

ある p 進完備な関数体 についての問題

東大 理 伊原 康隆

この小文の目的は (i) 問題の提出 (ii) それに関する予備的な結果 (定理 1, 2, 3) を記す事、及び (iii) その問題の生じた背景についての簡単な説明である。その問題とは以下に定義する「 p 進完備な関数体」 $\mathbb{Q}(t)_p$ の上の「類体論」(アーベル拡大の理論) を求める事で、Kronecker 次元 $= 2$ のこの体は、多分、その上の類体論が未だ知られていない体のうちで最も簡単且つ基本的なもの(の一つ)であろう。尚シンポジウムに於ては (iii) に重負をおいて話をしたが、ここでは紙数の関係もあって重負は (ii) におき、(iii) については極く簡単にふれるのみにとどめた。

§1. $\mathbb{Q}$: 有理数体、 p : 素数、 t : $\mathbb{Q}$ 上の変数とする。
有理関数体 $\mathbb{Q}(t)$ に於る加法的な離散付値 ord_p を

$$\mathbb{Q}(t) \ni x = p^v \frac{g(t)}{f(t)} ; \quad f(t), g(t) \in \mathbb{Z}[t], \nexists p \in \mathbb{Z}[t]$$

に対して

$$\text{ord}_p x = v$$

と定義する。ただし $\mathbb{Z}$ は有理整数環。これが加法付値の条件を満たす事は $p\mathbb{Z}[t]$ が $\mathbb{Z}[t]$ の素イデアルなる事(ガウスの補題)によりたゞちに確かめられる。又明らかに p は ord_p の素元であり、剰余体は標数 p の素体 F_p 上の有理関数体 $F_p(t)$ である。さて $\mathbb{Q}(t)$ の ord_p による完備化を

$$\mathbb{Q}(t)_p$$

と表わす。 ord_p の $\mathbb{Q}$ への制限は通常の p 進付値と一致するから $\mathbb{Q}(t)_p$ は p 進体 $\mathbb{Q}_p$ 上の有理関数体 $\mathbb{Q}_p(t)$ を含むが、これらは明らかに相異区別を要する。 $\mathbb{Q}(t)$ に於る ord_p の付値環 (valuation ring) を $\mathcal{O}$ とする。従って、

$$\mathcal{O} = \left\{ \frac{g(t)}{f(t)} \mid f(t), g(t) \in \mathbb{Z}[t]; f(t) \notin p\mathbb{Z}[t] \right\}$$

であり、 $\mathbb{Q}(t)_p$ の任意の元 $x \neq 0$ は p の巾級数として

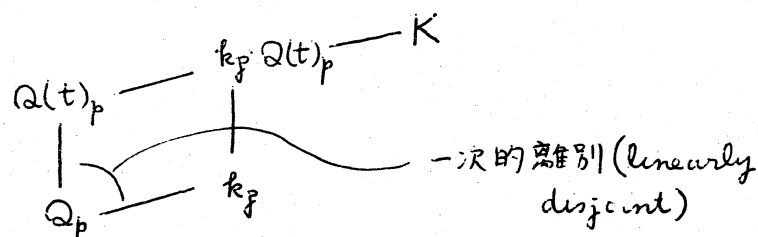
$$x = a_v(t)p^v + a_{v+1}(t)p^{v+1} + \dots$$

の形に一意的に表わされる。ただし $v = \text{ord}_p x$ で、各 $a_n(t)$ ($n \geq v$) はあらかじめ与えられた $\mathcal{O} \bmod p\mathcal{O}$ の代表の中の一元であり、 $a_v(t) \not\equiv 0 \pmod{p\mathcal{O}}$ 。

(注意) 容易に確かめられるように、 $\mathbb{Q}_p$ は $\mathbb{Q}(t)_p$ の中で代数的に閉じている。

$\mathbb{Q}(t)_p$ の有限次拡大 n : 自然数 K : $\mathbb{Q}(t)_p$ の n 次拡大

とする。 $\mathbb{Q}(t)_p$ は完備だから ord_p の一意的な延長によって K もまた完備な付値体となる。 K 中の $\mathbb{Q}_p$ の代数的閉包を k_p とすると図式



