岩澤理論の発展

加藤和也　（京都大学）

岩澤理論は、ゼータ関数という解析的なものの値と、代数的な整数論的な対象とが、両者の間の生来の性質の間の大きな距離を乗り越えて強く結ばれるというそのふしぎさを論ずる理論である。

１．歴史

(1) Euler

ゼータの値を始めて研究したのは、Euler であった。Euler は、後に Riemann ゼータ関数と呼ばれるようになった無限級数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

を研究し、1735 年に、

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} \cdots = \frac{\pi^2}{6}$$

であることを示した。ここに π は円周率である。Euler は、この、すべての平方数の逆数の和をもとめるという当時の大難問を解決したこと、また、その答えが、円周率が登場するふしぎなものであったことを、大変喜んだ。Euler はまた、

$$\zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}$$

一般に

$$\text{偶数}\ \ r > 0\ \ \text{について}\ \ \zeta(r) = \pi^r\ \times\ \text{有理数}$$

であることを証明した。

Euler はまた、0 以下の整数における $\zeta(s)$ の値も研究し、

$$\zeta(0) = -\frac{1}{2}, \quad \text{偶数}\ \ r < 0\ \ \text{について}\ \ \zeta(r) = 0$$

$$\text{奇数}\ \ r < 0\ \ \text{について}\ \ \zeta(r) = 2 \cdot (m-1)! \cdot \frac{\zeta(m)}{(2\pi i)^m} \quad \text{ここに}\ \ m = 1 - r\ \ (= \text{正の偶数})$$

であることを示した。たとえば、

$$\zeta(-1) = 2 \cdot (2-1)! \cdot \frac{\pi^2/6}{(2\pi i)^2} = -\frac{1}{12}.$$

実の所、0 以下の整数において $\zeta(s)$ は $\zeta(-1) = 1 + 2 + 3 + 4 + \cdots$ のように発散する。現在はこの値は、$\zeta(s)$ をその収束域である $Re(s) > 1$ から、解析接続の理論によって複素平面全体に拡張しておいて、その拡張された $\zeta(s)$ がとる値として定義されるのである

が、Euler の時代には解析接続の理論はまだ無かったから、Euler はこのような発散級数を直接相手にしたのである。しかし、Euler のような達人にとっては、このような収束しない、つまり和を持たない無限級数の和を求めることは、楽しいことだったようで、うまい方法によってこのような和を計算したのであり、それは現在解析接続によって定義される値と一致しているのである。いくつかの値を挙げる。

$$\zeta(-3) = \frac{1}{120} = \frac{1}{2^3 \cdot 3 \cdot 5} \qquad \zeta(-5) = -\frac{1}{2^2 \cdot 3^2 \cdot 7}$$

$$\zeta(-7) = \frac{1}{2^4 \cdot 3 \cdot 5} \qquad \zeta(-9) = -\frac{1}{2^2 \cdot 3 \cdot 11}$$

$$\zeta(-11) = \frac{691}{2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13}$$

$\zeta(s)$ の負の奇数での値の分母は、実は単純な性質のものであり、$\zeta(s)$ の負の奇数での値の分母に、どの素数が何乗の形で現れるかを簡単に言い表す公式が存在する。しかし、分子の方は大変に微妙で、$\zeta(-11)$ の分子に素数 691 が突然現れているけれども、それには微妙な整数論的な事柄が関係しているのである。

(2) Kummer

Kummer は、19 世紀の半ばに、$\zeta(s)$ の値が整数論的な性質を持つことについて次の二つの定理を証明した。この二つの定理は、岩澤理論の始まりと言える。これらの定理は、いずれも、$\zeta(s)$ の解析的な定義からは想像しがたいことである。

定理 A. (Kummer の合同式)　p を素数とし、r, r' を負の奇数とし、 $r \equiv r' \not\equiv 1 \mod p-1$ とすると、

$$\zeta(r) \equiv \zeta(r') \mod p$$

例。 r が $\equiv -11 \mod 691$ となる負の整数なら、$\zeta(r)$ の分子は 691 でわりきれる。

この Kummer の合同式は、やがて　$\mod p^n$ $(n \geq 1)$ の合同式へと強められていき、20 世紀になって、Kubota-Leopoldt の p 進 Riemann ゼータ関数という、$\zeta(s)$ の 0 以下での整数の値を p 進的に補間する p 進関数が存在する、という事実の現れと理解されるようになった（ [KL], [I]）。

