

モジュラー楕円曲線とフェルマーの最終定理

Andrew Wiles

序文

\mathbb{Q} 上の楕円曲線は、形式 $X_0(N)$ のモジュラー曲線で有限被覆ならば、モジュラーである。そのような任意の楕円曲線は、その Hasse-Weil ゼータ関数が解析接続を持ち、標準型の関数等式をみたすという特徴を持つ。与えられた j -不変量を持つ \mathbb{Q} 上の楕円曲線がモジュラーならば、同じ j -不変量を持つすべての楕円曲線はモジュラーである（これを、 j -不変量はモジュラーであるという）ことが容易に判る。1950 年代のおよび 1960 年代の、有名な志村と谷山による予想は \mathbb{Q} 上のすべての楕円曲線はモジュラーであると主張する。しかしながら、この予想は Weil の 1967 年の論文が出版されてようやく広く知られるようになった。Weil はその論文の中で、予想の概念的な証拠を与えた。多くの場合に数値的に確かめられたが、この論文の結果ができるまでは、多くのしかし有限な j -不変量がモジュラーであることが知られていたにすぎない。

1985 年、Frey は、この予想がフェルマーの最終予想を意味すると見抜いた。両者の厳密な関連のメカニズムについては、Serre が ε -予想として定式化した¹が、1986 年夏 Ribet がそれを証明した。Ribet の結果は、フェルマーの最終定理の証明を導くには、半安定な楕円曲線に対して予想が証明されればよいというものであった。

われわれは、ガロア表現と結びつけて楕円曲線を研究する。 ρ_p は \mathbb{Q} 上の楕円曲線の p -分割点における $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ の表現であるとする。またしばらく、 ρ_3 は既約であるとする。 ρ_3 が既約ならば、それはまたモジュラーであるという Langlands と Tunnell の決定的に重要な定理のために、3 の選択は決定的である。

われわれは、他の素数での ρ_3 の分岐に対してある柔軟な制限を行って、 ρ_3 が 3 で半安定であるという仮定の下で、 ρ_3 のすべての適切な持ち上げはモジュラーであることを示す必要がある。そのためには、可換代数からの幾つかの新しい議論によって、この問題をよく知られたタイプの類数問題に結び付けて考えなければならない。[TW] とともに我々はこの問題を解決した。このことは、よく知られているように、同伴 3 進表現がモジュラーのときそのときに限り E はモジュラーであるという、 E のモジュラリティーを証明するに十分である。

議論の展開のキーは、数論における異なった二つの強い流儀の間の新しく驚異的な結びつきである。一方に、ガロア表現とモジュラー形式、他方に L 関数の特殊値の解釈。前者はもちろんより最近のものであるが。1950 年代および 1960 年代の Eichler と志村のオリジナルな結果に続いて、1980 年までの間に、Deligne、Serre、Langlands によって他の主要定理が証明された。これらの結果には、モジュラー形式に同伴するガロア表現の構築、Deligne と Langlands の予想の精密化（後に Carayol が与えた）や、重み 1 のときの逆結果を与える底変換 (base change^{*1}) の方法の Langlands の厳格な応用が含まれる。かなり特別な重み 1 の例外的場

*1 「モチーフに関する最も簡単な operation はより大きな定義体へ渡すこと (base change すること) である。 F 上のガロア群或は Weil 群の表現のモチーフでは、base change は、単に E 上のガロア或は Weil 群への制限である。」(R.P.Langlands, "Base

合の結果で、Langlands のオリジナルの定理の Tunnell による拡張を含む、モジュラー形式をガロア表現に直接に結びつける議論の発展はなかった。1980 年代半ばから、その分野の主な推進の動機は、 ε 予想を以前にもまして精巧に仕上げようという Serre の諸予想によって与えられた。この問題に関する Ribet や他の研究者の研究の他に、1980 年代のさらに特別な発展の幾つか、とりわけ肥田や Mazur の研究、を用いなければならない。

2 番目の流儀 (L 関数の特殊値に関する流儀) は、Dirichlet の有名な解析的類数の定理にまで遡るが、その現代版 Birch-Swinnerton-Dyer 予想によるものである。実際には、われわれのおこなう分野においては、岩澤のアイデアによるものであって、かなりの程度までわれわれはそれを改変した (おきかえをおこなった)。Galois cohomology の原理、特に Poitou と Tate の基本定理はまた、ここで重要な役割を果たす。

ρ_3 は 3 で既約であるという制限は、 ρ_5 と共約を有する楕円曲線族の興味深い議論によって回避できる。このことを使って、われわれは、すべての半安定な楕円曲線はモジュラーであることを証明した。これは結果的に Fermat の最終定理の証明を与える。さらに、この方法は、 \mathbb{Q} 上のすべての楕円曲線はモジュラーであるという定理の証明、また、それを別の総実数体へ一般化するという証明のための十分適切な設定であると思う。さて、ここで、われわれの方法と結果についての詳細について説明しよう。

f を重み $k \geq 2$ 、指標 χ の $SL_2(\mathbb{Z})$ の合同部分群 $\Gamma_1(N)$ に関する固有形式とする。したがって、 T_n を整数 n に関する Hecke 作用素とすれば、各 n に対して $T_n f = \{c(n, f)\}$ であるような代数的整数 $c(n, f)$ が存在する。 K_f を $c(n, f)$ とともに χ で \mathbb{Q} 上で生成された数体とする。そして \mathcal{O}_f はその整数環とする。 \mathcal{O}_f の任意の prime λ に対して、 $\mathcal{O}_{f,\lambda}$ は λ での \mathcal{O}_f の完備化 (完備拡大) である。次の定理は ($k = 2$ に対して) Eichler と志村そして ($k > 2$ に対して) Deligne による。 $k = 1$ のときに対しては、Serre と Deligne のすばらしい定理の結果からの類似であるが、複素表現を使ってより自然な形で述べた。その場合の像は有限であり、逆にについては多くの場合に知られている。

定理 01 各素数 $p \in \mathbb{Z}$ および \mathcal{O} の各 prime $\lambda|p$ に対して、 Np を割る素数を除けば不分岐な連続表現

$$\rho_{f,\lambda} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathcal{O}_{f,\lambda})$$

が存在する。そして、すべての素数 $q \nmid Np$ に対して、

$$trace \rho_{f,\lambda}(Frob q) = c(q, f), \quad \det \rho_{f,\lambda}(Frob q) = \chi(q)q^{k-1}.$$

が成り立つ。

逆方向にこの結果を証明する、すなわち、 λ 進表現がそのようにしてモジュラー形式から生じるというもとの基準 (criteria) を立てることによって結果の証明を試みる。その表現が λ 進表現と両立系 (compatible system) の一部であると仮定しても^{*2}、他のものより或る λ に対しては証明が容易になるということ以外、何らのメリットも見いだせなかった。

$$\rho_0 : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\bar{\mathbb{F}}_p)$$

は標数 p の代数的閉包に値をもつ連続表現であり、 $\det \rho_0$ は奇であるとする。 f と λ に対して ρ_0 と $\rho_{f,\lambda}$ は λ を法として $\bar{\mathbb{F}}_p$ 上同型であり、 $\bar{\mathbb{F}}_p$ における \mathcal{O}_f/λ の或る埋め込みであるとき、 ρ_0 はモジュラーである

change for $GL(2)$)

*2 [訳註] 位相の微分化?

