数理解析研究所講究録
第411巻 1981年 77-87

Modular curves and cyclotomic fields
Mazur - Wiles の仕事の紹介

名大 理　小池 正夫

1980年の夏に、B. Mazur と A. Wiles が日本を訪れ、p進L関数に関する"Main Conjecture"を特別な場合に解決したという講演をされました。その講演記録のまとめで報告とします。

§1. Fitting ideal

A を可換環、M を有限生成 A-加群とする。次の exact 列を考える：

$$0 \longrightarrow K \xrightarrow{\psi} A^r \xrightarrow{\phi} M \longrightarrow 0$$

ここで

$$T = \left\{ \begin{pmatrix} \psi(k_1) \\ \vdots \\ \psi(k_r) \end{pmatrix} \in M_{r\times r}(A) \ ; \ k_i \in K \right\}$$

$$I = \{ \det X \ ; \ X \in T \}$$ で生成される A の ideal

とおく。

Lemma. I は r, ψ, ϕ のとり方によらない。

Def $I = F_A(M)$ とかいて M の Fitting ideal とよぶ。

Fitting ideal に関する基本的性質をのべる。

(1) G: 有限アーベル群とする時

$$F_{\mathbb{Z}}(G) = (\#G)\mathbb{Z}.$$

(2) A の ideal $\mathfrak{a}$ に対して

$$F_A(A/\mathfrak{a}) = \mathfrak{a}.$$

(3) $\Lambda = \mathbb{Z}_p[[T]]$ T: 変数, $f_i \in \Lambda$, $p \nmid f_1 \cdots f_r$ とする

M を Λ-加群で 次の exact 列をみたすものとする:

$$0 \longrightarrow M \longrightarrow \Lambda/(f_1) \oplus \cdots \oplus \Lambda/(f_r) \to (\text{finite}) \to 0$$

このとき

$$F_\Lambda(M) = (f_1 \cdots f_r)$$

(4) $M \to N \to 0$ (exact)

$$\Rightarrow \quad F_A(M) \subseteq F_A(N)$$

(5) A の ideal I に対して

$$F_{A/IA}(M/IM) = \overline{F_A(M)}$$

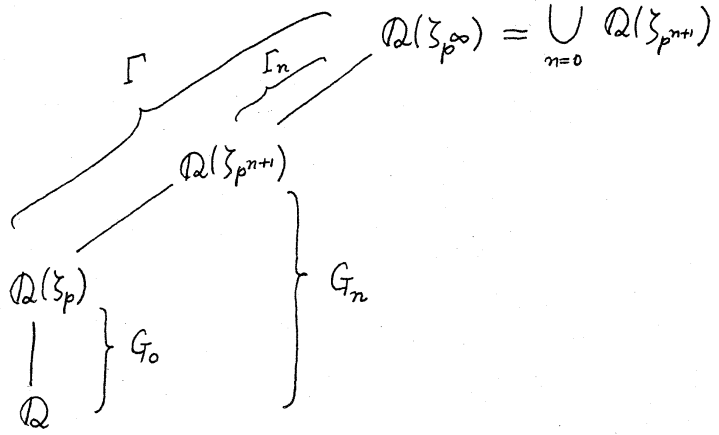
(image in A/IA)

(6) $A = \mathbb{Z}_p[\mathbb{Z}/p^n\mathbb{Z}]$, M = finite のとき

$$F_A(M) = F_A(\mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p))$$

§2. ideal class group

$p \neq 2$ 素数とする. $\zeta_{p^{n+1}}$ を 1 の原始 p^{n+1} 乗根, $\mathbb{Q}(\zeta_{p^{n+1}})$ の整数環を $\mathcal{O}_n$ とかく。



$G_n = Gal(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$, $\Gamma = Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))$,

$\Gamma_n = Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_{p^{n+1}}))$ とおく.

A_n を $\mathbb{Q}(\zeta_{p^{n+1}})$ の ideal 類群の p-シロー群として、$A_n \to A_{n+1}$ を $\mathfrak{a}\mathcal{O}_n \longrightarrow \mathfrak{a}\mathcal{O}_{n+1}$ で定義する。A_n には G_n が作用し、特に複素共役の作用で 固有値 ± 1 の固有空間の直和に分解する. それを各々 A_n^+, A_n^- とかく。このとき 上の写像で $A_n \hookrightarrow A_{n+1}$ (injection) がいえる.

