:q^\pi)$$

が成り立つ. また, $(q:p)=(p^\pi:q^\pi)$ より

$$(p^\pi:q^\pi)=(q:p)=(q:\mathrm{cl}(p))(\mathrm{cl}(p):p)=(p^\pi:q^\pi)(\mathrm{cl}(p):p)$$

となり, $(\mathrm{cl}(p):p)=1$ なので $p=\mathrm{cl}(p)$ である. すなわち p は closed. また, もし 2) が成り立つならば $(q:\mathrm{cl}(p))\leq(q:p)<\infty$ なので 1) に帰着する. □

次の定義は余り標準的ではないが, ここでは採用する.

定義 4.2.10. (P,Q) 上のガロア系 (π,ω) について, P のすべての元が閉じているとき, P は完全に閉じているという. Q についても同様である. P と Q が両方とも完全に閉じているとき, (P,Q) は完全に閉じているという.

1_P, 1_Q が存在すれば, それは公理から closed である. 0_P, 0_Q に関してはそうとは限らないことは既に述べた. しかし, 我々が学ぶ体の拡大とガロア群のガロア系 (ガロア対応) に関しては 0_Q が常に closed になるので, ここでは, その場合の性質を述べる.

命題 4.2.11. (0_Q is closed) (π,ω) が (P,Q) 上の次数付きガロア系であるとする. P, Q に最大元と最小元が存在すると仮定する. 0_Q が閉じているならば

$$\mathrm{index}(Q)\leq\mathrm{index}(P)$$

である. さらに

1) $\mathrm{index}(Q)<\infty$ または $\mathrm{index}(P)<\infty$ ならば Q は完全に閉じている.
2) $\mathrm{index}(P)<\infty$ かつ 0_P が閉じていれば, (P,Q) は完全に閉じている.

証明. ここで

$$\mathrm{index}(P)=(1_P:0_P)\geq(0_P^\pi:1_P^\pi)=(1_Q:1_P^\pi)=(1_Q:0_Q)=\mathrm{index}(Q)$$

よって P または Q が有限次数ならば $\mathrm{index}(Q)$ は有限なので, 命題 4.2.8 により Q は完全に閉じている. 2) は, 命題 4.2.8 の直接の帰結である. □

4.3 ガロア対応 (Galois Correspondence)

定義 4.3.1. E/F が体の拡大のとき, E の F 上の自己同型群 $\mathrm{Aut}_F(E)$ を $\mathrm{G}_F(E)$ と書き, E の F 上の**ガロア群 (Galois group of E over F)** という.

E/F が代数拡大ならば

$$\mathrm{G}_F(E)=\mathrm{Aut}_F(E)=\hom_F(E,E)$$

であり, E/F が正規拡大のときは

$$\mathrm{G}_F(E)=\hom_F(E,\overline{E})$$

である.

E/F が体の拡大のとき, F と E の中間体 (intermediate field) 全体の成す完全束を $\mathscr{F}$ と書く. また, $\mathrm{G}_F(E)$ の部分群全体の成す完全束を $\mathscr{G}$ と書く.[4] 写像 $\Pi : \mathscr{F} \to \mathscr{G}$ と $\Omega : \mathscr{G} \to \mathscr{F}$ を $K \in \mathscr{F}$ に対して

$$\Pi(K) = \mathrm{G}_K(E)$$

$H \in \mathscr{G}$ に対して

$$\Omega(H) = \mathrm{fix}(H) = \{\alpha \in E \,|\, \alpha^\sigma = \alpha \text{ for } {}^\forall\sigma \in H\}$$

によって定義する. $\mathrm{fix}(H)$ は H の**固定体 (fixed field)** という.

定理 4.3.2. E/F を体の拡大とする. 上で定義した写像の組

$$(\Pi : K \mapsto \mathrm{G}_K(E), \Omega : H \mapsto \mathrm{fix}(H))$$

は ($\mathscr{F}$,$\mathscr{G}$) 上のガロア系 (Galois connection) である. これを, 拡大 E/F の**ガロア対応 (Galois correspondence)** という.

証明. 定義 4.2.1 の 1), 2) をチェックすればよいので, 1) は拡大列 $F \subseteq K \subseteq L \subseteq E$ と部分群 $J \subseteq H \subseteq \mathrm{G}_F(E)$ に対して

$$\mathrm{G}_K(E) \supseteq \mathrm{G}_L(E), \qquad \mathrm{fix}(J) \supseteq \mathrm{fix}(H)$$

を示せばよい. また, 2) は中間体 $F \subseteq K \subseteq E$ と部分群 $H \subseteq \mathrm{G}\,F(E)$ に対して

$$K \subseteq \mathrm{fix}(\mathrm{G}_K(E)), \qquad H \subseteq \mathrm{G}_{\mathrm{fix}(H)}(E)$$

を示せばよい. 詳細は, 自分で確認を. □

例 4.3.3. $F = \mathbb{Q}$, $E = \mathbb{Q}\left(\sqrt[4]{2}\right)$ のとき写像 $\sigma \in \hom_F(E,E)$ を $\sigma\left(\sqrt[4]{2}\right) = -\sqrt[4]{2}$ によって定義する. このとき, $\mathscr{F} = \left\{F \subseteq \mathbb{Q}(\sqrt{2}) \subseteq E\right\}$, $\mathscr{G} = \{\{\iota\} \subseteq \{\iota,\sigma\}\}$ である. また, $G = \mathrm{G}_F(E) = \{\iota,\sigma\}$ で, $\mathrm{fix}_E(G) = \mathbb{Q}(\sqrt{2})$ である. よって, $\mathrm{cl}(F) = \mathrm{fix}(\mathrm{G}_F(E)) = \mathbb{Q}(\sqrt{2})$ なので $F = \mathbb{Q}$ は閉じていない.

系 4.3.4. $\mathrm{Cl}(\mathscr{F})$ と $\mathrm{Cl}(\mathscr{G})$ は完全束である. ここで meet $\wedge$ は, どちらも集合の交わりである.

証明. $\mathscr{F}$ と $\mathscr{G}$ が完全束であることより, 命題 4.2.5 を使え. □

例 4.3.5. 上の例では $\mathrm{Cl}(\mathscr{F}) = \left\{\mathbb{Q}(\sqrt{2}), \mathbb{Q}\left(\sqrt[4]{2}\right)\right\}$, $\mathrm{Cl}(\mathscr{G}) = \{\{\iota\}, G\}$ であり, $\mathrm{G}_{\mathbb{Q}(\sqrt{2})}(E) = G$, $\mathrm{G}_E(E) = \{\iota\}$, $\mathrm{fix}(\{\iota\}) = E$, $\mathrm{fix}(G) = \mathbb{Q}(\sqrt{2})$ は順序逆同型を与える.

$\mathscr{F}$ には最大元があり, $\mathscr{G}$ には最小元があることに注意しよう.[5] ここで $\mathscr{F}$ の最大元は E で, $\mathscr{G}$ の最小元は恒等写像 ι のみからなる部分群 $\{\iota\}$ である. $\mathscr{F}$ の最小元 F が閉じているかどうかは重要な問題である.[6]

4.4 ガロア対応は次数付きである

E/F が体の拡大, K, L が中間体のとき, $(K : L) = [K : L]$ を拡大次数とする. また, G が群で H, J が部分群のとき, $(H : J)$ を指数とする. このとき, 次の定理 4.4.1, 定理 4.4.2 から, ガロア対応 (Π, Ω) は次数付きガロア系であることが示される.

定理 4.4.1. $F \subseteq K \subseteq L \subseteq E$ が拡大列のとき,

$$(\mathrm{G}_K(E) : \mathrm{G}_L(E)) \leq [L : K]_s \leq [L : K]$$

である.

証明. これを証明するために, まず単射 $\mathrm{G}_K(E)/\mathrm{G}_L(E) \to \hom_K(L,E)$ を構成する. 写像 $\varphi : \mathrm{G}_K(E) \to \hom_K(L,E)$ を $\sigma \in \mathrm{G}_K(E)$ に対して, その制限 $\sigma|_L \in \hom_K(L,E)$ を対応させることによって定義する. このとき,

[4] 群 G の部分群の族 $\{H_\lambda\}_{\lambda\in\Lambda}$ に対して, $\bigcup_{\lambda\in\Lambda} H_\lambda$ を含む G の部分群全体の交わりを $\bigvee_{\lambda\in\Lambda} H_\lambda$ と定義する. これは, すべての H_λ を含む最小の G の部分群である.

[5] $\{\iota\} = \mathrm{G}_E(E) = 1_P^\Pi$ は $\mathscr{G}$ の最小元である.

[6] F が閉じている $\Leftrightarrow \mathrm{fix}\,(\mathrm{G}_F(E)) = F$

$$\varphi(\sigma)=\varphi(\tau)\Leftrightarrow\sigma|_L=\tau|_L\Leftrightarrow\sigma^{-1}\tau\in\mathrm{G}_L(E)\Leftrightarrow\sigma\,\mathrm{G}_L(E)=\tau\,\mathrm{G}_L(E)$$

なので, 単射 $\overline{\varphi}:\mathrm{G}_K(E)/\mathrm{G}_L(E)\to\hom_K(L,E)$ が誘導される. したがって. 定義 3.11.3, 定理 3.11.9 より

$$(\mathrm{G}_K(E):\mathrm{G}_L(E))\le|\hom_K(L,E)|\le|\hom_K(L,\overline{E})|=[L:K]_s\le[L:K]$$

である.[7] ここで $\overline{E}$ は E の代数的閉包. □

定理 4.4.2. 拡大 $F\subseteq E$ と, $\mathrm{G}_F(E)$ の部分群 $J\subseteq H$ に対して,

$$[\mathrm{fix}(J):\mathrm{fix}(H)]\le(H:J)$$

である.

証明. $(H:J)=\infty$ のときは明らかであるので, $(H:J)<\infty$ と仮定して証明する. H/J の元を基底とする E 上のベクトル空間を $E_{H/J}$ とし, その双対空間を $E^{H/J}$ と書く. すなわち, $E^{H/J}$ は H/J から E への関数 $H/J\to E$ 全体の集合で, E 上のベクトル空間としての構造を自然に入れたものである. このとき,

$$\dim_E E^{H/J}=(H:J)$$

である. また, $\mathrm{fix}(J)$ は $\mathrm{fix}(H)$ 上のベクトル空間で, その次元が $\dim_{\mathrm{fix}(H)}\mathrm{fix}(J)=[\mathrm{fix}(J):\mathrm{fix}(H)]$ である. よって $\dim_{\mathrm{fix}(H)}\mathrm{fix}(J)\le\dim_E E^{H/J}$ を示したい.

$\alpha\in\mathrm{fix}(J)$ に対して $\widehat{\alpha}\in E^{H/J}$ を $\widehat{\alpha}\,(h\,\mathrm{fix}(J))=h\alpha$ によって定義すると, 写像 $\varphi:\mathrm{fix}(J)\to E^{H/J}$ は well-defined である. 実際, $\alpha\in\mathrm{fix}(J)$, $h_1,h_2\in H$ $h_1^{-1}h_2\in J$ ならば, $h_1^{-1}h_2(\alpha)=\alpha$ より $h_1(\alpha)=h_2(\alpha)$ だから $\widehat{\alpha}\,(h\,\mathrm{fix}(J))$ は coset の代表元の取り方によらない.

このとき, $\alpha_1,\dots,\alpha_n\in\mathrm{fix}(J)$ が $\mathrm{fix}(H)$ 上線形独立ならば $\widehat{\alpha}_1,\dots,\widehat{\alpha}_n\in E^{H/J}$ が E 上線形独立であることを示す.[8] もし, $\widehat{\alpha}_1,\dots,\widehat{\alpha}_n$ が E 上線形従属であったとすると, $\{\widehat{\alpha}_1,\dots,\widehat{\alpha}_n\}$ の中の線形従属である極小部分集合を選び, 必要ならば, 番号も付け替えて

$$c_1\widehat{\alpha}_1+\cdots+c_s\widehat{\alpha}_s=0$$

としてよい. ここで $c_i\in E$ は全部 $\neq0$ であり, $s\ge1$ は最小である. また, $c_s\neq1$ のときは, c_s で割ることにより $c_s=1$ としてよい. よって

$$c_1\widehat{\alpha}_1+\cdots+c_{s-1}\widehat{\alpha}_{s-1}+\widehat{\alpha}_s=0\tag{4.4.1}$$

とする. (4.4.1) 式を $h\in H$ に施すと

$$c_1h(\alpha_1)+\cdots+c_{s-1}h(\alpha_{s-1})+h(\alpha_s)=0\tag{4.4.2}$$

であり, 特に, $h=\iota$ (恒等写像) のとき

$$c_1\alpha_1+\cdots+c_{s-1}\alpha_{s-1}+\alpha_s=0$$

である. ここで, $\alpha_1,\dots,\alpha_s$ は $\mathrm{fix}(H)$ 上線形独立であるから, すべての c_i が $\mathrm{fix}(H)$ では有り得ない. 例えば $c_1\notin\mathrm{fix}(H)$ としてよい. よって, $\tau\in H$ が存在して $c_1^\tau=c_1$ とできる.

(4.4.2) 式の h を $\tau^{-1}h$ に置き換えると

$$c_1\tau^{-1}h(\alpha_1)+\cdots+c_{s-1}\tau^{-1}h(\alpha_{s-1})+\tau^{-1}h(\alpha_s)=0$$

となる. この式の両辺に τ を施すと

$$c_1^\tau h(\alpha_1)+\cdots+c_{s-1}^\tau h(\alpha_{s-1})+h(\alpha_s)=0$$

が任意の $h\in H$ に対して成り立つ. したがって

$$c_1^\tau\widehat{\alpha}_1+\cdots+c_{s-1}^\tau\widehat{\alpha}_{s-1}+\widehat{\alpha}_s=0\tag{4.4.3}$$

である. 最後に, (4.4.1) 式と (4.4.3) 式を辺々引くと

$$(c_1^\tau-c_1)\widehat{\alpha}_1+\cdots+(c_{s-1}^\tau-c_{s-1})\widehat{\alpha}_{s-1}=0$$

となり, $c_1^\tau-c_1\neq0$ なので s の最小性に矛盾する. したがって, $\widehat{\alpha}_1,\dots,\widehat{\alpha}_n\in E^{H/J}$ が E 上線形独立であることが示されたので, $\dim_{\mathrm{fix}(H)}\mathrm{fix}(J)\le\dim_E E^{H/J}$ が示された. □

[7] $E\subseteq\overline{E}$ だから $\hom_K(L,E)\subseteq\hom_K(L,\overline{E})$ である.
[8] 逆も成り立つが, ここでは必要ない.

したがって, 任意の拡大のガロア対応は次数付きであることが示された. 次に, それをまとめる.

定理 4.4.3. (ガロア理論の基本定理 Part 1)　体の拡大 E/F のガロア対応 (Π, Ω) は次数付きガロア系であり, Ω の最小元である恒等写像のみからなる群 $\{\iota\} = \mathrm{G}_E(E)$ は閉じている. したがって, (Π, Ω) をガロア系の意味での閉じた元全体に制限すると, 順序を逆転させる 1 対 1 対応であり, 次数を保存し, 完全束の間の meet と join を入れ替える全単射を与える. すなわち, K_i を閉じた中間体, H_i を閉じた部分群とすると

$$\mathrm{G}_{\bigcap K_i}(E) = \bigvee \mathrm{G}_{K_i}(E), \qquad \mathrm{G}_{\bigvee K_i}(E) = \bigcap \mathrm{G}_{K_i}(E)$$

かつ

$$\mathrm{fix}\left(\bigcap H_i\right) = \bigvee \mathrm{fix}\,(H_i)\,, \qquad \mathrm{fix}\left(\bigvee H_i\right) = \bigcap \mathrm{fix}\,(H_i)$$

である.

証明. 命題 4.2.4, 命題 4.2.5, 命題 4.2.8 を見よ. □

系 4.4.4. 体の拡大 E/F のガロア対応を (Π, Ω) とする. このとき

$$|\,\mathrm{G}_F(E)| \leq [E : F]$$

であり, また, 次が成り立つ.

1) もし, $|\,\mathrm{G}_F(E)| < \infty$ ならば $\mathscr{G}$ は完全に閉じている.
2) もし, $[E : F] < \infty$ ならば $\mathscr{G}$ は完全に閉じている.
3) $[E : F] < \infty$ かつ F が閉じていれば[9], $(\mathscr{F}, \mathscr{G})$ は完全に閉じている.

証明. 命題 4.2.11 を使え. □

4.5　何が閉じているのか?

拡大 E/F のガロア対応 (Π, Ω) において, $\mathscr{F}$ の最大元 E は閉じている. また $\mathscr{G}$ の最小元 $\mathrm{G}_E(E) = \{\iota\}$ は閉じている. 閉じた元の有限次拡大は閉じている.

定義 4.5.1. E/F が分離的正規拡大のとき, **ガロア拡大 (Galois extension)** という.

命題 4.5.2.　1) $F \subseteq K \subseteq E$ が拡大列で, E/F がガロア拡大ならば E/K もガロア拡大である.
2) (Lifting property)　E/F がガロア拡大, K/F が拡大ならば EK/K もガロア拡大である.
3) (Composites and intersections)　E_λ/F $(\lambda \in \Lambda)$ がガロア拡大ならば $\bigvee_{\lambda\in\Lambda} E_\lambda/F$, $\bigcap_{\lambda\in\Lambda} E_\lambda/F$ もガロア拡大である.

証明.　1) 定理 3.7.10 1), 定理 3.12.1 1) を使え.
2) 定理 3.7.10 2), 定理 3.12.1 1) を使え.
3) 定理 3.7.10 3), 定理 3.12.1 2) を使え.
□

命題 4.5.3. 代数拡大 E/F のガロア対応 (Π, Ω) において中間体 K が $\mathscr{F}$ において閉じているための必要十分条件は E/K がガロア拡大であることである.

証明. $(\Rightarrow)$ K が $\mathscr{F}$ において閉じているとする. このとき, 任意の $\alpha \in E \setminus K$ に対して, 命題 3.4.3 により $K(\alpha)$ は K の有限次拡大だから, 命題 4.2.8 により $K(\alpha)$ も $\mathscr{F}$ において閉じている. よって, 命題 4.2.8 より

$$d = (\mathrm{G}_K(E) : \mathrm{G}_{K(\alpha)}(E)) = [K(\alpha) : K] < \infty$$

である. $S = \{\sigma_1, \ldots, \sigma_d\}$ を剰余類 $\mathrm{G}_K(E)/\,\mathrm{G}_{K(\alpha)}(E)$ の代表元とすると, 各 σ_i の α における値はすべて異なる. なぜなら, もし, $\alpha^{\sigma_i} = \alpha^{\sigma_j}$ であるとすると $\sigma_i^{-1}\sigma_j \in \mathrm{G}_{K(\alpha)}(E)$ となるからである. よって, α の K 上の最小多項式を $f(X)$ とすると α^{σ_i} $(i = 1, \ldots, d)$ は $f(X)$ の異なる根であり α は K 上分離的である. E の任意の元は分離的だから定義 3.11.4 より E/K は分離拡大である. また, $\sigma_i \in \mathrm{G}_K(E)$ より $\alpha^{\sigma_i} \in E$ であり, $f(X)$ は E で一次式の積に分解する. 定理 3.7.6 より E/K は正規拡大である.

[9] すなわち $F = \mathrm{fix}(\mathrm{G}_F(E))$ であること

($\Leftarrow$) 逆に E/K がガロア拡大とする. $\alpha \in \mathrm{cl}(K) = \mathrm{fix}(\mathrm{G}_K(E))$ とし, $f(X) \in K[X]$ を α の K 上の最小多項式とする. $\beta \in E$ を $f(X)$ の根とすると, E/K は代数拡大なので定理 3.6.12 より, K 上では恒等写像である埋込み $\sigma : E \to \overline{E}$ で $\alpha^\sigma = \beta$ となるものが存在する. E/K は正規拡大であるから, 定理 3.7.6 により, $E^\sigma \subseteq E$ であるから $\sigma \in \mathrm{G}_K(E)$ であり $\alpha \in \mathrm{fix}(\mathrm{G}_K(E))$ より $\beta = \alpha$ となる. ゆえに, $f(X)$ の根は α のみである. ところが $f(X)$ は分離的であることから $f(X) = X - \alpha$ となり, $\alpha \in K$ である. すなわち $\mathrm{cl}(K) \subseteq K$ が示された. 逆向きの包含関係は明らかだから $\mathrm{cl}(K) = \mathrm{fix}(\mathrm{G}_K(E)) = K$ となり, K は閉じている. □

これまでのことをまとめると, 次の定理になる.

定理 4.5.4. (ガロア理論の基本定理 Part 2)　代数拡大 E/F のガロア対応 (Π, Ω) を考える.