という。Serre は行列式の値が奇の全ての既約表現 ρ_0 はモジュラーであると予想した。この予想に関して、 $PGL_2(\bar{\mathbb{F}}_p)$ における ρ_0 の像が正 2 面体、 A_4 あるいは S_4 のときを除いて、知られていることは殆どない。正 2 面体のとき予想は成り立つ。本質的には Hecke による。 A_4 あるいは S_4 のときもまた予想は成り立つ。第 1 に Langlands, 1 つの重要な場合については Tunnell による。より厳密に述べれば、これらの予想は、重み 1 の形式を、対応する複素表現に結びつける。しかし、われわれの必要とするのは、複素表現からの直接の簡約である。可約な場合でも、我々が述べたような形での問題に関して、そう多くのことが知られているわけではない。そういう場合には、 $\overline{\rho_{f,\lambda}} = \rho_{f,\lambda} \bmod \lambda$ の半単純化が $K_{f,\lambda}^2$ における束の選択と独立であるのみに注意深く束を選ばねばならない。

もし \mathcal{O} が局所体 (\mathbb{Q}_p を含む) の整数環ならば、 $\bar{\mathbb{F}}_p$ における \mathcal{O} の特殊な埋め込みに対して、 $\bar{\rho}$ と ρ_0 が $\bar{\mathbb{F}}_p$ 上同型るとき、 $\rho: Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathcal{O})$ を ρ_0 の持ち上げという。われわれの観点からは、 ρ_0 はモジュラーであると仮定し、そのもとで、 ρ_0 の持ち上げ表現 ρ は、或る f, λ に対して $\overline{K_{f,\lambda}}$ 上同型 $\rho \sim \rho_{f,\lambda}$ であるという意味でモジュラー形式から生じるという条件を与えるつもりである。次の 2 つの場合に限って考えることとする。

- (I) p での分解群のもとで安定、その商空間への作用が不分岐でありまたその部分空間への作用と異なっているような、 $\bar{\mathbb{F}}_p^2$ の 1 次元部分空間が存在するという意味で、 ρ_0 は (p で) 通常表現である。
- (II) p での分解群の表現として、 ρ_0 は Z_p 上の有限平坦群スキームから生じるものの一つと同値であるという意味で、 ρ は (p で) 平坦である。そして p で慣性群に制限された $\det \rho_0$ は円分体の指標である。

$\bar{\mathbb{Q}}_p^2$ への表現としてみれば、 p での分解群のもとで安定な、そして商空間への作用が不分岐であるような、 $\bar{\mathbb{Q}}_p^2$ の 1 次元部分空間が存在するとき、 ρ は、同じく、(p で) 通常表現であるという。

$\varepsilon: Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{Z}_p^\times$ は円分指標を表すとする。定理 0.1 の逆については、証拠はないが、長年成り立つものと予想されてきた。関数体の場合に、Drinfeld は、両立系 (compatible system) なしで済むかもしれないという重要なアイデアをすでに研究していた。 p での分解群への制限に関する幾何学的条件さえあればいいというアイデアを最初に示したのは Fontaine と Mazur である。次の予想は、Serre 予想の自然な拡張であり、われわれの結果を述べる時都合がよい。また、少し形を変えてあるが、Fontaine と Mazur が提示したものである。(この形では、予想は、Serre 予想と関連していない。我々は代わりに ρ_0 はモジュラーであるという仮説を置いた)。

予想 $\rho: Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{Z}_p^\times$ は ρ_0 の既約持ち上げであり、また ρ は素数の有限集合以外では不分岐であるとする。二つの場合が存在する。

- (i) ρ_0 は通常表現であるとする。そのとき、 ρ が通常表現であり、或る整数 $k \geq 2$ と有限指数の或る χ に対して、 $\det \rho = \varepsilon^{k-1} \chi$ が成り立てば、 ρ は或るモジュラー形式から生じる。
- (ii) ρ_0 は平坦であり、 p は奇素数であるとする。そのとき、 p で分解群に制限された ρ が p 可約群上の表現に等しければ、 ρ はまた或るモジュラー形式から生じる。

(ii) の場合は、もしそのような形式が存在すれば、それは重み 2 でなければならないということが簡単にわかる。もちろん (i) の場合では、それは重み k をもつ。この予想は、もちろん、(i) と (ii) における条件を弱めることで、 \mathbb{Q} の別な数体を考えることで、また GL_2 以外の群を考えることで、幾つかの方法でこの予想を拡大できる。

われわれは、この予想に関する 2 つの結果を証明する。第 1 のものは ρ_0 はモジュラーであるという仮説を

含んでいる．これより以降， p は奇素数であると仮定する．

定理 02 ρ_0 は既約であるとして，上記の (I) か (II) を満たすとする．また， ρ_0 はモジュラーであり，

- (i) ρ_0 は， $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ へ制限するとき，絶対既約である．
- (ii) $q \equiv -1 \pmod{p}$ が ρ_0 において分岐すれば， D_q は q での分解群として， $\rho_0|_{D_q}$ が代数的閉包上で可約であるか，あるいは， I_q は q での慣性群であるとして， $\rho_0|_{I_q}$ が絶対既約であるかどうかである．

をみたとすれば，予想における任意の表現 ρ は，実際まさにモジュラー形式から生じる．

実際，われわれの方法で唯一の本質的条件は， ρ_0 はモジュラーであるということである．

現時点で最も興味のあるケースは， $p = 3$ で， ρ_0 が \mathbb{F}_3 上で定義できる場合である．そのとき， $PGL_2(\mathbb{F}_3) \simeq S_4$ なのだから，上述した Langlands と Tunnell の定理によって，すべてのそのような表現はモジュラーである．特に，その簡約が与えられた条件をみたら， $GL_2(\mathbb{Z}_3)$ の中へのすべての表現はモジュラーである．次を得る．

定理 03 E は \mathbb{Q} 上で定義された楕円曲線であり，また ρ_0 は 3 分割点へのガロア作用であるとする． E は次の条件を満たすとする．

- (i) E は，3 で良い還元あるいは乗法的還元をもつ．
- (ii) ρ_0 は $\mathbb{Q}(\sqrt{-3})$ へ制限するとき，絶対既約である．
- (iii) 任意の $q \equiv -1 \pmod{p}$ に対して， $\rho_0|_{D_q}$ が代数的閉包上で可約であるか， $\rho_0|_{I_q}$ が絶対既約であるかどうかである．

そのとき， E はモジュラーである．

ゼータ関数の特性が定理 02 から直接従う一方で， E は $X_0(N)$ で被覆されるというより強い定理は，Faltings の証明した同種定理 (E が非整数 j 不変量もち，半安定な曲線を含む場合については，より以前に Serre により証明された) も要求することを指摘しておく． E がモジュラーならば， E の任意のツイストもモジュラーであり，条件 (i) をやや緩めることができるということを注意しておく．

重要な半安定曲線すなわち平方数の導手を持たない曲線の類は，(ii) は必ずしも満たさないが，(i) と (iii) をみたら．(ii) を満たさない場合は， ρ_0 は可約である．かなり意外ではあるが，5 分割点上の表現が，定理 03 でモジュラーであることが証明された別の楕円曲線に対しても生じることを示すことによって，定理 02 をこの場合にも適用できる場合がある．したがって，そのときには定理 02 は $p = 5$ で適用される．この議論は，第 5 章で説明するが，ガロア表現の変形ではなく楕円曲線の変形を実際に使う唯一の部分である．この議論は，半安定よりも一般的なケースでも成り立つが，この設定で次を得る．