により k_p は f 進体で $[k_p: \mathbb{Q}_p]$ は n の約数である。これが n になるとき、即ち $K = k_p \cdot \mathbb{Q}(t)_p$ のとき K を $\mathbb{Q}(t)_p$ の 定数拡大 とよぶ。従って $\mathbb{Q}(t)_p$ の定数拡大は $\mathbb{Q}_p$ の有限次拡大と一対一に対応する。一方 K の剰余体を $\bar{K}$ とするとそれは $\mathbb{Q}(t)_p$ の剰余体 $F_p(\bar{x})$ の有限次拡大、従って有限体上の一変数代数関数体¹⁾ で $f = [\bar{K}: F_p(\bar{x})]$ は n の約数である。今 $f = n$ 且つ $\bar{K}/F_p(\bar{x})$ が分離的 (separable) のとき (一般論に於るよひ方を襲用して) $K/\mathbb{Q}(t)_p$ は 不分岐 と呼ぶ。従って (付値論の一般論により):

$\mathbb{Q}(t)_p$ の不分岐拡大は剰余体 $F_p(\bar{x})$ の分離拡大と一対一に対応する。

不分岐アーベル拡大とアーベルな定数拡大の合成に含まれるような $\mathbb{Q}(t)_p$ のアーベル拡大を 初等的な拡大 とよぶ事にする。

註1) 離散的生成 (separably generated) とは限らないが。

さて我々の提出したい内題は

$\mathbb{Q}(t)_p$ 上の「類体論」を求める事

である。より一般には $K \in \mathbb{Q}(t)_p$ 上の有限次拡大とするとき K 上の類体論の構成が問題である。ところで初等的なアーベル拡大を求める事は、剰余体のアーベル拡大と定数体のアーベル拡大を求める事に帰着するから、 K 上の類体論を求める問題は有限体上の一変数代数関数体上の類体論 (F.K. Schmidt) 及び局所類体論 (H. Hasse, F.K. Schmidt) の拡張である。

ところで

§2. 定理1 n が p で割れないなら $\mathbb{Q}(t)_p$ 上の n 次アーベル拡大は初等的な拡大に限る。

従って n が p のべきである場合のみを問題にすればよいわけである ($n = n_0 p^r$, $n_0 \not\equiv 0 \pmod{p}$) とするとき n 次アーベル拡大は n_0 次アーベル拡大と p^r 次アーベル拡大の合成だから、

(定理1の証明) 一般に k は離散付値で完備な体、 n は k の剰余体の標数 p で割れないとし、 $K \in k$ 上 n 次のガロア拡大とする。 K/k に於る分岐指数を e 、楕円体 k_T とおくと $e \not\equiv 0 \pmod{p}$ だから K/k_T は e 次の巡回拡大で、しかも k_T は1の原始 e 乗根 ζ を含む。従って $K = k_T(e\sqrt[n]{\pi})$ (π は k_T の素元) とかける。以上はよく知られているが更にこの事より、 K/k がアーベル拡大なるときは $\zeta \in k$ も容易にわかる。実

