Andrew Wiles は 1953 年イギリス生まれの数学者で, 周知の通り 20 世紀の終わりにドラマチックな展開で Fermat 予想を解決した. 近年で最も多くスポットライトを浴びた数学者かもしれない. 衝撃的な Fermat 予想解決から 10 年余りを経た現在, 彼が代数学や整数論に与えた影響を周りの風景を織り交ぜながらざっと眺めていきたい.

1 Wiles 以前の整数論

その人物を語るにはその人物の登場以前の世界から語る方がより正確に伝わるのではないだろうか. 19 世紀の末から 20 世紀半ば過ぎまでの相次ぐ代数学の理論革新に伴い整数論も大きく進歩した. また, 次の Fermat の予想[1]は整数論の発展に常に影響を与え続けた.

予想 (Fermat). $p \geq 3$ を素数とするとき $x^p + y^p = 1$ に $xy \neq 0$ なる有理数解 x, y は存在しないだろう[2].

さて, n-等分多項式 $t^n = 1$ の原始根 ζ_n を有理数体 $\mathbb{Q}$ に付け加えた体を $\mathbb{Q}(\zeta_n)$ と記す. 一般に $\mathbb{Q}$ にある代数方程式の根を付け加えて得られる代数体 F において, 既約元分解の一意性が成り立たないことがある. 例えば, $F = \mathbb{Q}(\sqrt{-5})$ では $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ と 2 通りに既約元分解がある. Kummer は $\mathbb{Q}(\zeta_p)$ において既約元分解の一意性の崩れ具合がひどくなければ, その素数 p で Fermat の予想が成り立つことを証明し Fermat 予想の成立する素数 p が飛躍的に増えた. かくして, F の既約元分解の一意性の成り立たなさ具合を定量的に表すイデアル類群 $\mathrm{Cl}(F)$ が大事な研究対象となる. 手短に $\mathrm{Cl}(F)$ の定義を述べよう. $\mathcal{O}_F$ を F の整数環とするとき F の中の有限生成な部分 $\mathcal{O}_F$ 加群全体は, 積をとることで自然にアーベル群になる. $\mathrm{Cl}(F)$ は,

$$\mathrm{Cl}(F) = \frac{\{F \text{ の中の有限生成な部分 } \mathcal{O}_F \text{ 加群全体 }\}}{\{F \text{ の中の単項な部分 } \mathcal{O}_F \text{ 加群全体 }\}}$$

で定義され, $\mathrm{Cl}(F)$ が有限群になることが代数的整数論の基本結果である. F において既約元分解の一意性が成り立つことが $\mathrm{Cl}(F) = \{0\}$ と同値で, 例えば $\mathrm{Cl}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Z}/(2)$ となる. F をひとつ決めれば $\mathrm{Cl}(F)$ を計算するアルゴリズムは確立されているが, F を変化させたときの $\mathrm{Cl}(F)$ の挙動は不規則で未解決な具体的問題を多く含んでいる[3].

[1] 上で述べたように既に Wiles によって解決済みである.

[2] すべての自然数 $n \geq 3$ に対して $x^n + y^n = 1$ を論ずる予想であるがすべての奇素数と $n = 4$ のみで言えればすべての自然数 $n \geq 3$ で正しいことは難しくない.

[3] 例えば $\mathrm{Cl}(F) = \{0\}$ なる実 2 次体 F が無限個あるだろうというガウス予想は今も未解決である.

一方で, 代数体 F に対してゼータ函数とよばれる複素函数が $\mathcal{O}_F$ の素イデアル $\mathfrak{P}$ をはしるオイラー積 $\zeta_F(s) = \prod(1 - \mathrm{N}(\mathfrak{P})^{-s})^{-1}$ で定義される ($N(\mathfrak{P})$ は素イデアルのノルム $N(\mathfrak{P}) = \sharp\mathcal{O}_F/\mathfrak{P}$ である). $\zeta_F(s)$ は全複素平面に有理型接続され $s = 1$ で 1 位の極をもつ. 次のような結果が古典的である.

(Dirichlet の) 類数公式. F の類数 $\sharp\mathrm{Cl}(F)$ は以下で与えられる :

$$\sharp\mathrm{Cl}(F) = \lim_{s\to 1}(s-1)\zeta_F(s)\frac{w_F|D_F|^{1/2}}{2^{r_1}(2\pi)^{r_2}R_F}$$

(w_F は F における 1 のベキ根の数, D_F, R_F は判別式と単数規準. r_1, r_2 は F の実と虚の埋め込みの数).

