数理解析研究所講究録
第 409 巻 1980 年 61-71

$\Pi+\Pi'$の持上げとその応用

東大・理　伊原康隆

C: 有限体 $\mathbb{F}_q$ 上の代数曲線で完備非特異絶対既約, 種数 g.

$\Pi, \Pi' \subset C\times C$:　Cのq乗写像のグラフ　とその転置(transpose),

$\Pi+\Pi'$ は C上の因子とみる.

問題　対$(C, \Pi+\Pi')$の標数0への持上げを考えること.

動機　(i) モジュラー関数との関係(とくに志村曲線), (ii) C の不分岐な。ア被覆の整数論との関係.

(i)についてはここでは触れない(cf.[1])。(ii)については これから述べる.　$g\leq 1$ のときは, 和$\Pi+\Pi'$ をとらなくても, (C, Π) (C, Π') 各々が標数0への持上げを有し, とくにCが ordinary elliptic curve のときそれらは本質的に一意的で Cのいわゆる canonical lifting を与えている(Deuring).　我々が主に考えるのは $g\geq 2$ のときで, このとき(C, Π)等は個々には標数0にあがらず, $(C, \Pi+\Pi')$を考えて初めて持上る場合が生ずるのである。

まず持上げの正確な定義から.　一般にAを $\mathbb{F}_q$ を剰余体とする局所環とするとき,

定義　三対 $(\mathcal{C}, \mathcal{C}'; \mathcal{J})$ が $(C, C; \Pi + \Pi')$ の A 上への持上げとは，$\mathcal{C}, \mathcal{C}'$：$A$ 上の proper smooth schemes で $\mathcal{C} \otimes_A \mathbb{F}_q = \mathcal{C}' \otimes_A \mathbb{F}_q = C$，　$\mathcal{J}$：$\mathcal{C} \times_A \mathcal{C}'$ の A 平坦かつ既約な閉部分 scheme で $\mathcal{J} \otimes_A \mathbb{F}_q = \Pi + \Pi'$ （$C \times C$ の中で）。

$g \geq 2$ のとき $\mathcal{J}$ の既約性は自動的に出る．$\mathcal{C}' = \mathcal{C}$，${}^t\mathcal{J} = \mathcal{J}$ のとき，$(\mathcal{C}, \mathcal{J})$ は $(C, \Pi + \Pi')$ の対称な持上げと呼ぶ．

与えられた C, A に対して $(\mathcal{C}, \mathcal{C}'; \mathcal{J})$ が存在するとは限らない．（存在の問題については後に述べる．）ここではまず A を標数 0 の離散付値環とし，A 上への持上げ $(\mathcal{C}, \mathcal{C}'; \mathcal{J})$ が存在したと仮定してその帰結について論じる．A から複素数体 $\mathbb{C}$ の中への埋めこみ $\varepsilon: A \to \mathbb{C}$ を一つ選び，$\mathcal{C}, \mathcal{C}'; \mathcal{J}$ 各々を複素化して得られる $\mathbb{C}$ 上の代数曲線の三対

$$(\mathcal{C}, \mathcal{C}'; \mathcal{J}) \otimes_A \mathbb{C} = (\mathcal{R}, \mathcal{R}'; \overline{\mathcal{R}}_0) \qquad \overline{\mathcal{R}}_0 \subset \mathcal{R} \times \mathcal{R}'$$

を考える．$\mathcal{R}, \mathcal{R}'$ を（種数 g の）コンパクト・リーマン面とみよう．$\Pi + \Pi'$ の特異点の集合は明らかに $\Pi \cap \Pi'$ で，$\Pi \cap \Pi'$ の各点は $\Pi + \Pi'$ の通常二重点であり，また第一射影 $\Pi \xrightarrow{\sim} C$ によって $\Pi \cap \Pi'$ は C の $\mathbb{F}_{q^2}$－有理点の集合と1対1に対応することに注意する．Reduction $\otimes_A \mathbb{F}_q$ を通して $\overline{\mathcal{R}}_0$ の特異点集合 $\mathrm{Sing}(\overline{\mathcal{R}}_0)$ と $\Pi \cap \Pi'$ を比べることにより，容易に次のことがわかる．

