博 士 論 文

多項式の分解の挙動を記述する剰余とその応用

平成２５年９月

高知大学大学院総合人間自然科学研究科

応用自然科学専攻

黒岩　朝

目 次

記号の説明

$\mathbb{C}$: 複素数体
$\mathbb{R}$: 実数体
$\mathbb{Q}$: 有理数体
$\mathbb{Z}$: 有理整数環 (整数全体のなす環)
$\mathbb{Z}_{\geq 0}$: 0 以上の整数全体の集合
$\mathbb{N}$: 自然数全体の集合
$\sharp A$: 集合 A の元の個数
$\mathrm{lcm}(a_1, \ldots, a_n)$: $a_1, \ldots, a_n$ の最小公倍元
$\gcd(a_1, \ldots, a_n)$: $a_1, \ldots, a_n$ の最大公約元
$a \mid b$: a は b の約元もしくは b は a の倍元
ζ_n : 1 の n 乗根で 1 でないもの
$[L : K]$: 体 K の有限次拡大 L の拡大次数
$\mathrm{Gal}(L/K)$: 体 K の有限次ガロア拡大 L におけるガロア群

第1章　導入

代数学の主な分野の一つである整数論では、古くから素数について成り立つ様々な性質について研究がなされてきた。そこで用いられた考え方や手法は、代数幾何学をはじめとして代数学全体の発展にも影響を及ぼした。

代数学でしばしば扱われるテーマである、”多項式の分解に関する法則”は素数とも密接に関わっており、それを記述するという研究は整数論における大きなテーマである。

素数 p に対して、$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は p 個の元を持つ体をなす。この体を有限素体という。文献 [2] において、次のような問題が挙げられた。

問題 1.1. 最高次係数が 1 である一変数整数係数多項式が与えられたとき、それがどのような素数を法とする有限素体において、相異なる一次式の積に分解するかを判定する解析関数を構成せよ。

この問題は整数論においての大きな結果である**類体論**と呼ばれる理論を応用することにより、ある条件を満たす多項式については解決されることが知られている。その条件とは、

”(有理数体上既約な) 多項式が一次式の積に分解される有理数体の拡大体 (**ガロア拡大**という) の自己同型写像のなす群 (**ガロア群**) が可換群である (この拡大を**アーベル拡大**という)”

という条件であり、これを満たす多項式であれば、類体論の結果を用いて、有限素体上で多項式が分解するか否かの判定法が簡明な形で得られる。

しかし、ガロア群が非可換群であるときは類体論による結果を使えず、上記の判定法を単純に一般化した形での判定法は通用しないことが知られている。

実は文献 [2] で挙げられた**問題 1.1.** は、ガロア群が非可換群であるときでも成り立つ類体論 (非可換類体論) が構築されれば解決されるであろ

う問題の一つとして挙げられたものである。**問題 1.1.** は (非可換類体論を構築したわけではないが) 肯定的に解決できることを、**定理 5.1.** から示した。

さらに素数と多項式の分解の関係を調べるため、上記の問題の逆問題、すなわち
「与えられた分解の一部の様子から元の多項式の候補が得られるか」
という問題 (第 6 章 **問題 6.2.**) を考えた。この問題は、**定理 6.3.** により部分的に解決した。

本論文の構成について述べる。

第 2 章では、整数論の基本的な道具である代数体や、その整数環の性質について述べた。特に、整数環のイデアルの、素イデアル分解の一意性について述べた。
第 3 章では、類体論を代数体に応用することによって得られる結果について述べた。特に、素イデアルの分解について、簡明な形の判定法が得られることを見た。
第 4 章では、本論文で扱う記号や語句を定義した。**定義 4.1.** では本論文の要である、多項式の有限素体上での分解の挙動を記述する剰余を定義した。これは、割り算の原理における剰余によって得られるものである。さらに、**定義 4.1.** で定義した剰余の基本的な性質について述べた。
第 5 章では、本論文の一つ目の主定理である**定理 5.1.** を述べた。この定理により、上で挙げた文献 [2] の問題を解決できる。
第 6 章では、**定義 4.1.** で定めた剰余を用いた**問題 6.2.** を挙げた。これは、
「与えられた分解の挙動を示すような整数係数多項式を求めよ」
という問題である。その後、本論文の二つ目の主定理である**定理 6.3.** について述べた。

第2章　代数的整数論

任意の整数を素因数分解するとき、その分解が一意的であることはよく知られている事実である。しかし、より一般的な環においては、任意の元が一意的に分解されるとは限らない。この事実は整数論を展開していく上で大きな障害となった。

その後、整数論において扱う基本的な環において、任意のイデアルは一意的に素イデアル分解されることが示された。この事実は整数論のさらなる発展を促すだけでなく、代数学全体にも影響を及ぼす概念を生み出させるきっかけとなった。

2.1　準備

定義 2.1. $f \in \mathbb{Z}[x] \setminus \{0\}$ が**原始多項式**であるとは、各係数の最大公約数が 1 であることである。

命題 2.2. 任意の有理数係数多項式 $f \in \mathbb{Q}[x] \setminus \{0\}$ に対し、原始多項式 $g \in \mathbb{Z}[x]$ と、互いに素な整数 a, b が存在して、$f = \dfrac{a}{b}\, g$ が成り立つ。

Proof. $^{\forall} f \in \mathbb{Q}[x] \setminus \{0\}$ は、

$$f = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} \quad (a_i, b_i\ (\neq 0) \in \mathbb{Z}、\gcd(a_i, b_i) = 1)$$

と書ける。ここで、$b = \mathrm{lcm}(b_0, \ldots, b_n)$ ととると、$^{\exists} c_i \in \mathbb{Z}$ s.t. $b = b_i c_i$ より、

$$f = \frac{1}{b}(a_n c_n x^n + \cdots + a_1 c_1 x + a_0 c_0)$$

である。次に、$a = \gcd(a_0, \ldots, a_n)$ ととると、$^{\exists} d_i \in \mathbb{Z}$ s.t. $a_i c_i = a d_i$ より、

$$f = \frac{a}{b}(d_n x^n + \cdots + d_1 x + d_0)$$

が成り立つ。 □

補題 2.3 (ガウスの補題)**.** $f,\ g \in \mathbb{Z}[x]$ が原始多項式ならば、fg も原始多項式である。

Proof. $f,\ g$ は

$$f = a_m x^m + \cdots + a_1 x + a_0、\ g = b_n x^n + \cdots + b_1 x + b_0 \quad (a_i, b_j \in \mathbb{Z})$$

と書ける。f, g は原始多項式であることから、各素数 p に対し、p で割り切れない最初の係数を a_s, b_t とすれば、fg の x^{s+t}の係数 c_{s+t} は

$$c_{s+t} = a_0 b_{s+t} + \cdots + a_s b_t + \cdots + a_{s+t} b_0 \equiv a_s b_t \not\equiv 0 \mod p$$

である。よって、fg は原始多項式である。 □

命題 2.4. $M \neq \{0\}$ を有限生成 $\mathbb{Z}$ 加群とし、

$$M = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

とする。また、N を M の任意の部分 $\mathbb{Z}$ 加群とする。このとき、$^{\exists}\beta_1, \ldots, \beta_m \in N\ s.t.\ m \leq n$、

$$N = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m、$$

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} k_{11} & \cdots & \cdots & \cdots & k_{1n} \\ & \ddots & & & \vdots \\ 0 & & k_{mm} & \cdots & k_{mn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad (k_{ii} \in \mathbb{Z}_{\geq 0})$$

Proof. まず、$\mathbb{Z}$ の部分集合 A を、

$$A = \{k \in \mathbb{Z} \mid k\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \in N \ \text{ for some } \ k_2, \ldots, k_n \in \mathbb{Z}\}$$

とおく。このとき A は $\mathbb{Z}$ の部分群となり、$\mathbb{Z}$ は加法に関して巡回群であるから、

$$^{\exists}k_{11} \in \mathbb{Z} \ \text{ s.t. } \ A = \mathbb{Z}k_{11},\ k_{11} \geq 0$$

となる。ゆえに、$^{\exists}\beta_1 \in N \quad \text{s.t.}$

$$\beta_1 = k_{11}\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \ \text{ for some } \ k_2, \ldots, k_n \in \mathbb{Z}$$

となる。ここから帰納法によって示そう。

$n = 1$ のときは、

$$N = \mathbb{Z}\beta_1,\ \beta_1 = k_{11}\alpha_1\ (k_{11} \geq 0)$$

と表せるので、命題は成り立つ。

次に、$n-1$ 個以下の元より成る生成系を持つ $\mathbb{Z}$ 加群に対して、命題が成り立つと仮定する。ここで、

$$M' = \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n\ (\neq \{0\})$$

$$N' = N \cap M'$$

とおく。$^{\forall}\alpha \in N$ は

$$\alpha = \sum_{i=1}^{n} h_i\alpha_i\ (h_i \in \mathbb{Z})$$

と書ける。これより、$h_1 \in A = \mathbb{Z}k_{11}$ である。よって、$^{\exists}m \in \mathbb{Z}$ s.t. $h_1 = mk_{11}$ である。

$$\begin{aligned}\alpha - m\beta_1 &= (h_1 - mk_{11})\alpha_1 + (h_2 - mk_2)\alpha_2 + \cdots + (h_n - mk_n)\alpha_n \\ &= (h_2 - mk_2)\alpha_2 + \cdots + (h_n - mk_n)\alpha_n \\ &\in N \cap M' = N'\end{aligned}$$

であるから、$\alpha \in \mathbb{Z}\beta_1 + N'$ を得る。したがって、

$$N = \mathbb{Z}\beta_1 + N'$$

が成り立つ。ここで、

$$N' \subset M' = \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$$

であるから、仮定より $^{\exists}\beta_2, \ldots, \beta_m \in N'$ s.t. $m \leq n$、

$$N' = \mathbb{Z}\beta_2 + \cdots + \mathbb{Z}\beta_m、$$

$$\begin{pmatrix} \beta_2 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} k_{22} & \cdots & \cdots & \cdots & k_{2n} \\ & \ddots & & & \vdots \\ 0 & & k_{mm} & \cdots & k_{mn} \end{pmatrix} \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \quad (k_{ii} \in \mathbb{Z}_{\geq 0}\ (2 \leq i \leq m))$$

が成り立つ。ここに $\beta_1 = k_{11}\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n$ を加えれば、

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} k_{11} & k_2 & \cdots & \cdots & \cdots & k_n \\ & k_{22} & \cdots & \cdots & \cdots & k_{2n} \\ & & \ddots & & & \vdots \\ 0 & & & k_{mm} & \cdots & k_{mn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \vdots \\ \alpha_n \end{pmatrix} \quad (k_{ii} \in \mathbb{Z}_{\geq 0})$$

$$N = \mathbb{Z}\beta_1 + N' = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m$$

が成り立つ。よって n のときも示された。 □

2.2　代数体

定義 2.5. 体 L を体 K の拡大体とする。L の元 α が K 上**代数的** であるとは、α がある (0 でない) K 係数一変数多項式の根であること、すなわち $f(\alpha) = 0$ を満たす多項式 $f(x) \in K[x] \setminus 0$ が存在することである。任意の L の元が K 上代数的であるとき、L は K 上代数的であるという。

特に、複素数 α が $\mathbb{Q}$ 上代数的であるとき、α を**代数的数** という。

例えば、$\sqrt{2}$ は $x^2 - 2 \in \mathbb{Q}[x]$ の根であるから代数的数である。また、自然対数 e、円周率 π は代数的数ではないことが知られている。しかし、$x - e$、$x - \pi \in \mathbb{R}[x]$ であるから、e、π は $\mathbb{R}$ 上代数的である。

