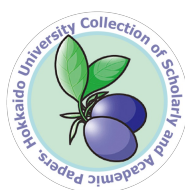




HOKKAIDO UNIVERSITY

Title	整数論札幌夏の学校
Author(s)	Hida, H.; Ito, T.; Katsurada, H. et al.
Citation	Hokkaido University technical report series in mathematics, 137, 1
Issue Date	2008-09
DOI	https://doi.org/10.14943/49026
Doc URL	https://hdl.handle.net/2115/45509
Type	departmental bulletin paper
File Information	tech137.pdf



整数論札幌夏の学校

Sapporo Summer School on Number Theory

Hokkaido University

Aug. 28 - Sep. 8, 2006

Series #137. September, 2008

HOKKAIDO UNIVERSITY
TECHNICAL REPORT SERIES IN MATHEMATICS

- #114 T. Abe, 第 8 回 COE 研究員連続講演会『超平面配置と対数的ベクトル場の幾何』, 23 pages. 2006.
- #115 H. Kubo and T. Ozawa, Sapporo Guest House Symposium on Mathematics 22 “Nonlinear Wave Equations”, 67 pages. 2006.
- #116 S. Okabe, 第 9 回 COE 研究員連続講演会『ある束縛条件下における平面弾性閉曲線のダイナミクス』, 31 pages. 2006.
- #117 A. Suzuki, T. Ito, N. Sato, K. Shibuya, D. Hirose, Y. Maekawa and K. Matsumoto, 第 3 回数学総合若手研究集会 – 他分野との学際的交流を目指して, 264 pages. 2007.
- #118 T. Yamamoto, Y. Sato, N. Kataoka and H. Takagi, Proceedings of the conference on New Aspects of High-dimensional Nonlinear Dynamics, 73 pages. 2007.
- #119 T. Yamamoto and T. Nakazi, 第 15 回関数空間セミナー報告集, 82 pages. 2007.
- #120 K. Hirata, 第 10 回 COE 研究員連続講演会『正值調和関数に対する Martin 積分表現と非線形楕円型方程式の正值解の存在』, 25 pages. 2007.
- #121 K. Izuchi, 第 12 回 COE 研究員連続講演会『I) Segal-Bargmann 空間の巡回ベクトルについて II) 2 重単位開円板上の逆シフト不変部分空間上のクロス交換子について』, 18 pages. 2007.
- #122 T. Ozawa, Y. Giga, S. Jimbo, G. Nakamura, Y. Tonegawa, K. Tsutaya and T. Sakajo, The 32nd Sapporo Symposium on Partial Differential Equations, 73 pages. 2007.
- #123 H. Kubo, T. Ozawa, H. Takamura and K. Tsutaya, Nonlinear Wave Equations, 53 pages. 2007.
- #124 N. Ishimura, T. Sakajo, T. Sakurai, M. Nagayama, T. Nara, D. Furihata and T. Matsuo, 応用数理サマーセミナー 2007 「計算ホモロジーとその応用」, 110 pages. 2007.
- #125 S. Hattori, 第 15 回 COE 研究員連続講演会『分岐理論と有限平坦 Galois 表現』, 28 pages. 2008.
- #126 T. Miyaguchi, M. Kon, R. Kamijo, S. Kawano, Y. Sato and D. Hirose, 第 4 回数学総合若手研究集会 – 他分野との学際的交流を目指して, 298 pages. 2008.
- #127 K. Saji, 第 13 回 COE 研究員連続講演会『波面とその特異点』, 15 pages. 2008.
- #128 T. Nakazi and S. Miyajima, 第 16 回関数空間セミナー報告集, 105 pages. 2008.
- #129 M. Kon, 学位論文 Doctoral thesis “Minimal submanifolds immersed in a complex projective space”, 77 pages. 2008.
- #130 S. Minabe, 第 14 回 COE 研究員連続講演会『開ミラー対称性における最近の進展』, 8 pages. 2008.
- #131 H. Kubo and T. Ozawa, Sapporo Guest House Symposium, Final “Nonlinear Partial Differential Equations”, 73 pages. 2008.
- #132 H. Kang, 第 16 回 COE 研究員連続講演会『CHAOS IN TRAVELING WAVES IN LATTICE SYSTEMS OF UNBOUNDED MEDIA』, 13 pages. 2008.
- #133 G.-J. Chung, editor: Y. Kimura, Introduction to Various Models in Image Processing, 61 pages. 2008.
- #134 H. Takagi and R. Uno, 研究会報告書『動的システムの情報論 (7)』, 110 pages. 2008.
- #135 T. Ozawa, Y. Giga, S. Jimbo, G. Nakamura, Y. Tonegawa, K. Tsutaya and T. Sakajo, 第 33 回偏微分方程式論札幌シンポジウム, 72 pages. 2008.
- #136 T. Sakajo, Y. Nishiura, H. Suito, K. Nishinari, M. Nagayama and T. Amemiya, JST さきがけ研究集会『環境問題における数理の可能性』, 83 pages. 2008.

整数論札幌夏の学校

Sapporo Summer School on Number Theory

Hokkaido University

Aug. 28 - Sep. 8, 2006

整数論札幌夏の学校

開校期間：平成 18 年 8 月 28 日～9 月 8 日

開校場所：北海道大学理学部 8 号館 3 階 8-309

北海道大学大学院理学研究院による大学院教育イニシアティブ「全国大学院共通滞在型プログラム」の一環として、肥田晴三教授 (UCLA) による講義を中心として、関連するテーマの基礎的知識の一部を survey lectures の形で解説する企画を「整数論札幌夏の学校」として、平成 18 年 8 月 28 日から 9 月 8 日の 2 週間に渡り、北海道大学理学部 8 号館にて開催しました。講師と講義タイトルは次の通りです：

伊藤哲史 (京都大学)	コホモロジー論とモチーフ
桂田英典 (室蘭工業大学)	モジュラー形式と L-関数
北川浩二 (北海道大学)	古典的岩澤理論
田口雄一郎 (九州大学)	類体論
肥田晴三 (UCLA)	L-invariant and Galois deformation
村瀬篤 (京都産業大学)	楕円曲線
山上敦士 (京都産業大学)	Galois 変形理論

また、第 2 週目には若手研究者による研究発表会も行いました：

新井啓介	4元数体による乗法をもつアーベル曲面に伴うガロア表現の像について
板倉兼介	Hasse-Weil L関数の関数等式から見る特殊値 (玉河数予想)
岡崎武生	Siegel modular form of degree 2 and Abelian variety
加塩朋和	On the p-adic CM-period symbol
河村尚明	A certain Dirichlet series of Rankin-Selberg type associated with the Ikeda lifting
木村巖	(In)divisibility of special values of zeta functions associated to quadratic fields
平岡敬浩	平方和2次形式に関する極大格子の種の類数
村田学	実2次体上のShimura mass formula
望月哲史	Motif理論の変形I

この冊子は「整数論札幌夏の学校」終了後に講演者並びに研究発表者に改めて書いて戴いた論文を集めた報告集です。その為、一部上記タイトルと掲載論文のタイトルが違うものがあります。また、北川浩二氏は平成19年1月10日に急逝されましたので、彼の論文は須田智彦氏に講義のノートを元を書いて貰ったものです。また、板倉兼介氏の論文は本人の要望により掲載しておりません。

肥田先生には御多忙にも拘わらず連続講義を御快諾戴き誠に有難うございました。また、桂田、田口、村瀬の三先生並びに河村尚明君にはプログラム作成の段階からお世話になりました。大きな理論を簡潔に纏め講義して戴いた講師の方々並びに多くの方の御協力に篤く御礼申し上げます。

前田芳孝

目 次

プログラム	i
参加者名簿	iii

第 I 部 講義録

1. 類体論	1
田口 雄一郎(九州大学)	
2. L 関数とモジュラー形式	16
桂田 英典(室蘭工業大学)	
3. 楕円曲線入門	39
村瀬 篤(京都産業大学)	
4. 古典的岩澤理論	49
北川浩二(北海道大学)(記 須田智彦(北海道大学))	
5. Galois 変形理論	56
山上敦士(京都産業大学)	
6. コホモロジー論とモチーフ	92
伊藤哲史(京都大学)	
7. $\mathcal{L}$ -invariant of tensor power of Hilbert modular forms	150
肥田晴三(UCLA)	

