

岩澤理論 – 過去と現在

小林 真一 (九州大学)*

1. はじめに

本講演のタイトルは、岩澤理論界の重鎮、R. Greenberg による論文[14]にちなんだものである。岩澤理論は1950年代に岩澤健吉によって、19世紀のKummerによる円分体の整数論を発展、精密化させる形で創始された理論である。岩澤理論の研究対象は当初は代数体にとどまっていたが、1970年代にB. Mazurにより楕円曲線などのアーベル多様体に拡張され、その後J. Coates, B. Perrin-Riou, R. Greenberg, K. Katoらによって、モチーフ、ガロワ表現およびその変形へとさらに一般化された。また道具立ても、類体論から出発し、 p 進Hodge理論などの数論幾何、そして最近では保型表現へと広がりを見せている。その中でBirch and Swinnerton-Dyer予想への応用など、著しい成果も得られてきた。しかし本講演ではこのようなことを体系的に述べようというわけではない。受賞内容である楕円曲線の岩澤理論に中心をおき、過去から現在までを振り返りながら、多くの方に岩澤理論の研究の一端を素朴に紹介したいというのが趣旨である。またその中で講演者の仕事にも触れたい。そのようなわけで内容にはかなり偏りがあり、重要な話題で触れてないことが非常に多い。岩澤理論をより総合的な見地から知りたい方は、落合理氏による解説記事[35]や本[36]があるので、そちらを参照されるのがよいと思う。また以下の解説も、わかりやすさや読み易さを重視し、専門的になりすぎないように書いたので、定義や内容をかなり省略している。詳しいことは引用文献を見ていただきたい。また有用と思える文献も参考文献に入れておいた。

2. 円分体の岩澤理論

ここでは原点である円分体の岩澤理論について簡単に振り返る。重要な結果や未解決課題も多くあるが、岩澤理論の最初の定理ともいえるべき岩澤の類数公式と、その名のとおり中心課題である岩澤主予想について絞って述べる。

2.1. 岩澤の類数公式

代数体のイデアル類群は代数的整数論における最も重要な群であるが、一般には不規則な振る舞いをし組織的な研究が難しい。岩澤理論の出発点は代数体 K を単独で考えるのではなく、素数 p を固定して K のいわゆる $\mathbb{Z}_p$ -拡大

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty := \bigcup_{n=0}^{\infty} K_n$$

を考えることである。ここで K_n は次数 p^n の K のガロワ拡大である。 $\mathbb{Z}_p$ -拡大の最も重要な例は、1の原始 p^n -乗根 ζ_{p^n} を添加してできる円分 $\mathbb{Z}_p$ -拡大である。つまり $K_\infty \subset \bigcup_{n=0}^{\infty} K(\zeta_{p^n})$ となる唯一つの $\mathbb{Z}_p$ -拡大 K_∞/K である。 $\mathbb{Z}_p$ -拡大においてはイデアル類群は族としては組織的な振る舞いをするというのが岩澤類数公式である。

* 〒819-0395 福岡県福岡市西区元岡 744
e-mail: kobayashi@math.kyushu-u.ac.jp

定理 1 ([17, Theorem 11]) A_n を K_n のイデアル類群の p -Sylow 部分群とし, $\sharp A_n = p^{e_n}$ とおく. このときある整数 λ, μ, ν があって, 十分大きな n に対し次が成り立つ.

$$e_n = \lambda n + \mu p^n + \nu$$

2.2. 円分体の岩澤予想

ここでは p と互いに素な自然数 N をひとつ固定して, $K_n = \mathbb{Q}(\zeta_{Np^{n+1}})$ で定義される円分 $\mathbb{Z}_p$ -拡大を考える.

$$G_n := \text{Gal}(K_n/\mathbb{Q}), \quad G_\infty := \text{Gal}(K_\infty/\mathbb{Q}) = \varprojlim_n G_n$$

$$\Gamma_n := \text{Gal}(K_n/K_0), \quad \Gamma_\infty := \text{Gal}(K_\infty/K_0) = \varprojlim_n \Gamma_n$$

とおく. A_n にはガロワ群 G_n が自然に作用し, ノルムによる逆極系 $\mathcal{A} := \varprojlim_n A_n$ には完備群環 $\mathbb{Z}_p[[G_\infty]]$ が自然に作用する. 重要な点は $\mathbb{Z}_p[[\Gamma_\infty]]$ は抽象的には一変数ベキ級数環 $\mathbb{Z}_p[[X]]$ と同型で, $\mathbb{Z}_p[[G_\infty]]$ は $\mathbb{Z}_p[[X]]$ の有限個の直積になっていることである. $\mathbb{Z}_p[[X]]$ は単項イデアル整域ではないが, それにかなり近い環であり, 有限生成 $\mathbb{Z}_p[[X]]$ -加群の構造定理がある. この構造定理からねじれ加群に対しては“単因子の積”として特性イデアルが定義される. 岩澤類数公式の証明も, $\mathcal{A}$ が有限生成ねじれ $\mathbb{Z}_p[[G_\infty]]$ -加群であることを示すのが鍵である. イデアル類群の有限性の類似が $\mathcal{A}$ が有限生成ねじれ $\mathbb{Z}_p[[G_\infty]]$ -加群であること, 類数の類似が $\mathcal{A}$ の特性イデアルとなる. そして解析的類数公式の類似が岩澤主予想である.

