

Construction of integral basis

学習院大学 理 奥津 果作

代数体の整数環の $\mathbb{Z}$ -basis について、Gauss が 2 次体の場合に求めて以来、多くの研究がなされた。たとえば

3 次体 [1], 4 次体 $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ [5], $\mathbb{Q}(\sqrt[3]{m})$ [4],

$\mathbb{Q}(\theta)$ (ここで $\theta^m + A\theta + B = 0, A, B \in \mathbb{Q}$) [3], 等である。

又、Berwick, Zassenhaus 等により、integral basis を求めるアルゴリズムの研究も行なわれているが、この方法はすべての場合に適応できるわけではなく、しかも次第に、

integral basis に近づけるというやり方なので、explicit formula を与えることはできない。([2], [6])

本講の目的は、一般的に integral basis の explicit formula を与えることにある。まず local field の場合に integral basis を求め、その結果を利用して、Global な場合の integral basis を定める。証明は簡単な場合を除いて、ほとんど省略されているので、詳細は [7], [8] を参照して下さい。

§ 1 local case

$\mathcal{O}$ を discrete valuation ring, $\mathfrak{f}$ をその max. ideal, π を $\mathfrak{f}$ の素元, k を $\mathcal{O}$ の商体 とする。 k は完備で, $\mathcal{O}/\mathfrak{f}$ は perfect と仮定する。 k 上の valuation を代数的閉包 $\bar{k}$ 上へ拡張したものを v で表わす。 さらに $f(x)$ を monic irreducible polynomial $\in \mathcal{O}[x]$, とし n を $f(x)$ の次数, θ を $f(x)=0$ の $\bar{k}$ における根の一つとする。 この条件のもとで, $K=k(\theta)$ の整数環 $\mathcal{O}_K$ の $\mathcal{O}$ -basis を求めよ。

Proposition 1 For $0 \leq m < n$, $\exists h_m(x) \in \mathcal{O}[x]$, monic s.t. $\deg h_m(x) = m$, & $|h_m(\theta)| \leq \frac{|g(\theta)|}{|g(x)|}$ (for $\forall g(x) \in \mathcal{O}[x]$, s.t. $\deg g(x) = m$). (ここで $g(x) = \sum_{i=0}^m a_i x^i$ に対して $|g(x)|_{\text{def}} \sup |a_i|$)

Definition 上の $h_m(x)$ に対して $\lambda_m = \text{ord}_{\mathfrak{f}}(h_m(\theta))$, $\nu_m = [\lambda_m]$ (ここで $[\]$ は Gauss 記号) とおく。 $h_m(x)$ を divisor polynomial of degree m of θ over k , ν_m を integrality index of degree m of θ over k とよぶ

divisor polynomial と integrality index により $\mathcal{O}_K$ の $\mathcal{O}$ -basis を explicit に表わすことができる。

Theorem 1 $\mathcal{O}_K = \sum_{m=0}^{n-1} \mathcal{O} \frac{h_m(\theta)}{\pi^{\nu_m}}$ (π は $\mathfrak{f}$ の素元)

Proof $\mathcal{O}_K \supset \sum_{m=0}^{n-1} \mathcal{O} \frac{h_m(\theta)}{\pi^{v_m}}$ は明らか。次に $\exists \ell \in \mathbb{N}$ s.t.

$\mathcal{O}_K \subset \frac{\mathcal{O}[\theta]}{\pi^\ell}$ 中 $\mathcal{O}_K \ni \alpha = \frac{g(\theta)}{\pi^\ell}$ ($\exists g(x) \in \mathcal{O}[x], \deg g(x) < n$).

$d = \deg g(x)$ とおくと, $\exists r_m \in \mathcal{O}$ ($m=0, 1, \dots, d$) s.t. $g(x) = \sum_{m=0}^d r_m h_m(x)$.

divisor polynomial の定義により $|g(\theta)| \geq |g(\alpha)| \cdot |h_d(\theta)| \geq |r_d| \cdot |h_d(\theta)|$.