第 II 部 若手研究発表会

1. 平方和 2 次形式に関する極大格子の種の類数について	173
平岡敬浩(立命館大学)	
2. 実 2 次体上の直交群に対する Shimura mass formula	177
村田学(立命館大学)	
3. 4 元数体による乗法をもつアーベル曲面に伴うガロア表現の像について	181
新井啓介(東京大学)	
4. On the p-adic absolute CM-period symbol	184
加塩朋和(大阪市立大学)	
5. (In)divisibility of special values of zeta functions associated to quadratic fields	186
木村巖(富山大学)	

6. Siegel modular form of degree 2 and Abelian variety	189
岡崎武生(大阪大学)	
7. Certain Dirichlet series of Rankin-Selberg type associated with the Ikeda lifting	192
河村尚明(北海道大学)	
8. Motif 理論変形考	196
望月哲史(東京大学)	

プログラム

第1週 8月28日 ～ 9月2日

8月28日(月)

13:30 - 15:00 田口雄一郎 「類体論 (I)」
15:30 - 17:00 田口雄一郎 「類体論 (II)」

8月29日(火)

10:00 - 11:30 桂田英典 「モジュラー形式とL-関数 (I)」
13:30 - 15:00 村瀬篤 「楕円曲線 (I)」
15:30 - 17:00 村瀬篤 「楕円曲線 (II)」

8月30日(水)

10:00 - 11:30 桂田英典 「モジュラー形式とL-関数 (II)」
13:30 - 15:00 桂田英典 「モジュラー形式とL-関数 (III)」

8月31日(木)

10:00 - 11:30 北川浩二 「古典的岩澤理論 (I)」
13:30 - 15:00 北川浩二 「古典的岩澤理論 (II)」
15:30 - 17:00 山上敦士 「Galois変形理論 (I)」

9月1日(金)

10:00 - 11:30 山上敦士 「Galois変形理論 (II)」
13:30 - 15:00 山上敦士 「Galois変形理論 (III)」

9月2日(土)

10:00 - 11:30 ディスカッション セッション

※第1週のsurvey lectures に関するディスカッションを行います。

第2週 9月4日 ~ 9月8日

9月4日(月)

10:00 - 11:30 肥田晴三 「L-invariant and Galois deformation (I)」

13:30 - 15:00 伊藤哲史 「コホモロジー論とモティーフ (I)」

〔若手研究発表会〕

15:30 - 16:00 平岡敬浩 「平方和2次形式に関する極大格子の種の類数」

16:15 - 16:45 村田学 「実2次体上のShimura mass formula」

9月5日(火)

10:00 - 11:30 肥田晴三 「L-invariant and Galois deformation (II)」

13:30 - 15:00 伊藤哲史 「コホモロジー論とモティーフ (II)」

〔若手研究発表会〕

15:30 - 16:00 新井啓介 「4元数体による乗法をもつアーベル曲面に伴う
ガロア表現の像について」

16:15 - 16:45 加塩朋和 「On the p-adic CM-period symbol」

17:00 - 17:30 木村巖 「(In)divisibility of special values of zeta
functions associated to quadratic fields」

9月6日(水)

10:00 - 11:30 肥田晴三 「L-invariant and Galois deformation (III)」

13:30 - 15:00 伊藤哲史 「コホモロジー論とモティーフ (III)」

〔若手研究発表会〕

15:30 - 16:00 岡崎武生 「Siegel modular form of degree 2 and Abelian
variety」

16:15 - 16:45 河村尚明 「A certain Dirichlet series of Rankin-Selberg
type associated with the Ikeda lifting」

9月7日(木)

10:00 - 11:30 肥田晴三 「L-invariant and Galois deformation(IV)」

13:30 - 15:00 伊藤哲史 「コホモロジー論とモティーフ (IV)」

〔若手研究発表会〕

15:30 - 16:00 板倉兼介 「Hasse-Weil L関数の関数等式から見る特殊値
(玉河数予想)」

16:15 - 16:45 望月哲史 「Motif理論の変形I」

9月8日(金)

10:00 - 11:30 肥田晴三 「L-invariant and Galois deformation (V)」

参加者名簿

新井啓介	(東京大学)	辻栄周平	(北海道大学)
板倉兼介	(東京大学)	津嶋貴弘	(東京大学)
伊藤哲史	(京都大学)	徳田洋平	(京都産業大学)
馬着敏郎	(岡山大学)	富山恭敬	(九州大学)
大川泰央	(東北大学)	中村明彦	(北海道大学)
岡崎武生	(大阪大学)	中村健太郎	(東京大学)
小関祥康	(九州大学)	長谷川雄之	(室蘭工業大学)
加塩朋和	(大阪市立大学)	原隆	(東京大学)
桂田英典	(室蘭工業大学)	原田新也	(九州大学)
河村尚明	(北海道大学)	肥田晴三	(UCLA)
北川浩二	(北海道大学)	平岡敬浩	(立命館大学)
木村巖	(富山大学)	平之内俊郎	(九州大学)
金城謙作	(東北大学)	平松直哉	(岡山大学)
久保田泰浩	(北海道大学)	平山聖治	(九州大学)
黒田知志	(高知大学)	廣瀬三平	(北海道大学)
後藤泰宏	(北海道教育大学)	深澤洋之	(北海道大学)
齋藤恆和	(早稲田大学)	藤田莊吉	(北海道大学)
白川達也	(京都大学)	前田芳孝	(北海道大学)
杉原栄次	(岡山大学)	松波周一	(北海道大学)
杉山滋規	(京都大学)	南出大樹	(神戸大学)
須田智彦	(北海道大学)	村上正典	(岡山大学)
田口雄一郎	(九州大学)	村瀬篤	(京都産業大学)
竹本隆	(九州大学)	村田学	(立命館大学)
田中秀和	(東京工業大学)	望月哲史	(東京大学)
谷口隆	(東京大学)	山上敦士	(京都産業大学)
千田雅隆	(東北大学)		

(所属は「夏の学校」開催当時のものです)

第 I 部

講義録

類体論¹

田口 雄一郎

序. この講演では 古典的 類体論について、その概略を解説する。類体論とは

特別な体のアーベル拡大についてはよくわかる

といふ話である。「特別な体」とは、大域体 (有限次代数体、有限体上の一変数代数関数体) 及び局所体 ($\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$ の有限次拡大、 $\mathbb{F}_p((t))$ の有限次拡大) の事²である。「よくわかる」とは、主に

- Abel 拡大 L/K の Galois 群の構造が K の言葉で書ける (わかり易い群で近似できる)、
- Abel 拡大 L/K に於いて、 K の素イデアルがどう分解するかがよくわかる、

といふ事を指す。

1. 古典的定式化. この節では K は代数体とする。 $\mathcal{O}_K$ により K の整数環を、 Cl_K により K のイデアル類群を表す。

19 世紀末、D. Hilbert は次の事を予想した。「 K の各素イデアル $\mathfrak{p}$ について

$$\mathfrak{p} \text{ は } L/K \text{ で完全分解} \iff (\mathfrak{p} \text{ の類})=1 \text{ in } \text{Cl}_K$$

となる Galois 拡大 L/K が存在する。」

この様な L を K の類体と呼んだ (現在は Hilbert 類体または絶対類体と呼ばれてゐる)。後に判明した事には、 L/K は K の最大不分岐アーベル拡大であり、 $\text{Gal}(L/K) \simeq \text{Cl}_K$ である。

1920 年、高木貞治はこれを一般化した形で証明した ([8])。 $\mathcal{O}_K$ のイデアル $\mathfrak{m}$ に対し

$$A_{K,\mathfrak{m}} = \{\mathfrak{m} \text{ と互ひに素な } K \text{ の分数イデアル}\},$$

$$P_{K,\mathfrak{m}} = \{(x) \mid x \in K^\times, x \equiv 1 \pmod{\mathfrak{m}}, x \text{ は “総正”}\},$$

$$\text{Cl}_K(\mathfrak{m}) = A_{K,\mathfrak{m}}/P_{K,\mathfrak{m}},$$

とおく。 $\text{Cl}_K(\mathfrak{m})$ を $\mathfrak{m}$ を法とする射類群 (ray class group) と呼ぶ。類体論の主定理は、古典的なスタイルで述べると、次の二つである：