古典的な解析的類数公式は, 類数をゼータ関数や L -関数の $s = 1$ での値で書くものであった. 円分体の岩澤理論においては, Kubota-Leopoldt の p -進 L -関数 $\mathcal{L}_p^{\text{KL}} \in \mathbb{Z}_p[[G_\infty]]$ が登場する. この関数を大雑把に説明すると, G_∞ の指標 χ は自然に Dirichlet 指標と解釈され, $\chi(\mathcal{L}_p^{\text{KL}})$ が χ に対応づけられる Dirichlet L -関数の $s = 1$ での値になるものである. 別の言い方をすると, Dirichlet L -関数の $s = 1$ での値を p -進的に貼り合わせてできる $\mathbb{Z}_p[[G_\infty]]$ の元といえる. そして岩澤主予想は標語的には, $\mathcal{A}$ の特性イデアルは $\mathcal{L}_p^{\text{KL}}$ で生成されるといえる. (正確に述べるのは少し技術的になるので省略する. 例えば [35], [36] を参照.)

3. 楕円曲線の岩澤理論

楕円曲線の岩澤理論は 1970 年代に B. Mazur ([29]) によって始められた. E を代数体 K 上定義された楕円曲線とする. この場合の整数論的に重要な不変量は, K -有理点の集合 $E(K)$, いわゆる Mordell-Weil 群と Tate-Shafarevich 群 $\text{III}(E/K)$ である. また $E(K)$ と $\text{III}(E/K)$ を合わせたものが Selmer 群 $\text{Sel}(E/K)$ である. より正確には

$$0 \rightarrow E(K) \otimes \mathbb{Q}/\mathbb{Z} \rightarrow \text{Sel}(E/K) \rightarrow \text{III}(E/K) \rightarrow 0$$

という完全列で結ばれている. 楕円曲線の岩澤理論とは K の $\mathbb{Z}_p$ -拡大 K_∞/K に対し, $E(K_n)$, $\text{III}(E/K_n)$, $\text{Sel}(E/K_n)$ の振る舞いを組織的に調べる理論といえる. この振る舞いは E が p で通常還元をもつか超特異還元をもつかでまったく異なる. 通常還元をもつ場合は非常に規則的で, 古典的岩澤理論との素直な類似が成立すると考えられている. 一方で超特異還元をもつ場合は一筋縄ではいかない. 本講演で述べる講演者の結果は

超特異の場合を扱っている.

定理 2 (Mazur [30]) E/K は素数 p 上の任意の素点で良通常還元をもつものとする. また K_∞/K は E の悪い素点においてマイルドな条件を満たすものとする. このときある整数 a, e があって, 十分大きな n に対して,

$$\text{rank } E(K_n) = ap^n + e.$$

a は考えている K_∞/K に依存し, Mazur がいくつかの場合に a の値を予想している. これに関しては §3.1 で円分 $\mathbb{Z}_p$ -拡大のとき, §3.2 で反円分拡大のときの結果を紹介する. この定理の証明や楕円曲線の岩澤理論において重要なのは次の Selmer 群の族である. $\text{Sel}_p(E/K_n) := \text{Sel}(E/K_n)[p^\infty]$ とおき, $\text{Sel}_p(E/K_n)$ の Pontryagin 双対の逆極系

$$\mathcal{X}(E/K_\infty) := \varprojlim_n \text{Sel}_p(E/K_n)^\vee$$

を考える. $\mathcal{X}(E/K_\infty)$ は有限生成 $\Lambda := \mathbb{Z}_p[[\text{Gal}(K_\infty/K)]]$ -加群となる. 次も本質的に Mazur によるものである.

定理 3 楕円曲線 E/K は素数 p 上の任意の素点で良通常還元をもつものとする. また $\mathcal{X}(E/K_\infty)$ は Λ -加群としてねじれ加群で, $\text{III}(E/K_n)[p^\infty]$ は有限群と仮定する. $\#\text{III}(E/K_n)[p^\infty] = p^{e_n}$ とおく. このときある整数 λ, μ, ν があって, 十分大きな n に対し次が成り立つ.

$$e_n = \lambda n + \mu p^n + \nu.$$

以下では岩澤主予想などの深い結果を述べるため, E は $\mathbb{Q}$ 上定義されているとし, 円分 $\mathbb{Z}_p$ -拡大と反円分 $\mathbb{Z}_p$ -拡大の 2 つの場合に分けて説明する.

3.1. 円分 $\mathbb{Z}_p$ -拡大の場合

$K = \mathbb{Q}$ とし $K_\infty = \mathbb{Q}_\infty$ を $\mathbb{Q}$ の唯一つの $\mathbb{Z}_p$ -拡大である円分 $\mathbb{Z}_p$ -拡大とする. 次は 70 年代に Mazur が予想し, 90 年代に加藤 [18] によって証明された深い結果である. (Rohrlich [45] も本質的に使われている.)

定理 4 (Kato[18]) E が p で通常還元をもつとき $\mathcal{X}(E/\mathbb{Q}_\infty)$ は有限生成ねじれ Λ -加群である. 超特異還元をもつならば自由階数 1 の有限生成 Λ -加群である.

これから定理 2 が $a = 0$ で成立することがわかる. つまり $\text{rank } E(\mathbb{Q}_n)$ は十分大きな n に対し一定値となる. 実は超特異の場合もやはり $\text{rank } E(\mathbb{Q}_n)$ が十分大きな n に対し一定値となることが示されている. ただしこの場合は定理 2 からただちに従うわけではない. 実際, いわゆる Selmer 群のコントロール定理が成り立たないため, $\mathcal{X}(E/\mathbb{Q}_\infty)$ と $\mathcal{X}(E/\mathbb{Q}_n)$ が直接的に結びつかず, それらを結びつける適当な理論が必要となる. B. Perrin-Riou は [41] においてそのような理論を構築した. また講演者も [19] において [41] をより精密化する理論を作り, $\text{rank } E(\mathbb{Q}_n)$ の上界を後述の R. Pollack による p -進 L -関数の λ -不変量を使って与えた.