数論幾何学の見地からは代数体 F は $\mathbb{Q}$ 上の 0 次元代数多様体とみなせる. Serre 他さまざまな人々の努力によって $\mathbb{Q}$ 上の d 次元代数多様体 X の Hasse-Weil ゼータ函数 $\zeta_X(s)$ が絶対ガロア群 $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の作用をもつエタール・コホモロジー $H^d_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)$ を用いて $\zeta_X(s) = \prod_{p:\text{素数}}(\det(1 - \mathrm{Frob}_p t; H^d_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)^{I_p})|_{t=p^{-s}})^{-1}$ で定義される[4]. 一方で, セルマー群というアーベル群 $\mathrm{Sel}(X)$ が $H^d_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}/\mathbb{Z})$ を係数にもつガロア・コホモロジー $H^1(G_{\mathbb{Q}}, H^d_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}/\mathbb{Z}))$ の部分群として各素数で局所条件を課すことで定まる. $\zeta_X(s)$ と $\mathrm{Sel}(X)$ は $\zeta_F(s)$ や $\mathrm{Cl}(F)$ の一般化にあたる対象であり $\zeta_X(s)$ に付随する値と $\mathrm{Sel}(X)$ の関係が問題となってくる. つまり 20 世紀の研究の積み重ねの中で

“類数公式の高次元化と非可換化および精密化”を追求したい[5]

というひとつの目指すべき夢が浮き彫りになってくるのである.
このような課題は不定方程式の有理数解など数論幾何の多くの中心問題に関係する. また Wiles の研究には常に底にこのようなテーマが流れている.

Wiles が切り開いた新しい局面を照らし出すためにそれ以前の研究の到達点と限界を思い出しておきたい.

1. 類体論の完成と応用 代数体 F のアーベル拡大のガロア群を乗法群もどきのわかりやすい群で記述する類体論が 20 世紀の前半に確立され, 豊かな数論的応用が得られた. また有理数体や虚 2 次体に対してはアーベル拡大の具体的構成に踏み込んだ Kronecker-Weber の定理や虚数乗法論などの一段深い理論も得られた.

[4] Frob_p は p でのフロベニウス, I_p は惰性群を表す.
[5] 高次元化については上でも触れた. 非可換化および精密化とは何であるかについては関連して次節以降で触れていきたい.

2. エタール・コホモロジーとガロア表現 Grothendieck のエタール・コホモロジー理論によって $\mathbb{Q}$ 上の代数多様体 X を $G_{\mathbb{Q}}$ 作用をもつベクトル空間 $H^*_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)$ という線形代数的な対象を通して調べられるようになった.

3. p-進理論 (特に岩澤理論) の出現と発展 元来 mod p^n の合同の議論は Diophantine 方程式の問題などに有効に用いられてきた. それに加えて 20 世紀中頃から出現した岩澤理論 (後でも少し説明する) でゼータ函数の値の p-進的な現象が深く追求され, 数論における p-進的手法が爆発的に進展した.

Hilbert, 高木, Artin らによる類体論によりアーベル拡大に関わる問題を扱う技術が完成し, 大規模な幹線道路ができたようでもある. 一方でひとたび非アーベルなガロア拡大が関ると, (ラングランズ予想その他の努力はあるものの) 現代においてはいまだに我々は常套手段がなく無力である.

次の節以降で Wiles の研究を時間の経過にしたがって辿っていきたい. Wiles のこれまでの仕事はあえて大きく分けると次の 3 つに分類される:

A. (虚数乗法をもつ) 楕円曲線の BSD 予想に関係する一連の研究 (第 2 節で説明する)

B. イデアル類群の岩澤主予想に関連する一連の研究 (第 3 節で説明する)

C. 谷山志村予想および Fermat 予想に関連する一連の研究 (第 4 節で説明する)

2 虚数乗法をもつ楕円曲線の BSD 予想

E を有理数体 $\mathbb{Q}$ 上で定義された楕円曲線とする. 楕円曲線とは重根をもたない 3 次式 $x^3 + ax + b$ によって $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Q})$ と定義される図形で, 種数 1 の代数曲線である. 種数 0 の代数曲線のゼータ函数やセルマー群は自明なので最初の高次元の研究対象である. さて, F が $\mathbb{Q}$ の有限次拡大のとき楕円曲線の有理点 $E(F)$ は Mordell-Weil の定理により有限生成アーベル群である.

Birch and Swinnerton-Dyer 予想 (以下, BSD 予想と略記). E を有理数体 $\mathbb{Q}$ 上で定義された楕円曲線とする. このとき, $\zeta_E(s)$ の $s = 1$ での零点の位数 $\mathrm{ord}_{s=1}\zeta_E(s)$ は $E(\mathbb{Q})$ のランクと等しい.

E の自己準同型環 $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ は n 倍写像からなる部分環 $\mathbb{Z} \subset \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ をもつ. たいてい $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z}$ であるが, 例外的に $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ が大きな楕円

曲線 E がある. その場合, $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ はある虚 2 次体 $K=\mathbb{Q}(\sqrt{-d})$ の整数環 $\mathcal{O}_K$ の部分環と同型なので, E は虚数乗法をもつという. 例えば, 楕円曲線 $E_D: y^2=x^3+Dx$ たちは虚数乗法をもち, $(x,y)\mapsto(-x,\sqrt{-1}y)$ は n 倍写像とは異なる自己同型である[6]. Wiles はイギリスのケンブリッジ大学大学院での彼の指導教官 Coates 氏との共同研究で次を示した:

定理 1 (Coates-Wiles/1977). E は $\mathbb{Q}$ 上の楕円曲線であって類数 1 の虚 2 次体 K が存在して $\mathrm{End}_{\overline{\mathbb{Q}}}(E)\cong\mathcal{O}_K$ とする. もし $\zeta_E(1)\neq 0$ ならば $E(\mathbb{Q})$ は有限アーベル群である.

