

Contents

1 復習	2
1.1 多項式環	4
1.2 部分集合で生成される部分環	5
1.3 部分集合で生成される部分体	5
1.4 体上のベクトル空間と体論	7
1.5 有限次拡大	8
2 代数拡大	10
2.1 代数的な元と単拡大	10
2.2 代数閉体・代数閉包の基本性質	14
2.3 $K - \text{Hom}$ ・延長定理	16
2.4 代数閉包の一意性	18
3 $\mathbb{Q}$ 上超越的な元	19
4 作図問題	23
5 多項式の最小分解体・正規拡大	25
5.1 最小分解体	25
5.2 正規拡大	26
6 分離拡大	29
6.1 分離多項式	29
6.2 分離拡大	30
6.3 完全体	32
6.4 原始根原理	33
7 有限体	36
8 Galois 理論	38
8.1 Galois 拡大と Galois 群	38
8.2 Galois の基本定理	40
8.3 Artin の定理	42
9 重要な例	45
9.1 多項式の Galois 群	45
9.2 有限体	48
9.3 円分体	48

1 復習

Definition 1.1.

$f(x) \in \mathbb{Q}[x]$ を多項式とし, 方程式 $f(x) = 0$ を代数方程式という

Theorem 1.1. 代数学の基本定理

$g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ ($a_n \neq 0$) とする. $g(x)$ は $\mathbb{C}$ において n 個の根を持つ

f の根を $\alpha_1, \alpha_2, \dots, \alpha_n$ とする. $\exists G_f \hookrightarrow S(\{\alpha_1, \dots, \alpha_n\})$ を満たす群 G_f を f の Galois 群とよぶ

- $\mathbb{Q}_f := \mathbb{Q}(\alpha_1, \dots, \alpha_n) = \left\{ \frac{g(\alpha_1, \alpha_2, \dots, \alpha_n)}{h(\alpha_1, \alpha_2, \dots, \alpha_n)} \in \mathbb{C} \mid g, h \in \mathbb{Q}[x_1, \dots, x_n], h(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$
- $G_f := \text{Aut}(\mathbb{Q}_f/\mathbb{Q}) = \{ \sigma : \mathbb{Q}_f \rightarrow \mathbb{Q}_f \mid \forall a \in \mathbb{Q}, \sigma(a) = a \text{ かつ 体の同形写像} \}$
- 有限群 G が可解とは, $G := G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$ という正規部分群の減少列で, $\forall i, G_i/G_{i+1}$ は可換群であるものが存在すること
- $f(x) = 0$ が代数的に解ける $\iff G_f$ が可解群

Definition 1.2. 体

可換環 K が体であるとは, $\forall a \in K \setminus \{0\} =: K^\times, \exists b \in K, s.t. ab = 1$

Example 1.1.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ は体
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ は体
- $\mathbb{Z}, \mathbb{Z}[x], \mathbb{R}[x], \mathbb{Z}/6\mathbb{Z}$ は体ではない

Lemma 1.1.

K, L を体とする

- K のイデアルは $\{0\}$ と (1) のみ
- $i : K \rightarrow L$ は準同型 $\Rightarrow i$ は単射

Remark 1.1. 部分体としてのみなし方は一通りとは限らない

Definition 1.3. 拡大 (体) ・ 中間体

- $K \subset L$ が部分体のとき, L は K の拡大 (体) といい, L/K と表す
- $K \subset M \subset L$ なる体 M を L/K の中間体という

Lemma 1.2.

L を体, $\emptyset \neq K \subset L$ を部分集合とする. $\forall \alpha, \beta \in K$ に対して, 以下の条件をみたすとき, K は L の部分体である

- $\alpha + \beta \in K$
- $-\alpha \in K$
- $\alpha\beta \in K$
- $\alpha \neq 0$ のとき $\alpha^{-1} \in K$

Definition 1.4. 商体・分数体

A を整域とする. $A \times A \setminus \{0\}$ に同値関係 $\sim$ を次で定める: $(a, b) \sim (c, d) \Leftrightarrow ad = bc$. このとき, $\text{Frac} A := (A \times A \setminus \{0\}) / \sim$ とおき, $\frac{a}{b} := ((a, b) \text{ の同値類 }) \in \text{Frac} A$ と書く

- $\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$
- $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$
- $\frac{0}{1}$ は零元, $\frac{1}{1}$ は単位元
- $\frac{a}{b}$ $a, b \neq 0$ の逆元は $\frac{b}{a}$

$i: A \rightarrow \text{Frac} A$ を $a \mapsto \frac{a}{1}$ と定めると, i は単射準同型

Example 1.2.

- $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$
- K を体とすると, $\text{Frac}(K[x]) =: K(x)$ は K の有理関数体という

Theorem 1.2. 商体の普遍性

A を整域, K を体とする. $i: A \rightarrow \text{Frac} A$ を $a \mapsto \frac{a}{1}$ と定める. B を可換環とする. $f: A \rightarrow B$ を環準同型で, $\forall a \neq 0 \in A, f(a) \in B^\times$ とする. このとき

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 \downarrow i & \nearrow \exists! f': \text{準同型} & \uparrow \\
 \text{Frac} A & &
 \end{array}$$

Remark 1.2.

特に, K が体で, $f: A \rightarrow K$ が単射のとき

$$\begin{array}{ccc}
 A & \xrightarrow{f} & K \\
 \downarrow i & \nearrow \exists! f' & \uparrow \\
 \text{Frac} A & &
 \end{array}$$

Definition 1.5. 体の標数

K を体とする. $f: \mathbb{Z} \rightarrow K$ を $n \mapsto n \cdot 1_K := \begin{cases} 1 + \cdots + 1 & n > 0 \\ 0 & n = 0 \\ (-1) + \cdots + (-1) & n < 0 \end{cases}$ は準同型 ($\mathbb{Z}$ から K への唯一の環準同型)

- $\text{Ker} f \neq (0)$ のとき, $\text{Ker} f = (p)$ となる素数 p が存在するなら, 準同型定理より, $\mathbb{F}_p = \mathbb{Z}/(p) \hookrightarrow K$ が存在する. このとき, K の標数は p であるといい, $\text{char} K := p$ と書く
- $\text{Ker} f = (0)$ のとき, f は単射であるから, 普遍性より準同型 $f': \mathbb{Q} \rightarrow K$ が得られる

Definition 1.6. 素体

どんな体でも $\mathbb{Q}$ か $\mathbb{F}_p$ を部分体にもち、素体という

Lemma 1.3. Frobenius 写像

K を標数 p の体とし、 $\phi: K \rightarrow K$ を $a \mapsto a^p$ は準同型である

Proof.

$$\phi(a+b) = (a+b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i = a^p + b^p = \phi(a) + \phi(b) \quad (1)$$

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a) \phi(b) \quad (2)$$

$$\phi(1) = 1^p = 1 \quad (3)$$

□

Remark 1.3.

$$\alpha \in \mathbb{F}_p, \alpha^p = \alpha$$

Proof.

$\mathbb{F}_p$ は位数 $p-1$ の群なので、 $\forall \alpha \in \mathbb{F}_p^\times, \alpha^{p-1} = 1$ で、 $\alpha^p = \alpha$ から、 $\alpha = 0$ でも $\alpha^p = \alpha$ は成り立つ □

K を体とする。 $K[x] = \left\{ \sum_{\substack{i \geq 0 \\ \text{有限}}} a_i x^i \mid a_i \in K \right\}$ はユークリッド整域である (PID でもあり、

UFD でもある)

1.1 多項式環**Proposition 1.1.**

K を体とし、 $f(x) \in K[x] \setminus \{0\}$ に対して、以下同値：

1. $f(x)$ は素元
2. $f(x)$ は既約元
3. $(f(x)) \subset K[x]$ は極大イデアル

これが成り立つとき、 $L = K[x]/(f(x))$ は体で、 K の拡大体である

Proof.

(1) $\Rightarrow$ (2) : 一般論

(2) $\Rightarrow$ (3) : PID より成り立つ

(3) $\Rightarrow$ (1) : 極大イデアルは素イデアル □

Theorem 1.3. 代入原理

A, B を可換環とし、 $i: A \rightarrow B$ を環準同型とする。 $n \geq 1$ として、 $b_1, \dots, b_n \in B$ とする。このとき、 $\varphi = \varphi_{b_1, \dots, b_n}: A[x_1, \dots, x_n] \rightarrow B$ を $\sum_{\substack{k_1, \dots, k_n \geq 0 \\ \text{finite}}} a_{k_1, \dots, k_n} x_1^{k_1} \cdots x_n^{k_n} \mapsto \sum_{\substack{k_1, \dots, k_n \geq 0 \\ \text{finite}}} i(a_{k_1, \dots, k_n}) b_1^{k_1} \cdots b_n^{k_n}$

と定めると、 φ は環準同型である

Remark 1.4.

準同型 $i: A \rightarrow B$ に対して、写像 $B^n \rightarrow \{\varphi: A \rightarrow B: \text{環準同型}, \varphi|_A = i\}$ を $(b_1, \dots, b_n) \mapsto \varphi_{b_1, \dots, b_n}$ と定めると、これは全単射である

Proof.

逆写像は $\varphi \mapsto (\varphi(x_1), \dots, \varphi(x_n))$

□

Remark 1.5.

L/K を体の拡大とし, $i: K \hookrightarrow L$ を包含写像とする. $\beta \in L$ に対して, 環準同型 $\varphi_\beta: K[x] \rightarrow L$ を $f(x) \mapsto f(\beta)$ と定める

1.2 部分集合で生成される部分環

B を環とし, $A \subset B$ を部分環とする. $\emptyset \neq S \subset B$ を部分集合とする

$A[S] := \bigcap_{\substack{A' \subset B: \text{部分環} \\ A' \supset A, S}} A'$ とおく

Lemma 1.4.

以下が成り立つ

- $A[S]$ は A と S を含む B の部分環のうち最小のもの
- $A[S] = \left\{ a \cdot b_1^{i_1} \cdots b_n^{i_n} \mid a \in A, b_j \in S, i_j \geq 0, n \geq 0 \right\}$ という形の元の有限和

Definition 1.7.

$A[S]$ を A 上 S で生成される部分環という

Example 1.3.

$S = \{b\}$ とする. このとき, $A[S] = \left\{ \sum_{i: \text{有限}} a_i b^i \mid a_i \in A \right\}$

Remark 1.6.

$S = \{b_1, \dots, b_n\} \subset B$ が有限集合のとき, 代入写像 $A[x_1, \dots, x_n] \rightarrow B, g(x_1, \dots, x_n) \mapsto g(b_1, \dots, b_n)$ の像が $A[S]$ である

Example 1.4.

$m \in \mathbb{Z}$ を平方因子なしとする. $\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$

Example 1.5.

$p \neq q$ を素数とする. $\mathbb{Q}[\sqrt{p}, \sqrt{q}] = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} : a, b, c, d \in \mathbb{Q}\}$

Example 1.6.

$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$

1.3 部分集合で生成される部分体

L/K を体の拡大とし, $\emptyset \neq S \subset L$ を部分集合とする. $K(S) := \bigcap_{\substack{K' \subset L: \text{部分体} \\ K' \supset K, S}} K'$ とおく. S によっ

て K 上生成される体という

Lemma 1.5.

以下が成り立つ

- $K(S)$ は K と S を含む L の部分体のうち最小のもの
- $K(S) \cong \text{Frac}(K[S])$
- $K(S)$ の元は, S と K の元の四則演算によって作られる元全体

Proof.

- 部分体の共通部分はまた部分体であるから明らか
- $K[S]$ の最小性より, $K[S] \subset K(S)$ はよい. 商体の普遍性より, $\text{Frac} K[S] \hookrightarrow K(S)$ が誘導される. $\text{Frac} K[S]$ の像も K と S を含む体なので, $K(S)$ の最小性より, $\text{Frac} K[S] \cong K(S)$

□

Example 1.7.

- $S = \{b\}$ のとき, $K(b) := K(\{b\}) = \left\{ \frac{f(b)}{g(b)} \in L : f, g \in K[x], g(b) \neq 0 \right\}$. 一つの変数で生成される拡大を単拡大という
- より一般に, $S = \{b_1, \dots, b_n\}$ のとき

$$K(b_1, \dots, b_n) := K(S) \quad (4)$$

$$= \left\{ \frac{f(b_1, \dots, b_n)}{g(b_1, \dots, b_n)} \in L : f, g \in K[x_1, \dots, x_n], g(b_1, \dots, b_n) \neq 0 \right\} \quad (5)$$

有限個の変数で生成される拡大を有限生成という

Example 1.8.

$$\mathbb{Q}(i) = \left\{ \frac{a+bi}{c+di} \mid a, b, c, d \in \mathbb{Q}, (c, d) \neq (0, 0) \right\} = \{r + si : r, s \in \mathbb{Q}\} = \mathbb{Q}[i]$$

Proof.

- $\subset$: $\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$
- $\supset$: 明らか

□

Remark 1.7.

生成元の取り方は無数にある : $\mathbb{Q}(i) = \mathbb{Q}(1+i) = \mathbb{Q}\left(\frac{1}{2i}\right) = \mathbb{Q}\left(\frac{1+4i}{2-i}\right)$

Example 1.9.

より一般に, $m \in \mathbb{Z}$ を平方因子なしとする. このとき, $\sqrt{m} \notin \mathbb{Q}$ であり

$$\mathbb{Q}(\sqrt{m}) = \left\{ \frac{f(\sqrt{m})}{g(\sqrt{m})} \in \mathbb{C} \mid f(x), g(x) \in \mathbb{Q}[x], g(\sqrt{m}) \neq 0 \right\} \quad (6)$$

$$= \left\{ \frac{a+b\sqrt{m}}{c+d\sqrt{m}} \mid a, b, c, d \in \mathbb{Q}, (c, d) \neq (0, 0) \right\} \quad (7)$$

$$= \{r + s\sqrt{m} \in \mathbb{C} : r, s \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{m}] \quad (8)$$

このような体を 2 次体という

Example 1.10.

- $\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in \mathbb{Q}[x], g(x) \neq 0 \right\}$
- $\mathbb{Q}(x_1, x_2, \dots, x_n) = \left\{ \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} : f, g \in \mathbb{Q}[x_1, \dots, x_n], g(x_1, \dots, x_n) \neq 0 \right\}$

Lemma 1.6.

$$K_1, K_2 \subset L, K_1(K_2) = K_2(K_1)$$

Proof.

どちらも $\bigcap_{\substack{K' \subset L \\ K' \supset K_1, K_2}} K'$ に等しい

□

Definition 1.8. 合成体

$K_1 K_2 := K_1 (K_2) = K_2 (K_1)$ を K_1 と K_2 の合成体という

Remark 1.8.

$$K(S) K(T) = K(S \cup T) = (K(S))(T)$$

Proof.

$$\begin{aligned} \bullet K(S) K(T) &= \bigcap_{\substack{K' \subset L \\ K' \supset K(S), K(T)}} K' \\ \bullet K(S \cup T) &= \bigcap_{\substack{K' \subset L \\ K \supset K, K' \supset K(S \cup T)}} K' \\ \bullet (K(S))(T) &= \bigcap_{\substack{K' \subset L \\ K' \supset K(S), K' \supset K(T)}} K' \end{aligned}$$

□

Example 1.11.

$$\begin{aligned} \bullet \mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(\sqrt{3}) &= \mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) \\ \bullet K(\alpha_1, \dots, \alpha_n) &= K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \end{aligned}$$

Remark 1.9.

$L/M/K, S \subset L$ とする. このとき, $M \cdot K(S) = M(S)$

Proof.

$$M \cdot K(S) = \bigcap_{\substack{K' \subset L \\ K' \supset M, K' \supset K(S)}} K', M(S) = \bigcap_{\substack{K' \subset L \\ K' \supset M, K' \supset S}} K'$$

□

1.4 体上のベクトル空間と体論

Definition 1.9. ベクトル空間

体 K 上のベクトル空間 V とは, $\left\{ \begin{array}{l} \text{和} \forall a, b \in V, a + b \in V \\ \text{スカラー倍} \forall a \in V, \forall k \in K, ka \in V \end{array} \right.$ を持つ集合で, 以下の条件をみたすもの:

1. $\forall a, b \in V, (a + b) + c = a + (b + c)$
2. $\exists 0 \in V, \forall a \in V, a + 0 = 0 + a = a$
3. $\forall a \in V, \exists x \in V, a + x = 0 = x + a$
4. $\forall a, b \in V, a + b = b + a$
5. $\forall a, b \in V, \forall k \in K, k(a + b) = ka + kb$
6. $\forall a \in V, \forall k, l \in K, (k + l)a = ka + la$
7. $\forall a \in V, 1a = a$

Definition 1.10. 線型写像

V, W を体 K 上のベクトル空間とする. 線型写像 $\varphi: V \rightarrow W$ とは以下をみたす写像:

$$\forall a, b \in V, \forall k \in K, \begin{cases} \varphi(a+b) = \varphi(a) + \varphi(b) \\ \varphi(ka) = k\varphi(a) \end{cases}$$

Remark 1.10.

K を体として

- $K^n = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} : a_i \in K \right\}$ は K 上のベクトル空間
- $M_{m,n}(K) = \{[a_{ij}] : a_{ij} \in K, m \times n \text{ 行列} \}$ は K 上のベクトル空間
- $\{K^n \rightarrow K^m \text{ の線型写像} \} \cong M_{m,n}(K)$
- 一次独立, 一次従属, 基底, 次元, 固有値, 固有ベクトルなど

Definition 1.11. 拡大次数

L/K を体の拡大とする. $[L:K] := \dim_K L$ を L の K 上の拡大次数という. さらに, $[L:K] < \infty$ のとき, L/K は有限拡大であるといい, そうでないとき, L/K を無限次拡大という

Remark 1.11.

$$L = K \iff [L:K] = 1$$

Example 1.12.

- $\mathbb{C}/\mathbb{R} : \mathbb{C}$ を $\mathbb{R}$ 上のベクトル空間とみなすと, 基底は例えば $1, i$ で, $[\mathbb{C}:\mathbb{R}] = 2$
- 2 次体 $\mathbb{Q}(\sqrt{m})$ は $\mathbb{Q}$ 上のベクトル空間とみなすと, 基底は例えば $1, \sqrt{m}$ で, $[\mathbb{Q}(\sqrt{m}):\mathbb{Q}] = 2$
- $\mathbb{R}/\mathbb{Q}$ は有限次元ではない (濃度を考えると明らか)

1.5 有限次拡大**Proposition 1.2.**

$L/M/K$ を体の拡大とする. このとき

1. $[L:K] < \infty \iff [L:M] < \infty, [M:K] < \infty$
2. $[L:K] < \infty$ のとき, $[L:K] = [L:M][M:K]$

Proof.