定理 04 E を \mathbb{Q} 上で定義された半安定な楕円曲線であるとすれば， E はモジュラーである．

より一般的なモジュラー楕円曲線の族については第 5 章で述べる．

1986 年，Frey のアイデアに刺激されて，Serre が予想し Ribet が証明した，モジュラー形式と結びついた

ガロア表現の特性によって、定理 04 がフェルマーの最終定理の証明を意味することを Ribet が示した。Frey の指摘したことは、次の定理の意味で、(仮説的な) 楕円曲線 $y^2 = x(x+u^p)(x-v^p)$ はモジュラーでないということだった。そのような楕円曲線はすでに [He] で研究されていたが、モジュラー形式に結びついていなかった。Serre は、Frey の考えを厳密にして、この特殊な楕円曲線 (Frey 曲線) の p 分割点上の表現は、それがモジュラーであれば、導手 2 の形式と結びつくだらうというモジュラー形式に関する予想を提示した。簡単な洞察から、そのようなモジュラー形式は存在しない。1986 年の夏、Ribet は Serre 予想を証明した。しかしさらに、問題の楕円曲線はモジュラーでなければならないこと、このことは定理 04 から出てくることを知る必要がある。そして、われわれは遂に次の定理を得た。

定理 05 $u, v, w \in \mathbf{Q}$ および $p \geq 3$ のとき、 $u^p + v^p + w^p = 0$ とすれば、 $uvw = 0$ である。(同じことだが、 $n > 2$ のとき、 $a^n + b^n = c^n$ であるような、0 でない整数 a, b, c, n は存在しない。)

予想の証明の第 2 の結果は、 ρ_0 がモジュラーであるという仮定を要求しない(それを仮定するケースについてはすでに判っているのだから)。

定理 06 ρ_0 は既約表現であり、上記の (I) を含む、予想に関する仮定をみたとすれば、さらに

- (i) p で不分岐な \mathbf{Q} の虚二次拡大 L の標数 κ_0 に対して、 $\rho_0 = \text{Ind}_L^{\mathbf{Q}} \kappa_0$ である。
- (ii) $\det \rho_0|_{\Gamma_p} = \omega$.

をみたとすれば、予想におけるような表現 ρ は、まさに実際、モジュラー形式から生じる。

この定理はまた、或る楕円曲線族がモジュラーであることを証明するのに使われる。この要約では、ガロア表現と楕円曲線を結び付ける主要定理のみをのべた。一般的類群に関する結果については、定理 3.3 で述べられる。

以下は、この研究のそもそもの起こりについてと、影響を受けた 1980 年代のより特殊な発展に関する説明である。1986 年の夏の終りに、直接には Ribet の結果を習得するために、これらの問題の研究を始めた。数年の間、全実体に対する岩澤予想の研究とその幾つかの応用に従事していた。その過程で、それらを使ってヒルベルト・モジュラー形式と結びついた ℓ 進表現に関する結果を発展させた。そういうことで、 ℓ 進表現の観点からモジュラリティーの問題を考えることは自然なことだった。まず、与えられた通常 ℓ 進表現の簡約(還元)は可約であると仮定し、この仮定の下で、その表現自体がモジュラーであることを証明しようとした。かなり単純に、この設定で岩澤理論を適用できると考えていた。またさらに、 $\ell = 2$ の場合に、この設定は Frey 曲線の研究に十分な導きをすると楽観的に考えていた。今後主要な文脈では、岩澤理論との関係から ℓ の代わりに p を使うことにする。

2 進表現での研究を数ヶ月続けた後、代わりに 3 進表現を使えるのではないか—Langlands-Tunnell の定理は、 \mathbf{Q} 上の任意の与えられた楕円曲線の 3 を法とする表現 ρ_3 は必然的にモジュラーであると述べている—という、この問題の解決のための最初の実質的な突破口が開けた。このことが、各 n に対して、 $GL_2(\mathbf{Z}/3^n\mathbf{Z})$ 表現はモジュラーであるという証明の試みに私を導いた。この時点では、通常ケースのみを考えていた。この場合の研究から、 $i = 1, 2$ に対する、 $H^i(\text{Gal}(F_\infty/\mathbf{Q}), W_f)$ の研究にたちまち移った。ここで、 F_∞ は適当なモジュラー曲線のヤコービアン m 進ねじれ分裂体であり、 m は ρ_3 に同伴する Hecke 環の最大イデアルである。また、 W_f は第 1 章で述べられるモジュラー形式に同伴する加群である。さらに、特に、このコホモロ

ジーを同じ加群に作用する $Gal(\mathbb{Q}_\Sigma/\mathbb{Q})$ のコホモロジーと比較する必要があった。

この問題に岩澤理論の適用を試みた。全実体に対する岩澤予想の証明のなかで、私は、自明な零点を扱うための新しいテクニックを導入したが、それは、 \mathbb{Z}_p 円分拡大体を考える標準の岩澤理論を無限に多くの異なる素数 $q_i \equiv 1 \pmod{p^{n_i}}$ ($i \rightarrow \infty$ のとき $n_i \rightarrow \infty$) の選択に基づく同様の解析に置き換えることを含む。この方法は、見方によっては、標準の岩澤理論に対して、 W_f を研究する場合の枠 (problematic) として考えられる方法を選択することは、体 \mathbb{Q} を固定して、 Σ が変わるときのコホモロジー群を比較することなのかも知れないということを示唆している。粗っぽくいえば、新たな原理は、従順に分岐するコホモロジー類によって不分岐なコホモロジー類を捕捉 (捕獲) することができるということである。論文 [Gre1] を読んだ後、Poitou と Tate の Galois コホモロジーについての双対定理は、この問題に対して役に立ちそうだと考えた。この定理 (Poitou-Tate) の厳密な要旨は第 1 章第 2 節で述べる。

これらの考えを実行するために、第 2 章の初めの 2 つの節で述べられたテクニックを開発していた。この研究は、特に、 f と様々なレベルのモジュラー形式の間のすべての合同の詳細な研究、この理論は肥田と Ribet によりはじめられていた、を必要とした。次の 2 つの仮定の下で、第 1 のコホモロジー群の良い評価ができたことが収穫だった。第 1 の仮定は、第 2 のコホモロジー群の或部分群は消滅するというものであり、第 2 の仮定は、形式 f は、 m に対して、ミニマル・レベルで選ばれるというものである。これらの仮定は、少なくとも正しい方向を向いているにしても、実際的な効果を持つには制限が厳しすぎた。これらの議論の幾つかは、第 1 章第 2 節にある。また、幾つかは第 3 章の議論への第 1 の弱い近似を成す。その時点では、しかし、([Ri1] におけるレベルの簡約の議論は、 $q \equiv 1 \pmod{p}$ のときはさらにずっと難しいという理由のために) 素数 $q \equiv 1 \pmod{p}$ に対しては一般には適用されない、幾何学的テクニックとして私の研究で使っていた Σ が変わるときの auxiliary primes $q \equiv -1 \pmod{p}$ を使っていた。この研究の全てにおいて、 $p = -3$ という前提よりも ρ_p はモジュラーであるというより一般的な前提を使った。

1980 年代の後半、私は、これらのアイデアを環論の言葉に翻訳した。数年前に、肥田は、幾つかのガロア表現の明示的な 1 パラメータ族を構成していた。この (肥田の) 研究を理解するための研究の過程で、Mazur は、ガロア表現の変形の言葉 (理論) を開発した。さらに、Mazur は、彼の見つけた普遍変形環は、少なくともある特別な場合には、Hecke 環であることをつきとめた。この重要な予想は、モジュラー表現のすべての通常持ち上げ (ordinary liftings) はモジュラーであるという期待を強めた。この環論への翻訳の過程で、必要とされた H^2 の部分群に関する消滅の仮定をその Hecke 環が完全交叉でなければならないというより強い条件に置き換えねばならないことが分かった。この条件は、ジェネレータの数と関係性を評価するそれらの変形環の存在と十分適合する。それで、仮定をもっと現実的なものにした。