なお、r が 0 以下の整数で $r \equiv 1 \mod (p-1)$ であるときは、$\zeta(r) \notin \mathbb{Z}_{(p)}$ である。これは、$\zeta(s)$ が $s = 1$ で極を持つのと同様に　p 進 Riemann ゼータ関数も $s = 1$ で極を持つことの、現れである。

定理 B (Kummer の判定法)　p を素数とすると、負の奇数 r で $\zeta(r)$ の分子が p でわりきれるものが存在することと、$\mathbb{Q}(\zeta_p)$ の類数が p でわりきれることは同値である。

ここに $\zeta_N = \exp(2\pi i/N)$ は 1 の原始 N 乗根である。代数体 K の類数は、K のイデアル類群 $Cl(K)$ (代数的整数論で最も重要で微妙な群、有限アーベル群である）の位数であり、したがって 「$\mathbb{Q}(\zeta_p)$ の類数が p でわりきれる」という条件は、「$Cl(\mathbb{Q}(\zeta_p))$ が、$\mathbb{Z}/p\mathbb{Z}$ に同型な部分群を持つ」とも言い換えられる。

例　$p = 691$ のとき、$\mathbb{Q}(\zeta_p)$ の類数は p でわりきれる。

Kummer がこのような定理を得たきっかけは、Fermat の最終定理を証明しようとしたことであった。Fermat の最終定理に関する Kummer の定理は次のものである。

定理　p を奇素数とする。もし $\mathbb{Q}(\zeta_p)$ の類数が p でわれなければ、$x^p + y^p = z^p$ は自然数の解をもたない。

Kummer の方法は次のものであった。$x^p + y^p = z^p$ は、$\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p$ と、積 = 積、の形に書き替えられる。整数の世界で積に関して最も重要なことは素因数分解がただ一通りにできるということであるが、Kummer は、ここに現れた ζ_p の入った世界 $\mathbb{Q}(\zeta_p)$ において、両辺を素元分解して考えようとしたが、代数体においては、一般にはただひととおりの素元分解はできないことに気付き、行き詰まった。しかしそのかわり、ただひととおりの素イデアル分解が成立することがわかり、両辺を素イデアル分解して考察した。代数体 K のイデアル類群 $Cl(K)$ は、

$$Cl(K) = \frac{K \text{ の分数イデアルのなす乗法群}}{\{(a) \mid a \in K^\times\}}$$

と定義される。すなわち、イデアル類群は、イデアルの世界と数の世界のずれをとらえるものである。$\mathbb{Q}(\zeta_p)$ の類数が p でわれないなら、乗法の理論が簡明なイデアルの世界と、数の世界の、ずれが小さくなり、積 = 積の形の上の式の考察がしやすくなり、そのことによって、Kummer は上の定理の結論を得ることができたのである。

このようにイデアル類群というものは、整数論における考察のじゃまをするもの、イデアル類群が大きければ大きいほど考察の困難が増すもの、で、苦しみを生む群である。しかし、Kummer の判定法の示していることは、イデアル類群というものが、ゼータ関数とのふしぎな関係を持つという、喜びを生む群だということである。

たとえば、$x^{13} + y^{13} = z^{13}$ が自然数の解をもたないこと（とても証明できそうにないこと）が次のようにして、Kummer の結果からわかる。13 は、 $r = -1, -3, -5, -7, -9$ のとき $\zeta(r)$ の分子に現れない（さきのゼータの値の表からわかる）。よって Kummer の合同式から、13 は負の奇数 r における $\zeta(r)$ の分子にあらわれない。これを Kummer の判定法から、$\mathbb{Q}(\zeta_{13})$ の類数は、13 でわりきれない。これと上の Kummer の定理から、$x^{13} + y^{13} = z^{13}$ は、自然数の解をもたない。

(3) 岩澤理論

ゼータの値の整数論的な意味をさぐる 1950 年代の半ばから、岩澤健吉氏が岩澤理論を始め、ゼータの値の整数論的な意味についてもっと深いことがわかるようになった。

これは、おおまかにいうと、

p 進 Riemann ゼータ関数　[ゼータ側]

$\leftrightarrow$　いろいろの N について、$\mathbb{Q}(\zeta_N)$ のイデアル類群の p べき部分 $Cl(\mathbb{Q}(\zeta_N))\{p\}$ を Galois 群 $Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ が作用する様子をこめて考えたもの　[数論側 (代数側)]

という関係を考察するものである。

ここに Galois 群の作用が現れるところが、Kummer の判定法との違いである。Kummer の判定法によれば、691 が $\zeta(-11)$ をわりきることが、691 が、$\mathbb{Q}(\zeta_{691})$ の類数をわりきる