定理 2.6. 体 L が体 K の有限次拡大体であれば、L は K 上代数的である。

Proof. $n = [L : K]$ とおく。$L \ni {}^{\forall}\alpha$ に対し、$\{1,\ \alpha, \ldots,\ \alpha^n\}$ は $n+1$ 個の元からなるので K 上一次従属である。よって、少なくとも一つは 0 でない K の元 $c_0, \ldots,\ c_n$ が存在して、

$$\sum_{i=0}^{n} c_i \alpha^i = 0$$

なる関係式をみたす。これは、α が

$$\sum_{i=0}^{n} c_i x^i \ \in K[x]$$

の根であることを示している。したがって、α は K 上代数的である。 □

定義 2.7. 体 L を体 K の拡大体とする。K 上代数的な L の元 α を根に持つ K 係数一変数多項式のうち、次数が最小で、最高次係数が 1 である (**モニック** であるという) ものを、α の (K 上の) **最小多項式** という。

命題 2.8. 体 L を体 K の拡大体とする。K 上代数的な L の元 α の最小多項式は一意に決まる。さらに、最小多項式は K 上既約である。

Proof. $f,\ g$ を α の K 上の次数 n の最小多項式とする。$f(x)-g(x)\in K[x]$ は α を根に持つ。また、$f,\ g$ ともにモニックであるから、

$$\deg(f(x)-g(x))<n$$

である。次数の最小性により、

$$f(x)-g(x)=0$$

を得る。したがって $f(x)=g(x)$ より、最小多項式は一意に決まる。

次に、α の最小多項式 $f(x)\in K[x]$ が可約であるとする。つまり、$^{\exists}p(x),\ q(x)\in K[x]\setminus K$ s.t.

$$f(x)=p(x)\ q(x)、\quad \deg(p(x)),\ \deg(q(x))<\deg(f(x))$$

である。

$$0=f(\alpha)=p(\alpha)\ q(\alpha)$$

より、$p(\alpha)\ =\ 0$ もしくは $q(\alpha)\ =\ 0$ だが、$f(x)$ の次数の最小性に反する。 □

定義 2.9. 有理数体 $\mathbb{Q}$ の有限次拡大体を**代数体** という。$\mathbb{Q}$ 上の拡大次数が n であれば、$\boldsymbol{n}$**次代数体** という。

代数体は $\mathbb{Q}$ の有限次拡大体であるから、**定理 2.6.** より、代数体の元は全て代数的数である。しかし代数的数全体のなす体は、いくらでも次数の大きい関係式が存在するため $\mathbb{Q}$ 上無限次拡大である。

定理 2.10. $\overline{\mathbb{Q}}\ =\ \{\alpha\ \in\ \mathbb{C}\ |\ \alpha\ :$ 代数的数 $\}$ は体である。この体を $\mathbb{Q}$ の**代数閉包** という。

Proof. $\overline{\mathbb{Q}}\ni{}^{\forall}\alpha,\beta$ とする。α の $\mathbb{Q}$ 上の最小多項式を $f(x)$ と書くと、

$$\mathbb{Q}(\alpha)\simeq\mathbb{Q}[x]/(f(x))$$

より、$\mathbb{Q}(\alpha)$ は代数体である。

さらに $\mathbb{Q}[x]\subset\mathbb{Q}(\alpha)[x]$ より、β は $\mathbb{Q}(\alpha)$ 上代数的である。よって、

$$\mathbb{Q}(\alpha,\beta)=(\mathbb{Q}(\alpha))(\beta)$$

は代数体である。したがって、

$$\alpha \pm \beta, \alpha\beta, \alpha^{-1}\ (\alpha \neq 0 \text{ のとき}) \in \mathbb{Q}(\alpha, \beta) \subset \overline{\mathbb{Q}}$$

を得る。 □

定理 2.11. $\alpha, \beta \in \mathbb{C}$ が代数的数であるとする。このとき、$^{\exists}\theta \in \mathbb{Q}(\alpha, \beta)$ *s.t.* $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ が成り立つ。

Proof. α の最小多項式を f、β の最小多項式を g とし、f の ($\mathbb{C}$ 上の) 根を $\alpha_1\ (=\alpha), \ldots,\ \alpha_m$、$g$ の根を $\beta_1\ (=\beta), \ldots,\ \beta_n$ とする。このとき、

$$c\alpha_i + \beta_j \quad (1 \leq i \leq m、1 \leq j \leq n)$$

が全て異なるように $c \in \mathbb{Q}$ を選ぶことが可能である。なぜならば、

$$c\alpha_i + \beta_j = c\alpha_k + \beta_l \iff c = \frac{\beta_l - \beta_j}{\alpha_i - \alpha_k} \quad (f \text{ は重根を持たないので、} \alpha_i - \alpha_k \neq 0)$$

であるから、どの $\dfrac{\beta_l - \beta_j}{\alpha_i - \alpha_k}$ にも一致しない c をとればよい。

そこで、そのような c を一つ固定し、

$$\theta = c\alpha + \beta、\ h(x) = g(\theta - cx) \in (\mathbb{Q}(\theta))[x]$$

ととる。$\beta = \theta - c\alpha$ であるから、$h(\alpha) = 0$ であり、$i \neq 1$ のとき、$h(\alpha_i) \neq 0$ である。よって、$f \in \mathbb{Q}[x] \subset (\mathbb{Q}(\theta))[x]$ であることより

$$\gcd(f, h) = x - \alpha \in (\mathbb{Q}(\theta))[x]$$

である。よって、$\alpha, \beta \in \mathbb{Q}(\theta)$ を得る。したがって、

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$$

が成り立つ。 □

定理 2.12. K を n 次代数体とすると、$^{\exists}\theta \in K\ s.t.\ K = \mathbb{Q}(\theta)$ と書ける。

また、K の $\mathbb{Q}$ 上の基底を $w_1, \ldots, w_n$、K から $\mathbb{C}$ の中への相異なる同型対応の全体を $\sigma_1, \ldots, \sigma_n$ とする。このとき、

$$\Omega = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{pmatrix}$$

は正則行列である。

Proof. K を n 次代数体とすると、K の $\mathbb{Q}$ 上の基底 $\{d_1, \ldots, d_n\}$ がとれて、

$$K = \mathbb{Q}(d_1, \ldots, d_n)$$

と書ける。**定理 2.11.** より、

$$^{\exists}\theta_1 \in K \text{ s.t. } \mathbb{Q}(d_1, d_2) = \mathbb{Q}(\theta_1)$$

である。$\mathbb{Q}(d_1, d_2, d_3) = \mathbb{Q}(\theta_1, d_3)$ より、**定理 2.11.** を繰り返し使うことによって、

$$^{\exists}\theta \in K \text{ s.t. } K = \mathbb{Q}(\theta)$$

である。このとき、$\{1, \theta, \ldots, \theta^{n-1}\}$ は K の $\mathbb{Q}$ 上の基底である。よって、

$$(w_1, \ldots, w_n) = (1, \theta, \ldots, \theta^{n-1})A \quad (A \in \mathrm{GL}_n(\mathbb{Q}))$$

と書ける。この式に σ_i を作用させると、

$$(\sigma_i(w_1), \ldots, \sigma_i(w_n)) = (1, \sigma_i(\theta), \ldots, \sigma_i(\theta)^{n-1})A$$

となる。よって、

$$\Omega = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{pmatrix} = \begin{pmatrix} 1 & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\theta) & \cdots & \sigma_n(\theta)^{n-1} \end{pmatrix} A$$

を得る。ここで、

$$\begin{vmatrix} 1 & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\theta) & \cdots & \sigma_n(\theta)^{n-1} \end{vmatrix} = \pm \prod_{i<j} (\sigma_i - \sigma_j)$$

が成り立つ (左辺を **ヴァンデルモンドの行列式**という)。$i \neq j$ ならば、$\sigma_i \neq \sigma_j$ であるから、

$$\pm \prod_{i<j} (\sigma_i - \sigma_j) \neq 0$$

である。したがって、$|\Omega| \neq 0$ より、Ω は正則行列である。 □

定義 2.13. K を n 次代数体、K の $\mathbb{Q}$ 上の基底を $\{w_1, \ldots, w_n\}$ とする。$^{\forall}\alpha \in K$ に対し、

$$\alpha(w_1, \ldots, w_n) = (w_1, \ldots, w_n)A \quad (A \in \mathrm{GL}_n(\mathbb{Q}))$$

と表せる。このとき、$\mathrm{trace}\, A$ を K における α の **トレース** といい、$T_K(\alpha)$ と書く。また、$|A|$ を K における α の **ノルム** といい、$N_K(\alpha)$ と書く。

定理 2.14. K を n 次代数体、K から $\mathbb{C}$ の中への相異なる同型対応の全体を $\sigma_1, \ldots, \sigma_n$ とする。このとき、$^\forall\alpha \in K$ に対し、

$$T_K(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)、N_K(\alpha) = \sigma_1(\alpha)\cdots\sigma_n(\alpha)$$

が成り立つ。よって、トレースとノルムは基底のとり方によらない。

Proof. $^\forall\alpha \in K$ とし、K の $\mathbb{Q}$ 上の基底を $\{w_1, \ldots, w_n\}$ とする。

$$\alpha(w_1, \ldots, w_n) = (w_1, \ldots, w_n)A \quad (A \in \mathrm{GL}_n(\mathbb{Q}))$$

と表せる。また、

$$A_0 = \begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix}、\ \Omega = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{pmatrix}$$

とおく。よって、

$$A_0\Omega = \begin{pmatrix} \sigma_1(\alpha)\sigma_1(w_1) & \cdots & \sigma_1(\alpha)\sigma_1(w_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha)\sigma_n(w_1) & \cdots & \sigma_n(\alpha)\sigma_n(w_n) \end{pmatrix} = \Omega A$$

である。**定理 2.12.** より、Ω は正則であるから、

$$A_0 = \Omega A \Omega^{-1}$$

を得る。ゆえに、

$$T_K(\alpha) = \text{trace } A = \text{trace } \Omega A\Omega^{-1} = \text{trace } A_0 = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

$$N_K(\alpha) = |A| = |\Omega A\Omega^{-1}| = |A_0| = \sigma_1(\alpha)\cdots\sigma_n(\alpha)$$

が成り立つ。 □

定理 2.15. K を n 次代数体、L を K を含む l 次代数体で K 上 m 次拡大とする。このとき $l = mn$ であって、$^\forall\alpha \in K$ に対し、

$$T_L(\alpha) = mT_K(\alpha)、\ N_L(\alpha) = (N_K(\alpha))^m$$

が成り立つ。

Proof. K の $\mathbb{Q}$ 上の基底を $\{w_1, \ldots, w_n\}$、L の K 上の基底を $\{v_1, \ldots, v_m\}$ とすると、L の $\mathbb{Q}$ 上の基底は $D = \{w_i v_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ であり、$l = mn$ である。

$^\forall \alpha \in K$ に対し、

$$\alpha(w_1, \ldots, w_n) = (w_1, \ldots, w_n)A \quad (A \in \mathrm{GL}_n(\mathbb{Q}))$$

とする。このとき α を D に作用させると、

$$\begin{aligned}
&\alpha(w_1v_1, \ldots, w_nv_1, w_1v_2, \ldots, w_nv_2, \ldots, w_1v_m, \ldots, w_nv_m) \\
&= (\alpha(w_1, \ldots, w_n)v_1, \ldots, \alpha(w_1, \ldots, w_n)v_m) \\
&= ((w_1, \ldots, w_n)Av_1, \ldots, (w_1, \ldots, w_n)Av_m) \\
&= ((w_1v_1, \ldots, w_nv_1), \ldots, (w_1v_m, \ldots, w_nv_m))B \\
&= (w_1v_1, \ldots, w_nv_1, w_1v_2, \ldots, w_nv_2, \ldots, w_1v_m, \ldots, w_nv_m)B
\end{aligned}$$

ただし、

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

よって、

$$T_L(\alpha) = \mathrm{trace}B = m \cdot \mathrm{trace}A = mT_K(\alpha)$$

$$N_L(\alpha) = |B| = |A|^m = (N_K(\alpha))^m$$

を得る。 □

系 2.16. K を n 次代数体とする。このとき、$^\forall \alpha \in \mathbb{Q}$ に対し、

$$T_K(\alpha) = n\alpha、\quad N_K(\alpha) = \alpha^n$$

である。

Proof.