Def $A_\infty^- = \varinjlim A_n^-$

A_∞^- は自然に Γ-加群 とみなせ 次の式が成立つ;

$$A_n^- = (A_\infty^-)^{\Gamma_n}$$

$\chi : G_0 \to \mathbb{Z}_p^{\times}$ p進指標に対して

$$A_n^{(\chi)} = \left\{ a \in A_n^{-} \; ; \; \sigma a = \chi(\sigma) a \quad \forall \sigma \in G_0 \right\}$$

とおく。 $A_\infty^{(\chi)}$ も同様に定義すれば 次式が成立つ：

$$A_n^{-} = \bigoplus A_n^{(\chi)}$$

χ : odd i.e $\chi(-1) = -1$ カッコの中は complex conjugation

$$A_\infty^{(\chi)} = \varinjlim A_n^{(\chi)}$$

〈問題〉 χ を odd な G_0 の p進指標とする.

(1) $F_{\mathbb{Z}_p[\Gamma/\Gamma_n]}\left(A_n^{(\chi)}\right)$ を求めよ。

(2) $F_{\mathbb{Z}_p[[\Gamma]]}\left(A_\infty^{(\chi)}\right)$ を求めよ。

ここで $\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]$ とする. Γ の位相群としての生成元 γ として $\zeta_{p^{n+1}}^{\gamma} = \zeta_{p^{n+1}}^{1+p} \quad \forall n \geq 0$ をみたすものをとって $\mathbb{Z}_p[[\Gamma]]$ と $\Lambda = \mathbb{Z}_p[[T]]$ の同型を $\gamma \leftrightarrow 1+T$ で与えておく。

Fitting ideal の性質 (6) を使えば (2) は次のようにいいかえられる：

(2)′ $F_{\mathbb{Z}_p[[\Gamma]]}\left(\mathrm{Hom}\left(A_\infty^{(\chi)}, \mathbb{Q}_p/\mathbb{Z}_p\right)\right)$ を求めよ.

今、上の χ に対して

$$X_\infty^{(\chi)} \underset{def}{=} \mathrm{Hom}\left(A_\infty^{(\chi)}, \mathbb{Q}_p/\mathbb{Z}_p\right)$$

とおく. $X_\infty^{(\chi)}$ は自然に Λ-加群とみなせ、その構造は次で

知られる：

Theorem (Iwasawa, Ferrero-Washington)

$X_\infty^{(\chi)}$ に対して、ある $f_i \in \Lambda$, $p \nmid f_1 \cdots f_r$ が存在して次の exact 列が成立つ：

$$0 \to X_\infty^{(\chi)} \to \Lambda/(f_1) \oplus \cdots \oplus \Lambda/(f_r) \to (\text{finite}) \to 0$$

従って Fitting ideal の性質(3)から

$$F_\Lambda(X_\infty^{(\chi)}) = (G_\chi(T))$$

ただし、$(G_\chi(T)) = (f_1 \cdots f_r)$ となる多項式 $G_\chi(T)$ がいえる。

§3. Main Conjecture

p進L関数と、それに関する "Main Conjecture" の一般の場合の紹介は別にかかれる予定なので、ここでは Mazur-Wiles が証明を与えた場合に限る。

$(\mathbb{Z}/p\mathbb{Z})^\times \ni a \longmapsto \sigma_a \in G_0$, $\zeta_p^{\sigma_a} = \zeta_p^a$ で G_0 と $(\mathbb{Z}/p\mathbb{Z})^\times$ の同型がある。$\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ を Teichmüller 指標とする。上の同型で G_0 の p進指標 と $(\mathbb{Z}/p\mathbb{Z})^\times$ の p進 Dirichlet 指標を同一視する。

p進L関数の一般論から $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$, $\chi(-1) = -1$

となる p進 Dirichlet 指標に対して ある $G_\chi^*(T) \in \mathbb{Z}_p[[T]]$ が存在して 次の式をみたす：

$$G_\chi^*\left((1+p)^s - 1\right) = L_p\left(\omega\chi^{-1}, -s\right) \qquad s \in \mathbb{Z}_p$$

ただし. $\chi \neq \omega$, $L_p(\omega\chi^{-1}, s)$ は p進L関数とする.