証明には楕円単数という $\zeta_E(s)$ の特殊値と関係の深い K の拡大体の元が活躍する. 楕円単数は少し複雑なので古典的な円単数の例で紹介しよう. $u\in\mathbb{Z}_p[\zeta_p]$ に対して $f_u(\zeta_p-1)=u$ となる生成ベキ級数 $f_u(t)\in\mathbb{Z}_p[[t]]$ を考え, $g_u^{(r)}(t)=\left((1+t)\frac{d}{dt}\right)^r\log(f_u(t))$ とおく. 各自然数 r に対して $\varphi^{(r)}:\mathbb{Z}_p[\zeta_p]\longrightarrow\mathbb{Z}/(p)\mathbb{Z}$ を

$$\varphi^{(r)}(u)=g_u^{(r)}(t)|_{t=0}\in\mathbb{Z}_p \bmod p \tag{1}$$

で定める. u に対し生成ベキ級数 $f_u(t)$ のとり方は不定性があり $g_u^{(r)}(t)$ も一意ではない. ただ, $g_u^{(r)}(t)$ が変わるときの値 $g_u^{(r)}(t)|_{t=0}$ の差は p で割り切れ, $\varphi^{(r)}$ は well-defined な準同型となる. 今, **円単数** $u=1+\zeta_p\in\mathbb{Z}[\zeta_p]$ をとる. このとき, $f_u(t)=2+t$ ととれる. 計算により函数 $g_u^{(r)}(t)|_{t=0}$ はリーマン・ゼータ函数 $\zeta(s)$ の特殊値 $(1-2^r)\zeta(1-r)$ と等しい[7].
(証明のあらすじ) 対偶をとり, $E(\mathbb{Q})$ が位数が無限と仮定して $\zeta_E(1)=0$ を示す. K において $p=\pi\overline{\pi}$ と分解する素数 p をとる[8]. $[\pi^r]\in\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ を $\pi^r\in\mathcal{O}_K$ に対応する準同型とするとき, $\mathrm{Ker}([\pi^r])\in E(\overline{\mathbb{Q}})$ の座標をすべて K に付け加えた拡大を $K(E_{\pi^r})$ とし, $\cup_{r\geq 1}K(E_{\pi^r})$ を $K(E_{\pi^\infty})$ と記す. 仮定から位数無限な点 $P\in E(\mathbb{Q})$ がある. $[\pi^n]Q_n=P$ なる $Q_n\in E(\overline{\mathbb{Q}})$ の座標を付け加えて巡回代数拡大 $K(E_{\pi^\infty})(Q_n)/K(E_{\pi^\infty})$ が得られる. 証明の山場として[9], 次が言える :

$K(E_{\pi^\infty})(Q_n)/K(E_{\pi^\infty})$ は
十分大きな n では π 上の素点で分岐する. (2)

[6] この場合, $\mathrm{End}_{\overline{\mathbb{Q}}}(E_D)\cong\mathbb{Z}[\sqrt{-1}]$ である.

[7] 変数変換 $t=T-1$ により $g_u^{(r)}(T)=(T\frac{d}{dT})^{r-1}\frac{T}{1+T}$ となり, $T=\exp(x)$ として $g_u^{(r)}(t)|_{t=0}=(\frac{d}{dx})^{r-1}\frac{e^x}{1+e^x}|_{x=0}$ を得る. これは $\frac{xe^x}{1+e^x}=\frac{(2x)e^{2x}}{e^{2x}-1}-\frac{xe^x}{e^x-1}$ の Taylor 級数展開の r 次の係数の $(r-1)!$ 倍でありベルヌーイ数や $\zeta(1-r)$ と結びつく.

[8] このような素数の密度は全ての素数の半分である.

[9] この部分の証明は Coates-Wiles は岩澤らによって研究された詳細相互法則を使って長い計算で乗り越えた. その後より簡単な別証明が判明したが彼らの思い入れの深さからか論文には両方の証明を採録している.

さて, $K(E_\pi)$ は K の完全分岐拡大であり $\mathcal{O}_{K(E_\pi)}$ では $(\pi) = \mathfrak{p}^{p-1}$ となる. $\mathcal{O}_{K(E_\pi)}$ の素イデアル $\mathfrak{p}$ での完備化を $\mathcal{O}_\mathfrak{p}$ と記す. 次のような 2 つの群を考える:

$$\mathcal{E} = \{x \in \mathcal{O}^\times_{K(E_\pi)} \mid x \equiv 1 \bmod \mathfrak{p}\},$$
$$\mathcal{U}_\mathfrak{p} = \{x \in \mathcal{O}^\times_\mathfrak{p} \mid x \equiv 1 \bmod \mathfrak{p}\}.$$