$$T_{\mathbb{Q}}(\alpha) = \alpha、\quad N_{\mathbb{Q}}(\alpha) = \alpha$$

と、**定理 2.15.** より分かる。 □

命題 2.17. K を n 次代数体とする。このとき、

$$(1)\quad T_K : K \longrightarrow \mathbb{Q}\ ;\ \alpha \longmapsto T_K(\alpha)$$

は $\mathbb{Q}$ 線型写像である。すなわち、$\alpha, \beta \in K$、$a, b \in \mathbb{Q}$ に対し、

$$T_K(a\alpha + b\beta) = aT_K(\alpha) + bT_K(\beta)$$

が成り立つ。

$$(2)\quad N_K : K \longrightarrow \mathbb{Q}\ ;\ \alpha \longmapsto N_K(\alpha)$$

は積を保存する。すなわち、$\alpha, \beta \in K$ に対し、

$$N_K(\alpha\beta) = N_K(\alpha)N_K(\beta)$$

が成り立つ。

Proof. K から $\mathbb{C}$ の中への相異なる同型対応の全体を $\sigma_1, \ldots, \sigma_n$ とすると、**定理 2.14.** から従う。 □

命題 2.18. K を n 次代数体とし、K の $\mathbb{Q}$ 上の基底を $\{w_1, \ldots, w_n\}$ とする。このとき、$T_K(w_i w'_j) = \delta_{ij}$ (クロネッカーのデルタ) となる K の $\mathbb{Q}$ 上の基底 $\{w'_1, \ldots, w'_n\}$ が存在する。

Proof. ベクトル空間の双対空間の議論から、次が成り立つ。

V を体 K 上の有限次ベクトル空間、$B : V \times V \longrightarrow K$ を非退化双線型写像とする。このとき、V の任意の K 上の基底 $\{w_1, \ldots, w_n\}$ に対して、$B(w_i w'_j) = \delta_{ij}$ となる V の K 上の基底 $\{w'_1, \ldots, w'_n\}$ が存在する。

あとは、$B : K \times K \longrightarrow \mathbb{Q}\ ;\ (x, y) \longmapsto T_K(xy)$ が非退化双線型写像であることを示せばよい。まず、$(0 \neq)\ y \in K$ を固定して、$B'_y(x) = T_K(xy)\ \ ({}^{\forall}x \in K)$ とおく。このとき、**系 2.16.** より、

$$B'_y(y^{-1}) = T_K(1) = n \neq 0 \text{ より、} B'_y \neq 0$$

を得る。同様に、$(0 \neq)\ x \in K$ を固定して、$B''_x(y) = T_K(xy)\ \ ({}^{\forall}y \in K)$ とおくと、

$$B''_x \neq 0$$

を得る。よって、B は非退化である。B が双線型写像であることは、**命題 2.17.** より従う。 □

2.3 代数的整数

定義 2.19. A, B を環とし、$A \subset B$ とする。B の元 α が A 上**整** であるとは、α がある (0 でない) A 係数モニック一変数多項式の根であること、すなわち $f(\alpha) = 0$ を満たすモニックな多項式 $f(x) \in A[x] \setminus 0$ が存在することである。任意の B の元が A 上整であるとき、B は A 上整であるという。

特に、複素数 α が $\mathbb{Z}$ 上整であるとき、α を**代数的整数** という。

命題 2.20. (1) $\alpha \in \mathbb{Q}$ が代数的整数であるならば、$\alpha \in \mathbb{Z}$ である。

(2) α が代数的数であるならば、ある 0 でない整数 m が存在して、$m\alpha$ は代数的整数となる。

Proof. (1) $\mathbb{Q} \ni \alpha$ とすると、$\alpha = \dfrac{d}{c}$ ($c, d \in \mathbb{Z}$、c, d は互いに素) と書ける。α は代数的整数より、

$$\left(\frac{d}{c}\right)^n + a_{n-1}\left(\frac{d}{c}\right)^{n-1} + \cdots + a_0 = 0 \quad (a_i \in \mathbb{Z})$$

が成り立つ。よって、

$$d^n = -c(a_{n-1}d^{n-1} + \cdots + a_0 c^{n-1})$$

であるから、$c \mid d^n$ である。c と d は互いに素であるから、$c = \pm 1$ を得る。

(2) α は代数的数より、

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0 \quad (a_i \in \mathbb{Q})$$

が成り立つ。各係数は $a_i = \dfrac{d_i}{c_i}$ ($c_i, d_i \in \mathbb{Z}$、c_i, d_i は互いに素) と書ける。ここで $m = \prod_{i=0}^{n-1} c_i$ とおき、両辺に m^n をかけると、

$$(m\alpha)^n + b_{n-1}(m\alpha)^{n-1} + \cdots + b_0 = 0 \quad (b_i \in \mathbb{Z})$$

となる。よって、$m\alpha$ は代数的整数である。 □

命題 2.21. $\alpha \in \mathbb{C}$ に対して、次は同値である。

(1) α は代数的整数

(2) α は代数的数で、α の $\mathbb{Q}$ 上の最小多項式は $\mathbb{Z}[x]$ に属する。

Proof. α を代数的整数とすると、モニックな多項式 $\varphi \in \mathbb{Z}[x]$ で、$\varphi(\alpha) = 0$ となるものが存在する。α の最小多項式を f とする。$^{\exists}\psi, r \in \mathbb{Q}[x]$ s.t.

$$\varphi = f\psi + r、\ \deg(r) < \deg(f)$$

より、$0 = \varphi(\alpha) = f(\alpha)\psi(\alpha) + r(\alpha) = r(\alpha)$ を得るが、f の次数の最小性から $r = 0$ である。よって、$\varphi = f\psi$ である。**命題 2.2.** より、原始多項式 $f_1,\ \psi_1 \in \mathbb{Z}[x]$ が存在して、

$$f = \frac{a}{b} f_1,\ \psi = \frac{c}{d}\psi_1 \quad (a, b, c, d \in \mathbb{Z}、\gcd(a, b) = 1、\gcd(c, d) = 1)$$

と書ける。これより、

$$bd\varphi = acf_1\psi_1$$

である。**補題 2.3.** より $f_1\psi_1$ は原始多項式であるから、係数比較によって $\varphi = \pm f_1\psi_1$ を得る。φ はモニックだから f_1 の最高次係数は ± 1 であり、f もモニックだから

$$f = \pm f_1 \in \mathbb{Z}[x]$$

となる。逆は定義から明らか。 □

定理 2.22. A, B を環とし、$A \subset B$ とする。有限個の B の元 $b_1, \ldots, b_n$ が全て A 上整であるための必要十分条件は、環 $A[b_1, \ldots, b_n]$ が有限生成 A 加群となることである。

Proof. $(\Rightarrow)$ b_1は A 上整であるから、

$$b_1^m + a_{m-1}b_1^{m-1} + \cdots + a_1b_1 + a_0 = 0 \ \ (a_i \in A)$$

が成り立つ。よって、

$$b_1^m = -(a_0 + a_1b_1 + \cdots + a_{m-1}b_1^{m-1})$$

であるから、

$$A[b_1] = A + Ab_1 + \cdots + Ab_1^{m-1}$$

より、$A[b_1]$ は A 上有限生成である。

$A \subset A[b_1]$ より、b_2は $A[b_1]$ 上整である。よって、$A[b_1, b_2]$ は $A[b_1]$ 上有限生成であるから、A 上有限生成である。帰納的に繰り返せば、$A[b_1, \ldots, b_n]$ は A 上有限生成である。

($\Leftarrow$) 逆に、$A[b_1, \ldots, b_n]$ は A 上有限生成であるとし、その生成系を $w_1, \ldots, w_r$ とする。$^\forall b \in A[b_1, \ldots, b_n]$ に対し、

$$b \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rr} \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} \quad (a_{ij} \in A)$$

と表すことができる。よって、

$$\begin{pmatrix} b - a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & b - a_{rr} \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} = 0$$

であるから、

$$\begin{vmatrix} b - a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & b - a_{rr} \end{vmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} = 0$$

が従う。$(w_1, \ldots, w_r) \neq 0$ より、

$$\begin{vmatrix} b - a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & b - a_{rr} \end{vmatrix} = 0$$

を得る。左辺の行列式を展開すると、A 係数モニック多項式に b を代入した形を得る。したがって、b は A 上整である。 □

命題 2.23. A, B, C を環とし、$A \subset B \subset C$ とする。C が B 上整であって、かつ B が A 上整であるならば、C は A 上整である。

Proof. $C \ni {}^\forall c$ とすると、c は B 上整であるから、

$$c^m + b_{m-1}c^{m-1} + \cdots + b_1 c + b_0 = 0 \ \ (b_i \in B)$$

が成り立つ。よって、$(A[b_0, \ldots, b_{m-1}])[c]$ は $A[b_0, \ldots, b_{m-1}]$ 上有限生成である。B が A 上整とすると、**定理 2.22.** により $A[b_0, \ldots, b_{m-1}]$ は A 上有限生成であるから、$(A[b_0, \ldots, b_{m-1}])[c]$ は A 上有限生成である。ゆえに、c は A 上整である。 □

定義 2.24. A, B を環とし、$A \subset B$ とする。

$$\{b \in B \mid b \text{は} A \text{上整}\}$$

は **定理 2.22.** より環をなす。これを B における A の**整閉包** という。

A の整閉包が A と一致するとき、A は B において**整閉** であるという。特に、A が整域で B が A の商体であるときは、単に A は**整閉** であるという。

定義 2.25. K を代数体とし、$\mathcal{O}_K = \{\alpha \in K \mid \alpha : \text{代数的整数}\}$ とおく。**定義 2.24.** の A として $\mathbb{Z}$、B として K をとれば、K における $\mathbb{Z}$ の整閉包 $\mathcal{O}_K$ は環となる (K の部分環であるから整域である)。この環を、K の**整数環** という。定義より、$\mathbb{Z} \subset \mathcal{O}_K \subset K$ である。

定理 2.26. K を代数体、$\mathcal{O}_K$ を K の整数環とする。このとき、
(1) $\mathcal{O}_K$ の商体は K である。
(2) $\mathcal{O}_K$ は整閉である。

Proof. (1) $\mathcal{O}_K$ の商体 $Q(\mathcal{O}_K)$ は

$$Q(\mathcal{O}_K) = \left\{ \frac{b}{a} \;\middle|\; a\ (\neq 0),\ b \in \mathcal{O}_K \right\}$$

である。これより、

$$\mathbb{Q}\mathcal{O}_K \subset Q(\mathcal{O}_K) \subset K$$

は明らか。一方、$^{\forall}\alpha \in K$ に対し、**命題 2.20.**(2) より

$$^{\exists}m\ (\neq 0) \in \mathbb{Z} \ \text{ s.t. } \ m\alpha \in \mathcal{O}_K$$

である。よって、

$$\alpha \in \frac{1}{m}\mathcal{O}_K \subset \mathbb{Q}\mathcal{O}_K$$

を得る。したがって、

$$Q(\mathcal{O}_K) = K$$

である。

(2) I を K における $\mathcal{O}_K$ の整閉包とすると、

$$\mathbb{Z} \subset \mathcal{O}_K \subset I$$

である。**命題 2.23.** より、

$$\mathcal{O}_K = I$$

が従う。 □

命題 2.27. K を n 次代数体、$\mathcal{O}_K$ を K の整数環とする。このとき、$^\forall\alpha \in \mathcal{O}_K$ に対し、

$$T_K(\alpha),\ N_K(\alpha) \in \mathbb{Z}$$

である。

Proof. **定義 2.13.** より、

$$T_K(\alpha),\ N_K(\alpha) \in \mathbb{Q}$$

である。また、$^\forall\alpha \in \mathcal{O}_K$ に対し、**命題 2.21.** より、α の最小多項式 f は $f \in \mathbb{Z}[x]$ である。K から $\mathbb{C}$ の中への相異なる同型対応の全体を $\sigma_1, \ldots, \sigma_n$ とすると、

$$f(\sigma_i(\alpha)) = 0 \quad (1 \leq i \leq n)$$

より、$\sigma_i(\alpha) \in \mathcal{O}_K$ である。**定理 2.14.** より

$$T_K(\alpha),\ N_K(\alpha) \in \mathcal{O}_K$$

を得る。**命題 2.20.**(1) より、

$$T_K(\alpha),\ N_K(\alpha) \in \mathbb{Z}$$

である。 □

定理 2.28. K を n 次代数体、$\mathcal{O}_K$ を K の整数環とする。このとき、$\mathcal{O}_K$ は階数 n の自由 $\mathbb{Z}$ 加群である。