使えるようにするには、変形理論は、いくらか発展させる必要があった。Boston と Mazur の調べた幾つかの特別な例の外には、それに関する研究は殆どなかった。ミニマル・レベルで変形理論を記述するために、その理論を適切に調整することができるかどうかを調べた。1989 年の秋、当時プリンストンでの私の学生だった Ramakrishna に、 \mathbb{Z}_p 上の有限平坦群スキームから生じる表現の変形理論の存在を証明するという課題を与えた。これは、通常の場合への制限を取り除くために必要だった。1991 年の秋まで Ramakrishna の研究は完成しなかったが、これらの発展については、第 1 章の最初の節に述べた。長い間、問題を環論化する成果は、より自然なものにはなかったが、あまり簡単になったとは思われなかった。環論の言葉に翻訳されたとき、岩澤理論の通常の方法は、base change の未知な原理を必要とするように思われた。 \mathbb{Q} の \mathbb{Z}_p 円分拡大における異なる体に対する Hecke 環の間の厳密な関係およびその関係がねじれまでのものでないことを知る必要が

あった。

1991年春、この問題と、そしてまた全証明のための turning point が訪れた。Kunz の論文 [Ku2] の出る数年前、懸案の可換代数から手懸かりを得ようと研究していた。第2章で展開した合同計算のために、その Hecke 環が Gorenstein であることを確かめる必要があった。この (Hecke 環の Gorenstein) 特性は、最初に、素数レベルの場合に、Mazur が証明していた。彼の議論は、必要に応じて他の研究者によって拡張されてきた。Kunz の論文は、Gorenstein 環の間の同型をテストするために、私もすでに考えていたが、不変量 (この論文の補遺に述べた η 不変量) を使うことを示唆していた。私は、別の不変量 (補遺に述べた p/p^2 不変量) が完全交叉の間の同型を調べるのに使えると既に調べていた。[Ti2] の第6章を読んでいるとき、完全交叉に対する Grothendieck 双対理論についての Tate の説明から、これら2つの不変量はそのような環に対して等しいということが従うことを知った。これらの不変量の同等性が、Gorenstein 環が完全交叉であるための実際的基準であるということは、最初ありそうもないと考えていたが、間もなく理解できた。これらの議論は補遺で述べてある。

主要問題にとって、この結果は大変な衝撃だった。まず、Hecke 環と変形環の関係はこれらの2つの不変量を使ってテストできる。制限分岐をもつ全ての持ち上げがモジュラーならば、全ての持ち上げはモジュラーであることを示すために第2章第3節の帰納的議論を用いることができる。これは、成功しないまま長く可換代数におけるブレイク・スルーを待った研究だった。次に、主要問題を、[Hi2] に要約された肥田の計算を使って、よく知られたタイプの岩澤理論の類数に関する問題に移すことができた。特に、Rubin と Kolyvagin の最近の定理を使って、通常の CM の場合に、このことを調べることができた。これについては、第4章に述べてある。第3に、それは、無限に多くの j 不変量がモジュラーであることを確かめた最初のものであることを意味していた。最後に、ミニマル・レベル、そこでは以前におこなった Galois コホモロジーの計算で与えられる評価がより有望であると思われる、に焦点を当てることができていることを意味していた。ここでまた、ミニマル・レベルが存在することを知らるために、Serre 予想 (第1に、Fermat の最終定理をモジュラー形式に結びつける Ribet の同様の研究) に関する Ribet や他の研究者の仕事を使った。

類数問題は、岩澤理論においてよく知られたタイプのものだったが、通常の場合には、Coates や Schmidt が既に予想していた。しかしながら、岩澤理論の従来的な方法は、このケースでは全く十分でないように思えた。前にも説明したように、環論の言葉に翻訳する場合、base change の未知な原理が要求されると思われた。そこで、岩澤理論で使われる体の変換の代わりに、auxiliary primes を使うアイデアをさらに発展させた。その時にはまだ素数 $q \equiv -1 \pmod{p}$ を使って考えていたが、第3章に述べられる Galois コホモロジーの評価は、今やずっと強められた。主要な困難は、第2章の結果から auxiliary レベルへ渡すときに、どのように η 不変量が変化するかは判っていたが、 p/p^2 不変量における変化をどのように厳密に見積もるか判らなかつたことである。しかしながら、この方法はまさに、ミニマルな Hecke 環は完全交叉であるという付加的な前提のもとで、この文脈ではよく Selmer 群と呼ばれる一般類群の正しいバウンドを与えるものだった。

auxiliary primes を使うこの方法が必要とされることは、冪級数環の代わりに岩澤理論に基づくより自然なアプローチで得られる構成で置き換えることであることは以前から概念的には分かっていた。この通常の設定のもとでは、少なくとも μ 不変量が消滅すると仮定すれば、円分塔 (cyclotomic tower) における体の変化に対して、Hecke 環の射影極限が冪級数環となることが期待できるだろう。しかしながら、auxiliary primes を

使う設定のもとでは、密接に関係する非常に重要な肥田の構成 [Hi1] を除けば、助けになるとは思えない。この肥田の方法は、通常の場合における冪級数環への足がかりをしばしば与えた。また、岩沢理論を修正する議論のための微かなヒントも存在していた ([Scho], [Wi4,§10])。私は、決定的なものをつかめぬまま、研究をつづけた。

そんなで、1991年8月、Flachの新しい構成法 [Fl] を調べて、Flachの方法を拡張すればかなり上手くいくのではないかとたちまち確信した。Flachのアプローチは、オイラーシステムの構築へ向けての第一歩となるものに思われた。もしそれを完全に成し得ているならば、Selmer群のサイズの上限を与えるアプローチ。1992年秋までには、私はこれを達成できたと信じて、残されている3を法とする表現が可約である場合について考え始めていた。数か月の間、変形環と Hecke 環を使う方法を再び単純に当てはめようと試みた。1993年5月、Mazurの論文 [Ma3] のモジュラー曲線のツイスト形式の構成を読んでいるとき、突然、決定的なそして驚くべきブレイクスルーが訪れた。第5章で述べる、 ρ_5 と共通の楕円曲線族を使う議論を見つけた。いまや証明は完全なものになったと信じて、イギリスのケンブリッジで6月21-23日に行われた3つの講演で、全理論の概要 (sketch) を述べた。しかし、1993年秋、Flachの方法を拡張するために使ったオイラーシステムの構成は不完全であり、もしかすると不備があるかもしれないことが明らかになってきた。

第3章では、Selmer群をバウンドする問題にたいして、最初はとったが Flachの論文から学んだことに基づいて捨てたアプローチに関して述べる。1994年2月、Darmonは私を励まして、完全交叉特性への還元を説明するように言った。そして、それがモジュラー j 不変量の無限族を網羅する賢い方法であると。プリンストンでの講演で、そのことを提案したとき、私はほとんど無意識に、倒れこむようにして (critical), auxiliary primes (副素数, 補助的素数) として第3章で使った特別な素数への切り換えをおこなった。Flachの研究を拡張しようと試みていた1992年秋に、これらの素数の存在と重要性を調べていただけだった。以前は、auxiliary primes として $q \equiv -1 \pmod{p}$ のみを使っていた。後から見ると、この転換は、de Shalit による発展のために決定的であった。以前述べたように、肥田の理論は、少なくとも ordinary ケースでは、冪級数環への足がかりをしばしば与えることは以前から分かっていた。Cambridgeでの会議で、de Shalit は、素数 $q \equiv 1 \pmod{p}$ を使ったときの肥田の結果のあるバージョンを得ていること私に説明した。しかし、Princetonでの講演の完全交叉の議論の説明に対して、1991年以來の私の第1のアプローチについては、オイラーシステムを使うアプローチは正しいものの一つであると信じていたので、何も述べずにおいた。