$\mathcal{U}_\mathfrak{p}$ はおおおそ $K(E_\pi)$ を完備化した体の単数群であるから, 定義より $\mathcal{E} \subset \mathcal{U}_\mathfrak{p}$ とみなせる. $\mathcal{U}_\mathfrak{p}$ は自然に $\mathcal{O}_\mathfrak{p}$-加群で, **類体論**より (2) は以下のように翻訳される[10].

$$\mathcal{E} \text{ は } \mathcal{U}_\mathfrak{p}^p \subset \mathcal{U}_\mathfrak{p} \text{ に含まれる} \tag{3}$$

(1) の準同型 $\varphi^{(r)}$ の類似として, ζ_p の代わりに E の π 等分点による生成べキ級数をとり, 対数函数 log や $((1+t)\frac{d}{dt})^r$ を合成すると準同型 $\psi^{(r)} : \mathcal{U}_\mathfrak{p} \longrightarrow \mathcal{O}_\mathfrak{p}/\mathfrak{p} \cong \mathbb{Z}/(p)$ が構成される. 楕円函数の特殊値を用いて構成される**楕円単数**と呼ばれる $\Theta_\mathfrak{p} \in \mathcal{E}$ があり,

$$\psi^{(1)}(\Theta_\mathfrak{p}) \equiv \zeta_E(1)/\Omega_E \mod \mathfrak{p} \tag{4}$$

となる. ここで, $\Omega_E = \int_{E(\mathbb{R})} \omega_E$ は周期積分であり, 古典的に $\zeta_E(1)/\Omega_E \in \mathbb{Q}$ が知られている. (3), (4) より $\zeta_E(1)/\Omega_E$ は p で割り切れる. 上の議論を無限個の素数 p で行うと, $\zeta_E(1) = 0$ でなければならない. (証明終)

証明の途中で現れる $K(E_{\pi^\infty})/K(E_\pi)$ のガロア群は $\mathbb{Z}_p$ と同型であり, 岩澤理論で用いられる「$\mathbb{Z}_p$-拡大」に他ならない. 誕生して新しかった岩澤理論の考え方が随所に活かされている. この Coates-Wiles に影響を受けたり深い関係をもつその後の発展については次の 2 つが顕著である.

1. 無限次拡大 $K(E_{p^\infty})/K$ の中間体すべてでゼータ函数とセルマー群の関係を追求すると 2 変数岩澤主予想の定式化に至るが, Rubin 氏は 80 年代後半に当時の最新手法「オイラー系」を楕円単数に適用して解決した. 2 変数岩澤主予想は正確に説明しないが, 2 変数べキ級数環のイデアルの等式 "$(\zeta^{\mathrm{alg}}_{K,p}(S,T)) = (\zeta^{\mathrm{anal}}_{K,p}(S,T))$" であり, Coates-Wiles の定理もこれの系として $S = T = 0$ を代入することでただひとつの素数 p のみから得られる.
2. 虚数乗法を持たない楕円曲線 E では等分点の座標による拡大はアーベル拡大とはほど遠いため, 類体論のような大道具が使えず更に困難となる. Kolyvagin や加藤和也氏は, それぞれ独立な方法によって虚数乗法を持たない場合も $\zeta_E(1) \neq 0$ なら $E(\mathbb{Q})$ が有限なことを示した.

[10] 以下の式は正確には $\mathcal{E}$ や $\mathcal{U}_\mathfrak{p}^p$ を $\mathrm{Gal}(K(E_\pi)/K)$ の作用で指標分解した部分に対する包含関係を記述しなければならない.

虚数乗法をもつ楕円曲線という特別なクラスながらBSD予想に関する一般的結果を出したのはCoates-Wilesが最初である．BSD予想自体の現状については$\mathrm{ord}_{s=1}\zeta_E(s)$が0または1のときそれぞれ$\mathrm{rank}E(\mathbb{Q}) = \mathrm{ord}_{s=1}\zeta_E(s)$が示されている．一方で，$\mathrm{ord}_{s=1}\zeta_E(s) \geq 2$のときには現状では$\mathrm{ord}_{s=1}\zeta_E(s)$と$\mathrm{rank}E(\mathbb{Q})$の間には個別な計算例以上の一般的な大小関係はまったく知られていない．$\mathrm{ord}_{s=1}\zeta_E(s) \geq 2$で何らかの一般的結果が与えられるかが現在の壁かもしれない．

