$R = T$ 定理の仕組みとその応用

安田 正大

この講座では, Fermat 予想の証明のために Wiles, Taylor-Wiles が確立した $R = T$ 定理に関する最近の発展と応用についてお話します.

この原稿は数学の専門家でない方を対象にして書かれており, 内容の正確さよりも, 大体の感じをつかんでもらうことを目標としています. 読者に難解な印象を与えないようにするために, 専門家向けの文章では許されないようなあいまいな表現の仕方をあえてしている部分があります.

1. Fermat 予想

まず Fermat 予想とは何か, ということからお話したいと思います. Fermat はフランス人で, 17 世紀, 今から約 400 年前に生まれた人です. そのころ日本は江戸時代です. 大体同じ時代の人に Descartes (デカルト) とか Corneille (コルネイユ), Milton (ミルトン), Velázquez (ベラスケス), Rembrandt van Rijn (レンブラント), 日本では狩野探幽, 西山宗因, 由井正雪がいます. Fermat 予想とは, Fermat が証明を見つけたと述べた主張で, その証明を Fermat は書かず, 1995 年に Wiles が証明するまで誰も正しく証明することができなかったので Fermat 予想と呼ばれています. 同じ主張を Fermat の大定理とか Fermat の最終定理とか呼ぶ人もいます. ご存知の方も多いかとは思いますが, Fermat 予想というのは次の主張です:

定理 1.1. *(Fermat 予想, Wiles の定理)* n を 3 以上の整数とするとき, 等式

$$a^n + b^n = c^n \tag{1.1}$$

を満たす 3 つの 0 でない整数は存在しない.

ここで整数とは 1, 2, 3, ... といった, いわゆる数のことをいいます. あと 0 やマイナスの -1, -2,... なども整数に含めます. $1/2$ や円周率 π, $\sqrt{-1}$ などは整数ではありません. 整数の全体を集合とみなし, 普通 $\mathbb{Z}$ という記号で書きます. 整数のほかに重要な数の概念として有理数, 実数, 複素数があります. それぞれの全体を通常 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ という記号で書きます. 有理数とは, 整数を 0 でない整数で割った形の数のことです. 実数, 複素数の正確な定義は少し難しいのでこの講座では与えませんが, 実数の全体 $\mathbb{R}$ を図に表すといわゆる数直線に, 複素数の全体 $\mathbb{C}$ を図に表すといわゆる複素平面となります.

$n = 4$ の場合の定理 1.1 の証明は Fermat 自身が知っていたようです. $n = 3$ の場合は Fermat よりも 100 ほど後に生まれた Euler が証明しました. n が, n よりも小さい 3 以上の整数 n' で割り切れるとき, n に対する定理は n' に対する定理から従いますから, もともと

(*) n は 3 と $n-1$ の間にあるどんな整数でも割り切れない

という条件を満たす n についてだけ定理を証明すれば十分です. さて重要な整数に素数というものがあります. 2 以上の整数 n であって 2 と $n-1$ の間にあるどんな整数でも割り切れないものを素数とよびます. 2 が一番小さい素数で, 素数を小さい順に書いてゆくと 2, 3, 5, 7, 11, ... という具合になります. 素数は無限にたくさんあります. この素数という概念を使うと, 上の条件 (*) は $n = 4$ または n は 3 以上の素数, と書くことができます. $n = 4$ のときは予想は証明されていますから, n が 3 以上の素数の場合に定理 1.1 を証明すれば十分です. 素数のことを普通 p や ℓ といった記号で表します. 以下では ℓ とかけば素数を表すものとし, $n = \ell \geq 3$ に対する定理 1.1 を定理 1.1_ℓ で表します. $n = 3$ の場合の予想は Euler が証明しました. 今年生誕 300 年です. 19 世紀には Kummer という人が現れ, かなり多くの ℓ に対して定理 1.1_ℓ を証明しました.

Kummer の証明は, 今の言葉でいうと円分体の整数論というものを用いる方法です. その後も Fermat 予想については Kummer の方法の延長線上にある方法で研究するのが主流だったのですが, 1980 年代に入って, Frey [Fr] がまったく違うアプローチを提唱しました. それは Hellegauarch が 1960 年代に思いつき, 現在 Frey 曲線とよばれているものを用いるやり方です. Frey 曲線とは, 定理 1.1_ℓ の反例 $a^\ell + b^\ell = c^\ell$ が与えられるごとに定義されるもので,

$$y^2 = x(x - a^\ell)(x + b^\ell) \tag{1.2}$$

という式で与えられます. ここで x, y は変数です. これは 2 個の変数 x, y に対する 1 個の関係式で与えられるので, 2 ひく 1 で 1 次元的な対象, 正確にいうと 1 次元の代数多様体というものになります. 1 次元の代数多様体のことを代数曲線というのが普通なので Frey 曲線といういい方をします.

式 (1.2) で定義される代数曲線に無限遠点 ∞ を付け加えたものを $E_{a,b}$ とおきます. 正確にはこの $E_{a,b}$ のことを Frey 曲線とよびます. $E_{a,b}$ は楕円曲線と呼ばれる, 特別なタイプの代数曲線となります. 式 (1.2) の係数がすべて整数, とくに有理数なので, Frey 曲線は $\mathbb{Q}$ 上の楕円曲線となります.

ここで考えている反例 $a^\ell + b^\ell = c^\ell$ において, 条件 a, b, c の最大公約数が 1 であり, さらに $a+1$ が 4 の倍数で b が偶数であると仮定しても一般性を失わないのでそう仮定することにします. このとき楕円曲線 $E_{a,b}$ が存在するとすると, 非常におかしなことが起こるということに Frey は気づきました. 一般に有理数体上の楕円曲線 E が与えられると, E の極小判別式と呼ばれる整数 Δ_E と E の導手と呼ばれる正の整数 N_E とが定まります. E の導手のほうが E の極小判別式の絶対値よりも小さいのですが, $E = E_{a,b}$ に関しては N_E が Δ_E と比べて極端に小さくなります. ところが Szpiro の予想[1]という予想があって, E の導手が E の極小判別式と比べて極端に小さくなることはないと思われているので $E_{a,b}$ が存在するとするとおかしなことになります.

Fermat 予想は, なぜ式 (1.1) に注目しているのかいまひとつはっきりせず, そういう意味で最近の数学の立場からはそれほど重要な問題であると思われていないのですが, Szpiro 予想に出てくる Δ_E と N_E とはともに重要な量であり, そのためこの 2 つの量を比較する Szpiro 予想は重要な問題だと思われます. E の判別式というのは E を $y^2 = f(x)$ に無限遠点を付け加えたものとして記述したとき, $f(x) = 0$ の根の差積の 16 倍のことをいいます. 楕円曲線の表示は色々考えられ, 表示によって判別式の値は違います. 判別式の値の絶対値が最小になるような表示に対する判別式を極小判別式といいます. 極小判別式を定義する際には, $y^2 = f(x)$ の形の表示だけではなく, $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (ここで a_1, a_2, a_3, a_4, a_6 は整数, [2]) という形の表示も本当は考えなくてはいけません. 導手を説明することは極小判別式を説明することよりも多少難しいのですが, 後に出てくる谷山-志村予想や Wiles の証明を理解するために導手をある程度理解しておくことは重要です. 導手というのは, 一般に (十分良い条件を満たす) Galois 表現というものに対して定義される値です. Galois 表現については後ほど説明します. 楕円曲線が与えられるとそれに付随して Galois 表現ができるので, その Galois 表現の導手のことを楕円曲線の導手とよびます. 導手がなぜ重要かというと, 楕円曲線の L 関数というものがあるのですが, それの解析的性質に導手が深く関わるということが谷山-志村予想の帰結としてわかるからです.

Fermat 予想の反例と Frey 曲線とを結びつける発想を一般化して, 0 でない 3 整数 a, b, c に関する等式 $a + b = c$ と, 楕円曲線 $y^2 = x(x - a)(x + b)$ とを結びつけて考えることもできます, このとき Szpiro 予想が何を意味するのかを考えることによって, Masser と Oesterlé は abc 予想と呼ばれる次の予想に到達しました[3]:

---

[1]予想の主張は以下の通りです: 任意の実数 $\varepsilon > 0$ に対し, 実数 $C(\varepsilon) > 0$ が存在して, $\mathbb{Q}$ 上の任意の楕円曲線 E に対し $\Delta_E \leq C(\varepsilon) N_E^{6+\varepsilon}$ が成り立つ.

[2]a_5 が出てこないで a_6 が出てくるのですがこれは誤植ではありません

[3]予想 1.2 の主張中の $N^{1+\epsilon}$ を $N^{6/5+\epsilon}$ に弱めたものが, $y^2 = x(x-a)(x+b)$ の形に表せる楕円曲線 E に制限した Szpiro 予想と同値になります.

予想 1.2. 任意の実数 $\varepsilon > 0$ に対して実数 $C(\epsilon) > 0$ が存在して次を満たす: 正の整数 a, b, c が $a+b=c$ を満たし, さらに a と b の最大公約数が 1 であるとき, a, b, c のいずれかを割り切る素数の積を N とすると, 不等式

$$c < C(\epsilon)N^{1+\epsilon} \tag{1.3}$$

が成立する.