Proof. K の $\mathbb{Q}$ 上の基底を $\{\alpha_1, \ldots, \alpha_n\}$ とする。このとき **命題 2.20.**(2) より、各 i に対して、

$$^\exists m_i\ (\neq 0) \in \mathbb{Z}\ \text{ s.t. }\ m_i\alpha_i \in \mathcal{O}_K$$

が成り立つ。ここで、$m = m_1 \cdots m_n$ とおくと、$m\alpha_i \in \mathcal{O}_K$ である。各 i に対して、

$$l_i = m\alpha_i$$

とおくと、$\{l_1, \ldots, l_n\}$ は K の $\mathbb{Q}$ 上の基底である。**命題 2.18.** より、

$$^\exists\{l'_1, \ldots, l'_n\} : K \text{ の } \mathbb{Q} \text{ 上の基底 s.t. } T_K(l_i l'_j) = \delta_{ij}$$

が成り立つ。さて、$^{\forall}z \in \mathcal{O}_K$ を考えよう。$\mathcal{O}_K \subset K$ より

$$z = \sum_{i=1}^{n} a_i l'_i \quad (a_i \in \mathbb{Q})$$

と書ける。$l_j = m\alpha_j \in \mathcal{O}_K$ より、

$$zl_j = \left(\sum_{i=1}^{n} a_i l'_i \right) l_j \in \mathcal{O}_K$$

である。**命題 2.27.** より、

$$\begin{aligned} \mathbb{Z} \ni T_K(zl_j) &= T_K \left(\sum_{i=1}^{n} a_i l'_i l_j \right) \\ &= \sum_{i=1}^{n} a_i T_K(l'_i l_j) \\ &= \sum_{i=1}^{n} a_i \delta_{ij} = a_j \end{aligned}$$

よって、

$$z \in \mathbb{Z}l'_1 + \cdots + \mathbb{Z}l'_n$$

である。したがって、

$$\mathcal{O}_K \subset \mathbb{Z}l'_1 + \cdots + \mathbb{Z}l'_n$$

が成り立つ。**命題 2.4.** より、

$$^{\exists}\{w_1, \ldots, w_m\} \subset \mathcal{O}_K \ \text{ s.t. } \ m \leq n、\mathcal{O}_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_m$$

であり、**定理 2.26.**(1) の証明中に示した、$K = \mathbb{Q}\mathcal{O}_K$ より

$$K = \mathbb{Q}\mathcal{O}_K = \mathbb{Q}(\mathbb{Z}w_1 + \cdots + \mathbb{Z}w_m) = \mathbb{Q}w_1 + \cdots + \mathbb{Q}w_m$$

を得る。したがって、$m = n$、$\{w_1, \ldots, w_n\}$ は K の $\mathbb{Q}$ 上の基底であって、

$$\mathcal{O}_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$$

より、$\mathcal{O}_K$は階数 n の自由 $\mathbb{Z}$ 加群である。　□

命題 2.29. K を n 次代数体、$\mathcal{O}_K$を K の整数環とし、A を $\mathcal{O}_K$の (0 でない) イデアルとする。このとき、
(1) $\alpha \in A \Rightarrow N_K(\alpha) \in A \cap \mathbb{Z}$
(2) $A \cap \mathbb{Z} \neq \{0\}$
(3) $K = \mathbb{Q}A$

Proof. (1) K から $\mathbb{C}$ の中への相異なる同型対応の全体を $\sigma_1(= id), \ldots, \sigma_n$ とすると、**定理 2.14.**、**命題 2.27** より、$\alpha \in A$ に対して、

$$N_K(\alpha) = \alpha\sigma_2(\alpha)\cdots\sigma_n(\alpha) \in \mathbb{Z}$$

よって、

$$\alpha = 0 \Longleftrightarrow N_K(\alpha) = 0$$

である。$\alpha \neq 0$ のとき、

$$\alpha^{-1}N_K(\alpha) = \sigma_2(\alpha)\cdots\sigma_n(\alpha)$$

であることと、

$$\alpha^{-1}N_K(\alpha) \in \alpha^{-1}\mathbb{Z} \subset \alpha^{-1}\mathcal{O}_K \subset K$$

より、$\alpha^{-1}N_K(\alpha) \in \mathcal{O}_K$ を得る。したがって、

$$N_K(\alpha) \in \alpha\mathcal{O}_K \cap \mathbb{Z} \subset A \cap \mathbb{Z}$$

を得る。
(2) (1) より、$0 \neq \alpha \in A \Longrightarrow 0 \neq N_K(\alpha) \in A \cap \mathbb{Z}$ である。
(3) $^{\forall}\beta \in K$ に対し、**命題 2.20.**(2) より、

$$^{\exists}m\ (\neq 0) \in \mathbb{Z}\ \text{ s.t. }\ m\beta \in \mathcal{O}_K$$

である。$(0 \neq)a \in A \cap \mathbb{Z} \subset A$ に対し、

$$a(m\beta) \in A\mathcal{O}_K = A$$

であるから、

$$\beta \in \frac{1}{am}A \subset \mathbb{Q}A$$

より分かる。 □

定義 2.30. K を n 次代数体、$\mathcal{O}_K$を K の整数環とし、A を $\mathcal{O}_K$の (0 でない) イデアルとする。剰余環 $\mathcal{O}_K/A$ の元の個数を A の**ノルム**といい、$N(A)$ と書く。

定理 2.31. K を n 次代数体、$\mathcal{O}_K$ を K の整数環とし、A を $\mathcal{O}_K$ の (0 でない) イデアルとする。このとき、
(1) A は階数 n の自由 $\mathbb{Z}$ 加群である。
(2) $N(A)$ は有限である。

Proof. (1) $\mathcal{O}_K$ は階数 n の自由 $\mathbb{Z}$ 加群であるから、

$$\mathcal{O}_K = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$$

と書ける。**命題 2.4.** より、

$$^{\exists}\{\alpha_1, \ldots, \alpha_m\} \subset A \ \text{ s.t. } \ m \leq n, A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} p_{11} & \cdots & \cdots & \cdots & p_{1n} \\ & \ddots & & & \vdots \\ 0 & & p_{mm} & \cdots & p_{mn} \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

(ただし、$p_{ij} \in \mathbb{Z}$、$p_{ii} \geq 0$)
命題 2.29.(3) より、

$$K = \mathbb{Q}A = \mathbb{Q}\alpha_1 + \cdots + \mathbb{Q}\alpha_m$$

だから、$m = n$、$\{\alpha_1, \ldots, \alpha_n\}$ は K の $\mathbb{Q}$ 上の基底であって、

$$A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

を得る。
(2) $\{w_1, \ldots, w_n\}$ も K の $\mathbb{Q}$ 上の基底であるから、

$$\begin{pmatrix} p_{11} & \cdots & p_{1n} \\ & \ddots & \vdots \\ 0 & & p_{nn} \end{pmatrix}$$

は正則行列であるから、$p_{11} \cdots p_{nn} > 0$ である。よって、$p_{ii} > 0$ を得る。ここで、

$$E = \left\{ \sum_{i=1}^{n} x_i w_i \;\middle|\; 0 \leq x_i < p_{ii},\ x_i \in \mathbb{Z} \right\}$$

とおく。$\sharp E = p_{11} \cdots p_{nn}$ である。これによって、E が $\mathcal{O}_K/A$ の完全代表系であることを示せば、題意を得る。

$^{\forall}\xi \in \mathcal{O}_K$ は、

$$\xi = \sum_{i=1}^{n} c_i w_i \quad (c_i \in \mathbb{Z})$$

と書ける。ここで、

$$\mathcal{O}_K^{(i)} = \mathbb{Z}w_{i+1} + \cdots + \mathbb{Z}w_n \quad (i = 1, \ldots, n-1)$$

とおく。まず、ξの係数 c_i を、

$$c_1 = m_1 p_{11} + x_1 \quad (0 \leq x_1 < p_{11},\ m_1 \in \mathbb{Z})$$

と書く。このとき、

$$\xi - x_1 w_1 - m_1 \alpha_1 = (c_2 - m_1 p_{12}) w_2 + \cdots + (c_n - m_1 p_{1n}) w_n \in \mathcal{O}_K^{(1)}$$

であり、この元を ξ_1 とおく。以下同様に、

$$\begin{aligned}
\xi_1 &= \xi - x_1 w_1 - m_1 \alpha_1 \in \mathcal{O}_K^{(1)} \\
\xi_2 &= \xi_1 - x_2 w_2 - m_2 \alpha_2 \in \mathcal{O}_K^{(2)} \\
&\vdots \\
\xi_{n-1} &= \xi_{n-2} - x_{n-1} w_{n-1} - m_{n-1} \alpha_{n-1} \in \mathcal{O}_K^{(n-1)} \\
\xi_n &= \xi_{n-1} - x_n w_n - m_n \alpha_n = 0
\end{aligned}$$

を得る。これらを全て足して、

$$\xi_1 + \cdots + \xi_n = \xi + \xi_1 + \cdots + \xi_{n-1} - \left(\sum_{i=1}^{n} x_i w_i + \sum_{i=1}^{n} m_i \alpha_i \right)$$

より、

$$\xi = \sum_{i=1}^{n} x_i w_i + \sum_{i=1}^{n} m_i \alpha_i \equiv \sum_{i=1}^{n} x_i w_i \pmod{A}$$

が成り立つ。これより、$\mathcal{O}_K$ の任意の元の A でのクラスは E の元の形である。次に、

$$\sum_{i=1}^{n} x_i w_i,\ \sum_{i=1}^{n} y_i w_i \in E$$

に対し、

$$\sum_{i=1}^{n} x_i w_i \equiv \sum_{i=1}^{n} y_i w_i \pmod{A}$$

とする。ここで、$a_i = x_i - y_i$ とおくと、$0 \leq x_i,\ y_i < p_{ii}$ より、

$$\sum_{i=1}^{n} a_i w_i \in A,\ |a_i| < p_{ii}$$

である。よって、

$$\sum_{i=1}^{n} a_i w_i = \sum_{i=1}^{n} l_i \alpha_i\ (l_i \in \mathbb{Z})$$

と書ける。これに、

$$\alpha_i = \sum_{i \leq j} p_{ij} w_j$$

を代入し、w_1 の係数を比較すれば、

$$a_1 = l_1 p_{11}$$

を得る。ここで、$|a_1| < p_{11},\ p_{11} > 0$ より、$a_1 = 0,\ l_1 = 0$ である。よって、

$$\sum_{i=2}^{n} a_i w_i = \sum_{i=2}^{n} l_i \alpha_i$$

となる。以下同様に繰り返して、$a_i = 0$ から $x_i = y_i\ (i = 1, \ldots n)$ を得る。

□

2.4　整数環のイデアルの分解

定義 2.32. R を単位元をもつ可換整域とする。R が**デデキント整域**であるとは、次をみたすものである。

$$\begin{cases} (1)\ R \text{ の各素イデアル } (\neq 0) \text{ は極大イデアルである。} \\ (2)\ R \text{ は整閉である。} \\ (3)\ R \text{ はネーター環である。} \end{cases}$$

定理 2.33. K を代数体とする。このとき、K の整数環 $\mathcal{O}_K$ はデデキント整域である。

Proof. (1) $\boldsymbol{p}$を$\mathcal{O}_K$の (0でない) 任意の素イデアルとする。**定理 2.31.**(2) より、$\mathcal{O}_K/\boldsymbol{p}$は有限整域であるから、体である。よって、$\boldsymbol{p}$は極大イデアルである。

(2) は**定理 2.26.**(2) で示した。

(3) $\mathcal{O}_K$ のイデアルの任意の増大列

$$A_1 \subset \cdots \subset A_m \subset \cdots$$

に対し、

$$A = \bigcup_i A_i$$

は$\mathcal{O}_K$ のイデアルであるから、**定理 2.31.**(1) より、

$$A = \mathbb{Z}d_1 + \cdots + \mathbb{Z}d_n \ \text{ for some } \ d_1, \ldots, d_n \in A$$

と表せる。このとき、

$$^{\exists}l \ \text{ s.t. } \ \{d_1, \ldots, d_n\} \subset A_l$$

より、

$$A = A_l = A_{l+1} = \cdots$$

を得る。 □

補題 2.34. K を代数体、$\mathcal{O}_K$を K の整数環とし、A を $\mathcal{O}_K$ のイデアルで、$A \neq \{0\}, \mathcal{O}_K$である (**真のイデアル**であるという) とする。このとき、A は$\mathcal{O}_K$のある (0でない) 素イデアルの積を含む。

Proof.