従って $|\frac{g(\theta)}{\pi^\ell}| \leq 1$ により $\text{ord}_y(\frac{r_d}{\pi^{\ell-v_d}} \frac{h_d(\theta)}{\pi^{v_d}}) \geq 0$ を得る。

一方 $\text{ord}_y(\frac{r_d}{\pi^{\ell-v_d}}) \in \mathbb{Z}$ かつ $0 \leq \text{ord}_y(\frac{h_d(\theta)}{\pi^{v_d}}) < 1$ 中 $\text{ord}_y(\frac{r_d}{\pi^{\ell-v_d}}) \geq 0$ を得る。従って $\sum_{m=0}^{d-1} r_m \frac{h_m(\theta)}{\pi^{v_m}} = \alpha - \frac{r_d}{\pi^{\ell-v_d}} \frac{h_d(\theta)}{\pi^{v_d}}$

は又、 $\mathcal{O}_K$ の元となる。そこで上と同様にして

$\frac{r_m}{\pi^{\ell-v_m}} \in \mathcal{O}$ ($m=0, 1, \dots, n-1$) を得る。従って $\mathcal{O}_K \subset \sum_{m=0}^{n-1} \mathcal{O} \frac{h_m(\theta)}{\pi^{v_m}}$ ■

$\mathfrak{p}$ を $\mathcal{O}_K$ の max. ideal とする。 λ_m を用いて $\mathfrak{p}$ の $k(\theta)/k$ における分枝指数 e 、および相対次数 f を求めることができる。

Theorem 2 $S_m = \{t \mid 0 \leq t \leq n-1, \lambda_t - [\lambda_t] = \lambda_m - [\lambda_m]\}$

とおき、 $\{0, 1, \dots, n-1\} = S_{m_0} \cup S_{m_1} \cup \dots \cup S_{m_k}$ (直和) かつ

$i < j$ ならば $\lambda_{m_i} - [\lambda_{m_i}] < \lambda_{m_j} - [\lambda_{m_j}]$ を満すようにする。

このとき i) S_{m_i} の元の個数はすべて f であり、従って $e = k+1$.

ii) $\lambda_{m_i} - [\lambda_{m_i}] = \frac{i}{e}$ ($i=0, 1, \dots, e-1$) となる。

Corollary 任意の j ($0 \leq j \leq e-1$) に対して

$\{(\frac{h_{m_j}(\theta)}{\pi^{v_{m_j}}})^{-1} \frac{h_t(\theta)}{\pi^{v_t}} \bmod \mathfrak{p} \mid t \in S_{m_j}\}$ は $\mathcal{O}_K/\mathfrak{p}$ の $\mathcal{O}_y$ -basis である。

とくに、 $\{\frac{h_t(\theta)}{\pi^{v_t}} \bmod \mathfrak{p} \mid t \in S_{m_0}\}$ は $\mathcal{O}_K/\mathfrak{p}$ の $\mathcal{O}_y$ -basis である。

integral basis が定まれば 体 K の k 上の判別式が計算できる。判別式と integrality index の関係は次のようになる。

$$\begin{aligned} \text{Theorem 3} \quad D_k(K) &= \pi^{-2 \sum_{m=1}^{n-1} \nu_m} \cdot D_{K/k}(\theta) \\ &= \pi^{f \cdot (e-1) - 2 \sum_{m=1}^{n-1} \lambda_m} \cdot D_{K/k}(\theta) \end{aligned}$$

(ここで $D_{K/k}(\theta)$ は $f(x)$ の判別式である。)

以上みたとおり、divisor polynomial により integral basis を表わすことができるから、divisor polynomial が $f(x)$ より explicit な形で構成されればよい。これに関しては §3 で述べることにして、global な場合に今までの議論がどうなるかを先にみる。

§2 global case

R を principal ideal domain, k を R の商体とする。 R の任意の max. ideal $\mathfrak{p}$ に対して、 $R/\mathfrak{p}$ は perfect と仮定する。 $f(x)$ を monic irreducible polynomial $\in R[x]$, n を $f(x)$ の次数, θ を $f(x)=0$ の $\bar{R}$ (k の代数的閉包) における根の一つとする。さらに $\{\mathfrak{p}_\lambda\}_{\lambda \in \Lambda}$ を R の max. ideal よりなる集合, k_λ を $\mathfrak{p}_\lambda$ に関する k の完備化, $\mathcal{O}_\lambda$ を k_λ の整数環, π_λ を R の元で $\text{ord}_{\mathfrak{p}_\lambda}(\pi_\lambda) = 1$ を満すものとする。 k_λ 上の valuation を代数的閉包 $\bar{k}_\lambda$ 上へ拡張したものを v_λ で表わす。

さて $f(x) = \prod_{i=1}^r f_{\lambda,i}(x)$ を $f(x)$ の $k_\lambda[x]$ における既約因数分解とする。 $f_{\lambda,i}(x)$ は $O_\lambda[x]$ の元で、monic irreducible である。