1. $[L:K] < \infty$ とする. $M \subset L$ は K 上のベクトル空間として部分空間であるから, $[M:K] < \infty$. また, $\alpha_1, \dots, \alpha_n \in L$ を L の K 上の基底とすると, L は M 上で $\alpha_1, \dots, \alpha_n$ によって張られるから, $[L:M] < \infty$
2. $\beta_1, \dots, \beta_s \in M$ を M の K 上の基底とし, $\gamma_1, \dots, \gamma_t \in L$ を L の M 上の基底とする. このとき, $s = [M:K], t = [L:M]$ である

Lemma 1.7. $\beta_i \gamma_j$ は L の K 上の基底

Proof. $a_{ij} \in K$ として $\sum_{i,j} a_{ij} \beta_i \gamma_j = 0$ とする. $\sum_j \left(\sum_i a_{ij} \beta_i \right) \gamma_j = 0$ で, γ_j は M 上一次独立だから, $\forall j, \sum_i a_{ij} \beta_i = 0$. $\alpha \in L$ とする. γ_j は L の M 上の基底だから, $\alpha = \sum_j a_j \gamma_j$ と表せるから, $\alpha = \sum_{i,j} a_{ij} \beta_i \gamma_j$ と表せる $\square$

Corollary 1.1. L/K が体拡大とし, $[L : K] = p$ を素数とする. このとき, L と K の中間体は L と K のみである. 特に, $\forall \alpha \in L/K, L = K(\alpha)$

Proof. $L/M/K$ とすると, $p = [L : K] = [L : M][M : K]$ であるから, $[L : M] = 1$ または $[M : K] = 1$ である. よって, $M = L$ または $M = K$ である $\square$

$\square$

Example 1.13.

2 次体 $\mathbb{Q}(\sqrt{m})$ に対して, $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ の真の中間体は存在しないから, $\forall \alpha \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}, \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\alpha)$

Example 1.14.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ の元は, $\alpha + \beta\sqrt{3}$ の形で表せるから, $(a + b\sqrt{2}) + (c + d\sqrt{3}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ という形で表せる ($a, b, c, d \in \mathbb{Q}$)

$\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ とすると, $\sqrt{3} = a + b\sqrt{2}$ と表せるから, $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ であり, $ab = 0$ となる. $a = 0$ とすると, $3 = 2b^2$ であり, $b = \pm\sqrt{\frac{3}{2}} \notin \mathbb{Q}$ であるから, $b = 0$ とする. このとき, $3 = a^2$ であり, $a = \pm\sqrt{3} \notin \mathbb{Q}$ であるから, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. すると, $K = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) \supsetneq \mathbb{Q}(\sqrt{2})$ で, これは 2 次拡大であるから, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$ である. よって, $1, \sqrt{2}, \sqrt{3}, \sqrt{6} \in K$ は $\mathbb{Q}$ 上 1 次独立であり, 基底となる

2 代数拡大

2.1 代数的な元と単拡大

Definition 2.1. 代数的・超越的

L/K を体の拡大とする. $\alpha \in L$ が K 上代数的とは, $\exists f(x) (\neq 0) \in K[x], s.t. f(\alpha) = 0$ となること. 代数的でないとき, K 上超越的という

Proposition 2.1.

L/K を体の拡大とし, $\alpha \in L$ とする. このとき, 以下同値:

1. α は K 上代数的である
2. $\varphi_\alpha: K[x] \rightarrow L, f(x) \mapsto f(\alpha)$ について, $\text{Ker} \varphi_\alpha \neq (0)$
3. $f(x) \in K[x]$ がモニック既約多項式であって, $f(\alpha) = 0$ となるものが存在する

Proof.

- (1) $\Rightarrow$ (2): (1) とすると, $\exists f(x) \in K[x] \setminus \{0\}, f(\alpha) = 0$ であるから, この f は $f(x) \in \text{Ker} \varphi_\alpha$
- (2) $\Rightarrow$ (3): $K[x]$ は PID より, $\text{Ker} \varphi_\alpha = (f(x))$ となるモニック多項式 $f(x)$ が存在する. このとき, (2) の仮定より, $f(x) \neq 0$ である. もし $f(x)$ がモニックでなければ定数倍すればよい. $\text{Ker} \varphi_\alpha$ は素イデアルであるから, $f(x)$ は素元となり, $K[x]$ において素元は既約元であるから, $f(x)$ は既約元である
- (3) $\Rightarrow$ (1): 明らか

□

Remark 2.1.

α が K 上代数的であるとき, $f(\alpha) = 0$ をみたすモニックな既約多項式 $f(x) \in K[x]$ は, α に対して一意である

Proof.

$\text{Ker} \varphi_\alpha \neq 0$ の生成元は定数倍を除き, 一意に定まる

□

Definition 2.2. 最小多項式

$\alpha \in L$ が K 上代数的であるとき, $f(\alpha) = 0$ をみたす既約なモニック多項式 $f(x) \in K[x]$ を α の K 上の最小多項式といい, $m_{\alpha, K}(x)$ または $m_\alpha(x)$ と表す

Remark 2.2.

$m_\alpha(x)$ は $f(\alpha) = 0$ をみたすモニックな $f(x) \in K[x]$ のうち次数最小のもの

Example 2.1. $L = \mathbb{C}, K = \mathbb{Q}$ とする

- $\alpha \in \mathbb{Q} \Rightarrow m_\alpha(x) = x - \alpha$
- $\alpha = \pm\sqrt{2} \Rightarrow m_\alpha(x) = x^2 - 2$
- $\alpha = \pm i \Rightarrow m_\alpha(x) = x^2 + 1$
- $\alpha = \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2} \Rightarrow m_\alpha(x) = x^3 - 2$
- $\alpha = \pm\sqrt[4]{2}, \pm i\sqrt[4]{2} \Rightarrow m_\alpha(x) = x^4 - 2$

Remark 2.3.

L/K を体の拡大とし, $\alpha \in L$ が K 上代数的であるとする. $\varphi_\alpha : K[x] \rightarrow L, f(x) \mapsto f(\alpha)$ の核は $(m_\alpha(x))$ であり, 像は $K[\alpha]$ である

よって, 準同型定理より, φ_α は同型 $\varphi_\alpha : K[x]/(m_\alpha(x)) \xrightarrow{\cong} K[\alpha]$ を導く

- $m_\alpha(x)$ が既約であるから, $(m_\alpha(x)) \subset K[x]$ は極大イデアルである. よって, $K[\alpha]$ は体である
- φ_α は K 上の線型写像である
- $\dim_K K[x]/(m_\alpha(x)) = \deg m_\alpha(x)$ である. 特に, $\dim_K K[\alpha] < \infty$

Proposition 2.2.

L/K を体の拡大とし, $\alpha \in L$ が K 上代数的であるとする. 以下同値:

1. α は K 上代数的である
2. $K(\alpha) = K[\alpha]$
3. $[K(\alpha) : K] < \infty$

Proof.

- $(1) \Rightarrow (2)$: $K[\alpha]$ は体であるから, $K(\alpha)$ の最小性より, $K(\alpha) \subset K[\alpha]$ である. $K(\alpha) \subset K[\alpha]$ は明らかであるから, $K(\alpha) = K[\alpha]$
- $(2) \Rightarrow (1)$: $\frac{1}{\alpha} \in K(\alpha) = K[\alpha]$ であるから, $\exists f(x) \in K[x], s.t. \frac{1}{\alpha} = f(\alpha)$ である. よって, $1 = \alpha f(\alpha)$ で, α は $x \cdot f(x) - 1$ の根である
- $(1) \Rightarrow (3)$: $(2) \Rightarrow (1)$ より, $K(\alpha) = K[\alpha]$ であるから, $\dim_K K[\alpha] = \deg m_\alpha(x) < \infty$
- $(3) \Rightarrow (1)$: $n := [K(\alpha) : K]$ とすると, $1, \alpha, \dots, \alpha^n$ は K 上一次従属であるから, 非自明な多項式 $a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$ が存在する

□

Remark 2.4.

L/K を体の拡大とし, $\alpha \in L$ が K 上代数的であるとする. このとき

- $K[x]/(m_\alpha(x)) \cong K(\alpha)$
- $[K(\alpha) : K] = \deg m_\alpha(x)$

Example 2.2.

- $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$
- $\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$
- $\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\omega \sqrt[3]{2})$

Corollary 2.1.

L/K を体の拡大とし, $\alpha_1, \dots, \alpha_n \in L$ が K 上代数的であるとする. このとき, $K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$ である

Proof.

$n = 1$ と $n = i - 1$ のとき成り立つと仮定すると

$$K(\alpha_1, \dots, \alpha_i) = (K(\alpha_1, \dots, \alpha_{i-1}))(\alpha_i) \quad (9)$$

$$= (K[\alpha_1, \dots, \alpha_{i-1}])(\alpha_i) \quad (10)$$

$$= (K[\alpha_1, \dots, \alpha_{i-1}][\alpha_i]) \quad (11)$$

$$= K[\alpha_1, \dots, \alpha_i] \quad (12)$$

□

Proposition 2.3.

$f(x) \in K[x]$ を非定数多項式とする. このとき, f は L に根を持つ L/K が存在する. さらに, L/K は有限次拡大にとれる

Proof.

$f(x)$: 既約として良い

$L := K[x]/(f(x))$ は K の有限次拡大体, $\alpha := \bar{x}$ は x の L での剰余類とすると, α は $f(x)$ の根である □

Remark 2.5.

$f(x) \in K[x]$ を既約で, L と α を上の証明の通り. このとき

- L の元 α の $\deg f$ 次未満の多項式として表せる
- α の最小多項式は $f(x)$

Remark 2.6.

$\alpha \in L$ が K 上代数的であるとき, $\varphi_\alpha: K[x] \rightarrow L, f(x) \mapsto f(\alpha)$ は $\text{Ker} \varphi_\alpha = (0)$ だから, $\varphi_\alpha: K[x] \xrightarrow{\cong} K[\alpha]$ で, $\varphi_\alpha: K(x) = \text{Frac} K[x] \xrightarrow{\cong} \text{Frac} K[\alpha] = K(\alpha)$ である. よって, 超越的な元を加えた体は有理関数体と同じである

Definition 2.3. 代数拡大・超越拡大

L/K を体の拡大とする

- L が K の代数拡大であるとは, $\forall \alpha \in L, \alpha$ は K 上代数的であること
- そうでないとき, L は K の超越拡大である

Proposition 2.4.

L/K を体の拡大とする

- L/K が有限次拡大 $\Rightarrow L/K$ は代数拡大
- L/K が有限個の代数的な元で生成される $\Rightarrow L/K$ は有限次拡大

Proof.

- $n = [L:K]$ とおき, $\alpha \in L$ とする. $1, \alpha, \dots, \alpha^n$ は K 上一次従属であるから, 非自明な多項式 $a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$ が存在する. よって, α は K 上代数的である
- $\alpha_i: K$ 上代数的とし, $L = K(\alpha_1, \dots, \alpha_n)$ とする. $L_i = K(\alpha_1, \dots, \alpha_i)$ とおく. $L_i = L_{i-1}(\alpha_i)$ であり, α_i は L_{i-1} 上代数的であるから, $[L_i: L_{i-1}] < \infty$ で, 乗法性より, $[L:K] < \infty$

□

Corollary 2.2.

L/K を体の拡大とする. $\exists S \subset L, s.t. \begin{cases} \forall \alpha \in S, \alpha \text{ は } K \text{ 上代数的} \\ L = K(S) \end{cases}$

このとき, L/K は代数拡大

Proof.

$\alpha \in L$ とする. $\exists S_0 \subset S$ は有限集合で, $\alpha \in K(S_0)$ である. $K(S_0)/K$ は有限次拡大であり, 代数拡大である. よって, α は K 上代数的である $\square$

Corollary 2.3.

L/K を体の拡大とする. $L/M_i/K$ ($i \in I$) を部分拡大, $M := M_i$ たちの合成体とする. このとき

- $\forall i, M_i/K$ は代数拡大 $\Rightarrow M/K$ は代数拡大
- $\#I$ が有限かつ $\forall i, M_i/K$ は有限次拡大 $\Rightarrow M/K$ は有限次拡大

Proof.

- $M = K\left(\bigcup_{i \in I} M_i\right)$ とかけるので, $\bigcup_{i \in I} M_i$ は K 上代数的な元の集合であるから, M/K は代数拡大
- $M_i = K(S_i)$ と書いておく. $S_i \subset M_i$ は有限部分集合で, $\bigcup_{i \in I} S_i$ は K 上代数的な元の集合であるから, $M = K\left(\bigcup_{i \in I} S_i\right)$ は K の有限次拡大である $\square$

Corollary 2.4.

L/K を体の拡大とする. $\alpha, \beta \in L$ が K 上代数的であるとする. このとき, $\alpha \pm \beta, \alpha\beta, (\alpha \neq 0 \text{ なら }) \frac{1}{\alpha}$ も K 上代数的である

Proof.

$K(\alpha, \beta)/K$ は代数拡大であるから明らか $\square$

Corollary 2.5.

L/K を体の拡大とする. 一時的に $L^{alg} := \{x \in L : x \text{ は } K \text{ 上代数的}\}$ とすると, L^{alg} は体であり, L^{alg}/K は代数拡大である

Proof.

$K \subset L^{alg}$ は明らかであり, $L^{alg} \subset L$ は部分体である. よって, 定め方より, L^{alg}/K は代数拡大である $\square$

Proposition 2.5.

$L/M/K$ を体の拡大とする. このとき

- L/K が代数拡大 $\Rightarrow L/M, M/K$ は代数拡大
- $L/M, M/K$ が代数拡大 $\Rightarrow L/K$ は代数拡大

Proof.

- 定義から明らか
- $\alpha \in L$ とする. α は M 上代数的であるから, $\exists 0 \neq g(x) \in M[x], g(\alpha) = 0$ である. $E := K(g \text{ の係数 })$ とすると, E/K は有限次拡大であり, α は E 上代数的であるから, $[E(\alpha) : K] = [E(\alpha) : E] \cdot [E : K] < \infty$ となり, $E(\alpha)/K$ は代数拡大である. よって, α は K 上代数的である $\square$

2.2 代数閉体・代数閉包の基本性質

Theorem 2.1. 代数学の基本定理

$\forall f(x) \in \mathbb{C}[x]$ が非定数多項式であるとき, $\exists \alpha \in \mathbb{C}, s.t. f(\alpha) = 0$ である

Definition 2.4. 代数閉体

$\forall f(x) \in \Omega[x]$ が非定数多項式であるとき, $\exists \alpha \in \Omega, s.t. f(\alpha) = 0$ であるとき, Ω は代数閉体である

Proposition 2.6.

体 Ω に対して, 以下同値:

1. Ω は代数閉体である
2. $\forall f(x) \in \Omega[x]$ が非定数多項式であるとき, $f(x)$ は一次式の積に分解する
3. $\Omega[x]$ の既約多項式はすべて一次式である
4. Ω の代数拡大は Ω のみ
5. Ω の有限次拡大は Ω のみ

Proof.

- (1) $\Rightarrow$ (2): $f(x) \in \Omega[x]$ を非定数多項式とすると, $\exists \alpha \in \Omega, s.t. f(\alpha) = 0$. 因数定理より, $\exists g(x) \in \Omega[x], s.t. f(x) = (x - \alpha)g(x)$ である. この g に対して同様の議論を行えばよい
- (2) $\Rightarrow$ (3): 2 次以上の多項式は 1 次式の積となり, 可約となるから, 既約多項式はすべて一次式である
- (3) $\Rightarrow$ (4): L/Ω を代数拡大とする. $\alpha \in L$ とすると, 最小多項式 $m_{\alpha, \Omega}(x)$ は仮定より一次式であるから, $\alpha \in \Omega$
- (4) $\Rightarrow$ (5): 有限次拡大は代数拡大であるから, Ω の有限次拡大は Ω のみ
- (5) $\Rightarrow$ (1): $f(x) \in \Omega[x]$ を非定数多項式とすると, $\exists L/\Omega$ が有限次拡大で, $f(x)$ は L に根を持つので, $L = \Omega$ なので良い

□

Theorem 2.2.

K を体とする. このとき, $\exists \Omega/K$ が代数拡大であって, Ω は代数閉体である

Remark 2.7.

$f(x) \in K[x]$ を非定数多項式とする. $A = K[x]/(f(x))$ で, $m \subset A$ を極大イデアルとする. ($\iff f(x)$ の既約因子 $g(x)$) $A/m \cong K[x]/(g(x))$ となる. x の剰余類 $\alpha = \bar{x}$ は $g(\alpha) = 0$ をみたす. 特に, $f(\alpha) = 0$ である. よって, A/m は f が根を持つ K の拡大体である

Proof. Artin による証明

$I := \{f(x) \in K[x] : f(x) \text{ は非定数多項式である}\}$ とし, $\mathfrak{X} = (X_f)_{f \in I}$ であるとする. $\mathfrak{X}$ は各 f に対して一つずつ変数を割り当てるものである. $K[\mathfrak{X}]$ は無限変数の多項式環であり, X_f や $a \in K$ たちの有限の和と積で表される元全体である

さらに, $\mathfrak{a} := (f(X_f) \ (f \in I) \text{ たちで生成される } K[\mathfrak{X}] \text{ のイデアル})$ とする

Lemma 2.1. $\mathfrak{a} \neq K[\mathfrak{X}]$

Proof. $\mathfrak{a} = K[\mathfrak{x}]$ とすると, $1 \in \mathfrak{a}$ であるから, $1 = \sum_{i=1}^n g_i \cdot f_i(X_{f_i})$ と書ける. $g_i \in K[\mathfrak{x}]$ で, $\exists K'/K$ が有限次拡大で, $s.t. \forall f_i(X_{f_i})$ は K' に根 α_i を持つ. $1 = \sum_{i=1}^n g_i \cdot f_i(X_{f_i})$ を K' 上で考え, X_{f_i} に α_i を代入すると, $1 = 0$ となり, 矛盾. この代入を厳密にいうと, 代入写像 $K[\mathfrak{x}] \rightarrow K'$ を考える. $X_{f_i} \mapsto \alpha_i$ で, それ以外の元は適当に代入すればいい $\square$

$\mathfrak{a}$ を含む $K[\mathfrak{x}]$ の極大イデアル $\mathfrak{m}$ をとる

Proof. $\mathfrak{a} \neq K[\mathfrak{x}]$ だから取れる. 極大イデアルの存在には Zorn の補題を用いるから, 選択公理を使っている $\square$

$L_1 := K[\mathfrak{x}]/\mathfrak{m}$ は, 以下の性質をもつ

- L_1/K は体の拡大である
- $\forall f \in I, f$ は L_1 で根をもつ
- $K = L_0$ から L_1 を作ったのと同様にして, L_1 から L_2 , L_2 から L_3 , $\dots$ を構成する
 - $K = L_0 \subset L_1 \subset L_2 \subset \dots$
 - $\forall i, \forall f \in L_i[x]$ が非定数多項式であるとき, f は $L_{i+1}[X]$ で根をもつ

$L_\infty := \bigcup_{i=0}^{\infty} L_i$ とおく

Lemma 2.2. L_∞ は代数閉体である

Proof. 体の増大列の和集合は体なので, 体であることは明らか. $f(x) \in L_\infty[x]$ を非定数多項式とする. $f(x) \in L_i[x]$ なる i をとる. L_i の構成より, f は $L_{i+1}[X]$ で根をもつ. よって, f は $L_\infty[X] \supset L_{i+1}$ に根を持つ $\square$

$\square$

Remark 2.8.