¹「整数論札幌夏の学校」に於ける講義 (2006 年 8 月 28 日) のノート。

²これらは 1 次元の体で、それを高次元の体 (或いは scheme) に一般化したものが「高次元類体論」である。

存在定理. 任意の m に対し或る有限次アーベル拡大 K_m/K があつて

$$\mathrm{Gal}(K_m/K) \simeq \mathrm{Cl}_K(m)$$

となる。

同型定理. 任意の有限次アーベル拡大 L/K は或る m に対する K_m に含まれ、 $N_{L/K}(A_{L,m}) \supset P_{K,m}$ かつ

$$\mathrm{Gal}(L/K) \simeq A_{K,m}/N_{L/K}(A_{L,m})$$

となる。

有限次アーベル拡大 L/K に対し、 $L \subset K_m$ となる最小の m を L/K の導手 (conductor, Führer) と呼ぶ。 K の素イデアル $\mathfrak{p}$ について、次の同値が知られてゐる：

$\mathfrak{p}$ は L/K で分岐する $\iff \mathfrak{p}$ は L/K の導手を割る。

導手は、素イデアルが分岐するか否かだけでなく、どれだけ深く分岐するかをも測るものである。

類体論の応用として

Kronecker の青春の夢. 虚二次体の任意の有限次アーベル拡大は CM 楕円曲線の j 不変量の値と等分点の座標を添加して得られる。

が解決した (これは Kronecker-Weber の定理の虚二次体への拡張である)。

ところで高木の論文では、上の定理に於ける同型写像は具体的に与へられたわけではなかつた。その後「1927年に Artin が驚嘆すべき発見を成した」([9], 14.2; 原論文は [1]):

Artin の相互法則. 相互写像

$$r_{K,m} : A_{K,m} \rightarrow \mathrm{Gal}(L/K)$$

$$\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}} \right)$$

があり、これが上の同型を導く。

ここに $\mathrm{Frob}_{\mathfrak{p}}$ や $\left(\frac{L/K}{\mathfrak{p}} \right)$ は $\mathfrak{p}$ の Frobenius 置換³を表す。

これにより L/K に於ける素イデアルの分解法則がわかる。即ち、 L/K で不分岐な K の素イデアル $\mathfrak{p}$ が $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ と分解したとき、その個数 g が、 $\mathfrak{p}$ が $\mathrm{mod} N_{L/K}(A_{L,m})$ のどの類に入るかでわかる。実際、 $[L : K] = fg$ とすると $N_{L/K}(\mathfrak{P}_i) = \mathfrak{p}^f$ であり、 $f = (\mathrm{Frob}_{\mathfrak{p}}$ の位数 $\mathrm{in} \mathrm{Gal}(L/K)) = (\mathfrak{p}$ の類の位数 $\mathrm{in} A_{K,m}/N_{L/K}(A_{L,m}))$ となる。

³文脈や都合や気分に応じて二つの (またはそれ以上) の記号を使ひ分ける。例へば肥田先生の講義では $[\mathfrak{p}, K]$ という記号が使はれた。

2. 局所類体論. 有理関数を冪級数体に於いて Taylor 展開出来る様に、有理数を “Taylor 展開” (p 進展開) 出来る様な体として p 進体 $\mathbb{Q}_p$ がある。これは「完備離散付値体」の一つであるので、先づこの概念を復習する。

体 K 上の (非アルキメデスの) 付値 v とは、群準同型 $v : K^\times \rightarrow \mathbb{R}$ であつて $v(x+y) \leq \min\{v(x), v(y)\}$ なるものの事である。通常 $v(0) := \infty$ により v を写像 $v : K \rightarrow \mathbb{R} \cup \{\infty\}$ に拡張しておく。一般に、一つの体に入り得る付値は沢山あり得る。値群 $v(K^\times)$ が $\mathbb{R}$ の離散部分群 (従つて $\mathbb{Z}$ と同型) であるとき、 v は 離散付値 であると言ひ、さらに $v(K^\times) = \mathbb{Z}$ のとき v は 正規付値 であると言ふ。付値体 (K, v) とは、体 K とその上の付値 v の組の事である。

付値体 (K, v) に対し

$$\mathcal{O}_v = \mathcal{O}_{K,v} := \{x \in K \mid v(x) \geq 0\}$$

$$\mathfrak{p}_v = \mathfrak{p}_{K,v} := \{x \in K \mid v(x) > 0\}$$

$$k_v = k_{K,v} := \mathcal{O}_v / \mathfrak{p}_v$$

$$Nv := \#k_v,$$

とおく (v は正規付値としておく)。 $\mathcal{O}_v$, $\mathfrak{p}_v$, k_v をそれぞれ (K, v) の 付値環、付値イデアル、剰余体 と呼ぶ。次の自然な短完全列がある：

$$1 \rightarrow \mathcal{O}_v^\times \rightarrow K_v^\times \xrightarrow{v} \mathbb{Z} \rightarrow 1,$$

$$1 \rightarrow (1 + \mathfrak{p}_v)^\times \rightarrow \mathcal{O}_v^\times \rightarrow k_v^\times \rightarrow 1.$$

$$x \mapsto x \pmod{\mathfrak{p}_v}$$

(K, v) が付値体のとき、実数 $a > 1$ を固定して $|x|_v = a^{-v(x)}$ とおくと、これは K 上の絶対値 (乗法的付値) を定め、 $|x - y|_v$ により K は距離空間になる。この距離に関する K の完備化を K_v と書き、 K の v での完備化と呼ぶ。標準的な埋込み $K \hookrightarrow K_v$ があるが、これが同型であるとき、即ち K が v の定める距離に関して初めから完備であるとき、 (K, v) を 完備付値体 と言ふ。 K が大域体ならば K_v は局所コンパクト体になる。

以下暫く、局所体 と言つたら完備離散付値体であつて剰余体が有限であるものの事⁴とする。局所体は或る素数 p に対する p 進体 $\mathbb{Q}_p$ の有限次拡大又は或る有限体 $\mathbb{F}_q$ 上の冪級数体 $\mathbb{F}_q((t))$ の有限次拡大と同型である。

⁴理念的には局所コンパクト体 (即ち Hausdorff, 局所コンパクトかつ非離散的な位相体) を局所体と呼ぶのがよい。この意味の局所体のうち、非アルキメデスの局所体は剰余体が有限な完備離散付値体であり、アルキメデスの局所体は $\mathbb{R}$ または $\mathbb{C}$ と同型である。

K を局所体、 $\mathcal{O}$ をその付値環、 $\mathfrak{p}$ をその付値イデアル、 $k = \mathcal{O}/\mathfrak{p}$ をその剰余体とし、

$$\begin{aligned} U^{(m)} &= (1 + \mathfrak{p}^m)^\times \\ &= \{x \in K^\times \mid v(x-1) \geq m\} \end{aligned}$$

とおく ($U^{(0)} := U := \mathcal{O}^\times$). 局所類体論の主定理を先づは古典的な大域類体論のもの (§1) と並行した形で述べる：

存在定理. 任意の $m \geq 0$ に対し或るアーベル拡大 K_m/K が存在して $\text{Gal}(K_m/K)$ は $K^\times/U^{(m)}$ の profinite 完備化と同型になる。

注意. K_m/K は無限次拡大である。実際 K_0 は K の 最大不分岐拡大 K^{ur} であり、 $\text{Gal}(K_0/K) \simeq \widehat{\mathbb{Z}}$ である。

同型定理. 任意の有限次アーベル拡大 L/K は或る $m \geq 0$ に対する K_m に含まれ、 $N_{L/K}(L^\times) \supset U^{(m)}$ かつ

$$\text{Gal}(L/K) \simeq K^\times/N_{L/K}(L^\times)$$

となる。

これらを纏めて次の様に述べられる：

相互律. 標準的準同型 (相互写像) $r_K : K^\times \rightarrow G_K^{\text{ab}}$ があり、

- 各 L/K に対し r_K は上の同型を導く。
- r_K は単射、 $\text{Im}(r_K)$ は G_K^{ab} の中で稠密。
- 素元 $\in K^\times$ の像 in G_k は Frobenius と一致する。
- “引戻し” により

$$\left\{ \begin{array}{c} K^\times \text{ の指数有限} \\ \text{開部分群} \end{array} \right\} \xleftarrow{1:1} \left\{ \begin{array}{c} G_K^{\text{ab}} \text{ の} \\ \text{開部分群} \end{array} \right\}.$$