Tate-Shafarevich 群の岩澤類数公式も、通常還元の場合は、定理 3, 4 より $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ の有限群性を認めれば成立する。しかし超特異の場合は 2000 年頃の栗原 [25] が契機となって解明が進んだ。(実は 70 年代に Nasybullin による仕事 [33] があったのだが、ロシア語の短い論文で証明がほとんど書いてないという状況だったためか忘れ去られていたようである。)

定理 5 (Nasybullin [33], Kurihara [25], Perrin-Riou [44], K. [19]) $p \geq 5$ とし、 E が p で超特異還元をもつとする。また $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ は有限と仮定し $\#\text{III}(E/\mathbb{Q}_n)[p^\infty] = p^{e_n}$ とおく。このときある整数 $\lambda^\pm, \mu^\pm, \nu$ があって、十分大きな n に対し次が成り立つ。

$$\begin{aligned} e_n = & \sum_{m=0}^{\lfloor \frac{n-2}{2} \rfloor} p^{n-1-2m} - \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n+1}{2} \right\rfloor \lambda_+ + \left\lfloor \frac{n}{2} \right\rfloor \lambda_- - n r_\infty \\ & + \sum_{m=1}^{\lfloor \frac{n-1}{2} \rfloor} (p^{2m+1} - p^{2m}) \mu_+ + \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} (p^{2m} - p^{2m-1}) \mu_- + \nu \end{aligned}$$

ここで $r_\infty = \text{rank } E(\mathbb{Q}_\infty)$, $[x]$ はガウス記号である。

次に岩澤主予想について述べる。円分体の岩澤主予想が解析的類数公式と関係していたように、楕円曲線の場合は Birch and Swinnerton-Dyer 予想と関係する。これについては §4 で述べる。 p が良通常素点の場合は岩澤主予想の定式化は円分体の岩澤主予想のときと同様である。

岩澤主予想 (良通常素点): $\mathcal{X}(E/\mathbb{Q}_\infty)$ の特性イデアル $\text{Char}(\mathcal{X}(E/\mathbb{Q}_\infty))$ は Mazur-Swinnerton-Dyer の p -進 L -関数 $\mathcal{L}_p(E/\mathbb{Q})$ で生成される。

Mazur-Swinnerton-Dyer の p -進 L -関数 $\mathcal{L}_p(E/\mathbb{Q})$ について簡単に説明する。 $E/\mathbb{Q}$ の Hasse-Weil L -関数を $L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ とする。また χ を Dirichlet 指標とし、 $L(E/\mathbb{Q}, \chi, s) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}$ とおく。 $\Omega_E \in \mathbb{R}$ を E の実周期とする。このとき $L(E/\mathbb{Q}, \chi, 1)/\Omega_E$ は代数的数になる。また χ として $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ を経由するものを動かすと、適当な p -進合同関係 (ある種の Kummer 合同関係) がある。これらの値を p -進解析関数で補間する形でできるのが p -進 L -関数 $\mathcal{L}_p(E/\mathbb{Q})$ である。正確には $\Lambda \otimes \mathbb{Q}$ の元として構成されるが常に Λ の元になると予想されており、実際ほとんどの場合にそうであることが示されている。

この主予想は 70 年代に Mazur によって予想されたが、90 年代にオイラー系の技法により、虚数乗法をもつときは Rubin [46]、一般の場合は加藤 [18] により、 $(\mathcal{L}_p(E/\mathbb{Q})) \subset \text{Char}(\mathcal{X}(E/\mathbb{Q}_\infty))$ が示された。虚数乗法をもつときは、解析的類数公式を使うと、実はこの包含関係から等式が自動的に従う。一般の場合はそのようなことは便利なことではない。岩澤主予想にはオイラー系を使うアプローチと Ribet に端を発する保型形式の合同を使う手法がある。Skinner-Urban は [49] において後者の方法を発展されることで、2010 年頃に多くの場合に逆向きの包含関係 $(\mathcal{L}_p(E/\mathbb{Q})) \supset \text{Char}(\mathcal{X}(E/\mathbb{Q}_\infty))$ を証明した。

超特異の場合は主予想の定式化自体が易しくない。 $\mathcal{X}(E/\mathbb{Q}_\infty)$ がねじれ加群ではないので特性イデアルが素朴には定義されない。また p -進 L -関数 $\mathcal{L}_p(E/\mathbb{Q})$ も Amice-Velu,

Vishik らによって構成されていたものの、 Λ の元とはほど遠い解析関数となっている。しかし B. Perrin-Riou による精力的な研究によって、90 年代中頃までには主予想の定式化を含め多くのことが解明された。([42], [43].) そのような中、2000 年代に入り R. Pollack が [37] においてまったく新しいアプローチを見つけた。それは p -進 L -関数 $\mathcal{L}_p(E/\mathbb{Q})$ を分解し、2 つの “よい” p -進 L -関数 $\mathcal{L}_p^+(E/\mathbb{Q}), \mathcal{L}_p^-(E/\mathbb{Q})$ を取り出す方法である。このよい p -進 L -関数 $\mathcal{L}_p^\pm(E/\mathbb{Q})$ は Λ の元で λ, μ -不変量も自然に定義される。定理 5 の岩澤型類数公式に現れる $\lambda_\pm, \mu_\pm$ はこの $\mathcal{L}_p^\pm(E/\mathbb{Q})$ の λ, μ -不変量として定義される。講演者は [19] において Selmer 群側でも Pollack の分解を実現し、2 つの “よい” Selmer 群 $\mathcal{X}^\pm(E/\mathbb{Q}_\infty)$ を定義した。この Selmer 群はねじれ加群となる。そして通常素点のときと同様に主予想を定式化した。