$P = \{A \mid A$は$\mathcal{O}_K$の真のイデアルで、素イデアルのどんな積も含まない$\}$

とおく。$P \neq \phi$ と仮定すると、$\mathcal{O}_K$ はネーター環であるから、P は極大元 を含む。それを A_0 とおくと、これは素イデアルではないから、

$$^{\exists}x_1, x_2 \in \mathcal{O}_K \ \text{ s.t. } \ x_1x_2 \in A_0, \ \ x_1, x_2 \notin A_0$$

である。ここで、

$$A_1 = A_0 + x_1\mathcal{O}_K, \ A_2 = A_0 + x_2\mathcal{O}_K$$

とおく。このとき、

$$A_0 \subsetneqq A_1, \ A_0 \subsetneqq A_2$$

である。A_0 より真に大きいから、A_1, A_2 は $\mathcal{O}_K$ の素イデアルの積を含む。よって、A_1A_2 も素イデアルの積を含む。

$$\begin{aligned} A_1A_2 &= (A_0 + x_1\mathcal{O}_K)(A_0 + x_2\mathcal{O}_K) \\ &= A_0^2 + x_1\mathcal{O}_KA_0 + x_2A_0\mathcal{O}_K + x_1x_2\mathcal{O}_K \\ &\subset A_0 \end{aligned}$$

より、A_0 も素イデアルの積を含むことになり、矛盾である。したがって、$P = \phi$ である。 □

定義 2.35. K を代数体、$\mathcal{O}_K$ を K の整数環とする。このとき、A が K の**分数イデアル**であるとは、A が K の有限生成 $\mathcal{O}_K$ 部分加群であることである。一方、$\mathcal{O}_K$ のイデアルを K の**整イデアル**という。

また、K の分数イデアル A が (K で) **可逆**であるとは、$AB = \mathcal{O}_K$ となる K の分数イデアル B が存在することである。

命題 2.36. K を代数体、$\mathcal{O}_K$ を K の整数環とし、$\boldsymbol{p}$ を $\mathcal{O}_K$ の (0 でない) 素イデアル、$B = \{x \in K \mid x\boldsymbol{p} \subset \mathcal{O}_K\}$ とする。このとき、B は分数イデアルで、$\boldsymbol{p}B = \mathcal{O}_K$ が成り立つ。($\boldsymbol{p}$ は可逆である。)

さらに、分数イデアル C に対して、$\boldsymbol{p}C = \mathcal{O}_K$ が成り立つとき、$B = C$ である。これにより、B を $\boldsymbol{p}^{-1}$ と書く。

Proof. $x, y \in B$、$a \in \mathcal{O}_K$ に対して、

$$(x + y)\boldsymbol{p} \subset x\boldsymbol{p} + y\boldsymbol{p} \subset \mathcal{O}_K$$

$$(ax)\boldsymbol{p} \subset a(x\boldsymbol{p}) \subset a\mathcal{O}_K \subset \mathcal{O}_K$$

より、$x+y, ax \in B$ であるから、B は K の $\mathcal{O}_K$ 部分加群である。さらに、$\mathcal{O}_K\boldsymbol{p} \subset \mathcal{O}_K$ より、$\mathcal{O}_K \subset B$ である。**命題 2.29.**(2) より、$0 \neq n \in \mathbb{Z} \cap \boldsymbol{p}$ に対し、

$$nB \subset \boldsymbol{p}B \subset \mathcal{O}_K$$

が成り立つ。よって、B は K の分数イデアルとなる。一方、$\mathcal{O}_K$ はデデキント環であるから、$\boldsymbol{p}$ は極大イデアルである。よって、

$$\boldsymbol{p} \subset \boldsymbol{p}B \subset \mathcal{O}_K$$

から、

$$\boldsymbol{p}B = \mathcal{O}_K \text{ または } \boldsymbol{p} = \boldsymbol{p}B$$

である。ここから、$\boldsymbol{p} = \boldsymbol{p}B$ を仮定する。このとき、$^{\forall}x \in B$ に対し、

$$x\boldsymbol{p} \subset \boldsymbol{p}$$

であって、$\boldsymbol{p}$ は有限生成 $\mathbb{Z}$ 加群であるから、**定理 2.22.** より B の元は全て代数的整数。ゆえに、$B = \mathcal{O}_K$ を得る。$0 \neq x \in \boldsymbol{p}$ とすれば、**補題 2.34** より、

$$\boldsymbol{p}_1 \cdots \boldsymbol{p}_r \subset x\mathcal{O}_K \subset \boldsymbol{p}$$

なる素イデアル $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_r$ が存在する。したがって、極大性から $^{\exists}k$ s.t. $\boldsymbol{p}_k = \boldsymbol{p}$ である。ここで、$k = r$ としてよい。よって、

$$x^{-1}\boldsymbol{p}_1 \cdots \boldsymbol{p}_{r-1}\boldsymbol{p}B \subset \mathcal{O}_K = B$$

ゆえに、

$$\boldsymbol{p}_1 \cdots \boldsymbol{p}_{r-1} \subset x\mathcal{O}_K$$

を得る。この操作を繰り返して、

$$\boldsymbol{p}_1 \subset x\mathcal{O}_K \subset \boldsymbol{p}$$

であるが、$\boldsymbol{p}_1$ の極大性から、$x^{-1}\boldsymbol{p} = \mathcal{O}_K$ が成り立つ。$x^{-1} \in B = \mathcal{O}_K$であるから、$\boldsymbol{p} \in x^{-1}x = 1$ を得る。つまり $\boldsymbol{p} = \mathcal{O}_K$ となって矛盾が生じる。よって、

$$\boldsymbol{p}B = \mathcal{O}_K$$

が成り立つ。

あとは、

$$\boldsymbol{p}B = \mathcal{O}_K = \boldsymbol{p}C$$

の両辺に左から B をかければよい。 □

定理 2.37. K を代数体とする。このとき、K の整数環 $\mathcal{O}_K$の真のイデアルは、$\mathcal{O}_K$ の素イデアルの積として順番を度外視して一意的に書ける。

Proof. A を $\mathcal{O}_K$ の真のイデアルとおく。**補題 2.34.** より、

$$\boldsymbol{p}_1 \cdots \boldsymbol{p}_n \subset A$$

なる素イデアル $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ が存在する。

ここから、A の素イデアルの積の分解が存在することを帰納法で示す。$n = 1$ のときは、$\boldsymbol{p}_1$ の極大性より、$A = \boldsymbol{p}_1$ である。次に、$n - 1$ のときに成り立つと仮定する。$\mathcal{O}_K$ はネーター環であるから、A は $\mathcal{O}_K$ の一つ

の素イデアル $\boldsymbol{p}$ に含まれる。したがって、極大性から $^{\exists}k$ s.t. $\boldsymbol{p}_k = \boldsymbol{p}$ である。ここで、$k = 1$ としてよい。**命題 2.36.** によって、

$$\mathcal{O}_K = \boldsymbol{p}_1{}^{-1}\boldsymbol{p} \supset \boldsymbol{p}_1{}^{-1}A \supset \boldsymbol{p}_2 \cdots \boldsymbol{p}_n$$

を得る。仮定により $\boldsymbol{p}_1{}^{-1}A$ は素イデアルの積への分解が存在する。したがって、

$$A = \boldsymbol{p}_1(\boldsymbol{p}_1{}^{-1}A)$$

は素イデアルの積への分解が存在する。

次に、分解の一意性を示す。

$$A = \boldsymbol{p}_1 \cdots \boldsymbol{p}_r = \boldsymbol{q}_1 \cdots \boldsymbol{q}_s$$

とする。このとき、

$$\boldsymbol{q}_1 \cdots \boldsymbol{q}_s \subset \boldsymbol{q}_1$$

であり、$\boldsymbol{q}_1$ は素イデアルであるから、$\boldsymbol{p}_1, \ldots, \boldsymbol{p}_r$ のうち一つが $\boldsymbol{q}_1$ に含まれる。それを $\boldsymbol{p}_1$ とする。素イデアルの極大性から、

$$\boldsymbol{p}_1 = \boldsymbol{q}_1$$

よって、

$$\boldsymbol{p}_2 \cdots \boldsymbol{p}_r = \boldsymbol{q}_2 \cdots \boldsymbol{q}_s$$

が成り立つ。同様に繰り返せば、$r = s$ で、

$$\{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_r\} = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_s\}$$

を得る。 □

代数体 K の整数環 $\mathcal{O}_K$ の分数イデアルの全体のなす群を、単項分数イデアルの全体のなす部分群で割った剰余群を、K の**イデアル類群** といい、$\mathrm{Cl}(K)$ と書く。代数的整数論の一つの目標は、「イデアル類群は有限群である」という定理である。この定理は、次章で説明する類体論の成立に大きく貢献している。

第3章　代数体における類体論

類体論とは、代数体 K のアーベル拡大 L の様子がその体に関係する群に映し出される、というものである。この関係から示されるのは、K の整数環 $\mathcal{O}_K$ の素イデアル $\boldsymbol{p}$ が L においてどのように分解するかが“ mod によって定まる ”という事実である。

定義 3.1. 代数体 K に対して、**定理 2.37.** より次のことが成り立つ。
L を K の有限次拡大、$\boldsymbol{p}$ を $\mathcal{O}_K$の 0 でない素イデアルとすると、$\mathcal{O}_L$のイデアル $\boldsymbol{p}\mathcal{O}_L$は $\mathcal{O}_L$の相異なる素イデアル $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_g$ を用いて、

$$\boldsymbol{p}\mathcal{O}_L = \boldsymbol{q}_1^{e_1} \cdots \boldsymbol{q}_g^{e_g} \quad (e_i \geq 1)$$

と分解される。
この分解の様子について、$e_1 = \cdots = e_g = 1,\ g = [L : K]$ が成り立つとき、$\boldsymbol{p}$ は L で**完全分解** するといい、$^{\exists} i \quad e_i \geq 2$ であるとき、$\boldsymbol{p}$ が L で**分岐** するという。

次の定理は、体の完備化の議論により示される。

定理 3.2. L が K 上の既約多項式 $u(x)$ を用いて $K[x]/(u(x))$ と書けているとき、

$$\boldsymbol{p} \text{ が } L \text{ で完全分解} \iff u(x) \text{ が } \mathcal{O}_K/\boldsymbol{p} \text{で 1 次式の積に分解する}$$

$$\boldsymbol{p} \text{ が } L \text{ で分岐} \iff u(x) \text{ が } \mathcal{O}_K/\boldsymbol{p} \text{で重根をもつ}$$

が成り立つ。

定義 3.3. 体 K の元 $\alpha\ (\neq 0)$ が**総正** であるとは、K から $\mathbb{R}$ への全ての体準同型について、 α の $\mathbb{R}$ での像が正であることである。

次のことを引用しよう。これは、代数体における類体論からの大事な帰結の一つである。

定理 3.4. 代数体 K に対して以下のことが成り立つ。

(1) $\mathcal{O}_K$の 0 でないイデアル $\boldsymbol{a}$ に対して、K の有限次アーベル拡大 $K(\boldsymbol{a})$ で次の性質を持つものがただ一つ存在する。