3　イデアル類群に対する岩澤主予想

Wilesは，その後Mazurと共同で当時の岩澤理論の最重要課題であった岩澤主予想にとりくんでいる．岩澤理論では円分体$K_n = \mathbb{Q}(\zeta_{p^n})$とその合成体$K_\infty = \cup_{1\leq n<\infty} K_n$，ガロア群$\Gamma = \mathrm{Gal}(K_\infty/K_1)$及び完備群環$\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$が大事な登場人物である．ここで$\Gamma$は円分指標$\chi_{\mathrm{cyc}}$によって標準的な同型$\chi_{\mathrm{cyc}} : \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$をもつことに注意したい．イデアル類群の$p$-ベキ部分$A_n = \mathrm{Cl}(K_n)\{p\}$を位数だけでなく$\mathrm{Gal}(K_n/\mathbb{Q})$の作用の精密な情報をこめて調べてたい．標準指標$\omega : \mathrm{Gal}(K_1/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/(p))^\times$によって$A_n = \oplus_{0\leq i\leq p-2} A_n^{\omega^i}$と指標分解され，岩澤氏によって$X^{(i)} = \varprojlim_n A_n^{\omega^i}$はそれぞれの$i$で有限生成ねじれ$\mathbb{Z}_p[[\Gamma]]$-加群である．また，一般に整域$R$とねじれ$R$-加群$M$があると$M$の大きさを表す特性イデアル$\mathrm{Char}_R(M)$が定まる．例えば$R = \mathbb{Z}$，$M = \oplus_{1\leq j\leq r}\mathbb{Z}/(n_j)$のときには，$\mathrm{Char}_R(M) = (n_1 \cdots n_r)$である．特性イデアル$\mathrm{Char}_{\mathbb{Z}_p[[\Gamma]]}(X^{(i)}) \subset \mathbb{Z}_p[[\Gamma]]$の生成元$L_p^{\mathrm{alg},(i)}$を代数的$p$-進$L$函数とよぶ．一方，久保田-Leopoldt，岩澤，Colemanにより解析的p-進L函数とよばれる$L_p^{\mathrm{anal},(i)} \in \mathbb{Z}_p[[\Gamma]]$で以下のようなものが構成されている：

$r \equiv i \bmod p-1$なるすべての自然数rで$\chi_{\mathrm{cyc}}^r(L_p^{\mathrm{anal},(i)}) = (1-p^r)\zeta(-r)$

岩澤によって結晶化された以下の岩澤主予想はMazur-Wilesによって解決された．

定理2 (岩澤主予想=Mazur-Wilesの定理/1984)．$0 < i < p-1$なる奇数iで$\mathbb{Z}_p[[\Gamma]]$のイデアルの等式$(L_p^{\mathrm{alg},(i)}) = (L_p^{\mathrm{anal},(i)})$が成り立つ．

(証明のアイデア) 拡大体K_nごとにDirichletの類数公式を用いる議論によって全てのiで$(L_p^{\mathrm{alg},(i)}) \subset (L_p^{\mathrm{anal},(i)})$を示せば全ての$i$で$(L_p^{\mathrm{alg},(i)}) = (L_p^{\mathrm{anal},(i)})$が得られる．よって，実際は$(L_p^{\mathrm{alg},(i)})$が相対的に小さいことをいえばよい．上の簡単な例でも推し量られるかもしれないがイデアル$\mathrm{Char}_R(M)$が小さいことはR-加群Mが大きいことと意味する．結局，

イデアル類群 (の親玉)$X^{(i)}$ が $L_p^{\mathrm{anal},(i)}$ に比べて大きいことをいえばよい. **類体論**によって, $H_n^{(p)}$ を拡大次数が p ベキの K_n の最大不分岐アーベル拡大とするとき $\mathrm{Gal}(K_1/\mathbb{Q})$-作用と両立する同型 $A_n \xrightarrow{\sim} \mathrm{Gal}(H_n^{(p)}/K_n)$ がある. よって, 各 n で $\mathrm{Gal}(K_1/\mathbb{Q})$ が ω^i で共役作用する不分岐準同型 $\mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \longrightarrow D_p = \cup_{r\geq 1}\mathbb{Z}/(p^r)$ で $L_p^{\mathrm{anal},(i)}$ の値に対応するだけ像が大きなものを構成したい. そのためには可約な表現

$$\rho_n^{(i)} :\ G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/p^{r_n}\mathbb{Z}), \quad g \mapsto \begin{pmatrix} 1 & b_n(g) \\ 0 & \omega^i(g) \end{pmatrix}$$

で次の条件をもつものがあればよい.

1. $\rho_n^{(i)}$ は p 以外の素数で不分岐.
2. $\mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \subset G_{\mathbb{Q}}$ に制限すると p の上でも不分岐.
3. $G_{\mathbb{Q}} \longrightarrow \mathbb{Z}/(p^{r_n}),\ g \mapsto b_n(g)$ の像が十分大きい.

実際, $g, g' \in \mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$ $(n \geq 1)$ に対して $\omega^i(g) = 1$ より $b_n(gg') = b_n(g) + b_n(g')$ がわかり準同型 $b_n : \mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \longrightarrow D_p$ を与える. $\rho_n^{(i)}$ の仮定から, b_n は不分岐性や $\mathrm{Gal}(K_1/\mathbb{Q})$ の共役作用に関する望まれた性質をもつ. 問題は $G_{\mathbb{Q}}$ の構造が未知ゆえにこういった要請を満たす $\rho_n^{(i)}$ を構成するのが難しいことである. 唯一の手段が最初の節で述べた代数幾何とエタール・コホモロジーである. Ribet が以前に行っていた研究でモジュラー曲線という特別な曲線が役立つことが知れらていた. モジュラー曲線は次節でも登場するので簡単に触れておきたい. 複素上半平面 $\mathfrak{H}$ には一次分数変換で $SL_2(\mathbb{R})$ が作用する. 自然数 N での合同部分群

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 1, c \equiv 0 \bmod N \right\}$$