この予想が正しいとすると Fermat 予想が十分大きな n について正しいことがわかります. この abc 予想には, 不等式 (1.3) にいくつかのバリエーションがあり, もっと精密な評価を与えるものもあります. この研究所の望月新一さんもこの予想に取り組んでいます.

Fery 曲線と関連させることにより, Fermat 予想は上述の Szpiro 予想だけでなく, 谷山-志村予想とよばれる $\mathbb{Q}$ 上の楕円曲線に関する予想と結びつきます. Frey 曲線を考察することにより, 谷山-志村予想から Fermat 予想が従うのではないかという Frey のアイデアを整備した Serre [Se2] は, 現在では Serre 予想とよばれる予想を定式化しました. その後 Ribet [R] が Serre 予想の一部を解決することによって, 実際に Fermat 予想を谷山-志村予想に帰着させました. この谷山-志村予想というのは, Langlands 予想, Langlands 対応, あるいは Langlands 哲学とよばれるより一般的な予想の特別な場合とみなせます. Langlands 予想というのは, たいへん綺麗な形をしている予想で, 広範な応用があり, なおかつ正しいと思われる証拠がたくさんあります.

2. 体, 群, Galois 理論

Frey 曲線を使って Fermat 予想を谷山-志村予想に帰着させるアイデアを説明するために, 代数学の基本的な概念である, 体, 群, Galois 理論について説明する必要があります.

体と群は, 適当な付加構造をもつ集合の呼称です. 体と群について述べる前に, 集合とはどんな感じのものであるかを話します. S を集合とすると, S は S の元と呼ばれるもので成り立っています. x が S の元であるということを $x \in S$ で表します. このとき, x は S に属する, ともいいます. 元 $x \in S$ と元 $y \in S$ とが等しいことを $x = y$ と書き, 異なることを $x \neq y$ と書きます. 集合 T が 集合 S の部分集合であることを $T \subset S$ または $S \supset T$ という記号で表します. $T \subset S$ のとき, S に属し T に属さない元の全体を $S \setminus T$ で表します.

有限個の元からなる集合を有限集合といいます. S を有限集合とするとき, S の元の個数を $\sharp S$ と書きます. $\sharp S$ を $|S|$ と書く人もいます. S, S' を集合とすると, S と S' との直積という集合 $S \times S'$ が定まります. 定義は $S \times S' = \{(x, x') \mid x \in S, x' \in S'\}$ です.

S, S' を集合とします. S の各元ごとに S' の元を割り当てる規則のことを S から S' への写像とよびます. S から S' への写像 f のことを $f : S \to S'$ と書きます. f によって $x \in S$ に $x' \in S'$ が割り当てられているとき, f は x を x' に送る (またはうつす), とか f は x に x' を対応させる, などといいます. このとき $x \mapsto x'$ とも書きます. また x' のことを x の f による像または f の x における値とよび $f(x)$ と書きます. さらに集合 S'' と写像 $g : S' \to S''$ が与えられると, $x \in S$ を $g(f(x)) \in S''$ に送ることにより S から S'' への写像ができますが, この写像を f と g との合成とよび $g \circ f : S \to S''$ という記号で表します.

$f : S \to S'$ を写像とします. 部分集合 $T \subset S$ に対し $f(T) = \{f(x) \mid x \in T\}$ とおきます. これは S' の部分集合となります. $f(T)$ のことを f による T の像と呼びます. $T = S$ のとき, $f(S)$ のことを f の像とよび, $\mathrm{Im}\, f$ と書きます. $x' \in S'$ のとき, S の部分集合 $\{x \in S \mid f(x) = x'\}$ を f による x の逆像とよび, $f^{-1}(x')$ で表します. $T' \subset S'$ のとき, S の部分集合 $\{x \in S \mid f(x) \in T'\}$ を f による T の逆像とよび, $f^{-1}(T')$ で表します. 写像 $f : S \to S'$ が単射であるとは, f が (任意の) 異なる S の 2 元を異なる S' の 2 元に送ることをいいます. 写像 $f : S \to S'$ が全射であるとは, $\mathrm{Im}\, f = S'$ を満たすことをいいます.

足し算, 引き算, 掛け算, 0 でない割り算が定義されている集合のことを体とよびます. 例えば $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は通常の四則演算で体となります. $\mathbb{Z}$ は割り算について閉じていないので体にはなりません. 他の体の例と

して有限体というものがあります. 有限体とは有限個の元からなる体のことをいいます. 有限体の元の個数はある素数 p の巾になっています. この p をその有限体の標数とよびます.

割り算を除いた足し算, 引き算, 掛け算の 3 つが定義されている集合のことを可換環とよびます. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ はすべて可換環となります. 可換環の可換というのは掛け算が交換法則 $xy = yx$ を満たすという意味です. 足し算, 引き算, 掛け算の 3 つが与えられているが, 掛け算が交換法則を満たさないようなものを考えることもあります. このようなものを単に環とよびます. 例えば 2×2 行列の集合 $M_2(\mathbb{Z})$, $M_2(\mathbb{R})$ などは可換環でない環となります.

群とは 2 項演算がひとつ定義されている集合 G であって, 2 項演算 $G \times G \to G$ を $(g_1, g_2) \mapsto g_1 g_2$ と書くことにしますと, 3 条件 (1) 結合法則: $(g_1 g_2)g_3 = g_1(g_2 g_3)$, (2) 単位元の存在: $1 \in G$ が存在して $g1 = 1g = g$ が任意の $g \in G$ に対して成り立つ, (3) 逆元の存在: 任意の $g \in G$ に対して $gh = hg = 1$ を満たす $h \in G$ が存在する, を満たすもののことをいいます. 群の例をあげます. X を集合とすると, 全単射 $X \to X$ の全体には, 写像の合成を演算とすることによって群の構造が入ります. この群を $\mathrm{Aut}(X)$ と書きます. また, R を環としますと, $R^\times = \{x \in R \mid xy = 1, \exists y \in R\}$ は掛け算を演算とすることによって群となります. 群 $(M_n(R))^\times$ のことを $\mathrm{GL}_n(R)$ と書きます. R が可換環のとき, 行列式 $\det : M_n(R) \to R$ というものが定義されます. 例えば $n = 2$ のとき $\det(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc$ です. このとき $\mathrm{GL}_n(R) = \{x \in M_n(R) \mid \det(x) \in R^\times\}$ が成り立っています. 群の他の例として基本群というものもあります. 一般に位相空間 X と点 $x \in X$ が与えられると基本群 $\pi_1(X, x)$ という群が定義できます. これは x を基点とするループ (連続写像 $\gamma : [0, 1] \to X$ あって $\gamma(0) = \gamma(1) = x$ を満たすもの) の適当な同値類の集合に適当な方法で群演算を入れたものです.

群 G の集合 X への作用とは, 群の演算を保つ写像 $G \to \mathrm{Aut}(X)$ のことをいいます. 群 G が集合 X に作用しているとき, X の空でない部分集合であって, G の作用で閉じている極小のものを X の G 軌道とよびます. X の G 軌道の全体を $G\backslash X$ で表します. 群 G の部分群というのは, 群の演算で閉じている部分集合 $H \subset G$ であって, その演算で H が群になるようなもののことをいいます. 同様に体 K の部分体, 環 R の部分環という概念が定義されます. 体 K' が体 K の部分体であるとき, K は K' の拡大体であるといいます. H を群 G の部分群とすると, 群 H は G を集合とみなしたものに $h \mapsto (g \mapsto hg)$ によって作用します. 集合 $H\backslash G$ が有限集合のとき, H を G の指数有限の部分群であるといい, $H\backslash G$ の元の個数を $[G : H]$ で表します. G, G' を 2 つの群とするとき, 集合としての直積 $G \times G'$ には自然に群の構造が定まります. この群 $G \times G'$ を群 G と群 G' との直積と呼びます. 同様に R, R' を 2 つの環とするとき, 集合としての直積 $R \times R'$ に環の構造が定まります. この環 $R \times R'$ のことを環 R と環 R' との直積と呼びます. R と R' がともに可換環のとき, $R \times R'$ も可換環となります. G, G' を 2 つの群とするとき, 写像 $G \to G'$ であって群の演算を保つものを群の準同型といいます. 同様に R, R' を 2 つの環とするとき, 写像 $R \to R'$ であって環の演算 (足し算, 引き算, 掛け算) を保つものを環の準同型といいます. $f : G \to G'$ を群の準同型とします. このとき $\mathrm{Im}\, f$ は G の部分群となります. また G' の単位元の逆像 $f^{-1}(1)$ のことを f の核とよび, $\mathrm{Ker}\, f$ と書きます. $\mathrm{Ker}\, f$ は G の部分群となります. ある G' とある f に対して $\mathrm{Ker}\, f$ の形に書ける G の部分群のことを G の正規部分群とよびます. 例えば R を可換環とするとき, 行列式写像 $\det$ を $\mathrm{GL}_n(R) \subset M_n(R)$ に制限したもの $\mathrm{GL}_n(R) \to R^\times$ は群の準同型となります. この準同型の核を $\mathrm{SL}_n(R)$ とおきます. これは群 $\mathrm{GL}_n(R)$ の正規部分群となります. H を G の正規部分群とするとき, 集合 $H\backslash G$ には自然に群の構造が入ります. これを G の H による商群とよびます. このとき $H\backslash G$ は通常 G/H という記号で書かれます.