$^{\forall}\boldsymbol{p}$: $\boldsymbol{a}$ を割らない $\mathcal{O}_K$の 0 でない素イデアル に対して、

$\boldsymbol{p}$ が $K(\boldsymbol{a})$ で完全分解 $\iff {}^{\exists}\alpha \in \mathcal{O}_K$ s.t. α : 総正、$\alpha \equiv 1 \bmod \boldsymbol{a}$、$\boldsymbol{p} = (\alpha)$

(2) $L : K$ の有限次アーベル拡大とすると、$L \subset K(\boldsymbol{a})$ となる $\mathcal{O}_K$の 0 でないイデアル $\boldsymbol{a}$ のうち最大のものが存在する。さらにその $\boldsymbol{a}$ について、次が成立する。

$^{\forall}\boldsymbol{p}$: $\mathcal{O}_K$の 0 でない素イデアルに対し、

$$\boldsymbol{p} \text{ が } L \text{ で分岐する} \iff \boldsymbol{p} \text{ は } \boldsymbol{a} \text{ を割り切る}$$

(3) (2) において 、$\boldsymbol{a}$ は L において分岐する $\mathcal{O}_K$の 0 でない素イデアルのいくつかの積である。

ここから、類体論におけるイデアル類群 (の拡張) とガロア群の関係を述べた一般的な定理を用いて**定理 3.4.**(1) の証明を述べよう。そのためにいくつか準備をする。

定義 3.5. 代数体 K に対して次のことを定義する。

(1) K の**イデール群** $\mathbb{A}_K^\times$ を

$$\mathbb{A}_K^\times \overset{\text{def}}{:=} \left\{ (a_v)_v \in \prod_{v:K \text{ の素点}} K_v^\times \;\middle|\; \text{ほぼ全ての有限素点について } a_v \in \mathcal{O}_v \right\}$$

で定義し、さらに K の**イデール類群** C_K を

$$C_K \overset{\text{def}}{:=} \mathbb{A}_K^\times / K^\times$$

と定義する。

(2) K の各素点υに対し、

$$U_\upsilon(\boldsymbol{a}) \overset{\text{def}}{:=} \begin{cases} \mathrm{Ker}(\mathcal{O}_\upsilon^\times \to (\mathcal{O}_\upsilon/\boldsymbol{a}\mathcal{O}_\upsilon)^\times) & \text{if } \upsilon : \text{有限素点} \\ \mathbb{C}^\times & \text{if } \upsilon : \text{複素素点} \\ \mathbb{R}_{>0}^\times & \text{if } \upsilon : \text{実素点} \end{cases}$$

と定める。次に

$$U(\boldsymbol{a}) \overset{\text{def}}{:=} \prod_\upsilon U_\upsilon(\boldsymbol{a})$$

とおき、

$$\overline{U}(\boldsymbol{a}) : U(\boldsymbol{a}) \text{ の } C_K \text{での像}$$

と定義する。

(3) K のイデアル類群の一般化として

$$\mathrm{Cl}(K, \boldsymbol{a}) \overset{\text{def}}{:=} \mathrm{Coker}(K^\times \to \mathbb{A}_K^\times / U(\boldsymbol{a})) = C_K/\overline{U}(\boldsymbol{a})$$

を定義する。

$\boldsymbol{a} = \mathcal{O}_K$のときは、$\mathrm{Cl}(K, \boldsymbol{a})$ は K のイデアル類群 $\mathrm{Cl}(K)$ と一致する。

(4) 一般に、L を K のガロア拡大、$\boldsymbol{p}$ を L において分岐しない $\mathcal{O}_K$の 0 でない素イデアル、 $\boldsymbol{q}$ を $\boldsymbol{p}$ の上にある $\mathcal{O}_L$ の素イデアルに対し、
$\mathrm{Gal}((\mathcal{O}_L/\boldsymbol{q})/(\mathcal{O}_K/\boldsymbol{p}))$ は自己同型

$$\mathcal{O}_L/\boldsymbol{q} \longrightarrow \mathcal{O}_L/\boldsymbol{q}\ ;\ x \longmapsto x^{\sharp(\mathcal{O}_K/\boldsymbol{p})}$$

を生成元とする群であり、この生成元の $\mathrm{Gal}(L/K)$ における像 $\mathrm{Frob}_{\boldsymbol{p},\boldsymbol{q}}$ が生じる。

ここで、L が K のアーベル拡大なら $\mathrm{Frob}_{\boldsymbol{p},\boldsymbol{q}}$の $\mathrm{Gal}(L/K)$ における共役類 $\mathrm{Frob}_{\boldsymbol{p},L}$ は一個の元からなることにより、$\mathrm{Frob}_{\boldsymbol{p},L}$は $\mathrm{Gal}(L/K)$ の元とみなされ、これを $\boldsymbol{p}$ の L に関する **フロベニウス置換** という。

次の定理は、類体論から示される。

定理 3.6. 代数体 K と、$\mathcal{O}_K$のイデアル $\boldsymbol{a}$ に対して、$\mathrm{Cl}(K, \boldsymbol{a})$ から $\mathrm{Gal}(K(\boldsymbol{a})/K)$ への群準同型が、L で分岐しない $\mathcal{O}_K$の素イデアル $\boldsymbol{p}$ の $\mathrm{Cl}(K, \boldsymbol{a})$ でのクラス $[\boldsymbol{p}]$ に $\mathrm{Frob}_{\boldsymbol{p},K(\boldsymbol{a})} \in \mathrm{Gal}(K(\boldsymbol{a})/K)$ を対応させることにより得られる。この準同型は実は同型を与える。

上に出てきた $\mathrm{Frob}_{\boldsymbol{p},L}$ と、$\mathrm{Cl}(K,\boldsymbol{a})$ を調べることにより、次の定理は比較的簡単に導かれる。

定理 3.7. (1) $L:K$ のガロア拡大、$\boldsymbol{p}:L$ において分岐しない $\mathcal{O}_K$ の 0 でない素イデアル に対し、

$$\boldsymbol{p} \text{ が } L \text{ で完全分解} \iff \mathrm{Frob}_{\boldsymbol{p},L} \text{が } \mathrm{Gal}(L/K) \text{ の単位元}$$

(2) $\mathrm{I}(\boldsymbol{a}):\boldsymbol{a}$と互いに素な K の分数イデアル群、$\mathrm{P}(\boldsymbol{a})=\{(\alpha)\mid \alpha\in K^\times$ は総正、$\alpha\equiv 1 \bmod \boldsymbol{a}\}$ とすると

$$\mathrm{Cl}(K,\boldsymbol{a})=\mathrm{I}(\boldsymbol{a})/\mathrm{P}(\boldsymbol{a})$$

この表示より、

$[\boldsymbol{p}]$ が $\mathrm{Cl}(K,\boldsymbol{a})$ の単位元 $\iff {}^{\exists}\alpha\in\mathcal{O}_K$ s.t. α : 総正、$\alpha\equiv 1 \bmod \boldsymbol{a}$、$\boldsymbol{p}=(\alpha)$

定理 3.6. 定理 3.7. を用いるとすぐに、**定理 3.4.**(1) の

$\boldsymbol{p}$ が $K(\boldsymbol{a})$ で完全分解 $\iff {}^{\exists}\alpha\in\mathcal{O}_K$ s.t. α : 総正、$\alpha\equiv 1 \bmod \boldsymbol{a}$、$\boldsymbol{p}=(\alpha)$

が示される。

ここから二つの例について、代数体 K のアーベル拡大 L に対し、あるイデアルにより素イデアル分解の法則がもたらされることを見る。ここから、$N\in\mathbb{N}$ とおく。

最初の例として、$\mathbb{Q}(\zeta_3)$ における $\mathbb{Q}$ の素イデアル (p) の分解について考えよう。$\mathcal{O}_{\mathbb{Q}}=\mathbb{Z}$ である。さらに次の補題により、**定理 3.4.**(2) をみたす $\boldsymbol{a}$ が得られる。

補題 3.8. p は N を割りきらない素数とする。このとき、

$$(p) \text{ が } \mathbb{Q}(\zeta_N) \text{ において完全分解} \iff p\equiv 1 \pmod{N}$$

Proof.

$$
\begin{aligned}
(p) \text{ が } \mathbb{Q}(\zeta_N) \text{ において完全分解} &\iff x^N - 1 \text{ が } \mathbb{F}_p \text{上 } 1 \text{ 次式の積に分解} \\
&\iff \mathbb{F}_p \text{の中に } 1 \text{ の原始 } N \text{ 乗根が入る} \\
&\iff \mathbb{F}_p^{\times} \supset (N \text{ 次巡回群}) \\
&\iff N \mid p-1 \\
&\iff p \equiv 1 \pmod{N}
\end{aligned}
$$

□

ここで、

$$\text{「}\mathcal{P} = (p)\text{、} p \equiv 1 \pmod{N}\text{」}$$

は、**定理 3.4** (1) の条件

$$\text{「}\mathcal{P} = (p)\text{、} p \equiv 1 \bmod N\mathbb{Z} \text{ なる } p \in \mathbb{Z} \text{ で総正なものが存在」}$$

と同値である。

つまり、$\mathbb{Q}(\zeta_N)$ は、**定理 3.4** (1) の性質を持つ。さらに、(1) の唯一性より、$\mathbb{Q}(\zeta_N) = K(N\mathbb{Z})$ が結論される。

特に $N = 3$ のとき、$K(3\mathbb{Z}) = \mathbb{Q}(\zeta_3)$ で、

$$(p) \text{ が } \mathbb{Q}(\zeta_3) \text{ において完全分解} \iff p \equiv 1 \pmod{3}$$

である。

一方、**定理 3.4**(2) を、$K = \mathbb{Q}$ 、$K(\boldsymbol{a}) = \mathbb{Q}(\zeta_N)$ として適用すると、次のように書き換えられる。

L をアーベル拡大とし、$L \subset \mathbb{Q}(\zeta_N)$ となる最小の N をとるとき、

$$(p) \text{ が } L \text{ で分岐する} \iff p \text{ は } N \text{ を割り切る}$$

特に $L = \mathbb{Q}(\zeta_3)$ とおくと、$N = 3$ であり、3 を割り切る p は 3 のみである。つまり、

$$(p) \text{ が } \mathbb{Q}(\zeta_3) \text{ で分岐する} \iff p = 3$$

が成り立つ。

以上の考察により、$\mathbb{Q}(\zeta_3)$ における $\mathbb{Q}$ の素イデアル (p) の分解は、mod 3 で判別される。まとめると、次のようになる。

(p) が $\mathbb{Q}(\zeta_3)$ で分岐するのは $p = 3$ のときであり、完全分解するのは $p \equiv 1 \pmod 3$ のときである。

次に、$\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ における $\mathbb{Q}(\zeta_3)$ の素イデアル $\mathcal{P}$ の分解について考えよう。$\mathcal{O}_{\mathbb{Q}(\zeta_3)} = \mathbb{Z}[\zeta_3]$ である。次の補題により、**定理 3.4** (2) をみたす $\boldsymbol{a}$ が得られる。

補題 3.9. $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ で分岐する $\mathbb{Z}[\zeta_3]$ の素イデアルは $\mathcal{P} = (1-\zeta_3)$ or (2) である。

これは、$x^3 - 2$ が $\mathbb{F}_p$ でべき根を持つか否かで分かる。

上の補題と**定理 3.4** (3) より、$\boldsymbol{a}$ は $(1-\zeta_3)$ と (2) の いくつかの積で書けることが分かる。つまり、$\boldsymbol{a} = ((1-\zeta_3)^l\ 2^m)$ である。
2 進整数環 $\mathbb{Z}_2$ 、3 進整数環 $\mathbb{Z}_3$ まで考察することにより、l、m が決定され、次のことが分かる。

命題 3.10.