従つて次の同型がある：

$$\text{Hom}(K^\times, \mathbb{Q}/\mathbb{Z}) \simeq \text{Hom}(G_K^{\text{ab}}, \mathbb{Q}/\mathbb{Z}).$$

ここに G_K は体 K の絶対ガロア群、 G_K^{ab} は K の最大アーベル拡大 K^{ab} のガロア群 $\text{Gal}(K^{\text{ab}}/K)$ である。

局所類体論の最初の証明は大域類体論を使つてなされた。しかし局所理論の方が大域理論より易しい筈だから、最初に局所類体論を独立に証明し、それを使つて大域類体論を証明できないか、と考へるのは自然である。実際それは可能で、幾つかの証明がある。

3. 証明について. 局所類体論の証明方針 (相互写像の構成法) を二つ紹介する。一つは Lubin-Tate 群を使ふもの、もう一つは巡回代数を使ふものである。前者は円分拡大の理論に類似してゐて、具体的であり、explicit reciprocity law などの、より詳しい研究に向いてゐる。後者は大域類体論との両立性を示し易いといふ利点がある。理論的に美しく、

cohomological な定式化と馴染みがよいので高次元化⁵などの一般化に適してゐる。

以下この節では K を局所体、 $\mathcal{O}$ をその付値環、 $U := \mathcal{O}^\times$ とする。

(1) Lubin-Tate 群を使う方法 (cf. e.g. [5], [10])。相互写像 r_K を、次の図式が可換になる様に作りたい：

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ur}}/K) \longrightarrow 1 \\ & & \uparrow & & \uparrow r_K & & \uparrow \\ 1 & \longrightarrow & U & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} \longrightarrow 1. \end{array}$$

$r_K(\pi)$ は Frobenius $\in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ の逆像、と定める (正確には後ほど述べる)。あとは $r_K|_U$ を決めればよいが、ここで Lubin-Tate 理論を使う。

K の素元 π を一つ選んで固定する。 q を剰余体 k の位数とすると、

$$f(X) = \pi X + \cdots + X^q + \cdots \in \mathcal{O}[[X]]$$

(X^q 以外の項の係数は π で割れる)

の形の冪級数に対して、 $\mathcal{O}$ の作用を持つ 形式群⁶

$$F(X, Y) = X + Y + \cdots \in \mathcal{O}[[X, Y]]$$

が定まる。形式群 F の「 $\mathcal{O}$ -加群構造」の意味する所は、各 $a \in \mathcal{O}$ に対し「 a 倍」を表す冪級数 $[a](X) \in \mathcal{O}[[X]]$ があつて「 $F(X, Y)$ と両立する」といふ公理を満たす、といふ事である。集合 $\overline{\mathfrak{m}} := \{x \in \overline{K} \mid v(x) > 0\}$ は

$$\text{加法: } (x, y) \mapsto F(x, y), \quad a \text{ 倍: } x \mapsto [a](x) \quad (x, y \in \overline{\mathfrak{m}}, a \in \mathcal{O})$$

により $\mathcal{O}$ -加群となる。

事実. $F[\pi^n] := \mathrm{Ker}([\pi^n]$ の作用 on $\overline{\mathfrak{m}})$ は $\mathcal{O}$ -加群として $\mathcal{O}/(\pi^n)$ と同型で、これに G_K が作用する：

$$G_K \rightarrow \mathrm{Aut}(F[\pi^n]) \simeq (\mathcal{O}/(\pi^n))^\times.$$

実はこれは全射。 $\varprojlim_n$ を取つて、 π のみに依存する全射準同型

$$\chi_\pi: G_K \rightarrow U$$

⁵Lubin-Tate 群の高次元版は未だ無い。

⁶ここに言ふ形式群とは「1 次元可換形式群」、即ち二変数の冪級数であつて合成に関して可換群と同様の公理を満たすもののことである。一般には高次元 (多変数) のものや非可換のものもある。

を得る。 $\text{Ker}(\chi_\pi)$ に対応する拡大を K_π/K とすると、実は $K_\pi K^{\text{ur}} = K^{\text{ab}}$ であり、

$$\begin{aligned}\widehat{\mathbb{Z}} &\simeq \text{Gal}(K^{\text{ur}}/K) \simeq \text{Gal}(K^{\text{ab}}/K_\pi), \\ U &\simeq \text{Gal}(K_\pi/K) \simeq \text{Gal}(K^{\text{ab}}/K^{\text{ur}}).\end{aligned}$$

そこで $K^\times$ を $K^\times = \langle \pi \rangle \times U$ と分解しておき、相互写像 $r_K : K^\times \rightarrow G_K^{\text{ab}}$ を次の様に定義する： $r_K(\pi)$ 及び各 $u \in U$ に対する $r_K(u)$ は

$$\begin{aligned}\widehat{\mathbb{Z}} &\simeq \text{Gal}(K^{\text{ab}}/K_\pi), & U &\simeq \text{Gal}(K^{\text{ab}}/K^{\text{ur}}), \\ 1 &\leftrightarrow r_K(\pi) & u^{-1} &\leftrightarrow r_K(u)\end{aligned}$$

なる元。

(2) 巡回代数を使う方法 (cf. e.g. [11], [6])。相互写像 $r_K : K^\times \rightarrow G_K^{\text{ab}}$ を与へる事は非退化 pairing

$$\widehat{G_K^{\text{ab}}} \times K^\times \rightarrow \mathbb{Q}/\mathbb{Z}$$

を与へる事と同じである。そこで、

事実. $\text{Br}(K) := (K \text{ 上の中心単純環の同値類})$ は K が局所体ならば $\mathbb{Q}/\mathbb{Z}$ と標準的に同型である

といふ事に注意して、 $\chi \in \widehat{G_K^{\text{ab}}}$ と $b \in K^\times$ に対し 巡回代数 $A(\chi, b)$ を定義し、上の pairing を

$$(\chi, b) \mapsto (A(\chi, b) \text{ の類}) \text{ in } \text{Br}(K)$$

と定義する。

巡回代数 $A(\chi, b)$ は次の様に定義する。先づ次の一対一対応がある：

$$\left\{ \begin{array}{l} \text{指標 } \chi : G_K^{\text{ab}} \rightarrow \mathbb{Q}/\mathbb{Z} \text{ で} \\ \text{像の位数} = n \text{ なるもの} \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{l} \text{組 } (L/K, \sigma); \text{ ここに} \\ L/K \text{ は } n \text{ 次巡回拡大、} \\ \sigma \text{ は } \text{Gal}(L/K) \text{ の生成元} \end{array} \right\}.$$

左辺の χ に対応するのは、 $\text{Ker}(\chi)$ に対応する L/K と $\chi(\sigma) = 1/n$ なる $\sigma \in \text{Gal}(L/K)$ との組である。そこで、文字 β を用意して、

$$\begin{aligned}A(\chi, b) &:= L + L\beta + \cdots + L\beta^{n-1}, \\ \text{交換関係は } &\beta^n = b, \beta x = \sigma(x)\beta \quad (x \in L),\end{aligned}$$

と定義する。

局所から大域へ. K を大域体とするとき、次の完全列がある：

$$0 \rightarrow \text{Br}(K) \rightarrow \oplus_v \text{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

ここに Σ は K の全ての素点 v に渡る inv_v の和である。この完全列を利用して局所類体論を貼合せる事により大域類体論を導く事が出来る。

注意. Cohomological interpretation:

$$\begin{aligned}\widehat{G_K^{\text{ab}}} &= H^1(K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(K, \mathbb{Z}), \\ K^\times &= H^0(K, \mathbb{G}_m), \\ \text{Br}(K) &= H^2(K, \mathbb{G}_m).\end{aligned}$$

上の pairing $\widehat{G_K^{\text{ab}}} \times K^\times \rightarrow \text{Br}(K)$ は $\chi \in H^1(K, \mathbb{Q}/\mathbb{Z})$ と $b \in H^0(K, \mathbb{G}_m)$ に対し $\delta(\chi) \cup b \in H^2(K, \mathbb{G}_m)$ を対応させるものである (δ は連結準同型、 $\cup$ はカップ積)。

