

Newton polygon から計算される整環の index

東京理科大学大学院 理学研究科 数学専攻

鈴木望夢 (Nozomu SUZUKI) *

概要

Montes と Nart は Ore の定理を拡張し、整環の index が Newton polygon から計算される量と一致する必要十分条件を与えた。しかしながら、彼らは定理の証明を省略しており、また与えられた条件には若干の不足がある。本講演では修正した定理を紹介し、講演者がその証明を与えたことを報告する。

1 Introduction

K を有理数体 $\mathbb{Q}$ の有限次拡大体とする。整数論において、拡大 $K/\mathbb{Q}$ で素数 p がどのように分解するかを求める問題は基本的かつ重要であり、その手法についてもさまざまな研究が知られている。

Dedekind は 1878 年に、 K の定義多項式がある条件を満たすとき、その有限体 $\mathbb{F}_p$ 上での分解と素数 p の $K/\mathbb{Q}$ の分解が対応することを示した。Dedekind の定理が適用できない多項式が存在することは知られているが、Ore は 1928 年に Newton polygon を用いることで Dedekind の定理を拡張し、より多くの多項式から素数の分解が計算できるようになった。

さらに 1992 年に Montes と Nart により Ore の定理が拡張され、適用可能な多項式が著しく増加した。Montes と Nart の定理における多項式に要求される条件は、それ自体を確認することは難しく、彼らは同じ論文でその条件に関する、多項式から容易に計算可能な判定法をも与えた。

しかしながら、彼らは論文内でその証明を省略しており、与えられた判定法にも若干の不備があったため、講演者はこの条件を修正し、その証明を与えた。本レポートでは、修正した判定法を例とともに紹介する。

* E-mail:1123702@ed.tus.ac.jp

2 Preliminaries

p を素数, $\mathbb{Q}_p$ を p 進数体とし, その代数閉包をひとつ固定して $\overline{\mathbb{Q}_p}$ とおく. $\mathbb{Q}_p$ で正規化された $\overline{\mathbb{Q}_p}$ の付値を v とする. また, $\mathbb{Z}_p$ を p 進整数環とする. 多項式

$$a(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_l X^l \in \mathbb{Z}_p[X]$$

に対し,

$$v(a(X)) = \min\{v(\alpha_i) \mid i = 0, 1, \dots, l\}$$

と定め, v を $\mathbb{Z}_p[X]$ まで拡張する. 多項式 $f(X) \in \mathbb{Z}_p[X]$ と, $\mathbb{F}_p$ 上で既約な monic 多項式 $\varphi(X) \in \mathbb{Z}_p[X]$ に対し, $0 \leq \deg a_i(X) < \deg \varphi(X)$ である $a_i(X) \in \mathbb{Z}_p[X]$ を用いて,

$$f(X) = a_0(X) + a_1(X)\varphi(X) + \cdots + a_n(X)\varphi(X)^n \quad (1)$$

と一意的にかき, $\mathbb{R}^2$ 内に点の集合 $V = \{(i, v(a_i(X))) \mid i = 0, 1, \dots, n\}$ をとる. これに対して, V の頂点をいくつか選んで線分で結んで作られる下に凸な折れ線 Γ であって, V の任意の点が Γ の下に存在しないようなものが一意にとれる. これを f の φ -polygon という. f が monic であるとき, φ -polygon の負の傾きをもつ辺全体を **principal part** という. Γ の各線分を Γ の**辺**という. S を Γ の辺としたとき, S の横軸方向の長さを S の**長さ**, 縦軸方向の長さを**高さ**という. また, S の長さ と 高さ の最大公約数を S の**次数**という.

Example 1. $p = 3$ とし, $f(X) = X^8 + X^7 + 7X^6 + 3^6 X + 3^6$ とする. このとき, f の $\mathbb{F}_3$ での既約分解は $\bar{f}(X) = X^6(X+2)^2$ である. もし $\varphi(X) \neq X, X+2$ であるとき, f の φ -polygon は長さ 8, 高さ 0 の辺のみからなり, principal part をもたない.

$\varphi(X) = X$ であるとき, f の X -polygon Γ_X は Figure 1 のようになる. Γ_X の辺を右から S_1, S_2 とすると, Γ_X の principal part は S_2 である. また, 例えば S_2 の長さ と 高さはどちらも 6 であり, したがって, 次数は 6 である.