1994年1月には、オイラーシステムを使う議論の修復のために、R.Taylorが加わった。1994年春、オイラーシステムの修復が思うようにならなかったため、Taylorと共に、 $p=2$ を使う新たな議論の考案を始めた。Taylorはまだ、オイラーシステムを使う議論がダメかどうか確認し終えてなかったため、9月には、障害となっている部分をより厳密に定式化して、Flachの一般化の議論に一旦区切りをつけることにした。その作業を行っている最中、突然の啓示が訪れた。1994年9月の19番目の日に、de Shalitの理論を一般化して使えばという一瞬の閃きのなか、適切な auxiliary レベルで Hecke 環を冪級数環の中に継ぎ合わせる (glue) 双対理論と一緒にそれを使えば上手くいくという考えが見えた。私は、一度捨てた元のアプローチに対してどうしても見つからなかったキーを突然見つけた。それは、持ち上げの手続きを達成するために使った、 $q_i \equiv 1 \pmod{p^{n_i}}$, $i \rightarrow \infty$ のとき $n_i \rightarrow \infty$, で q_i を取り出すという以前に使った考えである。これは、第3章での特別な素数への切り換えによって十分可能である。

この議論を Taylor と話し合った後、詳細の検討を数日行った。完全交叉特性を伴う全議論は [TW] にある。

結論として述べれば、補遺で導入した 2 つの不変量は変形環と Hecke 環を関連付けるのに使うことができるという、証明のための鍵となる突破口は、1991 年春実現した。基本的には、ガロア表現を数えるのに η 不変量が使えるということである。1993 年 6 月以降は、説明しにくいのだが、環論的設定のもとで岩沢理論に基づく方法を auxiliary primes の使用に基づく方法に置き換えることを目的とする長い手続きからの結果を公表するための最終の段階である。

Gorenstein 環は完全交叉でなければならないという基準は \mathbb{Z}_p 加群として有限かつ自由なより一般的な環についても拡張して使うことができるという Lenstra の研究を使って、第 2 章の議論の幾つかを簡単にするこは改善点の 1 つである。また、Faltings の指摘した第 3 章および [TW] の議論の改善も残されたままだったが、[TW] の補遺で説明されている。(続)

目次

第 1 章	
第 1 節	ガロア表現の変形
第 2 節	コホモロジー群の幾つかの計算
第 3 節	$GL_2(k)$ の部分群に関する幾つかの結果
第 2 章	
第 1 節	Gorenstein 特性
第 2 節	ヘッケ環の間の合同
第 3 節	主要定理
第 3 章	セルマー群に対する評価
第 4 章	
第 1 節	通常 CM のケース
第 2 節	η の計算
第 5 章	楕円曲線への応用
補遺	
参考文献	

第 1 章

この章は、或るガロア表現の研究に充てられる。最初の節で、Mazur の変形理論とその様々な精密化を議論する。これらの精密化は、普遍変形環と第 2 章の Hecke 環の間の対応を厳密にするために後々必要である。必要な主要結果は、様々な一般余接空間を Selmer 群と解釈するために用いる命題 1.2 とそれらの研究のために後に使われる (1.7) とである。節の終りのほうで、Selmer 群を Bloch-Kato 予想で使われる [Bloch-Kato 群, 局所コホモロジー群] に関連させる。しかし、この関連はわれわれの主要結果の証明には必要でない。

第 2 節で、ガロア・コホモロジーに関する Poitou と Tate の結果から、 Σ が変わるときの Selmer 群の間の関係、同様に Selmer 群とその双対の間の関係を抽出する。第 3 節での最も重要な研究結果は、第 3 章と [TW] で使われる特別な素数の存在を保証する Lemma 1.10(i) である。

1 ガロア表現の変形

p は奇素数、 Σ は p を含む素数の有限集合、そして \mathbf{Q}_Σ はこの集合 (Σ) と ∞ の他は不分岐な \mathbf{Q} の最大拡大であるとする。 \mathbf{C} への $\overline{\mathbf{Q}}$ の埋め込みを固定する。また同じく、 \mathbf{Q}_Σ の埋め込みを固定する。われわれはまた、 \mathbf{Z} におけるすべての素数 q に対する分解群 D_q の選択を固定する。 k は標数 p^{*3} の有限体であるとする。また

$$\rho_0 : Gal(\mathbf{Q}_\Sigma/\mathbf{Q}) \rightarrow GL_2(k) \quad (1.1)$$

は既約表現であるとする。序論とは対照的に、以降 ρ_0 は定義体 k に由来するとし、さらに $\det \rho_0$ は奇であるとする。特に、このことは、 ρ_0 の最小定義体 k_0 がそのトレースで生成される体 k_0 ($k = k_0$ を仮定しない) で与えられることを意味する。また、 ρ_0 が絶対既約であることを意味する。Mazur の意味での ρ_0 の $GL_2(A)$ への変形 $[\rho]$ を考える [Ma1]。したがって、 $W(k)$ が k の Witt ベクトル環ならば、 A は剰余体 k と最大イデアル m をもつ局所 $W(k)$ 完備 Noether (ネーター) 環 (代数) であり、変形 $[\rho]$ はちょうど、 $\rho \bmod m = \rho_0$ となるような、準同型 $\rho : Gal(\mathbf{Q}_\Sigma/\mathbf{Q}) \rightarrow GL_2(A)$ の strict な同値類である。2 つのそのような準同型は、核 $: GL_2(A) \rightarrow GL_2(k)$ の元による共役によって、一方からもう一方が導かれるとき厳密に同値であるという。しばしば同値類に対する $[\rho]$ を単に ρ と書く。

次のどちらかを仮定することによって、 ρ の選択にさらに制限を加える。

- (i) ρ_0 は ordinary (通常, 正則) である。すなわち、 ρ_0 の分解群 D_p への制限は (適切な基底を選べば)

$$\rho_0|_{D_p} \approx \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} \quad (1.2)$$

という形である。ここで、 χ_1 および χ_2 は D_p から不分岐な χ_2 をもつ k^* への準同型である。さらに $\chi_1 \neq \chi_2$ であると仮定する。ここで、 $\rho_0|_{D_p}$ が半単純となることを許容する。 (χ_1, χ_2 が双方とも不分岐で $\rho_0|_{D_p}$ が半単純なときには、 χ_1, χ_2 を固定するものとする)。

- (ii) ρ_0 は p で平坦 (flat) であるが ordinary でない ([Se1] 参照, そこでは有限という用語が使われている)。すなわち、 $\rho_0|_{D_p}$ は \mathbf{Z}_p 上の有限平坦群スキームに同伴する表現であるが、(i) の意味で ordinary でな

*3 体の標数—体の単位元 1 の n 個の和 $n1$ が 0 となるようなことがあるとき、そのような n で最小のもの (それは素数となる) を体の標数という。そのようなことがないとき標数は 0 であるという。『数学辞典』