際 $\sigma \in k_T/k$ の任意の自己同型とし $\sigma\zeta = \zeta^m$, $\sigma\pi = \pi'$ とおくと $k_T(e\sqrt{\pi'}) = k_T(e\sqrt{\pi})$ より $\pi' = \pi^l a^e$ ($a \in k_T$) の形でなくてはならない。従って $e\sqrt{\pi'}$ の一つとして $(e\sqrt{\pi})^l a$ をとり、 σ の K への延長 $\tilde{\sigma}: e\sqrt{\pi} \rightarrow e\sqrt{\pi'}$ をとると、 K/k_T の自己同型として $e\sqrt{\pi} \rightarrow \zeta e\sqrt{\pi}$ に対して $\tilde{\sigma}\tau(e\sqrt{\pi}) = \zeta^m e\sqrt{\pi'}$, $\tau\tilde{\sigma}(e\sqrt{\pi}) = \zeta^l e\sqrt{\pi'}$; 従って $\tilde{\sigma}\tau = \tau\tilde{\sigma}$ により $m \equiv l \pmod{e}$. 一方 π' もまた k_T の素元だから $l \equiv 1 \pmod{e}$, $\therefore m \equiv 1 \pmod{e}$. $\therefore \sigma\zeta = \zeta$. σ は k_T/k の任意の自己同型だから $\zeta \in k$.

さて $k = \mathbb{Q}(t)_p$, $K: k$ 上の n 次 アーベル拡大とすると $K = k_T(e\sqrt{\pi})$, π は k_T の素元で k は 1 の原始 e 乗根 ζ を含む。 k_T/k は不分岐ゆえ $p \notin k_T$ の素元、従って $\pi = p\pi_0$ (π_0 は k_T の単数) とかけて、 K は $K_1 = k_T(e\sqrt{\pi_0})$ と $K_2 = k(e\sqrt{p})$ の合成に含まれる。然るに K_1/k , K_2/k は各々不分岐な p -近接拡大であり、 $\zeta \in k$ だから 双方共に k 上のアーベル拡大である。従って K は k の初等的な拡大体である。 (証明おわり)

p 次の巡回拡大 ここで $\mathbb{Q}(t)_p$ 上の p べき乗アーベル拡大をすべて求める事が問題だが、未解決である。たゞ p 次のアーベル (従って巡回) 拡大を求める事は比較的容易にできるのでその結果をここに記す。(特に初等的でない p 次巡回拡大の存在が示される)

今度は ζ を 1 の原始 p 乗根として $k = \mathbb{Q}(t)_p$, $k' = k(\zeta)$ とおく。従って k' は k 上 $p-1$ 次の巡回拡大である。さて k 上 p 次の巡回拡大 K と、 k' 上 p 次の Kummer 拡大 K' で K'/k がアーベル拡大なるようなものが ($K' = K(\zeta)$ によって) 一対一に対応する事は明らかである。

$$\begin{array}{ccc}
 & K & K' = K(\zeta) \\
 & \uparrow & \uparrow \\
 Q(t)_p = k & \xrightarrow{p} & k' = k(\zeta)
 \end{array}$$

従って問題は $K' = k'(p\sqrt{x})$ (ただし $x \in k'$, $\notin (k')^p$) が k 上アーベル拡大になる為の必要十分条件を求める事に帰する。

まず $\mathbb{Q}_p(\zeta) = \mathbb{Q}_p(\pi)$, $\pi = p^{-1}\sqrt{-p}$ である事は容易に確かめられる。従って $k' = k(\pi)$ で π は k' の素元である。次に $y \in k'$, $y \equiv 1 \pmod{\pi}$ とするとき、 $y \in (k')^p$ なる為の必要十分条件は k' のある整数 c に対して

$$y \equiv 1 + (c^p - c)\pi^p \pmod{\pi^{p+1}}$$

となる事である。一方 $K' = k'(p\sqrt{x})$ が k 上アーベル拡大とすると x に適当な k' の p 乗元 z をかける事によって $x \equiv 1 \pmod{\pi}$ となる事は簡単にわかるから はいめから $x \equiv 1 \pmod{\pi}$ を仮定する。また 以下 x は k' の p 乗元ではないとする。上記注意により x は $\text{mod } \pi^{p+1}$ でのみ与えられればよい。まず、