1) $\mathscr{F}$ の閉じた元とは, $\mathrm{G}_F(E)$ のある部分群 H に対して $\mathrm{fix}(H)$ の形をしている中間体で
   a) 中間体 K が閉じているための必要十分条件は E/K がガロア拡大であることである.
   b) 閉じた体の任意の拡大体である中間体は閉じている. 特に, F が閉じていれば, $\mathscr{F}$ は完全に閉じている.[10]
   c) 拡大列 $F \subseteq \mathrm{cl}(K) \subseteq L \subseteq E$ において
   $$[L : K] = (\mathrm{G}_K(E) : \mathrm{G}_L(E)) < \infty$$
   ならば K は閉じている. 特に
   $$[E : K] = |\,\mathrm{G}_K(E)| < \infty$$
   ならば K は閉じている.
2) $\mathrm{G}_F(E)$ の部分群が $\mathscr{G}$ で閉じているとは E/F のある中間体 K が存在して $\mathrm{G}_K(E)$ の形をしていることである.
   a) 閉じた部分群の指数が有限の拡大群は閉じている.
   b) $\{\iota\} = \mathrm{G}_E(E)$ は閉じている. よって, $\mathrm{G}_F(E)$ の任意の有限部分群は閉じている.
   c) E/F が有限次拡大ならば $\mathrm{G}_F(E)$ は有限群である. よって, このとき $\mathscr{G}$ は完全に閉じている.
3) E/F が有限次ガロア拡大ならば, $(\mathscr{F}, \mathscr{G})$ は完全に閉じている.

証明.　1) 閉じた元が $\mathrm{fix}(H)$ の形をしていることは, 命題 4.2.3 を使う.
   a) 命題 4.5.3
   b) $F \subseteq K \subseteq M \subseteq E$ を拡大列として, K が $\mathscr{F}$ で閉じていれば a) より E/K はガロア拡大で, 命題 4.5.2 1) より E/M もガロア拡大となり a) より M も $\mathscr{F}$ で閉じている.
   c) 命題 4.2.9 2)

2) 閉じた部分群が $\mathrm{G}_K(E)$ の形をしていることは, 命題 4.2.3 を使う.
   a) 命題 4.2.8 2)
   b) 命題 4.2.8 2)
   c) 命題 4.2.11

3) 命題 4.2.11

□

例 4.5.5. p を素数とする. ここでは,

任意の p の冪 $q = p^d$ に対して, 位数 q の有限体 $\mathbb{F}_q$ が存在し, $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^r}$ である必要十分条件は $d|r$ である.

という未だ証明していない事実を使う. $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $E = \overline{\mathbb{F}}_p$ とする. F は有限群なので, F は完全体で E/F は分離的である. E は代数的閉体なので $F \lhd E$ である. したがって, E/F はガロア拡大で, 定理 4.5.4 1a) より F は閉じている. $F \subseteq E$ は

[10] 一般の代数拡大 E/F では, $\mathrm{fix}\,(\mathrm{G}_F(E))$ と E の中間体はすべて閉じているし, 逆に, 閉じた体は, 常に $\mathrm{fix}\,(\mathrm{G}_F(E))$ と E の中間体である. よって, $\mathrm{Cl}(\mathscr{F})$ と $\mathrm{Cl}(\mathscr{G})$ の間の 1 対 1 対応は $\mathrm{fix}\,(\mathrm{G}_F(E))$ と E の中間体と $\mathrm{G}_F(E)$ の閉じた部分群の間の 1 対 1 対応である. ここで, $\mathrm{G}_F(E)$ のすべての部分群が閉じている訳ではないことを, 次の例で見る. しかし, 命題 4.2.11 より $|\,\mathrm{G}_F(E)| < \infty$ または $[E : F] < \infty$ ならば $\mathrm{G}_F(E)$ の部分群はすべて閉じていて, ガロア対応は $\mathrm{fix}\,(\mathrm{G}_F(E))$ と E の中間体と $\mathrm{G}_F(E)$ の部分群との間の 1 対 1 対応を与える. さらに, E/F が有限次ガロア拡大ならば, F は閉じていて, ガロア対応は E と F の中間体と $\mathrm{G}_F(E)$ の部分群との間の 1 対 1 対応を与えることになる. これが, 古典的なガロア理論である.

有限次拡大ではないが, 任意の $k \geq 1$ に対して $\mathbb{F}_p \subseteq \mathbb{F}_{p^k} \subseteq E$ であり, 各中間体 $\mathbb{F}_{p^k}$ は閉じている. $\sigma_p : \alpha \mapsto \alpha^p$ を Frobenius map とし, $H = \langle \sigma_p \rangle$ を σ_p が生成する $\mathrm{G}_F(E)$ の部分群とする. $\mathrm{fix}(H)$ の元は $\alpha \in E$ の元で $\alpha^p = \alpha$ をみたすもの全体である. すなわち, 多項式 $f(X) = X^p - p$ の根だから高々 p 個しかないので, $\mathrm{fix}(H) = F$ である. よって

$$\mathrm{cl}(H) = \mathrm{G}_{\mathrm{fix}(H)}(E) = \mathrm{G}_F(E)$$

が言えた.

次に $H \neq \mathrm{G}_F(E)$ を示そう. H は σ_p で生成される巡回群なので, H の単位元でない元は $\tau = \sigma_p^k$ $(k \neq 0)$ の形をしている. よって, τ の固定体は

$$\{\alpha \in E \,|\, \sigma_p^k(\alpha) = \alpha\} = \{\alpha \in E \,|\, \alpha^{p^k} = \alpha\} = \mathbb{F}_{P^k}$$

であり, 有限体である. よって, $H \neq \mathrm{G}_F(E)$ を示すには $\mathrm{G}_F(E)$ に無限個の元を固定する写像が存在することを示せばよい.

q を素数として, E の部分体

$$K = \mathbb{F}_{p^q} \cup \mathbb{F}_{p^{q^2}} \cup \mathbb{F}_{p^{q^3}} \cup \cdots$$

を考えよう. 例えば, $\mathbb{F}_{p^{q+1}}$ は K の部分体ではないので $K \subsetneq E$ である. よって $[E : K] > 1$ であり, E/K はガロア拡大であるから $\mathrm{G}_K(E)$ は $\{\iota\}$ ではない. このとき, $\tau \in \mathrm{G}_K(E) \subseteq \mathrm{G}_F(E)$ は無限個の元を固定する. したがって, H が閉じていないことが示された. □

$G \subset \mathrm{Aut}(E)$ を $\mathrm{Aut}(E)$ の任意の部分群として固定する. G の固定する体

$$\mathrm{fix}(G) = \{\alpha \in E \,|\, \alpha^\sigma = \alpha \quad ({}^\forall\sigma \in G)\}$$

を考える. ここでは $E/\mathrm{fix}(G)$ は代数拡大であると仮定する. 命題 4.2.3 より $\mathrm{fix}(G)$ は $\mathscr{F}$ で閉じている. よって, 定理 4.5.4 1a) より $E/\mathrm{fix}(G)$ はガロア拡大であり $\mathscr{F}$ は完全に閉じている. さらに, $[E : \mathrm{fix}(G)] < \infty$ ならば, 系 4.4.4 より $(\mathscr{F}, \mathscr{G})$ は完全に閉じている. 一般に $G = \mathrm{G}_{\mathrm{fix}(G)}(E)$ となるとは限らず $G \subsetneq \mathrm{G}_{\mathrm{fix}(G)}(E)$ となることもあるが, もし G が有限群ならば G は $\mathscr{G}$ で閉じている. したがって, 次の定理をえる.

定理 4.5.6. *E が体で G を $\mathrm{Aut}(E)$ の部分群とする.*[11]

1) *$E/\mathrm{fix}(G)$ が代数拡大ならば $E/\mathrm{fix}(G)$ はガロア拡大であり $\mathscr{F}$ は完全に閉じている.*
2) *$E/\mathrm{fix}(G)$ が有限次拡大ならば $(\mathscr{F}, \mathscr{G})$ は完全に閉じている.*
3) *もし G が $\mathscr{G}$ で閉じているならば, $G = \mathrm{G}_{\mathrm{fix}(G)}(E)$ は $\mathscr{G}$ の最大元である.*

これまでの議論から $\mathrm{G}_F(E)$ が無限群であるときには, $\mathrm{G}_F(E)$ のすべての部分群が閉じているわけではないということがわかった.[12] 次の定理において, $\mathrm{G}_F(E)$ の閉じた部分群の特徴付けを行う. 次の定義は余り標準的ではない.

定義 4.5.7. *E/F を代数拡大とする. H を $\mathrm{G}_F(E)$ の部分群とするとき, 写像 $\tau : E \to E$ が H の* **閉点 (closure point)** *であるとは, E の任意の有限部分集合 $U \subseteq E$ に対して $\tau|_U = H|_U$ となることである.*[13] *H の閉点全体の集合を $\overline{H}$ と書く.*[14]

まず H の閉点 $\tau : E \to E$ は $\mathrm{G}_F(E)$ の元であり

$$H \subseteq \overline{H} \subseteq \mathrm{G}_{\mathrm{fix}(H)}(E) = \mathrm{cl}(H)$$

である. なぜなら $\alpha, \beta \in E$ に対して $h \in H$ が存在して $S = \{\alpha, \beta, \alpha \pm \beta, \alpha^{-1}\}$ 上で τ と h は一致するので τ は E から E への体の準同型である. 任意の $\alpha \in \mathrm{fix}(H)$ に対して, $h \in H$ が存在して $S = \{\alpha\}$ 上で τ と h が一致するので $\alpha^\tau = \alpha^h = \alpha$ となり, τ も $\mathrm{fix}(H)$ の元を動かさないので $\tau \in \mathrm{G}_{\mathrm{fix}(H)}(E)$ である. また, $h \in H$ は $h \in \overline{H}$ であることは明らか. 最後に $H^\Omega = \mathrm{fix}(H)$, $\mathrm{cl}(H) = H^{\Omega\Pi} = \mathrm{G}_{\mathrm{fix}(H)}(E)$ であることに注意しよう.

定理 4.5.8. *E/F を代数拡大で H を $\mathrm{G}_F(E)$ の部分群とする. このとき, $\mathrm{cl}(H) = \overline{H}$ である. 具体的には, 任意の写像 $\tau : E \to E$ に対して, 次の 1) 2) は同値である.*

1) *$\tau \in \mathrm{cl}(H)$*

[11] 読者は, 代数拡大 E/F において $G = \mathrm{G}_F(E) \subseteq \mathrm{Aut}(E)$ という状況を想定して, 定理を読み直して欲しい.
[12] 有限群のときは, すべての部分群は閉じていることが示された.
[13] $h \in H$ が存在して $\tau|_U = H|_U$ となること.
[14] 定義から $H \subseteq \overline{H}$ である. なぜなら $h \in H$ ならば, 有限集合 $U \subseteq E$ 上で $h|_U = h|_U$ と書ける.

2) E の任意の有限部分集合 $U \subseteq E$ に対して $\tau|_U = H|_U$ となる.

逆に, $\mathrm{G}_F(E)$ の部分群 H が $\mathscr{G}$ で閉じているための必要十分条件は H の閉点をすべて含むことである. 特に, $\mathrm{G}_K(E)$ の形をした部分群は, その閉点をすべて含む.

証明. $\overline{H} = \mathrm{cl}(H)$ を示す[15].E の任意の有限部分集合 $U \subseteq E$ に対して $\mathrm{fix}(H)$ に U を添加した体を $K_1 = \mathrm{fix}(H)(U)$ とおく. このとき, 命題 3.4.3 より $K_1/\mathrm{fix}(H)$ は $\mathrm{fix}(H)$ 上有限次拡大である. 定理 3.8.2 4) より $K = \mathrm{nc}(K_1/\mathrm{fix}(H))$ も $\mathrm{fix}(H)$ 上有限次拡大である. よって, 定理 4.5.4 1), 系 4.4.4 3) により, $K/\mathrm{fix}(H)$ に対応する $(\mathscr{F}(K/\mathrm{fix}(H)), \mathscr{G}(K/\mathrm{fix}(H)))$ は完全に閉じている.

$h \in H \subseteq \mathrm{G}_F(E)$ は $\mathrm{fix}(H)$ を固定するので $h \in \mathrm{G}_{\mathrm{fix}(H)}(E)$ であるが, $K/\mathrm{fix}(H)$ が正規拡大であるから, 定理 3.7.6 2) により $h(K) = K$ である. よって $h|_K$ は $\mathrm{G}_{\mathrm{fix}(H)}(K)$ の元と考えられ, $H|_K = \{h|_K \in \mathrm{G}_{\mathrm{fix}(H)}(K) | h \in H\}$ と書くことにすると, $H|_K$ は $\mathrm{G}_{\mathrm{fix}(H)}(K)$ の部分群である.

$\mathrm{G}_{\mathrm{fix}(H)}(K)$ は完全に閉じているので, $H|_K$ も $\mathscr{G}(K/\mathrm{fix}(H)))$ の中で閉じていることになり,

$$H|_K = \mathrm{cl}(H|_K) = \mathrm{G}_{\mathrm{fix}(H|_K)}(K) = \mathrm{G}_{\mathrm{fix}(H)}(K)$$

である. すなわち, 任意の $\sigma \in \mathrm{G}_{\mathrm{fix}(H)}(K)$ に対して, $h \in H$ が存在して, $\sigma = h|_K$ となる.

よって, もし $\tau : E \to E$ が $\tau \in \mathrm{G}_{\mathrm{fix}(H)}(E)$ ならば $K/\mathrm{fix}(H)$ が正規拡大であることより $\tau|_K \in \mathrm{G}_{\mathrm{fix}(H)}(K)$ となり, $h \in H$ が存在して, $\tau|_K = h|_K$ となる. $U \subseteq K$ より $\tau|_U = h|_U$ である. □

4.6 正規部分群と正規拡大

定義 4.6.1. K, L が拡大 E/F の中間体とする. $\sigma \in \mathrm{G}_F(E)$ が存在して $\sigma K = L$ となるとき, K と L は**共役 (conjugate)** という.

定理 4.6.2. E/F が体の拡大とする.

1) $F \subseteq K \subseteq E$ が拡大列のとき, 任意の $\sigma \in \hom_F(E, \overline{E})$ に対して

$$\sigma\, \mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_{K^\sigma}(E^\sigma)$$

2) $F \lhd K \subseteq E$ が拡大列のとき, 任意の $\sigma \in \hom_F(E, \overline{E})$ に対して

$$\sigma\, \mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_K(E^\sigma)$$

3) $F \subseteq K \subseteq E$ が拡大列で E/F が正規拡大のとき, 任意の $\sigma \in \hom_F(E, \overline{E})$ に対して

$$\sigma\, \mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_{K^\sigma}(E)$$

4) K, L が拡大 E/F の中間体で, E/F が正規拡大のとき, K と L が共役であるための必要十分条件は $\mathrm{G}_K(E)$ と $\mathrm{G}_L(E)$ が $\mathrm{G}_F(E)$ において共役であること.

証明. 1) $\tau \in \mathrm{G}_{K^\sigma}(E^\sigma)$ に対して $\sigma^{-1}\tau\sigma : E \to E^\sigma \to E^\sigma \to E$ であり, また $\alpha \in K$ に対して $\tau \in \mathrm{G}_{K^\sigma}(E^\sigma)$ より

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

よって $\sigma^{-1}\tau\sigma \in \mathrm{G}_K(E)$ である. したがって, $\sigma^{-1}\,\mathrm{G}_{K^\sigma}(E^\sigma)\sigma \subseteq \mathrm{G}_K(E)$ すなわち

$$\mathrm{G}_{K^\sigma}(E^\sigma) \subseteq \sigma\,\mathrm{G}_K(E)\sigma^{-1}$$

が示された. 逆の包含関係を示すには $\mu \in \mathrm{G}_K(E)$ に対して $\sigma\mu\sigma^{-1} \in \mathrm{G}_{K^\sigma}(E^\sigma)$ が定義されることを, 同様にして示せばよい. これも簡単なので省略.

2) $F \lhd K$ のとき, 定理 3.7.6 より, 任意の $\sigma \in \hom_F(E, \overline{E})$ に対して $K^\sigma = K$ だから 1) より従う.

[15] $\mathrm{cl}(H) = \mathrm{G}_{\mathrm{fix}(H)}(E)$ である. また, ここで示すべきは $^\forall\tau \in \mathrm{G}_{\mathrm{fix}(H)}(E)$ に対して $\tau \in \overline{H}$ (閉点) であること.

3) E/F が正規拡大のとき, 定理 3.7.6 より, 任意の $\sigma \in \hom_F(E, \overline{E})$ に対して $E^\sigma = E$ だから 1) より従う.

4) $L = K^\sigma$ ならば 3) より $\sigma\,\mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_L(E)$ なので $\mathrm{G}_K(E)$ と $\mathrm{G}_L(E)$ は共役である. 逆に, $\mathrm{G}_K(E)$ と $\mathrm{G}_L(E)$ が $\mathrm{G}_F(E)$ において共役であるとすると, $\sigma \in \mathrm{G}_F(E)$ が存在して, $\sigma\,\mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_L(E)$ となるので, 3) より $\mathrm{G}_{K^\sigma}(E) = \mathrm{G}_L(E)$ となる. E/F が正規拡大なので, 定理 4.5.4 1b) より $K^\sigma = L$ となる. よって K と L は共役である.

□

定理 4.6.3. (ガロア理論の基本定理 Part 3: 正規性) $F \subseteq K \subseteq E$ を拡大列とし, E/F は代数拡大とする. $\varphi : \mathrm{G}_F(E) \to \hom_F(K, E)$ を写像の制限

$$\varphi(\sigma) = \sigma|_K$$

とする. このとき, 次が成り立つ.

1) $F \lhd K$ ならば $\mathrm{G}_K(E) \lhd \mathrm{G}_F(E)$ であり, φ は単射

$$\overline{\varphi} : \mathrm{G}_F(E)/\,\mathrm{G}_K(E) \to \mathrm{G}_F(K)$$

を誘導し, E/F が正規拡大ならば $\overline{\varphi}$ は群としての同型写像である.

2) $\mathrm{G}_K(E) \lhd \mathrm{G}_F(E)$ であり, $F \lhd E$ かつ K が $\mathscr{F}$ で閉じた元 (すなわち E/K はガロア拡大) ならば, $F \lhd K$ であり, φ は同型写像

$$\overline{\varphi} : \mathrm{G}_F(E)/\,\mathrm{G}_K(E) \simeq \mathrm{G}_F(K)$$

を誘導する.

3) E/F がガロア拡大のとき,

$$F \lhd K \quad \Leftrightarrow \quad \mathrm{G}_K(E) \lhd \mathrm{G}_F(E)$$

証明. 1) の前半: $\sigma \in \mathrm{G}_F(E)$ のとき, 定理 4.6.2 1) より

$$\sigma\,\mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_{K^\sigma}(E^\sigma) = \mathrm{G}_{K^\sigma}(E)$$

となる. よって, $\mathrm{G}_K(E)$ が $\mathrm{G}_F(E)$ の中で正規部分群であるための必要十分条件は任意の $\sigma \in \mathrm{G}_F(E)$ に対して

$$\mathrm{G}_{K^\sigma}(E) = \sigma\,\mathrm{G}_K(E)\sigma^{-1} = \mathrm{G}_K(E)$$

となることである. K/F が正規拡大ならば, 定理 3.7.6 より, 任意の $\sigma \in \mathrm{G}_F(E)$ に対して $K^\sigma = K$ なので, この式は常に成り立ち, $\mathrm{G}_K(E) \lhd \mathrm{G}_F(E)$ となる.

2) の前半: 逆に, $\mathrm{G}_K(E) \lhd \mathrm{G}_F(E)$ ならば, 定理 4.6.2 1) より, 任意の $\sigma \in \mathrm{G}_F(E)$ に対して

$$\mathrm{G}_{K^\sigma}(E) = \mathrm{G}_K(E)$$

が成り立つから, 両辺の fix を取ることによって [16]

$$K^\sigma \subseteq \mathrm{cl}(K^\sigma) = \mathrm{cl}(K)$$

である. もし, K が $\mathscr{F}$ で閉じている [17] ならば $\mathrm{cl}(K) = K$ なので, 任意の $\sigma \in \mathrm{G}_F(E)$ に対して $K^\sigma \subseteq K$ となる. さらに $F \lhd E$ だから, 任意の $\sigma \in \hom_F(E, \overline{E})$ に対して定理 3.7.6 より $\sigma \in \mathrm{G}_F(E)$ なので $K^\sigma \subseteq K$ となる. よって, 再び, 定理 3.7.6 より K/F は正規拡大である.

1) 2) の後半: K/F, E/K, E/F がいずれも正規拡大のとき, 写像の制限

$$\varphi(\sigma) = \sigma|_K$$

によって $\varphi : \mathrm{G}_F(E) \to \hom_F(K, E)$ を定義する. $F \lhd E$ なので, 定理 3.7.6 より $\varphi(\sigma) \in \mathrm{G}_F(K)$ であり, φ は明らかに群 $\mathrm{G}_F(E)$ から群 $\mathrm{G}_F(K)$ への群としての準同型写像である. また, E/K は代数拡大なので, 定理 3.6.12, 定理 3.7.6 より $\mathrm{G}_F(K)$ の元は $\mathrm{G}_F(E)$ の元に延長できるので φ は全射である. さらに φ の核は $\mathrm{G}_K(E)$ に他ならない. よって, 群の第一同型定理により, 群として

$$\mathrm{G}_F(E)/\,\mathrm{G}_K(E) \simeq \mathrm{G}_F(K)$$

となる.

[16] $\mathrm{cl}(K^\sigma) = \mathrm{fix}(\mathrm{G}_{K^\sigma}(E))$ と $\mathrm{cl}(K) = \mathrm{fix}(\mathrm{G}_K(E))$ より, 次式の等号を得る. 包含関係は自明.

[17] 定理 4.5.4 1a) より E/K はガロア拡大ということ

3) の証明　(⇒) は 1) の帰結である.