い．(一般に，平坦な場合について述べるときには，特に定めがなければ， ρ_0 は ordinary でないとする．また， $\det \rho_0|_{I_p} = \omega$ と仮定する．ここで， I_p は p での慣性群であり， ω は 1 の p 乗根への作用を与える Teichmüller(タイヒミュラー) 指標である．)

(ii) の場合には，Raynaud の結果から， $\rho_0|_{D_p}$ は絶対既約であり， $\rho_0|_{I_p}$ を陽に書き表すことができる．(I_p 加群としての) 表現空間に対する Jordan-Hölder 列 (組成列)^{*4}を有限平坦群スキームに対する列に拡大すれば ([Ray1] 参照)，まず，自明な指標は部分商上で生じないことがわかり，(Oort-Tate 或いは Raynaud の分類を使う) 別な方法からは，群スキームは ordinary となることがわかる．それによって，Raynaud の結果から， $\rho_0|_{I_p} \otimes_k \bar{k} \cong \psi_1 \oplus \psi_2$ が分かる．ここで ψ_1 および ψ_2 は，次数 2 の二つの基礎指標である ([Ray1] の系 3.4.4 参照)． ψ_1 および ψ_2 は $Gal(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ への拡大指標とならないので， $\rho_0|_{D_p}$ は絶対既約でなければならない．変形に次のような制限のどれかを課したいことがある．

- (i) (a) セルマー変形. この場合には， ρ_0 は上記の意味で ordinary であり，その変形は次の特性を持つ表現 (representative) $\rho : Gal(\mathbf{Q}_\Sigma/\mathbf{Q}) \rightarrow GL_2(A)$ をもつ．

$$\rho|_{D_p} \approx \begin{pmatrix} \tilde{\chi}_1 & * \\ 0 & \tilde{\chi}_2 \end{pmatrix}$$

$\tilde{\chi}_2$ は不分岐であり， $\tilde{\chi} \equiv \chi_2 \pmod{m}$ ，および $\det \rho|_{I_p} = \varepsilon \omega^{-1} \chi_1 \chi_2$ が成り立つ．ここで ε は円分指標， $\varepsilon : Gal(\mathbf{Q}_\Sigma/\mathbf{Q}) \rightarrow \mathbf{Z}_p^*$ であり，1 の全ての冪乗根の上への作用を与える． ω は p を法として $\omega \equiv \varepsilon$ を満たす p と素な order^{*5}(of order prime to p) である． χ_1 と χ_2 は， $k^* \hookrightarrow A^*$ に値をとるとみたときの (i) の指標である．

(b) ordinary 変形. (i)(a) の場合と同じであるが，行列式に対して条件が付かない．

(c) strict^{*6}変形. これは (i)(a) の変種である．われわれは，これを $\rho_0|_{D_p}$ が半単純でなく，また flat でない (すなわち有限平坦群スキームに結びついていない) ときにのみ使う．このケースでは， $\chi_1 \chi_2^{-1} = \omega$ とする．そのとき strict 変形は， $(\tilde{\chi}_1/\tilde{\chi}_2)|_{D_p} = \varepsilon$ が条件に加わることを除けば (i)(a) のときと同じである．

- (ii) (p での) flat 変形. $GL_2(A)$ への各変形は，有限位数の任意の商 A/\mathfrak{a} に対して， $\rho|_{D_p} \pmod{\mathfrak{a}}$ は \mathbf{Z}_p 上の有限平坦群スキームの $\bar{\mathbf{Q}}_p$ -点に結びついたガロア表現である．

これら四つの各々の場合に，制限を加えない場合 (そのときには， p で何らの局所的な制限も課されない) と同様にして，Schlessinger の基準を使う Mazur の普遍変形

$$\rho : Gal(\mathbf{Q}_\Sigma \rightarrow GL_2(R))$$

の存在証明を確かめることができる．

ordinary かつ制限付きの場合には，これは Mazur が証明した．また，flat の場合には Ramakrishna が証明した [Ram]．その他の場合には，Mazur の議論のマイナーな修正が必要である．制限の付かない場合の普遍環を R_Σ で表し，制限付きの 4 つの場合を R_Σ^{se} ， R_Σ^{ord} ， R_Σ^{str} ， R_Σ^f で表わす．文脈から明らかな場合には，しばしば Σ は省略される．

^{*4} Jordan-Hölder の定理 因子群 $\mathfrak{g}/\mathfrak{g}_1, \mathfrak{g}_1/\mathfrak{g}_2, \dots, \mathfrak{g}_{r-1}/\mathfrak{g}_r = \mathfrak{g}_{r-1}$ の構造は，順序を無視すれば抽象群 \mathfrak{g} によって一意に決定する (Weyl 『群論と量子力学』)．或る形式的冪級数にする？

^{*5} 位数．他に整環 (order) や分岐指数 (order of ramification)．時々，階数 (普通 rank) と間違えることがある (個人的に)．of は同格？

^{*6} ‘関連続’ という訳語もある．『数学辞典』

これもまた必要となるのだが、上記の全ての場合に或る一般化が存在する。まず、 $W(k)$ 代数 A を考える代わりに、剰余体 k を持つ任意の局所体の整数環 \mathcal{O} に対する \mathcal{O} 代数を考える。 \mathcal{O} を用いることを示す必要のあるときには、 $R_{\Sigma, \mathcal{O}}$ など書く。局所 \mathcal{O} 代数の自然な局所写像

$$R_{\Sigma, \mathcal{O}} \rightarrow R_{\Sigma} \otimes_{W(k)} \mathcal{O}$$

が同型であること —— 機能的な理由から、その写像は、閉点 (closed point) で Zariski 接空間上の同型を誘導する自然な断面をもち、そういう場合中山 (正) のレンマ^{*7}を使うことができる —— をみるのは容易である。しかしながら、 $i: \rightarrow k'$ によって剰余体を取り換えるときには、表現 $\rho' = i \circ \rho_0$ に伴う新たな変形の問題が生じてしまう。ここでもまた、Zariski 接空間上の同型である、 $W(k')$ 代数の自然な写像

$$R(\rho'_0) \rightarrow R \otimes_{W(k)} W(k')$$

が存在する。

コホモロジー群の計算

$GL_2(k)$ の部分群に関する幾つかの結果

*7 【中山のレンマ】 R を単位的可換環とする。 \mathfrak{a} を R におけるイデアルとする。 M を R 上の有限生成加群とする。 $\mathfrak{a}M = M$ が成り立つとき、 $rM = 0$ となるような、 $r \equiv 1 \pmod{\mathfrak{a}}$ である $r \in R$ が存在する。
系 1 上の条件のもとで、 \mathfrak{a} が R の Jacobson radical (ヤコブソン根基) に含まれるならば、必然的に $M = 0$ 。
系 2 もし、 A のヤコブソン根基に含まれる或るイデアル \mathfrak{a} に対して、 $M = N \oplus \mathfrak{a}N'$ が成り立ち、また N' が有限生成ならば、 $M = N$ である。(Wikipedia, Nakayama Lemma から)

第 2 章

Gorenstein 特性

ヘッケ環の間の合同

主予想

第 3 章

セルマー群に対する評価

第 4 章

通常 CM の場合

η の計算

第 5 章

この章で楕円曲線に関する主要予想を証明する．特に，3 分割点に結びついた表現は既約でなければならないという仮定を取り除く方法を示す．

楕円曲線への適用

使われる鍵となる結果は，射影的像が正 2 面体 (dihedral) である場合における Hecke のより以前の結果を拡張する，次の Langlands と Tunnell の定理である．