4. Chevalley の定式化: 局所類体論を寄せ集めて大域類体論を作る。
 K を大域体とする。局所類体論によると、 K の各素点 v に於いて $K_v^\times$ が $G_{K_v}^{\text{ab}}$ を近似した。そこで

$$\begin{aligned}I_K &:= \prod_v K_v^\times \\ &:= \{(x_v)_v \in \prod_v K_v^\times \mid \text{殆ど全ての } v \text{ に対し } x_v \in U_v\},\end{aligned}$$

とにおいて、可換図式

$$\begin{array}{ccc} K_v^\times & \xrightarrow{r_{K_v}} & \text{Gal}(L_v/K_v) \\ \downarrow \text{\scriptsize } v \text{ 成分への埋込み} & & \downarrow \text{\scriptsize 制限} \\ I_K & \xrightarrow{???} & \text{Gal}(L/K) \end{array}$$

を念頭に置きつつ、 I_K をして G_K^{ab} を近似せしめる事を考える (I_K は K の idèle 群と呼ばれる)。先づ、古典的な定式化に倣つて存在定理、同型定理を述べるために、 $\mathcal{O}_K$ のイデアル $\mathfrak{m} = \prod \mathfrak{p}_v^{m_v}$ に対し

$$U_{\mathfrak{m}} := \prod_{v \nmid \infty} U_v^{(m_v)} \times \prod_{v \mid \infty} U_v \subset I_K$$

とおく。ここに v が有限素点のときは $U_v^{(m_v)} = (1 + \mathfrak{p}_v^{m_v})^\times$ は局所体 K_v に対する §2 の $U^{(m)}$ であり、 v が無限素点のときは $U_v = (K_v^\times \text{ の連結成分 } \ni 1)$ とおいた。

存在定理. 任意の $\mathfrak{m}$ に対し或る有限次アーベル拡大 $K_{\mathfrak{m}}/K$ が存在して

$$\text{Gal}(K_{\mathfrak{m}}/K) \simeq I_K/U_{\mathfrak{m}}K^\times$$

となる。

同型定理. 任意の有限次アーベル拡大 L/K は或る $\mathfrak{m}$ に対する $K_{\mathfrak{m}}$ に含まれ、 $N_{L/K}(I_L) \supset U_{\mathfrak{m}}$ かつ

$$\text{Gal}(L/K) \simeq I_K/N_{L/K}(I_L)K^\times$$

となる。

ここで

$$C_K := I_K / K^\times \quad (K^\times \text{ は対角的に } I_K \text{ に埋め込む})$$

とおく (C_K は K の idèle 類群 と呼ばれる) と、上の二つの同型の右辺はそれぞれ $C_K / (\overline{U_m \text{ の像}})$, $C_K / N_{L/K}(C_L)$ に等しく、上の二つの定理は次の様に纏められる：

相互律. 標準的な準同型 (相互写像) $r_K : C_K \rightarrow G_K^{\text{ab}}$ があり、

- 各 L/K に対し r_K は上の同型を誘導する。
- K が代数体ならば r_K は全射で
 $\text{Ker}(r_K)$ は 1 を含む C_K の連結成分 ($= \prod_{v|\infty} U_v$)、
 K が函数体ならば $\text{Im}(r_K)$ は G_K^{ab} の中で稠密で r_K は単射。
- 次の図式は可換：

$$\begin{array}{ccc} K_v^\times & \xrightarrow{r_{K_v}} & G_{K_v}^{\text{ab}} \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{r_K} & G_K^{\text{ab}}. \end{array}$$

- “引戻し” により

$$\left\{ \begin{array}{c} C_K \text{ の指数有限} \\ \text{開部分群} \end{array} \right\} \xleftarrow{1:1} \left\{ \begin{array}{c} G_K^{\text{ab}} \text{ の} \\ \text{開部分群} \end{array} \right\}.$$

従つて次の同型がある：

$$\text{Hom}(C_K, \mathbb{Q}/\mathbb{Z}) \simeq \text{Hom}(G_K^{\text{ab}}, \mathbb{Q}/\mathbb{Z}).$$

古典的定式化との関係は次の完全列から見て取れる：

$$1 \rightarrow U_m / (K^\times \cap U_m) \rightarrow C_K \rightarrow \text{Cl}_K(\mathfrak{m}) \rightarrow 1.$$

K を動かした時の変化： K'/K を有限次分離拡大とする。この時 次の可換図式がある：

$$\begin{array}{ccc} C_{K'} & \xrightarrow{r_{K'}} & G_{K'}^{\text{ab}} \\ N_{K'/K} \downarrow & & \downarrow \text{制限} \\ C_K & \xrightarrow{r_K} & G_K^{\text{ab}}, \end{array} \quad \begin{array}{ccc} C_{K'} & \xrightarrow{r_{K'}} & G_{K'}^{\text{ab}} \\ i_{K'/K} \uparrow & & \uparrow \text{移送} \\ C_K & \xrightarrow{r_K} & G_K^{\text{ab}}. \end{array}$$

ここに $i_{K'/K}$ は包含写像 $K \hookrightarrow K'$ が誘導する自然な写像であり、移送といふのは、一般に群 G とその指数有限部分群 H に対し定義される準同型写像 $t_{G/H} : G^{\text{ab}} \rightarrow H^{\text{ab}}$ が定義されるが、これを $G = G_K$, $H = G_{K'}$ に対して適用したものである。

5. L 函数. K を大域体、 L/K を有限次アーベル拡大とする。このとき、同型 $\text{Cl}_K(\mathfrak{m}) \simeq \text{Gal}(L/K)$ はその指標群の間の同型を誘導する。この事は「 L 函数の一致」としても見られる。

指標 $\chi : \text{Cl}_K(\mathfrak{m}) \rightarrow \mathbb{C}^\times$ に対し Hecke の L

$$\begin{aligned} L(s, K, \chi) &:= \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} \\ &= \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})/N\mathfrak{p}^s} \end{aligned}$$

が定義される (但し $(\mathfrak{a}, \mathfrak{m}) \neq 1$ のときは $\chi(\mathfrak{a}) = 0$ と定義する)。ここに $\sum_{\mathfrak{a}}$ は $\mathcal{O}_K$ のイデアル $\mathfrak{a} \neq 0$ に渡る和、 $\prod_{\mathfrak{p}}$ は $\mathcal{O}_K$ の素イデアル $\mathfrak{p} \neq 0$ に渡る積であり、 $N\mathfrak{a}$ は $\mathfrak{a}$ の絶対ノルムである。一方 Galois 群の指標 $\rho : G_K^{\text{ab}} \rightarrow \mathbb{C}^\times$ に対し Artin の L

$$L(s, K, \rho) := \prod_{\mathfrak{p}} \frac{1}{1 - \rho(\text{Frob}_{\mathfrak{p}})/N\mathfrak{p}^s}$$

が定義される。ここに $\prod_{\mathfrak{p}}$ は L/K で不分岐な $\mathcal{O}_K$ の素イデアル $\mathfrak{p} \neq 0$ に渡る積である。

注意. Hecke の L はより一般に C_K の量指標に対し定義される。また、Artin の L はより一般に有限次 Galois 拡大 L/K と $\text{Gal}(L/K)$ の任意の表現 $\rho : \text{Gal}(L/K) \rightarrow \text{GL}_{\mathbb{C}}(V)$ に対し定義される (V は有限次元 $\mathbb{C}$ ベクトル空間)。

相互律 $\widehat{\text{Cl}_K(\mathfrak{m})} \simeq \widehat{\text{Gal}(L/K)}$; $\mathfrak{p} \mapsto \text{Frob}_{\mathfrak{p}}$ は、指標群の間の同型 $\widehat{\text{Cl}_K(\mathfrak{m})} \simeq \widehat{\text{Gal}(L/K)}$; $\chi \mapsto \rho$ であつて $L(s, K, \chi) = L(s, K, \rho)$ なるものの存在を意味する。Artin はもともとこの様な「 L の一致」といふ事を考へてをり、後に相互律に思ひ至つたらしい (因みに Hecke が彼の L 函数を定義したのは 1918 年の論文 [4], Artin が相互律を発表したのは 1927 年の論文 [1] である)。このような L 函数の一致：

Hecke 的 L = Galois 的 L

は最近でも最も hot な topics の一つである。

6. G_K^{ab} の ℓ 進表現. 類体論によれば G_K^{ab} の位数有限な表現は C_K や $\text{Cl}_K(\mathfrak{m})$ の位数有限な表現と一対一に対応する。代数幾何では G_K や G_K^{ab} の (従つて C_K の) ℓ 進表現 (特に位数が無限のもの) が自然に現れるが、逆に任意の ℓ 進表現が「由緒正しい」(i.e. 代数幾何から来る) わけでは必ずしもない。