$\overline{\mathcal{R}}_0$ の特異点はすべて通常二重点で，$\otimes_A \mathbb{F}_q$ によって $\Pi \cap \Pi'$ の部分集合，従って C の $\mathbb{F}_{q^2}$ 有理点の集合のある部分集合と1対1

に対応する。 $\mathrm{Sing}(\overline{\mathcal{R}_0})$ と対応しない C の $\mathbb{F}_{q^2}$ 有理点を(この持ち上げに属する) 特殊素点 (special points) と呼ぶ。一方, $\overline{\mathcal{R}_0}$ を正規化して得られる閉リーマン面を $\mathcal{R}_0$ と書き,

(1)
$$\begin{tikzcd}[column sep=small] & \mathcal{R}_0 \arrow[dl, "\varphi"'] \arrow[dr, "\varphi'"] & \\ \mathcal{R} & & \mathcal{R}' \end{tikzcd}$$

を $\overline{\mathcal{R}_0}$ の射影から生ずる有限被覆写像(一般には分岐する)とする。$\mathcal{R}_0$ の任意の点 P_0 をとり, P_0, $P=\varphi(P_0)$, $P'=\varphi'(P_0)$ を基点とする $\mathcal{R}_0, \mathcal{R}, \mathcal{R}'$ の基本群をそれぞれ $\pi_1(\mathcal{R}_0), \pi_1(\mathcal{R}), \pi_1(\mathcal{R}')$, φ, φ' の誘導する基本群間の準同型(単射とは限らない)を

(2)
$$\begin{tikzcd}[column sep=small] & \pi_1(\mathcal{R}_0) \arrow[dl, "\Phi"'] \arrow[dr, "\Phi'"] & \\ \pi_1(\mathcal{R}) & & \pi_1(\mathcal{R}') \end{tikzcd}$$

と書く。Γ を, Φ, Φ' で定まる融合部分群つき自由積とする。

(3)
$$\Gamma = \pi_1(\mathcal{R}) \underset{\pi_1(\mathcal{R}_0)}{*} \pi_1(\mathcal{R}').$$

Γ の構造は, A, $(e, e'; J)$, $\varepsilon: A \hookrightarrow \mathbb{C}$ 等のとり方には依存するが, $P_0 \in \mathcal{R}_0$ のとり方には依存しない。

定理1 $K = \mathbb{F}_{q^2}(C)$ を C の $\mathbb{F}_{q^2}$ 上の関数体とし, M/K は C のすべての特殊素点が完全分解するような K の不分岐ガロア拡大のうち最大のものとすると, M/K の Galois 群は Γ の profinite completion と同型である. $\mathrm{Gal}(M/K) \cong \Gamma$.

これは，φ, φ' が不分岐の場合に得られていた以前の結果([1] §4) の拡張である。この定理を Grothendieck の比較定理([2] Exp X) と比べると，Grothendieck に於ては C の持上げと(のみ)を用いて K の最大不分岐ガロア拡大 L の $\overline{\mathbb{F}}_q\cdot K$ 上の Galois 群 $Gal(L/\overline{\mathbb{F}}_q\cdot K)$ と $\overline{\pi_1(R)}$ を比較しているが，これは p と素な部分の同型を引起す全射準同型 $\overline{\pi_1(R)}\to Gal(L/\overline{\mathbb{F}}_q\cdot K)$ の存在を保証するものの，この二つの群はそれ自体として同型でないから，完全な比較定理ではない。(その代わり $\pi_1(R)$ の構造はよく知られている)。一方我々の結果は同型定理になっているが，$\overline{\Gamma}$ の計算は容易でない。 また，不分岐拡大の中で，与えられた有限個の素点が完全分解するところだけに制限するのも，代数体の不分岐拡大に於ては無限素点が常に"完全分解"している事にかんがみると，むしろ自然な制限ではなかろうか。