定理2 $x \in k'$, $x \equiv 1 \pmod{\pi}$ とする。 K'/k がアーベル拡大で、
 且つ K/k が不¹⁾分岐である 為の必要十分条件は $x \equiv 1 \pmod{\pi^p}$
 なる事である。このとき $x \equiv 1 + \theta \pi^p \pmod{\pi^{p+1}}$ とおくと K/k の
 剰余拡大は方程式 $X^p - X = \bar{\theta}$ による ($\bar{k}$ の) Artin-Schreier 拡大
 である。ただし $\bar{\theta}$ は剰余類 $\theta \pmod{\pi}$ を表わす ($\bar{k}' = \bar{k}$ に注意)。

(証略)

従って k 上不分岐な p 次巡回拡大を法としてのみ K を考
 えるなら x は $\pmod{\pi^p}$ でのみ考えればよい事がわかった。さて我
 らの結果は

定理3 $x \in k'$, $x \equiv 1 \pmod{\pi}$ とするとき、 K' が k 上のアーベル
 拡大である為には k' の整数 a が存在して

$$x \equiv 1 + a\pi + \frac{a^2\pi^2}{2!} + \cdots + \frac{a^{p-1}\pi^{p-1}}{(p-1)!} \pmod{\pi^p}$$

となる事が必要十分である。このとき 対応する K を K_a と記
 すと K_a は k の p 次不分岐巡回拡大を法として一意的に定ま
 る。又 2 つの $K_a, K_{a'}$ が (上記 不分岐拡大を法として) 一致するた
 めにはある有理整数 r に対して $a' \equiv ra \pmod{p}$ となる事が必
 要十分である。²⁾最後に K_a が k の初等的な拡大なる為には ある
 有理整数 a_0 が存在して $a \equiv a_0 \pmod{p}$ となる事が必要十分である。

註1 明らかに K/k : 不分岐 $\iff K'/k'$: 不分岐 である (K'/k : アーベル 等によ)

註2 $p \sim \pi^{p-1}$ に注意

(証明略)

以上により k 上の p 次巡回拡大は(原則的には)すべて求まったわけである。又初等的でないものの存在も明らかである(例えば K_t)。

最後に次の事を注意する。 $k = \mathbb{Q}(t)_p$ の連続な(即ち付値を変えない)自己同型全体の群を G 、その中で $\text{mod } p$ の各類を変えないものの全体の作る部分群を G_1 とおくと、 G の元 σ は t のゆく先 t_1 によって一意に定まり、 t_1 は $\text{mod } p$ で t の1次関数であればよい。又 $\sigma \in G_1 \iff t_1 \equiv t \pmod{p}$ 。(例えば $t \rightarrow t+p$ は G_1 の元を与える) さて k の有限次拡大 K に対して、任意の $\sigma \in G_1$ が K の自己同型に延長できるとき K を G_1 -normal とよぶ事にする。実は k の G_1 -normal な拡大は(その剰余拡大がつばねても) k の剰余体の研究に本質的な意味をもつ事が確からしいのである。さて K が k の不分岐拡大と定数拡大の合成に含まれれば(アーベル拡大でなくても) G_1 -normal である事は簡単に示される。ところで定理3は、その逆は成り立たない事を示す。実際 Ka/k が G_1 -normal なる為の必要十分条件は a が $\text{mod } p$ で t^p の函数となる事である。

以上は問題の提示とその「入口付近の清掃」のような事であるが、全く無価値ではない事を期待する。

§3. 問題の由来 一般に有限体上の一般数代数関数体 F に対して、 F の素因子の集合(ただし有限箇の例外素因子を

除く) の上で定義され p -adic な値をとるようなある種の関数を数論的に説明する必要がある。その為の一つの試みとしてこのような問題が生じたので、一番簡単な例は次のものである。