ことを示しているのであったが、 では、この -11 にはどういう整数論的な意味があるのだろうか。岩澤健吉氏の結果ではないが今は岩澤理論の一部と見なされるようになった、Herbrand-Ribet の定理において、それは、イデアル類群への Galois 群の作用の様子としてとらえられる。

Herbrand-Ribet の定理。 p を素数、r を負の奇数とする。このとき、p が $\zeta(r)$ をわりきることと、$Cl(\mathbb{Q}(\zeta_p)$ が、$\mathbb{Z}/p\mathbb{Z}(r)$ に同型な $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 部分加群を持つことは同値である。

ここに $\mathbb{Z}/p\mathbb{Z}(r)$ は、$\mathbb{Z}/p\mathbb{Z}$ に $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ が次のように作用するものである。同型

$$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \ \ \sigma_a \leftrightarrow a, \quad \sigma_a(\zeta_p) = \zeta_p^a$$

がある。$\mathbb{Z}/p\mathbb{Z}(r)$ は、$\mathbb{Z}/p\mathbb{Z}$ に、σ_a が a^r 倍として作用するものである。

例 $p = 691$ のとき、$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 加群として、$\mathbb{Z}/p\mathbb{Z}(-11) \subset Cl(\mathbb{Q}(\zeta_p))$.

1984 年に、岩澤理論の最大の問題であった「岩澤主予想」が、Mazur と Wiles によって証明された。岩澤主予想は、

$$\begin{array}{ccc} I_1 \cdot \zeta_{p\,\text{進}} & = & \mathrm{Char}_\Lambda(X) \\ [\text{ゼータ側}] & & [\text{数論側(代数側)}] \end{array}$$

という形をしている。ここに

$$\zeta_{p\,\text{進}} = \ p \text{ 進 Riemann ゼータ関数}$$

$$X = Hom(\varinjlim_n \mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))^-, \mathbb{Q}_p/\mathbb{Z}_p)$$

(Λ は岩澤 algebra, $I_1 \subset \Lambda$ は、$s = 1$ での値をとるという環準同型 $\Lambda \to \mathbb{Z}_p$; $f \mapsto f(1)$ の核、$(\ )^-$ は複素共役写像が -1 倍で作用する部分、Char は Characteristic イデアルである。）詳細は略す。右辺は、いろいろな円分体のイデアル類群に $\mathbb{Q}$ 上の Galois 群が作用する様子を表わすものである。

その以前から、Mazur らによって、楕円曲線の岩澤理論が始まった ([M]) 。楕円曲線の岩澤理論は、本来の岩澤理論における Riemann ゼータ関数を楕円曲線のゼータ関数で置き換え、イデアル類群を楕円曲線のセルマー群で置き換えるものである。楕円曲線の岩澤理論を用いて、Coates と Wiles は、楕円曲線についての重要な予想である、Birch Swinnerton-Dyer 予想について、最初の大きな結果を得た（ [CW]) . Birch Swinnerton-Dyer 予想は、代数体 K 上の楕円曲線 E に関し、解析的な存在である楕円曲線のゼータ関数 $L(E, s)$ の $s = 1$ での零点の位数と、代数的な存在である楕円曲線の K - 有理点の群（ Mordell-Weil の定理により、有限生成アーベル群である）の、有限生成アーベル群としての階数が等しいという予想である。Coates と Wiles は、岩澤理論の方法により、解析的なものと p 進的なものを結んで、大きな結果を得たのである。これは p 進的な方法であり、もとの予想が全く p 進的なものを感じさせないことを思うと、意外な方法であった。

今は、代数体上の代数多様体の岩澤理論も、代数多様体のゼータ関数（ Hasse-Weil L 関数）と、代数多様体の代数的な性質の間の、ふしぎな関係として、定式化されている。

§2 楕円曲線の岩澤理論

楕円曲線の岩澤理論について解説する。

(1) 楕円曲線の岩澤主予想

E を $\mathbb{Q}$ 上の楕円曲線とする。p を素数とし、以下、簡単のため、E は、p で good ordinary reduction という仮定をみたすとする。

[ゼータ側（解析側）の登場人物]