$K \subset L_1 \subset L_2 \subset \dots$ より, L_∞/K は代数拡大である. よって, L_∞ は K の代数閉包でもある

Definition 2.5. 代数閉包

L/K を体の拡大とする. L が K の代数閉包であるとは, 以下の条件をみたすときである

- L/K は代数拡大である
- L は代数閉体である

Corollary 2.6.

体 K に対して, K の代数閉包が存在する

Remark 2.9.

- K の代数閉包は, 同型を除いて一意であり, それを $\overline{K}$ と書く
- K が代数閉包 $\iff \overline{K} = K$
- M/K を体の拡大とする. $\overline{M}$ は K の代数閉包でもある

Proof. $\overline{M}/M/K$ で, 推移性より, $\overline{M}/K$ も代数拡大であるから, $\overline{M}$ が代数閉なのは良い $\square$

- L/K を体の拡大とする. $L^{alg} = \{\alpha \in L : \alpha \text{ は } K \text{ 上代数的}\} \subset L$ を K の L における代数閉包というのだった. $\bar{K}$ と L^{alg} を混同しないように

しかし, 以下が成り立つ

Proposition 2.7. L/K が体拡大, L が代数閉体とすると, L^{alg} は K の代数閉包

Proof.

L^{alg}/K は代数拡大は明らか. L^{alg} が代数閉体であることを示す. $f(x) \in L^{alg}[x]$ を非定数多項式とする. L は代数閉体より, $\exists \alpha \in L, s.t. f(\alpha) = 0$ である. すると, α は L^{alg} 上代数的となり, K 上代数的でもある. よって, L^{alg} の定義より, $\alpha \in L^{alg}$ $\square$

2.3 K – Hom • 延長定理

Definition 2.6. K – Hom

$L/K, L'/K$ を体の拡大とする

- 体の準同型 $\sigma : L \rightarrow L'$ が $\forall \alpha \in K, \sigma(\alpha) = \alpha$ をみたすとき, σ は K 上の準同型という K – homomorphism
- K 上の準同型 φ が同型るとき, φ を K 上の同型という K – isomorphism
- $L = L'$ のとき, K 上の同型 $\varphi : L \xrightarrow{\cong} L$ を K 上の自己同型という K – automorphism

Example 2.3.

複素共役 $c : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$ は $\mathbb{C}$ の $\mathbb{R}$ 上の自己同型である

Example 2.4.

L/K を体の拡大とする. $\alpha \in L$ が K 上代数的であるとき, $K[x]/(m_\alpha(x)) \rightarrow L, f(x) \mapsto f(\alpha)$ は K 上の準同型で, K – 同型は $K[x]/(m_\alpha(x)) \xrightarrow{\cong} K(\alpha)$ を与える

Lemma 2.3.

K – Hom, K – Isom, K – Autom はそれぞれ合成しても K – Hom, K – Isom, K – Autom になる. また, K – Isom や K – Autom は逆写像も K – Isom, K – Autom になる

Proposition 2.8.

L/K を体の拡大とする. $\alpha, \beta \in L$ は K 上代数的であるとする. このとき, 以下は同値:

- $\exists f(x) \in K[x]$ が既約, $s.t. \alpha, \beta$ は $f(x)$ の根である
- $m_\alpha(x) = m_\beta(x)$
- K – Isom $K(\alpha) \cong K(\beta)$ で $\alpha \mapsto \beta$ を与えるものが存在する

Remark 2.10.

- これらが成り立つとき, α と β は共役という
- $K(\alpha) \cong K[x]$ の K – Isom は唯一である. なぜなら, $K(\alpha)$ の元は α と K によってかけるので, K – Hom : $K(\alpha) \rightarrow K(\beta)$ は α の行き先で決まる

Proof.

(1) $\Rightarrow$ (2) : (1) の f は α, β の最小多項式であるから, $m_\alpha = m_\beta$

(2) $\Rightarrow$ (1) : f として, $m_\alpha(x) = m_\beta(x)$ をとれば良い

(2) $\Rightarrow$ (3) :

$$\begin{aligned} K(\alpha) &\xleftarrow{\cong} K[x]/(m_\alpha(x)) \xrightarrow{\cong} K(\beta) \\ g(\alpha) &\mapsto g(x) \mapsto g(\beta) \\ \alpha &\mapsto x \mapsto \beta \end{aligned}$$

この合成 $K(\alpha) \xrightarrow{\cong} K(\beta)$ を考えれば良い

(3) $\Rightarrow$ (2) : $\sigma : K(\alpha) \xrightarrow{\cong} K(\beta)$ を (3) の K -Isom とする. $m_\alpha(\alpha) = 0$ を σ でおくと, $m_\alpha(\beta) = 0$ から, $m_\beta(x) \mid m_\alpha(x)$
 $m_\beta(\beta) = 0$ を σ^{-1} でおくと, $m_\beta(\alpha) = 0$ から, $m_\alpha(x) \mid m_\beta(x)$
 以上, $m_\alpha(x) = m_\beta(x)$ □

Example 2.5.

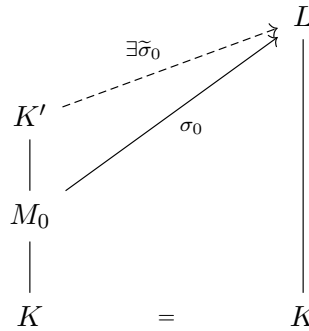
$\sqrt{2}$ と $-\sqrt{2}$ は $\mathbb{Q}$ 上共役である. 最小多項式は $x^2 - 2$ である. よって, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

Example 2.6.

$\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ は $\mathbb{Q}$ 上共役である. 最小多項式は $x^3 - 2$ である. よって, $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\omega\sqrt[3]{2}) \cong \mathbb{Q}(\omega^2\sqrt[3]{2})$

Theorem 2.3. 延長定理

K'/K を代数拡大, L/K は代数閉体で, $K'/M_0/K$ を部分体とする. また, $\sigma_0 : M_0 \rightarrow L$ を K 上の準同型とする. このとき, $\exists \tilde{\sigma}_0 : K' \rightarrow L$ は K 上の準同型, s.t. $\tilde{\sigma}_0|_{M_0} = \sigma_0$



Proof.

$\mathcal{G} := \{(M, \sigma) : K'/M/M_0 \text{ 部分体}, \sigma : M \rightarrow L \text{ は } K \text{ 上の準同型}, \sigma|_{M_0} = \sigma_0\}$
 $\mathcal{G}$ に反順序を次で定める:

$(M, \sigma), (M', \sigma') \in \mathcal{G}$ に対して, $(M, \sigma) \leq (M', \sigma') \iff M \subseteq M' \text{ かつ } \sigma'|_M = \sigma$

$((M_i, \sigma_i))_{i \in I}$ を $\mathcal{G}$ の全順序部分集合とすると

- $M = \bigcup_{i \in I} M_i$ は K'/K の部分体
- $\sigma = \bigcup_{i \in I} \sigma_i : M \rightarrow L$ を $x \mapsto \sigma_i(x)$ と定めると, σ は K 上の準同型である. なので, $(M, \sigma) \in \mathcal{G}$ であり, 上界である. ゆえに, Zorn の補題より, 極大元 $(\widetilde{M}, \tilde{\sigma}) \in \mathcal{G}$ が存在する

□

Remark 2.11. $\widetilde{M} = K'$

Proof.

$\widetilde{M} \subsetneq K'$ として, $\alpha \in K' \setminus \widetilde{M}$ をとる. $f(x) := m_{\alpha, \widetilde{M}}(x)$ は α の $\widetilde{M}$ 上の最小多項式. $\tilde{\sigma}f(x) \in L[x]$ で, f の係数を $\tilde{\sigma}$ で L に送ったものである. L は代数閉体であるから, $\tilde{\sigma}f(x)$ は L に根をもつ. この根を β とする. 準同型 $\widetilde{M}[x] \rightarrow L, g(x) \mapsto \tilde{\sigma}g(\beta)$ は $f(x) \mapsto 0$ なので, $\tilde{\sigma}' : \widetilde{M}(\alpha) \cong \widetilde{M}[x]/(f(x)) \rightarrow L$ を導く. 作り方より, $\tilde{\sigma}'$ は $\widetilde{M}$ 上では $\tilde{\sigma}$ に一致するから, $(\widetilde{M}, \tilde{\sigma}) \leq (\widetilde{M}(\alpha), \tilde{\sigma}')$ となり, $(\widetilde{M}, \tilde{\sigma})$ の極大性に矛盾する. よって, $\widetilde{M} = K'$ □

2.4 代数閉包の一意性

Theorem 2.4. 代数閉包の一意性

$L/K, L'/K, L, L'$ を K の代数閉包とする. $\exists \sigma : L \xrightarrow{\cong} L'$ は K 上の同型である. よって, K の代数閉包は同型をもぞいて一意的に定まる

Proof.

Lemma 2.4. σ は全射

Proof. L が代数閉体なので, $\sigma(L)$ も代数閉体である. よって, $\sigma(L)$ の代数拡大は $\sigma(L)$ のみである. 一方, L'/K が代数拡大より, $L'/\sigma(L)$ も代数拡大である. よって, $L' = \sigma(L)$ □

延長定理を $M = K$ とすれば適用:

$$\begin{array}{ccc} L & \xrightarrow{\exists \sigma} & L' \\ | & & | \\ M = K & = & K \end{array}$$

□

3 $\mathbb{Q}$ 上超越的な元

Lemma 3.1.

$\mathbb{C}^{alg} := \{x \in \mathbb{C} : x \text{ は } \mathbb{Q} \text{ 上代数的}\}$ は可算集合

Proof.

$d \geq 1$ に対して

- $X_d := \{\alpha \in \mathbb{C}^{alg} : [\mathbb{Q}(\alpha) : \mathbb{Q}] = d\}$
- $P_d := \{f(x) \in \mathbb{Q}[x] : f \text{ は } d \text{ 次の既約なモニック多項式}\}$
- $m : X_d \rightarrow P_d$ を $\alpha \mapsto m_{\alpha, \mathbb{Q}}(x)$ と定める

すると, P_d は可算集合で, m は高々 $d:1$ の写像であるから, X_d は可算集合である. よって, $\mathbb{C}^{alg} = \bigcup_{d=1} X_d$ は可算集合である $\square$

Corollary 3.1.

$\mathbb{Q}$ 上超越的な $\mathbb{C}$ の元は非可算集合である

Proof. $\mathbb{C} \setminus \mathbb{C}^{alg}$ は非可算集合なので $\square$

Theorem 3.1. Liouville の定理

$\alpha = \sum_{n \geq 1} \frac{1}{2^n} \in \mathbb{C}$ は $\mathbb{Q}$ 上超越的である

Proof.

α が代数的であると仮定する. α の $\mathbb{Q}$ 上の最小多項式を $m(x) := m_{\alpha, \mathbb{Q}}(x) = x^d + a_1 x^{d-1} + \dots +$

$a_d \in \mathbb{Q}[x]$ とする. $D \cdot m(x) \in \mathbb{Z}[x]$ となる $0 \neq D \in \mathbb{Z}$ をとる. $N \geq 1$ に対して, $\Sigma_N := \sum_{n=1}^N \frac{1}{2^n}$

とおく. すると, $(2^{N!})^d D \cdot m(\Sigma_N) \in \mathbb{Z} \setminus \{0\}$ なので, $|(2^{N!})^d D \cdot m(\Sigma_N)| \geq 1$ となる. 一方,

$m(x) = \prod_{i=1}^d (x - \alpha_i)$ と分解する. ただし, $\alpha_1 = \alpha, \alpha_i \in \mathbb{C}$ である

$$\cdot \Sigma_N - \alpha_1 = \sum_{n=N+1}^{\infty} \frac{1}{2^n} \leq \frac{1}{2^{(N+1)!}} \left(\sum_{n=0}^{\infty} \frac{1}{2^n} \right) = \frac{2}{2^{(N+1)!}}$$

• $M = \max\{1, |\alpha_2|, \dots, |\alpha_d|\}$ とおく. すると, $\forall i \neq 1, |\Sigma_N - \alpha_i| \leq \Sigma_N + M$

から $|m(\Sigma_N)| = \prod_{i=1}^d |\Sigma_N - \alpha_i|$ である. よって, $|m(\Sigma_N)| \leq \frac{2}{2^{(N+1)!}} (\Sigma_N + M)^{d-1}$. 右辺は

$N \rightarrow \infty$ で 0 に収束するので, $\lim_{N \rightarrow \infty} (2^{N!})^d D \cdot m(\Sigma_N) = 0$ となり, 矛盾する $\square$

Theorem 3.2.

e, π は $\mathbb{Q}$ 上超越的である

Proof.

•

$$e^x \int_0^x e^{-t} f(t) dt = e^x f(0) - f(x) + e^x \int_0^x e^{-t} f'(t) dt \quad (13)$$

ここで, RHS は LHS での f を f' に置き換えるだけなので, $f^{(n)}$ 同じ操作をしても良いから, $F(x) := \sum_{j=0}^{\infty} f^{(j)}(x)$ とおくと

$$e^x \int_0^x e^{-t} f(t) dt = e^x F(0) - F(x) \quad (14)$$

ここで, e が代数的であると仮定する. 定義より, 係数が $a_j, a_0 \neq 0$ である多項式 (t) が存在し, $\deg p(t) \geq 1$ で, $p(e) = 0$ である. また, $e^x \int_0^x e^{-t} f(t) dt = e^x F(0) - F(x)$ を $x = k$ に関して, a_k をかけた結果を和をとると

$$\sum_{k=0}^n a_k e^k \int_0^k e^{-t} f(t) dt = F(0) \sum_{k=0}^n a_k e^k - \sum_{k=0}^n a_k F(k) \quad (15)$$

$p(t)$ の仮定より, $\sum_{k=0}^n a_k F(k) = - \sum_{k=0}^n a_k e^k \int_0^k e^{-t} f(t) dt$ となる

ここまでの $f(t)$ はまだ自由に取れるから, LHS を零でない自然数である f を取れば, RHS は十分小さいので, 矛盾する. p を素数とし

$$f(t) = \frac{1}{(p-1)!} t^{p-1} g^p(t) \quad (16)$$

$$g(t) = (t-1)(t-2) \cdots (t-n) \quad (17)$$

とする. また, A を $tg(t)$ の最大値とおけば, $[0, n]$ 上で

$$\left| \sum_{k=0}^n a_k e^k \int_0^k e^{-t} f(t) dt \right| \leq \frac{1}{(p-1)!} \left(\sum_{k=0}^n |a_k| \right) e^n n A^p \quad (18)$$

ここで, $[0, n]$ 上の積分の上界は $\frac{A^p}{(p-1)!}$ である. こうすると, 十分大きな n を取れば, RHS は任意に小さくでき, $\sum_{k=0}^n a_k F(k)$ は非零整数であることをチェックすれば良い. $F(k)$ は k で f の全ての導関数を足したものであるから, f の $t=0$ での展開を考えると

$$f(t) = \frac{1}{(p-1)!} f^{(p-1)}(0) t^{p-1} + \frac{1}{p!} f^{(p)}(0) t^p + \cdots + \frac{1}{j!} f^{(j)}(0) t^j + \cdots \quad (19)$$

$j < p-1$ のとき, $f^{(j)}(0) = 0$ は明らかで, $f^{(p-1)}(0) = [(-1)^n n!]^p$ であり, $f^{(p-1)}(0)$ は整数である. p は n より大きい素数であるから, $n!$ の素因数分解にでない. $j \geq p$ のとき

$$f^{(j)}(0) = \frac{j!}{(p-1)!} \times \left(g^p(t) \text{ 上 } t^{j-(p-1)} \text{ の係数} \right) \quad (20)$$

$j \geq p$ であり, $g^p(t)$ の係数は整数であるから, $\frac{j!}{(p-1)!}$ も必ず整数であり, p の倍数である

$F(k)$ に対しても同じように k で展開する. 例として, $k=2$ のとき

$$f(t) = \frac{1}{p!} f^{(p)}(2) (t-2)^p + \cdots + \frac{1}{j!} f^{(j)}(2) (t-2)^j + \cdots \quad (21)$$

$$f^{(j)}(2) = \frac{j!}{(p-1)!} \times \left(t^{p-1} g^p(t) \text{ 上 } (t-2)^{j-p} \text{ の係数} \right) \quad (22)$$

すると, $j \geq p$ のとき, $f^{(j)}(2)$ は p の倍数であり, 整数である. よって, $\sum_{k=1}^n a_k F(k)$ も

整数で, p の倍数である. $S = \sum_{k=0}^n a_k F(k)$ とおくと, p の倍数にならない可能性がある

のは $a_0 F(0)$ のみである. $F(0)$ は p の倍数でなく, p は整数であるので, S が 0 になると a_0 を p の倍数にする必要がある. しかし, $p > |a_0|$ であるから, 証明終わり

• π が代数的であると仮定すると, π は

$$b_0 + b_1 \pi + \cdots + b_k \pi^k = 0 \quad (23)$$

の根である. すると, πi もこの多項式の根であるから

$$b_0 - i b_1 (\pi i) - b_2 (\pi i)^2 + \cdots + b_k \pi^k = 0 \quad (24)$$

$$\left[b_0 - b_2 (\pi i)^2 + \cdots \right] = i \left[b_1 (\pi i) - b_3 (\pi i)^3 + \cdots \right] \quad (25)$$

$$\left[b_0 - b_2 (\pi i)^2 + \cdots \right]^2 = - \left[b_1 (\pi i) - b_3 (\pi i)^3 + \cdots \right]^2 \quad (26)$$

$$\left[b_0 - b_2 (\pi i)^2 + \cdots \right]^2 + \left[b_1 (\pi i) - b_3 (\pi i)^3 + \cdots \right]^2 = 0 \quad (27)$$

となる. よって, $c_0 + c_1 x + \cdots + c_m x^m = 0$ $c_i \in \mathbb{Z}$ は m 個の根をもち, それぞれ $\omega_1, \dots, \omega_m$ とすると, 根 πi に注意して, $e^{\pi i} = -1 + 0i$ より $e^0 + e^{\pi i} = 0$ となる. よって

$$0 = \prod_{j=1}^m (e^0 + e^{\omega_j}) \quad (28)$$

$$= e^0 + \sum_{j=1}^m e^{\omega_j} + \sum_{1 \leq j < k \leq m} e^{\omega_j + \omega_k} + \cdots + e^{\omega_1 + \cdots + \omega_m} \quad (29)$$

