塔構造、分解素点、ゼータ函数

－「奇」の発見を原点とした整数論発展史に則ってー

Towered arithmetic structures, splitting primes and ζ-functions

—following history of number theory promoted by curiosity for 'odd' structures—

伊原康隆（Yasutaka Ihara）

第２回日本数学会賞小平邦彦賞講演会 9/16/2023

[Pre]

整数論の長い歴史、ふり返ると：

(1) 具体的対象への好奇心，工夫された数値計算（＋偶然） ⇒ 未知の構造（特異な）が発見され、

(2) （それを）パラメーターつきに一般化、奥なる函数の問題と捉える ⇒ 理論の構築

（たとえば）

ゼータ函数，楕円函数，モジュラー函数，……，岩澤理論，谷山理論，志村理論，

ところが、ここ四、五十年間 目立っているのは、（すばらしすぎる）否定的一般論の数々：

「そういう解は有限個しかない、全くない，この範囲にしかない」

「よい性質をもつ不連続群なり格子なりは既知のものに限られる」

「よい○○は、△△から生じるものだけだろう（未解決PQ予想）」

そろそろ期待したい、「時代の舵の切換わり」を：

「予想された結果の証明法の工夫」 → 「予期できなかった新構造の探索」

A1 ★★★

素数(Prime number)

[整数 $p \geqq 2$ で, $1 < * < p$ なる整数 $*$ で われないもののこと]

$p = 2, 3, 5, 7, 11, 13, 17, \cdots\cdots$ (100以下で25個), $\cdots\cdots\cdots$

素数は無限個あり, 大きな整数 x が素数である確率は $1/\log x$

[素因子分解の一意性] 整数 $\neq 0, \pm 1$ は、$\pm p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ ($p_1 < p_2 < \cdots$ は素数, $a_1, a_2, \cdots \geq 1$) の形に 唯一通りに 分解される。

(数論屋のひと言) $2\times2\times5 \neq 3\times7$ は、かけ算しなくても分かるよ (むしろ、わり算)

(解析的表現) 一斉に s 乗 $(s>1)$ して

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p:\text{素数}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}$$

$1 + \frac{1}{2^s} + \cdots + \frac{1}{20^s} + \frac{1}{21^s} + \cdots$

$\left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \cdots\right)\left(1 + \frac{1}{3^s} + \cdots\right)\left(1 + \frac{1}{5^s} + \cdots\right)\left(1 + \frac{1}{7^s} + \cdots\right)\left(1 + \frac{1}{11^s} + \cdots\right)$

Euler積分解

A2** リーマンのゼータ函数

$$\zeta(s)=\underset{(イ)}{\sum_{n=1}^{\infty}\frac{1}{n^s}}=\underset{(ロ)}{\prod_{p:\text{素数}}\left(1-\frac{1}{p^s}\right)^{-1}}\qquad (s>1)$$

[(イ)の帰結]

$$\zeta^*(s)=\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\int_0^{\infty}\left(\sum_{n=1}^{\infty}e^{-n^2\pi x}\right)x^{\frac{s}{2}-1}dx$$

ここで $\vartheta(\tau)=\sum_{n=-\infty}^{\infty}e^{n^2\pi\tau i}$ ($\mathrm{Im}(\tau)>0$ で急速に収束!) は

変換公式 $\vartheta(\tau+2)=\vartheta(\tau),\quad \vartheta\left(\frac{-1}{\tau}\right)=\sqrt{-i\tau}\,\vartheta(\tau)$ を満す

$\Longrightarrow$ $\zeta^*(s)$ は $\mathbb{C}$ 上の解析函数に解析接続され、

函数等式 $\zeta^*(1-s)=\zeta^*(s)$ を満す.