一方 $\varphi(X) = X+2$ とすると,

$$\begin{aligned} f(X) = & (X+2)^8 - 15(X+2)^7 + 105(X+2)^6 - 448(X+2)^5 \\ & + 1260(X+2)^4 - 2352(X+2)^3 + 2800(X+2)^2 - 1191(X+2) - 153 \end{aligned}$$

となるから, f の $(X+2)$ -polygon は Figure 2 のようになる. なお, X を $X-2$ とすることで, $f(X)$ に対する $(X+2)$ -polygon を考えることと $f(X-2)$ の X -polygon を考えることは同等である. すなわち,

$$g(X) := f(X-2) = X^8 - 15X^7 + 105X^6 - 448X^5 + 1260X^4 - 2352X^3 + 2800X^2 - 1191X - 153$$

の X -polygon を考えれば良い. これにより g の X -polygon と f の $(X+2)$ -polygon を同一視する.

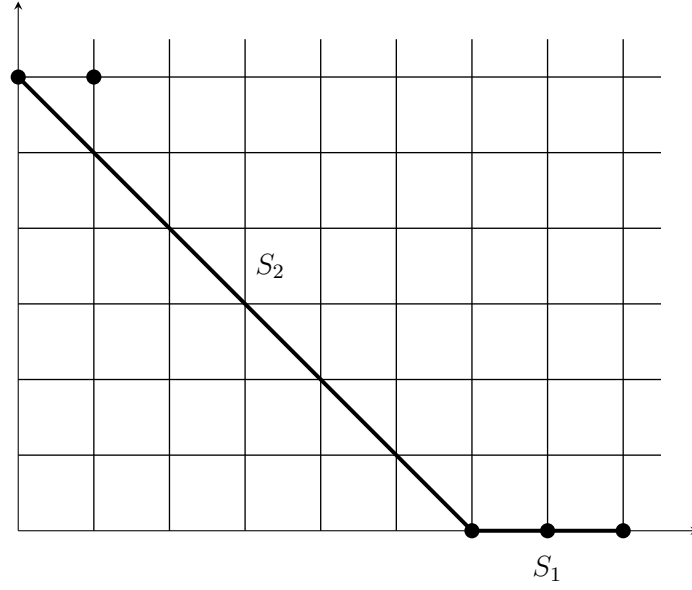


Figure 1 f の X -polygon

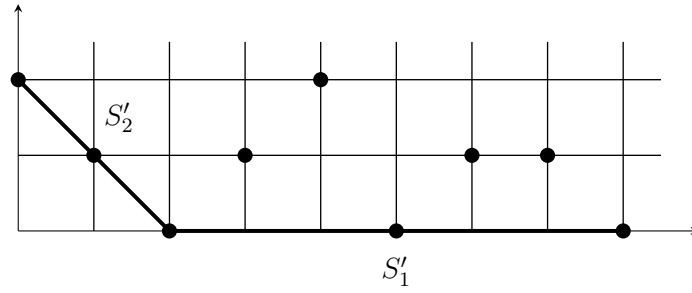


Figure 2 f の $(X+2)$ -polygon

また、特に $\varphi(X) = X$ の場合の φ -polygon は **Newton polygon** とよばれる。

Definition 2 (associated polynomial). 上の記号の設定の下、 S を φ -polygon の辺とし、その両端点を $(s_1, t_1), (s_2, t_2)$ とする。ただし、 $s_1 < s_2$ である。多項式 $f(X)$ の S に関する associated polynomial $f_S(Y)$ を次のように定義する。

$E = s_2 - s_1, H = t_1 - t_2, d = \gcd(E, H), e = E/d, h = H/d$ とおく。また、 φ で定まる不分岐拡大を T とし、その剰余体を $\mathbb{F}_T$ とする。このとき、

$$f_S(Y) = \overline{a_{s_2}/\pi^{t_2}}(\zeta)^{-1} \sum_{i=0}^d \overline{a_{s_1+ie}/\pi^{t_1-ih}}(\zeta) Y^i \in \mathbb{F}_T[Y]$$

と定める。ここで、 ζ は reduction $\overline{\varphi}(X) \in \mathbb{F}_p[X]$ の根である。

Example 3. Example 1 の記号を用いる。このとき

$$\begin{aligned} f_{S_1}(Y) &= Y^2 + Y + 1 = (Y + 2)^2, & f_{S_2}(Y) &= Y^6 + 1 = (Y^2 + 1)^3, \\ g_{S_1'}(Y) &= Y^6 + 2Y^3 + 1 = (Y + 1)^6, & g_{S_2'}(Y) &= Y^2 + 2Y + 1 = (Y + 1)^2 \end{aligned}$$

である。

Definition 4 (index). monic な既約多項式 $f(X) \in \mathbb{Z}[X]$ に対し, $f(X)$ の根 α をとって, $L = \mathbb{Q}(\alpha)$ とし, その整数環を $\mathcal{O}_L$ とする.

(i) $i_p(f) = v([\mathcal{O}_L : \mathbb{Z}[\alpha]])$ と定める.

(ii) $i_\varphi(f)$ を, f の φ -polygon と X 軸, Y 軸に囲まれた領域内の整数格子点であって, 軸上にないものの個数に $\deg \varphi$ をかけたものとして定義する.