$\theta_{\lambda,i}$ を $f_{\lambda,i}(x)=0$ の $\bar{k}_\lambda$ における根の一つとする。

さらに embedding $k \hookrightarrow k_\lambda$ を fix して k を k_λ の subfield とみなし、 $\varphi_{\lambda,i}: K=k(\theta) \rightarrow \bar{k}_\lambda$ (k -isomorphism) とおく。
 $\theta \mapsto \theta_{\lambda,i}$

このとき $\forall \lambda \in \Lambda$ に対して real valued function $\|\cdot\|_\lambda$ を

$\|\alpha\|_\lambda = \sup_{i=1, \dots, s} |\varphi_{\lambda,i}(\alpha)|_\lambda \quad (\alpha \in K)$ と定義する。このとき、

prop. 1 に対応して次の成り立つ。

Proposition 2 For $\forall \lambda \in \Lambda$, $\forall m < n \quad \exists g_{\lambda,m}(x) \in R[x]$,
 monic, $\deg g_{\lambda,m}(x) = m$ s.t. $\|g_{\lambda,m}(\theta)\|_\lambda \leq \frac{\|G(\theta)\|_\lambda}{\|G(x)\|_\lambda}$ (for $\forall G(x) \in R[x]$, $\deg G(x) = m$) (ここで $G(x) = \sum_{i=0}^m a_i x^i$ に対して $\|G(x)\|_\lambda = \sup_i |a_i|_\lambda$)

Definition 上の $g_{\lambda,m}(x)$ に対して $\mu_{\lambda,m} = \inf_i \text{ord}_{\varphi_\lambda}(g_{\lambda,m}(\theta_{\lambda,i}))$
 $\nu_{\lambda,m} = [\mu_{\lambda,m}]$ において、 $\nu_{\lambda,m}$ を integrality index of degree m for φ_λ of θ とよぶ。又、 $g_{\lambda,m}(x)$ を divisor polynomial of degree m for φ_λ of θ over k とよぶ。

Proposition 3 $R_\lambda = \sum_{m=0}^{n-1} R \frac{g_{\lambda,m}(\theta)}{\pi_{\lambda,\nu_{\lambda,m}}}$ とおくと

$R_\lambda = \{\alpha \in O_K \mid \pi_{\lambda,\ell} \alpha \in R[\theta] \text{ (for } \ell \in \mathbb{N})\}$ であって、 R_λ は O_K の subring となり、さらに R_λ の max. ideal で φ_λ を含むものはすべて R_λ で invertible となる。

上の proposition により、 $K=k(\theta)$ の整数環 $\mathcal{O}_K$ の R -basis が次のようにして求まることが容易に示される。

Theorem 4 任意の m $0 \leq m \leq n-1$, に対して $g_m(x) \in R[x]$ (monic, $\deg g_m(x) = m$) を $g_m(x) \equiv g_{\lambda, m}(x) \pmod{\pi_{\lambda}^{v_{\lambda, m}}}$ ($\forall \lambda \in \mathcal{L}$) を満すようにとる。(ここで $g_{\lambda, m}(x)$ は divisor polynomial, $v_{\lambda, m}$ は integrality index である。) このとき $\mathcal{O}_K = \sum_{m=0}^{n-1} R \frac{g_m(\theta)}{\prod_{\lambda \in \mathcal{L}} \pi_{\lambda}^{v_{\lambda, m}}}$ となる。

Remark 上の λ は π_{λ} が R で invertible でないもののみに動かせばよく、従って λ は実質的には有限個を動かすことになる。

以上より global な場合も divisor polynomial $g_{\lambda, m}(x)$ が $f(x)$ より explicit な形に構成されはよい。§3 で local な divisor polynomial を構成し、それを用いて §4 で global な divisor polynomial (for π_{λ}) を構成する。

§3 Construction of divisor polynomials (in local case)
notation は §1 と同じとする。さらに $k(\theta)/k$ は separable を仮定する。 $n = [k(\theta): k]$ とする。

Definition $\lambda_k(\theta) = \min_{\beta} \{ |\theta - \beta| \mid [k(\beta): k] < n, \beta \in \bar{k} \}$, さらに $K_k(\theta) = \min_{\gamma} \{ [k(\gamma): k] \mid |\theta - \gamma| = \lambda_k(\theta), \gamma \in \bar{k} \}$ とおく。