(⇐)　E/F がガロア拡大のとき, 定義 4.5.1 より $F \lhd E$ であり, 定理 4.5.4 1b) より K は閉じている. よって 2) の帰結である. □

例 4.6.4. $f(X) = x^4 - 2$ の $F = \mathbb{Q}$ 上の最小分解体 E を考察する. $r = \sqrt[4]{2}$ とおくと $f(X)$ の根は $r, -r, ri, -ri$ の 4 個だから $E = \mathbb{Q}\left(\sqrt[4]{2}, i\right) = \mathbb{Q}(i, r)$ である.

$$F = \mathbb{Q} \subseteq \mathbb{Q}(r) \subseteq \mathbb{Q}(i, r) = E$$

は代数拡大列で, $\mathbb{Q}(r)/\mathbb{Q}$ は 4 次の拡大, $\mathbb{Q}(i, r)/\mathbb{Q}(r)$ は 1 次または 2 次の拡大であるが $r \in \mathbb{R}$ は実数なので, $i \notin \mathbb{Q}(r)$ となり $\mathbb{Q}(i, r)/\mathbb{Q}(r)$ は 2 次の拡大であることがわかる. よって E/F は 8 次の拡大である. 標数 0 の体 $\mathbb{Q}$ は完全体なので E/F は分離拡大. E は $f(X)$ の最小分解体なので E/F は正規拡大であり, よってガロア拡大である. $[E : F] = 8$ は有限なので F は閉じていて ($\mathscr{F}$,$\mathscr{G}$) は完全に閉じていて, E/F の中間体 K と, そのガロア群 $\mathrm{G}_K(E)$ は 1 : 1 に対応する.

$\sigma, \tau \in \mathrm{G}_F(E)$ を

$$\sigma : r \mapsto ir, \quad \tau : i \mapsto i$$
$$\tau : r \mapsto r, \quad \tau : i \mapsto -i$$

によって定義すると, σ の位数は 4, τ の位数は 2 であることが, すぐにわかる. また, σ, τ の間には $\sigma^4 = 1$, $\tau^2 = 1$, $\tau\sigma\tau = \sigma^{-1}$ の関係式があるので, E/F のガロア群 $G = \mathrm{G}_F(E)$ は 2 面体群 D_4 と同型な群である. その包含関係によるハッセ図を描くと, 図 4.6.1 のようになる. この中で正規部分群は $\langle\tau^2\rangle$, $\langle\tau\rangle$, $\langle\tau, \sigma^2\tau\rangle$, $\langle\sigma\tau, \sigma^3\tau\rangle$ である.

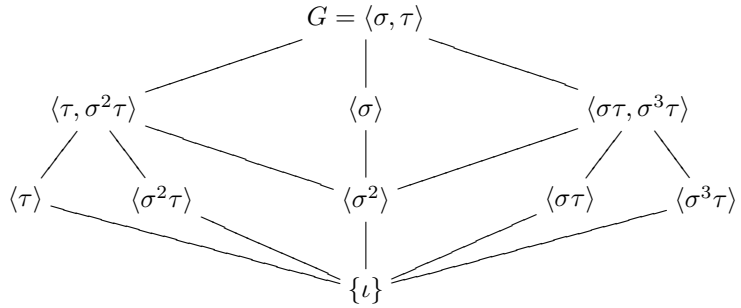

図 4.6.1: $G = \mathrm{G}_F(E) = \langle\sigma, \tau\rangle$ の部分群のなす束

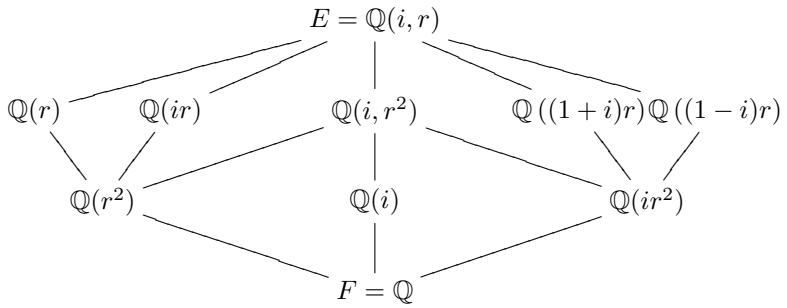

図 4.6.2: E/F の中間体のなす束

4.7 Lifting のガロア群

E/F が正規拡大で, K/F が拡大のとき, lifiting のガロア群の元 $\sigma \in \mathrm{G}_K(EK)$ は, その E への作用から決まる. よって, 写像の制限 $\sigma \mapsto \sigma|E$ は単射 $\mathrm{G}_K(EK) \to \mathrm{G}_F(E)$ を定める. E/F は正規拡大なので, $\sigma|_E \in \mathrm{G}_F(E)$ である. 実際には

$$\sigma|_E \in \mathrm{G}_{E \cap \mathrm{fix}_{EK}(\mathrm{G}_K(EK))}(E) = \mathrm{G}_{E \cap \mathrm{cl}_{EK}(K)}(E)$$

である. この写像 $\sigma \mapsto \sigma|_E$ は群の準同型なので $\mathrm{G}_K(EK)$ から $\mathrm{G}_F(E)$ への埋め込みである.

定理 4.7.1. (Lifting のガロア群)　E/F が正規拡大, K/F を任意の拡大とする. 写像の制限 $\varphi(\sigma)=\sigma|_E$ によって定義される写像

$$\varphi : \mathrm{G}_K(EK) \to \mathrm{G}_{E\cap \mathrm{cl}(K)}(E)$$

は群の同型写像であり

$$\mathrm{G}_K(EK) \simeq \mathrm{G}_{E\cap \mathrm{cl}(K)}(E)$$

となる. ここで $\mathrm{cl}(K)=\mathrm{cl}_{EK}(K)=\mathrm{fix}_{EK}\left(\mathrm{G}_K(EK)\right)$ とする.

証明. φ は群の埋込み (群としての準同型写像で単射であること) ということは既に述べたので, 全射であることを示せばよい. 混乱を避けるために, 拡大 EK/K に関するガロア対応に関しては fix_{EK} と書き, 拡大 E/F に関するガロア対応に関しては fix_E と書く.

$$\begin{aligned}
\mathrm{fix}_E(\mathrm{Im}(\varphi)) &= \{\alpha\in E \,|\, \alpha^\tau=\alpha \text{ for } {}^\forall\tau\in \mathrm{Im}(\varphi)\} \\
&= \{\alpha\in E \,|\, \alpha^{\sigma|_E}=\alpha \text{ for } {}^\forall\sigma\in \mathrm{G}_K(EK)\} \\
&= \{\alpha\in E \,|\, \alpha^{\sigma}=\alpha \text{ for } {}^\forall\sigma\in \mathrm{G}_K(EK)\} \\
&= E\cap \mathrm{fix}_{EK}\left(\mathrm{G}_K(EK)\right)
\end{aligned}$$

よって $\mathrm{Im}(\varphi)$ が E/F に関するガロア対応において閉じていることを示せば,

$$\mathrm{Im}(\varphi)=\mathrm{G}_{E\cap \mathrm{fix}_{EK}(\mathrm{G}_K(EK))}(E)$$

が示され, φ が全射であることが示される. もし E/F が有限次拡大ならばガロア群 $\mathrm{G}_F(E)$ のすべての部分群は閉じているので, やることはない.

よって, E/F が無限次拡大であるとし, E の F 上の基底を $\{e_i\}$ とする. このとき, $\{e_i\}$ は K 上 EK をベクトル空間として生成する. すなわち, EK の任意の元は $\{e_i\}$ の K-線形結合として書ける.

$I=\mathrm{Im}(\varphi)$ のすべての閉点が I に含まれることを示すことによって, I が閉じていることを示す. すなわち $\tau\in\overline{I}$ ならば $\sigma\in\mathrm{G}_K(EK)$ が存在して $\tau=\sigma|_E$ となることを示せばよい. ところが, $\sigma\in\mathrm{G}_K(EK)$ は τ の E への作用で完全に決まるはずである. $\tau\in\overline{I}$ ならば $\tau : E\to E$ は, E の任意の有限部分集合 U に対して $\tau|_U=\mathrm{Im}(\varphi)|_U$ である. このとき $\sigma : EK\to EK$ を次のように定義する. 任意の $\alpha\in EK$ に対して

$$\alpha=\sum_i k_i e_i$$

となる $k_i\in K$ が存在する. このとき

$$\sigma(\alpha)=\sum_i k_i\tau(e_i)$$

と定義する. この定義が well-defined であることを示すには $k_j\in K$ として

$$\alpha=\sum_j k'_j e_j$$

という別の表し方ができたときにこれら 2 通りの線形結合に表れる基底の有限個の元 $\{e_i,e_j\}$ の集合を U とすると $\sigma'\in\mathrm{G}_K(EK)$ が存在して $\tau|_U=\sigma'|_U$ となる. ゆえに

$$\sum_i k_i\tau(e_i)=\sum_i k_i\sigma'(e_i)=\sigma'\left(\sum_i k_i e_i\right)=\sigma'(\alpha)=\sigma'\left(\sum_j k'_j e_j\right)=\sum_j k'_j\sigma'(e_j)$$

となる. よって well-defined であることが示された.

σ は E 上では τ と一致する. なぜなら $\alpha\in E$ は $\alpha=\sum_i f_i e_i$ $(f_i\in F)$ と書けるが, $f_i\in K$ なので

$$\sigma(\alpha)=\sum_i f_i\tau(e_i)=\tau\left(\sum_i f_i e_i\right)$$

あきらかに σ は K の元を固定する. したがって, $\sigma\in\mathrm{G}_K(EK)$ が構成され, $\tau=\sigma|_E$ が示された. □

E/F がガロア拡大ならば, 上の定理は簡単になる.

系 4.7.2. (Lifting のガロア群) E/F がガロア拡大, K/F を任意の拡大とすると EK/K はガロア拡大である. 写像の制限 $\varphi(\sigma) = \sigma|_E$ によって定義される写像 $\varphi : \mathrm{G}_K(EK) \to \mathrm{G}_{E\cap K}(E)$ は群の同型写像であり

$$\mathrm{G}_K(EK) \simeq \mathrm{G}_{E\cap K}(E)$$

となる. さらに次が成り立つ.

1) $E \cap K = F$ ならば $\mathrm{G}_K(EK) \simeq \mathrm{G}_F(E)$ である.
2) E/F が有限次拡大とする. このとき $\mathrm{G}_K(EK) \simeq \mathrm{G}_F(E)$ ならば $E \cap K = F$ である.

証明. 定理 3.7.10 (1), 定理 3.12.1 より EK/K はガロア拡大である. よって, 定理 4.5.4 1a) より K は閉じていて $\mathrm{cl}_{EK}(K) = K$ である. 定理 4.7.1 を使え.

1) は, 明らかである.

2) に関しては $[E : F]$ が有限次元のときは, 定理 4.5.4 3) より, E/F も EK/K もガロア対応は $\mathscr{F}$ も $\mathscr{G}$ も完全に閉じている. 本来 $\mathrm{G}_{E\cap K}(E) \subseteq \mathrm{G}_F(E)$ は常に成り立つので

$$\mathrm{G}_{E\cap K}(E) \simeq \mathrm{G}_K(EK) \simeq \mathrm{G}_F(E)$$

より $\mathrm{G}_{E\cap K}(E) = \mathrm{G}_F(E)$ となる. ここで, 両辺の fix をとると $E \cap K = F$ である. □

系 4.7.2 より, 次数についての次の有用な系が得られる. 次数については, 図 4.7.1 より読み取れる.

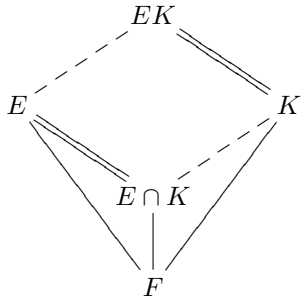

図 4.7.1: 有限次ガロア拡大の Lifiting

系 4.7.3. E/F がガロア拡大, K/F を任意の拡大とする. このとき, 次が成り立つ.

1) $[EK : K] = [E : E \cap K]$ である. よって $[EK : K] | [E : F]$ である.
2) $[EK : F] = [E : E \cap K][K : F]$
3) $[E : F][K : F]$ は $[EK : F]$ の倍数である. 等号が成り立つための必要十分条件は $E \cap K = F$ である.

さらに, E_i/F $(i = 1, \ldots, n-1)$ が有限次ガロア拡大で E_n/F が有限次拡大のとき [18], 次が成り立つ. ただし, $E_{n+1} = F$ とする.

4) $[E_1 \ldots E_n : F] = \prod_{i=1}^{n} [E_i : E_i \cap (E_{i+1} \ldots E_{n+1})]$
5) $[E_1 \ldots E_n : F] = \prod_{i=1}^{n} [E_i : E_i \cap F]$ であるための必要十分条件は $E_i \cap (E_{i+1} \ldots E_{n+1}) = F$ がすべての i について成り立つことである.

ただし, $E_{n+1} = F$ とする.

証明. 1) は系 4.7.2 より

$$[EK : K] = \sharp \mathrm{G}_K(EK) = \sharp \mathrm{G}_{E\cap K}(E) = [E : E \cap K]$$

2) に関しては $[EK : F] = [EK : K][K : F] = [E : E \cap K][K : F]$

[18] ここで, E_n/F が有限次は必要ないように見える.

3) に関しては 2) より $[E:F][K:F]=[E:E\cap K][E\cap K:F][K:F]=[EK:F][E\cap K:F]$ だから $[EK:F]|[E:F][K:F]$

4) に関しては, $E_1\dots E_{n+1}=E_1\dots E_n$ なので, 2) より

$$\begin{aligned}[E_1\dots E_{n+1}:F]&=[E_1\dots E_n:E_1\cap(E_2\dots E_{n+1})][E_2\dots E_{n+1}:F]\\&=[E_1\dots E_{n+1}:E_1\cap(E_2\dots E_{n+1})][E_2\dots E_{n+1}:E_2\cap(E_3\dots E_{n+1})][E_3\dots E_{n+1}:F]\\&=\cdots\\&=\prod_{i=1}^{n-1}[E_i\dots E_{n+1}:E_i\cap(E_{i+1}\dots E_{n+1})]\cdot[E_n:F]\end{aligned}$$

より, 求める式を得る.

5) に関しては $F\subseteq E_i\cap(E_{i+1}\dots E_{n+1})$ と 4) より明らか. □

4.8 合成体のガロア群

$F\lhd E$ かつ $F\lhd K$ とする. このとき, 任意の $\sigma\in \mathrm{G}_F(EK)$ は σ の E と K への作用から完全に決まる. すなわち, その制限 $\sigma|_E$ と $\sigma|_K$ が σ を決定する. また, 正規拡大だから

$$(\sigma|_E,\sigma|_K)\in \mathrm{G}_F(E)\times \mathrm{G}_F(K)$$

である. ゆえに, 写像 $\varphi:\mathrm{G}_F(EK)\to \mathrm{G}_F(E)\times \mathrm{G}_F(K)$ は単射であり, 群の埋込みになる. さらに, 有限次拡大で $E\cap K=F$ という条件が成り立つ場合には, 次の定理に見るように群の同型を与える.

定理 4.8.1. (合成体のガロア群)

1) $\mathscr{E}=\{E_i\,|\,i\in I\}$ を F の拡大体の族とし, すべての $i\in I$ に対して E_i/F は正規拡大とする. $G=\prod_{i\in I}\mathrm{G}_F(E_i)$ をガロア群 $\mathrm{G}_F(E_i)$ の直積とし, $\pi_i:G\to \mathrm{G}_F(E_i)$ を第 i 成分への射影とする.[19] このとき

$$\pi_i\left(\varphi(\sigma)\right)=\sigma|_{E_i}$$

によって定義される写像

$$\varphi:\mathrm{G}_F\left(\bigvee_{i\in I}E_i\right)\to\prod_{i\in I}\mathrm{G}_F(E_i)$$

は群としての単準同型写像である. よって $\mathrm{G}_F\left(\bigvee_{i\in I}E_i\right)$ は $\prod_{i\in I}\mathrm{G}_F(E_i)$ の部分群に同型である.

2) $\mathscr{E}=\{E_1,\dots,E_n\}$ を有限個の F の有限次ガロア拡大体の族とする. このとき, φ は全射となり,

$$\mathrm{G}_F\left(E_1\vee\cdots\vee E_n\right)\simeq \mathrm{G}_F(E_i)\times\cdots\times \mathrm{G}_F(E_i)$$

であるための必要十分条件は, すべての $i=1,\dots,n$ に対して

$$E_i\cap(E_{i+1}\cdots E_{n+1})=F$$

となることである. ただし, $E_{n+1}=F$ とする.

---

[19] $\{G_\lambda\}_{\lambda\in\Lambda}$ が群の族のとき, 群 G と群の全射準同型写像 $\pi_\lambda:G\to G_\lambda$ $(\lambda\in\Lambda)$ が存在して, 次をみたす:

群 G' と群の準同型写像 $\pi'_\lambda:G'\to G_\lambda$ が存在すれば, 群の準同型写像 $f:G'\to G$ で

$$\pi'_\lambda=\pi_\lambda\circ f\qquad\qquad {}^\forall\lambda\in\Lambda$$

となるものが唯一つ存在する.

このとき, 組 $(G,\{\pi_\lambda\}_{\lambda\in\Lambda})$ を $\{G_\lambda\}_{\lambda\in\Lambda}$ の直積という.

よって, 一意性より, G' が群で, 写像 $\varphi:G'\to G$ がすべての $\lambda\in\Lambda$ に対して, $\pi_\lambda\circ\varphi$ が群の準同型ならば φ も群の準同型である.

証明. まず, 1) を示す. $E = \bigvee_{i\in I} E_i$ とおく. $F \lhd E_i$ なので, 定理 3.7.10 3) より $F \lhd E$ である. 任意の $\sigma \in \mathrm{G}_F(E_k)$ を $\sigma : E_k \to \overline{E}$ ($\overline{E}$ は E の代数的閉包) と見ると, 定理 3.6.12 より, $\overline{\sigma} : E \to \overline{E}$ に延長され, E/F は正規拡大だから $\overline{\sigma}(E) = E$ となり, $\overline{\sigma} \in \mathrm{G}_F(E)$, $\overline{\sigma}|_{E_k} = \sigma$ となる. よって

$$\varphi_k = (\pi_k \circ \varphi) : \overline{\sigma} \mapsto \overline{\sigma}|_{E_k}$$

は $G_F(E)$ から $G_F(E_i)$ への全射の群準同型写像である.[20] また, 核は $\mathrm{G}_{E_k}(E)$ である. したがって, φ は $\mathrm{G}_F(E)$ から $\prod_{i\in I} \mathrm{G}_{E_i}(E)$ への群準同型写像である.

$\varphi(\sigma) = \iota$ ならば

$$\sigma|_{E_k} = \varphi_k(\sigma) = \pi_k \circ \varphi(\sigma) = \iota$$

より $\sigma = \iota$ でなければならない. よって, φ の核は $\mathrm{Ker}(\varphi) = \{\iota\}$ である. ゆえに, φ は群の単射準同型で, $\mathrm{G}_F\left(\bigvee_{i\in I} E_i\right)$ は $\prod_{i\in I} \mathrm{G}_F(E_i)$ の部分群に同型である.

次に, 2) を示す. $\mathscr{F} = \{E_1, \ldots, E_n\}$ が有限次ガロア拡大の有限族のとき, 定理 4.5.4 2c) より, すべてのガロア群は有限群で, すべての部分群および中間体は閉じている.

1) より φ が単射であり

$$|\,\mathrm{Im}(\varphi)| = |\,\mathrm{G}_F(E)| = [E : F]$$

であり

$$\left|\prod_{i\in I} \mathrm{G}_F(E_i)\right| = \prod_{i\in I} |\mathrm{G}_F(E_i)| = \prod_{i\in I} [E_i : F]$$

である. よって, φ が全単射であるための必要十分条件は $[E : F] = \prod_{i\in I} [E_i : F]$ であることになる. ゆえに, 系 4.7.3 5) により, 主張を得る. □

系 4.8.2. E/F がガロア拡大で, そのガロア群が

$$G = \mathrm{G}_F(E) = G_1 \times \cdots \times G_n$$

のような直積であるとする. このとき, G の部分群 H_i を

$$H_i = G_1 \times \cdots \times \{\iota\} \times \cdots \times G_n$$

とおき (ここで $\{\iota\}$ は第 i 成分 H_i の単位部分群),

$$E_i = \mathrm{fix}(H_i)$$

とする. このとき, 次が成り立つ.

1) E_i/F はガロア拡大で, そのガロア群について $\mathrm{G}_F(E_i) \simeq G_i$ である.
2) $E = E_1 \vee \cdots \vee E_n$
3) すべての $i = 1, \ldots, n$ に対して $E_i \cap (E_{i+1} \cdots E_{n+1}) = F$ である. ただし, $E_{n+1} = F$ とする.

証明. 1) H_i の形から $H_i = \mathrm{G}_{\mathrm{fix}(H_i)}(E)$ は $G = \mathrm{G}_F(E)$ の正規部分群で, 定理 4.5.4 1) より $E_i = \mathrm{fix}(H_i)$ も閉じている. $F \lhd E$ なので定理 4.6.3 2) により E_i/F は正規拡大であり, そのガロア群について

$$\mathrm{G}_F(E_i) \simeq \mathrm{G}_F(E)/\,\mathrm{G}_{E_i}(E) \simeq G/H_i \simeq G_i$$

となる.