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = (\mathbb{Q}(\zeta_3))(6\mathbb{Z}[\zeta_3])$$

すなわち、$\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ で完全分解する $\mathbb{Z}[\zeta_3]$ の素イデアルは、

$$\mathcal{P} = (\alpha)\ 、\alpha \equiv 1 \bmod 6\mathbb{Z}[\zeta_3] \text{ なる } \alpha \in \mathbb{Z}[\zeta_3] \text{ が存在する } \mathcal{P}$$

となる。

以上の考察により、$\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ における $\mathbb{Q}(\zeta_3)$ の素イデアル $\mathcal{P}$ の分解は、mod $6\mathbb{Z}[\zeta_3]$ で判別される。まとめると、次のようになる。

$\mathcal{P}$ が $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ で分岐するのは $\mathcal{P} = (1-\zeta_3)$ or (2) のときであり、完全分解するのは $\mathcal{P} = (\alpha)$ 、$\alpha \equiv 1 \bmod 6\mathbb{Z}[\zeta_3]$ なる $\alpha \in \mathbb{Z}[\zeta_3]$ が存在するときである。

上記の様子を具体的に表を書いてみる。

この表で、中段は、上段の各イデアルの $\mathbb{Q}(\zeta_3)$ での分解であり、下段は、中段の各イデアルが $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ で分解されるとき ○、分解しないとき× と書いている。

例えば、上段の (7) に対応する中段の欄は $(1+3\zeta_3)$、$(1+3\zeta_3^2)$ で、下段の欄は×、× である。

これは、(7) が $\mathbb{Q}(\zeta_3)$ において $(7) = (1+3\zeta_3)(1+3\zeta_3^2)$ と分解されること、およびこれらが $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ においては分解されないということを示している。

$F = \mathbb{Q}(\zeta_3)$、$E = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ とおく。

$\mathbb{Z}$ の素イデアル	(2)	(3)	(5)	(7)		(11)
F での分解	(2)	(分岐)	(5)	$(1+3\zeta_3)$	$(1+3\zeta_3^2)$	(11)
E で分解するか否か	(分岐)	(分岐)	○	×	×	○

(13)		(17)	(19)		(23)	(29)	(31)	
$(1+4\zeta_3)$	$(1+4\zeta_3^2)$	(17)	$(2-3\zeta_3)$	$(2-3\zeta_3^2)$	(23)	(29)	$(1+6\zeta_3)$	$(1+6\zeta_3^2)$
×	×	○	×	×	○	○	○	○

(37)		(41)	(43)		(47)	$\cdots$
$(3-4\zeta_3)$	$(3-4\zeta_3^2)$	(41)	$(1-6\zeta_3)$	$(1-6\zeta_3^2)$	(47)	$\cdots$
×	×	○	○	○	○	$\cdots$

上の表をみると、31 は $\mathbb{Q}(\zeta_3)$ では $(1+6\zeta_3)(1+6\zeta_3^2)$ と分解して、さらに $(1+6\zeta_3)$、$(1+6\zeta_3^2)$ は $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ で分解している。実際、

$$(1+6\zeta_3) = \prod_{i=1}^{3}(1+2\zeta_3 - \sqrt[3]{2}\zeta_3^i)$$

$$(1+6\zeta_3^2) = \prod_{i=1}^{3}(1+2\zeta_3^2 - \sqrt[3]{2}\zeta_3^i)$$

となる。よって、

$$\begin{aligned}(31) &= (1+6\zeta_3)(1+6\zeta_3^2)\\ &= \prod_{i=1}^{3}(1+2\zeta_3-\sqrt[3]{2}\zeta_3^i)(1+2\zeta_3^2-\sqrt[3]{2}\zeta_3^i)\end{aligned}$$

同様に、

$$\begin{aligned}(43) &= (1-6\zeta_3)(1-6\zeta_3^2)\\ &= \prod_{i=1}^{3}(1+2\zeta_3-\sqrt[3]{4}\zeta_3^i)(1+2\zeta_3^2-\sqrt[3]{4}\zeta_3^i)\end{aligned}$$

という具合になる。

上で考察した $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ および $\mathbb{Q}(\zeta_3,\sqrt[3]{2})/\mathbb{Q}(\zeta_3)$ はそれぞれアーベル拡大で、これらの拡大においては素イデアルが完全分解するかどうかが、あるイデアルによる剰余類で判定できた。

一方、これらの拡大をつなげた $\mathbb{Q}(\zeta_3,\sqrt[3]{2})/\mathbb{Q}$ という拡大はアーベル拡大ではない。

したがって、$\mathbb{Q}(\zeta_3,\sqrt[3]{2})/\mathbb{Q}$ に対しては直接は**定理 3.4.** は使えない。

第4章　多項式の分解の挙動を記述する剰余

本論文で重要な役割を果たす多項式を定義する。

定義 4.1. $u(x)$ を整数係数既約モニック d 次多項式、p を素数とする。$r_{u,p}(x)$ を、x^p を $u(x)$ で割った余り、すなわち

$$x^p \equiv r_{u,p}(x) \bmod u(x),\ \deg r_{u,p}(x) < d$$

とおく。

例 4.2. $u(x) = x^3 - 2$ のとき、

$$x^{11} = (x^8 + 2x^5 + 4x^2)u(x) + 8x^2$$

$$x^{13} = (x^{10} + 2x^7 + 4x^4 + 8x)u(x) + 16x$$

$$x^{31} = (x^{28}+2x^{25}+4x^{22}+8x^{19}+16x^{16}+32x^{13}+64x^{10}+128x^7+256x^4+512x)u(x)+1024x$$

より、$r_{u,11}(x) = 8x^2$、$r_{u,13}(x) = 16x$、$r_{u,31}(x) = 1024x$ である。

定義 4.3. $u(x)$ を整数係数モニック d 次多項式、p を素数とする。
$u(x)$ が $\mathbb{F}_p$ で完全分解するとは、$u(x)$ が $\mathbb{F}_p$ で d 個の相異なる一次式の積に分解することである。

例 4.4. $u(x) = x^3 - 2$ のとき、

$$\begin{aligned} u(x) &\equiv (x+4)(x^2-4x+5) && \bmod 11 \\ &\equiv x^3 - 2 && \bmod 13 \\ &\equiv (x-4)(x-7)(x+11) && \bmod 31 \end{aligned}$$

より、$u(x)$ は $\mathbb{F}_{31}$ で完全分解し、$\mathbb{F}_{11}$、$\mathbb{F}_{13}$ では完全分解しない。

$r_{u,p}(x) \bmod p$ は $\mathbb{F}_p[x]/u(x)$ への Frobenius 写像の作用を表現している。よって、次が成り立つ。

命題 4.5. $u(x) \in \mathbb{Z}[x]$：既約モニック多項式、p : 素数に対し、

$$u(x) \text{ が } \mathbb{F}_p \text{で完全分解する} \iff r_{u,p}(x) \equiv x \mod p$$

である。

Proof.

$$\prod_{a \in \mathbb{F}_p} (x - a) \equiv x^p - x \mod p$$

であるから、

$$u(x) \text{ が } \mathbb{F}_p \text{で完全分解する} \iff u(x) \mid x^p - x \quad \text{in } \mathbb{F}_p$$

である。$r_{u,p}(x)$ の定義より、

$$u(x) \mid x^p - x \quad \text{in } \mathbb{F}_p \iff r_{u,p}(x) - x \equiv 0 \mod p$$

□

ラグランジュの補間多項式について述べよう。多項式補間とは、いくつかの点での関数値が与えられているとき、これらの点において同じ値をとる多項式によって関数を近似することである。

定義 4.6. 相異なる n 個の点 $x_1, \ldots, x_n$ に対して、$f(x_1), \ldots, f(x_n)$ が与えられているとする。このとき、$f(x)$ の近似多項式

$$t_n(x) = \sum_{j=1}^{n} f(x_j)\, l_j(x) \quad \left(\text{ただし、} l_j(x) = \prod_{j \neq k} \frac{(x - x_k)}{(x_j - x_k)} \right)$$

をラグランジュの**補間多項式**と呼ぶ。$t_n(x)$ は $(n-1)$ 次多項式であり、$t_n(x_j) = f(x_j)$ をみたす。

$r_{u,p}(x)$ はラグランジュ補間によって次のように記述できる。

命題 4.7. $u(x) \in \mathbb{Z}[x]$ を既約モニック d 次多項式、$\alpha_1, \ldots, \alpha_d$ を $u(x)$ の $\mathbb{C}$ での根、p を素数とする。このとき、$r_{u,p}(x)$ は

$$r_{u,p}(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)}$$

と書ける。

Proof. $r_{u,p}(x)$ の定義より、$r_{u,p}(\alpha_j) = \alpha_j^p$ である。また、

$$\prod_{j \neq k} (x - \alpha_k) = \frac{u(x)}{(x - \alpha_j)}$$

であり、$u'(x) = \sum_{j=1}^{d} \prod_{k \neq j} (x - \alpha_k)$ より、

$$\prod_{k \neq j} (\alpha_j - \alpha_k) = u'(\alpha_j)$$

である。よって、$r_{u,p}(x)$ の補間多項式は

$$\sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)}$$

である。ここで、$h(x)$ を

$$h(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)} - r_{u,p}(x)$$

とおく。各α_jに対して、$h(\alpha_j) = 0$ であるから $u(x) \mid h(x)$ である。一方、$\deg h(x) \leq d - 1$ である。よって、$h(x) = 0$ を得る。 □

命題 4.8. $u(x) \in \mathbb{Z}[x]$ を既約モニック d 次多項式、$\alpha_1, \ldots, \alpha_d$ を $u(x)$ の $\mathbb{C}$ での根、p を素数、z を複素数とする。このとき、$u(x)$ に対して、$z = p$ のとき $r_{u,p}(x)$ に一致するような整関数 $r_{u,z}(x)$ が存在する。

Proof. 各α_jに対して、$\log\ \alpha_j$の主値 $\mathrm{Log}\ \alpha_j$をとると、$z \in \mathbb{C}$ に対して、α_j^z の値は一つに決まり、

$$r_{u,z}(x) = \sum_{j=1}^{d} \frac{\alpha_j^z u(x)}{u'(\alpha_j)(x - \alpha_j)} \in \mathbb{C}[x]$$

は整関数となる。$z = p$ のときは $r_{u,p}(x)$ のラグランジュ補間である。 □

定義 4.9. $u(x) \in \mathbb{Z}[x]$ を既約モニック d 次多項式、p を素数とする。$g_{u,p}^{(i)}$ を、$r_{u,p}(x)$ の各係数と定義する。すなわち、

$$r_{u,p}(x) = \sum_{i=0}^{d-1} g_{u,p}^{(i)} x^i$$

と定義する。

第5章　主定理1

文献 [2] で挙げられた**問題 1.1.** を解決する定理を述べる。これによって類体論を使えない場合の、多項式の有限体での分解の様子を知ることができる。

定理 5.1. $u(x)$ を整数係数既約モニック d 次多項式とする。このとき、次を満たす $\mathbb{C}^\times$ 上の正則関数 $F_{u,0}, F_{u,1}, \ldots, F_{u,d-1}$ が存在する。

任意の素数 p に対して、

$u(x)$ が $\mathbb{F}_p$ で完全分解する $\iff F_{u,0}(p) = 0, F_{u,1}(p) = 0, \ldots, F_{u,d-1}(p) = 0$

Proof. **命題 4.5.** より、$u(x)$ が $\mathbb{F}_p$ で完全分解するような素数 p に対して、$r_{u,p}(x) - x = 0 \bmod p$ が成り立つ。

$F_{u,i}$ $(0 \leq i \leq d-1)$ を、

$$F_{u,i}(p) = \exp\left(\frac{2\pi\sqrt{-1}}{p}(g_{u,p}^{(i)} - \delta_{i,1})\right) - 1$$

ととると、

$u(x)$ が $\mathbb{F}_p$ で完全分解する $\iff F_{u,0}(p) = 0, F_{u,1}(p) = 0, \ldots, F_{u,d-1}(p) = 0$

が成り立つ。 □

この定理により、**問題 1.1.** で提起された、多項式が完全分解するかどうかを判定する解析関数が作れた。

例 5.2. (1) $u(x) = x^2 - l$ $(l \in \mathbb{Z})$ のとき

$$r_{u,p}(x) = l^{\frac{p-1}{2}}x,\ g_{u,p}^{(0)} = 0,\ g_{u,p}^{(1)} = l^{\frac{p-1}{2}}$$