岩澤主予想 (超特異素点): $p \geq 5$ とする。特性イデアル $\text{Char}(\mathcal{X}^\pm(E/\mathbb{Q}_\infty))$ は Pollack の p -進 L -関数 $\mathcal{L}_p^\pm(E/\mathbb{Q})$ で生成される。

この予想は虚数乗法をもつ場合は [38] によって示され、一般の場合は講演者によって加藤のオイラー系を使うことで、 $(\mathcal{L}_p(E/\mathbb{Q})) \subset \text{Char}(\mathcal{X}(E/\mathbb{Q}_\infty))$ が示された。逆の包含関係は最近 X. Wan によって適当な仮定のもとで成り立つことがアナウンスされている ([54]). Wan の方法は Skinner-Urban と同じく保型形式の合同に基づくものであるが、これまでになかった新しい点がある。保型形式の合同理論は肥田理論などの変形理論に基づくもので、通常という仮定は決定的な役割を果たす。(非通常の場合も Coleman による理論はあるが、通常のとときと比べてかなり弱い合同性しかもたず取り扱いが難しい。) そのような理由から超特異のときに Skinner-Urban の理論を単純に拡張するのは難しい。鍵となるアイデアは E に付随する保型形式 f と f より重さの大きい CM 形式 g の Rankin-Selberg 積 $f \otimes g$ を考えることである。 $f \otimes g$ の岩澤理論は f が通常か超特異にかかわらず、Panchiskin 型と呼ばれるものになる。Panchiskin 型のときは通常のとときと同じく Greenberg 型の素朴な岩澤主予想の定式化が可能となり、保型形式の合同理論との相性もよい。Wan はこの Rankin-Selberg 型の岩澤主予想を Skinner-Urban の理論と同様の方法(ただし設定は異なる)で示し、[27] で発見された Beilinson-Flach 元という新しいオイラー系を仲介させることで、Rankin-Selberg 型の岩澤主予想と上述の超特異楕円曲線の岩澤主予想を結びつけた。

上述の岩澤主予想では $p \geq 5$ という仮定がついていたが、これはより正確には $a_p(E) = 0$ という仮定で、 $p \geq 5$ で超特異還元をもつ $\mathbb{Q}$ 上の楕円曲線なら自動的にみたされるものである。ただし超特異でも $\mathbb{Q}$ 上でない場合や、重さの高い保型形式では、 $a_p = 0$ という仮定は一般的とはいえない。Pollack と講演者による方法をより一般の場合に拡張する試みも続けられている。(例えば [51], [26].)

3.2. 反円分 $\mathbb{Z}_p$ -拡大の場合

以下、 E は $\mathbb{Q}$ 上定義されているとし、 K は虚二次体とする。虚二次体には $\mathbb{Z}_p$ -拡大が無限個存在し、すべての $\mathbb{Z}_p$ -拡大の合併は $\mathbb{Z}_p^2$ -拡大になる。その中でも環類体方向である反円分拡大が、Heegner 点や虚数乗法論との関わりで重要な役割を果たす。また前節の円分拡大のときの Skinner-Urban や Wan の結果も、適当な虚二次体をとって多変数の岩澤理論を展開することで、反円分拡大の岩澤理論を利用している。反円分拡大の岩澤

理論は様々な設定と話題がある. その中でも Bertolini-Darmon [3] は反円分拡大の岩澤理論の金字塔というべきもので, 結果だけでなく, その手法は現在でも大きな影響力をもっている. [3] 以後の反円分岩澤理論の展開としては, [12] を出発点として H. Darmon らによって, 多くの研究者を巻き込む形で始められた対角 cycle の話題がある. 前述の Beilinson-Flach 元という新しいオイラー系もこの流れで発見された. 現時点の岩澤理論の最もアクティブな話題は, 対角 cycle とそれに関連する保型形式の 3 重積 L -関数の岩澤理論 (とその周辺) である. 対角 cycle の岩澤理論は Heegner 点の岩澤理論, とくに Bertolini-Darmon-Prasanna による一般 Heegner cycle の理論 [4] と深い関わりがある. 実際, 対角 cycle で使われている技法は [4] をモデルとしている. ここではこれらの仕事の原点というべきもので, 講演者の仕事とも関わりが深い Heegner 点の岩澤理論について述べる. より詳しい解説記事としては [22] がある.