E のゼータ関数（ E の L 関数と呼ばれることの方が多い） $L(E,s)$ は、志村谷山予想の解決により、複素平面全体で正則な関数になることがわかっている。その p 進類似物である、E の p 進ゼータ関数 $L_{p\,進}(E)$ が、ゼータ側の登場人物である。

$$\zeta(s)=\prod_{\ell\ 素数}(1-\ell^{-s})^{-1}$$

であるのに似て、$L(E,s)$ は Euler 積

$$L(E,s)=\prod_{\ell\ 良い素数}(1-a_\ell\ell^{-s}+\ell^{1-2s})$$

($a_\ell=1+\ell-(E(\mathbb{F}_\ell)$ の元の個数), ここに、良い素数とは E が good reduction となる素数）と定義される。

$$\zeta(s)\in\ \text{複素平面上の有理型関数全体の環}$$

であるのに似て

$$L(E,s)\in\ \text{複素平面上の正則関数全体の環}$$

（これは、志村谷山予想の解決による）であるが、岩澤 algebra と呼ばれる p 進的な可換環 Λ （下に説明）について、

$$p\ \text{進 Riemann ゼータ関数}\ \in\ \Lambda\ \text{の全商環}$$

であるのに似て、

$$L_{p\,進}(E)\in\Lambda$$

である。 Λ は、

$$G_n=Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}),\quad \Lambda=\varprojlim_n \mathbb{Z}_p[G_n]$$

と定義される。

$L_{p\,進}(E)$ は、次のようなものである。$\zeta(s)$ の場合と異なり、$L(E,s)$ は、0 以下のすべての整数で値が 0 となってしまい、そこから p 進ゼータ関数を得ることはできない。$L(E,s)$ をディリクレ級数 $\sum_{n=1}^{\infty}a_nn^{-s}$ の形に書き、群準同型 (Dirichlet 指標） $\chi:(\mathbb{Z}/p^n\mathbb{Z})^\times\to\mathbb{C}^\times$ に対し $L(E,s,\chi)=\sum_{n=1}^{\infty}a_n\chi(n)n^{-s}$ を考えると、E の (+) 周期と呼ば

れる実数　$\Omega_+ \neq 0$, E の $(-)$ 周期と呼ばれる純虚数 $\Omega_- \neq 0$ が定まって、$\chi(-1) = 1$ なら、$L(E,1,\chi)/\Omega_+$ が代数的数になり、$\chi(-1) = -1$ なら $L(E,1,\chi)/\Omega_-$ が代数的数になる。これらの代数的数値を p 進補間してできるものが、$L_{p\text{進}}(E)$ である。

$\zeta(s)$ や $L(E,s)$ は、複素平面の上に住んでいるが、p 進 Riemann ゼータ関数や、$L_{p\text{進}}(E)$ は、Galois 群を使ってできる環　Λ に住んでいるから、Galois 理論の世界に住んでいるということができる。ゼータの居住場所は、複素平面から、Galois 理論の世界へと広がっており、そちらの世界において、代数的な対象と、岩澤主予想と呼ばれる深い関係を持つのである。

[代数（数論）側の登場人物]

K を代数体とすると、E の K 上の　Selmer 群というねじれアーベル群 $\mathrm{Sel}(E/K)$ が定義され、 これは代数体のイデアル類群の楕円曲線版であって、代数体のイデアル類群同様に微妙で重要な群である。

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}(E/K) \to (E \text{ の } K \text{ 上の Tate-Shafarevich 群}) \to 0$$

という形の完全列があり、Tate-Shafarevich 群はいつも有限であろうと予想されている。

$$X = Hom(\varinjlim_n \mathrm{Sel}(E/\mathbb{Q}(\zeta_{p^n})), \mathbb{Q}_p/\mathbb{Z}_p)$$

とおく。これは、Λ 加群とみなせ、それが有限生成 Λ 加群であることは容易に証明される。Λ 加群としての X は、E の $\mathbb{Q}$ 有理点の群 $E(\mathbb{Q})$ や、$Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ の作用するアーベル群としての $E(\mathbb{Q}(\zeta_{p^n}))$ $(n \geq 0)$ の情報も含んでいる。

楕円曲線の岩澤主予想 は、p 進ゼータ関数 $L_{p\text{進}}(E)$ と、X の Λ 加群としての不変量 $\mathrm{Char}(X)$ を比較するものである。$\mathrm{Char}(X)$ について述べる。