[(ロ)の帰結]

$$\frac{\zeta'(s)}{\zeta(s)}=(-s)\int_1^{\infty}\left(\sum_{p^m\le x}{}'\log p\right)x^{-s-1}dx\cdots(\mathrm{Re}(s)>1)$$

"主要項" $\frac{1}{1-s}$ ←----------→ x

"振動項" $\sum_{\rho;\,\zeta^*(\rho)=0}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)$ ←----------→ 評価の標的

Riemann予想 (1859) $\mathrm{Re}(\rho)=1/2$? "Es ist sehr wahrscheinlich daß..."

◎ 代数体の塔で $\frac{\zeta'(s)}{\zeta(s)}$ の類似物の limit を考える ⇝ 振動項が"主要項"に

後述

A3 ：　$\{p\ ;\ \zeta^*(p)=0\}$ $\longleftrightarrow$ $\{p^m\ ;\ p:$素数, $m=1,2,\cdots\cdots\}$ (重さ $1/m$)

↑ このイミを知りたい から　　↑ この集合の「オニの」構造を探りたい

「素数べきだけに対して自然に定まるものは?」

そう,「ガロア群のフロベニウス共役類」.

(ガロア群)　方程式　$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0$　($a_i\in\mathbb{Z}$, 重根なし)

まず　複素数の範囲では、

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\qquad(\alpha_i\neq\alpha_j \text{ for } i\neq j)$$

このガロア群とは、n 個の根 $\alpha_1,\cdots,\alpha_n$ (の添字) の置換のうちで、

「根の間の(有理数係数多項式による)いかなる関係式も壊さないもの

全体」がつくる群 G　(n次対称群 S_n の部分群)

根の間に非対称な関係があると　$G\subsetneq S_n$.

(たとえば　$f(-x)=f(x)$ とか、$x^nf(1/x)=f(x)$　のとき

$\alpha_{n-i}=-\alpha_i$,　$\alpha_{n-i}=\alpha_i^{-1}$, ととれるから, これらペアを壊す置換 $\notin G$.)

A4 有限体

有限集合に加減乗と $\neq 0$ なる元による商が定義されたもの.

$\Rightarrow$ 元の個数 $q = p^m$ (p:素数, $m \geq 1$) で, その構造は q のみで定まる. $\mathbb{F}_q$ と記される.

(e.g. $\mathbb{F}_2 = \{0, 1\}$; $1+1=0$; $\mathbb{F}_4 = \{a+b\omega;\ a, b \in \mathbb{F}_2,\ \omega^2 = \omega + 1\}$)

p: 素数 なら $\mathbb{F}_p = \mathbb{Z}/p$ (整数を mod p で類別したときの類の集合)

[$\mathbb{F}_q$ の特徴] $p = 0$; $\mathbb{F}_q \ni \alpha \to \alpha^p \in \mathbb{F}_q$ は自己同型 ($(\alpha+\beta)^p = \alpha^p + \beta^p$).

[フロベニウス共役類] 前述 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ をその判別式 $d_f = \prod_{i<j} (\alpha_i - \alpha_j)^2$ ($\in \mathbb{Z}, \neq 0$) を割らない各素数 p に対して定まるこのガロア群 G の共役類。

a_i を $a_i^* = a_i \pmod p \in \mathbb{F}_p$ に代えて得られる $\mathbb{F}_p$ 上の多項式 $f^*(x)$ は、ある $\mathbb{F}_q$ ($q = p^m$) で

$$f^*(x) = (x - \alpha_1^*) \cdots (x - \alpha_n^*) \qquad (\alpha_1^*, \ldots, \alpha_n^* \in \mathbb{F}_q,\ \alpha_i^* \neq \alpha_j^* \text{ if } i \neq j)$$
$$= (x - \alpha_1^{*p}) \cdots (x - \alpha_n^{*p})$$

と分解し, 置換 $\alpha_i^* \to \alpha_i^{*p}$ は元の $f(x) = 0$ のガロア置換をほぼ定める.

