斎藤 毅 氏

2009-10-5

Galois 表現の保型性

- 基本的用語
- 保型形式と Galois 表現との関係
- Serre 予想
- 証明の idea (modularity lifting / lifting theorem

reference
- 加藤和也氏
- 勉強会(2008)の報告集 Web
- home page Talks
  IHES Summer school の報告集の原稿
  Galois rep'n & modular forms

1994 Wiles - Taylor Fermat's last theorem の証明

志村-谷山 予想
Serre 〃 ← Khare
Sato-Tate 〃 ← Harris
Fontaine - Mazur 〃

11/21 ~ 23
高木 Lect

$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の2次元表現の保型性

から出てくる.

前回　1996年の講義では代数幾何的方法が主体
(modular curve)

今回　(なるべく勉強したいので)

- 保型形式の base change
- R=T theorem の改良

) 応用

ρ, $\overline{\rho}$: $G_{\mathbb{Q}}$ の2次元表現

↑ ℓ進表現　↖ 法ℓ表現

例　$E/\mathbb{Q}$　楕円曲線

$T_\ell E = \varprojlim E[\ell^n]$　Tate module

ρ の例

$E[\ell]$　$\overline{\rho}$ の例

これらは modular form と結びついている

modularity … 類体論の非可換化

Kronecker – Weber の定理

- Abel 拡大 ⇒ 円分体
- $G_{\mathbb{Q}}$ の1次元表現(指標) ($\mathbb{C}^\times$ 値連続)

はすべて Dirichlet 指標である

(2次元 ⟷ modular form)

$\{\pm 1\} \simeq \mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)/\mathbb{Q}\right)$

$p \neq 2$, 素数

$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$

⇓

平方剰余の相互法則

1. Galois 表現

$G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$　　$\mathbb{Q}$ の絶対 Galois 群.

($\mathbb{Q}$ だけでなく、その有限次拡大も同時に考えるのが今の主流.
今は説明が簡単のため $\mathbb{Q}$ で.)

p : 素数

$G_{\mathbb{Q}_p} = Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$　　: $\mathbb{Q}_p$ の絶対 Galois 群

$\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$　fix　　$\overline{\mathbb{Q}_p} = \mathbb{Q}_p \cdot \overline{\mathbb{Q}}$

$$G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{Q}}$$
$$\{$$
injective

局所体の Galois 群はわかりやすい:

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{ur} = \mathbb{Q}_p(\zeta_m : p \nmid m)$$
$$\bigcap \quad \text{最大不分岐拡大}$$
$$\mathbb{Q}^{tr} = \mathbb{Q}_p^{ur}(p^{1/m} : p \nmid m)$$
$$\cap \qquad \text{最大馴分岐拡大}$$
$$\overline{\mathbb{Q}}_p$$

⇝ normal subgroups

$$G_{\mathbb{Q}_p} \supset I \supset P \supset 1$$

惰性群 $(I_p$ とも$)$　　最分岐群

$$G_{\mathbb{Q}_p}/I = G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$$

$$\cup \qquad\qquad \cup$$

$$\mathrm{Fr}_p \longleftarrow 1$$

$$\|$$

$$(a \mapsto a^{1/p})$$

Kummer 拡大

$$I/P \simeq \hat{\mathbb{Z}}'(1) = \varprojlim_{p \nmid m} \mu_m$$

P　pro-p 群　　I の pro-p Sylow 群.

以下，表現に条件をつけよう.

S：素数（点）の有限集合

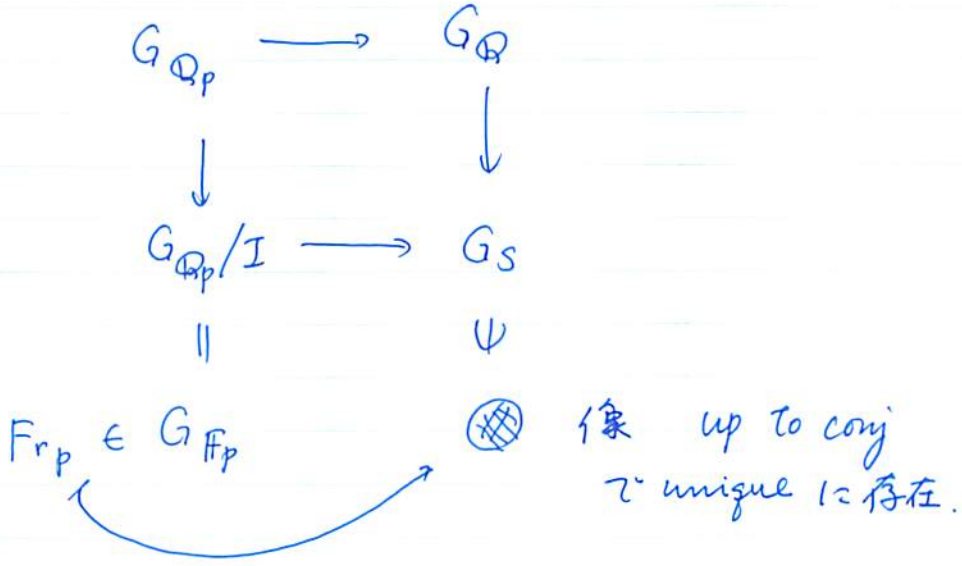
G_S ：$G_{\mathbb{Q}}$ の商　　$\forall p \notin S$ に対し