E の導手を N とすると志村-谷山予想の解決により, モジュラー曲線 $X_0(N)$ から定数でない射 $\pi : X_0(N) \rightarrow E$ がある. $X_0(N)$ は楕円曲線のモジュライ空間になっているので, $X_0(N)$ の点は楕円曲線に対応する. そして CM 楕円曲線に対応する $X_0(N)$ の点が Heegner 点である. もう少し詳しく述べると, まず虚二次体 K を固定する. K の導手 c の order $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ を考え, $\text{End } A = \mathcal{O}_c$ となる CM 楕円曲線 A_c をとる. A_c は環類体 H_c 上定義される. ($c = 1$ の場合がヒルベルト類体.) また Heegner 条件 (N の素因子が K で分裂) を課すと, A_c は CM 作用で不変的な $\Gamma_0(N)$ -レベル構造もつ. このとき A_c とこのレベル構造の組は, $X_0(N)$ の H_c -有理点を定め, これを導手 c の Heegner 点という. また π により Heegner 点を $E(H_c)$ に送ったものも Heegner 点という. 反円分拡大 K_∞/K は $H_\infty := \bigcup_n H_{p^n}$ に含まれる唯一の K の $\mathbb{Z}_p$ -拡大である. これより導手が p -ベキの Heegner 点から, $E(K_n)$ の有理点 z_n を作ることができる. Cornu-Vatsal によって, 十分大きな n に対しては z_n は $E(K_n)$ の非ねじれ元であることが知られている. ([10], [52].) z_n が $\mathbb{Z}_p[\text{Gal}(K_n/K)]$ -加群として生成する $E(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の部分群を $\mathcal{H}_n$ とおく. このとき $\mathcal{H}_n$ が $E(K_n)$ の中に占める割合に興味がある. z_0 が $E(K)$ のねじれ元でないならば, Gross-Zagier 公式と E/K の Birch and Swinnerton-Dyer 予想から, $E(K)/\mathbb{Z}z_0$ は有限で, その p -Sylow 部分群の位数は, 簡単な因子を除けば $\text{III}(E/K)[p^\infty]$ の位数の平方根に等しいことが予想されている. p が通常るとき, この予想を n に関する族にしたものが, 80 年代後半に Perrin-Riou [40] によって定式化された Heegner 点の岩澤主予想というべきものである. 以下詳しく述べる.

$\mathcal{X}_\infty$ を E/K_∞ の p -Selmer 群の Pontryagin 双対とする. $\mathcal{S}_\infty$ を E/K_∞ のコンパクト p -Selmer 群のノルムに関する射影系とする. すなわち $\mathcal{S}_\infty = \varprojlim_n \text{Sel}(K_n, T_p E)$. これは Kummer 写像により $\varprojlim_n E(K_n) \otimes \mathbb{Z}_p$ を自然に含んでおり, $\text{III}(E/K_n)[p^\infty]$ の有限性を認めるなら, $\mathcal{S}_\infty = \varprojlim_n E(K_n) \otimes \mathbb{Z}_p$ である. また $\Lambda := \mathbb{Z}_p[[\text{Gal}(K_\infty/K)]]$ とおく. ここで E が p で良通常還元を持つと仮定すると, $\mathcal{H}_\infty := \varprojlim_n \mathcal{H}_n$ は Cornut-Vatsal により Λ -加群として自由階数 1 となる.

Heegner 点の Perrin-Riou 予想: E は p で良通常還元をもち, pN の素因子は K で分解すると仮定する. このとき

- i) $\mathcal{S}_\infty$ はねじれのない自由階数 1 の Λ -加群.
- ii) ある有限生成 Λ -ねじれ加群 $\mathcal{M}$ に対し, $\mathcal{X}_\infty \sim \Lambda \oplus \mathcal{M} \oplus \mathcal{M}$ (擬同型).

iii) (岩澤主予想) $\text{Char}(\mathcal{M}) = \text{Char}(\mathcal{S}_\infty/\mathcal{H}_\infty)$.

i) は E の Mordell-Weil 群が Λ -族としては階数 1 であることを言っている. これは $E(K)$ の階数が不規則な振る舞いをするのと比較して, 岩澤理論化したことで, 階数が 1 という規則的な振る舞いになったことを意味する. ii) は Selmer 群の Λ -族は, Mordell-Weil 部分が Λ -階数 1 で, Tate-Shafarevich 部分が $\mathcal{M}^2$ であり, Tate-Shafarevich 群の Λ -族は, 有限性の類似である “ねじれ加群” で, その “位数は平方数” であることを意味している. そして iii) は Heegner 点の Λ -族の指数は Tate-Shafarevich 群の Λ -族の “位数の平方根” であるといっている.

この予想に関しては 2000 年代初頭に Heegner 点のオイラー系を使って, B. Howard が [16] において, 比較的マイルドな仮定のもと $\text{Char}(\mathcal{M}) \supset \text{Char}(\mathcal{S}_\infty/\mathcal{H}_\infty)$ を示した. 逆方向の包含関係は最近になって, 前述の X. Wan による Rankin-Selberg 型の岩澤主予想の進展により, 大きな前進がみられた. (厳密には上の設定と Wan の設定は異なり共通条件は空集合.) この保型形式の合同を使う方法においては, p -進 L -関数との関係が重要である. 岩澤主予想には大きく分けて 2 つのタイプの同値な定式化があると信じられている. 一つはこれまで説明した p -進 L -関数を使った定式化で, もう一つは円単数, 楕円単数, 加藤オイラー系, Heegner 点など, K -群の元や代数的サイクルといったいわゆるゼータ元を使った定式化である. Perrin-Riou 予想が岩澤主予想ならば p -進 L -関数を使った定式化も期待されるのだが, 定式化されたのはここ 4, 5 年の話で, F. Castella ([5], [6]) によって Bertolini-Darmon-Prasanna の p -進 L -関数 ([4]) と結びつける形で行われた.

Castella による反円分岩澤予想: $K \hookrightarrow \mathbb{C}_p$ を固定する. E は p で良還元をもち, pN の素因子は K で分解すると仮定する. $\mathcal{X}_{0,0}(E/K_\infty)$ を反円分 Selmer 群の双対で, p の上にある K 上の二つの素点における局所条件が, 一つは全体, もう一つは 0 とする. このとき $\mathcal{X}_{0,0}(E/K_\infty)$ は有限生成ねじれ Λ -加群で, その特性イデアルは Bertolini-Darmon-Prasanna の p -進 L -関数の平方で生成される.