2) さらに, 命題 4.5.2 3) より $\bigvee_i E_i$ は F 上ガロア拡大であり, 定理 4.4.3 より

$$\mathrm{G}_{\bigvee_i E_i}(E) = \bigcap \mathrm{G}_{E_i}(E) = \bigcap H_i = \{\iota\} = \mathrm{G}_E(E)$$

となる. 両辺の固定体を取ると $\bigvee_i E_i = E$ となる.

[20] 全射性は使われていないように見える.

3) よって

$$\mathrm{G}_F\left(\bigvee_i E_i\right) = G_F(E) = \prod_i G_i \simeq \prod_i \mathrm{G}_F(E_i)$$

となる. 定理 4.8.1 2) より $E_i \cap (E_{i+1}\cdots E_{n+1}) = F$ である.

□

4.9 正規閉包のガロア群

正規閉包のガロア群は合成体の特別な場合である.

定理 4.9.1. E/F が分離拡大とする.

1) もし

$$F \lhd K \lhd E \subseteq \mathrm{nc}(E/F)$$

とすると $\mathrm{G}_K(\mathrm{nc}(E/F))$ は

$$\prod_{\sigma\in\hom_F(E,\overline{E})} \mathrm{G}_K(\sigma E) = \prod_{\sigma\in\hom_F(E,\overline{E})} \sigma\,\mathrm{G}_K(E)\sigma^{-1}$$

の部分群と同型である.

2) 1) の条件のほかに, さらに E/F が有限次拡大ならば, 上の直積は有限個の直積である.

証明. 定理 3.8.2 より $N = \mathrm{nc}(E/F) = \bigvee_{\sigma\in\hom_F(E,\overline{E})} E^\sigma$ とおくことができるので

$$\mathrm{G}_K(N) = \mathrm{G}_K\left(\bigvee_{\sigma\in\hom_F(E,\overline{E})} E^\sigma\right)$$

である. E/K はガロア拡大だから, E^σ/K もガロア拡大である. よって, 定理 4.8.1 1) より $\mathrm{G}_K\left(\bigvee_{\sigma\in\hom_F(E,\overline{E})} E^\sigma\right)$ は $\prod_{\sigma\in\hom_F(E,\overline{E})} \mathrm{G}_K(E^\sigma)$ の部分群に同型である. 1) の残りの部分は, 定理 4.6.3 より導かれる.

2) については E/F が有限次拡大ならば

$$\left|\hom_F(E,\overline{E})\right| = [E:F]_s \le [E:F]$$

なので, 直積は有限直和である. □

4.10 アーベル拡大と巡回拡大

定義 4.10.1. E/F をガロア拡大とする. E/F のガロア群 $\mathrm{G}_F(E)$ がアーベル群 (可換群) のとき, E/F を **アーベル拡大 (abelian extension)** という. さらに, ガロア群 $\mathrm{G}_F(E)$ が巡回群のとき, E/F を **巡回拡大 (cyclic extension)** という.[21]

定理 4.10.2.

1) (アーベル拡大の合成体はアーベル拡大) 各 E_i/F ($^\forall i \in I$) がアーベル拡大ならば $\bigvee_{i\in I} E_i$ も F 上のアーベル拡大である.

2) (アーベル拡大/巡回拡大の lifting はアーベル拡大/巡回拡大) E/F がアーベル拡大 (resp. 巡回拡大) で, K/F が任意の拡大のとき, EK/K もアーベル拡大 (resp. 巡回拡大) である.

3) (アーベル拡大/巡回拡大の tower について) 体の拡大列 $F \subseteq K \subseteq E$ において, E/F がアーベル拡大 (resp. 巡回拡大) ならば K/F, E/K もアーベル拡大 (resp. 巡回拡大) である.

[21] E/F がアーベル拡大または巡回拡大というときは, E/F がガロア拡大であることを仮定する.

証明. 1) 定理 4.8.1 1) より $F \subseteq \bigvee_{i\in I} E_i$ のガロア群は $\prod_{i\in I} \mathrm{G}_F(E_i)$ の部分群に同型である. アーベル群の直積はアーベル群で, その部分群もアーベル群である.

2) 系 4.7.2 より, $\mathrm{G}_K(EK) \simeq \mathrm{G}_{E\cap K}(E)$ は $\mathrm{G}_F(E)$ の部分群に同型である. アーベル群 (resp. 巡回群) の部分群もアーベル群 (resp. 巡回群) である.

3) 命題 4.5.2 1) より E/K はガロア拡大であり, $\mathrm{G}_K(E)$ は $\mathrm{G}_F(E)$ の部分群である. また, 定理 4.6.3 2) より $F \lhd K$ であり $\mathrm{G}_F(K)$ は $\mathrm{G}_F(E)/$ であり, アーベル群 (resp. 巡回群) の部分群も剰余群もアーベル群 (resp. 巡回群) である.

□

一般に, アーベル拡大 (巡回拡大) は distinguished class ではない.

定理 4.10.3. もし, 体の拡大列

$$F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

において, 各拡大 F_{i+1}/F_i がアーベル拡大ならば, ガロア群 $\mathrm{G}_{F_1}(F_n)$ は可解群 (solvable group) である.[22]

証明. 体の拡大列

$$F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

各ステップ F_{i+1}/F_i がアーベル拡大とする. ガロア群を取ることにより, 群の拡大列

$$\{\iota\} = \mathrm{G}_{F_n}(F_n) \subseteq \mathrm{G}_{F_{n-1}}(F_n) \subseteq \cdots \subseteq \mathrm{G}_{F_1}(F_n)$$

が得られる. 部分列 $F_i \subseteq F_{i+1} \subseteq F_n$ を考えよう. $F_i \lhd F_{i+1}$ なので, 定理 4.6.3 2) より, $\mathrm{G}_{F_{i+1}}(F_n)$ は $\mathrm{G}_{F_i}(F_n)$ の正規部分群で

$$\mathrm{G}_{F_i}(F_n)/\mathrm{G}_{F_{i+1}}(F_n) \to \mathrm{G}_{F_i}(F_{i+1})$$

は群の単準同型である. ここで, $\mathrm{G}_{F_i}(F_{i+1})$ はアーベル群であるから, その部分群 $\mathrm{G}_{F_i}(F_n)/\mathrm{G}_{F_{i+1}}(F_n)$ もアーベル群である. したがって, 群の拡大列

$$\{\iota\} = \mathrm{G}_{F_n}(F_n) \lhd \mathrm{G}_{F_{n-1}}(F_n) \lhd \cdots \lhd \mathrm{G}_{F_1}(F_n)$$

において, 各ステップの商群はアーベル群である. 群論の用語を使えば, このような部分群の列は**アーベル群列 (abelian series)** という. アーベル群列をもつ群を**可解群 (solvable group)** という. □

[22] 群 G に有限の長さの部分群の列

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \cdots \supseteq G_n = \{\iota\}$$

で, $G_{i+1} \lhd G_i$ かつ G_i/G_{i+1} がアーベル群であるものが存在するとき, G を**可解群 (solvable group)** という.

第5章　代数的独立性

5.1　従属関係

この章では労力の節約のため, この節では, 形式的に述べることできる部分を抽出する.

定義 5.1.1. X を空でない集合, $\mathscr{P}(X)$ を X の部分集合全体とし, $\Delta \subseteq X \times \mathscr{P}(X)$ を X とその部分集合の間の二項関係とする. $(x, S) \in \Delta$ のとき, $x \prec S$ と書き, x は S に**従属する (dependent)** という. また, すべての $s \in S$ に対して $s \prec T$ が成り立つとき, $S \prec T$ と書き, S は T に**従属する (dependent)** という. このとき, 任意の $S, T, U \in \mathscr{P}(X)$ に対して $\prec$ が次の関係をみたすとき Δ は**従属関係 (dependence relation)** という.

1) (反射律 reflexivity)　$S \prec S$
2) (有限性公理 compactness)　$x \prec S$ ならば S のある有限部分集合 S_0 が存在して $x \prec S_0$
3) (推移率 transitivity)　$S \prec T$ かつ $T \prec U$ ならば $S \prec U$
4) (スタイニッツの交換公理 (Steinitz exchange axiom))　$x \prec S$ かつ $x \not\prec S \setminus \{x\}$ ならば $s \prec (S \setminus \{s\}) \cap \{x\}$

もし $x \not\prec S$ ならば x は S と独立であるという.

定義 5.1.2. 部分集合 $S \subseteq X$ に対して $s \in S$ が存在して $x \prec S \setminus \{s\}$ であるとき, S は**従属 (dependent)** であるという. そうでないとき, S は**独立 (independent)** であるという. 空集合は常に独立である.

補題 5.1.3.　1) $S \prec T$ ならば, T の任意の T を部分集合として含む集合 T' に対して $S \prec T'$ である.
2) 従属な集合を含む集合は従属である.
3) 独立な集合の部分集合は独立である.
4) S が従属な集合ならば, S の有限部分集合 S_0 で従属なものが存在する. すなわち S の任意の有限部分集合が独立ならば S は独立である.

証明.　1) 定義 5.1.1 1) より, $T' \prec T'$ で, よって $x \in T$ に対して $x \in T'$ だから $x \prec T'$ である. ゆえに $T \prec T'$ である. 定義 5.1.1 3) より, $S \prec T'$ である.
2) $S \subset T$ で, S が従属とすると, 定義 5.1.2 より, $^{\exists}s \in S$ が存在して $s \prec S \setminus \{s\}$ となる. このとき, $S \setminus \{s\} \subseteq T \setminus \{s\}$ なので 1) より $s \prec T \setminus \{s\}$ となり T は従属である.
3) 2) の対偶.
4) S が従属な集合ならば, $^{\exists}s \in S$ が存在して $s \prec S \setminus \{s\}$ となる. 定義 5.1.1 2) より, $S \setminus \{s\}$ の有限部分集合 S_1 が存在して $s \prec S_1$ となる. $S_0 = \{s\} \cup S_1$ とおけ. 後半は対偶.
□

定理 5.1.4. S が独立で $x \not\prec S$ ならば $S \cup \{x\}$ も独立である.

証明. $s \in S$ とする. もし $s \prec (S \cup \{x\}) \setminus \{s\}$ であったとすると, S は独立なので $s \not\prec S \setminus \{s\}$ だから, 定義 5.1.1 1) (スタイニッツの交換公理) より, $x \prec S$ となり矛盾する. よって $s \not\prec (S \cup \{x\}) \setminus \{s\}$ である. また, 明らかに $s \not\prec S = (S \cup \{x\}) \setminus \{x\}$ である. よって $S \cup \{x\}$ は独立である. □

定義 5.1.5. 部分集合 $B \subseteq X$ が**基底 (base)** とは, B が独立でかつ $X \prec B$ となること.

定理 5.1.6. X を空でない集合とし, $\prec$ を X の従属関係とする. このとき, 次が成り立つ.

1) $B \subseteq X$ が基底であるための必要十分条件は B が X の極大な独立集合であること
2) $X \subseteq X$ が基底であるための必要十分条件は B が $X \prec B$ である極小な集合であること

3) A が (空でもよい) 独立な集合, S は $X \prec S$ である集合で $A \subseteq S \subseteq X$ となっているとする. このとき, X の基底 B で, $A \subseteq B \subseteq S$ となるものが存在する.

証明. 1) まず B が基底とする. このとき, B は独立で, 任意の $x \in X \setminus B$ に対して, $x \prec B$ なので, $B \cup \{x\}$ は従属となり, B は独立な極大集合である.

逆に, B が独立な集合の中で極大であるとすると, 任意の $x \in X$ に対して $x \not\prec B$ ならば $B \cup \{x\}$ は独立なのでありえない. よって $x \prec B$ であり, $X \prec B$ だから B は基底である.

2) まず B が基底とする. このとき, $X \prec B$ である. また, もし B の真の部分集合 B_0 に対して $X \prec B_0$ となったとする. このとき $b_0 \in B \setminus B_0$ を取ると $b \prec B_0 \prec B \setminus \{b_0\}$ となり B の独立性に反する.

逆に, B が $X \prec B$ である集合の中で極小であるとする. もし, B が独立でないとすると $b \in B$ が存在して $X \prec B \prec B \setminus \{b\}$ となり, 極小であることに矛盾する.

3) Zorn の補題を使う. $A \subseteq B \subseteq S$ をみたす独立な X の部分集合 B 全体の集合を $\mathscr{B}$ とおく. $\mathscr{B}$ に包含関係で順序を入れる. このとき $(\mathscr{B}, \subseteq)$ が帰納的順序集合であることを示す.

> $\mathscr{C} = \{C_i\}$ が $\mathscr{B}$ の全順序部分集合とする. このとき, 定義 5.1.1 2) により $C = \bigcup C_i$ は独立である. また, 明らかに $A \subseteq B \subseteq S$ である. よって $C \in \mathscr{B}$ である.

よって, Zorn の補題より $\mathscr{B}$ に極大元 B が存在する. このとき B は独立である. また, $^\forall s \in S$ に対して $s \not\prec B$ ならば $B \cup \{s\}$ は独立となり, B の極大性に反するので $s \prec B$ である. よって $X \prec S \prec B$ となり, B は基底である.

□

補題 5.1.7. S が有限な従属集合で $A \subseteq S$ を独立な S の部分集合とする. このとき, $\alpha \in S \setminus A$ が存在して $S \prec S \setminus \{\alpha\}$ となる.

証明. 部分集合 $B \subseteq S \setminus A$ で $A \cup B$ が独立なものの中から極大なものを選ぶ.[1] このとき, 仮定より B は $S \setminus A$ の真部分集合で. $\alpha \in S \setminus (A \cup B)$ ならば $\alpha \prec A \cup B \prec S \setminus \{\alpha\}$ なので $S \prec S \setminus \{\alpha\}$ を得る. □

定理 5.1.8. X を空でない集合とし, $\prec$ を X の従属関係とする. このとき, 次が成り立つ.

1) B が $X \prec B$ である有限集合で, C が X の独立な集合ならば $|C| \leq |B|$ である.
2) X の任意の基底は同じ濃度をもつ.

証明. 1) $B = \{b_1, \ldots, b_m\}$ とし, $c_1 \in C$ を 1 つ選ぶ. $C_1 = \{c_1, b_1, \ldots, b_m\}$ とおくと. C_1 は, $A = \{c_1\}$ として, 補題 5.1.7 の条件をみたすので, 必要ならば適当に番号を付け替えて

$$X \prec C_1 \prec \{c_1, b_1, \ldots, b_{m-1}\}$$

となる. さらに, 任意の $c_2 \in C \setminus \{c_1\}$ に対して $C_2 = \{c_1, c_2, b_1, \ldots, b_{m-1}\}$ は, $A = \{c_1, c_2\}$ として, 補題 5.1.7 の条件をみたすので, また, 必要ならば適当に番号を付け替えて

$$X \prec C_2 \prec \{c_1, c_2, b_1, \ldots, b_{m-2}\}$$

とできる. この議論を繰り返すことによって, B の元が尽きる前に C の元を使い切れなければならない. なぜなら, もし, そうでなければ, C の真の部分集合 C' で $X \prec C'$ となるので C の独立性に矛盾する. よって, $|C||B|$ である. これより, C もまた有限集合である. もし, B と C が両方とも基底ならば, B と C の役割を入れ替えて $|B| = |C|$ となる.

2) B $\{b_i \,|\, i \in I\}$ と C が無限の基底とする. 任意の $c \in C$ に対して, 定義 5.1.1 2) より, $c \prec B$ なので 有限部分集合 $I_c \subseteq I$ が存在して $c \prec \{b_i \,|\, i \in I_c\}$ となる. これによって $c \mapsto I_c$ は C から I の有限部分集合への写像を決める. さらに, B が基底であることより

$$I = \bigcup_{c \in C} I_c$$

でなければ, ならない. なぜなら, もし, そうでないとすると $j \in I \setminus \bigcup_{c \in C} I_c$ を 1 つ選ぶと, 任意の $c \in C$ に対して

$$c \prec \{b_i \,|\, i \in I_c\} \prec B \setminus \{b_j\}$$

[1] S が有限集合なので元の数が最大のものを選ぶ.

となり, $b_j \prec C \prec B \setminus \{b_j\}$ であり, B が基底であることに矛盾する. したがって

$$|B| = |I| = \left| \bigcup_{c \in C} I_c \right| \leq |C|$$

である. B と C の役割を入れ替えることにより, 逆向きの不等式も示せて, $|B| = |C|$ となる.

□

5.2 代数的従属性

ここでは, 前の節で展開した「従属関係」の一般論を代数的従属性に適用する. まずは, 次の定義を再掲しよう.

定義 5.2.1. E/F を体の拡大とする. $t \in E$ が F 上代数的でないとき, t は F 上**超越的 (transcendental)** という. すなわち, 超越的とは $f(t) = 0$ となる 0 以外の多項式 $f(X) \in F[X]$ が存在しないことである.

定理 3.3.3 (i) より, t が超越的であるための必要十分条件は $F(t)$ が有理式体と同型であることであった.

定義 5.2.2. E/F を体の拡大とし, $S \subseteq E$ を部分集合とする. $\alpha \in E$ が $F(S)$ 上代数的であるとき, $\alpha \prec S$ と書き, α は F **上** S **に代数的従属している (algebraically dependent on** S **over** F**)** という. また, α が F 上 S に代数的従属ではないとき, すなわち, α が $F(S)$ 上超越的であるとき, $\alpha \not\prec S$ と書き, α は F **上** S **と代数的独立 (algebraically independent of** S **over** F**)** という.

基礎体 F に依存するので $\prec$ の代わりに $\prec_F$ と書くべきかもしれないが基礎体を入れ替えることは稀なので, 混乱のない限り, 単に $\prec$ と書く.

$\alpha \prec S$ は, 定義より α が $F(S)$ 上代数的なことであり, これは $F(S, \alpha)/F(S)$ が代数拡大であることと同値である. したがって, E/F が体の拡大で, $S \subseteq E$ が部分集合のとき, $A \prec S$ の必要十分条件は, 命題 3.4.5 より $F(S, A)/F(S)$ が代数拡大であることである. すなわち $A \prec S$ とは A が $F(S)$ 上代数的であることである.

定理 5.2.3. 代数的従属は, 従属関係である.

証明. 反射律 $S \prec S$ は自明である.

有限性公理を示す. $\alpha \prec S$ とすると α の $F(S)$ 上の最小多項式 $f(X)$ の係数全体の集合を $C \subseteq F(S)$ とおく. 各 $c \in C$ は S の有限個の元の有理関数であるから S の有限部分集合 S_0 が存在して $C \in F(S_0)$ となる. よって $\alpha \prec S_0$ となる.

次に, 推移率を示す. $S \prec T$ かつ $T \prec U$ とする. このとき, 拡大列

$$F(S) \subseteq F(S, T) \subseteq F(S, T, U)$$

の各拡大は代数拡大で, 定理 3.4.13 より, 全体も代数拡大になるから明らかである.

最後に, スタイニッツの交換公理を示す. $\alpha \prec S$ として, ある $s \in S$ に対して $\alpha \not\prec S \setminus \{s\}$. であるとする. 有限性公理より有限部分集合 $S_0 \subseteq S$ が存在して $\alpha \prec S_0$ となる. このとき $s \in S_0$ かつ $\alpha \not\prec S_0 \setminus \{s\}$ である.[2] このとき, $s \prec (S_0 \setminus \{s\}) \cup \{\alpha\}$ を示せば $s \prec (S \setminus \{s\}) \cup \{\alpha\}$ が示される.

ここで $\{s\}$ は独立である. なぜなら, もし s が F 上代数的ならば, 定理 3.4.13 より, 代数拡大は distinguished class だから Lifting property より S_0 は $S_0 \setminus \{s\}$ 上代数的である. よって, 拡大列 $F(S_0 \setminus \{s\}) \subseteq F(S_0) \subseteq F(S_0, \alpha)$ は代数拡大となり, 定理 3.4.13 の tower property より $\alpha \prec S_0 \setminus \{s\}$ ということになり矛盾する. 補題 5.1.7 を使って, $S_0 \setminus \{s\}$ の中のいくつかを取り除き, $S_0 \setminus \{s\}$ が代数的独立で, かつ $\alpha \prec S_0 \setminus \{s\}$ としてよい. このとき $S_1 = S_0 \setminus \{s\} = \{s_1, \ldots, s_m\}$ とおく. α の $F(S_0)$ 上の最小多項式を $f(X)$ とすると

$$f(X) = X^d + \sum_{i=0}^{d-1} \frac{f_i(s_1, \ldots, s_m, s)}{g_i(s_1, \ldots, s_m, s)} X^i$$

という形である. ここで $f_i(s_1, \ldots, s_m, s)$, $f_i(s_1, \ldots, s_m, s)$ は F 上の多項式である. このとき, 分母の積を

$$h(s_1, \ldots, s_m, s) = \prod_{i=1}^{d} g_i(s_1, \ldots, s_m, s)$$

[2] $s \notin S_0$ ならば推移律より $\alpha \prec S_0 \prec S \setminus \{s\}$ となり矛盾. また, $S_0 \ni s$ で $\alpha \prec S_0 \setminus \{s\}$ ならば推移律より $\alpha \prec S_0 \setminus \{s\} \prec S \setminus \{s\}$ となり, 矛盾する.