アーベル群とは, 群であって群演算が交換法則を満たすもののことをいいます. たとえば $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は足し算を演算とするアーベル群となります. このときの単位元は 0 です. アーベル群の群演算は足し算の記号で書き, 単位元を 0 と書くのが普通です. ただし可換環 R に対する $R^\times$ のような場合は例外で, 演算を掛け算で書き, 単位元を 1 と書きます. アーベル群の任意の部分群は正規部分群となり, その商群はアーベル群となります. n を整数とすると, n の倍数全体 $n\mathbb{Z}$ は $\mathbb{Z}$ の部分群となります. このとき商群　$\mathbb{Z}/n\mathbb{Z}$ には足し算だけでなく掛け算が定義できて, これは可換環となります. p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ は有限体となりま

す. この体を $\mathbb{F}_p$ と書きます. X, X' をアーベル群とするとき, 直積 $X \times X'$ もアーベル群となります. このアーベル群を通常 X と X' との直和とよび, $X \oplus X'$ で表します.

体 F であって, 条件 (*): 四則演算を保つ写像 (つまり環準同型) $F \to \mathbb{C}$ が存在し, かつその個数が有限個, を満たすものを (有限次) 代数体とよびます. 四則演算を保つ写像 $F \to \mathbb{C}$ の個数を F の $\mathbb{Q}$ 上の次数と呼び, $[F:\mathbb{Q}]$ で表します. 後の節で体上のベクトル空間という概念が出てきますが, ベクトル空間の用語を用いると, 体 F が代数体であることと, F が $\mathbb{Q}$ を含み, かつ F が $\mathbb{Q}$ ベクトル空間として有限次元であることとは同値となります. さらに F の $\mathbb{Q}$ ベクトル空間としての次元は $[F:\mathbb{Q}]$ に等しくなります. 一般に体 K を体 K' の拡大体とするとき, K の K' ベクトル空間としての次元を $[K:K']$ で表します. $[K:K'] < \infty$ のとき K は K' の有限次拡大であるといいます.

$\mathbb{C}$ に含まれるすべての代数体の合併を $\overline{\mathbb{Q}}$ と書きます. $\overline{\mathbb{Q}}$ も体となりますがもはや (*) を満たしません. 全単射 $\overline{\mathbb{Q}} \xrightarrow{\simeq} \overline{\mathbb{Q}}$ であって四則演算を保つものの全体を $G_{\mathbb{Q}}$ で表し, これを $\mathbb{Q}$ の絶対 Galois 群とよびます. これは写像の合成を演算とすることによって $G_{\mathbb{Q}}$ は群となります. Galois の理論という理論があって $\overline{\mathbb{Q}}$ に含まれる代数体 F と $G_{\mathbb{Q}}$ の指数有限の部分群 H との間に 1 対 1 対応が存在します. 代数体 $F \subset \overline{\mathbb{Q}}$ が部分群 $H \subset G_{\mathbb{Q}}$ に対応するとき, $H = \{\sigma \in G_{\mathbb{Q}} \mid \sigma(x) = x, \forall x \in F\}$, $F = \{x \in \overline{\mathbb{Q}} \mid \sigma(x) = x, \forall \sigma \in H\}$ が成り立っていて, これによって対応が与えられています. 代数体 $F \subset \overline{\mathbb{Q}}$ が $H \subset G_{\mathbb{Q}}$ に対応するとき, $[F:\mathbb{Q}]$ は集合 $H\backslash G_{\mathbb{Q}}$ の元の個数に一致します. また H のことを F の絶対 Galois 群と呼び G_F で表します. F, F' を $\overline{\mathbb{Q}}$ に含まれる代数体とすると, F' が F の拡大体であることと $G_{F'}$ が G_F の部分群であることとは同値になります. さらに $G_{F'}$ が G_F の正規部分群であるとき, F' は F の Galois 拡大体であるといいます. ここでは代数体についてのみ絶対 Galois 群を定義したのですが, 任意の体 K に対して, K の分離閉包とよばれる体 $\overline{K}$ をひとつ選ぶことによって, K の絶対 Galois 群という群 G_K を導入でき, K の拡大体に関する Galois 理論が展開できます. 例えば有限体 k の絶対 Galois 群 G_k は $\widehat{\mathbb{Z}}$ と書かれるアーベル群で, Frobenius 置換と呼ばれる特別な元 $\mathrm{Frob}_k \in G_k$ で (位相的に) 生成されます.

3. 楕円曲線の等分点のなす群

Frey 曲線 $E_{a,b}$ に話をもどします. $E_{a,b}$ の存在から矛盾を導くためのアイデアとして Serre は $\mathbb{Q}$ 上の楕円曲線 $E_{a,b}$ の等分点から得られる $G_{\mathbb{Q}}$ 加群に注目しました.

一般の $\mathbb{Q}$ 上の楕円曲線 E はある整数係数のモニックな 3 次多項式 $f(x) = x^3 + Ax^2 + Bx + C$ (A, B, C は整数) に対し, 式 $y^2 = f(x)$ で定義される代数曲線に無限遠点を付け加えて得られます. $f(x)$ のとり方は一意的ではありません. 逆に $f(x)$ が整数係数のモニックな 3 次多項式のとき $f(x) = 0$ が重根を持たなければ, 式 $y^2 = f(x)$ で定義される代数曲線に無限遠点を付け加えたものは $\mathbb{Q}$ 上の楕円曲線となります.

集合 $E(\mathbb{C}) = \{\infty\} \cup \{(x,y) \mid x, y \in \mathbb{C}, y^2 = f(x)\}$ を考えます. これは Riemann 面となります. Riemann 面とは, 複素平面 $\mathbb{C}$ を複素解析的に切り貼りしてできる図形のことです. $E(\mathbb{C})$ はドーナツの表面のような形をしています. ∞ を通るループ $\gamma : [0,1] \to \mathbb{C}$ に対し, 積分 $\int_\gamma \frac{dx}{2y}$ を考えるとこの値は収束し, しかも基本群 $\pi_1(E(\mathbb{C}), \infty)$ における γ の類にしか依存しないことがわかります. さらに得られる写像 $\pi_1(E(\mathbb{C}), \infty) \to \mathbb{C}$ は群の準同型になります (ただし $\mathbb{C}$ には足し算で群の構造を入れます). この準同型の像を Λ と書くことにします. $P \in E(\mathbb{C})$ に対し, ∞ と P とを結ぶ道 γ を取り, 積分 $\int_\gamma \frac{dx}{2y}$ を考えるとこの値は収束します. さらにこの値の商アーベル群 $\mathbb{C}/\Lambda$ における類は E と P にのみ依存し, γ の取り方に依存しません. P に $\int_\gamma \frac{dx}{2y}$ を対応させることによって写像 $E(\mathbb{C}) \to \mathbb{C}/\Lambda$ が得られますが, 実はこれが全単射となります. $\mathbb{C}/\Lambda$ はアーベル群なので, この全単射を通じて $E(\mathbb{C})$ にはアーベル群の構造が入ります. ∞ がこのアーベル群の単位元となります.

整数 n に対し $E[n] = \{\infty\} \cup \{(x,y) \in E(\mathbb{C}) \mid \overbrace{(x,y) + \cdots + (x,y)}^{n \text{ 個}} = \infty\}$ とおきます. これは $E(\mathbb{C})$ の部分アーベル群となります. $E[n]$ は元の個数が n^2 個のアーベル群となります. $(x,y) \in E[n]$ のとき, $x, y \in \overline{\mathbb{Q}}$

であることが分かります. 従って集合 $E[n]$ に群 $G_{\mathbb{Q}}$ が作用します. さらに $G_{\mathbb{Q}}$ はアーベル群 $E[n]$ に作用していることが分かります.

ここで ℓ を 3 以上の素数, $a^\ell+b^\ell=c^\ell$ を条件 (1) を満たす予想 1.1 の反例とし, E が Frey 曲線 $E=E_{a,b}$ の場合を考えます. ここでアーベル群 $E_{a,b}[\ell]$ への群 $G_{\mathbb{Q}}$ の作用を考えると, 非常に分岐が小さいという不自然なことがおこっています. 最後の文の意味を理解するために, 代数体の分岐の理論というものを知る必要があります. これを説明するために代数的整数論の基本的な概念をいくつか導入します. [4]

4. 素点の集合, 局所体, 分岐

代数体の理論は, Riemann 面の理論の類似で捉えられます. 先ほどドーナツの表面の形をした Riemann 面 $E(\mathbb{C})$ が出てきましたが, Riemann 面にはドーナツではなくてもっとたくさん穴の開いたお菓子の表面のような形をしたものがあります. 穴のないものもあります. こういった Rimann 面の間の複素解析的な写像 $f: X\to Y$ で, 定数でないものを考えます. その写像は全射で Y の各点の逆像は有限集合になります. 逆像の $f^{-1}(y)$ 元の個数は有限個を除くすべての点 $y\in Y$ で同じで, 残りの有限個の点ではそれよりも少なくなります. $f^{-1}(y)$ の元の個数が少なくなるような点 $y\in Y$ のことを f の分岐点とよびます.