による商リーマン面 $\mathfrak{H}/\Gamma_1(N)$ の自然なコンパクト化を $\mathfrak{X}_1(N)$ と記す. $X_1(N)(\mathbb{C}) = \mathfrak{X}_1(N)$ なる $\mathbb{Q}$ 上の代数曲線 $X_1(N)$ がありレベル N のモジュラー曲線と呼ばれる. $X_1(N)$ はよい対称性をもち保型形式や表現論などさまざまな分野に関わる大事な曲線である. GL_2 の局所ラングランズ理論や数論幾何的における有限群スキームの理論など各分野の手法を駆使することで各 n でエタール・コホモロジー $H^1_{\mathrm{et}}(X_1(p^n)_{\overline{\mathbb{Q}}}, D_p)$ の中に上で述べた条件をみたす $\rho_n^{(i)}$ が存在することを示していくことが証明の核心である.

Wiles は, その後単独で一般の総実代数体[11]へ拡張された岩澤主予想を示している. 拡大次数を $g = [F : \mathbb{Q}]$ とすると g 次元ヒルベルト・モジュラー多様体という高次元多様体が関ってくるように一般の総実体では技術的な困難が一気に増大する. Wiles は困難を緩和するために肥田理論を

[11]代数体 F をどう複素数体に埋め込んでも必ず実数体に入るとき F を総実代数体とよぶ, 実 2 次体 $\mathbb{Q}(\sqrt{d})$ は総実代数体の簡単な例である.

積極的に用いている．肥田理論は岩澤理論の一般の簡約代数群 G への一般化にあたり, 一番簡単な代数群 $G = GL_1(F)$ の肥田理論が岩澤理論に対応すると思える．肥田理論によって初めて巨大な環 $\mathcal{O}[[\Gamma]]$ を係数とする「大きなガロア表現」が直接扱えるようになり ($\mathcal{O}$ は $\mathbb{Z}_p$ の有限拡大), $G = GL_2(F)$ の肥田理論から表現 $\rho : G_F \longrightarrow GL_2(\mathcal{O}[[\Gamma]])$ が与えられる．$I = (p$-進函数) なるイデアル $I \subset \mathcal{O}[[\Gamma]]$ によって $\bmod I$ した ρ_I は

$$\rho_I : \ G_F \longrightarrow GL_2(\mathcal{O}[[\Gamma]]/I), \quad g \mapsto \begin{pmatrix} 1 & B(g) \\ 0 & D(g) \end{pmatrix}$$

という表示で $D(g)$ は $\mathbb{Z}_p$-拡大 $\widetilde{F}$ の上のガロア群で自明となり, ρ_I が不分岐性の条件も満たすことや B の像が大きいことも示される．これによって, n ごとにではなく一挙に不分岐準同型 $B : \mathrm{Gal}(\overline{F}/\widetilde{F}) \longrightarrow \mathcal{O}[[\Gamma]]/I$ が構成され, 以前の証明もだいぶ見通しがよくなる．一方で, 一般の総実体 F 上の 2 次元ガロア表現は数論幾何などの困難から未完成な部分もあり, それを補うために擬表現 (pseudo represenation) という新技術を編み出して切りぬけている．擬表現については詳しく述べないが非常に賢いガロア表現の持ち上げのテクニックである．この擬表現は道具として用いていたはずの肥田理論に逆に大きな副産物的進歩をもたらし, 肥田理論の一部を簡略化しその後の発展に寄与している．このあたりに必要な道具は自分で作り上げていく独創性と目的を定めた後の徹底した粘り強さが感じられる．

代数体の岩澤主予想ではイデアル類群の類数公式の精密化を与えるためにモジュラー曲線という代数多様体が活躍した．考えている幾何的対象に対してより大きな幾何的対象のガロア表現のブロックの中にほしい表現を取り出すテクニックは Skinner-Urban らに受け継がれて最近は楕円曲線のセルマー群の類数公式や BSD 予想に対しても Mazur-Wiles の高次元化にあたる仕事が進展しつつあるようである．

4 谷山-志村予想と Fermat 予想

天下りであるが, 自然数 N が存在して前の節で現れたモジュラー曲線からの全射 $X_1(N) \twoheadrightarrow E$ がある楕円曲線 E をモジュラーであるという．$\mathbb{Q}$ 上の楕円曲線 E がモジュラーなことは, $\zeta_E(s)$ が全複素平面に正則に解析接続されて (リーマンゼータのときと類似の)$\zeta_E(s)$ と $\zeta_E(2-s)$ の間の函数等式をもつことと同値であることが Weil によって示されており[12], このことからもモジュラーという概念が自然であると感じられる．

[12]正確には $\zeta_E(s)$ の指標による twist たちに対しても函数等式を仮定する必要がある．

定理 3 (Wiles, Taylor-Wiles/1994). E を半安定な[13] 楕円曲線とするとき, E はモジュラーである.

この定理 3 から次が導かれることは以前に 80 年代後半に Ribet によって示されていた.

系. Fermat 予想はすべての素数 $p \geq 3$ で正しい.

