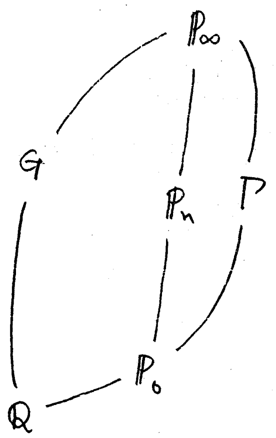
数理解析研究所講究録
第411巻 1981年 19-26

p進L関数入門III
($\mathbb{Z}_p$-拡大と不変量)

山形大 理 木田 祐司

この小文では $\mathbb{Z}_p$-拡大の理論の基本定理を概説する．本格的に勉強するには，S. Lang : Cyclotomic Fields (Springer) の chapter 5 を読まれたい。なお講演では§3は省略したが、書いておく事にする。

§1. p : 素数, $q = 4$ (if $p = 2$) or p (if $p \neq 2$)。$\zeta_m = \exp(2\pi i/m)$ とし, $\mathbb{P}_n = \mathbb{Q}(\zeta_{qp^n})$ $n \geqq 0$, $\mathbb{P}_\infty = \bigcup_{n=0}^{\infty} \mathbb{P}_n$ とする。



円分体論より $\left(\zeta_{qp^n}^{\sigma} = \zeta_{qp^n}^{a}\right)$

$$\begin{array}{ccc}
\sigma & \longleftrightarrow & a \bmod qp^n \\
\cap & & \cap \\
\mathrm{Gal}(\mathbb{P}_n/\mathbb{Q}) & \simeq & (\mathbb{Z}/qp^n\mathbb{Z})^\times \\
\downarrow \text{制限} & \circlearrowright & \downarrow \text{自然} \\
\mathrm{Gal}(\mathbb{P}_{n-1}/\mathbb{Q}) & \simeq & (\mathbb{Z}/qp^{n-1}\mathbb{Z})^\times
\end{array}$$

において projective limit をとれば

$$G \simeq \mathbb{Z}_p^\times$$

この部分群として　　$\Gamma \simeq 1+q\mathbb{Z}_p$　　で右辺は　$\mathbb{Z}_p$(の加法群)に位相同型。そこで一般に

<u>定義</u>　K/k を有限次代数体 k の Galois 拡大とする時，これが $\mathbb{Z}_p$-拡大であるとは

$$\mathrm{Gal}(K/k) \simeq \mathbb{Z}_p\text{(の加法群)}\quad\text{(位相同型)}$$

となる事。

この時は $\mathbb{Z}_p$ の閉部分群が 0 と $p^n\mathbb{Z}_p$ $(n \geqq 0)$ のみだから

$$\begin{array}{ccccccccc} \mathbb{Z}_p & \supset & p\mathbb{Z}_p & \supset \cdots \supset & p^n\mathbb{Z}_p & \supset \cdots \supset & 0 \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ k & \subset & k_1 & \subset \cdots \subset & k_n & \subset \cdots \subset & K = \bigcup_{n=0}^{\infty} k_n \end{array}$$ に対応して

と中間体が一列に並ぶ。K の他はすべて k 上有限次。

<u>例1</u>　$\underline{\underline{\mathbb{P}_\infty/\mathbb{P}_0}}$ が典型的な $\mathbb{Z}_p$-拡大。

<u>例2</u>　$G \simeq \mathbb{Z}_p^\times = (1+q\mathbb{Z}_p)\times W$，$W \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ より W に対応する G の部分群(Δ と書く事が多い)の固定体を $\mathbb{Q}_\infty$ とすると $\underline{\underline{\mathbb{Q}_\infty/\mathbb{Q}}}$ は $\mathbb{Z}_p$-拡大。しかも $\mathbb{Q}$ 上の唯一の $\mathbb{Z}_p$-拡大。

<u>例3</u>　k を有限次代数体とすると，$\underline{\underline{k\cdot\mathbb{Q}_\infty/k}}$ は $\mathbb{Z}_p$-拡大。これを k の cyclotomic (or basic) $\mathbb{Z}_p$-拡大と言う。有限体上の一変数代数函数体の理論との類似という点ではこれが最も重要な $\mathbb{Z}_p$-拡大。