とおくと

$$h(s_1,\dots,s_m,s)f(X)=h(s_1,\dots,s_m,s)X^d+\sum_{i=0}^{d-1}h_i(s_1,\dots,s_m,s)\,X^i$$

となる. ここで $h(s_1,\dots,s_m,Y)$ も

$$h_i(s_1,\dots,s_m,Y)=h(s_1,\dots,s_m,Y)f_i(s_1,\dots,s_m,Y)$$

も $F(S_1)$ 上の多項式で $h(s_1,\dots,s_m,s)\neq 0$ である. $X=\alpha$ とすることにより

$$h(s_1,\dots,s_m,s)\alpha^d+\sum_{i=0}^{d-1}h_i(s_1,\dots,s_m,s)\,\alpha^i=0$$

である. ここで, 多項式 $h(s_1,\dots,s_m,Y),h_i(s_1,\dots,s_m,Y)\in F(S_1)[Y]$ が, すべて Y について定数であるとすると

$$h(s_1,\dots,s_m,0)\alpha^d+\sum_{i=0}^{d-1}h_i(s_1,\dots,s_m,0)\,\alpha^i=0$$

となり $\alpha\not\prec S_0\setminus\{s\}=S_1$ に反する. よって, 多項式

$$h(s_1,\dots,s_m,Y)\alpha^d+\sum_{i=0}^{d-1}h_i(s_1,\dots,s_m,Y)\,\alpha^i$$

は, Y に関して, 定数でなく, $F(S_1,\alpha)$ 上の Y 変数の多項式で $Y=s$ がみたす. よって

$$s\prec(S_0\setminus\{s\})\cup\{\alpha\}$$

ということが示された. □

したがって, 我々は前節の従属性の性質を使うことができる.

定義 5.2.4. E/F を拡大とする.

1) 部分集合 $S\subset E$ が F **上代数的従属 (algebraically dependent over F)** とは, ある元 $s\in S$ が存在して s が $F(S\setminus\{s\})$ 上代数的となることである. すなわち, これは $F(S)/F(S\setminus\{s\})$ が代数拡大であることである.
2) 部分集合 $S\subset E$ が F **上代数的独立 (algebraically independent over F)** とは, 任意の元 $s\in S$ に対して s が $F(S\setminus\{s\})$ 上超越的となることである. (定義より, 空集合は代数的独立である.)

もし, $F(S)/F$ が代数拡大ならば, もちろん S は F 上代数的従属である. なぜなら, 任意の $s\in S$ は F 上代数的だから $F(S\setminus\{s\})$ 上も代数的となる. 逆は, もちろん成り立たない. 例えば t が F 上超越的であるとき, $S=\{t,2t\}$ は F 上代数的従属である. しかし, $F\subseteq F(S)=F(t)$ は超越拡大である.

補題 5.2.5. X を空でない集合とし, $\prec$ を X の従属関係とする. このとき, 次が成り立つ.

1) 代数的従属な集合を含む任意の集合は代数的従属である.
2) 代数的独立な集合の任意の部分集合は代数的独立である.

証明. 補題 5.1.3 の 2) と 3) を使え. □

定理 5.2.6. S が F 上代数的に独立で α が $F(S)$ 上超越的ならば, $S\cup\{\alpha\}$ は F 上代数的である.

証明. 定理 5.1.4 を使え. □

5.3 代数的従属性と多項式関係

定義 5.3.1. E/F を拡大とする. 部分集合 $S \subseteq E$ が F **上非自明な多項式関係 (nontrivial polynomial relationship over F)** をもつとは, 0 でない多項式 $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ と S の相異なる元 $s_1, \ldots, s_n \in S$ が存在して $f(s_1, \ldots, s_n) = 0$ となることである. これは, ある元 $s \in S$ が存在して s が $S \setminus \{s\}$ の F 上の多項式環 $F[S \setminus \{s\}]$ 上代数的であるということである.

証明. 上の 2 つの定義が同値であることを示す. 0 でない多項式 $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ と S の相異なる元 $s_1, \ldots, s_n \in S$ が存在して $f(s_1, \ldots, s_n) = 0$ となるとする. $n = 1$ ならば, これは, 単に s_1 が F 上代数的であることを意味する. $n > 1$ として, $s_2, \ldots, s_n$ に関して, このような多項式は存在しないと仮定してよい. このとき, $s_1, \ldots, s_n \in S$ に関して, 自明でない多項式関係 $f(s_1, \ldots, s_n)$ が存在するとして.

$$f(X_1, \ldots, X_n) = \sum_{i=0}^{d} f_i(X_2, \ldots, X_n) X_1^i$$

と X_1 について整理しておき, $f_d(s_2, \ldots, s_n) \neq 0$ としてよい. このとき

$$g(X) = \sum_{i=0}^{d} f_i(s_2, \ldots, s_n) X_1^i$$

と書くことにすれば $g(s_1) = 0$ なので s_1 は $F[S \setminus \{s_1\}]$ 上代数的である. □

定理 5.3.2. E/F を拡大とする. E の部分集合 S が F 上代数的従属であるための必要十分条件は, S が F 上非自明な多項式関係をもつことである.

証明. S が代数的従属であることを示すには $^{\exists}s \in S$ が存在して s が $S \setminus \{s\}$ 上代数的であることを言えばよい. これは, s が $S \setminus \{s\}$ の生成する多項式環上で代数的であることに同値である. 一方向は自明である. なぜならば, 多項式は有理式であるからである. 逆方向を示すには s の $F(S \setminus \{s\})$ 上の最小多項式が, 次数 d の多項式

$$f(X) = \sum_{i=0}^{d} \frac{p_i(s_1, \ldots, s_m)}{q_i(s_1, \ldots, s_m)} X^i$$

をみたすとする. ここで $p_d(s_1, \ldots, s_m) \neq 0$ としておく. この式の両辺に分母を全部かけて得られる Q を掛けることによって s がみたず 0 でない多項式が得られる. □

5.4 超越基底

定義 5.4.1. E/F を拡大とする. E の部分集合 $B \subseteq E$ が F 上代数的独立で $E/F(B)$ が代数拡大のとき, B を E の F 上の**超越基底 (transcendence basis)** という.

証明. 定義 5.1.5, 定義 5.2.2, 定理 5.2.3 を見よ. □

定理 5.4.2. E/F を拡大とする. E の部分集合 $B \subseteq E$ が F 上の超越基底であるための必要十分条件は次の条件のいずれか一つが成り立つこと.

1) B は F 上の代数的独立な極大の集合である.
2) B は $E \prec B$ である極小の集合である. すなわち $F(B) \subseteq E$ が代数拡大であるような極小の集合である.

証明. 定理 5.1.6 1) 2) を見よ. □

定理 5.4.3. E/F を拡大とする.

1) E の F 上の基底の濃度は B の取り方に依存せず, 一定であり, これを $[E : F]_t$ と書き, E の F 上の**超越次元 (transcendence degree)** という.

2) A, S が $F \subseteq A \subseteq S \subseteq E$ である部分集合で, A が F 上代数的独立, $E/F(S)$ が代数拡大であるとき, E の F 上の超越基底 B で $A \subseteq B \subseteq S$ となるものが存在する. 特に, $[E:F]_t \leq |S|$ である.

証明. 定理 5.1.8, 定理 5.1.6 3) を見よ. □

定理 5.4.4. $F \subseteq K \subseteq E$ を拡大列とする.

1) $S \subseteq K$ が F 上代数的独立で, $T \subseteq E$ が K 上代数的独立ならば, $S \cup T$ は F 上代数的独立である.
2) S が K の F 上の超越基底で, T が E の K 上の超越基底ならば, $S \cup T$ は E の F 上の超越基底である.
3) 超越次元は加法的である. すなわち

$$[E:F]_t = [E:K]_t + [K:F]_t$$

証明. 1) を証明する. $S \cup T$ の F 上の多項式関係を関係を考えよう. 多項式

$$f(X_1, \ldots, X_n, Y_1, \ldots, Y_m) \in F[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$$

と互いに異なる元 $s_i \in S$, $t_j \in T$ が存在して, $f(s_1, \ldots, s_n, t_1, \ldots, t_m)) = 0$ となったとする. このとき

$$f(X_1, \ldots, X_n, Y_1, \ldots, Y_m)) = \sum_{j_1, \ldots, j_m} \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_m^{j_m}$$

とおく. ここで $a_{i_1, \ldots, i_n} \in F$ である. K 上の多項式

$$g(Y_1, \ldots, Y_m) = f(s_1, \ldots, s_n, Y_1, \ldots, Y_m)) = \sum_{j_1, \ldots, j_m} \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} s_1^{i_1} \cdots s_n^{i_n} Y_1^{j_1} \cdots Y_m^{j_m}$$

を考えると T は K 上代数的独立だから

$$\sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} s_1^{i_1} \cdots s_n^{i_n} = 0$$

であり, S は F 上代数的独立だから $a_{i_1, \ldots, i_n} = 0$ でなければならない.

2) については, 1) より $S \cup T$ は F 上代数的に独立であることと, $F(S) \subseteq K$ と $K(T) \subseteq E$ が代数的であることより, $F(S \cup T) \subseteq K(T) \subseteq E$ の各拡大は代数的であり, よって, 定理 3.4.13 より $F(S \cup T) \subseteq E$ は代数拡大である. よって $S \cup T$ は E の F 上の超越基底である.

3) は 2) から, すぐに出る. □

5.5 純粋超越拡大

定義 5.5.1. E/F を拡大とする. E の F 上の超越基底 B が存在して $E = F(B)$ となるとき, E は F 上**純粋超越的 (purely transcendental)** という.

定理 5.5.2. E/F が純粋超越拡大ならば, 任意の $E \setminus F$ の元 α は F 上超越的である.

定理 5.5.3. $F \subseteq K \subseteq E$ が拡大列で K/F が代数拡大とする. $T \subseteq E$ が F 上代数的独立ならば, T は K 上代数的独立である. すなわち, T は F のどんな代数拡大体の上でも代数的独立である.

5.6 有限生成拡大は distinguished class

定理 5.6.1. $F \subseteq K \subseteq E$ が拡大列とする. E が F 上有限生成ならば, K も F 上有限生成である.

第6章　多項式のガロア群

6.1　多項式のガロア群

多項式 $f(X) \in F[X]$ の最小分解体を S とするとき S の F 上のガロア群 $\mathrm{G}_F(E)$ を $\mathrm{G}_F(f(X))$ と書き, 多項式 $f(X)$ のガロア群という. $f_1(X), \ldots, f_n(X)$ が F 上の既約多項式として, $f(X)$ が

$$f(X) = f_1(X)^{e_1} \cdots f_n(X)^{e_n}$$

という形で書けるとすると S は $g(X) = f_1(X) \cdots f_n(X)$ の最小分解体でもある.

さらに, S/F が分離拡大 (よって, ガロア拡大) になるのは, 各 $f_i(X)$ が F 上分離的であるときである. S_i を $F \subseteq S_i \subseteq S$ となる $f_i(X)$ の F 上の最小分解体とする.[1] このとき, S/F が分離拡大ならば, 定理 3.12.1 (1) より, S_i/F は分離拡大であり, 各 $f_i(X)$ は分離的となる. 逆に, 各 $f_i(X)$ が分離的ならば定理 3.11.10 (1) (標数 0 のときは, 定理 3.13.3) より, S は F 上分離的な元で生成されるから E/F は分離拡大である.

S は F 上 $f(X)$ の根で生成されるので, 各 $\sigma \in \mathrm{G}_F(S)$ はこれらの根への作用で完全に決まり, 根の置換を引き起こす. よって $n = \deg f(X)$ とするとガロア群 $\mathrm{G}_F(S)$ は $\mathfrak{S}_n$ の部分群である. また, ガロア群 $\mathrm{G}_F(S)$ が可移的 (transtive)[2] であるための必要十分条件は $f(X)$ が既約であることである.

定理 6.1.1. $f(X), g(X), h(X) \in F[X]$ で $f(X) = g(X)h(X)$, $\deg g > 0$ とする. $g(X)$ の最小分解体を E_g とするとき

$$\mathrm{G}_F(g(X)) \simeq \mathrm{G}_F(f(X)) / \mathrm{G}_{E_g}(f(X))$$

である.

証明. $f(X)$ の F 上の最小分解体を E_f, $g(X)$ の F 上の最小分解体を E_g と書く. このとき, $F \subseteq E_g \subseteq E_f$, $F \lhd E_g$, $F \lhd E_f$ なので, 定理 4.6.3 1) より,

$$\mathrm{G}_F(E_g) \simeq \mathrm{G}_F(E_f) / \mathrm{G}_{E_g}(E_f)$$

である. □

6.2　対称多項式

この説では, 多項式の根と係数の関係について論じる. よく知られているように, 多項式の定数項は, 根の積であり, 最高次の次の項の係数は, 根の和のマイナスである.

F が体で $t_1, \ldots, t_n$ が F 上代数的独立のとき,

$$g(X) = \prod_{i=1}^{n} (X_i - t_i)$$

によって定義される n 次多項式を**一般多項式 (generic polynomial)** という. 根 $t_1, \ldots, t_n$ が F 上代数的独立なので, この一般多項式 $g(X)$ はある意味で最も一般的な多項式である. $g(X)$ を展開すると

$$g(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$$

となり, ここで

$$s_1 = \sum_i t_i, \quad s_2 = \sum_{i<j} t_i t_j, \quad s_3 = \sum_{i<j<k} t_i t_j t_k, \quad \ldots, \quad s_n = \prod_i t_i$$

を**基本対称式 (elementary symmetric polynomials)** とよぶ.

[1] F に $f_i(X)$ の S の根を添加した体が S_i

[2] 対称群 $\mathfrak{S}_n$ の部分群 G が**可移的 (transtive)** であるとは, 任意の $^\forall i, j$ $(1 \leq i, j \leq n)$ に対して $\sigma \in G$ が存在して $\sigma(i) = j$ となること.

補題 6.2.1. $f(X) \in F[X]$ を monic な多項式とする. このとき, $f(X)$ の係数は符号を除いて $f(X)$ の根の基本対称式である. すなわち, $f(X)$ の, その分解体における根を $r_1, \ldots, r_n$ とすると

$$f(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$$

と書ける. ここで

$$s_k = \sum_{i_1 < \cdots < i_k} r_{i_1} \cdots r_{i_1}$$

である. □

$t_1, \ldots, t_n$ が F 上代数的独立のとき, $F(t_1, \ldots, t_n)$ は $F(s_1, \ldots, s_n)$ 上の代数拡大なので, 次に述べるように, $s_1, \ldots, s_n$ も F 上代数的独立である. すなわち, このことは, 定理 5.3.2 より $s_1, \ldots, s_n$ の間に非自明な多項式関係がないことである.

定理 6.2.2. $t_1, \ldots, t_n$ が F 上代数的独立のとき, 基本対称式 $s_1, \ldots, s_n$ も F 上代数的独立である.

証明. 体の拡大列

$$F \subseteq F(s_1, \ldots, s_n) \subseteq F(t_1, \ldots, t_n)$$

において $t_1, \ldots, t_n$ は $F(s_1, \ldots, s_n)$ 上代数的なので $F(s_1, \ldots, s_n) \subseteq F(t_1, \ldots, t_n)$ は代数拡大なので, 定理 5.4.3 2) より $S = \{s_1, \ldots, s_n\}$ の中に $F(t_1, \ldots, t_n)$ の F 上の超越基底を取ることができる.[3] ところが, $\{t_1, \ldots, t_n\}$ は $F(t_1, \ldots, t_n)$ の F 上の超越基底であるから $[F(t_1, \ldots, t_n) : F]_t = n$ である. よって, やはり, 定理 5.4.3 2) より S は $F(t_1, \ldots, t_n)$ の F 上の超越基底であり, F 上代数的独立である. □

6.3 一般多項式のガロア群

代数拡大 $F(s_1, \ldots, s_n) \subseteq F(t_1, \ldots, t_n)$ のガロア群を計算する. $F(t_1, \ldots, t_n)$ は $F(s_1, \ldots, s_n)$ 上の

$$g(X) = \prod_{i=1}^{n} (X - t_i)$$

の最小分解体であるから, 正規拡大で $g(X)$ は重根を持たないので, 分離拡大である. よって

$$F(s_1, \ldots, s_n) \subseteq F(t_1, \ldots, t_n)$$

は有限次ガロア拡大で

$$|G| = [F(t_1, \ldots, t_n) : F(s_1, \ldots, s_n)] \leq n!$$

である.[4] G が対称群 $\mathfrak{S}_n$ に同型であることを証明する.

n 次対称群 $\mathfrak{S}_n$ の元 $\sigma \in \mathfrak{S}_n$ に対して $\sigma^* : F(t_1, \ldots, t_n) \to F(t_1, \ldots, t_n)$ を $f(t_1, \ldots, t_n) \in F(t_1, \ldots, t_n)$ に対して

$$\sigma^* \left(f(t_1, \ldots, t_n) \right) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$$

によって定義する. $t_1, \ldots, t_n$ が代数的に独立であることより, σ^* は well-defined である. さらに, σ^* は基本対称式 $s_1, \ldots, s_n$ を動かさない. よって, σ^* は $F(s_1, \ldots, s_n)$ を動かさない $F(t_1, \ldots, t_n)$ の自己同型である. すなわち $\sigma^* \in G$ で任意の $h(X_1, \ldots, X_n) \in F(s_1, \ldots, s_n)(X_1, \ldots, X_n)$ に対して

$$\sigma^* \left(h(t_1, \ldots, t_n) \right) = h(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$$

となる. さらに, 各 σ^* は互いに異なる. なぜなら $\sigma^* = \tau^*$ ならば $t_{\sigma(i)} = t_{\tau(i)}$ $(i = 1, \ldots, n)$ となり, $\sigma = \tau$ だからである. したがって G は n 次対称群 $\mathfrak{S}_n$ に同型で,

$$|G| = [F(t_1, \ldots, t_n) : F(s_1, \ldots, s_n)] = n!$$

が示された.

---

[3] $A = \emptyset$ とせよ.

[4] $K = F(s_1, \ldots, s_n)$ とおくとき, $\deg g = n$ より $[K(t_1) : K] \leq n$ であり, $K(t_1)$ 上で $g(X)$ は $g(X) = (X - t_1)h(X)$ と因数分解するので, $[K(t_1, t_2) : K(t_1)] \leq n - 1$ となる. この議論を繰り返す. または $\mathfrak{S}_n$ の部分群であることよりも従う.

定理 6.3.1. $t_1,\dots,t_n$ が F 上代数的独立とし, $s_1,\dots,s_n$ をその基本対称式とする. このとき, 次が成り立つ.

1) $F(t_1,\dots,t_n)$ は $F(s_1,\dots,s_n)$ 上のガロア拡大で, 拡大次数は $n!$ であり, そのガロア群 G は n 次対称群 $\mathfrak{S}_n$ に同型である.
2) $\mathrm{fix}(G) = F(s_1,\dots,s_n)$ である. すなわち, すべての σ^* ($^\forall\sigma \in \mathfrak{S}_n$) で不変な多項式は $s_1,\dots,s_n$ の有理式である.
3) $t_1,\dots,t_n$ の一般多項式 $g(X)$ は $F[s_1,\dots,s_n]$ 上既約である.

証明. 3) を証明するために, $g(X) = a(X)b(X)$ と因数分解したとする. ここで $\deg(a(X)) = d > 0$, $\deg(b(X)) = e > 0$ とすると

$$\deg(g(X)) \le d!e! < (d+e)! = n!$$

となり, 矛盾する. □

6.4 対称多項式

定義 6.4.1. $t_1,\dots,t_n$ が F 上代数的独立とする. 有理式 $f(t_1,\dots,t_n) \in F(t_1,\dots,t_n)$ が $t_1,\dots,t_n$ について**対称 (symmetric)** であるとは任意の $\sigma \in \mathfrak{S}_n$ に対して

$$f(t_{\sigma(1)},\dots,t_{\sigma(n)}) = f(t_1,\dots,t_n)$$

となることである. 言いかえると $f \in \mathrm{fix}(G) = F(s_1,\dots,s_n)$ となることである. ここで G は $F(t_1,\dots,t_n)/F(s_1,\dots,s_n)$ のガロア群である.

定理 6.4.2. (ニュートンの補題) $t_1,\dots,t_n$ が F 上代数的独立とし, $s_1,\dots,s_n$ をその基本対称式とする. このとき, 次が成り立つ.

1) 多項式 $f(t_1,\dots,t_n) \in F[t_1,\dots,t_n]$ が $t_1,\dots,t_n$ について対称であるための必要十分条件は多項式 $g(X_1,\dots,X_n) \in F[X_1,\dots,X_n]$ が存在して
$$f(t_1,\dots,t_n) = g(s_1,\dots,s_n)$$
となることである. さらに, $f(t_1,\dots,t_n)$ が整数係数ならば $g(X_1,\dots,X_n)$ も整数係数である.
2) $f(X) \in F(X)$ とする. このとき, $f(X)$ の根の F 係数の対称多項式の集合と $f(X)$ の係数の F 係数の多項式の集合は一致する. 特に, $f(X)$ の根の F 係数の対称多項式は F の元である.
3) $f(X) \in \mathbb{Z}(X)$ が整数係数の多項式とする. このとき, $f(X)$ の根の整数係数の対称多項式の集合と $f(X)$ の係数の整数係数の多項式の集合は一致する. 特に, $f(X)$ の根の整数係数の対称多項式は整数である.