その共役類をきちんと

($a_i^{*p} = a_i^*$ より、$f^*(x)^p = f^*(x^p)$ が成立つことに注意)

A5

(例) $f(x) = x^4 + x + 1$

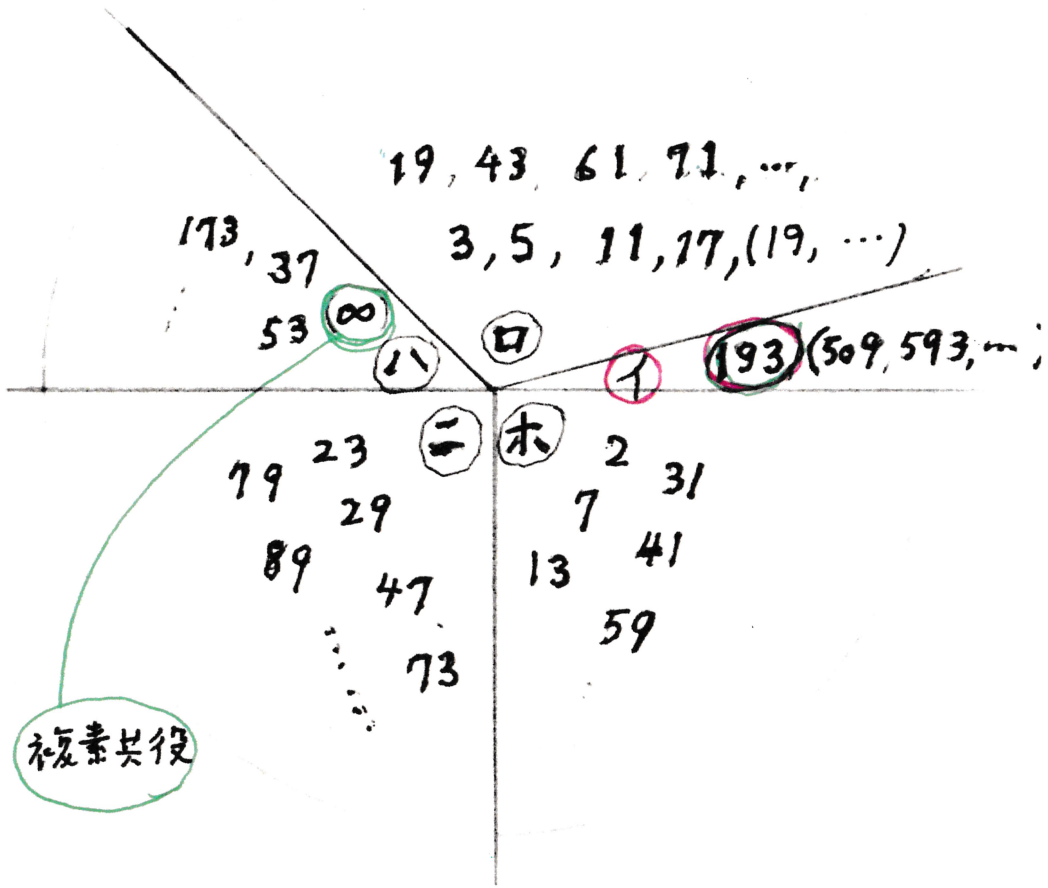
$G = S_4$ (4文字の置換すべて)

$d_f = 229$ (素数)

(ただし $f(x)=0$ の根はすべて虚根)

群Gの共役類		元の個数	$f(x)$ mod p の既約因子の次数
イ	(1)(2)(3)(4)	1	1+1+1+1
ロ	(1)(234)	8	1+3
ハ	(12)(34)	3	2+2
ニ	(1)(2)(34)	6	1+1+2
ホ	(1234)	6	4
	計	24	

pキ229のフロベニウス共役類



イ 補足 $f(x) \equiv (x-42)(x-45)(x-48)(x-58) \bmod 193$ など

Gの商群でより荒い分類

イ+ロ+ハ $\Longleftrightarrow$ $x^2 - 229 \pmod p$ が分解 $\Longleftrightarrow$ $229 \pmod p$ が平方数