<u>例4</u>　k が non-totally real ならば non-cyclotomic な $\mathbb{Z}_p$-拡大が k 上に存在する。

§2、$\mathbb{Z}_p$-拡大 K/k で何を調べるかと言うと．

<u>問1</u>　k_n の p-class group $A(k_n)$ は $n\to\infty$ でどう変化するか？ 特に位数は？

一般の $\mathbb{Z}_p$-拡大を考えると，あまり本質的でない部分で面倒があるので，$\mathbb{P}_\infty/\mathbb{P}_0$ についてのみ調べる。

L_n：$\mathbb{P}_n$ 上の最大不分岐 abel p-拡大　について

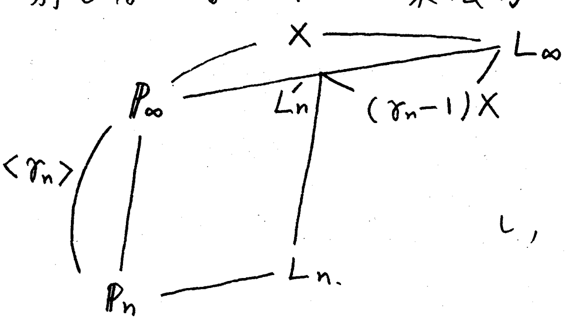
$$\begin{tikzcd} A(\mathbb{P}_n) \arrow[r, phantom, "\simeq"] \arrow[d, "\text{norm}"] & \mathrm{Gal}(L_n/\mathbb{P}_n) \arrow[d, "\text{制限}"] \\ A(\mathbb{P}_{n-1}) \arrow[r, phantom, "\simeq"] & \mathrm{Gal}(L_{n-1}/\mathbb{P}_{n-1}) \end{tikzcd} \qquad (\text{artin map})$$

において projective limit をとれば

$$\circledast \qquad X \simeq \mathrm{Gal}(L_\infty/\mathbb{P}_\infty)$$

ここに $L_\infty=\bigcup_{n=0}^{\infty} L_n$ は $\mathbb{P}_\infty$ の最大不分岐 abel p-拡大。

Γ は左辺に自然に作用する。右辺には $\gamma\in\Gamma$ に対して $u_\gamma\in \mathrm{Gal}(L_\infty/\mathbb{P}_0)$ を $u_\gamma \bmod \mathrm{Gal}(L_\infty/\mathbb{P}_\infty)=\gamma$ なるようにとり $a\in$ 右辺に対して $\gamma\circ a \overset{\text{def.}}{\equiv} u_\gamma\cdot a\cdot u_\gamma^{-1}$ とする。すると上の同型 ㊋ は Γ の作用も含めての同型。以下両者を区別しない。又，Γ は乗法的に X は加法的に記す。



γ_0 を $\Gamma=\mathrm{Gal}(\mathbb{P}_\infty/\mathbb{P}_0)$ の生成元とし，$\gamma_n=\gamma_0^{p^n}$ とする。

ここで $Gal(L_\infty/P_n)$ の交換子群は $(\gamma_n-1)X$ となる。
$\mathfrak{P}_n$ を p を割る P_n の素ideal とすると，これはただ1つで，これだけが P_∞/P_n で分岐する。従って L_n は L_n'/P_n における $\mathfrak{P}_n$ の惰性体。$\mathfrak{P}_n$ の分岐の状況を見れば

$$X/(\gamma_n-1)X \simeq Gal(L_n/P_n) \quad (\simeq A(P_n))$$

よって問1は次の事がわかれば良い。

<u>問2</u> $\mathbb{Z}_p[\Gamma]$-module としての X の構造は？

Iwasawa (Bull. A.M.S. 65(1959)) はこの方針。

Serre (Sem. Bourbaki 174 (1958/59)) はもう1つひねる。Γ の topological generator γ_0 を1つ fix して $\underline{\gamma_0 = 1+T}$ とおく。若干の議論により X は $\underline{\Lambda = \mathbb{Z}_p[[T]]}$ -module とみなせる。