証明. 2) と 3) は, 1) から, 補題 6.2.1 を使って導かれる. $f(t_1,\dots,t_n)$ が $g(s_1,\dots,s_n)$ の形をしていたら, 明らかに対称式である. 逆を示すためには, $g(X_1,\dots,X_n)$ を構成する. しかし, 残念ながら, この構成は帰納的で, 実際的ではない.

n に関する数学的帰納法を使う. $n = 1$ のときは, $t_1 = s_1$ だから, 明らかである. n より少ない個数の任意の個数の変数について, 定理が正しいとしよう. $f(t_1,\dots,t_n)$ を対称式として t_n の多項式として書くと

$$f(t_1,\dots,t_n) = f_0 + f_1 t_n + f_2 t_n^2 + \cdots + f_k t_n^k$$

という形になる. ここで, 各 f_i は $t_1,\dots,t_{n-1}$ の多項式である. $f(t_1,\dots,t_n)$ が $t_1,\dots,t_{n-1}$ について対称で, $t_1,\dots,t_n$ が代数的独立だから, 各 f_i は $t_1,\dots,t_{n-1}$ について対称である.[5] よって, 帰納法の仮定より, 各 f_i は $t_1,\dots,t_{n-1}$ の基本対称式の多項式である. ここで, $t_1,\dots,t_{n-1}$ の基本対称式を $u_1,\dots,u_{n-1}$ と書こう. このとき

$$f(t_1,\dots,t_n) = g_0 + g_1 t_n + g_2 t_n^2 + \cdots + g_k t_n^k \tag{6.4.1}$$

という形になる. ここで, 各 g_i は $u_1,\dots,u_{n-1}$ の多項式である. さらに, $f(t_1,\dots,t_n)$ が整数係数の多項式ならば, 帰納法の仮定により, 各 g_i も $u_1,\dots,u_{n-1}$ の整数係数の多項式になる.

[5] $\sigma \in \mathfrak{S}_{n-1}$ のとき, $f(t_{\sigma(1)},\dots,t_{\sigma(n-1)},t_n) = f(t_1,\dots,t_{n-1},t_n)$ だから $f_0^\sigma + f_1^\sigma t_n + f_2^\sigma t_n^2 + \cdots + f_k^\sigma t_n^k = f_0 + f_1 t_n + f_2 t_n^2 + \cdots + f_k t_n^k$ である. 代数的独立性より $f_0^\sigma = f_0,\dots,f_k^\sigma = f_k$ となる. すなわち, 各 f_i は $t_1,\dots,t_{n-1}$ の多項式である.

ここで,

$$\begin{aligned} s_1 &= u_1 + t_n \\ s_2 &= u_2 + u_1 t_n \\ &\cdots \\ s_{n-1} &= u_{n-1} + u_{n-2} t_n \\ s_n &= u_{n-1} t_n \end{aligned} \tag{6.4.2}$$

であることに注意しよう. この関係式を逆に解くと

$$\begin{aligned} u_1 &= s_1 - t_n \\ u_2 &= s_2 - u_1 t_n = s_2 - s_1 t_n + t_n^2 \\ u_3 &= s_3 - u_2 t_n = s_3 - s_2 t_n + s_1 t_n^2 - t_n^3 \\ &\cdots \\ u_{n-1} &= s_{n-1} - u_{n-2} t_n = s_{n-1} - s_{n-2} t_n + \cdots + (-1)^{n-1} t_n^{n-1} \end{aligned} \tag{6.4.3}$$

となる. また, (6.4.2) の最後の式から

$$0 = s_n - u_{n-1} t_n = s_n - s_{n-1} t_n + \cdots + (-1)^n t_n^n \tag{6.4.4}$$

を得る. ここで, これらの式を (6.4.1) 式に代入すると

$$f(t_1, \ldots, t_n) = h_0 + h_1 t_n + h_2 t_n^2 + \cdots + h_k t_n^k$$

ここで, 各 h_i は $s_1, \ldots, s_{n-1}, t_n$ の多項式になる. また, $f(X)$ が整数係数の多項式ならば, 各 h_i も整数係数の多項式になる. さらに, この式を, もう一度, t_n の多項式として, 整理しなおすと

$$f(t_1, \ldots, t_n) = r_0 + r_1 t_n + r_2 t_n^2 + \cdots + r_m t_n^m$$

となる. ここで各 r_i は $s_1, \ldots, s_{n-1}$ の多項式になる. また, $f(X)$ が整数係数の多項式ならば, 各 r_i も整数係数の多項式になる. もし, $m \geq n$ ならば (6.4.4) 式を使って, 次数を下げていくことによって, 最終的に,

$$f(t_1, \ldots, t_n) = p_0 + p_1 t_n + p_2 t_n^2 + \cdots + p_{n-1} t_n^{n-1} \tag{6.4.5}$$

とすることができる. ここで各 p_i は $s_1, \ldots, s_{n-1}, s_n$ の多項式になる. また, $f(X)$ が整数係数の多項式ならば, 各 p_i も整数係数の多項式になる.

(6.4.5) 式の左辺は, $t_1, \ldots, t_n$ に関する対称式だから, この式で t_n と t_i を交換することができて,

$$f(t_1, \ldots, t_n) = p_0 + p_1 t_i + p_2 t_i^2 + \cdots + p_{n-1} t_i^{n-1}$$

が, すべての $i = 1, \ldots, n$ について成り立つ. よって,

$$F(X) = p_0 + p_1 X + p_2 X^2 + \cdots + p_{n-1} X^{n-1} - f(t_1, \ldots, t_n)$$

は, X についての次数 $n-1$ の多項式であり, n 個の異なる根 $t_1, \ldots, t_n$ を持つので, 恒等的に 0 である. よって, $i = 1, \ldots, n-1$ に対して $p_i = 0$ であり, $f(t_1, \ldots, t_n) = p_0 = p_0(s_1, \ldots, s_n)$ となり, 求める結果を得る. □

6.5 代数学の基本定理

ガロア対応は代数学の基本定理の比較的簡単な証明に利用できる.

それはさておき, 代数学の基本定理の証明の歴史も興味深いものである. 代数学の基本定理の証明の試みは 1746 年にさかのぼる. ダランベールは複素数の幾何学的性質と連続性の概念を基礎として, 代数学の基本定理を証明したが, それは当時よく理解されなかった.

1799 年, ガウスは代数学の基本定理のこれまでに知られていたすべての証明に重大な過誤があることを示した. その批評の中でガウスは厳密な証明を生み出そうと試みた. しかし, ガウスの証明もやはりが過誤があるものだった. それはガウスが連続性の概念の完全な理解の欠如に直面したからだった. 1816 年には連続性の概念を最小限に抑えた第二の証明を発表した. それは, ある種の中間値の定理を使ったものだった.

しかし, ワイエルシュトラスが 1874 年に連続性の基本的性質を厳密に基礎付けるまで, この問題の完全な解決をみることはなかった. そのときに初めて, ダランベールの証明もガウスの第二証明も完全に厳密なものとなるのである. [6]

ここでも, 我々は中間値の定理を使う. すなわち $f(X)$ が実数係数の多項式で実数 $a < b$ に対して $f(a)$ と $f(b)$ が異符号ならば $a < c < b$ に $f(c) = 0$ となるものが存在するということである. これから奇数次の実数係数多項式には実根が存在することになり, $\mathbb{R}$ 上既約とはなりえない. したがって $\mathbb{R}$ 上の ($\mathbb{R}$ 自身以外の) 有限次拡大は必ず偶数次元である.

また, 任意の複素数の平方根が存在するという知識も仮定しなければならない. それは $z = re^{i\theta}$ という極座標表示を考えれば $z^{1/2} = r^{1/2}e^{i\theta/2}$ が z の平方根であるという事実に由来する. したがって, $\mathbb{C}$ には 2 次拡大体は存在しない.

定理 6.5.1. (代数学の基本定理 (The fundamental theorem of algebra)) $\mathbb{C}$ 係数の任意の多項式は $\mathbb{C}$ に根を持つ. すなわち, $\mathbb{C}$ は代数的閉体である.

証明. まず, この定理を実数係数の多項式について証明すれば十分であることを注意しよう. なぜなら, $f(X) \in \mathbb{C}[X]$ ならば, $g(X) = f(X)\overline{f}(X)$ は実数係数の多項式である. ここで, $\overline{f}(X)$ は各係数の複素共役を取った多項式である. もし, $g(X)$ が根 α を持てば, α は $f(X)$ か $\overline{f}(X)$ の根である. もし, α が $\overline{f}(X)$ の根であるときは, $\overline{\alpha}$ が $f(X)$ の根である. したがって, $f(X) \in \mathbb{R}[X]$ としてよい.

体の拡大列 $\mathbb{R} \subseteq \mathbb{C} \subseteq E$ を考えよう. ここで, E は 多項式 $h(X) = (X^2 + 1)f(X)$ の $\mathbb{R}$ 上の最小分解体である.[7] $[\mathbb{C} : \mathbb{R}] = 2$ なので $[E : \mathbb{R}]$ は, 2 の倍数で, $[E : \mathbb{R}] = 2^k m$ ($k \geq 1$, m は奇数) としてよい. よって, 目標は $E = \mathbb{C}$, すなわち $f(X)$ は $\mathbb{C}$ 上で分解することを示すことである.

H を $\mathrm{G}_{\mathbb{R}}(h(X))$ の 2-Sylow 群 [8] としよう. このとき, $|H| = 2^k$ であり,

$$[\mathrm{fix}(H) : \mathbb{R}] = (\mathrm{G}_{\mathbb{R}}(h(X)) : H) = m$$

である. ところが, $\mathbb{R}$ 上の ($\mathbb{R}$ 自身以外の) 有限次拡大は必ず偶数次元であることから, $m = 1$ すなわち $\mathrm{fix}(H) = \mathbb{R}$ でなければならない. よって $G = \mathrm{G}_{\mathbb{R}}(h(X))$ は位数が $2^k \geq 2$ の 2-群である.

したがって, 拡大列

$$\{\iota\} \subseteq \mathrm{G}_{\mathbb{C}}(h(X)) \subsetneq G = \mathrm{G}_{\mathbb{R}}(h(X))$$

を考えると $|\mathrm{G}_{\mathbb{C}}(h(X))| = 2^{k-1}$ である. よって, 有限群に関する定理 [9] から 2^{k-1} を割る任意の 2 の冪に位数が等しい $\mathrm{G}_{\mathbb{C}}(h(X))$ の部分群が存在する. ところが, $\mathrm{G}_{\mathbb{C}}(h(X))$ には, 位数が 2^{k-2} (すなわち, 指数が 2) の部分群は存在しえないことを示すことができる. 実際, 位数が 2^{k-2} である部分群 J があるとする. このとき

$$\{\iota\} \subseteq J \subsetneq \mathrm{G}_{\mathbb{C}}(h(X)) \subsetneq G$$

で, $(\mathrm{G}_{\mathbb{C}}(h(X)) : J) = |\mathrm{G}_{\mathbb{C}}(h(X))| / |J| = 2$ である. この場合には,

$$2 = (\mathrm{G}_{\mathbb{C}}(h(X)) : J) = [\mathrm{fix}(J) : \mathrm{fix}\,(\mathrm{G}_{\mathbb{C}}\,(h(X)))] = [\mathrm{fix}(J) : \mathbb{C}]$$

となるので, $\mathrm{fix}(J)$ は $\mathbb{C}$ の 2 次の拡大であるが, $\mathbb{C}$ の 2 次拡大体は存在しないという, 先に述べた事実に矛盾する. したがって, $k = 1$ で, $|\mathrm{G}_{\mathbb{C}}\,(h(X))| = 1$, $|G| = 2$ なので $[E : \mathbb{R}] = 2$ となり, $E = \mathbb{C}$ という結論を得る. □

---

[6] It seems that attempts to prove the fundamental theorem began with d'Alembert in 1746, based on geometric properties of the complex numbers and the concept of continuity, which was not well understood at that time.

In 1799, Gauss gave a critique of the existing "proofs" of the fundamental theorem, showing that they had serious flaws, and attempted to produce a rigorous proof. However, his proof also had gaps, since he suffered from the aforementioned lack of complete understanding of continuity. Subsequently, in 1816, Gauss gave a second proof that minimized the use of continuity, assuming a form of the intermediate value theorem.

It was not until Weierstrass put the basic properties of continuity on a rigorous foundation, in about 1874, that d'Alembert's proof and the second proof of Gauss could be made completely rigorous

[7] ここで $\mathbb{C}$ は X^2+1 の $\mathbb{R}$ 上の最小分解体と考える. 標数 0 なので, $E/\mathbb{R}$ は有限次ガロア拡大で, 中間体も部分群も完全に閉じているので, $\mathrm{fix}\,(\mathrm{G}_{\mathbb{R}}\,(h(X))) = \mathbb{R}$, $\mathrm{fix}\,(\mathrm{G}_{\mathbb{C}}\,(h(X))) = \mathbb{C}$ である.

[8] 与えられた素数 p に対する p-群（p-group）とは, 任意の元の位数が p の冪になっているようなねじれ群をいう. 有限群の場合には, p-群であることと, その群の位数が p の冪であることとは同値になる. 群 G の p-Sylow 部分群とは, G の極大 p-部分群である. Sylow の定理は有限群 G の位数の任意の素因数 p に対して, G の p-Sylow 部分群が存在するというものである.

[9] 群 G の位数 $|G|$ が素数 p のベキ p^r で割り切れるならば, 位数が p^r であるような G の部分群が存在する.

6.6 多項式の判別式

n 次の多項式 $f(X) \in F[X]$ のガロア群 $\mathrm{G}_F(f(X))$ は n 次対称群 $\mathfrak{S}_n$ の部分群に同型であり, また, 一般多項式 $g(X)$ のガロア群は $\mathfrak{S}_n$ 自身に同型であることは既に見た. この節では, ガロア群 $\mathrm{G}_F(f(X))$ が交代群 $\mathfrak{A}_n$ の部分群に同型かどうかを判別する道具を与える, 判別式という根の対称式を定義する.

$f(X) \in F[X]$ を F 係数の n 次の多項式とし, $r_1, \ldots, r_n$ を $f(X)$ の F 上の最小分解体 E における根とする.

$$\delta = \prod_{i<j}(r_i - r_j)$$

とおくとき, $\Delta = \delta^2$ を $f(X)$ の**判別式 (discriminant)** という. Δ は, 明らかに, 根の対称式である. また $\Delta \neq 0$ と $f(X)$ が重根を持たないことは同値である.

$\Delta \neq 0$ と仮定しよう. このとき $f(X)$ は相異なる分離的な既約多項式の積である. また, E/F はガロア拡大 [10] であり, 有限次拡大だから ($\mathscr{F}$ も $\mathscr{G}$ も完全に閉じているので)

$$\mathrm{fix}(\mathrm{G}_F(f(X))) = F$$

である. ここで, $^\forall\sigma \in \mathrm{G}_F(f(X))$ に対して $\Delta^\sigma = \Delta$ なので $\Delta \in F$ である. (ニュートンの補題からも $\Delta \in F$ がいえる.)

任意の互換 [11] は δ を $-\delta$ に移すので $\sigma \in \mathrm{G}_F(f(X))$ に対して

$$\delta^\sigma = \mathrm{sgn}\,\sigma \cdot \delta$$

が成り立つ. ここで $\mathrm{sgn}\,\sigma$ は σ の符号, すなわち, 偶置換には $+1$, 奇置換には -1 を対応させる写像である. よって $\delta \in F$ かどうかは, ガロア群の元 (置換) の parity に関する情報を我々に与える. ただし, $\mathrm{ch}(F) = 2$ のときは, 常に $\delta^\sigma = \delta$ で, $\delta \in F$ なので, 何の情報も得られない. しかし, $\mathrm{ch}(F) \neq 2$ のときは, $\sigma \in \mathrm{G}_F(f(X))$ が δ を固定する (i.e., $\delta^\sigma = \delta$) ための必要十分条件は σ が偶置換であることと言える. 言い換えると, $\delta \in F = \mathrm{fix}\,(\mathrm{G}_F\,(f(X)))$ であるための必要十分条件は $\mathrm{G}_F\,(f(X))$ が偶置換だけを含むということ, すなわち $\mathrm{G}_F\,(f(X)) \subseteq \mathfrak{A}_n$ であることである.

また, 一方, $\delta \notin F$ ならば $\mathrm{G}_F\,(f(X))$ には, 奇置換が必ず含まれる.[12] 対称群 $\mathfrak{S}_n$ の部分群 G が奇置換を含むならば, G は必ず偶数位数で, G は奇置換と偶置換を同数含むということを示すのは難しくない.[13]

したがって, $\delta \notin F$ のとき, $G = \mathrm{G}_F\,(f(X))$ は偶数位数で, $|G \cap \mathfrak{A}_n| = |G|/2$ となり

$$(G : G \cap \mathfrak{A}_n) = 2$$

である. $f(X)$ の最小分解体を E と書くと, E/F は有限次拡大だから, 定理 4.5.4 2c) より, 全ての部分群は閉じているので $\mathrm{G}_{\mathrm{fix}(G\cap\mathfrak{A}_n)}(E) = \mathrm{fix}\,(G \cap \mathfrak{A}_n)$ である. ゆえに

$$[\mathrm{fix}\,(G \cap \mathfrak{A}_n) : F] = (\mathrm{G}_F(E) : \mathrm{G}_{\mathrm{fix}(G\cap\mathfrak{A}_n)}(E)) = (G : G \cap \mathfrak{A}_n) = 2$$

となる. $[F(\delta) : F] = 2$ かつ [14] $F(\delta) \subseteq \mathrm{fix}\,(G \cap \mathfrak{A}_n)$ だから [15]

$$F(\delta) = \mathrm{fix}\,(G \cap \mathfrak{A}_n)$$

である. したがって, $F(\delta)$ は $G = \mathrm{G}_F\,(f(X))$ の偶置換全体の固定体である. 以上をまとめると次の定理を得る.

定理 6.6.1. $f(X) \in F[X]$ を F 係数の n 次の多項式とし, E を $f(X)$ の F 上の最小分解体とする. $\sqrt{\Delta}$ を $f(X)$ の判別式の (任意の) 平方根とする. このとき, 次が成り立つ.

1) $\Delta = 0$ は $f(X)$ が E において重根を持つための必要十分条件である.

2) $\Delta \neq 0$ かつ $\mathrm{ch}(F) \neq 2$ とする. このとき, 次が成り立つ.

[10] $\Delta \neq 0$ より分離的で, 最小分解体だから, 定理 3.7.6, 定義 3.7.7 より正規拡大である.

[11] 置換のうち, 特に二つの元のみを入れ替えて他の元は変えないものを互換 (transposition) という.

[12] $f(X)$ は分離的な既約多項式の積だから, 同じ既約成分の根を r, s とするとき, 互換 (r, s) はガロア群の元である.

[13] $\mathfrak{S}_n$ の部分群 G に対して, G に含まれる奇置換の 1 つを σ_0 とする. このとき, $H = \mathfrak{A}_n \cap G$ は G の部分群であり $G = H \cup \sigma_0 H$ は剰余類 G/H を与えので $|H| = |\sigma_0 H|$, $2|H| = |G|$ である.

[14] $\delta^2 = \Delta \in F$ かつ $\delta \notin F$ より, δ は最小多項式 $X^2 - \Delta \in F[X]$ の根である.

[15] $\sigma \in G$ が偶置換のときは $\delta^\sigma = \delta$ なので $\delta \in \mathrm{fix}\,(G \cap \mathfrak{A}_n)$ である. よって $F(\delta) \subseteq \mathrm{fix}\,(G \cap \mathfrak{A}_n)$.

a) $\sqrt{\Delta} \in F$ ならば $\mathrm{G}_F(f(X))$ は交代群 $\mathfrak{A}_n$ の部分群に同型である. また, 逆も成り立つ.

b) $\sqrt{\Delta} \notin F$ ならば $\mathrm{G}_F(f(X))$ は対称群 $\mathfrak{S}_n$ の部分群に同型であり, かつ, $\mathrm{G}_F(f(X))$ の元の半分は奇置換で, 残りの半分は偶置換である. また, 逆も成り立つ.

3) $\Delta \neq 0$ かつ $\mathrm{ch}(F) = 2$ とする. このとき, $\sqrt{\Delta} \in F$ であっても $\mathrm{G}_F(f(X))$ は交代群 $\mathfrak{A}_n$ の部分群に同型であるとは限らない.

証明. 3) の証明は, generic な多項式 $g(X) = (X - t_1)\cdots(X - t_n)$ の $F(s_1, \ldots, d_n)$ 上のガロア群が $\mathfrak{S}_n$ であることを使え. □

定理 6.6.1 の便利さは. 判別式 Δ が $f(X)$ の根を具体的に求めなくても, 計算できる点である. 実際, δ は Vandermonde の行列式

$$\delta = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ r_1 & r_2 & \ldots & r_n \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{n-1} & r_2^{n-1} & \ldots & r_n^{n-1} \end{vmatrix}$$

なので, この行列式の転置をかけることによって Δ はハンケル行列式

$$\Delta = \delta^2 = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ r_1 & r_2 & \ldots & r_n \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{n-1} & r_2^{n-1} & \ldots & r_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & r_1 & \ldots & r_1^{n-1} \\ 1 & r_2 & \ldots & r_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & r_n & \ldots & r_n^{n-1} \end{vmatrix} = \begin{vmatrix} u_0 & u_1 & \ldots & u_{n-1} \\ u_1 & u_2 & \ldots & u_n \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-1} & u_n & \ldots & u_{2n-2} \end{vmatrix}$$

になる. ここで, $u_i = r_1^i + \cdots + r_n^i$ とする. 各 u_i は対称式なので, 基本対称式 ($f(X)$ の係数) で書くことができる.[16]

6.7 小さい次数の多項式のガロア群

この節では, 小さい次数の多項式のガロア群について調べる.