Definition $|\theta - \alpha| = \lambda_k(\theta)$, $[k(\alpha):k] = K_k(\theta)$ を満す $\bar{k}$ の元 α の k 上の最小多項式を first primitive divisor polynomial of $f(x)$ over k とよぶ。さらに i -th primitive divisor polynomial of $f(x)$ over k を帰納的に $(i-1)$ -th primitive divisor polynomial of $f(x)$ over k の first primitive divisor polynomial over k として定義する。

i -th primitive divisor polynomial of $f(x)$ over k を $P_i(x)$ とかくことにすると、 $P_i(x) \in \mathcal{O}[X]$, monic irreducible であり、さらに $d_i = \deg P_i(x)$ とすれば、§1 の意味で、 $P_i(x)$ は divisor polynomial of degree d_i of θ over k となる。

first primitive divisor polynomial of $f(x)$ over k の根 α と θ との間関係は次の proposition 4, 5, 6 により与えられる。

Proposition 4 α, η を $\bar{k}$ の元で $|\theta - \alpha| = |\theta - \eta| = \lambda_k(\theta)$, $[k(\alpha):k] = K_k(\theta)$ を満すものとする。このとき $k(\alpha) \ni \forall \beta \neq 0$ に対して $\exists \gamma \in k(\theta)$, $\exists \delta \in k(\eta)$ s.t. $|\beta - \gamma| < |\beta|$ & $|\beta - \delta| < |\beta|$.

次に α, η は上の prop. におけるものとする。 F を $k(\theta, \alpha, \eta)$ を含む k 上の任意の finite galois extension とする。明らかに $H_{\text{alg}} = \{ \sigma \in G(F/\bar{k}) \mid |\theta - \theta^\sigma| \leq \lambda_k(\theta) \}$ は $G(F/\bar{k})$ の部分群となるから、 H に対応する $F/\bar{k}$ の中間体を L とする。 L は F の

とり方によらないことは明らかである。

Proposition 5 notation は上のとおりとする。 T を maximal tamely subextension of $k(\alpha)$ over k とする。

このとき $T \subset L \subset k(\theta) \cap k(\eta)$ となる。

Prop. 4, 5 により 次の Prop. 6 が示される。

Proposition 6 $e(k(\alpha)/k) \mid e(k(\theta)/k)$, $f(k(\alpha)/k) \mid f(k(\theta)/k)$
 $\Rightarrow e(k(\alpha)/k) \mid e(k(\eta)/k)$, $f(k(\alpha)/k) \mid f(k(\eta)/k)$

(ここで $e(k(\alpha)/k)$ は $k(\alpha)/k$ における分岐指数, $f(k(\alpha)/k)$ は $k(\alpha)/k$ における相対次数である。他も同様。)

Corollary $P_i(x)$ を i -th primitive divisor polynomial of $f(x)$ over k とすると $\deg P_i(x) \mid \deg P_{i-1}(x)$ ($i=1, 2, \dots$)
 (ここで $P_0(x) = f(x)$ とする。)

Prop. 5 と Prop. 6 より 次が容易に示される。

Proposition 7 $k(\theta)/k$ が tamely ramified extension であれば、 $k(\alpha) \subset k(\theta)$ となり、さらに $k(\alpha)$ は α のとり方によらず一意的に定まる。

Remark $k(\theta)/k$ が tamely ramified でないとき 一般に $k(\alpha) \subset k(\theta)$ とはならない。

$P_i(x)$ についてはさらに次の性質が証明される。

Proposition 8 m を $m-1 < \text{ord}_y(P_i(\theta)) \leq m$ を満たす自然数とすると $P_i(x)$ は $\text{mod } y^m$ で irreducible である。

Primitive divisor polynomial を用いて §1 における divisor polynomial of degree m ($m < n$) を explicit に構成することができる。

Theorem 5 $P_i(x)$ ($i=1, \dots, r$) を i -th primitive divisor polynomial of $f(x)$ over k , $P_r(x)=1$ とする。
 $d_i = \deg P_i(x)$ ($i=1, 2, \dots, r-1$), $d_0 = n = \deg f(x)$ とおく。

このとき 任意の自然数 $m < n$ に対して、 r 個の自然数

$g_1(m), \dots, g_r(m)$ を次の条件により定める。

$m = g_r(m) + \sum_{i=1}^{r-1} g_i(m) \cdot d_i$ かつ $0 \leq g_i < \frac{d_{i-1}}{d_i}$ ($i=1, \dots, r-1$)
 かつ $0 \leq g_r < d_{r-1}$. (このとき $g_i(m)$ は m により一意に定まることは明らか.) このとき $x^{g_r(m)} \cdot \prod_{i=1}^{r-1} P_i(x)^{g_i(m)}$ は $f(x)$ の m 次の divisor polynomial (over k) である。