これは $\{\omega_1, \dots, \omega_m\}$ の部分集合であるから, それらの指標を $\alpha_1, \dots, \alpha_{2^m}$ とおくと,

$$\sum_{i=1}^{2^m} e^{\alpha_i} = 0 \text{ となる. } \alpha_1 = 0 \text{ であり, } \alpha_i = 0 \text{ となるのもあるから, } \sum_{i=1}^n e^{\alpha_i} + \sum_{i=n+1}^{2^m} e^0 =$$

$0, \sum_{i=1}^n e^{\alpha_i} + q = 0$ である. ここで, $a = 2^m - n$ である. また, $p > q, p > c_m, p > |(c_m \alpha_1)(c_m \alpha_2) \cdots (c_m \alpha_m)|$ をみたす素数 p をとり

$$\phi(x) = \frac{c_m^{p-1}}{(p-1)!} x^{p-1} [c_m^n (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)]^p \quad (30)$$

とおくと, $\deg \phi = np + p - 1$ である. すると

$$\phi(h) \sum_{i=1}^n e^{\alpha_i} + q \phi(h) = 0 \quad (31)$$

$$\sum_{i=1}^n e^{\alpha_i} \phi(h) + q \phi(h) = 0 \quad (32)$$

$$\sum_{i=1}^n \left(\phi(\alpha_i + h) + e^{|\alpha_i|} \phi^*(\alpha_i) \right) + q \phi(h) = 0 \quad (33)$$

$$\sum_{i=1}^n \phi(\alpha_i + h) + \sum_{i=1}^n \phi^*(\alpha_i) e^{|\alpha_i|} + q \phi(h) = 0 \quad (34)$$

これを $s_1 + s_2 + s_3 = 0$ とおく

—

$$\phi(x + \alpha_i) = \frac{c_m^{p-1}}{(p-1)!} (x + \alpha_i)^{p-1} [c_m^n (x + \alpha_i - \alpha_1) \cdots (x + \alpha_i - \alpha_n)]^p \quad (35)$$

$$= \frac{x^p}{(p-1)!} c_m^{p-1} (x + \alpha_i)^{p-1} [c_m^n (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_n)]^p \quad (36)$$

和をとると

$$\sum_{i=1}^n \phi(x + \alpha_i) = \frac{x^p}{(p-1)!} \sum_{i=1}^n c_m^{p-1} (x + \alpha_i)^{p-1} [c_m^n (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_n)]^p \quad (37)$$

これを $\sum_{i=1}^n \phi(x + \alpha_i) = \frac{x^p}{(p-1)!} \sum_{j=1}^{np} \beta_j x^j$ とすると, $\sum_{j=1}^n \phi(x + \alpha_i) \equiv 0 \pmod{p}$ で

あり, $s_1 \equiv 0 \pmod{p}$ である

— $\forall i, |z_1 z_2| = |z_1| |z_2|, |x - \alpha_i| \leq |x| + |\alpha_i|$ より

$$|(x - \alpha_1) \cdots (x - \alpha_n)| \leq (|x| + |\alpha_1|) \cdots (|x| + |\alpha_n|) \quad (38)$$

で

$$|\phi(x)| \leq \left| \frac{c_m^{p-1}}{(p-1)!} x^{p-1} [c_m^n (x - \alpha_1) \cdots (x - \alpha_n)]^p \right| \quad (39)$$

$$|\phi(x)| \leq \frac{|c_m|^{np+p-1} |x|^{p-1} (|x| + |\alpha_1|)^p \cdots (|x| + |\alpha_n|)^p}{(p-1)!} \quad (40)$$

$$|s_2| = \left| \sum_{i=1}^n \phi^*(\alpha_i) e^{|\alpha_i|} \right| < 1 \quad (41)$$

—

$$\phi(x) = \frac{c_m^{p-1}}{(p-1)!} x^{p-1} [c_m^n (x - \alpha_1) \cdots (x - \alpha_n)]^p \quad (42)$$

$$= \frac{x^{p-1}}{(p-1)!} c_m^{p-1} [c_m^n (x - \alpha_1) \cdots (x - \alpha_n)]^p \quad (43)$$

$$\Rightarrow \phi(x) = \frac{x^{p-1}}{(p-1)!} \sum_{j=0}^{np} \gamma_j x^j \quad (44)$$

$$\Rightarrow \phi(h) \equiv (-1)^{np} c_m^{p-1} [(c_m \alpha_1)^p \cdots (c_m \alpha_n)^p] \pmod{p} \quad (45)$$

よって

$$s_3 = q\phi(h) \quad (46)$$

$$\equiv (-1)^{np} q c_m^{p-1} [(c_m \alpha_1)^p \cdots (c_m \alpha_n)^p] \pmod{p} \quad (47)$$

同じように, $p > q, p > c_m, p > |(c_m \alpha_1)(c_m \alpha_2) \cdots (c_m \alpha_n)|$ をみたす素数 p をとると, $s_3 \not\equiv 0 \pmod{p}$ である. すると, $s_1 + s_3 \not\equiv 0 \pmod{p}$ であり, $|s_1 + s_3| \geq 1$ となる. 一方, $|s_2| \geq 1$ なので, 矛盾する

□

Theorem 3.3.

α, β は代数的であるとする. $\alpha \neq 0, 1$ かつ $\beta \notin \mathbb{Q}$ のとき, α^β は $\mathbb{Q}$ 上超越的である

4 作図問題

平面上に一つの線分が与えられたとする. 例として, $(0, 0), (1, 0)$ が与えられているとする. 以下の操作を行う:

1. 与えられた二点を結ぶ直線を引く
2. 与えられた点を中心として, 与えられた長さを半径とする円を描く
3. 「直線や円の交点」「二点を結ぶ線分の長さ」も与えられた点, 与えられた長さによぶ

Definition 4.1.

これらの操作を有限回繰り返して得られる点・長さを作図可能な点・長さによぶ

Definition 4.2.

$a \in \mathbb{R}$ に対して, $|a|$ が作図可能な長さのとき, a を作図可能 (な数) という

Lemma 4.1.

$L := \{\alpha \in \mathbb{R} : |\alpha| \text{ は作図可能な長さ} \}$ とすると, L は $\mathbb{R}$ の部分体である

Proof.

$1 \in L$ に注意する. $\alpha, \beta \in L$ とすると, $|\alpha|, |\beta|$ は作図可能である

- $|- \alpha| = |\alpha|$ より, $- \alpha \in L$
- $\alpha + \beta$ は $\pm |\alpha| \pm |\beta|$ のいずれかであるから, $\alpha + \beta \in L$
- $\alpha\beta$ と $\frac{\alpha}{\beta}$ は直交座標系で直接に斜線を引けばよいので, $\alpha\beta, \frac{\alpha}{\beta} \in L$

□

Lemma 4.2.

$0 < \alpha \in L$ に対して, $\sqrt{\alpha} \in L$ である

Proof.

$(-\alpha, 0), (1, 0)$ を直径とする円と y 軸の交点と原点の距離が $\sqrt{\alpha}$ であるから, 作図可能である

□

Lemma 4.3.

$(a, b) \in \mathbb{R}^2$ または $a + bi \in \mathbb{C}$ が作図可能 $\iff a, b \in L$

Proof.

(a, b) が作図可能なら, 各軸に垂線を下ろせば, a, b は作図可能である. 逆に, $a, b \in L$ なら, $(a, 0), (0, b)$ を結ぶ線分の交点が (a, b) であるから, 作図可能である

□

Theorem 4.1.

$\alpha \in \mathbb{R}$ に対して, 以下は同値:

- $\alpha \in L$
- 体の列 $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{R}$ が存在して, $\forall i, [K_i : K_{i-1}] = 2$ かつ $\alpha \in K_n$

Proof.

$\Rightarrow$

直線同士の交点は一次方程式をとく, 円と直線または円同士の交点は二次方程式をとくことに対応する. また, 二点の距離は $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ であるから, L の元は, 二次拡大の積み重ねの元となる

$\Leftarrow$

$\mathbb{Q} = K_0 \subset_2 K_1 \subset_2 \cdots \subset_2 K_n \subset \mathbb{R}$ として, 帰納的に, $K_i \subset L$ を示せば良い. $K_0 = \mathbb{Q} \subset L$ は明らかである. $K_i = K_{i-1}(\sqrt{\alpha_i})$ $\alpha_i \in K_{i-1}$ と書けるので, $K_{i-1} \subset L \Rightarrow K_i \subset L$

□

Remark 4.1.

$$[K_i, K_{i-1}] = 2 \iff \exists \alpha_i \in K_{i-1}, K_i = K_{i-1}(\sqrt{\alpha_i})$$

Proof. $[K_i : K_{i-1}] = 2$ とする. $\alpha \in K_i \setminus K_{i-1}$ をとる. 最小多項式は $x^2 + bx + c$ とかけて,
 $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ であるから, $K_i = K_{i-1}(\alpha) = K_{i-1}(\sqrt{b^2 - 4c})$ □

Corollary 4.1.

$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ は 2 冪でないとき, α は作図不可能である

Example 4.1. Delos 島の問題

与えられた立方体の二倍の体積をもつ立方体は作図可能か?

$\sqrt[3]{2}$ の作図可能性が問題で, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ は 2 冪でないので, 作図不可能である

Proof.

60° の角を定規とコンパスによって三等分することはできない

Proof. できたと仮定すると, $(\cos 20^\circ, \sin 20^\circ)$ も作図可能である. このとき, $\alpha = \cos 20^\circ \in L$ となる. 特に, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ は 2 冪である. 一方, $\cos 3\theta = 4\cos^3 \theta - 3\cos \theta$ と $\cos 60^\circ = \frac{1}{2}$ より, $8\alpha^3 - 6\alpha - 1 = 0$ となる. しかし, $8x^3 - 6x - 1$ は $\mathbb{Q}$ 上既約であるから, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ となり, 矛盾する □

□

5 多項式の最小分解体・正規拡大

5.1 最小分解体

Definition 5.1. 分解体・最小分解体 L/K を体の拡大とし, $f \in K[x]$ を $d \geq 1$ 次の多項式とする (既約とは限らない)

- L 上で f が一次式の積 $f = C \prod_{i=1}^d (x - \alpha_i)$ に分解するとき, L を f の分解体という. つまり, f の全ての根は L に属し, $L \supset K(\alpha_1, \dots, \alpha_d)$
- さらに, $L = K(\alpha_1, \dots, \alpha_d)$ となるとき, L は f の K 上の最小分解体という. つまり, L は f の根で, K 上生成される

Remark 5.1. より一般に, 多項式の族 $\mathcal{F} = \{f_i\}_{i \in I} \subset K[x]$ に対して, f_i たちの根によって生成される拡大体 L/K を $\mathcal{F}$ の最小分解体という

Lemma 5.1.

$f \in K[X]$ とし, L/K を f の最小分解体とする. このとき, L/K は有限次拡大である (特に代数拡大)

Proof.

定義より, L 上で $f(x) = C \prod_{i=1}^d (x - \alpha_i)$ であり, $L = K(\alpha_1, \dots, \alpha_d)$ である. よって, L は, 有限個の K 上代数的な元で生成されるので, L/K は有限次拡大である $\square$

Lemma 5.2.

$f(x) \in K[x]$ を $d \geq 1$ 次の多項式とし, L, L' を f の最小分解体とする. このとき, K -Isom $\sigma: L \xrightarrow{\cong} L'$ が存在する

Proof.

$f(x) = C \prod_{i=1}^d (x - \alpha_i) \in L[x]$ と分解する. 延長定理より

$$\begin{array}{ccc} & & \overline{L'} \\ & \nearrow \exists \sigma & \downarrow \\ L & & L' \\ \downarrow & & \downarrow \\ K & = & K \end{array}$$

このとき, $E[x]$ において

$$C \prod_{i=1}^d (x - \sigma(\alpha_i)) = (\sigma f)(x) = f(x) \quad (48)$$

となるので, $\sigma(\alpha_i)$ たちは $\overline{L'}$ における $f(x)$ の根である. よって, $L' = K(\sigma(\alpha_1), \dots, \sigma(\alpha_d))$ である. これより, σ は L' への全射を導くので, $\sigma: L \xrightarrow{\cong} L'$ が得られる $\square$

Remark 5.2. 最小分解体の作り方

K の代数閉包 $\overline{K}$ をとって固定する. $f(x) \in K[x]$ とする. $\overline{K}$ 上で $f(x) = C \prod_{i=1}^d (x - \alpha_i)$ と分解する. このとき, $K(\alpha_1, \dots, \alpha_d) \subset \overline{K}$ は f の最小分解体である

Example 5.1.

- $f(x) = x^2 + 1 \in \mathbb{Q}[x] \Rightarrow \mathbb{Q}_f = \mathbb{Q}(i, -i) = \mathbb{Q}(i)$
- $f(x) = x^3 - 2 \in \mathbb{Q}[x] \Rightarrow \mathbb{Q}_f = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$
- $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x] \Rightarrow \mathbb{Q}_f = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
- $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x] \Rightarrow \mathbb{Q}_f = \mathbb{Q}(\pm(\sqrt{2} + \sqrt{3}), \pm(\sqrt{2} - \sqrt{3})) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

5.2 正規拡大**Definition 5.2. 正規拡大**

L/K を有限次拡大とする. L が K の正規拡大であるとは, $\exists f \in K[x], s.t. L = K_f$ となること

Remark 5.3.

L/K が有限次拡大とは限らないときも, 正規性を定義できる. L がある多項式の族 $\mathcal{F} = \{f_i\}_{i \in I} \subset K[x]$ の最小分解体となるときのときと定める

Theorem 5.1.

$\overline{K}/L/K, L/K$ を有限次拡大とするととき, 以下同値:

1. L/K は正規拡大である
2. $\forall \sigma: L \rightarrow \overline{K}$ が K -準同型であるとき, 同型 $\sigma: L \xrightarrow{\cong} L$ を導く
3. $\forall g(x) \in K[x]$ を既約多項式とし, g が L に一つでも根を持つならば, g の全ての根は L に属する, つまり, 共役元は全て L に入る

Proof.

- (1) $\Rightarrow$ (2)

$L = K_f$ とする. L 上で $f(x) = \prod_{i=1}^d (x - \alpha_i)$ と分解, $L = K(\alpha_1, \dots, \alpha_d)$ である. $\sigma: L \hookrightarrow \overline{K}$ を K -準同型とすると,
$$\begin{cases} \sigma(L) = K(\sigma(\alpha_1), \dots, \sigma(\alpha_d)) \\ \prod_{i=1}^d (x - \sigma(\alpha_i)) = (\sigma f)(x) = f(x) \end{cases} \quad \text{なので, } \sigma(L) = K_f = L$$
 となる

- (2) $\Rightarrow$ (3)

$f(x) \in K[x]$ が L に根 α をもつとする. $\beta \in \overline{K}$ を別の根とすると, 延長定理より

$$\begin{array}{ccccc}
 & & & & \overline{K} \\
 & & & \nearrow \exists \sigma & \\
 L & & & & \\
 | & & & & | \\
 K(\alpha) & \cong & K[\alpha]/(f(x)) & \cong & K(\beta) \\
 | & & & & | \\
 K & \xlongequal{\quad} & & & K
 \end{array}$$

から, $\sigma(\alpha) = \beta$ で, 仮定より $\sigma: L \xrightarrow{\cong} L$ となり, $\beta \in L$ となる

- (3) $\Rightarrow$ (1)
 $L = K(\alpha_1, \dots, \alpha_d)$ と書く. 仮定より, $m_{\alpha_i, K}(x)$ は全て L で分解するので, $f(x) = \prod_i m_{\alpha_i, K}(x)$ とすると, $K_f = L$ となる. 逆の包含も明らか

□

Lemma 5.3.

$L/M/K$ を体の拡大とする. L/K が正規拡大であるとき, L/M も正規拡大である

Proof.

$\exists f(x) \in K[x], L = K_f$ と書ける. このとき, $L = M_f$ でもあるから, L/M は正規拡大である □

Example 5.2.

- $\mathbb{Q}(i)/\mathbb{Q}$ は正規拡大
- $\alpha \in L \setminus K$ を取ると, $L = K(\alpha)$ で, $m_\alpha(x)$ の根は α と $-\alpha - b$ である. $K(\alpha) = K(\alpha, -\alpha - b)$ なので, L は $m_\alpha(x)$ の最小分解体である. よって, 一般的に, 二次拡大 L/K は正規拡大
- $\sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^4 - 2$ で, 共役元の一つ $i \cdot \sqrt[4]{2}$ は $\mathbb{Q}(\sqrt[4]{2})$ に入らないので, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大でない

Remark 5.4.

$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ で, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ は二次正規拡大で, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ も二次正規拡大であるが, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大でない. したがって, 正規拡大が推移的ではない

Example 5.3.

$x^4 - 2$ の $\mathbb{Q}$ 上の最小分解体は $\mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ であるから, $\mathbb{Q}$ の正規拡大である. さらに, $\mathbb{Q}(\sqrt[4]{2})$ の拡大で $\mathbb{Q}$ 上正規なものうち最小の体

Remark 5.5.

$M_i = K_{f_i}$ とする. $M = K_{\prod f_i}$ なので, $M_1, \dots, M_r/K$ は正規拡大であるとき, 合成体 $M := M_1 \cdots M_r$ も K の正規拡大である

Proposition 5.1.

$i = 1, 2, L/M_i/K$ を体の拡大とし, M_i/K を正規拡大とする. このとき, $M = M_1 \cap M_2$ も K の正規拡大である

Proof.

$g(x) \in K[x]$ が M に根をもつとする. $M_1, M_2/K$ が正規拡大なので, g の根は全て M_1, M_2 に属する. よって, g の根は M にも属する. すると, M/K は正規拡大である □

Definition 5.3. 正規閉包

$L'/L/K$ を有限次拡大とする. L' が L/K の正規閉包とは

- L'/K は正規拡大
- $L'/L''/L$ で, L''/K が正規拡大なら $L' = L''$

Proposition 5.2. L/K を有限次拡大とする

1. $L = K(\alpha_1, \dots, \alpha_n)$ として, $f(x) := \prod m_{\alpha_i}(x)$ とおく. $L' = K_f$ は L/K の正規閉包である. 特に, L/K の正規閉包は存在する
2. L/K の正規閉包は必ず (1) の形
3. $L'_1, L'_2/K$ を L/K の正規閉包とすると, $L'_1 \cong L'_2$ となる K -同型が存在する

Proof.

- L'/K が正規拡大であることは明らかである. $L'/L''/L$ で, L''/K が正規拡大とする. L''/K の正規性と $\alpha_i \in L''$ より, $m_{\alpha_i}(x)$ の他の根も L'' に属する. これより, $L' = K_f \subset L''$ となるので, $L' = L''$ である
- L' を L/K の正規閉包とする. 正規性より $L' \supset K_f$ を得る. K_f は $K_f \supset L$ となる K の正規拡大なので, 正規閉包の定義より, $L' = K_f$ となる
- L'_1, L'_2 を L/K の正規閉包とする. どちらも f の最小分解体であるから, $L'_1 \cong L'_2$ となる K -同型が存在する

□

Example 5.4.