このとき

Main Conjecture. Λ の ideal として

$$\left(G_\chi(T)\right) = \left(G_\chi^*(T)\right) \quad \text{が成立つ.}$$

上の予想は次のようにいいかえられる：

$R_n = \Lambda/\left((1+T)^{p^n} - 1\right)$ とおくと. $\Lambda \twoheadrightarrow \mathbb{Z}_p[[\Gamma]]$ から

$R_n \twoheadrightarrow \mathbb{Z}_p[\Gamma/\Gamma_n]$ がいえる. 全ての $n \geq 0$ について次の式が成立つ：

$$F_{R_n}\left(A_n^{(\chi)}\right) = \left(\overline{G_\chi^*(T)}\right)$$

更に 類数公式 を使うことで. Main Conjecture の証明には

$$F_{R_n}\left(A_n^{(\chi)}\right) \subseteq \left(\overline{G_\chi^*(T)}\right)$$

がいえれば充分なことがわかる. 先にあげた問題の答がこのように得られる.

§4 explicit construction of unramified extensions.

CM型のアーベル多様体の等分点から 対対な体上のアーベル拡大がえられるという虚数乗法論の延長上で. $\Gamma_1(N)$ に関する weight 2 の原始的な cusp 形式に付随するアーベル多様体の等分点からえられる体がいろいろ研究されている. その中で Ribet [ ] は Bernoulli 数の分子が p で割れるとき $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ のガロア群の作用を定めた. non-trivial な $\mathbb{Q}(\zeta_p)$ 上の不分岐アーベル p-拡大をそのような体で実現した. この idea で Mazur-Wiles は $\Gamma_1(p^n)$ に関するヤコビ多様体の適当な等分点から得られる体で G_{n-1} の作用を定めた $\mathbb{Q}(\zeta_{p^\infty})$ 上の不分岐アーベル p 拡大を構成する. その拡大が"充分たくさん"あることから前の頁にあげた最後の形の Main Conjecture がえられる. ここでは1番下の Step. を説明する.

$p \neq 2$. 素数とする.

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{p} \right\},$$

$$\Gamma_1(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p) \;\middle|\; a \equiv d \equiv 1 \pmod{p} \right\}$$

とおく.

上の群は 上半平面 $\mathbb{H}$ に対し種 Fuchs 群として作用し. cusp の集合は $\mathbb{P}_1(\mathbb{Q})$ で与えられる. それらで割ってえら

れる代数曲線を $X_0(p)$, $X_1(p)$ とかく. $X_0(p)$ の cusp は $\{0, i\infty\}$ の2個の元からなり. $X_1(p)$ の cusp は $X_0(p)$ の各 cusp の上に $\frac{p-1}{2}$ 個ずつの点からなる。

$J_1(p)$ を $X_1(p)$ のヤコビ多様体とし, $C^{(\infty)}$ で $i\infty$ の上にある $X_1(p)$ の cusp に support をもつ divisor class のなす $J_1(p)$ の部分群をあらわす。 Manin-Drinfeld により $C^{(\infty)}$ は有限群であることが知られている. 従って C_p で $C^{(\infty)}$ の p-シロー群をあらわす. $X_1(p) \longrightarrow X_0(p)$ はガロア群 $\Delta = \left\{ \langle a \rangle \,;\, a \in (\mathbb{Z}/p\mathbb{Z})^\times / \pm 1 \right\}$ をもつガロア被覆で. Δ は C_p の上に作用している. 従って $\chi : \Delta \to \mathbb{Z}_p^\times$ に対して

$$C_p(\chi) = \left\{ c \in C_p \;\middle|\; \langle a \rangle c = \chi(a) c \quad \forall \langle a \rangle \in \Delta \right\}$$