むしろ「定理 3 $\Rightarrow$ 系」が先にわかっていたことが Wiles の 7 年間の長い苦闘を支え続けた強い動機であった. さて, 定理 3 は集合の単射写像

$$\{\mathbb{Q} \text{ 上のモジュラーかつ半安定な楕円曲線 }\} \hookrightarrow \{\mathbb{Q} \text{ 上の全ての半安定な楕円曲線 }\}$$

が全射であるという主張である. もしこれらの集合が有限ならば数え上げて位数を比べたいところかもしれない. 実際は両者は無限集合であり素朴に一対一対応をつけようとしても成すすべがない. Wiles の最初の一歩は, 表面的にはガロア表現と結びつかないこの問題もガロア表現が非常に有効なアプローチであると見抜いたことである. 一般に, d 次元数論的代数多様体 X の p-進ガロア表現 $H^d_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)$ (以下 $H_p(X)$ と略記) は X 自身の幾何的な性質をさまざまに反映し, X の幾何学的性質は線形代数的な対象 $H_p(X)$ で調べがつくことが多い. 実際, 楕円曲線 E に対しては「$H_p(E)$ から E の幾何学的な情報がほぼ回復される」という **Faltings による定理** があることから, モジュラーな楕円曲線 E' で $H_p(E') \cong H_p(E)$ [14]なるものが存在すれば E は元々モジュラーでなければならない. 今ガロア表現が同型なものを同一視した商集合 $\{\mathbb{Q} \text{ 上の全ての楕円曲線 }\}/\sim$ も無限集合でありただガロア表現に問題を移行しただけでは問題の難しさは何も変わらない. Wiles は, ここで素数を注意深く選び, 前人未到の道に踏み込んでいく. $H_p(E)$ を $\bmod p^n$ した $H_p(E)/(p^n)H_p(E)$ は $(\mathbb{Z}/(p^n))^{\oplus 2}$ と同型である. この表現 $G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/(p^n))$ を $\overline{\rho}_{E,p^n}$ と記す. さて, 素数 $p = 3$ で $GL_2(\mathbb{F}_3)$ は可解群となることが非常に大事である. 群論を学ばれた方はご存知のように可解群はアーベル群を積み重ねたアーベル群に非常に近い群である. 類体論や表現論を駆使した Langlands-Tunnell の結果があり, $\overline{\rho}_{E,3}$ が既約表現のときには $\overline{\rho}_{E,3} \cong \overline{\rho}_{E',3}$ なるモジュラーな楕円曲線 E' が存在することが示せる. 一方で素数 $p \geq 5$ では $GL_2(\mathbb{F}_p)$ は非可換単純

[13] 有理数係数の多項式 $f(x) = x^3 + ax + b$ を適当な一次変換で分母を払い $\bmod p$ して位数 p の有限体 $\mathbb{F}_p$ を係数とする多項式 $f_p(x) \in \mathbb{F}_p[x]$ が得られる. すべての素数 $p \geq 5$ でこの $f_p(x)$ が高々2 重根しかもたず, $p = 2, 3$ でも比較的よい状況であるとき $y^2 = x^3 + ax + b$ は半安定な楕円曲線であるという.

[14] もう少し弱く $H_p(E') \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong H_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ で十分である.

群を組成因子として含み, 現代の数論では直接モジュラーな楕円曲線と結びつけるすべがないことに注意したい. 次のような集合を考えよう :

$$R_n = \{\overline{\rho} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/(3^n)) \\ \mid \overline{\rho} \equiv \overline{\rho}_{E,3} \bmod (3) + (\text{若干の局所条件})\}$$

$$T_n = \{\overline{\rho} \in R_n \mid \text{モジュラーな } E'' \text{ があり } \overline{\rho} \cong \rho_{E'',3^n}\}$$

上の Langlands-Tunnell によって $R_1 = T_1$ でありまた各 n で $T_n \neq \emptyset$ である. 各 n で係数環の全射 $\mathbb{Z}/(3^{n+1}) \twoheadrightarrow \mathbb{Z}/(3^n)$ があることより, R_{n+1}, T_{n+1} はそれぞれ R_n, T_n を「持ち上げ」ていると思える. R_n の局所条件を説明しなかったが, 定義より実は勝手な n で $\overline{\rho}_{E,3^n} \in R_n$ である. Faltings の定理によると勝手な n で $\overline{\rho}_{E,3^n}$ が $T_n \subset R_n$ に入ることを示せば E はモジュラーであることがわかる. T_n, R_n それぞれの T_{n+1}, R_{n+1} への持ち上がり具合を表す不変量 $\eta(R_n), \eta(T_n) \in \mathbb{Z}$ があり $\eta(R_n) \geq \eta(T_n)$ は定義から容易である. Wiles は実際, $\eta(R_n)$ があるセルマー群というものを用いて解釈でき, 勝手な n で逆の不等式 $\eta(R_n) \leq \eta(T_n)$ を示すことが現代の岩澤理論の枠内で理解できることを見抜いた. この不等式が示せれば $T_n = R_n$ が従い証明がすべて完了するはずである[15]. このような構想が独力で人知れず行われた研究で進展してきたことは驚きである. さて, Wiles はこの $\eta(R_n) \leq \eta(T_n)$ をオイラー系の理論によって挑戦し華々しく解決を宣言したが論文の最終チェックの段階で証明の核心部分のオイラー系の議論に間違いがあることに気づいた. 修復を試みたがこの方法では修復できなかった[16]. 世界中が注視する大変なプレッシャーの中での長い修復活動も実らずほぼ諦めかけた最後の瞬間でオイラー系の理論の一部と類似のアイデアは含むがより古典的なアプローチで克服することができた.