<u>問3</u> Λ-module としての X の構造は？

。Λ の構造：local ring で maximal ideal $\mathfrak{M} = (p, T)$ は高さ2。高さ1の素 ideal は単項で (p) の他は既約な distinguished polynomial で生成される。ここに distinguished polynomial とは $\pi(T) = T^d + \sum_{i=0}^{d-1} a_i T^i$, $a_i \in p\mathbb{Z}_p$ $0 \le i \le d-1$ なるもので $\mathbb{Z}_p[[T]]/(\pi(T)) \simeq \mathbb{Z}_p[T]/(\pi(T))$ なる事が特徴。 abel群としては $\Lambda/(p) \simeq (\mathbb{Z}/p\mathbb{Z})^\infty$, $\Lambda/(\pi(T)) \simeq \mathbb{Z}_p^{\,d}$ と全く type が違う事に注意。

中山の補題によりXは有限生成Λ-moduleとなるので、Λ-moduleの基本定理（see ① ブルバキ「可換代数」＋前記のSerreの論文．又は ② 冒頭に掲げたLangの本）よりXは

$$E(X) = \Lambda^{m_0} \oplus \Lambda/(\pi_1^{m_1}) \oplus \cdots \oplus \Lambda/(\pi_s^{m_s})$$

（ここに π_i は p 又は既約な distinguished polynomial）型のΛ-moduleに pseudo (quasi)-isomorphic となる。

つまり Λ-hom. $\rho : X \longrightarrow E(X)$ で $\mathrm{Ker}\,\rho$, $\mathrm{Coker}\,\rho$ が共に位数有限なるものが存在する。

（注 単因子論の modification と見られる。実際②の証明は体係数の多項式環上のmoduleにおける証明と同様なもの。）

すると $E = E(X)$ へのTの作用は具体的だから $p^{e'_n} = |E/(\gamma_n - 1)E|$ は計算出来る。（recall : $\gamma_n = (1+T)^{p^n}$）

まず、有限でなければならぬので $m_0 = 0$。そして

$$f = \prod_{i=1}^{s} \pi_i^{m_i} = p^{\mu}(T^{\lambda} + \cdots) \quad とすると$$

$$e'_n = \lambda \cdot n + \mu \cdot p^n + \text{constant} \qquad \text{for all } n \gg 0$$

となる。これから $p^{e_n} = |X/(\gamma_n - 1)X|$ を求める。

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\gamma_n - 1)X & \longrightarrow & X & \longrightarrow & X/(\gamma_n - 1)X & \longrightarrow & 0 \\
 & & \downarrow \rho'_n & & \downarrow \rho & & \downarrow \rho''_n & & \\
0 & \longrightarrow & (\gamma_n - 1)E & \longrightarrow & E & \longrightarrow & E/(\gamma_n - 1)E & \longrightarrow & 0
\end{array}$$

（ここで ρ'_n, ρ''_n は ρ から自然に induce されるもの）

なる図式において $|\mathrm{Image}\,\rho''_n|$ を計算すれば

$$|X/(\gamma_n-1)X| / |\mathrm{Ker}\,\rho_n''| = |E/(\gamma_n-1)E| / |\mathrm{Coker}\,\rho_n''|$$

ここで $|\mathrm{coker}\,\rho_n''|$ は $n\to\infty$ で単調増加、しかし $\leqq$ $|\mathrm{coker}\,\rho|_0$ 又、$|\mathrm{Ker}\,\rho_n''|$ は有限かつ単調減少。よって十分大きい n でどちらも一定の値をとる。

$$\therefore \quad e_n = e_n' + \text{constant} \qquad \text{for all } n \gg 0$$

$$= \lambda\cdot n + \mu\cdot p^n + \text{constant} \qquad \text{for all } n \gg 0 .$$

本質的に同様な議論により、一般の $\mathbb{Z}_p$-拡大についても

<u>$\mathbb{Z}_p$-拡大の基本定理</u>

・ K/k : $\mathbb{Z}_p$-拡大

・ $X = \varprojlim A(k_n)$ ただし $A(k_n) \xrightarrow{\text{norm}} A(k_{n-1})$ 。

$\mathrm{Gal}(K/k)$ の生成元 γ_0 を1つとり $\gamma_0 = 1+T$ とおけば K/k, γ_0 によって定まる $\Lambda = \mathbb{Z}_p[[T]]$-module $E(X)$ $= \Lambda/(\pi_1^{m_1}) \oplus \cdots \oplus \Lambda/(\pi_s^{m_s})$ が存在して