p : 素数 $\neq 2, 3$, F_p : 標数 p の素体, $\widehat{F}_p$: その代数的閉包とする。各 $j \in \widehat{F}_p$, $j \neq 0, 1$ に対して $d_j = [F_p(j) : F_p]$ とおき、 $\mathbb{Q}_p^\times$ ($\mathbb{Q}_p$ の乗法群) の部分群 Π_j を次のように定義する。 $\widehat{F}_p$ で定義された modulus j の楕円曲線 E を任意にえらび、 E が $\mathbb{Q}_p$ の上で定義されるような有限体 F_q ($q = p^d$, $d \equiv 0 \pmod{d_j}$) を勝手にとって、 E の F_q 上の合同類の分子を $(1 - \alpha u)(1 - \alpha' u)$ ($\alpha\alpha' = q$) とおく。そのとき α'/α は $\mathbb{Q}_p^\times$ に属し、与えられた j に対して E 及び F_q を上記条件のもとで勝手に動かすときこのような α'/α 全体は $\mathbb{Q}_p^\times$ の部分群をなす。それを Π_j とおく。そうすると、 j が supersingular のときは $\Pi_j = \{\pm 1\}$ ($d_j = 1$ のとき) または $\Pi_j = \{1\}$ ($d_j = 2$ のとき) となり、 j が supersingular でなければ Π_j は $\text{ord}_p \pi_j = d_j$ なる元 π_j で生成される無限巡回群となる。又 j, j' が F_p 上互いに共役なら $\Pi_j = \Pi_{j'}$ 。さて、こうして得られる j ($\neq 0, 1$, supersingular) の関数 π_j を問題にするのであるが、その為には(本質的には π_j よりむしろ Π_j なる事に眼をつけて) 次のように考えてみる。即ち、 Π_j をホルムスの群とするような $\mathbb{Q}_p$ のアーベル拡大が

局所類体論によって唯一つ定まる、それ K_j とする。 K_j は $\mathbb{Q}_p$ の d_j 次不分離拡大 $\mathbb{Q}_p^{(d_j)}$ を含み $K_j/\mathbb{Q}_p^{(d_j)}$ は巡回拡大、完全分岐でガロア群は $\mathbb{Q}_p$ の p 進乗数群 $\mathbb{U}_p$ と同型である。従って $j \rightarrow K_j$ なる対応を説明する事が内題となる。ところでこれに関し次の事がいえるのである。 $\mathbb{Q}(t)_p$ 上の無限次巡回拡大 K で、完全分岐、 $K/\mathbb{Q}(t)_p$ のガロア群は $\mathbb{U}_p$ と同型なるものが存在し、次の性質を満たす。各 $j \in \widehat{\mathbb{F}_p} (\neq 0, 1, \text{supersingular})$ に対して その $\mathbb{F}_p$ 上の共役元全体 $j = j_1, \dots, j_d$ ($d = d_j$) とおき、 $\mathbb{Q}_p^{(d_j)}$ の元 $\tilde{j}_1, \dots, \tilde{j}_d$ を $\tilde{j}_i \pmod{p} = j_i$ ($i = 1, \dots, d$) なるようにとる。そのとき K の「 $t \rightarrow \tilde{j}_i$ 上の specialization」 $K_{\tilde{j}_i}$ が定義され $K_{\tilde{j}_1}, \dots, K_{\tilde{j}_d}$ を「平均」したものであるとして K_j を得るのである。即ち関数 $j \rightarrow K_j$ は $\mathbb{Q}(t)_p$ 上の一つの拡大 K によって与えられる、従って K を類体論的に特徴づけらねば 関数 $j \rightarrow K_j$ 従って関数 $j \rightarrow \pi_j$ の数論的説明(猜内曲線をはなれた)ができるというわけである。

以上大雑把な説明だが最後に一つ注意を述べて終りとする。上記 $K_{\tilde{j}_i}$ は ($\mathbb{Q}_p$ 上の拡大として) $\tilde{j}_i \pmod{p}$ の類にしかよらない。その事は K が G_1 -normal という事と関連している！ところがこの K は更に $\mathbb{Q}(t)_p$ の初等的な拡大なのである。たゞ、同様の内題から生ずる他の K については一般には初等的な

拡大にならぬ(しかし G_1 -normal にはなる)ように思われる。

[文献] 特になし。