定理 5.1 (Langlands-Tunnell) $\rho : Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL_2(\mathbf{C})$ は，その像が有限および可解な連続既約表現であるとする．さらに， $\det \rho$ は奇であるとする．そのとき，有限個のオイラー因子までは $L(s, f) = L(s, \rho)$ が成り立つような重み 1 の newform f が存在する．

Langlands は実際，論文 [La] で，行列式や数体 (われわれの場合では \mathbf{Q} である) への制限のないさらはずっと一般的な結果を証明している．しかしながら， $PGL_2(\mathbf{C})$ の像が S_4 である決定的に重要な場合では，或る付加的な仮定のもとでのみその結果は得られているにすぎない．後に，Tunnell ([Tu]) がその付加的仮定を取り除いた．

$$\rho_0 : Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL_2(\mathbf{F}_3)$$

は奇の行列式をもつ既約表現であるとする．われわれはここで，定理を使って，この表現が $\bar{\mathbf{F}}_3$ 上で，重み 2 の或る newform g をもつ或る対 (g, μ) に対して， μ を法として $\rho_0 \approx \rho_{g, \mu}$ が成り立つ ([Se, §5.3] 参照) という意味でモジュラーであることを示す．表現

$$i : GL_2(\bar{\mathbf{F}}_3) \hookrightarrow GL_2(\mathbf{Z}[\sqrt{-2}]) \subset GL_2(\mathbf{C})$$

が存在する． i を $GL_2(\mathbf{F}_3)$ の自己同形と組み合わせることによって，必要ならば， $(1 + \sqrt{-2})$ を法とする還元に基づいて， i は恒等 (identity) を導くと仮定することができる．そこで， $Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL_2(\mathbf{C})$ を考えれば，既約表現が得られる．それは奇であることまたその像が可解であることが容易に分かる．定理を適用すれば，この表現に結びついた重み 1 の newform f を見つけることができる．その固有値は $\mathbf{Z}[\sqrt{-2}]$ の中に存在する．いま， $E \equiv 1(3)$ であるような重み 1 のモジュラー形式 E を選ぶ．例えば， $E = 6E_{1, \chi}$ をとる．ここで $E_{1, \chi}$ は， $\mathbf{Q}(\sqrt{-3})$ に伴う 2 次指標 χ に対する $\zeta(s)\zeta(s, \chi)$ で与えられるメルン変換を持つアイゼンシュタイン級数である．そのとき $fE \equiv f \pmod{3}$ が成り立ち，また Deligne-Serre のレンマ [DS, Lemma 6.11] を使えば，上記の $(1 + \sqrt{-2})$ について，或る素数 μ' を法とする f と同じ固有値を持つ重み 2 の固有形式 g' を見つけることができる．ほとんど全ての T_l に対して g' と同じ固有値を持つ，重み 2 の newform g が存在する． $(1 + \sqrt{-2})$ に関する或る素数 μ に対して (g, μ) で (g', μ') を置き換える．そのとき，対 (g, μ) は $(\mu'$ と両立する) μ の適切な選択に対して，われわれの要求を満たす．

$E[3]$ を考え合わせて， \mathbf{Q} 上で定義された楕円曲線 E にこのことをあてはめれば，楕円曲線を調べる場合，どのようにして変形理論における既約表現への制限をなしにすませられるかを述べる．

定理 5.2 \mathbf{Q} 上のすべての半安定な楕円曲線はモジュラーである．

定理5.3 E を次の特性

- (i) E は 3, 5 で良いあるいは乗法的還元を持つ .
- (ii) $p = 3, 5$ に対しておよび任意の素数 $q \equiv -1 \pmod{p}$ に対して, $\bar{\rho}_{E,p}|_{D_q}$ は $\bar{\mathbb{F}}_p$ 上可約であるかあるいは $\bar{\rho}_{E,p}|_{I_p}$ は $\bar{\mathbb{F}}_p$ 上既約である .

を持つ, \mathbb{Q} 上で定義された楕円曲線であるとき, E はモジュラーである .

補遺 Gorenstein 環と局所完全交叉

命題 1

- (i)
- (ii)

証明 1

□

余分な章

概念が難しそうなので、可能な限りで書いておくことにしました。

表現の既約性：Baire 空間と Banach 空間，離散空間とコンパクト化 (アレクサンドロフのコンパクト化定理) など 参照 河田・三村著『現代数学概説 II』

“A REPORT ON WILES’ CAMBRIDGE LECTURES”, K.RUBIN AND A.SILBERBERG
arXiv:math.NT/9407220 v1 1 JUN 1994

[概要]

1993 年 6 月の Newton 研究所での講演で、Andrew Wiles は、谷山-志村予想の大部分の証明およびそれから結果するフェルマーの最終定理の証明を宣言した。このレポートは、その背景および数学史的知識を含む、Wiles の講演の数学的内容の非専門家への解説である。

[序文]

1993 年 6 月 23 日、Andrew Wiles は、英国 Cambridge にある Newton 研究所での講演で、聴衆を前にした黒板に、 p を素数、 u, v および w を有理数として、 $u^p + v^p + w^p = 0$ が成り立つならば、 $uvw = 0$ であると書いた。換言すれば、Fermat の最終定理 (予想) の解決を宣言した。彼の宣言は、1 週間に及ぶ、“ p 進 Galois 表現、岩沢理論そしてモチーフの玉川数”に関する分科会での“モジュラー形式、楕円曲線そして Galois 表現”と題された 3 回の連続講義の最後になされた。Pierre de Fermat (1601—1665) は、Diophantus の本の写しの欄外に、ピタゴラスの 3 つ組数 (Phitagorean triples) の問題に続けて、次のように書き留めた。

或る立方数を 2 つの立方数に、あるいは或る四乗数を 2 つの四乗数に、さらに一般的に 2 乗よりも大きい或るべき乗を同じべきの 2 つのべき乗に分けることは不可能である。私は真に驚嘆すべき証明を発見したが、この余白はそれを書き留めるには狭すぎる。

Fermat の予想を次のように書き改めよう。

Fermat’s Last Theorem $n > 2$ とすれば、 $a^n + b^n = c^n$ は 0 以外の整数解 (a, b, c) を持たない。

Fermat による証明は結局見つからず、未解決の問題として残り、何代もの数学者を奮い立たせて証明に向かわせた。現代数論の多くは、Fermat の最終定理を証明するために組み立てられてきた。Fermat の最終定理 (最終という意味は Fermat の残した問題のなかで最後まで残った問題であるからである) に関する史的詳細は [5], [6] および [26] を見よ。

Cambridge で Andrew Wiles が宣言したことは、Fermat の最終定理を意味するのに十分なだけの、“多くの”楕円曲線がモジュラーであることを証明したということである。この論文では、Wiles の楕円曲線に関する研究とその Fermat の最終定理との結びつきを説明する。

§1 で、楕円曲線とモジュラリティーについて説明し、Fermat の最終定理と楕円曲線のモジュラリティーに関する谷山-志村予想との結びつきについて説明する。

§2 では, Wiles が, Langlands と Tunnell の定理を使って, 谷山-志村予想を (谷山-志村予想の弱形式とみなすことのできる) モジュラー持ち上げ予想と呼ばれる予想にどのようにして弱めて証明できたか解説する.

§3 および §4 では, 半安定モジュラー Lifting 予想が Galois 表現の変形に関する Mazur の予想 (予想 4.2) にどのように関係するかを説明する. そして §5 では, この予想の攻略の Wiles の方法を解説する.

楕円曲線 \mathcal{Q} 上の楕円曲線は次の形の方程式で定義される非特異曲線である.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

ここで, 係数 a_i は整数であり, 解 (∞, ∞) は楕円曲線上の点であると見なす.