F を代数体とすると, F の素点の集合と呼ばれる無限集合 S_F が定まります. $F=\mathbb{Q}$ のとき S_F は素数全体の集合 $\{2,3,5,7,\ldots\}$ に無限素点とよばれる元 ∞ を付け加えたものです. 2 つの代数体 $F\subset F'$ に対して写像 $S_{F'}\to S_F$ が定まります. この写像は全射で S_F の各元の逆像は有限集合となります. $v'\in S_{F'}$ の像が v のとき, $v'|v$ と書き, v' は v の上にある, または v は v' の下にあるといいます. 代数体 F は $\mathbb{Q}$ を部分体に持つことから, F の任意の素点 v に対して, v の下にある $\mathbb{Q}$ の素点 w がただひとつ定まります. $w=\infty$ のとき v を無限素点, そうでないとき v を有限素点とよびます. 有限素点 v に対しては v での剰余体 k_v という有限体が定まります. $v'|v$ のとき k_v は $k_{v'}$ の部分体となります. 有限個を除くすべての $v\in S_F$ に対して等式 $\sum_{v'|v}[k_{v'}:k_v]=[F':F]$ が成り立ちます. ここで $[k_{v'}:k_v]$ は $[F':F]$ と同様の方法で定義されます (v が無限素点のときは k_v, $k_{v'}$ が定義されていませんが, このときは $[k_{v'}:k_v]=1$ と約束します). この等式が成り立たないとき F'/F は v で分岐するといいます.

$S_{\overline{\mathbb{Q}}}$ を射影極限 $\varprojlim_F S_F$ として定義します. ここで F は $\overline{\mathbb{Q}}$ に含まれる代数体をすべて動きます. 群 $G_{\mathbb{Q}}$ が集合 $S_{\overline{\mathbb{Q}}}$ に作用します. 各代数体 $F\subset\overline{\mathbb{Q}}$ に対して, 全射 $S_{\overline{\mathbb{Q}}}\to S_F$ が定まります. この写像が $w\in S_{\overline{\mathbb{Q}}}$ を $v\in S_F$ に送るとき $w|v$ と書くことにします. $v\in S_F$ に対して $w|v$ となる $w\in S_{\overline{\mathbb{Q}}}$ をとり, G_F における w の固定部分群を G_{F_v} で表します. この群を F の v での分解群とよびます. G_{F_v} は w の取り方に依存するのですが, w を取り替えたときの違いはあまり大きなものではないので w は省略して書きます. F の各素点 v に対し, 完備化という操作によって F を部分体として含む体 F_v が定まり, G_{F_v} は F_v の絶対 Galois 群と同型になります.

$F=\mathbb{Q}$, $v=p$ のとき $F_v=\mathbb{Q}_p$ は p 進数のなす体と呼ばれるものになります. 私たちは普段 10 進法を用いて数, 整数や実数を記述しているのですが, 2 進法とか 3 進法とかでも整数や実数を記述できます. このなんとか進法というのと今出てきた p 進数というのは少し関係があります. p を素数としますと, 0 から $p-1$ までの数に文字を割り当てて実数を p 進法で書くことができます. 普通の実数の p 進法による表記では小数点より上が有限で, 小数点以下が無限に続きうるのですが, p 進数というのは小数点以下が有限で小数点より上が無限に続きうるような表記をもちます. 通常の感覚と異なり高い位の数字になればなるほど重要でなくなります. 小数点以下がでてこない p 進数の全体は $\mathbb{Q}_p$ の部分環となります. この部分環を $\mathbb{Z}_p$ と書きます. 整数 $n\geq 1$ が素数でない場合も p 進数と同じようにして n 進数を考えることができます.
その場合は足し算と掛け算が定義でき可換環にはなりますが, n が素数の巾でない場合は割り算の定義が必ずしもできないため体にはなりません. 実数の p 進表記というのは, p をいろいろと取り替えても, 同じ実数の異なる記述の仕方を与えるにすぎないのですが, p 進数のなす体 $\mathbb{Q}_p$ は p を取り替えるとまったく同型

[4] より詳しいことは [高木], [ノ], [藤崎-森田-山本] をご参照ください.

から程遠い体になります. 代数体 F の素点 v が素数 p の上にあるとき, F_v は $\mathbb{Q}_p$ の有限次拡大体となります. このような体を p 進体とよびます. v が ∞ の上にあるとき F_v は $\mathbb{R}$ または $\mathbb{C}$ と同型になります.

代数体 F に対し, その整数環と呼ばれる部分環 $\mathcal{O}_F \subset F$ が定まります. 同様に F の有限素点に対し, 局所体 F_v の整数環と呼ばれる部分環 $\mathcal{O}_{F_v} \subset F_v$ が定まります. v が素数 p の上にあるとき, $\mathcal{O}_{F_v}$ は $\mathbb{Z}_p$ を部分環として含みます. また可換環 $\mathcal{O}_{F_v}$ から F_v の剰余体 k_v への全射準同型が定まります. さらに標準的な全射準同型 $G_{F_v} \to G_{k_v}$ が存在します (ここで v が ∞ の上にあるときは $G_{k_v} = 1$ と約束します). この核を I_{F_v} と書き G_{F_v} の惰性群とよびます. ∞ の上ある F の素点 v に対しては, $I_{F_v} = G_{F_v}$ とおきます. F の素点からなる集合 S に対し, 全ての $v \notin S$ に対する $I_{F,v}$ を含むような最小の G_F の (閉) 正規部分群による G_F の商を $G_{F,S}$ と書きます. $v \notin S$ のとき, 合成 $G_{F_v} \to G_F \to G_{F,S}$ は $G_{F_v}/I_{F,v} \cong G_{k.v}$ を経由します. 誘導される写像 $G_{k_v} \to G_{F,S}$ による $\mathrm{Frob}_{k_v} \in G_{k_v}$ の像を Frob_v とおきます.

5. 圏

Galois 表現について述べる前に, 圏について説明します. [5] 圏 $\mathcal{C}$ は (1) $\mathrm{Obj}(\mathcal{C})$ というクラス, (2) $\mathrm{Obj}(\mathcal{C})$ の各元 X, Y に対する集合 $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, (3) $\mathrm{Obj}(\mathcal{C})$ の各元 X に対する元 $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$, (4) $\mathrm{Obj}(\mathcal{C})$ の各元 X, Y, Z に対する写像

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z) \tag{5.1}$$

から成ります. これらの間に適当な関係式を要請します. $\mathrm{Obj}(\mathcal{C})$ の元を $\mathcal{C}$ の対象, 集合 $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ の元を X から Y への射とよびます. 対象を点, 射を矢印のように思うと圏の感じをイメージしやすいかと思います. f が集合 $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ の元であるということをしばしば $f : X \to Y$ とも書きます. 上の写像 (5.1) は, 2 つの矢印があって, 一方の矢印の終点ともう一方の矢印の始点とが一致するとき, 2 つの矢印をつなげて新たな矢印が得られる, ということを意味します. $f : X \to Y$ と $g : Y \to Z$ をつなげたものを $g \circ f : X \to Z$ と書きます. 要請する適当な関係式のうち最も重要なものは, この矢印のつなげ方に対する結合法則です. 例えば, G を群とするとき, (1) $\mathrm{Obj}(\mathcal{C}) = \{X\}$, (2) $\mathrm{Hom}_{\mathcal{C}}(X, X) = G$, (3) $\mathrm{id}_X = 1$, (4) 群演算 $\mathrm{Hom}_{\mathcal{C}}(X, X) \times \mathrm{Hom}_{\mathcal{C}}(X, X) = G \times G \to G = \mathrm{Hom}_{\mathcal{C}}(X, X)$ という 4 つのデータは圏を与えます. この圏はすべての射が同型になるという意味で特殊な圏です. 一般に圏 $\mathcal{C}$ の射 $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ が同型であるとは, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ が存在して, $f \circ g = \mathrm{id}_Y$, $g \circ f = \mathrm{id}_X$ が成立することをいいます. このようにすべての射が同型となる圏のことを亜群とよびます. 圏 $\mathcal{C}$ の対象 X, Y に対し, 同型射全体のなす $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ の部分集合を $\mathrm{Isom}_{\mathcal{C}}(X, Y)$ と書きます. また $X = Y$ のとき, $\mathrm{Hom}_{\mathcal{C}}(X, X) = \mathrm{End}_{\mathcal{C}}(X)$, $\mathrm{Isom}_{\mathcal{C}}(X, X) = \mathrm{Aut}_{\mathcal{C}}(X)$ と書きます. 誤解の恐れのないときには $\mathrm{Hom}_{\mathcal{C}}$, $\mathrm{End}_{\mathcal{C}}$ に出てくる $\mathcal{C}$ を省略して Hom, End などと書くこともあります. 群 G の圏 $\mathcal{C}$ の対象 X への作用とは準同型 $G \to \mathrm{Aut}_{\mathcal{C}}(X)$ が与えられていることをいいます. もっと大きな圏の例として集合の圏, 群の圏などが考えられます. 集合の圏というのは $\mathrm{Obj}(\mathcal{C})$ を集合全体のなすクラス, $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ を X から Y への写像全体の集合, (5.1) を写像の合成として定まる圏です. 群の圏というのは $\mathrm{Obj}(\mathcal{C})$ を群全体のなすクラス, $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ を X から Y への準同型写像全体の集合, (5.1) を写像の合成として定まる圏です. 同じように体の圏, 可換環の圏, 代数多様体の圏などいろいろな圏が考えられます. どうしてそうなのか私にはよく分からないのですが, 重要な数学的対象は大抵, 圏の理論の枠組みで考えることができ, またそうすることによって見通しのよい取り扱いができるようになります.