- L/K が正規拡大なら, 正規閉包は L 自身である
- $L = \mathbb{Q}(\sqrt[3]{2})/K = \mathbb{Q}$ とすると, 正規閉包は $\mathbb{Q}_{x^3-2} = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

Proposition 5.3. $\overline{K}/L'/L/K$ を体の拡大とし, L/K を有限次拡大とする. L' に関して, 以下は同値:

1. $\forall \alpha_i \in L$ が K 上の生成元であるとき, $L' = K_f$ で, $f(x) = \prod_i m_{\alpha_i}(x)$
2. $\exists \alpha_1, \dots, \alpha_n \in L$ が K 上の生成元で, $L' = K_f$ で, $f(x) = \prod_i m_{\alpha_i}(x)$
3. L' は L/K の正規閉包

Proof.

- (1) $\Rightarrow$ (2) は明らか
- (2) $\Rightarrow$ (3)
 $L' = K_f$ とし, $L'/L''/L/K$ とする. $\forall i, \alpha_i \in L \subset L''$ で, L''/K が正規であるから, α_i の K 上の共役元は全て L'' の元である. よって, $L' = K_f \subset L''$ である
- (3) $\Rightarrow$ (1)
 $\alpha_1, \dots, \alpha_n$ と f を (1) のものとする. L' は $L = K(\alpha_1, \dots, \alpha_n)$ を含む K 上の正規拡大なので, α_i たちの K 上の共役元も含む. $L' \supset K_f$ である. 正規閉包の定義より, $L' = K_f$ である

□

Corollary 5.1.

L/K の $\overline{K}$ における正規閉包は一意的である

Proof.

$L'_1 = K_f, L'_2 = K_g$ を正規閉包とする. また, f, g は L/K のある生成元の最小多項式の積である. よって, $L'_1 = L'_2$ となる

□

6 分離拡大

6.1 分離多項式

Definition 6.1. 形式的微分

$f(x) = \sum_{i=0}^d a_i x^i \in K[x]$ に対して, $f'(x) := \sum_{i=1}^d i a_i x^{i-1} \in K[x]$ とおく. このように多項式の形式的に微分を定める

Lemma 6.1.

- $(af(x) + bg(x))' = af'(x) + bg'(x)$
- $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Proof. $f(x) = \sum a_i x^i, g(x) = \sum b_j x^j$ と書いて計算すれば良い □

Lemma 6.2. $f(x) \in K[x]$ を非定数多項式とする. このとき

- $\alpha \in \bar{K}$ に対して, f が α を重根にもつ $\iff f$ と f' が α を根にもつ
- f が K 上既約のとき, f が $\bar{K}$ に重根をもつ $\iff f' = 0$

Proof.

- $\Rightarrow$
 $f(x) = (x - \alpha)^2 g(x)$ と書ける. $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$ なので, $f'(\alpha) = 0$
 $\Leftarrow$
 $f(\alpha) = f'(\alpha) = 0$ と仮定する. α が f の重根でないとすると, $f(x) = (x - \alpha)g(x), g(x) \neq 0$ と書ける. すると, $f'(x) = g(x) + (x - \alpha)g'(x)$ より, $f'(\alpha) = g(\alpha) \neq 0$ となり仮定に反する
- $\Rightarrow$
 f が重根をもつとする. (1) より, f と f' はある共通根 α をもつ. f の既約性より, $f(x) = (\text{定数}) \times m_\alpha(x)$ の形で, これと $f'(\alpha) = 0$ より, $f(x) \mid f'(x)$ となる. しかし, $\deg f' < \deg f$ なので, $f' = 0$ となる
 $\Leftarrow$
 $f' = 0$ なら, f と f' は共通根をもつ. よって, (1) より, f は重根をもつ

□

Definition 6.2. 分離多項式

$f(x) \in K[x]$ を非定数多項式とする. f が分離多項式とは, f が重根をもたないこと. つまり, f の異なる根の数が $\deg f$ に等しいこと.

Example 6.1.

$\text{char} K = 0$, $f(x) \in K[x]$ が非定数かつ既約多項式であるとき, $f' \neq 0$ なので, f は分離多項式である

Example 6.2.

$K = \mathbb{F}_p(t)$ とし, $f(x) = x^p - t \in K[x]$ とする. このとき, Gauss の補題かつ Eisenstein の判定法より, $f'(x) = p \cdot x^{p-1} = 0$ なので, f は重根をもつ. よって, f は分離多項式でない

Proposition 6.1. $f(x) \in K[x]$ を既約多項式とする

- $\text{char} K = 0$ なら, f は分離多項式

- $\text{char}K = p > 0$ とする. $f(x) = g(x^{p^r})$ とかけるような最大の $r \geq 0$ をとる. このとき
 - g は既約かつ分離的
 - f の根は全て重複度 p^r

Proof.

- 例でやった
- f が既約であるから, g も既約である. もし $g' = 0$ とすると, $g(x) = h(x^p)$ の形になるから, $f(x) = h(x^{p^{r+1}})$ となり, r の最大性に反する. よって, $g' \neq 0$ で, g は分離的である. $g(x) = C \prod (x - \alpha_i), \alpha_i \in \bar{K}$ と分解すると, $f(x) = g(x^{p^r}) = C \prod (x^{p^r} - \alpha_i)$ となる. $\beta_i \in \bar{K}$ を $x^{p^r} - \alpha_i$ の根とすると, β_i たちは相異なり, $x^{p^r} - \alpha_i = x^{p^r} - \beta_i^{p^r} = (x - \beta_i)^{p^r}$ となる. よって, $f(x) = \prod (x - \beta_i)^{p^r}$ となるので, f の根は全て重複度 p^r である

□

6.2 分離拡大

Definition 6.3. 分離的・分離拡大

L/K を代数拡大とする

- $\alpha \in L$ が K 上分離的とは, α が K 上の分離多項式の根であること. 言い換えれば, $m_\alpha(x) \in K[x]$ が分離多項式であること
- L/K が分離拡大とは, $\forall \alpha \in L, \alpha$ は K 上分離的であること

Definition 6.4. 分離次数

L/K を有限次拡大とする. $\text{Hom}_K(L, \bar{K}) = \{\sigma : L \rightarrow \bar{K} : \sigma \text{ は } K\text{-準同型}\}$ とし, $[L : K]_s := |\text{Hom}_K(L, \bar{K})|$ とおく. これを L の K 上の分離次数という

Lemma 6.3. $L = K(\alpha)/K$ を代数的単拡大とし, $m_\alpha(x) \in K[x]$ を α の K 上の最小多項式とする. このとき

- $[L : K]_s = m_\alpha(x)$ の異なる根の数
- α が分離的である $\iff [L : K] = [L : K]_s$
- $\text{char}K = p > 0$ とし, p^r は α の重複度であるとする. このとき, $[L : K] = p^r [L : K]_s$

Proof.

$L \cong K[x]/(m_\alpha(x))$ なので, $\text{Hom}_K(L, \bar{K}) \cong \{\beta \in \bar{K} : \beta \text{ は } m_\alpha(x) \text{ の根}\}$ を $\phi \mapsto \phi(x)$ で対応させると, $\begin{cases} [L : K] = \deg m_\alpha \\ [L : K]_s = m_\alpha(x) \text{ の異なる根の数} \end{cases}$. これより, (1) と (2) がわかる. 以下,

$\text{char}K = p > 0$ とする. $m_\alpha(x) = g(x^{p^r})$ と書ける. ただし, g は分離的かつ既約であり, $m_\alpha(x)$ の根は全て重複度 p^r である. よって, $m_\alpha(x)$ は $\deg g$ 個の相異なる根をもち, それぞれ重複度 p^r である. よって, $\deg m_\alpha(x) = p^r \deg g = p^r [L : K]_s$ となる □

Proposition 6.2.

$L/M/K$ を有限次拡大とする. このとき, $[L : K]_s = [L : M]_s [M : K]_s$

Proof.

$\Omega := \bar{L}$ とすると, Ω は K, M の代数閉包でもある. $\text{Hom}_K(M, \Omega) = \{\sigma_i : i \in I\}, \text{Hom}_M(L, \Omega) = \{\tau_j : j \in J\}$ と書いておく. $|I| = [M : K]_s, |J| = [L : M]_s$ である. $\sigma_i : M \rightarrow \Omega$ の延長を同型 $\bar{\sigma}_i : \Omega \rightarrow \Omega$ 一つずつとる

Lemma 6.4. $\forall i \in I, \forall j \in J, \bar{\sigma}_i \circ \tau_j$ は相異なる

Proof. $\bar{\sigma}_i \circ \tau_j = \bar{\sigma}_{i'} \circ \tau_{j'}$ とする. $x \in M$ とすると, $\tau_j, \tau_{j'}$ は M -同型より, $\bar{\sigma}_i \circ \tau_j(x) = \bar{\sigma}_{i'} \circ \tau_{j'}(x)$ より, $\bar{\sigma}_i = \bar{\sigma}_{i'}$ となる. よって, $\tau_j = \tau_{j'}$ となる $\square$

Lemma 6.5. $\text{Hom}_K(L, \Omega) = \{\bar{\sigma}_i \circ \tau_j : i \in I, j \in J\}$

Proof. $\supset$ は明らかである. $\tau \in \text{Hom}_K(L, \Omega)$ とする. $\tau|_M: M \rightarrow \Omega$ は K -同型なので, $\exists i \in I, s.t. \tau|_M = \sigma_i$ である. $\bar{\sigma}_i^{-1} \circ \tau: L \rightarrow \Omega$ は M -同型なので, $\exists j \in J, s.t. \bar{\sigma}_i^{-1} \circ \tau = \tau_j$ である. よって, $\tau = \bar{\sigma}_i \circ \tau_j$ となる $\square$

以上

$$[L : K]_s = \text{Hom}_K(L, \Omega) \quad (49)$$

$$= |I| \cdot |J| \quad (50)$$

$$= [M : K]_s \cdot [L : M]_s \quad (51)$$

$\square$

Proposition 6.3. L/K を有限次拡大とする. このとき

- $\text{char} K = 0$ なら, $[L : K] = [L : K]_s$
- $\text{char} K = p > 0$ とすると, $[L : K] = \exists p^r [L : K]_s$. 特に, $1 \leq [L : K]_s \leq [L : K], [L : K]_s \mid [L : K]$

Proof.

単拡大の列 $K = M_0 \subset M_1 \subset \cdots \subset M_r = L$ をとると

$$\bullet [L : K] = \prod_{i=1}^r [M_i : M_{i-1}]$$

$$\bullet [L : K]_s = \prod_{i=1}^r [M_i : M_{i-1}]_s$$

$\square$

Theorem 6.1.

L/K を有限次拡大とする. 以下同値:

1. L/K は分離的
2. $\exists \alpha_1, \dots, \alpha_n \in L$ は K 上分離的で, $L = K(\alpha_1, \dots, \alpha_n)$
3. $[L : K]_s = [L : K]$

Proof.

- (1) $\Rightarrow$ (2) は分離拡大の定義より明らか
- (2) $\Rightarrow$ (3)
 $M_i := K(\alpha_1, \dots, \alpha_i)$ とおく. $M_0 = K, M_n = L$ である. $M_i = M_{i-1}(\alpha_i)$ かつ $m_{\alpha_i, M_{i-1}}(x) \mid m_{\alpha_i, K}(x)$ なので, M_i/M_{i-1} は分離拡大である. よって, $[M_i : M_{i-1}] = [M_i : M_{i-1}]_s$ である. よって, i に関してかけ合わせて, $[L : K] = [L : K]_s$ となる

- (3) $\Rightarrow$ (1)

$$\alpha \in L \text{ とする. } \begin{cases} [L : K] = [L : K(\alpha)] [K(\alpha) : K] \\ [L : K]_s = [L : K(\alpha)]_s [K(\alpha) : K]_s \end{cases}$$

また, $\begin{cases} [L : K] = [L : K]_s \\ [L : K(\alpha)] \geq [L : K(\alpha)]_s \\ [K(\alpha) : K] \geq [K(\alpha) : K]_s \end{cases}$ から, $[K(\alpha) : K] = [K(\alpha) : K]_s$ となる. よって, α は K 上分離的である

□

Corollary 6.1.

$L/M/K$ を有限次拡大とする. L/K が分離拡大 $\iff L/M$ と M/K が分離拡大である

Proof.

$$\begin{cases} [L : K] = [L : M] [M : K] \\ [L : K]_s = [L : M]_s [M : K]_s \end{cases} \quad \text{かつ} \quad \begin{cases} [L : K] \geq [L : K]_s \\ [L : M] \geq [L : M]_s \\ [M : K] \geq [M : K]_s \end{cases} \quad \text{よりわかる} \quad \square$$

Corollary 6.2.

$M_1, \dots, M_r/K$ を有限次分離拡大とする. このとき, 合成体 $M_1 \cdots M_r$ も K の有限次分離拡大である

6.3 完全体

Definition 6.5. 完全体

体 K が完全体とは

- $\text{char} K = 0$ である
- または, $\text{char} K = p > 0$ かつ $\phi : K \rightarrow K, x \mapsto x^p$ が全射である

Example 6.3.

- K が有限体なら, K は完全体である

Proof. $\phi : K \xrightarrow{\text{Frob}} K$ は体の準同型なので, 単射である. よって, $|\text{Im} \phi| = |K|$ なので, $\text{Im} \phi \subset K$ は等号である $\square$

- K が代数閉体なら, K は完全体である

Proof. $\text{char} K = p > 0$ で考えれば十分. $a \in K$ とすると, K は代数閉体なので, $x^p - a \in K[x]$ は K に根 α をもつ. よって, $a = \alpha^p = \phi(\alpha) \in \text{Im} \phi$ $\square$

- $K = \mathbb{F}_p(t)$ ($\mathbb{F}_p$ 上の一変数有理関数体) とすると, K は完全体ではない

Proof. $\varphi : K \rightarrow K$ を

$$\frac{\sum a_i t^i}{\sum b_j t^j} \mapsto \left(\frac{\sum a_i t^i}{\sum b_j t^j} \right)^p = \frac{\sum a_i^p t^{ip}}{\sum b_j^p t^{jp}} \quad (52)$$

と定めると, $t \notin \text{Im} \varphi$ $\square$

Proposition 6.4.

体 K に対して、以下は同値：

1. K は完全体である
2. $\forall f(x) \in K[x]$ が既約多項式なら、 f は分離多項式である
3. $\forall L/K$ が代数拡大なら、 L/K は分離拡大である

Proof.

$\text{char}K = 0$ のときは明らかであるから、以下では $\text{char}K = p > 0$ とする

- (1) $\Rightarrow$ (2)
 $f(x) \in K[x]$ が既約多項式とすると、 $f(x) = g(x^{p^r})$ と書け、 $g(x) = \sum a_i x^i$ と表す。 K は完全体より、 $\forall i, \exists b_i \in K, s.t. a_i = b_i^{p^r}$ と書ける。すると、 $f(x) = g(x^{p^r}) = \sum b_i^{p^r} x^{ip^r} = \left(\sum b_i x^i\right)^{p^r}$ となり、 f の既約性より、 $r = 0$ でなくてはならない。よって、 $f(x) = g(x)$ となり、 f は分離多項式である
- (2) $\Rightarrow$ (1)
 K が完全体でないとすると、 $a \notin \text{Im}\varphi$ が取れる。 φ は Frobenius 準同型である。 $(x^p - a)' = 0$ より非分離で、根を α とすると、 $x^p - a = x^p - \alpha^p = (x - \alpha)^p \in \overline{K}[x]$ であるから、 $K[x]$ で可約とすると、 $0 < \exists i < p, (x - \alpha)^i \in K[x]$ となる。 x^{i-1} の係数を見て、 $\alpha \in K$ となる。このとき、 $a = \alpha^p = \varphi(\alpha)$ となり、矛盾。よって、 $x^p - a \in K[x]$ は非分離かつ既約多項式である
- (2) $\Rightarrow$ (3)
 L/K を代数拡大とする。 $\forall \alpha \in L$ 、最小多項式 $m_\alpha(x)$ は (2) より、分離多項式である。よって、 L/K は分離拡大である
- (3) $\Rightarrow$ (2)
 $f(x) \in K[x]$ が既約多項式とする。(3) より、 $L = K[x]/(f(x))$ は K の分離拡大である。特に、 $\alpha = \bar{x}$ の最小多項式 $f(x)$ は分離多項式である

□

6.4 原始根原理**Lemma 6.6.**

$G \leq K^\times$ を有限部分群とすると、 G は巡回群である

Proof.

有限生成アーベル群の基本定理より、 $G \cong \mathbb{Z}/d_1 \times \mathbb{Z}/d_2 \times \cdots \times \mathbb{Z}/d_l$ で、 $d_i > 1, d_i \mid d_{i+1}$ である。 $l \geq 2$ とすると、 $\#\{\alpha \in G : \alpha^{d_1} = 1\} > d_1$ となる。 $x^{d_1} - 1$ の根は K に属し、 d_1 個以下なので矛盾。よって、 $l = 1$ であり、 G は巡回群である □

Theorem 6.2.

L/K を有限次分離拡大とする。このとき、 $\exists \alpha \in L, s.t. L = K(\alpha)$

Proof.

- K が有限のとき、 L/K は有限次拡大より、 L も有限である。補題より、 $L^\times = \langle \alpha \rangle$ である。特に、 $L = K(\alpha)$ である

- K が無限のとき, $L = K(\alpha, \beta)$ のときに, $\exists \gamma \in L, L = K(\gamma)$ を示せば良い. $\forall c \in K, \alpha + c\beta$ という元を考える. $K(\alpha + c\beta) \subsetneq L = K(\alpha, \beta)$ とすると, $[L : K(\alpha + c\beta)]_s = [L : K(\alpha + c\beta)] \neq 1$ なので, $\exists \sigma \neq \tau : L \rightarrow \Omega$ で, $K(\alpha + c\beta)$ - 準同型であり, Ω が代数閉体である. すると, $\sigma(\alpha + c\beta) = \tau(\alpha + c\beta)$ で, $\sigma(\beta) = \tau(\beta)$ とすると, $\sigma(\alpha) = \tau(\alpha)$ となり, $\sigma = \tau$ となって, 矛盾する. よって, $\sigma(\beta) \neq \tau(\beta)$ である. したがって, $c = -\frac{\sigma(\alpha) - \tau(\alpha)}{\sigma(\beta) - \tau(\beta)}$ となる. 対偶を考えると, $c \notin \left\{ -\frac{\sigma(\alpha) - \tau(\alpha)}{\sigma(\beta) - \tau(\beta)} : \sigma, \tau : L \rightarrow \Omega, \sigma(\beta) \neq \tau(\beta) \right\}$ ならば, $K(\alpha, \beta) = K(\alpha + c\beta)$ となる. K は無限体なので, このような $c \in K$ が取れる. $\gamma = \alpha + c\beta$ とおけば良い

□

Proposition 6.5.