M が有限アーベル群なら、M の最も大切な不変量は、M の位数 $\sharp(M)$ である。$M \cong \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)$ ($a_1, \cdots, a_n$ は 0 でない整数）であり、$\mathbb{Z}$ のイデアルとして、

$$(\sharp(M)) = (\prod_{i=1}^{n} a_i)$$

である。

M が有限生成ねじれ Λ 加群であるとき、M は、$\Lambda/(a_1) \oplus \cdots \oplus \Lambda/(a_n)$ ($a_1, \cdots, a_n$ は Λ の非零因子）と、quasi-isomorphic (位数有限の Λ 加群のずれを除いて同型）である。Λ のイデアル $\mathrm{Char}_\Lambda(M)$ を、

$$\mathrm{Char}_\Lambda(M) = (\prod_{i=1}^{n} a_i)$$

と定義する。(これは $a_1, \cdots, a_n$ のとりかたによらず、well　defined である。）$\mathrm{Char}_\Lambda(M)$ は、有限アーベル群の位数の類似物であり、有限生成ねじれ Λ 加群の最も大切な不変量である。

筆者は、X がねじれ Λ 加群であることを [Ka] において証明した。それゆえ、$\mathrm{Char}_\Lambda(M)$ が定義される。

楕円曲線の岩澤主予想は、

$$\begin{array}{ccc} (L_{p\text{進}}(E)) & = & \mathrm{Char}_\Lambda(X) \\ [\text{ゼータ側}] & & [\text{数論側（代数側)}] \end{array}$$

というものである。

最近 Skinner-Urban によって、次のことがほぼ証明された。（証明の詳細はまだ書かれていない。[Sk] などにまとめがある。）

定理　E に関する小さな仮定のもとで、 楕円曲線の岩澤主予想は正しい。

Mazur-Wiles ののち２０年にして、古典的岩澤主予想から楕円曲線の岩澤主予想へと、前進がおこなわれたのである。この定理で

E に関する小さな仮定のもとで、$\mathrm{Char}_\Lambda(X)|(L_{p\text{進}}(E))$

は、筆者が証明してあった。Skinner-Urban は、

E に関する小さな仮定のもとで、$(L_{p\text{進}}(E))|\mathrm{Char}_\Lambda(X)$

をほぼ証明した（ほぼ、というのは、大事なポイントである、$U(2,2)$ の保型形式にともなう Galois 表現の存在証明が、証明できることであることは確かであるとのことであるが、まだ書かれておらないので、ほぼ、と入れたのである。）なお、Λ の単項イデアル I, J について、$I|J$ とは、$J \subset I$ を意味する。

岩澤理論において、こういうことを証明するのに、二つの方法がある。

数論側がねじれ加群であることと、　数論側 | ゼータ側　であること

を証明するのに有効な「 Euler system の方法」と、

ゼータ側 | 数論側　　であること

を証明するのに有効な「保型形式の方法」である。以下にそれぞれの方法を簡単にではあるが、解説する。古典的岩澤主予想を証明した、Mazur-Wiles の方法は、「保型形式の方法」であり、後にその別証明を与えた Rubin の方法 ([La], [Wa]) は　「 Euler system 」の方法であった。古典的岩澤主予想の場合、数論側がねじれ加群であることは、イデアル類群の有限性の帰結となる。また古典的岩澤主予想の場合、上の二つの可除性（ $\cdots$ 側 $|\cdots$ 側）のうち、一方の可除性がでると、代数体の類数公式を用いて、もう一方の可除性をだすことができる。

(2) Euler system の方法

Euler system の方法は、 Kolyvagin によって始められた。

Euler system の方法は、ゼータ関数が、数論的（代数的）な対象に化身をすることを知って、その化身の力にすがる方法である。

ゼータ関数（解析的）　　$\leftarrow$ （遠い） $\rightarrow$ 数論的（代数的）対象

性格のおおいに異なる、互いに遠いものを結びつけるのは、困難であるが、ゼータさんは、数論的（代数的）対象にみずから近づこうと化身をして、数論的（代数的）な対象になる、そこをとらえるのである。

たとえば古典的岩澤理論で扱われる、Riemann ゼータ関数や、Dirichlet の L 関数の、ゼータの化身は、

$$1-\alpha \quad (\alpha \text{ は } 1 \text{ のべき根、} \alpha \neq 1)$$

であり、これらは円単数と言われる。ゼータの化身はみずから「私はゼータの化身です」と語ることはない。しかし、

$$-\log(1-\alpha) = \sum_{n=1}^{\infty} \frac{\alpha^n}{n} = \text{ ゼータの関数 } \sum_{n=1}^{\infty} \frac{\alpha^n}{n^s} \text{ の } s=1 \text{ での値}$$

$$\sum_{a \in (\mathbb{Z}/N)^\times} \chi(a) \log(|1-\zeta_N^a|) = -2L'(0,\chi)$$

（ここに、$\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ は Dirichlet 指標、$\chi(-1)=1$ と仮定する）