Castella によりこの予想は Perrin-Riou 予想と同値であることが知られている. オイラー系から示される包含関係は Perrin-Riou の定式化, Wan の仕事と関係する保型形式の合同を使った包含関係は Castella の定式化と相性がよい.

Perrin-Riou 予想は通常素点の話であったが, Castella-Wan [9] は超特異素点においても講演者の [19] のアイデアに基づいて, Heegner 点を二つに分解することで, いわゆる $\pm$ -Perrin-Riou 予想を定式化し通常素点と同様の結果を得ている. これに対し注目すべきことは Castella による反円分岩澤予想で, こちらは通常素点でも超特異素点でもまったく同じ形で定式化されている. これは円分拡大のときの Wan の仕事と同じ着眼点で, E は超特異だが, 実は考えている岩澤理論は E を無限次反円分指標で twist したものになっており, Panchiskin 型になっているからである. よって Greenberg 型の岩澤主予想の素朴な定理化がうまくいっているわけである. (BDP の p -進 L -関数は超特異でも Λ の元.) 講演者と慶応大学の太田和惟は, 重さが 2 以上の保型形式で p で非通常の場合に, Castella 型の反円分岩澤予想の半分の包含関係を示した. ([21], [22]. 通常素点の場合は Castella-Hsieh[8] によって得られていた.) [21], [22] では [19] によって始められたプラ

ス/マイナス岩澤主予想のアイデアは使わない. とくに $a_p = 0$ という仮定もいらない. これは超特異だが Panchiskin 型なので, プラス/マイナス技法までは必要ないという理由である. ただし証明には [4] の一般 Heegner cycle のオイラー系を使い, このオイラー系の p -ベキ方向の振る舞いは通常か非通常でまったく異なり, 通常のとときと同様にはいかない. そこで [21], [22] では新しく integral Perrin-Riou twist という理論を開発した. この技法は他の場合にも有用と思われ, 実際, [28] の中で同種のものが考えられている.

4. Birch and Swinnerton-Dyer 予想の現状

楕円曲線の岩澤理論は Birch and Swinnerton-Dyer 予想と関係が深い. また講演者のささやかな貢献もあるので最後にそれを述べる. ただし BSD 予想の現状を網羅的に述べるには余白がせますぎるので, 目立った結果のみを簡単に触れるだけにとどめたい.

Birch and Swinnerton-Dyer 予想:

$$(i) \quad \text{ord}_{s=1} L(E/\mathbb{Q}, s) = \text{rank } E(\mathbb{Q}).$$

$$(ii) \quad r = \text{ord}_{s=1} L(E/\mathbb{Q}, s) \text{ とおくと,}$$

$$\frac{1}{r!} \frac{d^r}{ds^r} L(E/\mathbb{Q}, s)|_{s=1} = \frac{\#\text{III}(E/\mathbb{Q}) \prod_{\ell|\Delta} c_\ell}{\#E(\mathbb{Q})_{\text{tor}}^2} \cdot \Omega_E \cdot \text{Reg}_\infty(E).$$

ここで c_ℓ は各素数 ℓ ごとに定まる局所玉河数と呼ばれる比較的簡単な量である. $E(\mathbb{Q})$ には Néron-Tate height pairing と呼ばれる 2 次形式があり, レギュレーター $\text{Reg}_\infty(E)$ はその 2 次形式の判別式である.

(i) が階数予想, (ii) は先頭項予想と呼ばれる. 代数体との類似では (i) が単数定理, (ii) が類数公式である. まず r が 2 以上かどうかで状況がまったく違うことに注意しておく. 数値計算等から一般的には $\text{rank } E(\mathbb{Q})$ は 0 か 1 かのどちらかであることがほとんどで, そのどちらになるかはルートナンバーで決まると信じられている. (数値計算データは例えば [2].)

$\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$ のときは Heegner 点を用いることで非自明な有理点を構成できる. このことから階数予想 (i) は $r \leq 1$ なら Tate-Shafarevich 群の有限性を含めて解決されている. (Gross-Zagier, Kolyvagin の結果.) 最近の進展としては, Gross-Zagier, Kolyvagin の逆と呼ばれる種類の研究がある. ([48], [58] など.) これは Selmer 群の階数が 1 ならば $\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$ というもので, 証明には反円分拡大の岩澤理論が使われている. とくに [4] や, [3] の技法が重要な役割を果たす.

階数が 2 以上のときは例外的な場合で, 有理点の組織的な構成は期待できない. 階数 2 以上でも知られていることは, Tate-Shafarevich 群の有限性を認めれば, (i) が mod 2 で正しいということである. (例えば [11], [34].) これは階数の偶奇を表すルートナンバーがガロワ表現的に捉えられることが大きい. 階数が 2 以上のとき, (i), (ii) に関して無条件で証明されている例はひとつもない.