イ+ハ $\Longleftrightarrow$ $x^3 - 4x + 1 \pmod p$ が分解

A6

より一般に数論的な体 k の素因子の集合を $\mathrm{Primes}(k)$ とかくと、k 上の有限次ガロア拡大 K をとるごとに全射

共役類の集合

$$\mathrm{Primes}(k) \supset \{K\text{に依存する有限個}\} \xrightarrow{\text{フロベニウス射}} \mathrm{Conj.Classes\ of\ Gal}(K/k)$$

が $\mathrm{Primes}(k)$ を 分類している

k を固定し、K/k の塔を 無限に高く 延ばす中に、「これぞ」という 希少構造をもつ「素因子ー共役類 表示塔」は ないのだろうか？
（$\mathbb{F}_q$ 上の 函数体では あったように …後述）

塔が 満たすべき 明らかな 必要条件：

* K/k で 分岐する k の素因子は 限定的（不分岐など）
* アーベル拡大 部分が 少ないこと … 素数の中と一般合成数の区別を要す.
* $\mathrm{Gal}(K/k)$ も Conj… も、可算無限な 群厂 の それで 代表されること
* $\mathrm{Gal}(K/k)$ の 表現次数ごとに 切る 話とは、[×] で 重心が 変わる.

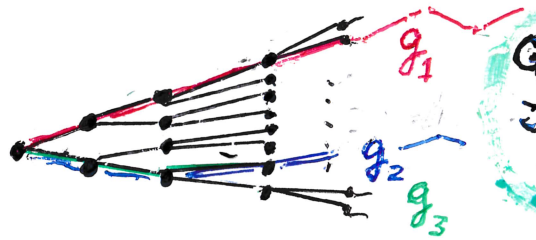
B1 表示塔を求めて

k：有限次代数体、　$\mathcal{O}_k$：その整数環　（of kernel）

kの素点（prime, 記号 $\mathfrak{P}$）
- 有限素点：$\mathcal{O}_k \twoheadrightarrow \mathbb{F}_q$　　$N(\mathfrak{P}) \underset{\text{def}}{=} q$
- 無限素点：$k \hookrightarrow \mathbb{R}$, $k \hookrightarrow \mathbb{C}$
  - $k \hookrightarrow \mathbb{R}$：実素点
  - $k \hookrightarrow \mathbb{C}$：虚素点 $\sim$ up to complex conjug.

K/k ：（とりあえず）不分岐な 無限次ガロア拡大

$G = G_{K/k}$ ：ガロア群（コンパクト, 完全非連結）



Gの各元はこういう無限列

フロベニウス射：
$$\mathrm{Primes}(k) \ni \mathfrak{P} \overset{\text{we}}{\longrightarrow} \left(\frac{K/k}{\mathfrak{P}}\right) \in \mathrm{ConjugacyClasses\ of}\ G_{K/k}$$

集合濃度 $\aleph_0$　　image is dense　　集合濃度 $\aleph$

$\mathfrak{P}$ が K/k で完全分解 $\underset{\text{def}}{\Longleftrightarrow}$ $\left(\frac{K/k}{\mathfrak{P}}\right) = \{1\}$

// 準完全分解 $\underset{\text{def}}{\Longleftrightarrow}$ $\left(\frac{K/k}{\mathfrak{P}}\right)^f = \{1\}$　　$(1 \le {}^{\exists} f < \infty)$; $f_{\mathfrak{P}} \underset{\text{def}}{=} \mathrm{Min}(f)$

◎ 無限素点は完全分解（不分岐でなくても、$f_{\mathfrak{P}} \le 2$ の準完全分解）

B2　K/k で準完全分解する k の素点 $\mathfrak{P}$ の集合を S とおくと、

一般リーマン予想 GRH（後述）の仮定のもとで

Th.1 (Y-I; 1983)　$\displaystyle\sum_{\mathfrak{P}\in S} \alpha_{\mathfrak{P}} \leqq \log\sqrt{|d_k|}$　(under GRH)