のような、円単数とゼータ関数との関係を見ると、円単数がゼータの化身であることは隠れもない。さらに、こういう、$\mathbb{R}$ や $\mathbb{C}$ の中における関係ばかりでなく、円単数は p 進世界でもゼータ関数と関係し、$(1-\zeta_{p^n})_{n\geq 1}$ という円単数の系の、Kummer- 岩澤- Coates-Wiles-Coleman が定義した p 進的な準同型による像が、p 進 Riemann ゼータ関数になることが知られている。このことを通して、円単数は、0 以下の整数での Riemann ゼータ関数の値 $\zeta(-1), \zeta(-3), \zeta(-5), \cdots$ などとも、p 進的に関係するのである。

ゼータ関数は、みずから Euler system （ゼータの化身）に姿を変えて、数論的（代数的）世界にはいり、

数論側 | ゼータ側

という可除性を示そうとするのである。

ゼータの故郷から、ゼータさんは、

実数や複素数の世界にやってきて、ゼータ関数（ Euler 積）となり、

p 進世界にやってきて、p 進ゼータ関数となり、

数論的（代数的）世界にやってきて、ゼータの化身（ Euler 系）となる。

このゼータの故郷、ゼータのすみか、がどこにあるかについては、（ある材木置き場、鎌倉の関レンタカーの裏庭など）候補地についての考えを筆者は何度かいろいろな所に書いた。

見つかっている Euler system についてまとめてみる。

ゼータの化身	円単数	Beilinson elements	Heegner points
どんなゼータの化身か	$\zeta(s)$	$L(E,s)$	$L(E,s)$
どこに現れる	$K_1(\mathbb{Q}(\zeta_N))$	modular curve の K_2	modular curve の K_0
$\mathbb{R}$ や $\mathbb{C}$ において関係するのは	$L'(0,\chi)$	$L'(E,0,\chi)$	$L'(E_K,1,\nu)$
$\mathbb{Q}_p$ において関係するのは	$\zeta_{p\text{ 進}}$	$L_{p\text{ 進}}(E)$	$L^{\mathrm{anti}}_{p\text{ 進}}(E)$

(χ は、Dirichlet 指標、K は虚２次体、ν は anti-cyclotomic character というもの、$L^{\mathrm{anti}}_{p\text{ 進}}(E)$ は E の anti-cyclotomic p 進 L 関数というもの。ゼータの化身は K 群に現れることを

強調するため、K 群のことばで、化身がどこに現れるかを書いたが、普通のことばでは、$K_1(\mathbb{Q}(\zeta_N)) = \mathbb{Q}(\zeta_N)^\times$ であり、 modular curve の K_0 に現れると書いたものは、その部分群である modular curve の Jacobian variety の有理点の群に現れる。)

Euler system の方法の弱い所は、(ゼータの化身はあまねく存在すると思われるにもかかわらず) ゼータの化身 (Euler system) があまり見つかっていないことである。

いろいろな所ですでに論じたことではあるが、ゼータが化身をする様子は、鶴の恩返しの話で鶴が化身をするのと似ている。ゼータが、解析的な存在である自分とは遠い数論的 (代数的) 対象に近づくため、みずから化身だとは名乗らずに数論的 (代数的) 対象に姿を変えるように、鶴は、鳥である自分とは遠い存在である人間に近づくため、みずから化身だとは名乗らずに娘に変える。鶴が人間の家にはいった後に鶴のあやにしきというきれいな織物を織り上げるように、ゼータは数論的世界に入った後、数論側 | ゼータ側、というきれいな式を織り上げるのである。

どうやって実際にこの、「数論側 | ゼータ側」が示されるかは、簡単にいうと、次のとおりである。古典的岩澤理論の場合を述べる。

円単数の系は、Kolyvagin によって発見されたある過程によって (これは、ゼータの化身が、Euler 積の代数的化身であることの反映である、Euler system の性質と呼ばれる特別の代数的な性質を持つことから生ずる過程)、期待されるだけ十分多くの、円分体の単項イデアルを生み出す。これにより、商群

$$\text{イデアル類群} = \frac{\text{分数イデアル群}}{\text{単項イデアル群}}$$

が、期待されるだけ小さい、ということがわかる。

$$\text{イデアル類群側} \mid \text{ゼータ側}$$

となりうるだけ小さいことが示されるのである。

(3) 保型形式の方法

Riemann ゼータ関数 $\zeta(s)$ や Dirichlet L 関数 $L(s,\chi)$ は、代数群 GL_1 の保型形式のゼータ関数であるといえる。Mazur と Wiles はこれらのゼータ関数についての岩澤主予想の ゼータ側 | 数論側 を証明するのに、 GL_1 より大きな代数群 GL_2 の保型形式を用いた。GL_2 の代数群とは、通常の、上半平面上の保型形式のことである。