$I_p \subset G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ の像が自明となるような

最大の商

（有限個の素点をのぞいて不分岐としたい）

$p \notin S$



「$G_{\mathbb{Q}}$ の ℓ 進表現」 $\Leftrightarrow$ G_S の ℓ 進表現 for some S

E_λ : $\mathbb{Q}_\ell$ の有限次拡大　　ℓ : 素数

$$\rho : G_S \longrightarrow GL_{E_\lambda}(V) \simeq GL_n(E_\lambda)$$

連続準同型

V 有限次元 E_λ-vect space

$n = \dim_{E_\lambda} V$

F : $\mathbb{F}_\ell$ の有限次拡大　　V : 有限次元 F-v.sp

$$\bar{\rho} : G_{\mathbb{Q}} \longrightarrow GL_F(V)$$

法 ℓ 表現

↑

(ρ に対する $\bar{\rho}$ でなく)
新しい表現とみる

($\bar{\rho}$ は G_S でなく $G_{\mathbb{Q}}$ にしておくと便利)

$\rho : G_S \longrightarrow GL_{E_\lambda}(V)$ ℓ進表現

$p \nmid S$ $\quad \det(1-\rho(Fr_p)t) \in E_\lambda[t]$

$(\Leftrightarrow p \in S)$ 特性多項式

compatible systems (整合系)

(weakly)

ℓ進表現 をたくさん考える.

E : 有限次代数体 fix

(ρ_λ) : λ (E の素点) ごとに定まる ℓ進表現の系

S : 素点の有限集合

λ : Eの有限素点.

$S_\lambda = S \cup \{\ell : \lambda | \ell\}$

$\rho_\lambda : G_{S_\lambda} \longrightarrow GL_{E_\lambda}(V_\lambda)$ ℓ進表現

(ρ_λ) が weakly compatible とは

λ, λ' $\forall p \notin S_\lambda \cup S_{\lambda'}$

$\Rightarrow \det(1 - \rho_\lambda(Fr_p)t) \in E_\lambda[t]$

$= \det(1 - \rho_{\lambda'}(Fr_p)t) \in E_{\lambda'}[t]$

$E_\lambda[t] \cup E[t] \cap E_{\lambda'}[t]$

両辺ともここに入って一致する.

Why Frobenius が大事?

Cebotarev 密度定理 の帰結

ℓ 進表現 ($\bmod \ell$ ではうそ)

ρ^{ss} ($=\rho$ の半単純化) は $\mathrm{Tr}\,\rho(Fr_p)$

$p \notin S$ で決まる

nilpotent part は 特性多項式からはわからないはずだが

Tate 予想 の一部

有限体上の proper smooth な代数体の etale cohomology への Frobenius 作用は半単純.

を信じれば, 固有多項式だけ見る.

(cf Serre の本)

compatible system の例

$X_{\mathbb{Q}}$: $\mathbb{Q}$ 上の proper smooth alg var.

$X / \mathbb{Z}[\frac{1}{n}]$ proper smooth な model

base change で上になる.

$E = \mathbb{Q}$

$\lambda = \ell$ $\quad G_{\mathbb{Q}}$ が作用.

$H^q(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ q 次 etale cohom

有限次元 $\mathbb{Q}_\ell$-vect space. $\leftarrow$ $G_{\mathbb{Q}}$ の ℓ 進表現

$S = \{ p \mid n \}$

これが compatible でなること $\leftarrow$ Weil conj

$p \notin S_\ell$ $\quad p \nmid n\ell$ 素数

$$\det(1 - \mathrm{Fr}_p t : H^q(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)) \in \mathbb{Q}_\ell[t]$$

$$\| !!$$

$P_q(X_{\mathbb{F}_p}, t)$ とおく.

$X_{\mathbb{F}_p}$: X の mod p reduction $\quad X \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{F}_p$

$$Z(X_{\mathbb{F}_p}, t) = \exp\left(\sum_{m=1}^{\infty} \frac{\# X(\mathbb{F}_{p^m})}{m} t^m \right)$$

$X_{\mathbb{F}_p}$ の合同ゼータ関数 $\in \mathbb{Q}[[t]]$ $(t = p^{-s})$

($\overset{\text{Weil c.}}{\Rightarrow}$ $P_i(X, t) \in \mathbb{Z}[t]$)

$$Z(X_{\mathbb{F}_p}, t) = \frac{P_1(X_{\mathbb{F}_p}, t) \cdots P_{2d-1}}{P_0(X_{\mathbb{F}_p}, t)\, P_2(\ ) \cdots P_{2d}(X_{\mathbb{F}_p}, t)}$$

$d = \dim X_{\mathbb{Q}}$

Grothendieck の跡公式

Weil conj

$$P_g(X_{\mathbb{F}_p}, t) = (1 - \alpha_1 t) \cdots (1 - \alpha_{b_g} t)$$

α_i : 代数的整数

$|\alpha_i| = p^{g/2}$

絶対値 複素数としての

これの帰結として.