（d_k：k の判別式）

ただし、$\alpha_{\mathfrak{P}} = \frac{1}{2}(\log 8\pi + \gamma) + \frac{\pi}{4}$ (resp. $\log 8\pi + \gamma$) … $\mathfrak{P}$：実 (resp. 虚)

$\alpha_{\mathfrak{P}} = (N(\mathfrak{P})^{f_{\mathfrak{P}}/2} - 1)^{-1} \log N(\mathfrak{P})$ …… $\mathfrak{P}$：有限素点

（γ：Euler 定数 $(|\Gamma'(1)| = 0.57721\ldots)$）

実は、右辺−左辺 $= -\dfrac{\zeta_{k,S}'(1/2)}{\zeta_{k,S}(1/2)}$；

"S-modified $\zeta_k(s)$" at $s = 1/2$.

$\zeta_k(s) \times \prod_{\mathfrak{P}\in S,\ \text{有限}} (1 - N(\mathfrak{P})^{-f_{\mathfrak{P}}s})^{1/f_{\mathfrak{P}}} \times (s-\frac{1}{2})^{2m}$

ここで、2つの可能性（互いに逆方向）のそれぞれに近寄ってみよう……

GRH に反例 ??
（基本的）

Th 1 で 等式成立の場合は ??
（素因子−共役類表示塔の候補として）

B3

GRH = デデキント $\zeta_k(s)$ の"リーマン予想"

「一般には不成立かもしれない」と一応疑うべきだし、調べる試金石として

Th 1 は、わるくない …(定年頃におすすめ)

$$\text{もし、}\quad \frac{1}{2}\log|d_k| < (2.6861\cdots)r_1 + (3.8014\cdots)r_2$$

(k の実素点, 虚素点, の個数)

!

なる k で無限次不分岐ガロア拡大 K/k を有するものが「万一」あれば、

$k \subseteq^{\exists} k' \subset K$ s.t. GRH false for $\zeta_{k'}(s)$.

!

虚2次体 ($r_1=0, r_2=1$) では $|d_k| < 2003.8\cdots$ に相当

(候補) $d_k = -2003, -1999, -1996, -1995\ (=(-3)\times 5\times(-7)\times(-19)), \cdots$

$$\mathbb{Q}(\sqrt{-1995}) \overset{8次}{\subset} \mathbb{Q}(\sqrt{-3},\sqrt{5},\sqrt{-7},\sqrt{-19}) \overset{64次}{\subset} \cdots$$

(類体塔 = 最大不分岐アーベル拡大体の塔)

(方針) あるところ迄登ってから Golod-Safarevic の「この塔が無限になる十分条件」を適用…。

単数を全部知る必要あり。(各段階で)

単数群の rank 7, $(\infty\times 2)$-adic analysis

$$\varepsilon^{(7)} = \frac{1}{4}(-1030 - 464\sqrt{5} - 225\sqrt{-3}\sqrt{-7} + 101\sqrt{-3}\sqrt{5}\sqrt{-7} + 137\sqrt{-3}\sqrt{-19}$$
$$+ 90\sqrt{-7}\sqrt{-19} + 61\sqrt{-3}\sqrt{5}\sqrt{-19} + 40\sqrt{5}\sqrt{-7}\sqrt{-19})$$

B4

塔 K/k が緊密 (tight) $\overset{\text{def}}{\Longleftrightarrow}$ $\sum_{P\in S}\alpha_P = \log\sqrt{|d_k|}$ が成立

(この場合、$K \supseteq K' \supset k' \supseteq k$ (infin, fin) なら K'/k' も tight となる)

さらに 最大緊密 (maximal-tight) $\overset{\text{def}}{\Longleftrightarrow}$ tight、且つ同じ f_P $(P\in S)$ 系の塔として最大.