アーベル群とその準同型のなす圏は, 次の点で重要です. X, Y をアーベル群とすると, $\mathrm{Hom}(X, Y)$ はアーベル群の構造を持ちます. X をアーベル群とすると $\mathrm{End}(X)$ は準同型写像の合成を掛け算とすることによって環の構造を持ちます. R を環とするとき, アーベル群 X と, 環の準同型 $R \to \mathrm{End}(X)$ との組 $(X, R \to \mathrm{End}(X))$ のことを (左) R 加群とよびます. $(X, R \to \mathrm{End}(X))$ のことをしばしば X と省略して書きます. 例えば $X = R$ を足し算を演算とするアーベル群とみなすと, $a \in R$ を $x \mapsto ax$ で与えられる準同型 $X \to X$ に送る写像 $R \to \mathrm{End}(X)$ は環の準同型となり, これによって $X = R$ を R 加群とみなすこ

[5] より詳しいことは [河田], [マク] をご参照ください.

とができます. X, Y を R 加群とするとき, アーベル群としての直和 $X \oplus Y$ には自然に R 加群の構造が入ります. $X \oplus X = X^{\oplus 2}$, $X^{\oplus 2} \oplus X = X^{\oplus 3}$, ... とおくことによって, 任意の整数 $n \geq 0$ に対し $X^{\oplus n}$ を定義します. ただし $X^{\oplus 0} = \{0\}$ とおきます. X, Y を R 加群とするとき, アーベル群の準同型 $f : X \to Y$ であって,

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{End}(X) \\ \downarrow & & \downarrow \\ \mathrm{End}(Y) & \longrightarrow & \mathrm{Hom}(X,Y) \end{array}$$

が可換になるもののことを X から Y への R 準同型とよびます. 全単射となる R 準同型のことを R 同型, または R を省略して同型とよびます. X から Y への R 準同型の全体を $\mathrm{Hom}_R(X,Y)$ と書きます. これは $\mathrm{Hom}(X,Y)$ の部分アーベル群となります. R が可換環のとき, $\mathrm{Hom}_R(X,Y)$ は自然に R 加群の構造をもちます. $n \geq 0$ を整数とします. R 加群 X が, 階数 n の自由 R 加群であるとは, $R^{\oplus n}$ から X への R 同型が存在することをいいます. K を体とすると, K はとくに環になりますが, このとき R 加群のことを K ベクトル空間と呼び, X, Y を K ベクトル空間とするとき, X から Y への K 準同型のことを X から Y への K 線型写像とよびます. 階数 n の自由 K 加群のことを n 次元 K ベクトル空間とよびます.

6. Galois 表現

G を群とするとき, アーベル群 X と G の作用 $\rho : G \to \mathrm{Aut}(X)$ の組 (X, ρ) のことを G 加群とよびます. しばしば記号を省略して (X, ρ) のことを X と書いたり ρ と書いたりします. R を環とするとき, R 加群 X と G の作用 $G \to \mathrm{Aut}(X)$ の組のことを $R[G]$ 加群もしくは G の R 上の表現とよびます. K を体とするとき, 絶対 Galois 群 G_K の, (適当な条件を満たす位相) 環 R 上の (連続) 表現のことを K の R 上の Galois 表現とよびます. あまり一般的ないい方ではありませんが, K の R 上の Galois 表現 $(X, \rho : G_K \to \mathrm{Aut}(X))$ であって, X が R 加群として階数 n の自由 R 加群となるとき, ρ を K の R 上の階数 n の Galois 表現とよぶことにします. ℓ を素数とするとき, K の, 標数 ℓ の有限体上の Galois 表現のことを K の mod ℓ Galois 表現とよびます. F を代数体, v を F の素点とします. F_v の R 上の表現 M が不分岐であるとは $G_{F_v} \to \mathrm{Aut}_R(M)$ が $G_{F_v} \to G_{k_v}$ を経由することをいいます. F の R 上の表現 M が v で不分岐であるとは, M の G_{F_v} への制限が不分岐であることをいいます. S を F の素点の集合とするとき, M が S の外不分岐であるとは任意の $v \notin S$ で M が不分岐であることをいいます. M が S の外不分岐であることは $G_F \to \mathrm{End}_R(M)$ が $G_F \to G_{F,S}$ を経由することと同値となります.

F を代数体, K を ℓ 進体, V を F の K 上の階数 n の Galois 表現とします. v を F の素点であって ∞ の上にないものとすると, $I_{F,v}$ 固定部分 $V^{I_{F,v}} = \{x \in V \mid \sigma(x) = x,\ \forall \sigma \in I_{F,v}\}$ は F_v の K 上の階数 n 以下の不分岐な Galois 表現となります. F_v の剰余体の元の個数を q_v とおきます. ℓ の上にある F の全ての素点 w について V が F_w の de Rham 表現とよばれる表現であることを仮定します. このとき, V の L 関数とよばれる複素数 s についての関数 $L(V,s)$ を Euler 積

$$L(V,s) = \prod_v \det(1 - \mathrm{Frob}_v q_v^{-s}; V^{I_{F,v}})^{-1} \prod_{w|\ell} L_w(V,s)$$

によって定義します. ここで v は F の素点であって ∞ の上にも ℓ の上にもないもの動きます. $L_w(V,s)$ の定義は難しいのでこの原稿では省略します. 通常考えるような Galois 表現 V に対しては, 上の Euler 積は s の実数部分が十分大きいときに (絶対) 収束し, その範囲で s についての正則関数になります. 通常考えるような Galois 表現 V に対する $L(V,s)$ は全複素平面上に有理型に解析接続され, 適当な関数等式を満たすと予想されていますが, そのことが証明されている場合はあまり多くなく, $L(V,s)$ と保型 L 関数との関連が確立されている場合ぐらいしかありません.

7. 保型形式

$\mathfrak{H} = \{x + \sqrt{-1}y \mid x, y \in \mathbb{R},\ y > 0\}$ とおきます. これを複素上半平面とよびます. Γ を $\mathrm{SL}_2(\mathbb{Z})$ の指数有限の部分群とします. 整数 $k \geq 0$ に対し, $\mathfrak{H}$ 上の正則関数 f であって, 任意の $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ に対し $f((az+b)/(cz+d)) = (cz+d)^{-2k} f(z)$ をみたし, さらにいくつかの付加的な条件を満たすものを, Γ に関する重さ k の尖点形式とよびます. Γ に関する重さ k の尖点形式 f の全体を $S_k(\Gamma)$ とおきます. これは $\mathbb{C}$ ベクトル空間となります. Γ, Γ' を $\mathrm{SL}_2(\mathbb{Z})$ の指数有限の部分群であって $\Gamma' \subset \Gamma$ を満たすものとするとき, $S_k(\Gamma) \subset S_k(\Gamma')$ が成立します.

$N \geq 1$ を整数とします.

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; N|c,\ N|(d-1) \right\}$$

とおきます (ここで $N|c$ というのは c が N で割り切れる, という意味です. $N|(d-1)$ についても同様です). これは $\mathrm{SL}_2(\mathbb{Z})$ の指数有限の部分群となります. $k \geq 0$, $f \in S_k(\Gamma_1(N))$ とします. このとき $f(z+1) = f(z)$ が成立することなどから, $f(z) = \sum_{n \geq 1} a_n(f) q^n$ の形に書けます. ここで $q = e^{2\pi\sqrt{-1}z}$ で, 各 n に対し $a_n(f) \in \mathbb{C}$ です. これを f の q 展開とびます. $\mathbb{C}$ の部分環 R に対し, $\Gamma_1(N)$ に属する重さ k の保型形式 f であって, その q 展開を $f(z) = \sum_{n \geq 1} a_n(f) q^n$ としたとき, 任意の $n \geq 1$ に対して $a_n(f) \in R$ を満たすようなものの全体を $S_k(\Gamma_1(N), R)$ とおきます. これは R 加群となります. $f \in S_k(\Gamma_1(N), R)$ とします. N を割らない素数 p に対し, $\mathfrak{H}$ 上の関数 $T_p f$ を

$$(T_p f)(z) = f(pz) + \sum_{i=0}^{p-1} f((z+i)/p)$$

によって定めると, $T_p f$ も $S_k(\Gamma_1(N), R)$ に属します. また $\overline{d} \in (\mathbb{Z}/N\mathbb{Z})^\times$ に対し, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ であって $c \mod n = 0$, $d \mod n = \overline{d}$ を満たすものが存在しますが, $\mathfrak{H}$ 上の関数 $\langle \overline{d} \rangle f$ を

$$(\langle \overline{d} \rangle f)(z) = (cz+d)^{-2k} f((az+b)/(cz+d))$$

によって定めると, $\langle \overline{d} \rangle f$ は $\overline{d}$ にしか依存せず, $S_k(\Gamma_1(N), R)$ に属します. T_p (p は N を割らないすべての素数を動く) および $\langle \overline{d} \rangle$ ($\overline{d}$ は $(\mathbb{Z}/N\mathbb{Z})^\times$ の元を動く) を元として持つ $\mathrm{End}(S_k(\Gamma_1(N), \mathbb{Z}))$ の最小の部分環のことを Hecke 環とよびます. これは可換環となります.

