

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
 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：

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

ここで

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

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

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 : 有限アベル群とする時

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

(2) A の ideal α に対して

$$F_A(A/\alpha) = \alpha.$$

(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:

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

このとき

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

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

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

(5) A の ideal I に対して

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

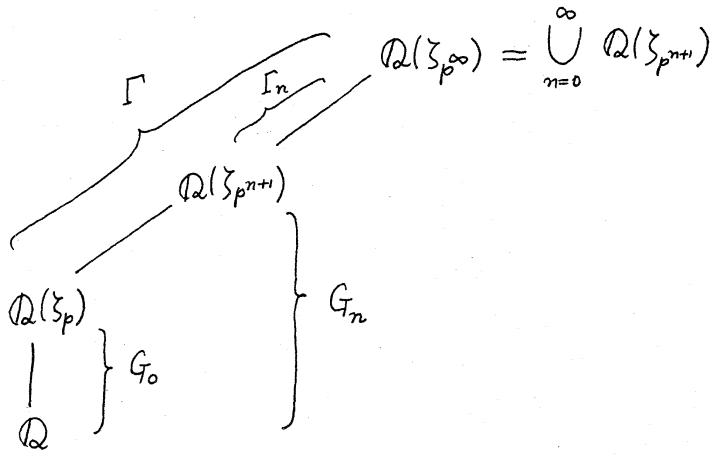
(image in A/IA)

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

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

§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.



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

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

A_n を $\mathbb{Q}(\zeta_{p^{n+1}})$ の ideal 類群の p -シロー群として, $A_n \rightarrow A_{n+1}$ を $\alpha\mathcal{O}_n \rightarrow \alpha\mathcal{O}_{n+1}$ 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.

$$\text{Def } A_\infty^- = \varinjlim A_n^-$$

A_∞^- は自然に Γ -加群とみなせ 次の式が成立つ;

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

$\chi: G_0 \rightarrow \mathbb{Z}_p^\times$ 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:

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

$\chi: \text{odd}$ i.e. $\chi(-1) = -1$ $\pi, \bar{\pi}$ の中は complex conjugation

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

<問題> χ を odd の G_0 の p 進指標とする.

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

(2) $F_{\mathbb{Z}_p[[\Gamma]]}(A_\infty^{(\chi)})$ 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 $\gamma_{p^{n+1}} = \gamma_{p^n}^{1+p} \quad \forall n \geq 0$ とみえるものとして $\mathbb{Z}_p[[\Gamma]]$ と $\Lambda = \mathbb{Z}_p[[T]]$ の同型 $\gamma \leftrightarrow 1+T$ 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)' $F_{\mathbb{Z}_p[[\Gamma]]}(\text{Hom}(A_\infty^{(\chi)}, \mathbb{Q}_p/\mathbb{Z}_p))$ を求めよ.

今、上の χ に対して

$$X_\infty^{(\chi)} \stackrel{\text{def}}{=} \text{Hom}(A_\infty^{(\chi)}, \mathbb{Q}_p/\mathbb{Z}_p)$$

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)

$X_\infty^{(x)}$ 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:

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

従って Fitting ideal の性質 (3) から

$$F_\Lambda(X_\infty^{(x)}) = (G_x(T))$$

ただし、 $(G_x(T)) = (f_1 \cdots f_r)$ とする多項式 $G_x(T)$ 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。

$(\mathbb{Z}/p\mathbb{Z})^X \ni a \mapsto \sigma_a \in G_0$, $\zeta_p^{\sigma_a} = \zeta_p^a$ で G_0 と $(\mathbb{Z}/p\mathbb{Z})^X$ の同型

がある。 $\omega: (\mathbb{Z}/p\mathbb{Z})^X \rightarrow \mathbb{Z}_p^X$ を Teichmüller 指標とする。

上の同型で G_0 の p 進指標 と $(\mathbb{Z}/p\mathbb{Z})^X$ の p 進 Dirichlet 指標
を同一視する。

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

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:

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

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

このとき

Main Conjecture. Λ の ideal として

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

上の予想は次のようにいえる:

$$R_n = \Lambda / ((1+T)^{p^n} - 1) \quad \text{とおくと} \quad \Lambda \cong \mathbb{Z}_p[[\Gamma]] \quad \text{から}$$

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

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

更に 類数公式 を使うことで Main Conjecture の証明には

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

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 対応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 -拡大と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。

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

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

とおく。

上の群は 上半平面 H にオ1種 Fuchs 群として作用し。cusp の集合は $P_1(\mathbb{Q})$ で与えられる。それらで割、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 より $C^{(\infty)}$ は有限群である: とが知られている. 従, C_p で $C^{(\infty)}$ の

p -シロ-群をあらわす. $X_1(p) \rightarrow X_0(p)$ はガロア群

$$\Delta = \{ \langle a \rangle ; a \in (\mathbb{Z}/p\mathbb{Z})^\times / \pm 1 \}$$

をもちガロア被覆で.

Δ は C_p の上に作用している. 従, $\chi: \Delta \rightarrow \mathbb{Z}_p^\times$

に対して

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

とおく

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

$$C_p(\chi) \cong \mathbb{Z}_p / B_{2, \bar{\chi}'} \mathbb{Z}_p$$

以下. $\chi \neq \omega^2$, $p^m \parallel B_{2, \bar{\chi}'}$, $m \geq 1$ 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 $\text{End}(J_1(p))$ の中にヘッケ環 Π が入っている. Π はヘッケ作用素からなる準同型 T_ℓ ,

$\ell \neq p$ prime, U_p , $w^{-1}U_p w = U_p'$ $w = (p^{-1})$, Δ で

生成される.

Def. $I = \text{Annihilator}_{\Pi}(C)$ は 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

$$\Pi/I \cong \mathbb{Z}/p^n\mathbb{Z}$$

が成立つ.

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

$V = J_1(p)/J_0(p)$ とすれば V は $\mathbb{Q}(\zeta_p)^+$ 上いたると $\mathbb{F}_p$ good reduction である. V の上に Π は自然に作用する. C の V での image を C と同型で それと同じ記号でかく.

$V[\mathfrak{m}^n]_{/\mathbb{Q}}$ で $\mathfrak{m}^n$ 分岐のなす group scheme とあらわし.

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

M は $V_{\mathfrak{m}}$ の sub group scheme で $\mu_{p^r} \times \dots \times \mu_{p^r}$ 型で最大のものをとる. M は $\Pi_{\mathfrak{m}}$ -不変である.

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

とおく. これは isogeny である.

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

$$0 \rightarrow C \rightarrow B_m(\overline{\mathbb{Q}})[I] \rightarrow N \rightarrow 0$$

$$N \cong \mu_{p^{a_1}} \times \cdots \times \mu_{p^{a_t}}, \quad a_1 + \cdots + a_t \geq m$$

が成立つ.

ここで K を $B_m(\overline{\mathbb{Q}})[I]$ 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拡大

(2) $G = \text{Gal}(K(\zeta_{p^\infty})/\mathbb{Q}(\zeta_{p^\infty}))$ 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 (すぐたではないか) 見える.

n が高い場合には V に代りて $J_1(p^n)$ の部分多様体で $\mathbb{Q}(\zeta_{p^n})^+$ 上いたるところ good reduction となるものそうまくとりだして上の議論を続けるといふのだが、それはいつか 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 $\mathbb{Q}(\mu_p)$. Inv. Math., 34, 151-162 (1976)
- [4] A.Wiles: Modular curves and the class group of $\mathbb{Q}(\zeta_p)$. Inv. Math., 58, 1-35 (1980)