Theorem 5 (Ore [2, Theorem of the index]) 多項式 $\bar{f}(X)$ の各既約因子の $\mathbb{Z}_p[X] \rightarrow \mathbb{F}_p[X]$ による monic な引き戻しをひとつずつ選んできたものからなる集合を $\Phi \subset \mathbb{Z}_p[X]$ とする. このとき, 次が成り立つ.

$$i_p(f) \geq \sum_{\varphi \in \Phi} i_\varphi(f).$$

Example 6. 再び Example 1 の状況を考える. このとき

$$i_X(f) = 15, \quad i_{X+2}(f) = 1$$

である. したがって $i_3(f) \geq 16$ を得る.

Definition 7. monic 多項式 $f(X) \in \mathbb{Z}_p[X]$ を (1) のようにかいたとき, $a_n(X) = 1$ であると仮定する. f の φ -polygon の辺を $S_1, \dots, S_g$ とし, $S = S_i$ をひとつ固定する. S に関する f の associated polynomial を $\mathbb{F}_T$ 上で

$$f_S(Y) = \psi_1(Y)^{e_1} \cdots \psi_k(Y)^{e_k}$$

と既約分解する. 各 $\psi_j(Y)$ を, ζ を X とするようにして $\mathbb{Z}_p[X, Y] \rightarrow \mathbb{F}_T[Y]$ で引き戻したものを $\Psi_j(X, Y)$ とする. S に対し, E, H, d, e, h を Definition 2 のようにとる. このとき,

$$f_i^0(X) = p^H \prod_{j=1}^k \Psi_j(X, \varphi(X)^e / p^h)^{e_j}$$

と定め,

$$f^1(X) = f(X) - \prod_{i=1}^g f_i^0(X)$$

と定義する.

Example 8. 再度 Example 1 を用いることとし, $\varphi(X) = X$ とする. このとき Example 3 により

$$\begin{aligned} f_1^0(X) \cdot f_2^0(X) &= (X+2)^2 \cdot 3^6((X/3)^2 + 1)^3 \\ &= X^8 + 4X^7 + 31X^6 + 108X^5 + 351X^4 + 972X^3 + 1701X^2 + 2916X + 2916 \end{aligned}$$

ととることができ, これを用いることで

$$f^1(X) = -3X^7 - 24X^6 - 108X^5 - 351X^4 - 972X^3 - 1701X^2 - 2187X - 2187$$

を得る．同様に， $\varphi(X) = X + 2$ の場合，

$$\begin{aligned} g_1^0(X) \cdot g_2^0(X) &= (X + 1)^6 (X + 3)^2, \\ g^1(X) &= -27X^7 + 45X^6 - 612X^5 + 990X^4 - 2628X^3 + 2628X^2 - 1251X - 162 \end{aligned}$$

となる．

3 Main theorem

講演者は Montes と Nart による判定法を修正し，次の定理を与え証明した．

Theorem 9 (Montes-Nart の判定法の修正版 (cf.[2, Theorem 2])) Theorem 5 と同じ記号を用いる．このとき

$$i_p(f) = \sum_{\varphi \in \Phi} i_\varphi(f)$$

が成り立つ必要十分条件は，任意の $\varphi \in \Phi$ と，任意の f の φ -polygon の principal part の辺 S に対し，以下の条件が成り立つことである．

$$\psi(Y) \mid f_S(Y) \text{ に対し, } \psi(Y)^2 \nmid f_S(Y) \text{ または } \psi(Y) \nmid f_S^1(Y).$$

ここで， $\tilde{S}$ は S を $1/e$ だけ上に並行移動して，それを延長して得られる直線である．

Example 10. Example 1 の多項式に対して Theorem 9 を適用する．Example 8 により，

$$f_{\tilde{S}_1}^1(Y) = Y^6 + 2Y^4 + 2Y^2 + 2, \quad g_{\tilde{S}_1}^1(Y) = 2$$

であり，Example 3 より f は Theorem 9 の条件を満たすことがわかる．したがって Example 6 より

$$i_3(f) = 16 \tag{2}$$

を得る．

Remark 11. Example 10 において non-principal part については条件を確認しなかった．元の Montes と Nart の主張では，すべての辺に対して条件を確認する必要があったが，実際， $g_{S_2'}^1(Y) = 0$ であるから，non-principal part S_2' に対しては定理の条件は満たしていない．しかしながら，等式 (2) は代数計算ソフト Magma[1] による計算で確かめることができる．ゆえに定理は Theorem 9 のように修正されなければならない．

参考文献

- [1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
- [2] Jesús Montes and Enric Nart, *On a theorem of Ore*, J. Algebra **146** (1992), no. 2, 318–334. MR 1152908