さて，特殊素点の個数を H とおくと：

<u>命題</u> (i) $H \geq (q-1)(g-1)$ であり，等号が成立する為の必要十分条件は φ, φ' が共に不分岐なること

(ii) $H = (q-1)(g-1)$ のとき，$\Gamma, \overline{\Gamma}$ は共に無限群，従って M/K は無限次拡大になる。

(iii) $H > (q-1)(g-1)$ のとき，Φ, Φ' は全射で

(4) $$\Gamma \cong \pi_1(\mathcal{R}) / (\mathrm{Ker}\,\Phi)(\mathrm{Ker}\,\Phi') .$$

予想　$H > (q-1)(g-1)$ のとき Γ は有限，従って M/K は有限次拡大？

より一般に，三つの閉リーマン面と有限被覆写像の系 (1) に対して，φ, φ' がある意味で"独立"（例えば $\mathcal{R}, \mathcal{R}'$ の関数体の $\mathcal{R}_0$ への引戻しの共通部分は定数体 $\mathbb{C}$ しかない，等）で Φ, Φ' が全射なら Γ は有限であろうか？

$(\varphi, \varphi'; J)$ が，$PSL_2(\mathbb{R}) \times PGL_2(F_{\mathfrak{p}})$（$\mathbb{R}$：実数体，$F_{\mathfrak{p}}$：$\mathfrak{p}$進体 $N\mathfrak{p}=q$）の格子部分群 $\tilde{\Gamma}$ に対応する志村曲線の合同関係式 (cf. [1] p6) の場合は，上記予想は正しい．この場合，$\tilde{\Gamma}$ は Margulis により arithmetic となり，E を $\tilde{\Gamma}$ の parabolic 及び torsion elements で生成される正規部分群とすると，$\Gamma \cong \tilde{\Gamma}/E$ となり，更に，$H > (q-1)(g-1)$ となるための必要十分条件は $E \neq \{1\}$. この場合 E は $\tilde{\Gamma}$ の中心には含まれないから，再び Margulis によって $\Gamma \cong \tilde{\Gamma}/E$ は有限群になるのである。尚，$H = (q-1)(g-1)$ を満す三対 $(\varphi, \varphi'; J)$ はすべて $PSL_2(\mathbb{R}) \times PGL_2(F_{\mathfrak{p}})$ の格子部分群 $\tilde{\Gamma}$ と対応する（従って $\Gamma \cong \tilde{\Gamma}$）ことも予想されるが $H > (q-1)(g-1)$ のときは，少くとも $g=0$ では，反例がある。

定理の証明のポイントは，Grothendieck の比較定理の証明における Abhyankar's lemma の代わりに次のレンマを用いるところにある。

補助定理（三木-伊原 [3]） $\mathfrak{K} \supset \mathbb{Q}_p$ を，p 進体 $\mathbb{Q}_p$ を含み p 進付値の延長によって完備な離散付値体で $\mathbb{Q}_p$ 上代数的な素元を含むものとする（例えば 有理関数体 $\mathbb{Q}_p(x_1,\cdots,x_n)$ の自然な p 進付値による完備化）。 $\mathfrak{M}/\mathfrak{K}$ を有限次拡大とする。もし，$\mathfrak{K}$ から $\mathfrak{K}$ の中への付値体としての同型写像 $\sigma:\mathfrak{K}\hookrightarrow\mathfrak{K}$ が存在して剰余体の p^n 乗写像 $(n>0)$ を引起し，しかも $\mathfrak{M}$ から $\mathfrak{M}$ の中への同型写像 $\tilde{\sigma}:\mathfrak{M}\hookrightarrow\mathfrak{M}$ で $\mathfrak{M}^{\tilde{\sigma}}\cdot\mathfrak{K}=\mathfrak{M}$ を満すもの $\tilde{\sigma}$ への延長を許すなら，$\mathbb{Q}_p$ の有限次拡大 $\mathbb{Q}_p'$ が存在して $\mathfrak{M}\cdot\mathbb{Q}_p'/\mathfrak{K}\cdot\mathbb{Q}_p'$ は不分岐となる。

尚，定理を現在の形に一般化するに際しては，Γ を φ と φ' の mapping cylinders の自然な融合和の基本群と見ることが基本的役割を果した。この事を示唆して下さったトポロジーの森田茂之氏に感謝の意を表したい。