例. 円分指標 $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_{\ell}^\times$ は分解 $\mathbb{Z}_{\ell}^\times = \mu_{\ell-1} \times (1 + \ell\mathbb{Z}_{\ell})^\times$ に従つて $\chi = \omega\chi_1$ ($\omega : G_{\mathbb{Q}} \rightarrow \mu_{\ell-1} \subset \mathbb{Z}_{\ell}^\times$, $\chi_1 : G_{\mathbb{Q}} \rightarrow (1 + \ell\mathbb{Z}_{\ell})^\times$) と分解出来る。

$k \in \mathbb{Z}_\ell$ に対し

$$\chi_1^k: G_{\mathbb{Q}} \rightarrow (1 + \ell\mathbb{Z}_\ell)^\times$$

が考へられるが、これは $k \notin \mathbb{Z}$ のとき「由緒正しく」ない。

なほ、 $\omega\chi_1^k$ は $\bar{\chi} = \chi \pmod{\ell}$ の $(\{\ell\})$ の外不分岐な) 普遍変形 (の変数を k に特殊化したもの) である。

K を代数体、 F_λ を ℓ 進体、 $\rho: G_K^{\text{ab}} \rightarrow F_\lambda^\times$ を連続表現とする。 ρ は類体論により C_K の連続表現とも思へる。 ρ が「由緒正しい」といふ事を特徴付ける幾つかの条件があり、それらの同値性が知られてゐる：

定理. ρ についての次の各条件は同値である：

- (1) CM アーベル多様体 (と位数有限の表現) から来る。
- (2) 局所代数的。
- (3) 代数的 Hecke 指標から来る。
- (4) Serre 群の代数的表現 $S_K \rightarrow \mathbb{G}_m$ から来る。
- (5) Hodge-Tate at all $v|\ell$.
- (6) de Rham at all $v|\ell$.
- (7) Potentially semi-stable at all $v|\ell$.
- (8) Potentially crystalline at all $v|\ell$.

言葉の意味の説明は省略するが、(1) は「代数幾何から来る」といふ事、(3) は “modular” といふ感じの条件である。(4) の S_K は、(1) の様な表現全体のなす圏の “淡中基本群” と呼ばれるものである。(5) ~ (8) の条件は p 進 Hodge 理論 (ここでは $p = \ell$) を用ゐて定義されるもので、一般 (アーベルと限らないとき) には

$$\begin{aligned} \text{Hodge-Tate} &\Leftarrow \text{de Rham} \Leftrightarrow \text{potentially semi-stable} \\ &\Leftarrow \text{potentially crystalline} \end{aligned}$$

である。この定理について、さらに詳しくは [7], [2], [3] や岩波の『数学辞典』第4版の「類体論」の項を参照されたい。

REFERENCES

- [1] E. Artin, *Beweis des allgemeinen Reziprozitätsgesetzes*, Hamb. Abb. **5** (1927), 353–363
- [2] P. Deligne, J. S. Milne, A. Ogus, Arthur and K. Shih, *Hodge Cycles, Motives, and Shimura Varieties*, Lect. Notes in Math. **900**, Springer-Verlag, Berlin-New York, 1982
- [3] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in: *Elliptic Curves, Modular Forms, & Fermat’s Last Theorem* (Hong Kong, 1993), Internat. Press, Cambridge, MA, 1995, pp. 41–78 (190–227 in the 2nd ed.)
- [4] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, Erste Mitteilung*, Math. Zeit. **1** (1918), 357–376; *Zweite Mitteilung*, Math. Zeit. **6** (1920), 11–51

- [5] K. Iwasawa, *Local Class Field Theory*, Oxford University Press, New York, 1986, viii+155 pp.
- [6] 加藤和也、黒川信重、斎藤毅『数論 I』, 岩波書店
- [7] J.-P. Serre, *Abelian ℓ -adic Representations and Elliptic Curves*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Company, Redwood City, CA, 1989, xxiv+184 pp.
- [8] *Über eine Theorie des relativ-Abel'schen Zahlkörpers*, 東京帝大理学部紀要 **41** (1920)
- [9] 高木貞治『代数の整数論』第二版, 1971, 岩波書店
- [10] T. Yoshida, *Local class field theory via Lubin-Tate theory*, preprint, <http://www.math.harvard.edu/~yoshida/>
- [11] A. Weil, *Basic Number Theory*, 3rd ed., Die Grundlehren der Mathematischen Wissenschaften **144**, Springer-Verlag, New York-Berlin, 1974, xviii+325 pp.

札幌整数論夏の学校
類体論 レポート問題

1. 冪剰余記号 (cf. [4], pp. 348–350, Exercise 1)

K は大域体で 1 の原始 m 乗根を含むものとする。 $a, a' \in K^\times$ とし、以下に現れる K の分数イデアル $\mathfrak{b}, \mathfrak{b}'$ や素イデアル $\mathfrak{p}$ は maa' と互いに素と仮定する。 $L = K(a^{1/m})$ とおき、記号 $\left(\frac{a}{\mathfrak{b}}\right) \in L^\times$ を次により定義する：

$$r_{L/K}(\mathfrak{b})(a^{1/m}) = \left(\frac{a}{\mathfrak{b}}\right) a^{1/m}.$$

ここに $r_{L/K}$ は L/K の相互写像である。

(1) $\left(\frac{a}{\mathfrak{b}}\right)$ は 1 の m 乗根であり、しかも a の m 乗根 $a^{1/m}$ の選び方に依らない事を示せ。

(2) 体 $L = K(a^{1/m}, (a')^{1/m})$ に於いて記号 $\left(\frac{aa'}{\mathfrak{b}}\right), \left(\frac{a}{\mathfrak{b}}\right), \left(\frac{a'}{\mathfrak{b}}\right)$ を上と同様に定義するとき、次の等式が成り立つ事を示せ：

$$\left(\frac{aa'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right) \left(\frac{a'}{\mathfrak{b}}\right).$$

(3) 次の等式が成り立つ事を示せ：

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right) \left(\frac{a}{\mathfrak{b}'}\right).$$

が成り立つ事を示せ。(従つて $\mathfrak{b} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$ ならば

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod \left(\frac{a}{\mathfrak{p}}\right)^{n_{\mathfrak{p}}}$$

が成り立つ。)

(4) $\left(\frac{a}{\mathfrak{p}}\right)$ は

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{(N\mathfrak{p}-1)/m} \pmod{\mathfrak{p}}$$

を満たす唯一の 1 の m 乗根である事を示せ。(ここに $N\mathfrak{p}$ は $\mathfrak{p}$ の絶対ノルム; $N\mathfrak{p} = \#(\mathcal{O}_K/\mathfrak{p})$. 整数 $N\mathfrak{p} - 1$ は m で割り切れる事に注意せよ。)

(5) K の素イデアル $\mathfrak{p}$ と $a \in K^\times$ について、次の三条件は同値である事を示せ：

(i) $\left(\frac{a}{\mathfrak{p}}\right) = 1.$

(ii) 合同式 $x^m \equiv a \pmod{\mathfrak{p}}$ は解 $\in \mathcal{O}_{\mathfrak{p}}$ を持つ。

(iii) 方程式 $x^m = a$ は解 $\in K_{\mathfrak{p}}$ を持つ。

(6) 1 の m 乗根 ζ に対し

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \zeta^{(N\mathfrak{b}-1)/m}$$

である事を示せ。

(7) $a, a', \mathfrak{b}$ が整イデアルのとき、

$$a \equiv a' \pmod{\mathfrak{b}} \quad \text{ならば} \quad \left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a'}{\mathfrak{b}}\right)$$

である事を示せ。

(8) $\mathfrak{b}'\mathfrak{b}^{-1} = (c)$ は単項イデアル ($c \in K^\times$) であり、 ma と素な全ての素イデアル $\mathfrak{p}$ に対し $c \in (K_{\mathfrak{p}}^\times)^m$ であると仮定する。このとき $\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}'}\right)$ である事を示せ。