• 注意書き

- (i) 曲線 $f(x, y) = 0$ の特異点は, 変数 x に関しても y に関してもその偏導関数が消滅 (vanish) する点である. 曲線は, 特異点を持たないとき非特異である.
- (ii) \mathcal{Q} 上の 2 つの楕円曲線は, 座標変換 $x = A^2x' + B, y = A^3y' + Cx' + D$ ($A, B, C, D \in \mathcal{Q}$) によって, 一方からもう一方へ移ることができるとき, また A^6 を法として合同多項式であるとき同型である (and dividing through by A^6).
- (iii) \mathcal{Q} 上のすべての楕円曲線は, 係数 a_i は整数として

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

の形の方程式に同型である. この形の曲線は, 右辺の 3 次式が重根を持たないときに限り非特異である.

Modularity

\mathfrak{H} を複素上半平面 $\{z \in \mathbf{C} : \Im z > 0\}$ を表すとする. ここで $\Im z$ は z の虚部である. N を正の整数とすると, 行列の群

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) : c \text{ は } N \text{ で割り切れる} \right\}$$

を定義する. 群 $\Gamma_0(N)$ は線形分数変換

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d}$$

によって \mathfrak{H} の上に作用する. 商空間 $\mathfrak{H}/\Gamma_0(N)$ は (非コンパクト) Riemann 面である. それは, カスプ (cusp, 尖点) と呼ばれる有限個の点を付加することでコンパクト Riemann 面 $X_0(N)$ に完備化できる. カスプは, $\Gamma_0(N)$ の作用のもとで $\mathbf{Q} \cup \{i\infty\}$ の有限個の同値類である. 楕円曲線の複素点はコンパクト Riemann 面と見なされる.

定義 楕円曲線 E は, 或る整数 N に対して, $X_0(N)$ から E の上への正則写像が存在するとき, モジュラーである.

Langlands-Tunnell の定理を述べるには, $\Gamma_0(N)$ の部分群に対する重み 1 のモジュラー形式が必要である.

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) : c \equiv 0 \pmod{N}, a \equiv d \equiv 1 \pmod{N} \right\}$$

とおく．§16における $\Gamma_0(N)$ を $\Gamma_1(N)$ で置き換えれば， $\Gamma_1(N)$ に関するカスプ形式の概念を定義できる． $\Gamma_1(N)$ に対する重み 1 のカスプ形式空間上の Hecke 演算子の定義に関しては [35] の第 3 章参照．

Langlands-Tunnell の定理 $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$ は， $PGL_2(\mathbb{C})$ における像 (image) が S_4 (4 つの元に関する対称群) の或る部分群である連続既約表現であり， τ は複素共役，および $\det \rho(\tau) = -1$ であるとする．そのとき，或る $\Gamma_1(N)$ に対して重み 1 のカスプ形式 $\sum_{n=1}^{\infty} b_n e^{2\pi i n z}$ が存在する．それは対応するすべての Hecke 演算子に対する固有形式であり，有限個を除く全ての素数 q に対して

$$b_q = \text{trace}(\rho(\text{Frob}_q))$$

が成り立つ．

セルマー群 (Selmer groups)

一般に， M がねじれ $G_{\mathbb{Q}}$ 加群ならば， M に付随する Selmer 群は次のようにして或る局所条件から決定されるガロワコホモロジー群 $H^1(G_{\mathbb{Q}}, M)$ の部分群である． q を分解群 $D_q \subset G_{\mathbb{Q}}$ を持つ素数であるとすれば，制限写像

$$\text{res}_q : H^1(G_{\mathbb{Q}}, M) \rightarrow H^1(D_q, M)$$

が存在する．考えている個別の問題によって部分群の集合を固定すれば，対応する Selmer 群は

$$S(M) = \bigcap_q \text{res}_q^{-1}(J_q) \subset H^1(G_{\mathbb{Q}}, M)$$

Weyl 『群論と量子力学』「群とその表現」

[前書から]

量子論の一般法則の発見に対して群論が与えた立脚点の重要性は，ますます明らかになってきている．何年にもわたって連続群の表現論に深く関わってきた経緯から，量子物理の要求に適うような形で，数学者の研究から得られたこの分野の知識を解説することは適切であり重要であると考えている．純粋に数学的立場からは，表現論を議論する場合に，この問題を扱う教科書のなかでこれまで成されてきたように有限と連続の間にはっきりとした線引きを行うことはもはや適切なことではない．群論から生じる概念が物理の中にその応用をどのように見出すか手短かに言えば，目的が首尾良く達せられたならば，この書は，群論と量子力学の本質を学ぶと同時にこれら二つの主題の間の関連を学べるものとなるだろう．特に，対称置換群の表現と完備線形群の表現の間の相互律を強調したいと思う．この相互律は，量子力学の概念的構造からもっとも自然に導かれるという事実にもかかわらず，物理的文脈では未だ不当に無視されているものである．

新しいハイゼンベルグ-シュレジンガー-ディラックの量子力学の本質は，技巧的な数学的な意味での非可換代数の構成のなかで，それ自身物理量である要素の量の一組と各物理系とが結びついているという事実の中に見出される．

【変換群】

最も古くまた最も深遠な数学の概念の一つである群の概念は，変換群^{*8}の概念を抽象することから得られる．変換がその上に作用する，点と呼ばれる元の領域である点場 (point-field) が，変換の基礎に横たわる．点

*8 群 G ，集合 M にたいして，写像 $G \times M \rightarrow M$ を f で表す． $f(g, x) = g(x)$ ($g \in G, x \in M$) とおく．次の 2 つの条件が成り立

場は、弁別的に列挙された有限個の元の全部であるか無限集合、特に時間や空間のような連続体である。それ自身の上の点場の写像或いは対応 S は、点場の各点 p を写像による像 p' に結合する法則によって定義される、 $p \rightarrow p' = Sp$ 。2つの対応 S と T は、すべての点 p に対してその像 S_p と T_p が一致するとき同じ対応である。有限個の元からなる点場では、対応 S は各点 p の像となる点を明示的に与えれば得られるが、無限集合である場合には、結合は、関数 S の法則を与えることでのみ可能となる。対応の中には各点 p を p 自身に結合する恒等対応とよばれる特別な対応が存在する、 $p \rightarrow p$ 。2つの対応を続けて行うことができる。まず、任意の点 p を $p' = Sp$ に対応させたら、次に p' を $p'' = Tp'$ に対応させる。2つの対応の合成の結果である対応を $p \rightarrow p'' = T(Sp)$ で定義し TS で表す(右から左へ読む)。合成対応は2つの対応の順序に依存する。合成が可能となるには、対応が、別の点場へではなく、それ自身への写像となることが本質的である。

【抽象群】

抽象群 (abstract group) は、群の任意の (同じものでも異なってもいい) 二つの元 a, b から一つの元 ab を生じる合成の法則に従う元の体系 (a system of elements) である。これに関して、次の条件が満たされる。

1. 合成法則 $c(ba) = (cb)a$
2. 任意の元 a に対する合成でその元を変化させない、単位元 1 が存在する。 $a1 = 1a = a$
3. 各元 a に対する合成で単位元 1 となるような元、すなわち a の逆元 a^{-1} が存在する。 $aa^{-1} = a^{-1}a = 1$

つとき G を集合 M の変換群という。

- 1) G の単位元 1 に対して $1(x) = x (x \in M)$
- 2) $g, h \in G$ に対して $(gh)(x) = g(h(x)) (x \in M)$