この表示が ℓ によらないことがわかる.

$\therefore$ compatible system.

特に $X_{\mathbb{Q}} = E_{\mathbb{Q}}$ elliptic curve

$$H^1(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) = \mathrm{Hom}(\underbrace{T_\ell E}_{\varprojlim E[\ell^n]}, \mathbb{Q}_\ell)$$

2次元表現　　Tate module の dual

$$P_1(E_{\mathbb{F}_p}, t) = 1 - a_p(E)\,t + p t^2$$

$t=1$ とおくと

$$\#E(\mathbb{F}_p) = 1 - a_p(E) + p.$$

$$H^0(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$$

$$H^2(E_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-1)$$　　Fr_p は p 倍で作用

$p \notin S_\lambda$　good prime, good place

$p \nmid S_\lambda$

$p \mid S_\lambda \Rightarrow$ $p \mid S$ (monodromy theorem) or $p = \ell$ (p-adic Hodge theory) (mixing 有り)

の ℓ 進表現 $p \neq \ell$.

$G_{\mathbb{Q}_p} \rightsquigarrow P$ 大きい pro-p.

$\hat{\mathbb{Z}} \to \hat{\mathbb{Z}}'(1) \to \mathbb{Z}_\ell(1) \to$

$GL_n(E_\lambda)$

$\cup$

$GL_n(\quad_\lambda)$

$\mathcal{O}_\lambda$ の剰余体 有限

$GL_n(F_\lambda)$

$1 + \underbrace{m_\lambda}_{\text{極大 ideal}} M_n(\quad_\lambda)$ pro-ℓ

有限の違いを無視すると

$\hat{\mathbb{Z}}$ の $\mathbb{Z}_\ell(1)$ による extension の表現

finite cyclic.

くらいを知ればよい

Monodromy theorem (Grothendieck)

1の m乗根全体

$$I/p \twoheadrightarrow \hat{\mathbb{Z}}'(1) = \varprojlim_{p \nmid m} \mu_m$$

$$\downarrow$$

t_ℓ と書く.

$$\mathbb{Z}_\ell(1) = \varprojlim_{n} \mu_{\ell^n}$$

$\mathbb{Z}_\ell$ 上

Thm

$\rho : G_{\mathbb{Q}_p} \longrightarrow GL_{E_\lambda}(V)$ 連続準同型

とすると, I の開部分群 J と V の巾零

自己準同型 N で $\forall \sigma \in J$ に対し

$$\rho(\sigma) = \exp\left(t_\ell(\sigma) \cdot N\right)$$

となるものが存在する

(:) J, N の存在は 線型代数

中零： N の固有値はすべて 0 を示せばよい.

$\forall \sigma \in I$ に対し, $\rho(\sigma)$ の固有値が
1 の巾根であることを示せばよい) ↗ 線型代数.

$\hat{\mathbb{Z}}$ の $\mathbb{Z}_\ell(1)$ への 共役による作用
$\|$ $\|$
$G_{\mathbb{F}_p} \curvearrowright \varprojlim \mu_{\ell^n}$ の自然な作用
ψ
$(Fr_p)^{-1}$ は p 乗で作用.

α が $\rho(\sigma)$ の固有値ならば
α^p も 〃 〃 .
α^{p^2} ...
固有値は有限個しかないので
α は 1 の巾根. ▨

monodromy thm の帰結.

ℓ 進表現 $\Rightarrow$ Weil-Deligne 群の表現 $(p \neq \ell)$

楕円 $\Rightarrow$ 〃

↑

$p=\ell$ のとき p 進 Hodge で

Weil 群

$$\begin{array}{ccc} G_{\mathbb{Q}_p} & \twoheadrightarrow & G_{\mathbb{F}_p} = \hat{\mathbb{Z}} \\ \cup & & \cup \\ W_{\mathbb{Q}_p} & \twoheadrightarrow & \mathbb{Z} \\ \text{逆像} & & \\ \cup & & \\ I & & \end{array}$$

$\mathrm{Fr}_p \mapsto 1 \in \mathbb{Z}$

I open subgroup.

subgroup だが小さくなっている.

Weil-Deligne 群.

$$WD_{\mathbb{Q}_p} = W_{\mathbb{Q}_p} \ltimes G_a$$

F_r が p 倍で作用.

G_a : ($\mathbb{Q}$ 上の) 代数群としての加法群.

WD の表現 ← 群よりも表現が大事.

W の表現 ρ と (巾零) 自己準同型 N の対で.

$$\rho(F) N \rho(F)^{-1} = pN$$

をみたすもの.

lift. $F \in W_{\mathbb{Q}_p}$

$\downarrow$ $\downarrow$

$Fr_p \in G_{\mathbb{F}_p}$

Monod thm

$\Rightarrow$

$\rho(F^n \sigma) = \rho'(F^n \sigma) \exp(T_\ell(\sigma) N)$

$n \in \mathbb{Z}$ $\sigma \in I$ とおくと

ρ' は $W_{\mathbb{Q}_p}$ の表現.