最近の最も大きな進展は $r \leq 1$ の場合の (ii) の先頭項予想である．まず $r = 0$ のときは (ii) は

$$\frac{L(E/\mathbb{Q}, 1)}{\Omega_E} = \frac{\sharp \text{III}(E/\mathbb{Q}) \prod_{\ell|\Delta} c_\ell}{\sharp E(\mathbb{Q})_{\text{tor}}^2}$$

と書け，両辺は有理数なので，符号と任意の素数 p に対して p -進付値を比較する問題になる．そして両辺の p -進付値が等しいことは岩澤主予想から従う．よって Skinner-Urban [49], Skinner [47], Wan [54] らの岩澤主予想の仕事によって多くの p について確かめられている．

$r = 1$ のときも同様に，(ii) は

$$\frac{L'(E/\mathbb{Q}, 1)}{\Omega_E \text{Reg}_\infty(E)} = \frac{\sharp \text{III}(E/\mathbb{Q}) \prod_{\ell|\Delta} c_\ell}{\sharp E(\mathbb{Q})_{\text{tor}}^2} \quad (1)$$

と書き換えられる．Gross-Zagier, Kolyvagin の結果により，左辺も右辺も well-defined な有理数となる．よってやはり符号と任意の素数 p に対して p -進付値を比較する問題になる．この場合は岩澤主予想だけでは不十分である．岩澤理論はあくまで p -進の理論なので，微分も p -進的なものであり， p -進 L -関数の微分値は扱っても複素解析的な微分値 $L'(E/\mathbb{Q}, 1)$ は扱えないからである．ただし Gross-Zagier 公式と p -進 Gross-Zagier 公式の両方があると，Heegner 点を經由して複素の微分値と p -進の微分値が比較でき，この問題にアプローチすることができる．このアプローチは p が通常の場合は，Perrin-Riou [39] に遡るが，当時は岩澤主予想が未解決であったことや p -進高さの非自明性の問題があって，忘れ去られていたようである．講演者は超特異な p に対し (円分) p -進 Gross-Zagier 公式を示し，岩澤主予想が成り立てば式 (1) の両辺の p -進付値が等しいことを示した ([20])．超特異の場合は幸運にも p -進高さの非自明性の問題がなかった．とくに虚数乗法をもつ場合や，Wan により主予想が示されている p に対しては，式 (1) の両辺の p -進付値が等しいことがわかる．通常素点の場合は円分 p -進高さの非自明性の問題があるため，このアプローチは困難と思われたが，反円分拡大の岩澤理論の技術を持いて，[13], [58], [7] において通常素点 p に対しても，多くの場合に式 (1) の両辺の p -進付値が等しいことが示された． p に課された詳しい条件はこれらの論文を参照していただきたい．結果として，例えば $r = 1$ の semi-stable な楕円曲線に対しては，(ii) はほとんど示されていると言ってよいだろう．

参考文献

- [1] Y. Amice, J. Vlu: Distributions p -adiques associes aux sries de Hecke. Journes Arithmtiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), pp. 119–131. Asterisque, Nos. 24-25, Soc. Math. France, Paris, 1975.
- [2] J. Balakrishnan, W. Ho, N. Kaplan, S. Spicer, W. Stein, J. Weigandt Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks, preprint, <https://arxiv.org/abs/1602.01894>
- [3] M. Bertolini, H. Darmon, Iwasawa’s main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$ -extensions. Ann. of Math. (2) 162 (2005), no. 1, 1–64.
- [4] M. Bertolini, H. Darmon, K. Prasanna, Generalized Heegner cycles and p -adic Rankin L -series. With an appendix by Brian Conrad. Duke Math. J. 162 (2013), no. 6, 1033–1148.

- [5] F. Castella, On the p -adic variation of Heegner points, PhD thesis, McGill, 2013.
- [6] F. Castella, p -adic heights of Heegner points and Beilinson-Flach classes. *J. Lond. Math. Soc.* (2) 96 (2017), no. 1, 156–180.
- [7] F. Castella, On the p -part of the Birch-Swinnerton-Dyer formula for multiplicative primes. *Camb. J. Math.* 6 (2018), no. 1, 1–23.
- [8] F. Castella, M-L. Hsieh, F. Castella, M-L. Hsieh, Heegner cycles and p -adic L-functions. *Math. Ann.* 370 (2018), no. 1-2, 567–628.
- [9] F. Castella, X. Wan, Iwasawa Main Conjecture for Heegner Points: Supersingular Case, preprint.
- [10] C. Cornut, Mazur’s conjecture on higher Heegner points. *Invent. Math.* 148 (2002), no. 3, 495–523.
- [11] T. Dokchitser, V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math.* (2) 172 (2010), no. 1, 567–596.
- [12] H. Darmon, V. Rotger, Diagonal cycles and Euler systems I: A p -adic Gross-Zagier formula. *Ann. Sci. Éc. Norm. Supér.* (4) 47 (2014), no. 4, 779–832.
- [13] D. Jetchev, C. Skinner, X. Wan, The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. *Camb. J. Math.* 5 (2017), no. 3, 369–434.
- [14] R. Greenberg, Iwasawa theory -past and present. *Class field theory-its centenary and prospect* (Tokyo, 1998), 335–385, *Adv. Stud. Pure Math.*, 30, Math. Soc. Japan, Tokyo, 2001.
- [15] B. Gross, D. Zagier, Heegner points and derivatives of L-series. *Invent. Math.* 84 (1986), no. 2, 225–320.
- [16] B. Howard, The Heegner point Kolyvagin system, *Compos. Math.* 140 (2004), no. 6, 1439–1472.
- [17] K. Iwasawa, On Γ -extensions of algebraic number fields. *Bull. Amer. Math. Soc.* 65 1959 183–226.
- [18] K. Kato, p -adic Hodge theory and values of zeta functions of modular forms. *Cohomologies p -adiques et applications arithmétiques. III. Astérisque No. 295* (2004), ix, 117–290.
- [19] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.* 152 (2003), no. 1, 1–36.
- [20] S. Kobayashi, The p -adic Gross-Zagier formula for elliptic curves at supersingular primes. *Invent. Math.* 191 (2013), no. 3, 527–629.
- [21] S. Kobayashi, A p -adic interpolation of generalized Heegner cycles and integral Perrin-Riou twist, preprint, submitted.
- [22] 小林真一, 円分拡大の岩澤理論と一般 Heegner サイクル, RIMS 講究録別冊, 「代数的整数論とその周辺 2016」に投稿中.
- [23] 小林真一, p 進バーチ-スィンナートン・ダイヤー予想と岩澤理論的現象, 現象を通して見る岩澤理論, 数学セミナー 2018 年 1 月号.
- [24] S. Kobayashi, K. Ota, Anticyclotomic main conjecture for modular forms and integral Perrin-Riou twists, preprint, submitted.
- [25] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I. *Invent. Math.* 149 (2002), no. 1, 195–224.
- [26] A. Lei, D. Loeffler, S. Zerbes, Wach modules and Iwasawa theory for modular forms. *Asian J. Math.* 14 (2010), no. 4, 475–528.
- [27] A. Lei, D. Loeffler, S. Zerbes, Euler systems for Rankin-Selberg convolutions of modular forms. *Ann. of Math.* (2) 180 (2014), no. 2, 653–771.
- [28] D. Loeffler and S. L. Zerbes, Rankin-Eisenstein classes in Coleman families, *Res. Math. Sci.* 3 (2016), Paper No. 29, 53.