Corollary $\gamma_i = \text{ord}_y(P_i(\theta))$ ($i=1, \dots, r-1$) とおくと

$$Q_K = \sum_{m=0}^{n-1} Q \frac{\theta^{g_r(m)} \prod_{i=1}^{r-1} P_i(\theta)^{g_i(m)}}{\pi \left[\sum_{i=1}^{r-1} \gamma_i g_i(m) \right]} \quad \text{となる。}$$

従って i -th primitive divisor polynomial of $f(x)$ が、 $f(x)$ より具体的に求まればよいことになる。 i -th primitive

9.

divisor polynomial of $f(x)$ は $(i-1)$ -th primitive divisor polynomial of $f(x)$ の first primitive divisor polynomial 中. $f(x)$ の first primitive divisor polynomial $P_1(x)$ の構成の algorithm のみで済むはよい. この algorithm の詳細は [8] を参照していただくが, 次の性質を一つだけあげておく.

Proposition 9 $f(x) = \sum_{i=0}^{\frac{n}{d_1}} a_i(x) P_1(x)^{\frac{n}{d_1}-i}$ (ここで,

$a_i(x) \in \mathcal{O}[x]$, $\deg a_i(x) < d_1$, $a_0(x) = 1$) とおく. ...

$m_i = [\text{ord}_y(P_1(\theta)^{i-1})] + 1$ とする $a_i(x) \equiv 0 \pmod{y^{m_i}}$ ($i=2, \dots, \frac{n}{d_1}$).

Corollary $m = [\text{ord}_y(P_1(\theta))] + 1$ とおくと

$f(x) \equiv P_1(x)^{\frac{n}{d_1}} + a_1(x) P_1(x)^{\frac{n}{d_1}-1} \pmod{y^m}$. とくに $n \neq y$ であれば, $P_1(x)$ を適当にとることにより, $f(x) \equiv P_1(x)^{\frac{n}{d_1}} \pmod{y^m}$ となる.

§4 Construction of divisor polynomials (in global case)
local な divisor polynomial 8.3. global な divisor polynomial を構成する方法は次の Thm による. notation は §2 と同じ.

Theorem 6 R の max. ideal $\mathfrak{f}_\lambda$ を一つ fix する.

$f(x) = \prod_{i=1}^s f_{\lambda,i}(x)$ を $f(x)$ の $k_\lambda[x]$ における既約因数分解と
/0.

1. $n_{\lambda,i} = \deg f_{\lambda,i}(x)$ とする。このとき 自然数 $m < n = \deg f(x)$ に対して 1 個の自然数 $m_{\lambda,i}$ ($i=1,2,\dots$) が存在して、次の性質をもつ。 $0 \leq m_{\lambda,i} < n_{\lambda,i}$ ($i=1,2,\dots$) かつ $m = \sum_{i=1}^s m_{\lambda,i}$ であって、 $\prod_{i=1}^s h_{\lambda,i,m_{\lambda,i}}(x)$ は $\mathcal{F}_\lambda$ に対する $f(x)$ の m 次の divisor polynomial となる。ここで $h_{\lambda,i,m_{\lambda,i}} \in R[x]$ は $m_{\lambda,i}$ 次の $f_{\lambda,i}(x)$ の local divisor polynomial である。とくに、 $h_{\lambda,i,m_{\lambda,i}}(x)$ と $\prod_{j \neq i} h_{\lambda,j,m_{\lambda,j}}(x)$ は互いに素になるようにとれる。

上の定理により global な場合も integral basis の explicit construction ができるとが示されたが、又、 TK_2 も考慮に入れば、 $k(\theta)/k$ における $\mathcal{F}_\lambda$ ($\lambda \in L$) の素ideal 分解も $f(x)$ より "explicit" に与えられるともいえる。これは Dedekind の素ideal 分解に関する定理の拡張である。

Reference

- [1] Albert, A. A. : A determination of integers of all cubic fields
Ann. of Math. 31 (1930)
- [2] Berwick, W. : Integral basis, Cambridge Tracts 22 (1927)
- [3] Komatsu, K. Integral basis in algebraic number fields.
J. Reine Angew Math (1975)
- [4] Tietze, H. S.-B. Math.-Nat. Abt. Bayer Akad. Wiss. (1944)
- [5] Williams, Kenneth S. Integers of biquadratic fields.
Canad. Math. Bull. (1970)
- [6] Zassenhaus, H. Funk. approx. Numer. Math (Oberwolfach) 1965
- [7],[8], Okutsu, K. Construction integral basis I, II (to appear)