6.7.1 2 次多項式のガロア群

$f(X) \in F[X]$ が monic な 2 次多項式ならば

$$f(X) = X^2 + bX + c = (X - r)(X - s)$$

と書ける. ここで $a, b \in F$ であり, 最右辺は $f(X)$ の最小分解体 $E = F(r, s)$ の中での因数分解とする. 判別式を計算するには $u_1 = r + s = s_1 = -b$ と

$$u_2 = r^2 + s^2 = (r + s)^2 - 2rs = s_1^2 - 2s_2 = b^2 - 2c$$

[16] Macdonald の本 [7] によると, $k \geq 1$ のとき, u_k は

$$u_k = \begin{vmatrix} s_1 & 1 & 0 & \ldots & 0 \\ 2\,s_2 & s_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k\,s_k & s_{k-1} & s_{k-2} & \ldots & s_1 \end{vmatrix}$$

のように k 次の行列式で書ける. ここで s_i は i 次の基本対称式であり, $i > n$ のときは $s_i = 0$ とする (n は変数の個数). また, $u_0 = n$ を使うと, 判別式はすべて係数で書ける. 例えば, $n = 2$ のとき,

$$\Delta = \begin{vmatrix} u_0 & u_1 \\ u_1 & u_2 \end{vmatrix}$$

である. さらに, $u_0 = 2$, $u_1 = s_1$, $u_2 = \begin{vmatrix} s_1 & 1 \\ 2\,s_2 & s_1 \end{vmatrix} = s_1^2 - 2\,s_2$ を使うと, 2 次式の判別式は

$$\Delta = \begin{vmatrix} 2 & s_1 \\ s_1 & s_1^2 - 2\,s_2 \end{vmatrix} = s_1^2 - 4\,s_2$$

となる.

を使う. したがって

$$\Delta = \begin{vmatrix} 2 & -b \\ -b & b^2 - 2c \end{vmatrix} = b^2 - 4ac$$

となり, 中学校より慣れ親しんだ公式を得る.

重根をもつ場合

もし, $\Delta = 0$ ならば $f(X)$ は重根 r をもち

$$f(X) = (X - r)^2 = X^2 - 2rX + r^2$$

となる. このことから, ほとんどの振る舞いの良い基礎体 F について $r \in F$ であることがわかる. 実際, $\mathrm{ch}(F) \neq 2$ ならば $-2r \in F$ より, $r \in F$ となる. $\mathrm{ch}(F) = 2$ の場合も, (例えば F が有限体の場合のように) F が完全体ならば, $f(X) = (X - r)^2$ は非分離的なので既約多項式ではありえない. よって $X - r \in F[X]$ で, $r \in F$ でなければならない.

しかし, 次にあげる例のように, r が F に含まれない場合も有り得る. t を $\mathbb{F}_2$ 上超越的な元として, $F = \mathbb{F}_2(t^2)$ とおく.

$$f(X) = X^2 - t^2 = (X - t)^2$$

を考える. $t \notin \mathbb{F}_2(t^2)$ なので $f(X)$ は $\mathbb{F}_2(t^2)$ 上の既約多項式で, 重根 $t \notin \mathbb{F}_2(t^2) = F$ をもつ. よって, $\mathbb{F}_2(t)/F$ は純粋非分離拡大で, この場合もガロア群は $\{\iota\}$ である.

重根をもたない場合

$\Delta \neq 0$ の場合, $f(X)$ は相異なる 2 つの根をもち, 次の 2 つに場合分けされる.[17]

1) 2 根が共に F に含まれるならば, $f(X)$ は F 上可約で, ガロア群 $\mathrm{G}_F(f(X))$ は単位元のみから成る.[18]
2) 2 根が F に含まれない場合は $f(X)$ は既約である.[19] また, $\mathrm{G}_F(f(X)) \simeq \mathfrak{S}_2$ で, ガロア群は根の置換 (r, s) で生成される.[20]

さらに, $\mathrm{ch}(F) \neq 2$ のときには, $f(X)$ の根が F に含まれるかどうかを, 判別式の値を調べることによって判別できる. それは, $\mathrm{ch}(F) \neq 2$ のとき, 2 次方程式の根の公式

$$r, s = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-b \pm \sqrt{\Delta}}{2}$$

が使えるからである. すなわち, $\mathrm{ch}(F) \neq 2$ として, $\sqrt{\Delta} \notin F$ ならば, 根の公式から $r, s \notin F$ でなければならない [21] ので, 上の 2) のケースとなり, $\mathrm{G}_F(f(X)) \simeq \mathfrak{S}_2$ と結論できる. また, $\mathrm{ch}(F) \neq 2$ として, $\sqrt{\Delta} \in F$ ならば, 根の公式から $r, s \in F$ であり, 上の 1) のケースとなり, $\mathrm{G}_F(f(X)) \simeq \{\iota\}$ である. したがって, 以上をまとめると, 次の定理を得る.

定理 6.7.1. $f(X) \in F[X]$ を F 係数の 2 次の多項式とする. このとき, 次が成り立つ.

1) $\Delta = 0$ ならば $f(X) = (X - r)^2$ という形で r が重根である. このとき, $\mathrm{ch}(F) \neq 2$ か, または F が完全体ならば $r \in F$ である. いずれの場合 [22] も $\mathrm{G}_F(f(X)) = \{\iota\}$ である.
2) $\Delta \neq 0$ ならば $f(X)$ は相異なる 2 根をもち, 次のいずれかが成り立つ.
   a) 2 根が共に F に含まれ, $f(X)$ は可約で $\mathrm{G}_F(f(X)) = \{\iota\}$ である.
   b) 2 根がどちらも F に含まず, $f(X)$ は既約である. また, $\mathrm{G}_F(f(X)) \simeq \mathfrak{S}_2$ で, ガロア群は根の置換 (r, s) で生成される.

   $\mathrm{ch}(F) \neq 2$ のときは, 上の 2 つの場合は, 次のようにして判別できる. $\sqrt{\Delta} \in F$ ならば a) となり, $\sqrt{\Delta} \notin F$ ならば b) である.

---

[17] もし, $r \in F$ ならば, 系 2.1.6 を使って, $X - s \in F[X]$ も言えるので, r も s も F に含まれる. 同様にして, $r \notin F$ ならば $s \notin F$ である. したがって $f(X)$ の根は, 両方とも F に含まれるか, または, 両方とも F に含まれないかの 2 通りの場合分けしかない. よって, 次の 1) 2) に分けられる.

[18] $r, s \in F$ のときは, $E = F$ で $\mathrm{G}_F(f(X)) = \mathrm{G}_F(E) = \{\iota\}$.

[19] 2 次式なので, 可約とすると 1 次の因子を持ち, 根が F に含まれる.

[20] ガロア群は $\mathfrak{S}_2$ の部分群であるが, 単位群ではありえない ($\because |G| = [E : F] = 2$) ので, $\mathfrak{S}_2$ 自身である.

[21] もし, $r \in F$ とすると $\sqrt{\Delta} \in \pm(2r + b) \in F$ となり, 矛盾である.

[22] $\mathrm{ch}(F) = 2$ で F が完全体でなくてもよい. 1) のときは, 常にという意味.

6.7.2 3 次多項式のガロア群

3 次多項式

$$f(X) = X^3 + bX^2 + cX + d = (X - r)(X - s)(X - t) \in F[X]$$

の最小分解体を E とする.[23] 3 次多項式なので, 既約であるか, 既約な 2 次式と 1 次式の積か, 3 つの 1 次式の積とになる. ゆえに, $f(X)$ が可約であれば, 必ず 1 次の因子をもつので, $f(X)$ が既約であるための必要十分条件は, $f(X)$ が F で根をもつことである.

$f(X)$ が F で 3 つの 1 次式の積に分解すれば [24], $E = F$ で, そのガロア群は $\{\iota\}$ である.

$f(X)$ が可約であるが F で 1 次式の積に分解しない [25] とすれば,

$$f(X) = (X - \alpha)(X^2 + pX + q)$$

の形をしていて, ここで, $\alpha \in F$ かつ $g(X) = X^2 + pX + q$ は F 上既約である. よって, E は $g(X)$ の F 上の最小分解体なので $[E : F] = 2$ であり, 定理 6.7.1 より, 次の 2 つの場合がある.

1) $\Delta = 0$, $\mathrm{ch}(F) = 2$ かつ $f(X) = (X - r)^2 = X^2 - r^2$, $r \notin F$, $r^2 \in F$ で, E/F は純粋非分離拡大である. このとき, ガロア群は $\mathrm{G}_F(g(X)) = \{\iota\}$ となる.
2) $\Delta \neq 0$ のとき, そのガロア群は $\mathrm{G}_F(g(X)) \simeq \mathfrak{S}_2$ と同型である.

以上で, 可約な場合は尽くしたので, 以下, $f(X)$ を既約としよう. 長い面倒な計算をすれば

$$\Delta = -4\,b^3d + b^2c^2 + 18\,bcd - 4\,c^3 - 27\,d^2$$

であることがわかる.[26] もし, $\Delta = 0$ ならば, $f(X)$ が既約であるから, 系 3.10.5 より, 全ての根の重複度は等しいので, $\mathrm{ch}(F) = 3$ で

$$f(X) = (X - r)^3 = X^3 - r^3$$

しかありえない. よって, $E = F(r)/F$ は 3 次の純粋非分離拡大で, 補題 3.6.9 より, そのガロア群は $\{\iota\}$ である. $\Delta \neq 0$ ならば $f(X)$ は重根をもたないので分離的である. よって, E/F はガロア拡大であり, そのガロア群は $\mathfrak{S}_3$ の部分群に同型なので, $|\,\mathrm{G}_F(f(X))|$ は $\mathfrak{S}_3$ の位数 $3! = 6$ の約数である. また, (定理 4.5.4 より, $|\,\mathrm{G}_F(f(X))| = [E : F]$ で), $f(X)$ が既約だから, $\mathrm{G}_F(f(X))$ は可移的であり, (可移的部分群の性質から)

$$3 \leq |\,\mathrm{G}_F(f(X))| = [E : F] \leq 3!$$

なので $|\,\mathrm{G}_F(f(X))| = [E : F] = 3$ または $|\,\mathrm{G}_F(f(X))| = [E : F] = 6$ である. 以下の定理は, 3 次多項式のガロア群の完全な分類を与える. また, $\mathrm{ch}(F) \neq 2$ の場合は, $f(X)$ が既約か可約かという情報と $\sqrt{\Delta}$ の値が F に属するか否かという情報によって, 3 次多項式のガロア群と最小分解体が完全に決定されることに注意しておこう.

---

[23] 右端の因数分解は, 最小分解体 E においてである.
[24] $r, s, t \in F$ ということ.
[25] 既約な 2 次式と 1 次式の積ということ
[26] $n = 3$ のとき Δ は

$$\Delta = \begin{vmatrix} u_0 & u_1 & u_2 \\ u_1 & u_2 & u_3 \\ u_2 & u_3 & u_4 \end{vmatrix}$$

である. ここで, $u_0 = 3$, $u_1 = s_1 = -b$, $u_2 = \begin{vmatrix} s_1 & 1 \\ 2\,s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 \\ 2\,c & -b \end{vmatrix} = b^2 - 2\,c$, $u_3 = \begin{vmatrix} s_1 & 1 & 0 \\ 2\,s_2 & s_1 & 1 \\ 3\,s_3 & s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 & 0 \\ 2\,c & -b & 1 \\ -3\,d & c & -b \end{vmatrix} = -b^3 + 3\,bc - 3\,d$,

$$u_4 = \begin{vmatrix} s_1 & 1 & 0 & 0 \\ 2\,s_2 & s_1 & 1 & 0 \\ 3\,s_3 & s_2 & s_1 & 1 \\ 4\,s_4 & s_3 & s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 & 0 & 0 \\ 2\,c & -b & 1 & 0 \\ -3\,d & c & -b & 1 \\ 0 & -d & c & -b \end{vmatrix} = b^4 - 4\,b^2c + 4\,bd + 2\,c^2$$

を使うと

$$\Delta = \begin{vmatrix} 3 & -b & b^2 - 2\,c \\ -b & b^2 - 2\,c & -b^3 + 3\,bc - 3\,d \\ b^2 - 2\,c & -b^3 + 3\,bc - 3\,d & b^4 - 4\,b^2c + 4\,bd + 2\,c^2 \end{vmatrix} = -4\,b^3d + b^2c^2 + 18\,bcd - 4\,c^3 - 27\,d^2$$

である.

定理 6.7.2. 3 次多項式 $f(X)$ の最小分解体を E, そのガロア群を $G = \mathrm{G}_F(f(X))$ とする. また, 判別式が $\Delta \neq 0$ のとき, 次の 4 つの場合のどれか 1 つだけが排他的に起こる. また, それぞれが 4 つの同値な条件で特徴付けられる.[27]

1) a) $[E : F] = 1$
   b) $E = F$ が $f(X)$ の最小分解体である.
   c) $\mathrm{G}_F(f(X)) = \{\iota\} \simeq A_2$
   d) ($\mathrm{ch}(F) \neq 2$ のとき) $f(X)$ は可約, かつ $\sqrt{\Delta} \in F$
2) a) $[E : F] = 2$
   b) $f(X)$ は可約で, $f(X)$ の根 $r \notin F$ が存在して $E = F(r)$ が $f(X)$ の最小分解体となる.
   c) $\mathrm{G}_F(f(X)) = \{\iota\} \simeq A_2$
   d) ($\mathrm{ch}(F) \neq 2$ のとき) $f(X)$ は可約, かつ $\sqrt{\Delta} \notin F$
3) a) $[E : F] = 3$
   b) $f(X)$ は既約で, $r \notin F$ を $f(X)$ の任意の根とすると $E = F(r)$ が $f(X)$ の最小分解体である.
   c) $\mathrm{G}_F(f(X)) = \{\iota\} \simeq \mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$
   d) ($\mathrm{ch}(F) \neq 2$ のとき) $f(X)$ は既約, かつ $\sqrt{\Delta} \in F$
4) a) $[E : F] = 6$
   b) $f(X)$ は既約で, $r \notin F$ を $f(X)$ の任意の根とすると $E = F(\sqrt{\Delta}, r)$ が $f(X)$ の最小分解体である.
   c) $\mathrm{G}_F(f(X)) = \{\iota\} \simeq \mathfrak{S}_3$
   d) ($\mathrm{ch}(F) \neq 2$ ならば) $f(X)$ は既約, かつ $\sqrt{\Delta} \notin F$

証明. $\Delta \neq 0$ ならば $f(X)$ は重根をもたないので分離的である. よって, E/F はガロア拡大であり, そのガロア群は $\mathfrak{S}_3$ の部分群に同型なので, $[E : F] = |\mathrm{G}_F(f(X))|$ は $\mathfrak{S}_3$ の位数 $3! = 6$ の約数である. よって, 上の 1a) ～ 4a) が排他的に, すべての場合を尽くしている. $f(X)$ が可約な場合が 1), 2) であり, 既約な場合が 3), 4) である. 可約な場合の分類は既に述べたので 1), 2) については既に証明されている. よって 3), 4) の a) ～ d) の同値性を言えばよい.

$f(X)$ が既約のときは, ガロア群 $\mathrm{G}_F(f(X))$ は可移的だから, $3 \leq |\mathrm{G}_F(f(X))| \leq 6$ であり, $|\mathrm{G}_F(f(X))| = 3, 6$ なので, $\mathrm{G}_F(f(X)) = \mathfrak{A}_3$ または $\mathrm{G}_F(f(X)) = \mathfrak{S}_3$ である.

3), 4) の a) ⇔ c) に関しては, $\mathrm{G}_F(f(X))$ は $\mathfrak{S}_3$ の部分群に同型で, $[E : F] = |\mathrm{G}_F(f(X))|$ なので, 明らかである.

3), 4) の c) ⇔ d) に関しては, $\mathrm{ch}(F) \neq 2$ のとき定理 6.6.1 2) より, 明らかである.

3) の a) ⇔ b) に関しては, $f(X)$ が既約という前提条件より, $[E : F] = 3$ ならば $E = F(r)$ である. 逆に, $E = F(r)$ ならば $[E : F] = 3$ である.

4) の a) ⇔ b) に関しては, $F(r) \subsetneq F(r, \sqrt{\Delta}) \subseteq E$ ならば $E = F(r, \sqrt{\Delta})$ で, $[E : F] = 6$ である. 逆に $[E : F] = 6$ ならば $F(r) \subsetneq E$ である. □

以下, $\mathrm{ch}(F) \neq 2, 3$ かつ $\sqrt{-3} \in F$ ならば[28] のときに, カルダノの解法を使った解の公式との関係を述べる. $f(X)$ において, X を $X - \dfrac{b}{3}$ で置き換えることによって, 2 次の項を消すことができて,

$$g(X) = X^3 + pX + q$$

という形に変形される.[29] $f(X)$ と $g(X)$ は同じ最小分解体をもち, よって, 同じガロア群を持つ. また, それぞれの解の集合から, 他方の解の集合を簡単に計算できる. よって, $g(X)$ の最小分解体を E, そのガロア群を $G = \mathrm{G}_F(E)$, $g(X)$ の E における

[27] d) は $\mathrm{ch}(F) \neq 2, 3$ の場合のときだけの判定条件である. また, $f(X)$ が既約のときは $\sqrt{-3} \in F$ の条件も必要である.

[28] $\sqrt{-3} \in F$ という条件は $\omega = \frac{-1 \pm \sqrt{-3}}{2} \in F$ という条件と同値である. ここで, ω は $\omega^2 + \omega + 1 = 0$ をみたすので 1 の原始 3 乗根である.

[29] X を $X - \dfrac{b}{3}$ で置き換えることによって,

$$f(X - \frac{b}{3}) = X^3 + \left(-\frac{b^2}{3} + c\right) X + \frac{2}{27} b^3 - \frac{bc}{3} + d$$

となるので,

$$p = -\frac{b^2}{3} + c, \qquad q = \frac{2}{27} b^3 - \frac{bc}{3} + d$$

である. また, このとき, 判別式は $\Delta = -4\, p^3 - 27\, q^2$ となる.

解を r_1, r_2, r_3 としよう. $g(X)$ の根を $X = u + v$ とおくと

$$g(X) = g(u+v) = u^3 + v^3 + q + (3\,uv + p)(u+v)$$

なので

$$u^3 + v^3 + q = 0, \qquad 3\,uv + p = 0$$

となる u, v が見つければ $g(X)$ の根は求まる. ここで, v^3, w^3 を根に持つ 2 次の多項式

$$h(X) = X^2 + qX - \left(\frac{p}{3}\right)^3$$

を考える. $h(X)$ の判別式を Δ_h, $g(X)$ の判別式を Δ_g と書くことにすると,

$$\Delta_h = q^2 + \frac{4}{27}\,p^3 = -\frac{\Delta_g}{27} \neq 0$$

である. また, 解の公式を使って, 根を求めると

$$u^3 = \frac{-q \pm \sqrt{\Delta_h}}{2} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

である. u と v は対称なので, 1 つの解を u^3 に取れば, もう一方が v^3 になる. $\omega = \dfrac{-1+\sqrt{-3}}{2} \in F$ という仮定より, 3 乗根は 3 つあって, $uv = -\dfrac{p}{3}$ という条件より, $X = u + v$ は

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$\omega\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$\omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

という 3 つの根をすべて尽くし, $g(X)$ は分解する. また, $\sqrt{-3} \in F$ という仮定より, $\sqrt{\Delta_h} \in F \Leftrightarrow \sqrt{\Delta_g} \in F$ であり, $\sqrt{\Delta_g} \in F$ のときは $[E:F] = 3$, $\sqrt{\Delta_g} \notin F$ のときは $[E:F] = 6$ である.

$\Delta \in F$ であった. $F = \mathbb{Q}$ のときは, Δ の符号を調べることによって, 3 次多項式の根のさらなる情報を得ることができる. $\mathbb{Q}$ 係数の 3 次多項式は, 1 つの実根 r と 2 つの複素数根 $\{a+bi, a-bi\}$ を持つか, または, 3 つの実根 r, s, t を持つかの 2 通りである. 前者の場合は

$$\delta = \{(r-a) - bi\}\{(r-a) + bi\} \cdot 2bi = \{(r-a)^2 + b^2\} \cdot 2bi$$

よって, $\Delta < 0$ である. また, 後者の場合は, $\Delta = \{(r-s)(r-t)(s-t)\}^2 > 0$ である.

定理 6.7.3. $f(X)$ が 3 次多項式で $\Delta \neq 0$ とする.

1) $\Delta < 0$ であるための必要十分条件は $f(X)$ が 1 つの実根と 2 つの複素数根を持つことである.
2) $\Delta > 0$ であるための必要十分条件は $f(X)$ が 3 つの実根を持つことである.