---

k が、代数体の仲間「$\mathbb{F}_q$ 上の代数曲線の函数体」の枠内では これらが存在し、

tight	→	$\mathbb{F}_{q^2}$-有理点を最大限豊富にもつ無限次被覆系列
max-tight	→	素因子-共役類 (discrete な) 表示塔 (後述)

もどって:

S が大きいことで塔が引締る. 実際 $G = Gal(K/k)$ は、そのわずか1つの共役類 $\left(\frac{K/k}{P}\right)^m$ で生成される正規部分群で割ると有限群になる.

(有限に極めて近い無限群)

ただし, $1 \le m < f_P$, たとえば $P \notin S$ なら $m \ge 1$ は何でもよい

これらは G 内で dense に分布

B5　代数体の代わりに $\mathbb{F}_q$ 上の代数曲線 X の函数体 k をとった場合，
（種数 $g_X > 1$）

k の素点 P $\longleftrightarrow$ $\{$ X の $\mathbb{F}_{q^d}$-有理点 の共役類 $/\mathbb{F}_q$ $\}$;　　$d = \deg P$, $q^d = N(P)$

この場合 GRH 相当は A.Weil の定理で，Th 1 の類似は

$$\sum_{P \in S} \frac{\deg P}{q^{f_P \deg P/2} - 1} \leqq g_X - 1$$

と対応

◎ 発見された* tight tower（不分岐 coverings $\{Y \to X\}$ の無限系列）では
この等式が $S = S_1 \sqcup S_2$ & $|S_1| + 2|S_2| = (q-1)(g_X - 1)$, で成立.

$$\begin{pmatrix} \deg P \\ f_P \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

(* もとは 1960年代中頃)

◎ S_1, S_2 は、代数体の実素点，複素素点に 不思議に寄り添う……

◎ Tight $\longleftrightarrow$ S 上の Y の点はすべて $\mathbb{F}_{q^2}$-有理点 → その個数 $|Y(\mathbb{F}_{q^2})| \geqq (q-1)(g_Y - 1)$
Max_Tight $\longleftrightarrow$ そういう最大の系

B5-Suppl

では k が本来の代数体の場合の tight tower の存在は？

まず、条件「不分岐」を多少ゆるめ、$|S|=\infty$ を込める必要はあろう。

「函数体の場合は存在しても代数体では存在し得ない」と考えるに足る理由は、今のところ見当たらない。見つけるには、何かから自然に見えてくるものを…（$\hat{\pi}_1(\mathbb{P}^1 \setminus \{0,1,\infty\}, *)$ でのガロア表現では？等）

