数理解析研究所講究録
第 41 巻 1968 年 7-17

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」$Q(t)_p$ 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) に重点をおいて話をしたが、ここでは紙数の関係もあって重点は (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　Q：有理数体、　p：素数、　t：Q 上の変数とする。有理関数体 $Q(t)$ に於る加法的な離散付値 ord_p を

$$Q(t) \ni x = p^\nu \frac{g(t)}{f(t)} ; \qquad f(t), g(t) \in \mathbb{Z}[t], \notin p\mathbb{Z}[t]$$

に対して

$$\mathrm{ord}_p\, x = \nu$$

と定義する。たゞし $\mathbb{Z}$ は有理整数環。これが加法付値の条件を満す事は $p\mathbb{Z}[t]$ が $\mathbb{Z}[t]$ の素イデヤルなる事(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 $F_p(\bar{t})$ である。さて $Q(t)$ の ord_p による完備化を

$$Q(t)_p$$

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

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

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

$$x = a_\nu(t)p^\nu + a_{\nu+1}(t)\,p^{\nu+1} + \cdots$$

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

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

<u>$Q(t)_p$ の有限次拡大</u>　n: 自然数　K: $Q(t)_p$ の n 次拡大とする。$Q(t)_p$ 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 の中での Q_p の代数的閉包を $k_{\mathfrak{p}}$ とすると図式

$$\begin{tikzcd}[arrows=dash]
 & k_{\mathfrak{p}}\cdot Q(t)_p \arrow[r] & K \\
Q(t)_p \arrow[ur] \arrow[d] & & \\
Q_p \arrow[r] & k_{\mathfrak{p}} \arrow[uu] &
\end{tikzcd}$$

一次的離別 (linearly disjoint)

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

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

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 $Q(t)_p$ のアーベル拡大を<u>初等的な拡大</u>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問題は

<u>$Q(t)_p$ の上の「類体論」を求める事</u>

である。より一般には K を $Q(t)_p$ 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の上の類体論 (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 <u>n が p で割れないなら $Q(t)_p$ 上の n 次アーベル拡大は初等的な拡大に限る。</u>

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 を k 上 n 次のガロア拡大とする。K/k に於る分岐指数を e、惰性体を 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 $K = k_T(\sqrt[e]{\pi})$ (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、<u>K/k がアーベル拡大なるときは $\zeta \in k$</u> も容易にわかる。実

際 σ を k_T/k の任意の自己同型とし $\sigma\zeta=\zeta^m$, $\sigma\pi=\pi'$ とおくと $k_T(\sqrt[e]{\pi'})=k_T(\sqrt[e]{\pi})$ 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 $\sqrt[e]{\pi'}$ の一つとして $(\sqrt[e]{\pi})^l a$ をとり、σ の K への延長 $\tilde{\sigma}:\sqrt[e]{\pi}\to\sqrt[e]{\pi'}$ をとると、K/k_T の自己同型 $\tau:\sqrt[e]{\pi}\to\zeta\sqrt[e]{\pi}$ に対して $\tilde{\sigma}\tau(\sqrt[e]{\pi})=\zeta^m\sqrt[e]{\pi'}$, $\tau\tilde{\sigma}(\sqrt[e]{\pi})=\zeta^l\sqrt[e]{\pi'}$; 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 $k=Q(t)_p$, K: k 上の n 次アーベル拡大とすると $K=k_T(\sqrt[e]{\pi})$, 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 も 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 $K_1=k_T(\sqrt[e]{\pi_0})$ と $K_2=k(\sqrt[e]{p})$ の合成に含まれる。然るに K_1/k, K_2/k は各々不分岐ないし完全拡大であり、$\zeta\in k$ 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　そこで $Q(t)_p$ 上の p べき次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。ただ 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 $k=Q(t)_p$, $k'=k(\zeta)$ 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。