$S_k(\Gamma_1(N), \mathbb{C})$ にはレベル N, 重さ k の正規化された新形式と呼ばれる, 特別な性質をもつものがあります.

$f(x)$ を整数係数のモニックな 3 次多項式であって $f(x) = 0$ が重根を持たないものとします. E を, 式 $y^2 = f(x)$ で定義される代数曲線に無限遠点を付け加えた $\mathbb{Q}$ 上の楕円曲線とします. 集合

$$\{(x, y) \mid x, y \in \{0, 1, \ldots, p-1\}, y^2 - f(x) \text{ が } p \text{ の倍数 }\}$$

を考えます. これは有限集合です. p からこの集合の元の個数を引いた数を $a_p(E)$ とおきます. E に対する $f(x)$ のとり方は一意的ではなく, $a_p(E)$ の値は $f(x)$ のとり方に依存しますが, $f(x)$ のとり方を変えたときに $a_p(E)$ の値が変化するのは有限個の p についてだけです.

谷山-志村予想とは次の定理 7.1 のことです. これは Wiles [W], Taylor-Wiles [TW] によって特別な場合に証明がなされ, その手法を発展させることによって最終的に [BCDT] によって証明が完成しました.

定理 7.1. E を $\mathbb{Q}$ 上の楕円曲線とする. このとき整数 $N \geq 1$ [6] および, レベル N, 重さ 2 の正規化された新形式 $f = \sum a_n(f)q^n$ であって, 有限個を除くすべての素数 p に対し, $a_p(f) = a_p(E)$ を満たすものが存在する.

8. 保型形式に伴う Galois 表現の構成

$N, k \geq 1$ を整数, $f = \sum_{n\geq 1} a_n(f)q^n \in S_k(\Gamma_1(N), \mathbb{C})$ をレベル N, 重さ k の正規化された新形式とします. $K(f)$ を, どの $a_n(f)$ をも元にもつような $\mathbb{C}$ の部分体のうち最小のものとします. $K(f)$ は代数体となります. $K(f)$ の有限素点 λ に対し, $\mathcal{O}_{f,\lambda}$ を $K(f)_\lambda$ の整数環とします. このとき f に伴う $\mathbb{Q}$ の $\mathcal{O}_{f,\lambda}$ 上の Galois 表現 $(V_{f,\lambda}, \rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{Aut}(V_{f,\lambda}))$ が構成されます. この Galois 表現は以下の 3 性質を満たします.

性質 8.1. (1) $V_{f,\lambda}$ は階数 2 の Galois 表現, すなわち $\mathcal{O}_{f,\lambda}$ 加群として $V_{f,\lambda}$ は階数 2 の自由 $\mathcal{O}_{f,\lambda}$ 加群である.

(2) S を f のレベル N を割る素数の全体とすると, $(V_{f,\lambda}, \rho_{f,\lambda})$ は S の外で不分岐となる.

(3) 任意の $p \notin S$ に対し, Frob_p の作用 $V_{f,\lambda} \to V_{f,\lambda}$ のトレースは $a_p(f)$ に等しい.

f に付随する Galois 表現 $V_{f,\lambda}$ の構成は $k = 2$ の場合は Eichler [E] -志村 [Sh1] によって, $k \geq 2$ の場合は志村 [Sh2], Deligne [De] によって, $k = 1$ の場合は Deligne-Serre [DS] によって与えられました. ここでは Deligne による $k \geq 2$ の場合の構成について説明します.

Riemann 面 $\Gamma_1(N)\backslash\mathfrak{H}$ は付加構造つき楕円曲線のパラメータ空間とみなすことができます. モジュライの理論を用いてこの見方を精密化します. 楕円曲線のモジュライとは楕円曲線の同型類の全体の空間に代数多様体の構造を与えたものです. モジュライをきちんと説明するためには関手とその表現可能性のような, 圏論の基本的な概念について知っておく必要があります. [

$\mathcal{C}$ を圏とするとき, $\mathcal{C}^{\mathrm{op}}$ という圏が自然に定まります. これは $\mathcal{C}$ において矢印の向きを逆にしたものです. もう少し正確に述べると, $\mathrm{Obj}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Obj}(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$ とおくことによって定まる圏のことです.

$\mathcal{C}, \mathcal{C}'$ を 2 つの圏とします. $\mathcal{C}$ から $\mathcal{C}'$ への共変関手とは, (1) $\mathrm{Obj}(\mathcal{C})$ に属する各 X に対して $\mathrm{Obj}(\mathcal{C}')$ に属する $F(X)$ を与える対応, (2) $\mathrm{Obj}(\mathcal{C})$ に属する各 X, Y に対する写像 $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ の 2 つから成り立ちます. これらの間には適当な関係を要請します. 最も重要な要請は $g \circ f$ が定義可能なとき $F(g) \circ F(f) = F(g \circ f)$ が成り立つという要請です. $\mathcal{C}$ から $\mathcal{C}'$ への共変関手 F が与えられていることを $F : \mathcal{C} \to \mathcal{C}'$ と書きます. $\mathcal{C}^{\mathrm{op}}$ から $\mathcal{C}'$ への共変関手のことを $\mathcal{C}$ から $\mathcal{C}'$ への反変関手とよびます.

群 G に対して $F(G) = G$, 群の準同型 $f : G \to G'$ に対して $F(f) = f$ とおくと, F は群の圏から集合の圏への共変関手となります. $\mathcal{C}$ を圏, X_0 を $\mathcal{C}$ の対象とすると, $\mathcal{C}$ の対象 X に集合 $F(X) = \mathrm{Hom}_{\mathcal{C}}(X_0, X)$ を対応させ, $\mathcal{C}$ における射 $f : X \to Y$ に対し $g : X_0 \to X$ を $f \circ g : X_0 \to Y$ に送る写像 $\mathrm{Hom}_{\mathcal{C}}(X_0, X) \to \mathrm{Hom}_{\mathcal{C}}(X_0, Y)$ を与えることによって, 圏 $\mathcal{C}$ から集合の圏への共変関手が得られます. この関手を h_{X_0} と書くことにします.

圏 $\mathcal{C}$ から圏 $\mathcal{C}'$ への 2 つの共変関手 F, F' が同型であるとは, $\mathrm{Obj}(\mathcal{C})$ に属する各 X に対し全単射 $F(X) \to F'(X)$ を与えて, $\mathcal{C}$ における任意の射 $f : X \to Y$ に対し

$$\begin{array}{ccc} F(X) & \longrightarrow & F(Y) \\ \downarrow & & \downarrow \\ F'(X) & \longrightarrow & F'(Y) \end{array}$$

が可換になるようにできることをいいます. 2 つの圏 $\mathcal{C}, \mathcal{C}'$ が圏同値であるとは, 関手 $F : \mathcal{C} \to \mathcal{C}'$ および関手 $F' : \mathcal{C}' \to \mathcal{C}$ とが存在して合成関手 $F' \circ F$ が $\mathcal{C}$ の恒等関手, $F \circ F'$ が $\mathcal{C}'$ の恒等関手とそれぞれ同型となることをいいます. 例えば有限集合の圏と, $\emptyset, \{0\}, \{0, 1\}, \{0, 1, 2\}, \ldots$ を対象の全体, それらの間の写像を

[6] この整数 N は実は E の導手 N_E に等しくなります.

射とする圏とは圏同値になります. 圏同値となるような圏を同一視して考えることが, 見通しのよい数学的考察をするためにしばしば行われます.

圏 $\mathcal{C}$ から集合の圏への共変関手 F が表現可能であるとは, $\mathcal{C}$ の対象 X が存在して, F が h_X と同型になることをいいます. このとき X は同型を除いて一意的に定まります.

$\mathcal{C}, \mathcal{C}'$ を圏, $F : \mathcal{C} \to \mathcal{C}'$ を共変関手とします. 共変関手 $F' : \mathcal{C}' \to \mathcal{C}$ が F の左随伴関手であるとは, $\mathcal{C}'$ の対象 X と, $\mathcal{C}$ の対象 Y に対して同型 $\mathrm{Hom}_{\mathcal{C}'}(X, F(Y)) \cong \mathrm{Hom}_{\mathcal{C}}(F'(X), Y)$ が存在し, この同型が関手的であることをいいます. ここで関手的というのは圏 $\mathcal{C}^{\mathrm{op}} \times \mathcal{C}'$ から集合の圏への 2 つの関手の間の同型を与えているという意味です. F の左随伴関手は標準的な同型を除いて一意的に定まります. 共変関手 $F' : \mathcal{C}' \to \mathcal{C}$ が F の右随伴関手であるとは, $\mathcal{C}$ の対象 X と, $\mathcal{C}'$ の対象 Y に対して同型 $\mathrm{Hom}_{\mathcal{C}'}(F(X), Y) \cong \mathrm{Hom}_{\mathcal{C}}(X, F'(Y))$ が存在し, この同型が関手的であることをいいます. F の右随伴関手は標準的な同型を除いて一意的に定まります.