次に $g \geq 2$ とし，対 $(C, \Pi + \Pi')$ の対称な持上げについて論ずる。C の $\mathbb{F}_{q^2}$ 有理点からなる（ある）集合 $\mathfrak{S}$ で，$\mathbb{F}_{q^2}/\mathbb{F}_q$ の共役で全体として変わらないものを一つとって固定し，(C, J) としてはその special points の集合が与えられた $\mathfrak{S}$ に含まれるようなもののみを考える。$\mathfrak{S}$ に含まれる $\mathbb{F}_q$ 上1次ないし2次の点の集合を各々 $\mathfrak{S}_1, \mathfrak{S}_2$ と記し，$\mathfrak{S}_2$ における $\mathbb{F}_q$ 共役類を $\sim$ で表わす。$|\mathfrak{S}_1| = H_1$, $|\mathfrak{S}_2| = 2H_2$ （従って $|\mathfrak{S}| = H_1 + 2H_2$）と記す。

$C, \mathfrak{S}$ に対して定まる二つの不変量 $m, r \in \mathbb{Z}, \geq 0$ を定義する。

$$U = \left\{ \xi \;\middle|\; \begin{array}{l} \xi : C \text{ 上の } q+1 \text{ 重正則微分で，} \xi = \xi_1 \otimes \xi_2^{\otimes q} \text{ と分解} \\ \text{するとき } \gamma^f(\xi_1) = 0 \end{array} \right\}$$

（ただし γ は Cartier 作用素, $q = p^f$, p: 素数）とおくと，U は $\mathbb{F}_q$ 上 $2(q-1)(g-1)$ 次元のベクトル空間である。各 $Q \in \mathfrak{S}$ に対して Q における局所一意化変数 t_Q （C 上の関数）を選び，各 $\xi \in U$ に対して C 上の関数 $\xi/(dt_Q)^{\otimes(q+1)}$ が Q でとる値を $\left(\xi/(dt_Q)^{\otimes(q+1)}\right)_Q$，その Q の剰余体 k_Q （$= \mathbb{F}_q$ または $\mathbb{F}_{q^2}$）から $\mathbb{F}_q$ への trace を $\mathrm{tr}_{k_Q/\mathbb{F}_q}\left(\xi/(dt_Q)^{\otimes(q+1)}\right)_Q$ で表わし，U から $\mathbb{F}_q^{H_1+H_2}$ の中への $\mathbb{F}_q$ 線型写像

$$\lambda : U \ni \xi \longrightarrow \left(\mathrm{tr}_{k_Q/\mathbb{F}_q}\left(\xi/(dt_Q)^{\otimes(q+1)}\right)_Q\right)_{Q \in \mathfrak{S}_1 \sqcup (\mathfrak{S}_2/\sim)} \in \mathbb{F}_q^{H_1+H_2}$$

を考える。（Q は $\mathfrak{S}_1 \sqcup (\mathfrak{S}_2/\sim)$ の上を動く）。t_Q のとり方を変えて

も，λ は $\mathbb{F}_q^{H_1+H_2}$ の自己同型による変換しか受けないから，

(5) $\qquad m = \dim_{\mathbb{F}_q}(\mathrm{Coker}\,\lambda), \qquad r = \dim_{\mathbb{F}_q}(\mathrm{Ker}\,\lambda)$

はともに C, σ のみで定まる不変量で明らかに

(6) $\qquad m - r = H_1 + H_2 - 2(g-1)(q-1).$

さて $\mathbb{F}_q$ を剰余体とする完備なネーター的局所 $W(\mathbb{F}_q)$ 環全体のなす圏 $\mathcal{A}$ を考える（$W(\mathbb{F}_q)$ は $\mathbb{F}_q$ 上の Witt vectors のなす環）．圏 $\mathcal{A}$ の対象 A に対して $(C, \Pi+\Pi')$ の A 上への対称な持上げ $(\mathcal{C}, \mathcal{T})$ の A 同型類全体のつくる集合を対応させる関手 $f: \mathcal{A} \to \{\mathrm{Sets}\}$ を考えると