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash, bend right, "p"'] & K'=K(\zeta) \arrow[d, dash] \\
Q(t)_p = k \arrow[r, dash] \arrow[r, dash, bend right, "p-1"'] & k'=k(\zeta)
\end{tikzcd}$$

従って問題は $K'=k'(\sqrt[p]{x})$ （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 $Q_p(\zeta)=Q_p(\pi)$, $\pi=\sqrt[p-1]{-p}$ 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 $K'=k'(\sqrt[p]{x})$ がk上アーベル拡大とするとxに適当なk'のp乗元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 はじめから $x\equiv 1 \pmod{\pi}$ 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 $\bmod\ \pi^{p+1}$ でのみ与えられればよい。まず、

<u>定理2</u>　$x\in k'$, $x\equiv 1 \pmod{\pi}$ とする。K'/k がアーベル拡大で且つ K/k が不分岐[1]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 $x\equiv 1+b\pi^p \pmod{\pi^{p+1}}$ とおくと K/k の剰余拡大は方程式 $X^p-X=\bar{b}$ による($\bar{k}$の) Artin-Schreier 拡大である。ただし $\bar{b}$ は剰余類 $b \pmod{\pi}$ 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 $\mathrm{mod}\ \pi^p$ でのみ考えればよい事がわかった。さて我々の結果は

<u>定理3</u>　$x\in k'$、$x\equiv 1 \pmod{\pi}$ 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 $\longleftrightarrow$ K'/k'：不分岐 である(K'/k：アーベル等により)
註2　$p\sim\pi^{p-1}$ に注意

(証略)

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。$k=Q(t)_p$ 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 mod p の各類を変えないも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 mod p で t の1次関数であればよい。又 $\sigma \in G_1 \longleftrightarrow t_1 \equiv t \pmod{p}$。(例えば $t \to t+p$ 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(その剰余拡大がつぶれても)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 K_a/k が G_1-normal なる為の必要十分条件は a が 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変数代数関数体 F に対して、F の素因子の集合(ただし有限個の例外素因子を

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生じる。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、$Q_p^\times$（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 がそ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 ζ の分子を $(1-\alpha u)(1-\alpha' u)$（$\alpha\alpha' = q$）とおく。そのとき α'/α は $Q_p^\times$ 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 $Q_p^\times$ 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 $\mathrm{ord}_p \pi_j = d_j$ 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（本質的なのは 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 をノルムの群とするような 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。それを K_j とする。K_j は Q_p の d_j 次不分岐拡大 $Q_p^{(d_j)}$ を含み $K_j/Q_p^{(d_j)}$ は巡回拡大、完全分岐でガロア群は Q_p の p 進単数群 U_p と同型である。従って $j \to K_j$ なる対応を説明する事が問題となる。ところでこれに関し次の事がいえるのである。$Q(t)_p$ 上の無限次巡回拡大 K で、完全分岐，$K/Q(t)_p$ のガロア群は U_p と同型なるものが存在し、次の性質を満す．各 $j \in \hat{F}_p$ ($\neq 0, 1$, supersingular) に対して　その F_p 上の共役元全体を $j = j_1, \cdots,$ j_d ($d = d_j$) とおき、$Q_p^{(d_j)}$ の元 $\tilde{j}_1, \cdots, \tilde{j}_d$ を $\tilde{j}_i \pmod{p} = j_i$ ($i = 1, \cdots, d$) なるようにとる．そのとき K の「$t \to \tilde{j}_i$ 上の specialization」$K_{\tilde{j}_i}$ が定義され $K_{\tilde{j}_1}, \cdots, K_{\tilde{j}_d}$ を「平均」したものとして K_j を得るのである．即ち関数 $j \to K_j$ は $Q(t)_p$ 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れれば　関数 $j \to K_j$ 従って関数 $j \to \pi_j$ の数論的説明（楕円曲線をはなれた）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 (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 $Q(t)_p$ の初等的な拡大なのである．ただ同様の問題から生ずる他の 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。