R, R' を環, $R \to R'$ を環準同型とします. R' 加群 $(M, R' \to \mathrm{End}(M))$ に対して, $R \to R' \to \mathrm{End}(M)$ を考えることによって R 加群が得られます. これは R' 加群の圏から R 加群の圏への共変関手を与えます. この共変関手は左随伴関手を持ちます. この左随伴関手による R 加群 M の行き先を $R' \otimes_R M$ と書きます. $R' \otimes_R M$ をもっと具体的に書くこともできるのですが, この原稿では省略します. R 加群 $R^{\oplus n}$ の, この左随伴関手による行き先は $R'^{\oplus n}$ になります. R, R' がともに可換環の場合には $R' \otimes_R M$ を $M \otimes_R R'$ とも書きます.

代数多様体の代わりにスキーム論の枠組みで考えます. スキームとは, 大まかにいうと可換環を図形のようなものとみなして, それを切り貼りして得られるもののことです. [7] たとえば代数多様体はスキームとなります. 可換環 R を, 切り貼りの操作をせずにそのままスキームをみなしたもののことを $\mathrm{Spec}\, R$ と書きます. S をスキームとするとき, スキーム X とスキームの射 $f : X \to S$ との組 (X, f) のことを S 上のスキームとよびます. 記号を省略して (X, f) のことをしばしば X と書きます.

先ほど, $f(x)$ を整数係数のモニックな 3 次多項式であって $f(x) = 0$ が重根を持たないものに対し $y^2 = f(x)$ に無限遠点を付け加えたものが $\mathbb{Q}$ 上の楕円曲線となると述べました. 一般にスキーム S に対して, S 上の楕円曲線という概念が定義されます. $S = \mathrm{Spec}\, \mathbb{Q}$ のとき, $\mathrm{Spec}\, \mathbb{Q}$ 上の楕円曲線を与えることと $\mathbb{Q}$ 上の楕円曲線を与えることとは同等になります. 詳しい定義はここでは述べないのですが, 一般のスキーム S 上の楕円曲線は, S 上のスキーム E と, S 上のスキームの圏における射 $S \to E$ のなす組 $(E, S \to E)$ であって適当な条件を満たすものです. $(E, S \to E)$ と書くのは面倒なので $S \to E$ を省略して S 上の楕円曲線 E とも書きます. 大まかにいうと S 上の楕円曲線とは, S をパラメータ空間とする楕円曲線の族のような感じのものです. 射 $S \to E$ は無限遠点にあたります. $(E, S \to E)$ をスキーム S 上の楕円曲線とします. このとき任意の S 上のスキーム T に対し, S 上の射 $T \to E$ の全体を $E(T)$ とおきます. このとき $E(T)$ にはアーベル群の構造が入ります.

$N \geq 1$ を整数とします. N が可逆となるスキーム S に対し, S 上の楕円曲線 E とアーベル群 $E(S)$ の元 x であって, 条件 (1) x を N 回足すと単位元になる, (2) 任意の整数 $1 \leq N' < N$ と任意の S の連結成分 S' に対して x を $E(S')$ に制限したものを N' 回足しても単位元にならない, を満たすものの組 (E, x) の同型類の集合を対応させることによって N が可逆となるスキームの圏から集合の圏への反変関手が構成されます. $N \geq 5$ のときこの関手は表現可能となります. この関手を表現する N が可逆となるスキームを $Y_1(N)$ と書きます. このとき $Y_1(N)(\mathbb{C}) \cong \Gamma_1(N) \backslash \mathfrak{H}$ が成立します. $f : E^{\mathrm{univ}} \to Y_1(N)$ を普遍楕円曲線とします. $Y_1(N)$ は自然なコンパクト化 $X_1(N)$ を持ちます. 空間 $S_k(\Gamma_1(N))$ は $X_1(N) \otimes \mathrm{Spec}\, \mathbb{C}$ 上のとある直線束の大域切断の空間と標準的に同型になります. ℓ を素数, $k \geq 2$ を整数とし, $Y_1(N) \otimes \mathbb{Z}[1/N\ell]$ 上の ℓ 進局所系 $\mathrm{Sym}^{k-2}(R^1 f_* \mathbb{Q}_\ell)$ を考えます. これの中間延長の $X_1(N) \otimes \overline{\mathbb{Q}}$ 上の中間次元コホモロジー $V_1(N)$ には Hecke 環 T と $G_{\mathbb{Q}}$ が同時に作用します.

[7] より詳しいことは [ハ], [マン] をご参照ください.

$N, k \geq 1$ を整数, $f = \sum_{n\geq 1} a_n(f)q^n \in S_k(\Gamma_1(N))$ をレベル N, 重さ k の正規化された新形式, λ を ℓ の上にある $K(f)$ の素点とします. Hecke 加群の準同型の空間 $V_{f,\lambda,\mathbb{Q}} = \mathrm{Hom}_{T\otimes K(f)}(K(f)f, V_1(N)\otimes_{\mathbb{Q}_\ell} K(f)_\lambda)$ は $\mathbb{Q}$ の $K(f)_\lambda$ 上の階数 2 の Galois 表現となります. $K(f)_\lambda$ ベクトル空間としての同型 $\iota : V_{f,\lambda,\mathbb{Q}} \xrightarrow{\cong} K(f)_\lambda^{\oplus 2}$ をうまくとると, $\iota^{-1}(\mathcal{O}_{f,\lambda}^{\oplus 2})$ は $\mathbb{Q}$ の $\mathcal{O}_{f,\lambda}$ 上の階数 2 の Galois 表現となります. この Galois 表現を $(V_{f,\lambda}, \rho_{f,\lambda})$ とおきます. $k_{f,\lambda}$ を $\mathcal{O}_{f,\lambda}$ の剰余体とします. $V_{f,\lambda}\otimes_{\mathcal{O}_{f,\lambda}} k_{f,\lambda}$ の半単純化は $G_{\mathbb{Q}}$ の $k_{f,\lambda}$ 上の階数 2 の Galois 表現となります. この Galois 表現を $\overline{\rho}_{f,\lambda}$ とおきます.

性質 8.1(3) は, 合同関係式と呼ばれる関係式から従います. これは Hecke 作用素 T_p の作用, Frob_p の作用を, それぞれ代数的対応という概念を用いて幾何的に表したもの間の関係式で, 代数的対応のモジュライ解釈をすることによって証明がなされます. 性質 8.1(3) は, Galois 表現 $V_{f,\lambda}$ の L 関数 $L(V_{f,\lambda}, s)$ が, f の保型 L 関数 $L(f,s)$ と, $N\ell$ を割る素数での Euler 因子を除いて一致する, とも述べられます. 実は $L(V_{f,\lambda}, s)$ と $L(f,s)$ とは, $N\ell$ を割る素数での Euler 因子を除かなくても完全に一致することが知られています.

9. 谷山-志村予想を仮定した定理 1.1 の証明

E を $\mathbb{Q}$ 上の楕円曲線とします. 整数 $n \geq 1$ に対して, アーベル群 $E[n]$ は $\mathbb{Q}$ の $\mathbb{Z}/n\mathbb{Z}$ 上の階数 2 の Galois 表現 $(E[n], \overline{\rho}_{E,n})$ を与えます. 素数 ℓ に対し, $E[\ell^n]$ の射影極限によって得られる $\mathbb{Q}$ の $\mathbb{Z}_\ell$ 上の階数 2 の Galois 表現を $(T_\ell E, \rho_{E,\ell})$ と書き, E の ℓ 進 Tate 加群といいます. 谷山-志村予想 (定理 7.1) が E について成立すると仮定します. f を E に対応するレベル N, 重さ 2 の正規化された新形式とします. このとき, $K(f) = \mathbb{Q}$ となります. さらに $T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ は $V_{f,\ell}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$ と同型となります.

K を ℓ 進体, $\mathcal{O}$ をその整数環とします. $(V, \rho : G_{\mathbb{Q}} \to \mathrm{Aut}(V))$ を $\mathbb{Q}$ の $\mathcal{O}$ 上の階数 2 の Galois 表現とします. このとき ρ が保型的であるとは, ある整数 $k \geq 1$, $N \geq 1$, 重さ k, レベル N の正規化された新形式 f, $K(f)$ の素点 λ, および環の (連続) 準同型 $\mathcal{O}_{f,\lambda} \to \mathcal{O}$ が存在して, $V \otimes_{\mathcal{O}} K$ が $G_{\mathbb{Q}}$ の K 上の表現として $V_{f,\lambda}\otimes_{\mathcal{O}_{f,\lambda}} K$ と同型となることをいいます. κ を K の剰余体とします. $(V, \overline{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(V))$ を $\mathbb{Q}$ の κ 上の階数 2 の Galois 表現とします. このとき $\overline{\rho}$ が保型的であるとは, ある整数 $k \geq 1$, $N \geq 1$, 重さ k, レベル N の正規化された新形式 f, $K(f)$ の素点 λ, および環の (連続) 準同型 $\mathcal{O}_{f,\lambda} \to \mathcal{O}$ が存在して, $V \otimes_{\mathcal{O}} k$ の半単純化が $G_{\mathbb{Q}}$ の κ 上の表現として $\overline{\rho}_{f,\lambda}$ と同型となることをいいます.