例 6.7.4. $f(X) = X^3 - 2\,X^2 - X + 1 \in \mathbb{Q}[X]$ とする. $f(X)$ の有理数根は, 定数項の約数なので ± 1 しかありえないが, これらは根ではないので, $f(X)$ は $\mathbb{Q}$ 上既約である. 判別式は $\Delta = 49 > 0$ なので, 3 つの実根を持つ. $7 = \sqrt{49} \in \mathbb{Q}$ なので, 定理 6.7.2 より $\mathrm{G}_{\mathbb{Q}}(f(X)) \simeq \mathbb{Z}/3\mathbb{Z}$ で, r を $f(X)$ の任意の根とすると, $f(X)$ の最小分解体は $\mathbb{Q}(r)$ である.

一方, $p \in \mathbb{Z}$ が任意の素数とするとき, 多項式 $f(X) = X^3 - p \in \mathbb{Q}[X]$ は, 定理 2.3.17 より, 既約多項式であり, 判別式は $\Delta = -27p^2 < 0$ なので $\sqrt{\Delta} \notin \mathbb{Q}$ である. したがって, $f(X)$ は 1 つの実根と 2 つの複素数根を持つ. また, $f(X)$ のガロア群は $\mathfrak{S}_3$ と同型であり, $f(X)$ の最小分解体は $\mathbb{Q}\left(\sqrt{-3}, \sqrt[3]{p}\right)$ である.

6.7.3 4 次多項式のガロア群

4 次の既約多項式のガロア群は, $\mathfrak{S}_4$ の可移的部分群に同型だから, まず最初に, $\mathfrak{S}_4$ の可移的部分群をすべて決定する. $\mathfrak{S}_4$ の可移的部分群 G の位数は

$$|G| = 4, 8, 12, 24$$

である [30] ので, 次に, この位数の $\mathfrak{S}_4$ の可移的部分群をすべて挙げよう.

1) (位数 4: 巡回群)　4 次巡回群 $\mathbb{Z}/4\mathbb{Z}$ が $\mathfrak{S}_4$ の部分群として, 現れる. それは $\mathfrak{S}_4$ の位数 4 の元で生成されるから, $\mathfrak{S}_4$ の位数 4 の元をすべて求めれば良いが, 位数 4 の元は cycle typle が 4^1 なので, 全部で $\dfrac{4!}{4^1 \cdot 1!} = 6$ 個あり, $\sigma = (1abc) = (1c)(1b)(1a)$ の形をしている. (ここで a, b, c は $2, 3, 4$ の permutation) したがって, $\mathfrak{S}_4$ には, 次の 4 個の $\mathbb{Z}/4\mathbb{Z}$ に同型な部分群がある.

$$Z_1 = \{\iota, (1234), (13)(24), (1432)\}$$
$$Z_2 = \{\iota, (1342), (14)(23), (1243)\}$$
$$Z_3 = \{\iota, (1423), (12)(34), (1324)\}$$

2) (位数 4: クラインの四群)　クラインの四群 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が $\mathfrak{S}_4$ の部分群として, 現れる. すなわち

$$V = \{\iota, (12)(34), (13)(24), (14)(23)\}$$

とおくと, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ に同型である. 読者は, V が $\mathfrak{S}_4$ の正規部分群であることを示して欲しい.[31] また, V は偶置換のみからなるから $\mathfrak{A}_4$ の部分群である. $\mathfrak{S}_4$ の位数 4 の可移的部分群は, これで尽きる. $\mathfrak{S}_4$ には

$$\{\iota, (12), (34), (12)(34)\}$$

というタイプのクラインの四群に同型な部分群が存在する. しかし, このタイプの部分群は可移的にはなりえない. なぜなら, もし, $\mathfrak{S}_4$ の部分群 G が可移的であるとするとしよう. このとき, G の単位元でない元 $\sigma \in G$ は全て位数 2 であるから, σ のサイクルタイプは 2 か 2^2 である. すなわち, 互換か, または, 2 つの共通元のない互換の積である. ところが, 互換は $\{1, 2, 3, 4\}$ の中の 1 組の文字を動かすのみである. $\{1, 2, 3, 4\}$ の中の 2 つの文字の組は $\binom{4}{2} = 6$ 通りあるがとって, 互換が存在すれば G は可移的にはなりえない. ゆえに, 可移的部分群でクラインの四群に同型なものは V のみである.

3) (位数 8: 二面体群)　$\mathfrak{S}_4$ の位数 8 の部分群は, 正方形の対称性を実現する二面体群であり. 正方形の各頂点の置換と考えることができる. また, これらの部分群は 2-Sylow 群である.

$$D_1 = \{\iota, (12)(34), (13)(24), (14)(23), (24), (13), (1234), (1432)\}$$
$$D_2 = \{\iota, (12)(34), (13)(24), (14)(23), (14), (23), (1342), (1243)\}$$
$$D_3 = \{\iota, (12)(34), (13)(24), (14)(23), (12), (34), (1423), (1324)\}$$

各 $i = 1, 2, 3$ に関して $V \subseteq D_i$ であることに注意しよう.

4) (位数 12: 交代群)　交代群 $\mathfrak{A}_4$ が $\mathfrak{S}_4$ の位数 12 の唯一の部分群である.

5) (位数 24: 対称群)　もちろん $\mathfrak{S}_4$ 自身が $\mathfrak{S}_4$ の位数 24 の唯一の部分群である.

F 上の 4 次既約多項式を

$$f(X) = X^4 + bX^3 + cX^2 + dX + e$$

[30] G が対称群 $\mathfrak{S}_n$ の可移的部分群ならば, G の位数 $|G|$ は n の倍数である.

[31] 共役は cycle type を変えない. V には cycle tyle 1^4 (単位元) と, cycle type 2^2 の元しかないが, cycle type 2^2 の元は, $\dfrac{4!}{2^2 \cdot 2!} = 3$ 個であり, 全部 V に入っているから共役で V は動かない.

と置き, $\mathrm{ch}(F) \neq 2,3$ と仮定しよう.[32] このとき, $4 \neq 0$ であるから $f(X))$ は分離的である.[33] また, この後に我々が必要とする任意の 3 次多項式が分離的であることも保証する.

X を $X - \dfrac{b}{4}$ で置き換えると, 3 次の項を消すことができて,

$$g(X) = X^4 + pX^2 + qX + r$$

となる.[34] これを, $f(X)$ の**簡約化された多項式 (reduced polynomial)** と呼ぶことにしよう. $f(X)$ と $g(X)$ は同じ最小分解体をもち, よって, 同じガロア群を持つ. また, それぞれの解の集合から, 他方の解の集合を簡単に計算できる. よって, $g(X)$ の最小分解体を E, そのガロア群を $G = \mathrm{G}_F(E)$, $g(X)$ の E における解を r_1, r_2, r_3, r_4 としよう.

記述をわかりやすくするために, ガロア群 G を対称群 $\mathfrak{S}_4$ の部分群と同一視する. 例えば, 互換 (12) は根 r_1 と r_2 を入れ替えると解釈する等々である.

4 次多項式 $g(X)$ を解析するために, 我々は暫定的に戦略的に置く或る中間体を考える. これは, ガロア群の或る部分群を指定することと同じであるから, 上に挙げた部分群の中から好都合な交叉条件 (intersection property) を持つものを選ぶ. まず, 最初に思い浮かぶ候補は, 交代群 $\mathfrak{A}_4$ であるが, 実は, これは大き過ぎる. 実際, $\sqrt{\Delta} \in F$ が G が $\mathfrak{A}_4$ の部分群であるための必要十分条件であることは, 既に見たとおりだが, それ以上の情報は得られないからである. そこで, クライン (Klein) の四群 V を試してみよう. これは, 図 6.7.1 に示したように, G の部分群 $V \cap G$ を与える.

G の位数と比較すると $V \cap G$ は次の一覧のようになる.

1) $V \cap Z_1 = \{\iota, (13)(24)\} \simeq \mathbb{Z}/2\mathbb{Z}$

---

[32] $n = 3$ のとき, 判別式 Δ は

$$\Delta = \begin{vmatrix} u_0 & u_1 & u_2 & u_3 \\ u_1 & u_2 & u_3 & u_4 \\ u_2 & u_3 & u_4 & u_5 \\ u_3 & u_4 & u_5 & u_6 \end{vmatrix}$$

である. ここで, $u_0 = 4$, $u_1 = s_1 = -b$, $u_2 = \begin{vmatrix} s_1 & 1 \\ 2\,s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 \\ 2\,c & -b \end{vmatrix} = b^2 - 2\,c$, $u_3 = \begin{vmatrix} s_1 & 1 & 0 \\ 2\,s_2 & s_1 & 1 \\ 3\,s_3 & s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 & 0 \\ 2\,c & -b & 1 \\ -3\,d & c & -b \end{vmatrix} = -b^3 + 3\,bc - 3\,d$,

$$u_4 = \begin{vmatrix} s_1 & 1 & 0 & 0 \\ 2\,s_2 & s_1 & 1 & 0 \\ 3\,s_3 & s_2 & s_1 & 1 \\ 4\,s_4 & s_3 & s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 & 0 & 0 \\ 2\,c & -b & 1 & 0 \\ -3\,d & c & -b & 1 \\ 4\,e & -d & c & -b \end{vmatrix} = b^4 - 4\,b^2c + 4\,bd + 2\,c^2 - 4\,e$$

$$u_5 = \begin{vmatrix} s_1 & 1 & 0 & 0 & 0 \\ 2\,s_2 & s_1 & 1 & 0 & 0 \\ 3\,s_3 & s_2 & s_1 & 1 & 0 \\ 4\,s_4 & s_3 & s_2 & s_1 & 1 \\ 5\,s_5 & s_4 & s_3 & s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 & 0 & 0 & 0 \\ 2\,c & -b & 1 & 0 & 0 \\ -3\,d & c & -b & 1 & 0 \\ 4\,e & -d & c & -b & 1 \\ 0 & e & -d & c & -b \end{vmatrix} = -b^5 + 5\,b^3c - 5\,b^2d - 5\,bc^2 + 5\,be + 5\,cd$$

$$u_6 = \begin{vmatrix} s_1 & 1 & 0 & 0 & 0 & 0 \\ 2\,s_2 & s_1 & 1 & 0 & 0 & 0 \\ 3\,s_3 & s_2 & s_1 & 1 & 0 & 0 \\ 4\,s_4 & s_3 & s_2 & s_1 & 1 & 0 \\ 5\,s_5 & s_4 & s_3 & s_2 & s_1 & 1 \\ 6\,s_6 & s_5 & s_4 & s_3 & s_2 & s_1 \end{vmatrix} = \begin{vmatrix} -b & 1 & 0 & 0 & 0 & 0 \\ 2\,c & -b & 1 & 0 & 0 & 0 \\ -3\,d & c & -b & 1 & 0 & 0 \\ 4\,e & -d & c & -b & 1 & 0 \\ 0 & e & -d & c & -b & 1 \\ 0 & 0 & e & -d & c & -b \end{vmatrix} = b^6 - 6\,b^4c + 6\,b^3d + 9\,b^2c^2 - 6\,b^2e - 12\,bcd - 2\,c^3 + 6\,ce + 3\,d^2$$

を使うと

$$\Delta = \begin{vmatrix} 4 & -b & b^2 - 2\,c & -b^3 + 3\,bc - 3\,d \\ -b & b^2 - 2\,c & -b^3 + 3\,bc - 3\,d & b^4 - 4\,b^2c + 4\,bd + 2\,c^2 - 4\,e \\ b^2 - 2\,c & -b^3 + 3\,bc - 3\,d & b^4 - 4\,b^2c + 4\,bd + 2\,c^2 - 4\,e & -b^5 + 5\,b^3c - 5\,b^2d - 5\,bc^2 + 5\,be + 5\,cd \\ -b^3 + 3\,bc - 3\,d & b^4 - 4\,b^2c + 4\,bd + 2\,c^2 - 4\,e & -b^5 + 5\,b^3c - 5\,b^2d - 5\,bc^2 + 5\,be + 5\,cd & u_6 \end{vmatrix}$$
$$= -27\,b^4e^2 + 18\,b^3cde - 4\,b^3d^3 - 4\,b^2c^3e + b^2c^2d^2 + 144\,b^2ce^2 - 6\,b^2d^2e - 80\,bc^2de + 18\,bcd^3 + 16\,c^4e - 4\,c^3d^2 - 192\,bde^2$$
$$- 128\,c^2e^2 + 144\,cd^2e - 27\,d^4 + 256\,e^3$$

である.

[33] $f'(X) = 4\,X^3 + 3\,bX^2 + 2\,cX + d \neq 0$ なので, 定理 3.10.3 より, $f(X)$ は分離的である. よって, $\Delta \neq 0$ も得られる.

[34] ここで

$$f\left(X - \frac{b}{4}\right) = \left(X - \frac{b}{4}\right)^4 + b\left(X - \frac{b}{4}\right)^3 + c\left(X - \frac{b}{4}\right)^2 + d\left(X - \frac{b}{4}\right) + e$$

を展開すると

$$p = -\frac{3}{8}\,b^2 + c, \qquad q = \frac{1}{8}\,b^3 - \frac{1}{2}\,bc + d, \qquad r = -\frac{3}{256}\,b^4 + \frac{1}{16}\,b^2c - \frac{1}{4}\,bd + e$$

を得る. また, 上の判別式は

$$\Delta = 16\,p^4r - 4\,p^3q^2 - 128\,p^2r^2 + 144\,pq^2r - 27\,q^4 + 256\,r^3$$

となる.

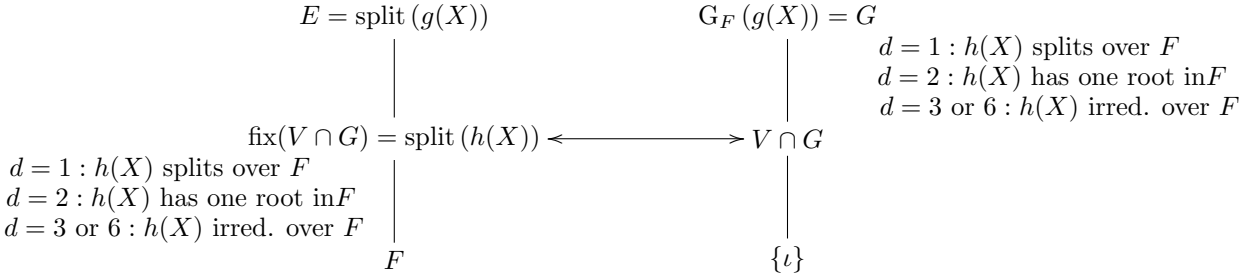

図 6.7.1: クラインの四群との交叉 $V \cap G$

2) $V \cap Z_1 = \{\iota, (14)(23)\} \simeq \mathbb{Z}/2\mathbb{Z}$
3) $V \cap Z_1 = \{\iota, (12)(34)\} \simeq \mathbb{Z}/2\mathbb{Z}$
4) $V \cap V = V = \{\iota, (12)(34), (13)(24), (14)(23)\}$
5) $V \cap D_i = V$ $(i = 1, 2, 3)$
6) $V \cap \mathfrak{A}_4 = V$
7) $V \cap \mathfrak{S}_4 = V$

したがって, 次の 3 条件のいずれもが成り立つ.

1) $|G| = 4, 8, 12$ または 24.
2) $|V \cap G| = 2$ または 4.
3) $(G : V \cap G) = 1, 2, 3, 4, 6, 12$.

次に, 固定体 $K = \mathrm{fix}(V \cap G)$ を決定しよう. V の任意の元は

$$u = (r_1 + r_2)(r_3 + r_4)$$
$$v = (r_1 + r_3)(r_2 + r_4)$$
$$w = (r_1 + r_4)(r_2 + r_3)$$

を動かさないので $F(u, v, w) \subseteq K$ である. $\mathfrak{S}_4$ の置換を全て調べることによって V の元以外に u, v, w の全てを動かさない置換はないことがわかる. よって,

$$\mathrm{G}_{F(u,v,w)}(E) \subseteq V \cap G$$

となる. 固定体を取ることによって, $K \subseteq F(U, v, w)$ となるので

$$K = \mathrm{fix}(V \cap G) = F(u, v, w)$$

でなければならない. 次に, K が

$$k(X) = (X - u)(X - v)(X - w)$$

の F 上の最小分解体であることを示したい. しかし, このためには, $k(X)$ を展開した係数は, すべて F に含まれなければならない.

実際, $k(X)$ の係数は u, v, w の対称式であるが, $\sigma \in \mathfrak{S}_4$ は u, v, w を置換するので, 任意の u, v, w の対称式は $\mathfrak{S}_4$ で固定される. よって, $k(X)$ の係数は F に含まれる. したがって, K は 3 次多項式 $k(X) \in F[X]$ の最小分解体であり,

$$(G : V \cap G) = [K : F] = 1, 2, 3, 6$$

である. 図 6.7.1 を見よ.

定義 6.7.5. 3 次多項式 $k(X) = (X - u)(X - v)(X - w)$ を, 4 次多項式 $g(X) = X^4 + pX^2 + qX + r$ の**特性 3 次多項式 (resolvent cubic)** という.

6.7.4 4 次多項式の特性 3 次多項式

ここでは, 特性 3 次多項式の係数を求めよう. 最初に, $g(X)$ は 3 次の項がないので $r_1+r_2+r_3+r_4=0$ に注意しよう. このとき

$$r_{ij}=r_i+r_j$$

と書くと, $u=-r_{12}^2$, $v=-r_{13}^2$, $w=-r_{14}^2$ となる. $g(X)$ は E 上 2 次多項式の積で書けるので, 例えば

$$g(X)=(X^2+AX+B)(X^2-AX+C)$$

としてよい. なぜなら, $g(X)$ の 3 次の項がないことから, 積の因子の X の係数は互いに, 他のマイナスで消しあうからである. 最初の因子の根は r_1, r_2 なので $A=-r_{12}$ であり

$$A^2=r_{12}^2=-u$$

である. 上の $g(X)$ の右辺を展開し, もとの $g(X)$ と係数比較をすると

$$\begin{aligned} B+C-A^2&=p\\ AC-AB&=q\\ BC&=r \end{aligned}$$

という方程式を得る. 最初の 2 つの式を B, C について解いて, 最後の式に代入すると

$$A^6+2\,pA^4+(p^2-4\,r)A^2-q^2=0$$

となり, よって, $A^2=-u$ は

$$\varphi(X)=X^3+2\,pX^2+(p^2-4\,r)X-q^2$$

の根であり, ゆえに, u は

$$\psi(X)=X^3-2\,pX^2+(p^2-4\,r)X+q^2$$

の根である. しかし, 我々は同じ議論を繰り返して, 最初の $g(X)$ が 2 次式の積としたところで, 最初の因子の根が r_1, r_3 として, 同様の分解

$$g(X)=(X^2+A'X+B')(X^2-A'X+C')$$

を考えることができる. よって $A'=-r13$, $(A')^2=-v$ である. 前と全く同様の計算をすることによって $\psi(v)=0$ を示すことができる. 同様にして, $\psi(w)=0$ であり, したがって, $\psi(X)$ は $g(X)$ の特性 3 次多項式であることがわかる.

6.7.5 4 次多項式のガロア群の完全な解析

最初に示すべきことは, 特性 3 次多項式 $\psi(X)$ の判別式が, もとの多項式 $g(X)$ に等しいことである. すなわち $\Delta_g=\Delta_\psi$ である. G_φ を $\varphi(X)$ のガロア群, G_ψ を $\psi(X)$ のガロア群 とすれば, 定理 6.7.2 から, 次のことがすぐにわかる.

1) $\psi(X)$ が既約, かつ $\sqrt{\Delta_\psi}\in F$ (この場合は $\psi(X)$ が F で一次式に分解する.) ならば $(G:V\cap G)=[K:F]=1$, よって $|V\cap G|=4=|V|$ で $G=V$ である.
2) $\psi(X)$ が既約, かつ $\sqrt{\Delta_\psi}\notin F$ (この場合は $\psi(X)$ は F にちょうど 1 つ根をもつ.) ならば $(G:V\cap G)=[K:F]=2$ で, 次の 2 つの可能性がある. $|V\cap G|=2$ ならば $|G|=4$ で, よって $G=Z_i$ $(i=1,2,3)$ か, または, $G=V$ である. しかし, $G=V$ とはなりえないので, $G=Z_i$ である.
3)
4)

関連図書

[1] Emil Artin, *Galois Theory* (Nortre Dame Mathematical Lectures) 2nd Edition, University of Nortre Dame Press (1944), Dover Books on Mathematics 1997.

[2] Sunil K. Chebolu and Ján Mináč, "Counting Irreducible Polynomials Over Finite Fields Using the Inclusion-Exclusion Principle", *Mathematics Magazine*, **84** (2011), 369-371, `arXiv:1001.0409`.

[3] 藤崎 源二郎, 体と *Galois* 理論 *I*, 岩波講座 基礎数学, 岩波書店, 1977.

[4] 藤崎 源二郎, 体と *Galois* 理論 *II*, 岩波講座 基礎数学, 岩波書店, 1977.

[5] 桂 利行, 代数学〈*3*〉体とガロア理論 *(*大学数学の入門*)*, 東京大学出版会, 2005.

[6] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Cambridge University Press (1997).

[7] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Oxford Mathematical Monographs (1999).

[8] Steven Roman, *Field Theory* (Graduate Texts in Mathematics 158) 2nd Edition, Springer-Verlag (2006).