とおく

Theorem (Kubert-Lang) $\chi \neq \omega^2$ のとき

$$C_p(\chi) \supsetneq \mathbb{Z}_p / B_{2,\chi^{-1}} \mathbb{Z}_p$$

以下. $\chi \neq \omega^2$, $p^m \parallel B_{2,\chi^{-1}}$, $m \geq 1$ とする. このとき $C_p(\chi)$ のことを単に C とかく。

$J_1(p)$ の準同型環 $End(J_1(p))$ の中にヘッケ環 T が入っている. T はヘッケ作用素からくる準同型. T_ℓ, $\ell \neq p$ prime, U_p, $w^{-1} U_p w = U_p'$ $w = \begin{pmatrix} & p^{-1} \\ & \end{pmatrix}$, Δ で

生成される.

Def $I = \mathrm{Annihilator}_{\mathbb{T}}(C)$ を Eisenstein ideal と呼ぶ.

Mazur [ ] で $J_0(p)$ の時に Eisenstein ideal が詳しく研究されている.

このとき

$$\mathbb{T}/I \xrightarrow{\sim} \mathbb{Z}/p^m\mathbb{Z}$$

が成立つ.

$\mathfrak{m} = (I, p)$ i.e. $\mathbb{T}$ の maximal ideal で I を含むものとする.

$V = J_1(p)/J_0(p)$ をとれば V は $\mathbb{Q}(\zeta_p)^+$ 上いたるところ good reduction である. V の上に $\mathbb{T}$ は自然に作用する. C の V での image をも, C と同型で それを同じ記号でかく.

$V[\mathfrak{m}^n]_{\bar{\mathbb{Q}}}$ で $\mathfrak{m}^n$ 分点のなす group scheme をあらわし.

$V_{\mathfrak{m}} = \varinjlim V[\mathfrak{m}^n]_{\bar{\mathbb{Q}}}$ とおく.

M を $V_{\mathfrak{m}}$ の sub group scheme で $\mu_{p^{r_1}} \times \cdots \times \mu_{p^{r_s}}$ 型で最大のものをとる. M は $\mathbb{T}_{\mathfrak{m}}$-不変である.

$$B \underset{\text{def}}{=} V/M, \quad B_{\mathfrak{m}} = \varinjlim B[\mathfrak{m}^n]_{\bar{\mathbb{Q}}}$$

とおく. これは isogeny である.

このとき次のことが成立つ： group scheme ($\mathbb{Q}$上) の exact 列が存在して

$$0 \longrightarrow C \longrightarrow B_m(\bar{\mathbb{Q}})[I] \longrightarrow N \longrightarrow 0$$

$$N \supseteq \mu_{p^{a_1}} \times \cdots \times \mu_{p^{a_t}}, \qquad a_1 + \cdots + a_t \geqslant m$$

が成立つ.

ここで K を $B_m(\bar{\mathbb{Q}})[I]$ の分解体とする.

Theorem (Mazur - Wiles)

(1) $K(\zeta_{p^\infty})/\mathbb{Q}(\zeta_{p^\infty})$ は有限次不分岐アーベル p 拡大

(2) $G = Gal(K(\zeta_{p^\infty})/\mathbb{Q}(\zeta_{p^\infty}))$ とおくと

$$F_{\mathbb{Z}}(G) \subseteq p^m\mathbb{Z}$$

(2)より Main Conjecture の最後の inclusion の $n=0$ の場合が（すぐにではないが）いえる.

n が高い場合には. V に代って $J_1(p^n)$ の部分多様体で $\mathbb{Q}(\zeta_{p^n})^+$ 上いたるところ good reduction となるものをうまくとりだして 上の議論を続けるというのだが. それはいづれでも Mazur - Wiles の論文にまかせたい。

References

[1]D.Kubert, S.Lang: The p-primary component of the cuspidal divisor class group on the modular curve X(p). Math. Ann. 234, 25-44(1978)

[2]B.Mazur: Modular curves and the Eisenstein ideal. Publications Math. I.H.E.S., 47 (1978)

[3]K.Ribet: A modular construction of unramified p-extensions of $Q(\mu_p)$. Inv. Math., 34, 151-162(1976)

[4]A.Wiles: Modular curves and the class group of $Q(\zeta_p)$. Inv. Math., 58, 1-35(1980)