うまれる前の孫に名前をつけた爺さんにできることは？

それより、ご質問：

$$8\pi e^{\gamma} \quad (= 44.763232\cdots)$$

は何かの Volume か？

B6

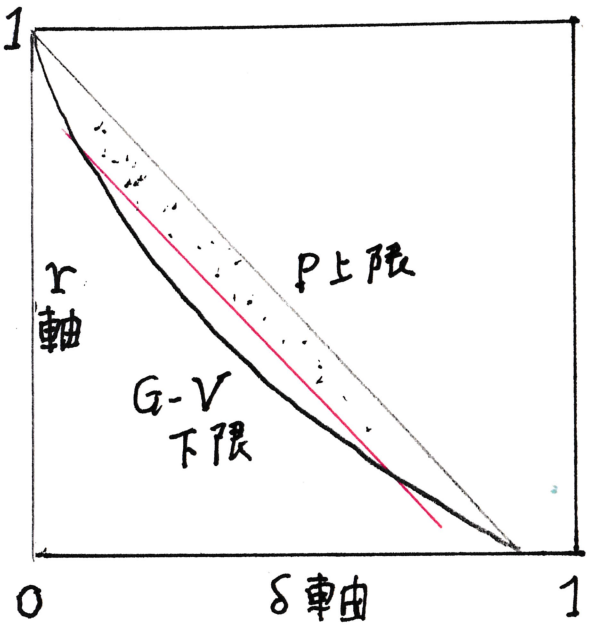
Code 理論との関わり

q 個の文字，長さ n の列を用いて，

{ (a) なるべく 多数、$(q^n)^r$ 人 $(0<r<1)$ に通信用個人番号を，ただし
(b) 異る番号は，なるべく多くの positions $n\delta$ ヶ所 $(0<\delta<1)$ で相異るよう，割り振りたい。

> q：固定，n；動かし，点 $(\delta, r) \in (0,1)\times(0,1)$ の集積点で なるべく右上のものと その構成法を 知ることが 役に立つ

q-dependent plotting



Gilbert-Varshamov 下限
約25年間，下限として best possible だった。

[Goppa-code] $\mathbb{F}_q$ 有理点 $P_0, P_1, \cdots, P_n$ をもつ $X/\mathbb{F}_q$ で、linear map

$$L(P_0^m) \ni f \longmapsto (f(P_1), \cdots, f(P_n)) \in \mathbb{F}_q^n$$

の image の集合 を使う。

$f \neq 0$ なら
座標 $=0$ となる position は $\leqq m$ ケ
$\therefore f_1 \neq f_2$ なら $n-m$ 個以上の i で $f_1(P_i) \neq f_2(P_i)$

$\geq g-2 < m < n$ とすると

$$r = \frac{m-g+1}{n}, \quad \delta \geqq 1 - \frac{m}{n}$$

$$\therefore \quad r+\delta \geqq 1 - \frac{g-1}{n} \qquad \left(\rightsquigarrow 1 - \frac{1}{\sqrt{q}-1}\right)$$

われわれの n より，$n+1 \geqq (\sqrt{q}-1)(q-1)$ が 組織的に存在。

Y.I. Manin が 私の 昔のを 憶えてくれていて，ロシアで Tsfasman, Vladut，それに 伝えてくれて，生かされた。

構造発見のモデル

C1 有限体 $\mathbb{F}_q$ 上の代数曲線 X $(q>1)$ に固有な lifting の問題

X の点 P の座標 (x_i).　　P が $\mathbb{F}_{q^d}$-rational $\iff x_i^{q^d}=x_i$ $(\forall i)$

とくに $\mathbb{F}_{q^2}$-rat'l $\iff x_i^{q^2}=x_i \iff \{x_i'=x_i^q,\ x_i=x_i'^q\}$

そこで $X'=X$ として $\{(x_i,x_i^q)\}=\Pi\subset X\times X'\supset\Pi'=\{(x_i'^q,x_i')\}$

(曲面上の2つの因子)

を考えると $X(\mathbb{F}_{q^2}) \underset{pr_X}{\xleftarrow{\sim}} \Pi\cap\Pi' \underset{pr_{X'}}{\xrightarrow{\sim}} X'(\mathbb{F}_{q^2})$.

Π と Π' を、指定された $S\subseteq X(\mathbb{F}_{q^2})$ と対応する点のみで交わらせたもの

$$\mathfrak{X}_q := \{X \leftarrow X^0=\Pi \underset{S}{+} \Pi' \longrightarrow X'\}$$ (triple of curves)