Wiles の結果は谷山-志村予想という以下の予想を Fermat 予想の証明に必要な半安定の条件下で解決したものであった. この仮定を外すと局所条件に関する技術的困難が増すが Wiles の方針に沿って次の人によって谷山-志村予想自体も完全解決している:

谷山-志村予想 (=Breuil-Conrad-Diamond-Taylor の定理/2001). $\mathbb{Q}$ 上の楕円曲線 E はモジュラーである.

[15]細かくいうと, Langlands-Tunnell らの結果の仮定や R_n が表現可能函手として機能するために $\overline{\rho}_{E,3}$ が既約な必要がある. たいてい $\overline{\rho}_{E,3}$ は既約であるが, そうでない場合は綱渡り的に隣の素数 $p = 5$ での持ち上げの議論を巧みに使ってすべての半安定楕円曲線をカバーすることも Wiles の重要なアイデアである.

[16]Wiles が最初に試みたオイラー系の理論による証明は現在も未完で, この方向で解決ができれば非常に興味深い別証明となるはずである.

上述の Wiles のアイデアをより高次元的な幾何対象のガロア表現に拡張してゼータ函数の “モジュラー性”を示す試みが多くの人々よって盛んに試みられている.

5 最後に

今まで見たように Wiles の研究は一貫して p-進的な方法であり, 岩澤理論の哲学に沿って歩んできたといえる. 最初の節で触れた現代整数論が当面する非アーベルの壁という観点に立ち戻り概観すると, Wiles は楕円曲線という非アーベルな対象のゼータ函数を解析接続する驚くべきブレークスルーを与えた. その方法は, 小さな素数でアーベルな状況と結びつく幸運な偶然をうまく持ち上げていくことでもあり決して非アーベルなものを真っ向からとり扱う幹線道路を建設できたわけではない. しかしそれ以前は目指す山塊は見えていてもそこに至る手段が全くなかった我々に現代でも非アーベルな頂の一部に至る細い道が確かに存在することを指し示した.

特に Wiles の研究はどれも既存の大問題を解決するものでありながら同時に周辺の研究に新しい実りをもたらすようなものが多い. 決して多産でもなく極度な一般化は追い求めないが常にその時代の壁である最も正道の本質的問題に力をしぼり結果を出してくる「センスとそれを支える力強さ」が感じられるのではないだろうか. 一方で, Wiles 氏自身のスタイルには秘密主義なところもあり彼が現在何を目指しているのかははっきりしない. 楕円曲線の BSD 予想に取り組んだりリーマン・ゼータ函数に関する解析数論の予想に興味を示しているなど不確かに伝え聞くが真相は霧の中である. Wiles の数学を足早に眺めてみると, 常に何をしたいかという強い気持ちとしっかりした問題意識がことさらに伝わってくる. 時代精神の変化に伴って我々と数学との関わりは今日も変化にさらされ続けている. Wiles の精神も吸収し引き継ぎながら我々は常に数学に伝統と変化のバランスのとれた新しい息吹をこめていかねばならない.

この連載の本来の目的である学部や大学院初期の学生への周辺事項の勉強の指針のための簡単な参考文献やガイドを述べて本稿を終わりとしたい. 数学の知識を仮定せずにフェルマーの定理の解決のドラマや数学者の生態についてよく書かれた本として「フェルマーの最終定理」サイモン・シン著 (新潮社) をあげておきたい. これから専門として周辺分野に進む方には素養として代数的整数論, 楕円曲線, 保型形式, 可換環論及び代数幾何, p-進数などが大切な要素である. 近年和書洋書ともに多くの良書があるのでしっかりと身に着けておかれることをおすすめしたい. もう少し専

門的には,「数論 II」(黒川, 栗原, 斉藤共著) が一般の出版物としては岩澤理論を扱っている初めての和書である. また「フェルマー予想 1」(「フェルマー予想 2」は近刊予定)(斉藤毅著) なども証明と関連する理論を解説した教科書である. 岩澤理論に次いで 3 節および 4 節の内容に関わる肥田理論については和書ではまだ適当なものは見当たらないが「Elementary theory of L-functions and Eisenstein series」(肥田晴三著) の特に 7 章がコンパクトな導入であり先に述べた擬表現についても説明がある. 本記事においては 2 節, 3 節, 4 節と 3 つに分けて説明したがそれぞれのテーマにおいて Wiles 自身による関連論文が数編ある. Fermat 予想の証明の論文をはじめとして序文などから熱が伝わってくるものも多く, さらに進んだ勉強を手がける方は Wiles の原論文も眺められたい.