L/K を有限次拡大とすると, 以下同値:

1. $\exists \alpha \in L, s.t. L = K(\alpha)$
2. L/K の中間体は有限個

Proof.

- (1) $\Rightarrow$ (2) 略
- (2) $\Rightarrow$ (1)
 K が無限のときに示す. L/K の真の部分体全部を $M_1, \dots, M_n$ とし, $M_i \neq K, L$ とする. 部分体は K 部分空間でもあるので, $L \neq \bigcup_{i=1}^n M_i$ となる. $\alpha \in L \setminus \bigcup_{i=1}^n M_i$ とすると, $K(\alpha) \not\subseteq M_i$ となるので, $K(\alpha) = L$ となる

□

Example 6.4.

$\mathbb{F}_p(S, T) / \mathbb{F}_p(S^p, T^p)$ は単拡大ではない

Proof.

$\forall \alpha = \frac{f(S, T)}{g(S, T)} \in L$ とする. $\alpha^p = \frac{f(S, T)^p}{g(S, T)^p} = \frac{f(S^p, T^p)}{g(S^p, T^p)} \in K$ である. つまり, $m_\alpha(x)$ は $\deg \leq p$ である. 特に, $\deg m_\alpha(x) = p^2$ となる α がないから, $L = K(\alpha)$ となる $\alpha \in L$ はない □

$f(T) \in \mathbb{F}_p(T)$ に対して, $M_f := \mathbb{F}_p(S^p, T^p, S(1 + Tf(T^p)))$ とおく, $\mathbb{F}_p(S, T) / M_f / \mathbb{F}_p(S^p, T^p)$ である

Proposition 6.6. M_f は真の中間体

Proof.

$M_f(S) = \mathbb{F}_p(S, T)$ で, S は $x^p - S^p$ の根であるから, $[\mathbb{F}_p(S, T) : M_f] \leq p$ である. $M_f = \mathbb{F}_p(S^p, T^p)(S(1 + Tf(T^p)))$ で, $\alpha^p \in \mathbb{F}_p(S^p, T^p)$ なので, $[M_f : \mathbb{F}_p(S^p, T^p)] \leq p$ である □

Proposition 6.7. $f(T) \neq g(T)$ ならば $M_f \neq M_g$

Proof.

$f \neq g$ として, $M_f \cdot M_g = \mathbb{F}_p(S, T)$ を示せば良い

$$M_f \cdot M_g = \mathbb{F}_p(S^p, T^p, \alpha := S(1 + Tf(T^p)), \beta := S(1 + Tg(T^p))) \quad (53)$$

$$= \mathbb{F}_p\left(S^p, T^p, \alpha, \frac{\beta}{\alpha}\right) \quad (54)$$

ここで, $h(T) := \frac{1 + Tg(T^p)}{1 + Tf(T^p)}$ とし

$1 + Tg(T^p) = (1 + Tf(T^p))h(T)$ より, $T(g(T^p) - f(T^p)h(T)) = h(T) - 1$ となる. $f \neq g$ より, $h \neq 1$ から, 両辺は共に 0 ではない. よって

$$T = \frac{h(T) - 1}{g(T^p) - f(T^p)h(T)} \in M_f \cdot M_g \quad (55)$$

$$S = \frac{\alpha}{1 + Tf(T^p)} \in M_f \cdot M_g \quad (56)$$

よって, $M_f \cdot M_g = \mathbb{F}_p(S, T)$ となる. 特に, $M_f \neq M_g$

□

7 有限体

K を有限体とする. $\text{char} K > 0$ でなくてはならないから, $\text{char} K = p > 0$ とすると, $K \supset \mathbb{F}_p$ であり, これは有限次拡大である. $n = [K : \mathbb{F}_p]$ とすると, $\mathbb{F}_p$ -ベクトル空間として, $K \cong \mathbb{F}_p^{\oplus n}$ なので, $|K| = p^n$ である. 言い換えれば, 有限体の元の数はず素数である

Example 7.1.

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p[x] / (d\text{次既約多項式})$ は有限体である

Example 7.2. $\mathbb{F}_p(x) = \text{Frac} \mathbb{F}_p[x]$ は無限体であり, $\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p^3\mathbb{Z}$ は体ですらない

Theorem 7.1.

p を素数とし, $n \geq 1$ とする. K を $X^{p^n} - X$ の $\mathbb{F}_p$ 上の最小分解体とすると, $[K : \mathbb{F}_p] = n$

Proof.

$f(x) = X^{p^n} - X$ とおく. $f'(x) = -1 \in \mathbb{F}_p[x]$ は f と共通根を持たないので, $f(x)$ は分離多項式である. $K_0 := \{\alpha \in K : \alpha^{p^n} = \alpha\}$ とおくと, $|K_0| = p^n$ である

$$\alpha, \beta \in K_0 \text{ とすると, } \begin{cases} (\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \\ (\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \\ \alpha \neq 0 \Rightarrow \left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha^{p^n}} = \frac{1}{\alpha} \end{cases} \quad \text{より, } \alpha + \beta, \alpha\beta, \frac{1}{\alpha} \in K_0 \text{ である. よっ}$$

て, $K_0 \subset K$ は部分体である. また, K が $\text{char} p$ より, K_0 も $\text{char} p$ である. よって, $K_0 \supset \mathbb{F}_p$ となる. よって, K_0 は K の部分体であり, $K_0 \supset \mathbb{F}_p$ である. $K = \mathbb{F}_p(K_0)$ となり, $|K| = p^n$ である $\square$

Proposition 7.1.

$K/\mathbb{F}_p$ を n 次拡大とする. このとき

- $\forall \alpha \in K, \alpha$ は $X^{p^n} - X$ の根
- K は $X^{p^n} - X$ の最小分解体

Proof.

- $|K| = p^n$ なので, $K^\times$ は位数 $p^n - 1$ の群であるから, $\alpha \in K^\times$ に対して, $\alpha^{p^n-1} = 1$ である. 特に, $\alpha^{p^n} = \alpha$ である
- (1) より, $K \subset \{\alpha \in K : \alpha \text{ は } X^{p^n} - X \text{ の根}\}$ であり, 左側は p^n 個であり, 右側は p^n 個より小さいから, 等号が成り立つ. よって, $X^{p^n} - X$ は K で分解する. すると, $(X^{p^n} - X \text{ の最小分解体}) \subset K$ である. 両辺は共に $\mathbb{F}_p$ の n 次拡大であるから, 等号が成り立つ

$\square$

Remark 7.1.

p を素数とし, $n \geq 1$ とする. $\forall n, \mathbb{F}_p$ の n 次拡大は一意であり, これを $\mathbb{F}_{p^n}$ と書く. また

- $\mathbb{F}_{p^n}$ は $X^{p^n} - X$ の最小分解体
- $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^n} = \alpha\}$
- $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

$f_1(x), f_2(x) \in \mathbb{F}_p[x]$ が d 次既約とすると, $\mathbb{F}_p[x] / (f_1(x)) \cong \mathbb{F}_p[x] / (f_2(x)) \cong \mathbb{F}_{p^d}$ である

Corollary 7.1.

$\mathbb{F}_{p^n}/\mathbb{F}_p$ は正規かつ分離拡大である

Proposition 7.2.

m, n に対して, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$

Proof.

- $\Rightarrow$
 $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ を体の拡大とすると, $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$ とおく. $p^n = (p^m)^d$ より, $n = md$
- $\Leftarrow$
 $n = md$ と書く. $x \in \mathbb{F}_{p^m}$ とすると, $x^{p^m} = x$ である
よって, $x^{p^n} = x^{p^{md}} = (x^{p^m})^{p^{m(d-1)}} = (x^{p^m})^{p^{m(d-2)}} = \cdots = x^{p^m} = x$ となる. したがって,
 $x \in \mathbb{F}_{p^n}$

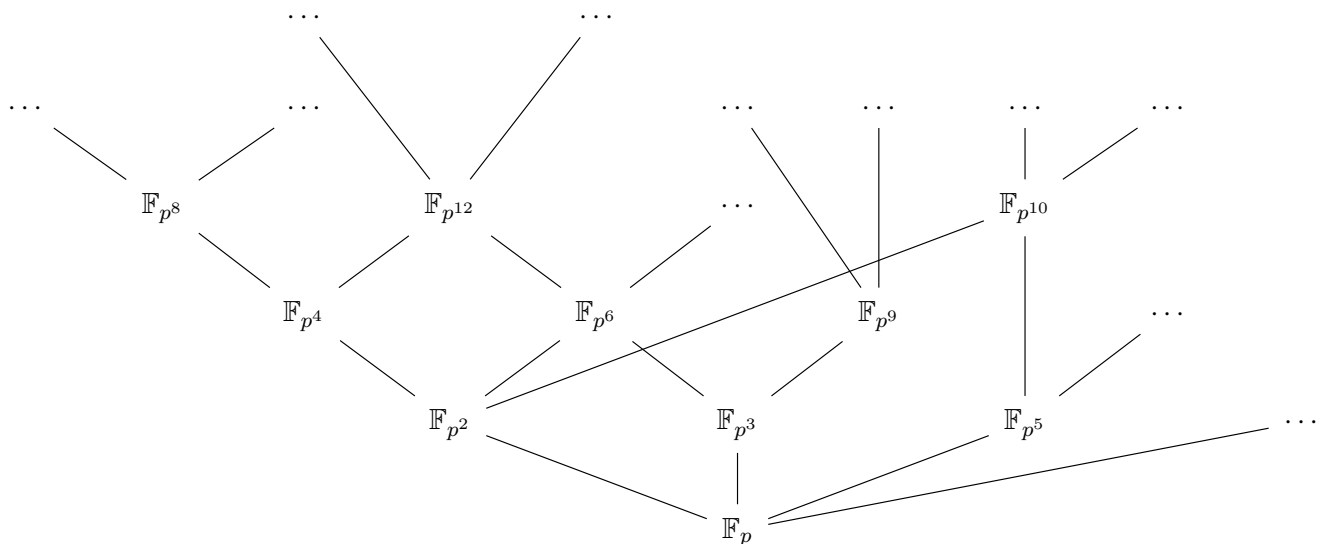
☐

Corollary 7.2. 有限体は完全体

Proof.

$\mathbb{F}_q$ の有限次拡大は $\mathbb{F}_{q^r}$ という形で, $\mathbb{F}_{q^r}/\mathbb{F}_q$ は分離拡大であるから, 有限体は完全体である $\square$

Remark 7.2.



8 Galois 理論

8.1 Galois 拡大と Galois 群

Definition 8.1. Galois 拡大・Galois 群・アーベル拡大

L/K を有限次拡大とする

- L/K が正規拡大かつ分離拡大のとき, L/K を Galois 拡大という
- Galois 拡大 L/K に対して

$$\text{Gal}(L/K) := \text{Aut}_K(L) \quad (57)$$

$$= \left\{ \sigma : L \xrightarrow{\cong} L : \sigma \text{ は } K \text{ 上の自己同型} \right\} \quad (58)$$

とおき, L/K の Galois 群という

- Galois 拡大 L/K に対して, $\text{Gal}(L/K)$ がアーベル群のとき, L/K をアーベル拡大という

Remark 8.1.

- K が完全体なら, 有限次拡大 L/K は必ず分離拡大であるから, この場合では, L/K が正規拡大であることと Galois 拡大であることは同値である
- L/K を有限次拡大とする. $\text{Aut}_K(L) \subset \text{Hom}_K(L, \bar{K})$ で, $\#\text{Hom}_K(L, \bar{K}) = [L : K]_s \leq [L : K]$ である. よって, L/K が Galois 拡大 $\iff |\text{Aut}_K(L)| = [L : K]$
- L/K を Galois 拡大とする. $f(x) \in K[x]$ を L に根をもつ既約多項式とする. $\forall \sigma \in \text{Gal}(L/K), \forall \alpha$ が $f(x)$ の根であるとき, $\sigma(\alpha)$ も $f(x)$ の根である. つまり, $\text{Gal}(L/K)$ は $f(x)$ の根たちを置換している

Proposition 8.1.

L/K を有限次拡大とする. このとき, 以下は同値である

1. L/K は Galois 拡大
2. $\exists f(x) \in K[x], s.t.$ 分離多項式 $L = K_f$

Proof.

- (1) $\Rightarrow$ (2)
原始元定理より, $\exists \alpha \in L, s.t. L = K(\alpha)$ で, $f(x) = m_\alpha(x)$ とおくと, L/K は分離拡大なので, $f(x)$ は分離多項式であり, L/K は正規拡大なので, $f(x)$ の根は全て L に属する. よって, $L = K(\alpha) \subset K_f \subset L$ となり, $L = K_f$ である
- (2) $\Rightarrow$ (1)
 L/K は正規かつ分離拡大であるから, L/K は Galois 拡大である

□

Lemma 8.1.

L/K を $\bar{K}$ の有限次拡大とし, $\tilde{L} := L/K$ の $\bar{K}$ の正規閉包とする. このとき, $\tilde{L}$ は L を含む最小の Galois 拡大であり, $\tilde{L}$ を L/K の Galois 閉包という

Proof.

L の生成元の最小多項式は分離多項式であるから, その根全てを添加して得られる $\tilde{L}$ は K 上正規かつ分離的である. よって, $\tilde{L}$ は Galois 拡大である. また, L'/K を $L' \supset L$ なる Galois 拡大とすると, 正規閉包になるから, $\tilde{L} \subset L'$ である □

Lemma 8.2.

$L/M/K$ とすると, L/M が Galois 拡大で, $\text{Gal}(L/M) \subset \text{Gal}(L/K)$

Proof.

L/K が正規かつ分離であるから, L/M も正規かつ分離である. よって, Galois 群の包含は明らか $\square$

Remark 8.2.

- $L/M/K$ で, L/K が Galois 拡大 $\nRightarrow M/K$ が Galois 拡大
- $L/M/K$ で, L/M と M/K が Galois 拡大 $\nRightarrow L/K$ が Galois 拡大

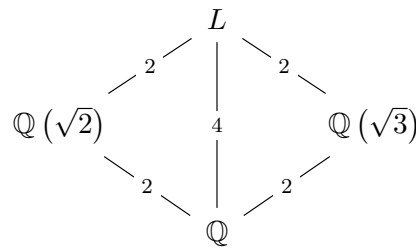
Example 8.1.

K を標数 $\neq 2$ の体とし, L/K を 2 次拡大とする. このとき, $L = K(\sqrt{\alpha}) \exists \alpha \in K$ と書ける

- L/K は Galois 拡大
- $\text{Gal}(L/K) = \{id_L, \sigma\}$. ただし, $\sigma : L = K(\sqrt{\alpha}) \rightarrow K(\sqrt{\alpha}) = L$ は $\sqrt{\alpha} \mapsto -\sqrt{\alpha}$ である. よって, $\text{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ である

Example 8.2.

$L := \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ とする. このとき, $(x^2 - 2)(x^2 - 3)$ の最小分解体より, $L/\mathbb{Q}$ は Galois 拡大である



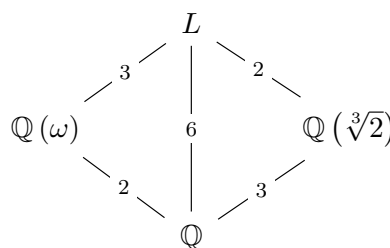
という状況 (拡大次数も含む) である

$$\text{Gal}(L/\mathbb{Q}) \supset \begin{cases} \text{Gal}(L/\mathbb{Q}(\sqrt{3})) \ni \sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \\ \text{Gal}(L/\mathbb{Q}(\sqrt{2})) \ni \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \end{cases} \quad (59)$$

すると, $\{id_L, \sigma, \tau, \sigma\tau = \tau\sigma\} \subset \text{Gal}(L/\mathbb{Q})$. 群としては, $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である

Example 8.3.

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ は正規でないので, Galois 拡大ではない. その Galois 閉包は $x^3 - 2$ の最小分解体 $L := \mathbb{Q}(\sqrt[3]{2}, \omega)$ である



という状況

$$\text{Gal}(L/\mathbb{Q}) \supset \begin{cases} \text{Gal}(L/\mathbb{Q}(\omega)) \ni \sigma : \begin{cases} \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} \\ \omega \mapsto \omega \end{cases} \\ \text{Gal}(L/\mathbb{Q}(\sqrt[3]{2})) \ni \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega^2 = \bar{\omega} \end{cases} \end{cases} \quad (60)$$

すると, $\begin{cases} \langle \sigma \rangle = \text{Gal}(L/\mathbb{Q}(\omega)) \\ \langle \tau \rangle = \text{Gal}(L/\mathbb{Q}(\sqrt[3]{2})) \end{cases}$ であり, $\langle \sigma, \tau \rangle = \text{Gal}(L/\mathbb{Q})$ である. また, $\tau\sigma\tau^{-1} = \sigma^{-1}$ なので, $\text{Gal}(L/\mathbb{Q}) = D_3 = S_3$ である

8.2 Galois の基本定理

Remark 8.3.

L/K を有限次 Galois 拡大とする. $G = \text{Gal}(L/K)$ を Galois 群とする

- 部分群 $H \triangleleft G$ に対して, $L^H := \{\alpha \in L : \forall \sigma \in H, \sigma(\alpha) = \alpha\}$ と定めると, L^H は L/K の中間体である. また, $H \leq G = \text{Gal}(L/K)$ なので, H の元は K を固定するから, $L^H \supset K$. また, $\alpha, \beta \in L^H$ に対し, $\alpha + \beta, \alpha\beta, \frac{\alpha}{\beta}$ ($\beta \neq 0$) $\in L^H$ も H の元の準同型性より確かめられる. よって, L^H は L の部分体である. L^H を L の H による固定体・不変体という
- 中間体 $L/M/K$ に対して, $\text{for all } \alpha \in L, m_{\alpha,L}(x) \mid m_{\alpha,K}(x)$ に注意し, L/K が分離拡大より, $m_{\alpha,K}(x)$ も分離である. よって, $m_{\alpha,L}(x)$ も分離である. L/K が正規拡大より, $m_{\alpha,K}$ は L 上で分解する. よって, $m_{\alpha,L}(x)$ も L 上で分解する. よって, L/M も分離かつ正規で, Galois 拡大である. よって, $\text{Gal}(L/M)$ が定まる. これは $G = \text{Gal}(L/K)$ の部分群である

Theorem 8.1. 基本定理の前半

L/K を有限次 Galois 拡大とし, $G = \text{Gal}(L/K)$ とする. このとき

$$\begin{aligned} \{\text{部分群 } H \leq G\} &\longleftrightarrow \{\text{部分体 } L/M/K\} \\ H &\mapsto L^H \\ \text{Gal}(L/M) &\longleftarrow M \end{aligned}$$

この対応は, 互いに逆の全単射である

Proof.