(9) $K = \mathbf{Q}$ のとき、Artin の相互律を用ゐて (古典的) 平方剰余の相互法則を導け。

2. 講義で扱はなかつた類体論に関連する事実を述べよ。

3. 類体論がどんな所に応用されてゐるか調べよ。

2006.8.28

札幌整数論夏の学校
類体論関係文献案内

有名な古典として

[1] 高木貞治『代数的整数論』(第2版), 岩波書店, 1971

があります。なかなか味はひ深いので一度は読んでみたい本です。特に代数的整数論への入門としては(具体的なので)よいと思ひます。ただ、分岐理論のところはどうしても古さを感じさせるのと、後半の類体論のところもありスッキリとは読めないので、別の本、例へば

[2] 加藤和也, 黒川信重, 斎藤毅『数論1』, 岩波書店

を参考にした方がよいかと思ひます。動機付け的な話題から始めて類体論に至るまで丁寧に解説してあります。特に類体論の定式化及び証明は非常にスッキリ書いてあります。

この本と同様、中心単純環の理論を使つて類体論を展開するものの代表としては、

[3] A. Weil, *Basic Number Theory*, Springer-Verlag, Berlin, 1995 (reprint of the second (1973) edition)

があります。Basic と銘打ちながら決して easy ではないので初心者にはお薦め出来ませんが、Langlands 予想などに向けて表現論的なアプローチを試みようとする人にはまさに basic, 必読の書です。

その他、類体論を含む諸々の事柄が書かれてゐる本として

[4] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967

があります。これは 1965 年に Sussex 大学で行はれた「夏(秋?)の学校」の講究録で、章ごとに著者が異なるので必ずしも読み易くはないですが、参考になる点は多々あるかと思ひます。

分岐理論については

[5] J.-P. Serre, *Corps Locaux* (2ème éd.), Hermann, Paris, 1968

が圧巻です。局所類体論(剰余体が quasi-finite の場合)についても後半の方で書かれてゐます(cohomology による定式化)。が、実は前半で既に局所類体論の主定理にかなり近い定理(Hasse-Arf の定理)が証明されてゐます。

局所類体論を Lubin-Tate 理論を使つて証明してゐる本としては

[6] K. Iwasawa, *Local Class Field Theory*, Oxford University Press, New York, 1986

があります。Preface に曰く、“This approach, though not the shortest, seems particularly well suited to prove some deeper theorems on local fields.” 最後の章で Wiles の explicit reciprocity law も証明されています。

大域類体論は書いてないが代数的整数論と代数函数論についての本で私が個人的にわりと好きなのは

[7] E. Artin, *Algebraic Numbers and Algebraic Functions*, AMS Chelsea Publishing, Providence, 2006 (reprint of the 1967 original)

です。付値論についても詳しく書いてあります。もとは E. Artin の 1950/51 年の Princeton 大学での講義録です。

虚数乗法論については

[8] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Forms*, Princeton Univ. Press, 1998

が決定版です。これは原典 G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan, 1961, の全面改訂版です。

「局所代数的表現」についての実質唯一の本は

[9] J.-P. Serre, *Abelian ℓ -Adic Representations and Elliptic Curves*, Addison-Wesley, 1989 (Originally published in 1968 by W. A. Benjamin)

です。局所代数的表現についての記述 (第 II, III 章) だけでも貴重な文献ですが、その他にもいろいろ面白い事が書いてあります。

他にも紹介すべき文献はたくさんあるかと思ひますが、取敢へず今回の講義に直接関係ありさうなものの中から個人的な趣味で選んでみました。

L関数とモジュラー形式

Hidenori Katsurada

May 31, 2007

はじめに

Riemann の zeta 関数

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

は $\operatorname{Re}(s) > 1$ で広義一様絶対収束し, s の正則関数となる. さらに, $\zeta(s)$ は以下に述べる性質をもっている.

(Z-1).

$$\xi(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$$

とおくと, $\xi(s) + s^{-1} + (1-s)^{-1}$ は全 s 平面に正則に解析接続され関数等式

$$\xi(1-s) = \xi(s)$$

を持つ.

(Z-2). $\operatorname{Re}(s) > 1$ で Euler 積

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

(Z-3). m が正の整数のとき,

$$\zeta(2m) = \frac{(-1)^{m-1} (2\pi)^{2m} B_{2m}}{2(2m)!}$$

となる. ここで B_n は Bernoulli 数と呼ばれる有理数で以下のように定義される.

$$\frac{te^t}{e^t - 1} = \sum_{n=1}^{\infty} \frac{B_n}{n!} t^n.$$

このことは, 関数等式を使うと

$$\zeta(1-2m) = -\frac{B_{2m}}{2m}$$

と言い換えられる.
一般に

$$D(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$$

の形をもつ級数を Dirichlet 級数という. Dirichlet 級数の中でも前に述べた性質 (Z-1) を持つものは整数論にとって特に重要でここでは良い Dirichlet 級数と呼ぼう. さらに, (Z-2) のような Euler 積を持つものは "zeta 関数" あるいは "L 関数" と呼ばれる.¹ 本論では主として, モジュラー形式に付随した Dirichlet 級数について上の (Z-1)~(Z-3) と同様のことが成り立つことを [Miyake, 1989] および [Shimura, 1976] に基づき述べる. 本論の構成は以下のとおりである.

0. Hecke の L-関数
1. モジュラー群
2. モジュラー形式
3. モジュラー形式に付随する Dirichlet 級数
4. Hecke 環
5. Hecke 作用素とモジュラー形式の L 関数の Euler 積表示
6. モジュラー形式の L 関数の特殊値の代数性

本論は 2006 年 8 月 29 日~9 月 4 日にかけて北海道大学理学研究科数学専攻で行われた「整数論札幌夏の学校」での講演原稿に加筆したものである. このサマースクールの運営にあたり尽力された前田芳孝氏はじめ関係者の皆様に感謝します.

0 Hecke の L 関数

この節では, モジュラー形式に付随する Dirichlet 級数や L 関数を論ずる前に, Riemann の zeta 関数の直接の一般化である, Hecke 指標に付随する L 関数すなわち Hecke の L 関数について論じよう.

F を有限次代数体, $\mathfrak{O}_F$ をその整数環, U_F を $\mathfrak{O}_F$ の単数群とする. F の複素数体 $\mathbf{C}$ への埋め込み $v: F \rightarrow \mathbf{C}$ の同値類を F の archimedes 素点という. 特に $v(F) \subset \mathbf{R}$ であるとき, v を実素点といい, そうでないとき複素素点という. $\mathbf{a}$ で F の archimedes 素点全体のなす集合を表す. また, $\mathbf{r}$ および $\mathbf{c}$ でそれぞれ F の実素点および複素素点全体のなす集合を表す. A_F で F の零でない分数イデアル全体のなす集合を表す. A_F はイデアルの積について群をなす. また, F の単項イデアル全体のなす A_F の部分群を P_F で表す. $\mathfrak{M}$ を F の零でない整イデアルとする. このとき,

$$A_{F,\mathfrak{M}} = \{\mathfrak{A} \in A_F; (\mathfrak{A}, \mathfrak{M}) = 1\},$$

$$P_{F,\mathfrak{M}} = \{(a) \in P_F; a \equiv 1 \pmod{\mathfrak{M}^\times}\}$$

¹講演ではこれを "良い Dirichlet 級数" と呼んだが, 整数論的に意味のある Dirichlet 級数が必ずしも Euler 積を持たないということもあるので, ここではこう呼ぶことにする. ちなみに, ここでは (Z-3) を満たす zeta 関数のことを "良い zeta 関数" と呼びたい.