$L(E,s)$ は (志村谷山予想の解決により) GL_2 の保型形式のゼータ関数である。Skinner と Urban は、$L(E,s)$ に関するの岩澤主予想の「ゼータ側 | 数論側」を証明するのに、 GL_2 より大きな代数群 $U(2,2)$ の保型形式を用いた。

それがどのような方法であるか、古典的岩澤理論の方を解説する。ここでは、さきに紹介した、Herbrand と Ribet の定理のうちの Ribet の部分、

$$p|\zeta(r) \Rightarrow Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \text{ 加群として } \mathbb{Z}/p\mathbb{Z}(r) \subset Cl(\mathbb{Q}(\zeta_p))$$

(これは、イデアル類群が十分大きい、つまり数論側がゼータ側に比べて十分大きい、「ゼータ側 | 数論側」、の方向の話である) の、保型形式を用いた Ribet の証明方法を紹介する。Mazur-Wiles の証明は、この Ribet の方法を発展させたものであった。

この「保型形式の方法」には、次の３つのキーポイントがあった。

(i) Riemann ゼータ関数 $\zeta(s)$ の 0 以下の整数での値が、上半平面上の保型形式である Eisenstein 級数の、定数項に現れる。

実際、偶数 $k \geq 4$ に対し、Eisenstein 級数

$$E_k = \frac{(k-1)!}{2\cdot(2\pi i)^k}\sum_{m,n}(m\tau+n)^{-k}$$

（ここに $\sum_{m,n}$ は、$(m,n) \in \mathbb{Z}^2, (m,n) \neq (0,0)$ についての和）は、上半平面 $\{\tau \in \mathbb{C} \,|\, Im(\tau) > 0\}$ の元 τ の関数として、重み k の保型形式となり、$q = e^{2\pi i\tau}$ についての q 展開

$$E_k = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

を持つ。ここに、$\sigma_m(n)$ は、d が n の約数を走る時の、d^m の和。（この定数項が $\zeta(1-k)/2$ であるわけは、E_k の定義式で、$q \to 0$ つまり τ の虚部を $\to \infty$ としていくと、(m,n) のうち $m=0$ の項だけが残り、E_k の定数項 $E_k|_{q=0}$ は、

$$\frac{(k-1)!}{2\cdot(2\pi i)^k}\sum_{n\in\mathbb{Z},n\neq 0}n^{-k} = \frac{(k-1)!}{2\cdot(2\pi i)^k}\cdot 2\zeta(k) = \frac{\zeta(1-k)}{2}$$

となるからである。

(ii) GL_2 の固有保型形式（固有、とは、Hecke 作用素の固有関数になっていること）f には、$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ の　p 進体上の２次元表現

$$\rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(p \text{ 進体})$$

が伴う。f が尖点形式なら、ρ_f は既約表現である。

(iii) イデアル類群は有限アーベル群における Galois 表現の、拡大（ extension　）の類のなす群と見なすことができる。

たとえば、

$$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \text{ 加群として } \quad \mathbb{Z}/p\mathbb{Z}(r) \subset Cl(\mathbb{Q}(\zeta_p))$$

という条件は、$Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ の $\mathbb{Z}/p\mathbb{Z}$ 上の表現の完全系列

$$0 \to \mathbb{Z}/p\mathbb{Z}(r) \to ? \to \mathbb{Z}/p\mathbb{Z} \to 0$$

で、次の条件をみたすものが存在することと同値である。

? は p の外で不分岐であり、この完全列は分解せず、この完全列は　$Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ ($\subset Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$) の表現の完全列としては分解する。

Herbrand と Ribet の定理のうちの Ribet の部分は、以上のキーポイント (i)-(iii) を用いて、だいたい次のように証明される。

$p|\zeta(r)$

とする。(r は負の奇数。)　$k = 1 - r$ とする。

(i) により、

$E_k \mod p$ は定数項をもたない。

これは

$E_k \equiv f \mod p$ となる、固有尖点形式　f が存在する

ということを意味する。(尖点形式とは、だいたい、定数項が 0 の保型形式、ということなので、定数項　mod p が 0 になると、こういう尖点形式との関係が出てくる。) たとえば、$691|\zeta(-11)$ であるが、

$$E_{12} \cong \Delta \mod 691 \quad \text{(これは有名な Ramanujan の合同式)}$$

ここに、

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

で、Δ は固有尖点形式である。

(ii) により、既約　Galois 表現

$$\rho_f : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(p\,\text{進体})$$

があるが、この Galois 表現の　mod p

$$\rho_f \mod p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/p\mathbb{Z})$$