Rmk　$\mathfrak{X}_q$ の finite etale cover $\mathfrak{Y}_q \xrightarrow{\varphi} \mathfrak{X}_q \approx X$ の finite etale cover $Y\xrightarrow{\varphi}X$ s.t. $\varphi^{-1}(S)\subseteq Y(\mathbb{F}_{q^2})$

categorical equivalence

arithmetic

Y^0
$\downarrow$
X^0

S の点

flat ゆえ こういうことは ない

Gro-geometric

C2

$\mathcal{X}_q$ が 標数 0 への 持上げ を 有する 場合 を 考察。 $\mathcal{X}$ とする。

$\mathcal{X}$ は $(\infty \times p)$-adic な 対象。 その ∞ 成分 $\mathcal{X}_\infty$ を 中心に 述べると、

$$\mathcal{X}_\infty = \left\{ \Delta \backslash \mathcal{H}_\infty \xleftarrow{pr_1} \Delta^0 \backslash \mathcal{H}_\infty \xrightarrow{pr_2} \Delta' \backslash \mathcal{H}_\infty \right\}$$

複素上半平面 と 基本群

と 表わせる。 融合部分群つき 自由積 $\Gamma = \Delta *_{\Delta^0} \Delta'$ が 主役として 登場。

Th.0 (Y.I., 1979) (i) $\mathcal{X}_q$ の connected finite etale covers $\overset{(\text{イ})}{\approx}$ $\mathcal{X}_\infty$ の それら $\overset{(\text{ロ})}{\approx}$ Γ の finite index subgroups

(ii) pr_1, pr_2 : 不分岐 $\Longleftrightarrow$ $|S| = (q-1)(g_X - 1)$

(iii) (ii) のもとでは この 塔 の 第1成分 は X の 函数体 $k = \mathbb{F}_q(X)$ の max-tight tower を 与え、それは 次の 意味で「表示塔」。 Γ は $\mathcal{H}_{\infty,p} = \mathcal{H}_\infty \times \mathcal{H}_p$ に 不連続に 作用し、 $\mathcal{H}^{\text{arith}}_{\infty,p} = \{ z \in \mathcal{H}_{\infty,p} ;$ $\Gamma_z \neq \{1\}$ とおくと $\Gamma_z = (\exists \gamma_z) \cong \mathbb{Z}$ で、

$$\left\{ \begin{matrix} \Gamma\text{-conjugacy classes} \\ \text{of type } \{\gamma_z\} \end{matrix} \right\} \approx \Gamma \backslash \mathcal{H}^{\text{arith}}_{\infty,p} \rightleftarrows \text{Primes}(X) \setminus S$$

(i) の $\approx$ は categorical equivalence

森田茂之さんの ヘルプも

(イ) の ポイント は Good reduction 方向 $\leftarrow$ で、 with H. Miki。

これは、Grothendieck, Abhyankar に ない ポイント

三木博左生

(ロ) は "I's lemma", used in Ribet, Wiles, Taylor (on "Fermat" etc.)

C3　$\mathcal{X}_g$ の持上げ…**存在**が判明しているのは：

(i) Shimura Curves　4元数体 B/F (s.t. …) それぞれから系列として生じる ⇒ mod p

ポイントは合同関係式 $T(p) \equiv \Pi + \Pi'$ (mod p)　(Shimura, $\zeta_p(s)$, 森田康夫, 太田雅己)

群 Γ は $SL_2(\mathbb{Z}[\frac{1}{p}])$ の B-バージョン, $H^{arith}_{\infty,p}$ は {B の 虚の p-単数たちの幾何的配置}

(ii) $\mathcal{X}_g$ から出発して その universal deformation を与える基礎環 (ある $m \geq 0$ に対する $\mathbb{Z}_p[[t_1, \cdots, t_m]]$ の商環) が 標数 0 ("flat / $\mathbb{Z}_p$") となる条件を求める問題.

(★) S の問題 ≃ ある p-adic な微分 ω の問題 ($2S = (\omega^{\otimes(p-1)} \bmod p)$ など)

(i), (ii) 双方とかかわる.

cf. アブストラクトの文献(6)

再び 代数体の世界では？ ωも!!!

未知の格子の発見に期待
Arithmetic Spirit
個人的リスク

VS

エタール・コホモロジーによるもの以外にガロア表現は「なかろう」予想に走る
Arithmetic Algebraic Geometry…
集団的リスク？