$H \subset \text{Gal}(L/L^H)$ は明らかである

Remark 8.4. $H = \text{Gal}(L/L^H)$

Proof. $\#H = \#\text{Gal}(L/L^H)$ を示せば良い. L/K は分離拡大より, L/L^H もそうである. よって, 原始元定理より, $\exists \alpha \in L, \text{s.t. } L = L^H(\alpha)$ である. ここで, $f(x) = \prod_{\alpha \in H} (x - \sigma(\alpha))$ とする

$$\text{と, } \begin{cases} f(x) \in L^H[x] \\ f(\alpha) = 0 \\ \deg f = \#H \end{cases} \Rightarrow m_{\alpha,L^H} \mid f. \text{ すると, } [L : L^H] = \deg m_{\alpha,L^H} \leq \deg f = \#H \text{ となる} \quad \square$$

$\Phi \circ \Psi = L^{\text{Gal}(L/M)}$ で, $M \subset L^{\text{Gal}(L/M)}$ は明らかで, $[L : L^{\text{Gal}(L/M)}] = \#\text{Gal}(L/M) = [L : M]$ より, $M = L^{\text{Gal}(L/M)}$ である $\square$

Theorem 8.2. 基本定理の後半

- $H_1, H_2 \longleftrightarrow M_1, M_2$ とする. このとき, $H_1 \supset H_2 \iff M_1 \subset M_2$
- $\text{Gal}(L/M) = H \longleftrightarrow M = L^H$ とする. $\sigma \in \text{Gal}(L/K)$ に対して, $\sigma H \sigma^{-1} \longleftrightarrow \sigma(M)$
- $H \longleftrightarrow M$ とすると, $H \triangleleft \text{Gal}(L/K) \iff M/K$ は Galois 拡大である. さらにこのとき, $\text{Gal}(L/K)/H \cong \text{Gal}(M/K)$

Proof.

- $H_1 \supset H_2$ のとき, $M_1 = L^{H_1} \subset L^{H_2} = M_2$ である. 逆に, $M_1 \subset M_2$ のとき, $H_1 = \text{Gal}(L/M_1) \supset \text{Gal}(L/M_2) = H_2$ である
- $x \in L$ に対して, $x \in L^{\sigma H \sigma^{-1}} \iff \forall \tau \in H, \sigma \tau \sigma^{-1}(x) = x \iff \sigma^{-1}(x) \in L^H \iff x \in \sigma(L^H)$ である. よって, $\tau \in \mathcal{G}\text{-}\downarrow(L/K)$ に対して, $\tau \in \mathcal{G}\text{-}\downarrow(L/\sigma(M)) \iff \forall x \in M, \tau(\sigma(x)) = \sigma(x) \iff \sigma^{-1}\tau\sigma \in \mathcal{G}\text{-}\downarrow(L/M) \iff \tau \in \sigma \mathcal{G}\text{-}\downarrow(L/M) \sigma^{-1}$ である
- $\forall \sigma \in \text{Gal}(L/K), H = \sigma H \sigma^{-1} \iff M = \sigma(M)$. これより, $H \triangleleft G \iff M/K$ は正規拡大 $\iff M/K$ は Galois 拡大である. このとき, $p: \text{Gal}(L/K) \rightarrow \text{Gal}(M/K)$ を $\sigma \mapsto \sigma|_M$ を得られる. 準同型性は自明であり, 全射性は延長定理より示せるので, p は全射準同型である. $\text{Ker } p = \text{Gal}(L/M) = H$ なので, 準同型定理より, $\bar{p}: \text{Gal}(L/K)/H \xrightarrow{\cong} \text{Gal}(M/K)$

□

Corollary 8.1.

L/K を有限次分離拡大とすると, L/K の中間体は有限個

Proof.

$\tilde{L}$ を L/K の Galois 閉包とすると, L/K の中間体は $\text{Gal}(\tilde{L}/K) \supset H \supset \text{Gal}(\tilde{L}/L)$ をみたす部分群 H に対応するので, 有限個である □

Proposition 8.2.

L/K を Galois 拡大とし, Galois 対応において, $H_i \longleftrightarrow M_i$ とするとき, $H = \bigcap_i H_i \longleftrightarrow$

$\prod_i M_i = M$ であり, $H' = \langle H_1, \dots, H_n \rangle \longleftrightarrow \bigcap_i M_i = M'$ である

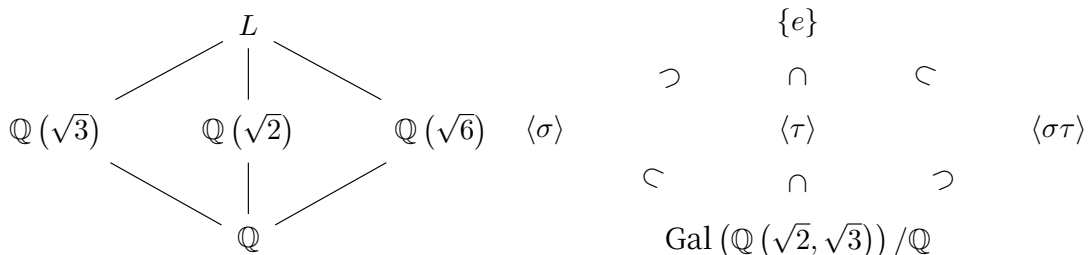
Proof.

M に対応する部分群は, $\text{Gal}(L/M) = \{\sigma \in \text{Gal}(L/K) : \sigma|_M = \text{id}_M\} = \bigcap_i \text{Gal}(L/M_i) = H$. H' に対応する部分体は $L^{H'} = \{x \in L : \forall \sigma \in H', \sigma(x) = x\} = \{x \in L : \forall i, \forall \sigma \in H_i, \sigma(x) = x\} = \bigcap_i L^{H_i} = \bigcap_i M_i$ である □

Example 8.4.

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q} = K$ とおくと, $\text{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は $\begin{cases} \sigma \longleftrightarrow (1, 0) \\ \tau \longleftrightarrow (0, 1) \end{cases}$ だった.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ の非自明な部分群は位数 2 で, $\langle \sigma \rangle = \langle (1, 0) \rangle$, $\langle \tau \rangle = \langle (0, 1) \rangle$, $\langle \sigma\tau \rangle = \langle (1, 1) \rangle$ である. それぞれの L の固定体は $L^{\langle \sigma \rangle} = \mathbb{Q}(\sqrt{3})$, $L^{\langle \tau \rangle} = \mathbb{Q}(\sqrt{2})$, $L^{\langle \sigma\tau \rangle} = \mathbb{Q}(\sqrt{6})$ である. よって, $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ の非自明な部分体は三つで



8.3 Artin の定理

Lemma 8.3.

L を体とする. $G = \{\sigma_1, \dots, \sigma_m\} \subset \text{Aut}(L) = \{\sigma : L \xrightarrow{\cong} L\}$ とし, $\alpha_1, \dots, \alpha_n \in L$ $n > m$ とすると, $\alpha_1, \dots, \alpha_n$ は L^G 上の一次従属である

Proof.

連立方程式 $\sigma_i(\alpha_1)X_1 + \dots + \sigma_i(\alpha_n)X_n = 0$ を考える. 非自明な解 $(X_1, \dots, X_n) = (c_1, \dots, c_n)$ で, 0 でない元の数 が最小のもの をとる. $\sigma_i(\alpha_1)c_1 + \dots + \sigma_i(\alpha_n)c_n = 0$ で, 並べ替えて, $c_i \neq 0$ とできる. 定数倍して, $c_1 \in L^G$ とできる. このとき, $\forall j, c_j \in L^G$ が成り立つ. そうでなかったとする. $\exists j \neq 1, \exists k \neq 1, s.t. \sigma_k(c_j) \neq c_j$ となる. σ_k を作用すると

$$\sigma_k \sigma_i(\alpha_1) \sigma_k(c_1) + \dots + \sigma_k \sigma_i(\alpha_n) \sigma_k(c_n) = 0 \quad (61)$$

$$\{\sigma_k \sigma_1, \dots, \sigma_k \sigma_m\} = \sigma_k G = G = \{\sigma_1, \dots, \sigma_m\} \quad (62)$$

なので, $\sigma_i(\alpha_1) \sigma_k(c_1) + \dots + \sigma_i(\alpha_n) \sigma_k(c_n) = 0$ となる. これより, $\sigma_i(\alpha_1)(c_1 - \sigma_k(c_1)) + \dots + \sigma_i(\alpha_n)(c_n - \sigma_k(c_n)) = 0$ となる. よって, $(c_1 - \sigma_k(c_1), \dots, c_n - \sigma_k(c_n))$ も解である. $(c_1, \dots, c_n)$ よりも, 0 でない元が 少ないので, 最小性に矛盾する $\square$

Theorem 8.3. Artin の定理

L を体とし, $G \leq \text{Aut}(L)$ を有限部分群とする. このとき

- L/L^G は Galois 拡大
- $\text{Gal}(L/L^G) = G$

Proof.

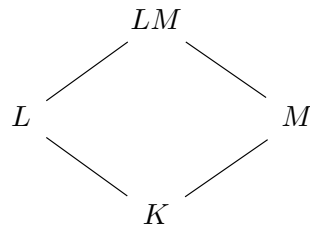
- $\alpha \in L$ とする. $\{\sigma(\alpha) : \sigma \in G\} = \{\alpha_1, \dots, \alpha_r\}$ と書く. $f(x) = \prod_{i=1}^r (x - \alpha_i)$ とおくと, f は分離多項式であり, $f(x) \in L^G[x]$ である. α は f の根なので, α は L^G 上分離的であるから, L/L^G は分離拡大である. また, $m_\alpha(x) \mid f(x)$ であり, m_α の根は全て L に属している. よって, L/L^G は正規拡大である. よって, L/L^G は Galois 拡大である
- $G \subset \text{Gal}(L/L^G)$ に注意すると, $[L : L^G] \leq \#G \leq \#\text{Gal}(L/L^G) = [L : L^G]$ なので, 全て等号である. よって, $G = \text{Gal}(L/L^G)$

$\square$

Remark 8.5.

Artin の定理から基本定理を導ける. L/K を有限次 Galois 拡大とする. $H \leq \text{Gal}(L/K)$ に対して, Artin の定理より, $H = \text{Gal}(L/L^H)$ で, これは $\Psi\Phi = id$ である

Proposition 8.3. 推進定理



このとき, LM/M も Galois 拡大で, $\pi : \text{Gal}(LM/M) \rightarrow \text{Aut}(L)$ を $\sigma \mapsto \sigma|_L$ とすると, π は同型 $\pi : \text{Gal}(LM/M) \xrightarrow{\cong} \text{Gal}(L/L \cap M)$ を導く

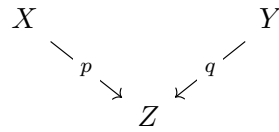
Proof.

$f \in K[x]$ を分離多項式とし, $L = K_f$ とかける. このとき, $LM = M_f$ なので, L/M が Galois 拡大である. $\sigma \in \text{Ker} \pi$ とすると, $\sigma|_M$ も $\sigma|_L$ も恒等写像なので, σ は LM での恒等写像であるから, π は単射である. $G = \text{Gal}(LM/M) \subset \text{Aut}(L)$ に Artin の定理を用いて, $G = \text{Gal}(L/L^G)$ となる, ここで, $L^G = \{x \in L : \forall \sigma \in \text{Gal}(LM/M), \sigma(x) = x\} = L \cap (LM)^{\text{Gal}(LM/M)} = L \cap M$ より, π の像は $\text{Gal}(L/L \cap M)$ である $\square$

Remark 8.6.

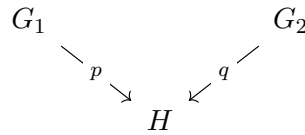
$$\frac{[LM : K]}{[M : K]} = [LM : M] = [L : L \cap M] = \frac{[L : K]}{[L \cap M : K]} \text{ から, } [LM : K] = \frac{[L : K][M : K]}{[L \cap M : K]}$$

Definition 8.2. ファイバ積



とすると, $X \times_Y Y := \{(x, y) \in X \times Y : p(x) = q(y)\}$ をファイバ積という

Remark 8.7.



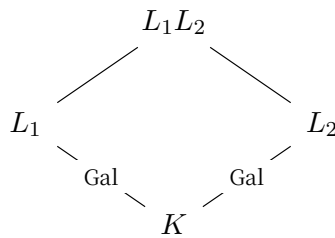
とし, p, q を有限群の全射準同型とする. このとき, $\left| G_1 \times_H G_2 \right| = \frac{|G_1||G_2|}{|H|}$ である

Proof.

$$p, q \text{ は全射準同型なので, } \forall h \in H, \begin{cases} |p^{-1}(h)| = |\text{Ker}(p)| = \frac{|G_1|}{|H|} \\ |q^{-1}(h)| = |\text{Ker}(q)| = \frac{|G_2|}{|H|} \end{cases}$$

$$\text{すると, } G_1 \times_H G_2 = \bigsqcup_{h \in H} (p^{-1}(h) \times q^{-1}(h)) = |H| \times \left(\frac{|G_1|}{|H|} \times \frac{|G_2|}{|H|} \right) = \frac{|G_1||G_2|}{|H|} \quad \square$$

Proposition 8.4.



とする. このとき, $L_1 L_2 / K$ は Galois 拡大で, $\varphi : \text{Gal}(L_1 L_2 / K) \rightarrow \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K)$ を $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ とすると, φ は単射準同型である. さらに

$$\text{Im} \varphi = \{(\sigma_1, \sigma_2) \in \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K) : \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}\} \quad (63)$$

Proof.

$L_1 = K_{f_1}, L_2 = K_{f_2}$ とし, $f_i \in K[x]$ を分離多項式とする. このとき, $L_1 L_2 = K_{f_1 f_2}$ なので, K 上正規である. また, $L_1 L_2 = L_{1, f_2} / L_1 / K$ より, K 上分離的である. よって, $L_1 L_2 / K$ は Galois 拡大である. $\sigma \in \text{Ker} \varphi$ とすると, $\sigma|_{L_1} = \text{id}_{L_1}, \sigma|_{L_2} = \text{id}_{L_2}$ なので, $L_1 L_2$ 全体で σ は恒等写像である.

よって, φ は単射である. $\sigma \in \text{Gal}(L_1 L_2 / K)$ に対して, $(\sigma|_{K_1})|_{L_1 \cap L_2} = \sigma|_{L_1 \cap L_2} = (\sigma|_{L_2})|_{L_1 \cap L_2}$ なので, $\text{Im}\varphi \subset \{(\sigma_1, \sigma_2) \in \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) : \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}\}$ である. よって, $|\text{Im}\varphi| = |\{(\sigma_1, \sigma_2) \in \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) : \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}\}|$ を示せば良い

$$|\text{Im}\varphi| = |\text{Gal}(L_1 L_2 / K)| \quad (64)$$

$$= [L_1 L_2 : K] \quad (65)$$

$$= \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]} \quad (66)$$

$$= \frac{|\text{Gal}(L_1/K)| \cdot |\text{Gal}(L_2/K)|}{|\text{Gal}(L_1 \cap L_2/K)|} \quad (67)$$

$$= |\{(\sigma_1, \sigma_2) \in \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) : \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}\}| \quad (68)$$

□

Corollary 8.2.

$L_1 \cap L_2 = K$ のとき, $\text{Gal}(L_1 L_2 / K) \cong \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K)$, $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ は同型である

Proof.

単射で位数等しいので同型

□

Example 8.5.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ を L/K とする. $(x^2 - 2)(x^2 - 3)$ の最小分解体より Galois 拡大である. $L = \mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(\sqrt{3})$ と $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ なので

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \quad (69)$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad (70)$$

9 重要な例

9.1 多項式の Galois 群

K を体とし, $\overline{K}$ を固定する. $f(x) = a_d x^d + \dots + a_0$ を分離多項式とすると, $f(x) = a_d \prod_{i=1}^d (x - \alpha_i)$ と分解できる. $X_f := \{\alpha_1, \dots, \alpha_d\}$ とおく. $K_f := (f \text{ の } K \text{ 上の最小分解体}) = K(\alpha_1, \dots, \alpha_d)$ とおくと, K_f/K は Galois 拡大である. $G_f := \text{Gal}(K_f/K)$ とおく. $\forall \sigma \in G_f, \forall \alpha \in X_f$

$$f(\sigma(\alpha)) = \sum_{i=0}^d a_i \sigma(\alpha)^i \quad (71)$$

$$= \sigma \left(\sum_{i=0}^d a_i \alpha^i \right) \quad (72)$$

$$= \sigma(0) = 0 \quad (73)$$

から, $\sigma(\alpha) \in X_f$ である. これにより, 作用 $G_f \curvearrowright X_f$ を得る. 言い換えれば, 群準同型 $i_f: G_f \rightarrow S(X_f) \cong S_d$ を得る

Lemma 9.1. i_f は単射

Proof.

$\sigma \in \text{Ker } i_f$ とする. このとき, $\sigma(\alpha_j) = \alpha_j$ である. よって, σ は $K_f = K(\alpha_1, \dots, \alpha_d)$ 上の恒等写像である $\square$

Lemma 9.2. $f(x) \in K[x]$ が既約 $\iff G_f \curvearrowright X_f$ は推移的

Proof.

延長定理より

$$\begin{array}{ccc} K_f & \dashrightarrow \exists \sigma \dashrightarrow & \overline{K} \\ | & & | \\ K(\alpha) & \dashrightarrow \exists \cong \dashrightarrow & K(\alpha') \\ | & & | \\ K & = & K \end{array}$$

K_f/K は正規なので, $\sigma: K_f \xrightarrow{\cong} K_f$ を導く $\square$

Definition 9.1. 差積・判別式

$f(x) \in K[x]$ を d 次のモニック分離多項式とすると, $f(x) = \prod_{i=1}^d (x - \alpha_i) \in K_f[x]$ と分解できる. このとき

$$\bullet \Delta(f) := \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j) \neq 0 \text{ を差積という}$$

$$\bullet D(f) := \Delta(f)^2 = \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)^2 \text{ を } f \text{ 判別式という}$$

Proposition 9.1.

$f(x) \in K[x]$ を d 次のモニック分離多項式とし, $\sigma \in G_f (\hookrightarrow S_d)$ とする. このとき

$$\bullet \sigma(\Delta(f)) = \text{sgn}(\sigma) \Delta(f)$$

$$\bullet \sigma(D(f)) = D(f)$$

Proof.

•

Lemma 9.3. $S_d \curvearrowright K[X_1, \dots, X_d]$ を $\sigma(g(X_1, \dots, X_d)) = g(\sigma(X_1), \dots, \sigma(X_d))$ と定めると, $\sigma\left(\prod_{i<j}(X_i - X_j)\right) = \text{sgn}(\sigma) \prod_{i<j}(X_i - X_j)$

Proof.