を考える。この $\mathbb{Z}/p\mathbb{Z}$ 上の２次元表現を ? と書くとき、$E_k \equiv f \mod p$ であることを用いると完全列 $0 \to \mathbb{Z}/p\mathbb{Z}(r) \to ? \to \mathbb{Z}/p\mathbb{Z} \to 0$ で、さきの条件をみたすものが存在することがわかる。ここで、この完全列が分解しないことは、ρ_f が既約であることによる。

(iii) により、

$$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \text{ 加群として } \quad \mathbb{Z}/p\mathbb{Z}(r) \subset Cl(\mathbb{Q}(\zeta_p))$$

となる。

Skinner-Urban の方法は、この道筋に沿って、これを発展させたものである。そこにも次の３つのキーポイントがある。

(i) $L(E, 1, \chi)$ は、$U(2,2)$ の Eisenstein 級数の定数項に現れる。

(ii) $U(2,2)$ の固有保型形式には、p 進 Galois 表現が伴う。

(iii) 楕円曲線の Selmer 群も、有限アーベル群における Galois 表現の拡大の類のなす群とみなすことができる。$\mathrm{Sel}(E/K)$ の部分 $\mathrm{Sel}_{p^n}(E/K)$ は、$Gal(\bar{K}/K)$ の $\mathbb{Z}/p^n\mathbb{Z}$ 上の表現の完全列

$$0 \to E[p^n] \to ? \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

（である条件をみたすもの）の類のなす群である。

(ii) の Galois 表現の存在が、まだ、書かれていない。この、固有保型形式（保型表現）から Galois 表現が得られるということは、保型表現と Galois 表現の間の対応を予想する　Langlands 予想（非可換類体論）の一部であって、最近この方面の発展が著しい。Langlands 予想（非可換類体論）の発展にしたがって、この Skinner-Urban の「保型形式の方法」はどんどん拡張発展し、ゼータ側　| 数論側、という可除性の証明は、 GL_1, GL_2 の保型形式のゼータ関数のみならず、いろいろな代数群の保型形式のゼータ関数に拡張されていくであろうと思われる。一方、Euler system 方法の方は、Euler system があまり見つからないので、停滞している。Rubin さんにお会いしたとき、Skinner-Urban の方向はどんどん進んでいきそうですが、私達　Euler system 人間はいまそんなに元気でないですね、と言ったら、いつも強気の　Rubin さんも、かすかにうなづいたように見えた。私は、Euler system（ゼータの化身）をもっと見つけるためには、鶴の恩返しのような日本昔話を読むのが大切、と考え、だいぶ読んだのであるが、まだその効果はあらわれないでいる。

本稿では、楕円曲線の岩澤理論についての、Bertolini-Darmon（[BD] など）らによる、anti-cyclotomic 岩澤理論の紹介をしなかった。また、代数学シンポジウムでは、楕円曲線の非可換岩澤理論の解説もおこなったが、本稿では省いた。

文献

[CW] J. Coates, A. Wiles; On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), no. 3, 223–251.

[DB] M. Bertolini, H. Darmon; The p-adic L-functions of modular elliptic curves. Mathematics unlimited—2001 and beyond, 109–170, Springer, 2001.

[I] K. Iwasawa; Lectures on p-adic L-functions. Annals of Mathematics Studies, No. 74. Princeton University Press.

[Ka] K. Kato; p-adic Hodge theory and values of zeta functions of modular forms. Astérisque No. 295 (2004), 117–290.

[KL] T. Kubota, H. Leopoldt; Eine p-adische Theorie der Zetawerte. I. Einfuhrung der p-adischen Dirichletschen L-Funktionen. J. Reine Angew. Math. 214/215 1964 328–339.

[La] S. Lang; Cyclotomic fields I and II. Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, 121. Springer, 1990.

[M] B. Mazur; Rational points of abelian varieties with values in towers of number fields. Invent. Math. 18 (1972), 183–266.

[MW] B. Mazur; A. Wiles; Class fields of abelian extensions of $\mathbb{Q}$. Invent. Math. 76 (1984), 179–330.

[Sk] C. Skinner; Main conjectures and modular forms, preprint.

[Wa] L. Washington; Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer, 1997.