(π_i は p 又は既約な *distinguished polynomial*)

X はこれに *pseudo-isomorphic* となる。更に

$$f = \prod_{i=1}^{s} \pi_i^{m_i} = p^{\mu}(T^{\lambda} + \cdots)$$

$$p^{e_n} = |A(k_n)|$$

とすると

$$e_n = \lambda\cdot n + \mu\cdot p^n + \text{constant} \qquad \text{for all } n \gg 0$$

が成立する。

定義 ここで定まる非負整数 λ, μ を K/k の岩沢不変量（Iwasawa invariants）と言い $\lambda(K/k)$, $\mu(K/k)$ と記す。e_n の式から γ_0 のとり方に関係しない事がわかる。

これを調べたい。より詳しく

問4 多項式 f はどんなものか？（ただし f は K/k のみならず γ_0 のとり方にも関係する。）

§3 K/k を絶対 abel 体 k の cyclotomic $\mathbb{Z}_p$-拡大とし，$G = \mathrm{Gal}(k/\mathbb{Q})$，$\hat{G} = \mathrm{Hom}(G, \overline{\mathbb{Q}_p})$ とする。

X と $E(X)$ に $\otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}_p}$ を作用させると

$$V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}_p} \simeq \overline{\mathbb{Q}_p}[T]/(\pi_1^{m_1}) \oplus \cdots \oplus \overline{\mathbb{Q}_p}[T]/(\pi_s^{m_s})$$

（有限位数の部分は消えて）$\overline{\mathbb{Q}_p}$ 上の vector spaces としての同型を得る。π_i の中に p があれば，そこも消えるが，Ferrero-Washington の定理より，それは起こらない。すると $f = \prod_{i=1}^{s} \pi_i^{m_i}$ は V の線型変換としての $T = \gamma_0 - 1$ の特性多項式に他ならない。これを分解する。

$k \cap \mathbb{Q}_\infty = \mathbb{Q}$ の場合だけを示せば十分。その時は自然に $\mathrm{Gal}(K/\mathbb{Q}_\infty) \simeq G$ ゆえ X は $\mathbb{Z}_p[G]$-module でもある。よって V は $\overline{\mathbb{Q}_p}[G]$-module。ここで

$$1 = \sum_{\chi \in \hat{G}} e_\chi \quad , \quad e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g$$

は $\overline{\mathbb{Q}}_p[G]$ における 1 の直交巾等元への分解。従って

$V = \bigoplus_{\chi} e_\chi V$ と分解されるが，G と Γ は可換ゆえ，各 $e_\chi V$ は Γ-invariant。(又，$e_\chi V$ は $\{v \in V \mid gv = \chi(g)v$ for all $g \in G\} = V_\chi$ に等しい。)

結局次の問に達したわけである。

<u>問 5</u>　<u>$e_\chi V$ の線型変換 $\gamma_0 - 1$ の特性多項式は何か？</u>

(ただし，K/k，γ_0，χ の 3 つに関係する。)

<u>注</u>　この辺は Greenberg による Iwasawa の main conjecture の formulation (Nagoya Math. J. 56 (1974), 67 (1977)) を参照の事。

<u>付記</u>　岩沢不変量に関する open questions をいくつか。

K/k を cyclotomic $\mathbb{Z}_p$-拡大とする。

Q1. $\mu(K/k) = 0$? (k が abel/$\mathbb{Q}$ なら yes, by Ferrero–Washington)　— Iwasawa の予想 —

Q2. k が totally real ならば更に $\lambda(K/k) = 0$?

(全然わかっていない)　— Iwasawa–Greenberg の予想 —

Q3　k を固定して p を動かす時，λ は bounded ?

(全然わかっていない)　— Ferrero の予想 —

Q4　絶対 abel 体の Cyclotomic $\mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_r}$-拡大 ($p_1, \cdots, p_r$ は異なる素数) において類数の p_i-part，および non p_i-part を調べよ。　— 小生の問 —