注 9.1. 保型的という概念は総実代数体 F の $\mathcal{O}$ または κ 上の階数 2 の Galois 表現に対して一般化されています. ここで代数体 F が総実であるとは, 任意の環準同型 $F \to \mathbb{C}$ の像が $\mathbb{R}$ に含まれることをいいます.

Serre [Se2] は次の予想を立てました:

予想 9.2. *κ を有限体, S を素数の有限集合とする. $(V, \overline{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(V))$ を $\mathbb{Q}$ の κ 上の階数 2 の Galois 表現であって, 条件: (1) $\overline{\rho}$ は絶対既約, (2) $\overline{\rho}$ は S の外で不分岐, (3) $c \in G_{\mathbb{Q}}$ を複素共役とするとき $\det(\overline{\rho}(c)) = -1$, を満たすものとすると $\overline{\rho}$ は保型的.*

Serre はさらに予想 9.2 の (1)–(3) を満たす $\overline{\rho}$ に対し, 整数 $k(\overline{\rho})$, $N(\overline{\rho})$ を定義し, [8] 予想 9.2 を精密化した次の予想を提唱しました.

予想 9.3. *κ を有限体. S を素数の有限集合とする. $(V, \overline{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(V))$ を $\mathbb{Q}$ の κ 上の Galois 表現であって, 予想 9.2 条件 (1), (2), (3) を満たすものとする. このときレベル $N(\overline{\rho})$, 重さ $k(\overline{\rho})$ の正規化された新形式 f, $K(f)$ の有限素点 λ, および環準同型 $\mathcal{O}_{f,\lambda} \to \kappa$ が存在して, $\overline{\rho}$ は $V_{f,\lambda}\otimes_{\mathcal{O}_{f,\lambda}} \kappa$ の半単純化と同型になる.*

Ribet [R] は Jacobian の Neron モデルを計算する Mazur のアイデアを用いて, とある条件を満たす重さ 2, レベル N の正規化された新形式 f, N を一回だけ割る素数 p, および N の約数でない素数の上にある $K(f)$ の素点 λ に対し, $\overline{\rho}_{f,\lambda}$ が p で不分岐ならば, $\overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f',\lambda'}$ を満たすようなレベル N/p の正規化さ

[8] $k(\overline{\rho})$, $N(\overline{\rho})$ の他に, Serre は準同型 $\varepsilon : (\mathbb{Z}/N(\overline{\rho})\mathbb{Z})^\times \to \mathbb{C}^\times$ を定義していますが, この稿ではその説明を省略します.

れた新形式 f' および $K(f')$ の素点 λ' が存在することを証明しました. この結果を適用することにより, 予想 9.2 の 3 条件のほかにいくつかの技術的条件を満たす $\overline{\rho}$ に対し, $\overline{\rho}$ について予想 9.2 が成り立てば $\overline{\rho}$ について予想 9.3 が成り立つことを示しました. この種の議論をレベルの引き下げとよびます.

その後, レベルの引き下げに関する結果は多くの人たちによって改良され, 任意の $\overline{\rho}$ に対し, $\overline{\rho}$ について予想 9.2 が成り立てば $\overline{\rho}$ について予想 9.3 が成り立つことが現在では証明されています. また予想 9.2 も, 昨年 Khare と Wintenbeger によって証明されました ([KW1], [KW2]). このように現在ではいろいろと結果に進展があるのですが, Fermat 予想を谷山-志村予想から導くためには前述の Ribet の結果で十分です.

谷山-志村予想 (定理 7.1) を仮定した下での定理 1.1 の証明は以下のようになります. ここで ℓ を素数, $a^\ell + b^\ell = c^\ell$ を条件 (1) を満たす予想 1.1 の反例とし, Frey 曲線 $E_{a,b}$ を考えます. 谷山-志村予想を $E_{a,b}$ に適用すると $E_{a,b}$ は保型的となります. $\mathbb{Q}$ の $\mathbb{F}_\ell$ 上の Galois 表現 $E_{a,b}[\ell]$ を $\overline{\rho}$ とおくと, $\overline{\rho}$ は保型的となります. この $\overline{\rho}$ に対しては Ribet の結果が適用できるため, 予想 9.3 が $\overline{\rho}$ に対して成り立つことが分かります. ところが計算してみると $N(\overline{\rho})$ は 1 または 2, $k(\overline{\rho})$ は 2 になります. 特にレベルが 1 または 2, 重さが 2 の正規化された新形式が存在することになります. ところが $S_2(\Gamma_1(1)) = S_2(\Gamma_1(2)) = \{0\}$ であることが知られているのでこれは矛盾です.

10. 谷山-志村予想の証明

この節では, 谷山-志村予想 (定理 7.1) の証明の方針を述べます. 証明は主に保型性持ち上げ定理 (MLT), Langlands-Tunnell の定理, (3, 5) trick という 3 つの部分から成りたっています. このうち MLT を証明するさいに $R = T$ 定理を用います.

MLT とは, $\overline{\rho}_{E,\ell}$ が保型的かつ $\overline{\rho}_{E,\ell}$ を $G_{\mathbb{Q}(\sqrt{\ell^*})}$ (ここで $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$) に制限したものが絶対既約なら $\rho_{E,\ell}$ も保型的であるという定理です. ここでは, Kisin [Ki1] によって改良された形の MLT (定理 14.1) を用います.

Langlands-Tunnell の定理とは, $\overline{\rho}_{E,3}$ が既約ならば保型的である, という主張です. MLT と合わせて, $\overline{\rho}_{E,3}$ を $G_{\mathbb{Q}(\sqrt{-3})}$ に制限したものが絶対既約なら E は保型的であることが分かります. $\overline{\rho}_{E,3}$ を $G_{\mathbb{Q}(\sqrt{-3})}$ に制限したものが絶対既約でない場合, とある楕円モジュラ曲線の有理点の数え上げを行うと, 例外的な E を除いて, $\overline{\rho}_{E,5}$ を $G_{\mathbb{Q}(\sqrt{5})}$ に制限したものが絶対既約であることがわかります. 例外的な E については E が保型的であることが容易に証明できるので, $\overline{\rho}_{E,5}$ を $G_{\mathbb{Q}(\sqrt{5})}$ に制限したものが絶対既約の場合に E が保型的であることを示せば十分です. MLT を用いることによって, この場合には $\overline{\rho}_{E,5}$ が保型的であれば E は保型的となります. ここで (3, 5) trick を用いると, $\mathbb{Q}$ 上の楕円曲線 E' が存在して $\overline{\rho}_{E,5} \cong \overline{\rho}_{E',5}$ かつ $\overline{\rho}_{E',3}$ を $G_{\mathbb{Q}(\sqrt{-3})}$ に制限したものが絶対既約となることが分かります. これより E' が保型的になり, したがって $\overline{\rho}_{E,5}$ は既約かつ保型的になります. 以上で谷山-志村予想が証明できました.

11. Langlands 予想

$R = T$ が成り立つということの根拠に Langlands 予想があります. Langlands 予想は類体論を一般化するものです.

類体論について簡単に説明します. [9] アデール環という可換環があります. アデール環とは, 通常 $\mathbb{A}$ または $\mathbb{A}_\mathbb{Q}$ という記号で書かれ, 実数体 $\mathbb{R}$ と有限アデール環と呼ばれる環 $\mathbb{A}_f$ との直積になっています. 標準的な環の準同型 $\mathbb{Q} \to \mathbb{A}$ があります. 代数体 F に対し, $\mathbb{A}_F = \mathbb{A} \otimes_\mathbb{Q} F$ とおき, これを F のアデール環とよびます. $\mathbb{A}_F$ は可換環で, 標準的な環の準同型 $F \to \mathbb{A}_F$ が定まります. $\mathbb{A}_F$ の可逆元全体 $\mathbb{A}_F^\times$ を F のイデール群とよびます. これは位相群となります. 類体論とは, F のイデール類群 $F^\times\backslash\mathbb{A}_F^\times$ の 1 次元表現と G_F の 1 次元表現との間の対応を与える理論です.

G を代数体 F 上の簡約代数群とします. 簡約とは巾単正規部分群が存在しないことをいいます. $\mathbb{A}_F$ を F のアデール環とします. $G(F)\backslash G(\mathbb{A}_F)$ 上の $\mathbb{C}$ 値関数であって適当な条件を満たすものを $G(\mathbb{A}_F)$ 上の保

[9] より詳しいことは [加藤-黒川-斎藤], [ノ] をご参照ください.