であるから、

$$F_{u,0}(p) = 0,\ F_{u,1}(p) = G_u(p) = \exp\left(\frac{2\pi\sqrt{-1}}{p}(l^{\frac{p-1}{2}} - 1)\right) - 1$$

が得られる。これにより、

$$u(x)\text{が}\mathbb{F}_p\text{で完全分解} \Longleftrightarrow (\tfrac{l}{p}) = 1 \Longleftrightarrow F_{u,1}(p) = 0$$

($(\frac{l}{p})$ は平方剰余記号)

(2) $u(x) = x^2 - x - 1$ のとき

$$r_{u,p}(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x-\alpha_j)} = F_p x + F_{p-1} \quad (F_n\text{は}n\text{番目のフィボナッチ数})$$

となる。フィボナッチ数に関しての性質

$$F_p \equiv 1、F_{p-1} \equiv 0 \bmod p \iff p \equiv 1, 4 \bmod 5$$

より、

$$u(x)\text{が}\mathbb{F}_p\text{で完全分解} \Longleftrightarrow p \equiv 1, 4 \bmod 5$$

である。

(3) $u(x) = x^3 - l$ のとき

$$\begin{aligned} r_{u,p}(x) &= \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x-\alpha_j)} = \sum_{j=1}^{3} \frac{1}{3}\alpha_j^{p-2}(x^2 + \alpha_j x + {\alpha_j}^2) \\ &= \frac{1}{3}\Big\{(1 + \omega^{p-2} + l^{\frac{p-2}{3}}\omega^{2(p-2)})l^{\frac{p-2}{3}}x^2 + (1 + \omega^{p-1} + l^{\frac{p-1}{3}}\omega^{2(p-1)})l^{\frac{p-1}{3}}x \\ &\quad + (1 + \omega^p + l^{\frac{p}{3}}\omega^{2p})l^{\frac{p}{3}}\Big\} \end{aligned}$$

第6章　主定理2

次に、多項式の高さを定義する。

定義 6.1. $u(x)$ を複素数係数 d 次多項式とする。$u(x)$ の高さ $\mathrm{height}(u(x))$ とは、次数、各係数の絶対値のうち最小のもの、すなわち $u(x)=\sum_{i=1}^{d} a_i x^i$ とおくと、

$$\mathrm{height}(u(x))=\min\{d,|a_1|,\ldots,|a_d|\}$$

と定義する。

次に以下のような問題を考えよう。

問題 6.2. $u(x)$ を整数係数既約モニック d 次多項式とする。h を $u(x)$ の高さ、L を $\mathbb{Q}[x]/(u(x))$ のガロア閉包とする。d、h、$G=\mathrm{Gal}(L/\mathbb{Q})$、いくつかの素数 p について $r_{u,p}(x) \bmod p$ が与えられているとき、もとの多項式 $u(x)$ を求めよ。

文献 [2] の問題は、多項式が与えられたときにその分解の様子を問うものであったが、**問題 6.2.** は逆問題、つまり与えられた分解の様子からそのような挙動をする多項式を求める問題である。
問題 6.2. は以下の定理により部分的に解決される。

定理 6.3. $u(x)$ を整数係数既約モニック d 次多項式、$\alpha_1,\ldots,\alpha_d$ を $u(x)$ の $\mathbb{C}$ での根、$r_{u,p}(x)$ を定義1で定義した多項式、h を $u(x)$ の高さ、L を $\mathbb{Q}[x]/(u(x))$ のガロア閉包、G を $\mathrm{Gal}(L/\mathbb{Q})$、$N$ を与えられた正の整数とする。このとき、素数 p が h、d、N に比べて十分大きければ、次をみたす多項式 $s_{u,p}(x)\in L[x]$ が一意に存在する。

$$\begin{cases} (1)\ s_{u,p}(x) \text{ は } r_{u,p}(x) \bmod p \text{ の } L \text{ への lift である。} \\ (2)\ \deg(s_{u,p}(x)) \le d-1 \\ (3)\ \mathrm{height}(s_{u,p}(x)) \le N \\ (4)\ {}^{\exists}\sigma\in G \quad s_{u,p}(\alpha_j)=\sigma(\alpha_j) \quad (1\le j\le d) \end{cases}$$

Proof. ここから、$r_{u,p}(x) \mod p$ を $\overline{r_{u,p}}\,(x)$ と書くことにする。
$\mathfrak{P}$ を、$\mathfrak{P} \cap \mathbb{Z} = (p)$ をみたす L の整数環 $\mathfrak{O}_L$ の素イデアル ((p) の上にあるイデアル)、$\alpha_j^{(\mathfrak{P})}$ $(1 \leq j \leq d)$ を $u(x)$ の $\mathfrak{P}$ での根とおく。$\overline{r_{u,p}}\,(x)$ は $\mathfrak{P}$ での作用を与える。よって、

$$\overline{r_{u,p}}\,(\alpha_j^{(\mathfrak{P})}) = (\alpha_j^{(\mathfrak{P})})^p \bmod \mathfrak{P}$$

である。$\overline{r_{u,p}}\,(x)$ は $\deg\ \overline{r_{u,p}}\,(x) \leq d-1$、$\overline{r_{u,p}}\,(\alpha_j^{(\mathfrak{P})}) = \sigma(\alpha_j^{(\mathfrak{P})}) \mod \mathfrak{P}$ ($^{\exists}\sigma \in G$) をみたす唯一の多項式である。ここで、$\overline{r_{u,p}}\,(x) = \sum_{i=0}^{d-1} \overline{b_i} x^i$ とおく。各係数 $b_i \mod \mathfrak{P}$ のクラスに属する $c_i \in L$ で、$|c_i| \leq N$ なるものをとる。$s_{u,p}(x)$ を、

$$s_{u,p}(x) = \sum_{i=0}^{d-1} c_i x^i$$

ととると、h、d、$N \ll p$ のとき $s_{u,p}(x)$ はup to conjugate で一意にとれて、(1)〜(4) をみたす。 □

注意 6.4. 一般的に、$r_{u,p}(x)$ と $s_{u,p}(x)$ は異なる。例えば $u(x) = x^3 - 2$ のとき、

$$r_{u,13}(x) = 16x$$

$$s_{u,13}(x) = \zeta_3 x \quad (\ \zeta_3 \text{は } 1 \text{ の } 3 \text{ 乗根で } 1 \text{ でないもの})$$

である。 実はこの $s_{u,p}(x)$ が $p \gg 0$ で近似するのが、ガロア対応を表現する多項式

$$s_{u,\sigma}(x) = \sum_{j=1}^{d} \frac{\sigma(\alpha_j) u(x)}{u'(\alpha_j)(x - \alpha_j)} \quad (\alpha_j \text{は } u \text{ の根、} \sigma \in G)$$

である。

問題 6.2. について考察する。以下の仮定の下で考える。

仮定 6.5. $u(x)$ を整数係数既約モニック d 次多項式、$\alpha_1, \ldots, \alpha_d$ を $u(x)$ の $\mathbb{C}$ での根、h を $u(x)$ の高さ、p を素数、N を正の整数、L を $\mathbb{Q}[x]/(u(x))$ のガロア閉包、G を $\mathrm{Gal}(L/\mathbb{Q})$ とする。

$d = \deg(u(x))$、$h = \mathrm{height}(u(x))$、$N \in \mathbb{Z}_{\geq 0}$、$d, h, N \ll p$ なるいくつかの素数に対して $r_{u,p}(x)$、p の上の素イデアル $\mathfrak{P}$ が与えられたとする。さらに、$G = \mathrm{Gal}(L/\mathbb{Q})$ の各元の位数もしくは各元の演算結果が与えられたとする。**定理 6.3.** により、定理の (1)〜(4) をみたす多項式 $s_{u,p}(x)$ が得られる。$s_{u,p}(x)$ は対応する$\sigma \in G$ の多項式による表現である。ここから、σに対応する $s_{u,p}(x)$ を $s_\sigma(x)$ と書く。

まず G の各元の位数が与えられた場合を考える。σの位数を e_σと書くと、$s_\sigma^{(e_\sigma)}(\alpha_j) = \alpha_j$ より、

$$u(x) \mid s_\sigma^{(e_\sigma)}(x) - x$$

である。よって、$u(x)$ の候補は

$$\gcd\{s_\sigma^{(e_\sigma)}(x) - x \mid \sigma \in G\}$$

で得られる。

一方、G の各元の演算結果が与えられた場合を考える。$\sigma, \tau \in G$ に対し、$s_\sigma \circ s_\tau \equiv s_{\sigma\circ\tau} \bmod u(x)$ より、

$$u(x) \mid s_\sigma \circ s_\tau - s_{\sigma\circ\tau}$$

である。よって、$u(x)$ の候補は

$$\gcd\{s_\sigma \circ s_\tau - s_{\sigma\circ\tau} \mid \sigma, \tau \in G\}$$

でも得られる。

例 6.6. $p = 13$ のとき、

$$\overline{r_{u,p}}(x) = 3x$$

が与えられ、そして他のいくつかの素数に対しても $\overline{r_{u,p}}(x)$ が与えられているとする。

(13) の上の素イデアルは $(1 + 4\zeta_3)$ であり、$\zeta_3 - 3 \in (1 + 4\zeta_3)$ より、

$$s_{u,p}(x) = s_{\sigma_1}(x) = \zeta_3 x \ (\sigma_1 \in G)$$

である。他の素数に対しても同様に $s_{u,p}(x)$ を得るが、一般的に拡大体の素イデアルを知ることは難しい。

u が 3 次式であること や、u の根の置換の対応を与えれば、**注意 6.4.** の $s_{u,\sigma}(x)$ によって、

$$s_{id}(x) = x、s_{\sigma_1}(x) = \zeta_3 x、s_{\sigma_2}(x) = \zeta_3^2 x、$$

$$s_{\sigma_3}(x) = \frac{\sqrt[3]{4}}{2}x^2、s_{\sigma_4}(x) = \frac{\sqrt[3]{4}\zeta_3}{2}x^2、s_{\sigma_5}(x) = \frac{\sqrt[3]{4}\zeta_3^2}{2}x^2$$

を得る。

$$\gcd\{s_\sigma^{(e_\sigma)}(x) - x \mid \sigma \in G\} = \frac{x}{2}(x^3 - 2)$$

$$\gcd\{s_\sigma \circ s_\tau - s_{\sigma\circ\tau} \mid \sigma, \tau \in G\} = x(x^3 - 2)$$

$u(x)$ は 3 次式である、という情報を知っていれば、$u(x)$ の候補は $x^3 - 2$ であると分かる。

今後の課題

定理 5.1. で得られた解析関数は、各素数を代入することで多項式が分解するか否かを判定する関数であるが、類体論や、類体論の裾野の一つであった平方剰余の相互法則のように、分解する素数が直接的に分かる形の判定法が望まれるところである。

よって、今回得られた解析関数の”逆関数”が得られないか調べる。

また、$r_{u,p}$や s_σ を用いた様々な集合の代数構造を調べることにより、素数や多項式の分解についての研究を進めていきたい。

参考文献

[1] H.Kuroiwa, A family of entire functions which determines the splitting behavior of polynomials at primes, Hiroshima Math. J. 41 (2011), no.3, 409-414.

[2] 伊原康隆「これもあれも... いまだ解けていません」, 数理科学, サイエンス社, 1994 年 8 月

[3] 永瀬賢, 本瀬香 , 代数的整数論入門 , 学術図書出版社 , 1998 年 4 月

[4] 加藤和也, 黒川信重, 斎藤毅, 岩波講座 現代数学の基礎 10 数論 1, 岩波書店, 1996 年 10 月

[5] 加藤和也, 黒川信重, 斎藤毅, 岩波講座 現代数学の基礎 10 数論 2, 岩波書店, 1998 年 2 月

[6] J. ノイキルヒ, 代数的整数論, シュプリンガー・フェアラーク東京, 2003 年 3 月