定理2 関手 f は，ある $A^* \in \mathcal{A}$，$(\mathcal{C}^*, \mathcal{T}^*) \in f(A^*)$ によって表現可能で，A^* は上記 m, r を用いて次のように表される．

$$A^* = W(\mathbb{F}_q)[[t_1, \cdots, t_m]]/(F_1, \cdots, F_r),$$

$F_i \in (\mathfrak{m}^2, p)$ $(i=1, \cdots, r)$． ここに $\mathfrak{m}$ は $W(\mathbb{F}_q)[[t_1, \cdots, t_m]]$ の極大イデャル．（F_i たちは互いに"独立"とは限らない．すべて 0 になることもある．）

系1 $r=0$ なら $(C, \Pi+\Pi')$ は任意の $A \in \mathcal{A}$ の上に（例えば $A = W(\mathbb{F}_q)$）持上がる。更に $m=0$ ならそれは一意的．

例えば $q=g=2$ のとき，同型を除いて C は 20ケ存在するが，G を C のすべての $\mathbb{F}_{q^2}$ 有理点の集合にとるとき，そのうち 13ケの C に対して上記系の仮定 $r=0$ が満されており従って $(C, \Pi+\Pi')$ は標数 0 に（対称に）持上がる。

しかし $r=0$ が成立つのは (6) によって $H_1+H_2 \geq 2(q-1)(g-1)$ の場合に限られており，重要な場合 $|G|=(q-1)(g-1)$ などは含まれない。そこで，この場合には C の自己同型群を有効に用いる事も試みられている（伴原[4]）. [4]に於て $|G|=(q-1)(g-1)$ の場合にも標数 0 に持上げられるための criterion と実例がいくつか計算されている。

Spec A^* は $(C, \Pi+\Pi')$ の（対称な）局所的変形の moduli space と見なせるが，実例として例えば次のような環が（各々特定の p に対して）A^* として出てくる。

$$A^* = \mathbb{Z}_p[[t_1, t_2, t_3, t_4]], \quad \mathbb{Z}_p, \quad \mathbb{Z}_p/(p^2),$$
$$\mathbb{F}_p[[t_1, t_2, t_3]].$$
（吉村曲線の方から，多分，$\mathbb{Z}_p[\sqrt{p}]$ なども出てくる）

<u>系 2</u>　$H_1+H_2 \geq 2(q-1)(g-1)$ <u>なら</u>，$(C, \Pi+\Pi')$ <u>は標数 0 への対称な持上げを有するか，または $\mathbb{F}_q[[t]]$ 上への自明でない変形をもつ。</u>

尚 $(C, \Pi+\Pi')$ の持上げは，ある種の p 進的微分対と1対1に対応することもわかっている([7])が，この理論は今のところ，持上がるための必要条件を出すことと，最初の二段階の infinitesimal liftings ($A = \mathbb{Z}/p^2$, $\mathbb{Z}/p^3$ 上への持上げ)をすべて求める事などには役に立つが標数0に迄上がるための簡単な十分条件は与えないので，ここでは省略した。

最後になったが，古川吉弘氏の修士論文(東大. 1980)で，$g=2$ の場合の持上げの問題がやはり自己同型を有効に用いて扱われていて[4]にはない十分条件が得られていること，及び堀川氏が $g=2$ の場合 Kummer surface を用いた議論をされた事(未出版)を付記したい。

[1] Y. Ihara Congruence relations and Shimura curves I (AMS Proc Symp. Pure Math 33 Vol 2), II (J. Fac. Sci. Univ. Tokyo, IA 25-3 (1979))

[2] A. Grothendieck Revêtements étales et groupe fondamental (SGA 1) Springer Lecture Notes 224 (1971)

[3] Y. Ihara - H. Miki Criteria related to potential unramifiedness and reduction of unramified coverings of curves J. Fac. Sci. Univ Tokyo IA 22 (1975)

[4] Y. Ihara Lifting curves together with the characteristic correspondence $\Pi + \Pi'$. (to appear)

[5] 〃 Congruence relations and fundamental groups (to appear)

[6] Y. Furukawa 修士論文 (東大・理・1980).

[7] Y. Ihara On the Frobenius correspondences of algebraic curves, Proc. Intern. Symp. on Alg. number theory, Kyoto (1976) "Algebraic Number Theory" Japan Soc. Prom. Sci.