$\sigma, \sigma' \in S_d$ に対して, $\sigma(\sigma'(\Delta)) = (\sigma\sigma')(\Delta)$ であり, 置換は互換の積で表せるので, $\tau = (kl)$ 互換 $\Rightarrow \tau(\Delta) = -\Delta$ を示せば良い

$$\begin{aligned} \Delta = & \prod_{i<k \text{ なる } i} (X_i - X_k) \times \prod_{k<j \text{ なる } j \neq l} (X_k - X_j) \times \prod_{i<l \text{ なる } i \neq k} (X_i - X_l) \times \prod_{l<j \text{ なる } j} (X_l - X_j) \\ & \times (X_k - X_l) \times (\text{それ以外}) \end{aligned} \quad (74)$$

$$\begin{aligned} \tau(\Delta) = & \prod_{i<k \text{ なる } i} (X_i - X_l) \times \prod_{k<j \text{ なる } j \neq l} (X_l - X_j) \times \prod_{i<l \text{ なる } i \neq k} (X_i - X_k) \times \prod_{l<j \text{ なる } j} (X_k - X_j) \\ & \times (X_l - X_k) \times (\text{それ以外}) \end{aligned} \quad (75)$$

$$= (-1)^{l-k-1} \cdot (-1)^{l-k-1} \cdot (-1) \cdot \Delta = -\Delta \quad (76)$$

$\sigma \in G_f$ を $G_f \hookrightarrow S(\{\alpha_1, \dots, \alpha_d\}) \cong S_d$ により, S_d の元とみたものを $\tilde{\sigma}$ と書く. 定め方から, 以下は可換:

$$\begin{array}{ccc} K[X_1, \dots, X_d] & \xrightarrow{\tilde{\sigma}} & K[X_1, \dots, X_d] \\ \downarrow X_i \mapsto \alpha_i & \circlearrowleft & \downarrow X_i \mapsto \alpha_i \\ K[\alpha_1, \dots, \alpha_d] & \xrightarrow{\sigma} & K[\alpha_1, \dots, \alpha_d] \end{array}$$

すると

$$\begin{array}{ccc} \Delta & \xrightarrow{\tilde{\sigma}} & \text{sgn}(\sigma) \Delta \\ \downarrow & & \downarrow \\ \Delta(f) & \longmapsto & \sigma(\Delta(f)) = \text{sgn}(\sigma) \Delta(f) \end{array}$$

よって, 示された □

• (1) より従う □

Corollary 9.1.

$f(x) \in K[X]$ を d 次のモニック分離多項式とする. $\text{char} K \neq 2$ とする. $G_f \hookrightarrow S_d$ とみなす. このとき, Galois 対応により, $G_f \cap A_d \longleftrightarrow K(\Delta(f))$. 特に, 以下は同値

- $G_f \subset A_d$
- $\Delta(f) \in K$

- $D(f)$ は K で平方元

Proof.

$\sigma \in G_f = \text{Gal}(K_f/K)$ に対して

$$\sigma \in \text{Gal}(K_f/K(\Delta(f))) \iff \sigma(\Delta(f)) = \Delta(f) \quad (77)$$

$$\iff \text{sgn}(\sigma) = 1 \quad (78)$$

$$\iff \sigma \in G_f \cap A_d \quad (79)$$

□

Example 9.1.

- $X^2 + aX + b = 0$ の根を α, β とすると, $D(X^2 + aX + b) = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = a^2 - 4b$
- $X^3 + aX + b = 0$ の根を α, β, γ とすると, $D(X^3 + aX + b) = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = -4a^3 - 27b^2$

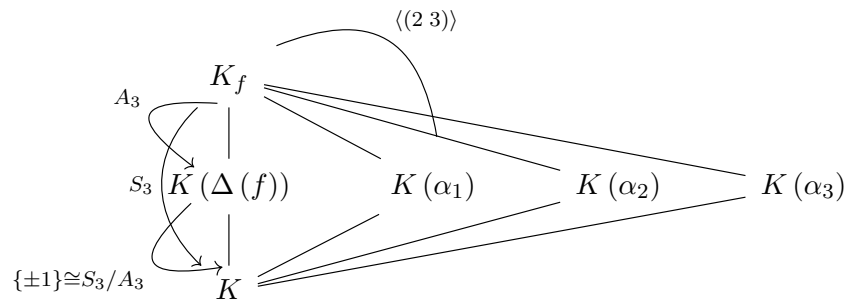
Example 9.2. 3 次多項式の Galois 群

K を $\text{char} \neq 2$ とし, $f(x) \in K[X]$ を 3 次既約モニック多項式とする

- $D(f)$ が K で平方元 $\Rightarrow G_f \cong A_3$
- $D(f)$ が K で平方元でない $\Rightarrow G_f \cong S_3$

Proof.

$G_f \hookrightarrow S(X_f) \cong S_3$ に注意. f が既約より, $G_f \curvearrowright X_f$ は推移的である. すると, $\alpha \in X_f$ に対して, $G_f/\text{Stab}(\alpha) \xrightarrow{1:1} X_f$ は $\bar{\sigma} \mapsto \sigma(\alpha)$ であるから, $|G_f|$ は 3 の倍数である. S_3 の部分群で位数が 3 の倍数のものは A_3 または S_3 のみから, $D(f)$ が K で平方元るとき, $G_f \subset A_3$. そうでないとき, $G_f \not\subset A_3$ である. また, $G_f \cong S_3$ のとき, $X_f = \{\alpha_1, \alpha_2, \alpha_3\}$ とすると, 群と体の対応は



□

Example 9.3.

- $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x] \Rightarrow D(f) = 81 = 9^2$ から, $G_f \cong A_3$
- $f(x) = x^3 + 3x + 1 \in \mathbb{Q}[x] \Rightarrow D(f) = -135$ は平方元でないから, $G_f \cong S_3$

9.2 有限体

Theorem 9.1.

$q : p^m, \mathbb{F}_{q^r}/\mathbb{F}_q$ とする. $\mathbb{F}_{q^r}/\mathbb{F}_q$ は Galois 拡大で, $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ は φ_q で生成される位数 r の巡回群である. つまり, $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) \cong \mathbb{Z}/r\mathbb{Z}$ である. ここで, φ_q は q 乗写像 (Frobenius 写像) である

Proof.

体の準同型なので単射で, 位数を考えると全射でもあるから, $\varphi_q : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_{q^r}$ が $\mathbb{F}_{q^r}$ の自己同型であることは良い. Artin の定理から, $\langle \varphi_q \rangle = \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q^{\langle \varphi_q \rangle})$ $\square$

Remark 9.1.

- あるいは, $\langle \varphi_q \rangle \leq \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ と, $\mathbb{F}_{q^r}^{\langle \varphi_q \rangle} = \mathbb{F}_q = \mathbb{F}_{q^r}^{\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)}$ から, Galois 対応より, $\langle \varphi_q \rangle = \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ を導いても良い
- さらに, $\#\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) = [\mathbb{F}_{q^r} : \mathbb{F}_q] = r$ なので, これが言えると $\langle \varphi_q \rangle = \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ から, あるいは, φ_q の位数が r を示しても良い. 巡回群 $\mathbb{F}_{q^r}^\times$ の生成元 α をとる, $\alpha^{q^r-1} = 1$ より, $\varphi_q^r(\alpha) = \alpha$ で, $\alpha^i \neq 1$ ($1 \leq i < q^r - 1$) より, $\varphi_q^j(\alpha) \neq \alpha$ ($1 \leq j < r$) である. よって, φ_q の位数は r である

9.3 円分体

K を簡単のため, 標数 0 とする. $n \geq 1$ に対して, $\mu_n(\overline{K}) := \{x \in \overline{K} : x^n = 1\}$ とおく

- $x^n - 1$ は分離多項式より, $\|\mu_n(\overline{K})\| = n$ である
char $K = 0$ より, $x^n - 1 = nx^{n-1}$ は共通根ない
- 体の乗法群の有限部分群なので, 巡回群 $\cong \mathbb{Z}/n\mathbb{Z}$ より, $\mu_n(\overline{K}) \leq \overline{K}^\times$ は部分群
- $\mu_n(\overline{K})$ を 1 の n 乗根のなす群という

Definition 9.2. 1 の原始 n 乗根

巡回群 $\mu_n(\overline{K})$ の生成元を 1 の原始 n 乗根という

Definition 9.3. totient 関数

$n \geq 1$ に対して, $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$ を Euler の totient 関数という

Remark 9.2.

- $\varphi(n) := \{a : 1 \leq a \leq n, \gcd(a, n) = 1\}$
- $n = \prod_i p_i^{e_i}$ とすると, 中国剰余定理より, $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ である. よって,
$$\varphi(n) = \prod_i \varphi(p_i^{e_i}) = \prod_i (p_i^{e_i} - p_i^{e_i-1})$$

Lemma 9.4.

$\overline{K}$ の 1 の原始 n 乗根は $\varphi(n)$ 個存在する

Proof.

$\mu_n(\overline{K})$ の生成元の一つを ζ とする. $\mu_n(\overline{K})$ の元は ζ^a ($1 \leq a < n$) とかける. ζ^a の位数は $\frac{n}{(n,a)}$ なので, ζ^a が原始 n 乗根 $\iff (n,a) = 1$ である. よって, 原始 n 乗根の個数は $\varphi(n)$ である $\square$

Remark 9.3.

- 原始 n 乗根の一つを固定したものを ζ_n と書くことが多い. これは, 同型 $\mu_n(\overline{K}) \cong \mathbb{Z}/n\mathbb{Z}$ を固定することと同じ
- $x^n - 1$ の根は $\mu_n(\overline{K}) = \{\zeta_n^a : a = 1, \dots, n-1\}$ なので, $K_{x^n-1} = K(\zeta_n)$ とかける
- $\sigma \in \text{Gal}(K(\zeta_n)/K)$ に対し, $\sigma(\zeta_n)$ も原始 n 乗根であるので, $\sigma(\zeta_n) = \zeta_n^a$ ($a \in \mathbb{Z}, (a, n) = 1$) とかける. $\overline{X}_n(\sigma) := a \pmod{n} \in (\mathbb{Z}/n\mathbb{Z})^\times$ とおく

Proposition 9.2.

$\overline{X}_n : \text{Gal}(K(\zeta_n)/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ は $\sigma \mapsto \overline{X}_n(\sigma)$ と定めると, 単射準同型である. 特に, $K(\zeta_n)/K$ はアーベル拡大である

Proof.

$\sigma, \tau \in \text{Gal}(K(\zeta_n)/K)$ とし, $\sigma(\zeta_n) = \zeta_n^a, \tau(\zeta_n) = \zeta_n^b$ とする. このとき, $(\sigma\tau)(\zeta_n) = \sigma(\zeta_n^b) = \sigma(\zeta_n)^b = \zeta_n^{ab}$ である. よって, $\overline{X}_n(\sigma\tau) = ab \pmod{n} = \overline{X}_n(\sigma) \cdot \overline{X}_n(\tau)$ である. したがって, $\overline{X}_n$ は準同型である. また, $\sigma \in \text{Ker } \overline{X}_n$ とすると, $\sigma(\zeta_n) = \zeta_n$ となり, σ は $K(\zeta_n)$ 上の恒等写像である. よって, $\overline{X}_n$ は単射である $\square$

Remark 9.4.

この単射は実は ζ_n の取り方によらない. 次のように定義することもできる. 作用 $\text{Gal}(K(\zeta_n)/K) \curvearrowright \mu_n(\overline{K})$ により, 単射準同型 $\text{Gal}(K(\zeta_n)/K) \hookrightarrow S(\mu_n(\overline{K}))$ を得る. これは, $\text{Gal}(K(\zeta_n)/K) \hookrightarrow \text{Aut}(\mu_n(\overline{K}))$ を導く. 一般に, 位数 n の巡回群 G に対して, 自然な同型 $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ がある. ($g \mapsto g^a \mapsto a \pmod{n}$). 以上を合わせて

$$\text{Gal}(K(\zeta_n)/K) \hookrightarrow \text{Aut}(\mu_n(\overline{K})) \cong (\mathbb{Z}/n\mathbb{Z})^\times \quad (80)$$

Theorem 9.2.

$K = \mathbb{Q}$ のとき, $n \geq 1$ に対して, $\overline{X}_n : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$ は同型である

以下, $K = \mathbb{Q}$ とする. $n \geq 1$ に対して

$$\Phi_n(x) := \prod_{\zeta \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (x - \zeta) = \prod_{\substack{1 \leq a \leq n \\ \gcd(a, n) = 1}} (x - \zeta_n^a) \quad (81)$$

とおく (第 n 円分多項式)

- $\deg \Phi_n(x) = \varphi(n)$
- $\mu_n(\overline{\mathbb{Q}}) := \{\zeta \in \overline{\mathbb{Q}} : \zeta^n = 1\} = \bigsqcup_{d|n} \{\zeta \in \overline{\mathbb{Q}} : \zeta \text{ は } 1 \text{ の原始 } d \text{ 乗根}\}$ なので, $x^n - 1 = \prod_{d|n} \Phi_d(x)$ がわかる

Example 9.4.

$x^n - 1 = \prod_{d|n} \Phi_d(x)$ より, $\Phi_1, \Phi_2, \dots$ を計算できる:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = \frac{x^2 - 1}{\Phi_1(x)} = x + 1$
- $\Phi_3(x) = \frac{x^3 - 1}{\Phi_1(x)} = x^2 + x + 1$
- $\Phi_4(x) = \frac{x^4 - 1}{\Phi_2(x) \cdot \Phi_1(x)} = x^2 + 1$

素数 p に対して, $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ である

Remark 9.5.

係数 $-1, 0, 1$ 以外も出てくる. 例えば, $\Phi_{105}(x) = x^{48} + x^{47} + \cdots - 2x^{41} - x^{40} + \cdots$

Lemma 9.5.

$\Phi_n(x)$ はモニックで整係数多項式である

Proof.

定義よりモニックは明らかで, $\Phi[x]$ を帰納法で示す

$n = 1$ のとき, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ である

n 未満で正しいとすると, $P(x) := \prod_{\substack{d|n \\ d < n}} \Phi_d(x)$ とおく. $P(x)$ はモニックで, 帰納法の仮定

より, $P(x) \in \mathbb{Z}[x]$ であるから, $x^n - 1$ を $\mathbb{Z}[x]$ の中で $P(x)$ で割れる: $\exists Q(x), \exists R(x) \in \mathbb{Z}[x], s.t. x^n - 1 = P(x)Q(x) + R(x), \deg R < \deg P$

一方, $\mathbb{C}[x]$ において, $x^n - 1 =$

$\prod_{d|n} \Phi_d(x) = P(x)\Phi_n(x)$ であるから, $P \cdot Q + R = P \cdot \Phi_n$ であり, $R = P \cdot (\Phi_n - Q)$ である. $\Phi_n - Q \neq 0$ としたら, $\deg(\text{RHS}) \geq \deg P$ となり矛盾. よって, $\Phi_n = \mathbb{Q}$ となり, これは $\mathbb{Z}[x]$ に属している $\square$

Proposition 9.3.

$\Phi_n(x) = m_{\zeta_n}(x)$ である. すなわち, $\Phi_n(x)$ は $\mathbb{Q}$ 上既約である

Proof.

$\Phi_n(\zeta_n) = 0$ より, $m_{\zeta_n}(x) \mid \Phi_n(x)$ である

Lemma 9.6. $\forall p \nmid n$ を素数とすると, ζ_n^p も $m_{\zeta_n}(x)$ の根である

Proof.

$\exists p \nmid n, m_{\zeta_n}(\zeta_n^p) \neq 0$ とする. ζ_n^p は $\Phi_n(x)$ の根ではあるから, $\Phi_n(x) = m_{\zeta_n}(x)f(x)$ かつ $f(\zeta_n^p) = 0$ となる $\deg f \geq 1$ の多項式 $f(x) \in \mathbb{Z}[x]$ が存在する. $f(x^p)$ は ζ_n を根に持つので, $m_{\zeta_n}(x) \mid f(x^p)$ である. $(\text{mod } p)$ して, $\overline{m_{\zeta_n}(x)} \mid \overline{f(x^p)} = \overline{f(x)}^p$ となるから, $\overline{m_{\zeta_n}(x)}$ と $\overline{f(x)}$ は $\mathbb{F}_p$ 上で共通因子を持つ. したがって, $\Phi_n(x) = m_{\zeta_n}(x) \cdot f(x)$ は分離的でない. 一方, $x^n - 1$ は $p \nmid n$ より分離的なので, その因子である $\Phi_n(x)$ も分離的である. 矛盾 $\square$

$\square$

Theorem 9.3.

$\overline{x_n} : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ は同型である. その対応は $\zeta_n^k \mapsto \zeta_n^{ka} \longleftrightarrow a \pmod{n}$

Proof.

単射準同型は示した

$$|\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \quad (82)$$

$$= \deg m_{\zeta_n}(x) = \deg \Phi_n(x) = \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times \quad (83)$$

よって, 位数が等しいので同型である $\square$

Example 9.5.

p を素数とすると, $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ は位数 $p - 1$ の巡回群である

$\text{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^\times$ の生成元 3 で

$$(\mathbb{Z}/17\mathbb{Z})^\times = \langle 3 \rangle \supset \langle 3^3 \rangle \supset \langle 3^4 \rangle \supset \langle 3^8 \rangle \supset \langle 3^{16} \rangle = \{1\} \quad (84)$$

対応する $\mathbb{Q}$ の拡大の列 $\mathbb{Q} = K^{(3)} \subset_2 K^{(9)} \subset_2 K^{(13)} \subset_2 K^{(16)} = K^{\{1\}} = K$ である. K は二次拡大

の列で得られるので, K の元は作図可能. 特に, $\begin{cases} \cos\left(\frac{2\pi}{17}\right) = \frac{1}{2}(\zeta_{17} + \zeta_{17}^{-1}) \\ \sin\left(\frac{2\pi}{17}\right) = \frac{1}{2i}(\zeta_{17} - \zeta_{17}^{-1}) \end{cases}$ も作図可能

である. よって, 正 17 角形は作図可能である

$\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$ で, $\mathbb{Q}(\zeta_7) \subset_2 \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \subset_3 \mathbb{Q}$ であるから, 二次拡大の積み重ねではないので, $\cos\left(\frac{2\pi}{7}\right)$ は作図不可能である

Remark 9.6.

$$(\mathbb{Z}/n\mathbb{Z})^\times \left(\begin{array}{c} \mathbb{Q}(\zeta_n) \\ | \\ \forall M \\ | \\ \mathbb{Q} \end{array} \right) \supset = H$$

$H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ は正規部分群であるから, $M/\mathbb{Q}$ も Galois 拡大である. $\text{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times / H$ もアーベル群である. 逆に, $\forall M/\mathbb{Q}$ は有限次アーベル拡大であるとき, $\exists n \in \mathbb{N}, s.t. M \subset \mathbb{Q}(\zeta_n)$ も成り立つ (Kronecker-Weber の定理)

Example 9.6.

2 次体は $\mathbb{Q}$ のアーベル拡大, $d \in \mathbb{Z}$ を平方因子のない整数とすると

$$\begin{cases} d \equiv 1 \pmod{4} \implies \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta_{4|d|}) \\ d \equiv 2, 3 \pmod{4} \implies \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta_{4|d|}) \end{cases}$$