- [29] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18 (1972), 183–266.
- [30] B. Mazur, Modular curves and arithmetic. *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Warsaw, 1983), 185–211.
- [31] B. Mazur, P. Swinnerton-Dyer, Arithmetic of Weil curves. *Invent. Math.* 25 (1974), 1–61.
- [32] B. Mazur, J. Tate and J. Teitelbaum, On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* 84 (1986), no. 1, 1–48.
- [33] A. G. Nasybullin, p -adic L -series of supersingular elliptic curves. *Funkcional. Anal. i Priložen.* 8 (1974), no. 1, 82–83.
- [34] J. Nekovář, A. Plater, On the parity of ranks of Selmer groups. *Asian J. Math.* 4 (2000), no. 2, 437–497.
- [35] 落合理, 岩澤理論の高次元化をとりまく風景, 第60回代数学シンポジウム, http://mathsoc.jp/section/algebra/algsymp_past/algsymp15.html
- [36] 落合理, 岩澤理論とその展望(上), (下), 岩波数学叢書, 岩波書店.
- [37] R. Pollack, On the p -adic L -function of a modular form at a supersingular prime. *Duke Math. J.* 118 (2003), no. 3, 523–558.
- [38] R. Pollack, K. Rubin, The main conjecture for CM elliptic curves at supersingular primes. *Ann. of Math.* (2) 159 (2004), no. 1, 447–464.
- [39] B. Perrin-Riou, Points de Heegner et dérivées de fonctions L p -adiques. *Invent. Math.* 89 (1987), no. 3, 455–510.
- [40] B. Perrin-Riou, Fonctions L p -adiques, théorie d’Iwasawa et points de Heegner. *Bull. Soc. Math. France* 115 (1987), no. 4, 399–456.
- [41] B. Perrin-Riou, Théorie d’Iwasawa p -adique locale et globale. *Invent. Math.* 99 (1990), no. 2, 247–292.
- [42] B. Perrin-Riou, Théorie d’Iwasawa des représentations p -adiques sur un corps local, *Invent. Math.* 115 (1994), 81–149.
- [43] B. Perrin-Riou, Fonctions L p -adiques des représentations p -adiques. *Astérisque* No. 229 (1995), 198 pp.
- [44] B. Perrin-Riou, Arithmétique des courbes elliptiques à réduction supersingulière en p . *Experiment. Math.* 12 (2003), no. 2, 155–186.
- [45] D. Rohrlich, On L -functions of elliptic curves and cyclotomic towers. *Invent. Math.* 75 (1984), no. 3, 409–423.
- [46] K. Rubin, The “main conjectures” of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* 103 (1991), no. 1, 25–68.
- [47] C. Skinner, Multiplicative reduction and the cyclotomic main conjecture for GL_2 . *Pacific J. Math.* 283 (2016), no. 1, 171–200.
- [48] C. Skinner, A converse to a theorem of Gross, Zagier, and Kolyvagin, preprint.
- [49] C. Skinner, E. Urban, The Iwasawa main conjectures for GL_2 . *Invent. Math.* 195 (2014), no. 1, 1–277.
- [50] シュプルング フローリアン, 楕円曲線の岩澤理論について, 第6回城崎新人セミナー報告集, <https://www.math.kyoto-u.ac.jp/insei/>
- [51] F. Sprung, Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures. *J. Number Theory* 132 (2012), no. 7, 1483–1506.
- [52] V. Vatsal, Special values of anticyclotomic L -functions. *Duke Math. J.* 116 (2003), no. 2, 219–261.
- [53] M. Višik, Nonarchimedean measures associated with Dirichlet series. *Mat. Sb. (N.S.)* 99

(141) (1976), no. 2, 248–260, 296.

- [54] X. Wan, Iwasawa Main Conjecture for Supersingular Elliptic Curves.
- [55] X. Wan, Iwasawa Main Conjecture for Rankin-Selberg p -adic L-functions: Non-Ordinary Case, preprint.
- [56] X. Wan, Iwasawa Main Conjecture for Rankin-Selberg p -adic L-functions, preprint.
- [57] X. Wan, Heegner Point Kolyvagin System and Iwasawa Main Conjecture, preprint.
- [58] W. Zhang, Selmer groups and the indivisibility of Heegner points. *Camb. J. Math.* 2 (2014), no. 2, 191–253.