とおく. ここで F の元 a が $a \equiv 1 \pmod{\mathfrak{M}^\times}$ であるとは, a がある $\mathfrak{O}_F$ の元 α, β で $(\alpha, \mathfrak{M}) = (\beta, \mathfrak{M}) = 1, \alpha \equiv \beta \pmod{\mathfrak{M}}$ を満たすものにより $a = \alpha/\beta$ と表されることを意味する. $A_{F, \mathfrak{M}}$ と $P_{F, \mathfrak{M}}$ はいずれも, A_F の部分群となる. ψ が $\mathfrak{M}$ を法とする F の Hecke 指標であるとは, ψ が $A_{F, \mathfrak{M}}$ から $\mathbf{C}^1 = \{x \in \mathbf{C}; |x| = 1\}$ への準同型で次を満たすものとする:

”ある整数 m_v と実数 κ_v ($v \in \mathbf{a}$) が存在して

$$(*) \quad \psi((a)) = \prod_{v \in \mathbf{a}} (a_v/|a_v|)^{m_v} |a_v|^{\kappa_v} \quad (a) \in P_{F, \mathfrak{M}},$$

$$(**) \quad \sum_{v \in \mathbf{a}} \kappa_v / e_v = 0.$$

ここで $v \in \mathbf{a}$ と $a \in F$ に対して, $v(a)$ を a_v と表す. また, e_v は $v \in \mathbf{r}$ であるか $v \in \mathbf{c}$ であるかに従って 1 または 2 とする. 特に, すべての $v \in \mathbf{a}$ について $\kappa_v = 0$ かつ, すべての $v \in \mathbf{c}$ について $m_v = 0$ のとき, ψ は類指標 (class character) であるという. ψ を $\mathfrak{M}$ を法とする F の Hecke 指標とすると, F の整イデアル $\mathfrak{M}_\psi$ で次を満たすものがただひとつ存在する:

(1) $(*)$ がすべての $(a) \in P_{F, \mathfrak{M}_\psi} \cap A_{F, \mathfrak{M}}$ について成り立つ.

(2) $\mathfrak{M}'$ を整イデアルとし, すべての $(a) \in P_{F, \mathfrak{M}'} \cap A_{F, \mathfrak{M}}$ について $(*)$ が成り立つならば $\mathfrak{M}' \subset \mathfrak{M}_\psi$.

この $\mathfrak{M}_\psi$ を ψ の導手 (conductor) という. $\mathfrak{M}$ を法とする Hecke 指標 ψ が原始的 (primitive) とは $\mathfrak{M}_\psi = \mathfrak{M}$ であるときをいう.

さて, F の分数イデアル $\mathfrak{A}$ で $A_{F, \mathfrak{M}}$ に属さないものに対して $\psi(\mathfrak{A}) = 0$ とおき, ψ を A_F から $\mathbf{C}$ への写像に拡張しておく. このとき, ψ の Hecke L 関数 $L(s, \psi)$ を

$$L(s, \psi) = \sum_{\mathfrak{A} \in A_F} \frac{\psi(\mathfrak{A})}{N(\mathfrak{A})}$$

で定義する. ここで, $N(\mathfrak{A})$ は $\mathfrak{A}$ の絶対ノルムを表す. 特に $F = \mathbf{Q}$ で ψ が単位指標のとき, $L(s, \psi)$ は Riemann の zeta 関数 $\zeta(s)$ となる. $L(s, \psi)$ は $\text{Re}(s) > 1$ で広義一様絶対収束し, s の正則関数となる. さらに, $L(s, \psi)$ は Riemann の zeta 関数 $\zeta(s)$ と似た性質をもっている. それを述べるために, いくつかの関数, 記号を用意する. まず, $\Gamma_\psi(s)$ を次のように定義する.

$$\Gamma_\psi(s) = \prod_{v \in \mathbf{r}} \pi^{-s_v} \Gamma(s_v) \prod_{v \in \mathbf{c}} (2\pi)^{1-s_v} \Gamma(s_v),$$

$$s_v = \begin{cases} (s + m_v + i\kappa_v)/2 & v \in \mathbf{r} \\ (s + |m_v| + i\kappa_v)/2 & v \in \mathbf{c} \end{cases}.$$

次に, ψ の Gauss 和 τ_ψ を

$$\tau_\psi = \begin{cases} \psi(\mathfrak{d}) & \mathfrak{M}_\psi = \mathfrak{O}_F \\ \sum_{a \in (\mathfrak{M})^{-1}/\mathfrak{d}^{-1}} \psi_\infty(a)^{-1} \psi(a\mathfrak{M}) \mathbf{e}(\text{tra}) & \mathfrak{M}_\psi \neq \mathfrak{O}_F \end{cases},$$

$$\psi_\infty((a)) = \prod_{v \in \mathbf{a}} (a_v/|a_v|)^{m_v} |a_v|^{\kappa_v},$$

と定義する. ここで $\mathrm{tr}(a) = \sum_{v \in \mathbf{a}} a_v$ を表し, 複素数 x に対して $\mathbf{e}(x) = \exp(2\pi i x)$ とおく.

$$W_\psi = (-i)^{\sum_{v \in \mathbf{a}} |m_v|} N(\mathfrak{M}_\psi)^{-1/2} \tau(\psi)$$

とおく. このとき, (Z-1) ~ (Z-3) に対応する次の性質が成り立つ.

(H-1).

$$\xi(s, \psi) = |D_F N(\mathfrak{M})|^{s/2} \Gamma_\psi(s) L(s, \psi)$$

とおく. ここで, D_F は F の判別式である. このとき, $\xi(s, \psi)$ は全 s 平面に有理型に解析接続され関数等式

$$\xi(1-s, \bar{\psi}) = W_{\bar{\psi}} \xi(s, \psi)$$

を持つ.

(H-2). $\mathrm{Re}(s) > 1$ で Euler 積

$$L(s, \psi) = \prod_{\mathfrak{p}} (1 - \psi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}$$

を持つ.

(H-3). F は d 次の総実代数体とし, ψ は原始指標で, $\psi_\infty(b) = \prod_{v \in \mathbf{a}} (b_v / |b_v|)^k$ を満たすとする. このとき,

$$P(k, \psi) = \tau(\psi)^{-1} (2\pi)^{-kd} L(k, \psi)$$

とおくと, $P(k, \psi)$ は $\mathbf{Q}$ 上 ψ の値で生成された体 $\mathbf{Q}(\psi)$ に属する. このことは, 関数等式を使うと

$$L(1-k, \psi) \in \mathbf{Q}(\bar{\psi})$$

と言い換えられる. $P(k, \psi)$ の具体的な表示に関する新谷卓郎の研究については [Yoshida, 2003] を参照のこと.

例 $F = \mathbf{Q}$ のとき, すべての Hecke 指標は類指標である. これをもう少し詳しく述べよう. N を正の整数とすると, $\mathbf{Z}$ から $\mathbf{C}$ への写像 χ で以下を満たすものを N を法とする Dirichlet 指標という.

- (i) $m, n \in \mathbf{Z}$ に対して $\chi(mn) = \chi(m)\chi(n)$.
- (ii) $m \equiv n \pmod{N}$ のとき, $\chi(m) \equiv \chi(n)$.
- (iii) $(n, N) = 1$ のときかつそのときに限り $\chi(n) \neq 0$.

さて, $F = \mathbf{Q}$ のとき, すべてのイデアルは単項イデアルである. 従って,

$$A_{\mathbf{Q}} = \{(a/b) \mid a, b \in \mathbf{Z}, a \neq 0, b > 0, (a, b) = 1\},$$

であり, 整数 N に対して,

$$A_{\mathbf{Q},(N)} = \{(a/b) \in A_{\mathbf{Q}} ; (a, N) = (b, N) = 1\},$$

$$P_{\mathbf{Q},(N)} = \{(a/b) \in A_{\mathbf{Q},(N)} ; a \equiv b \pmod{N}\}$$

となる。さて、 χ を N を法とする Dirichlet 指標とする。このとき、 $(a/b) \in A_{\mathbf{Q},(N)}$ に対して、 $\hat{\chi}((a/b)) = \chi(|a|)\bar{\chi}(b)$ とおくと、 $\hat{\chi}$ は N を法とする Hecke 指標である。逆に、 $\mathbf{Q}$ の Hecke 指標は Dirichlet 指標からこのようにして得られる。さて、Dirichlet 指標 χ に対して Dirichlet の L 関数 $D(s, \chi)$ を

$$D(s, \chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}$$

で定義する。定義により、Dirichlet の L 関数であり、逆に $\mathbf{Q}$ の Hecke の L 関数は Dirichlet の L 関数である。

2 次体の Hecke 指標と L 関数については 3 節で詳しく述べる。

さて、上の事の詳細な証明については [Yoshida, 2003] に譲ることとして、ここでは (H1) が成り立つからくりを Riemann の zeta 関数を例にあげて説明しよう。

$$\xi(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$$

とおく。theta 関数 $\theta(t)$ を

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}$$

で定義すると、Poisson の和公式

$$\theta(t) = \frac{1}{\sqrt{t}} \sum_{n=-\infty}^{\infty} e^{-\pi n^2/t} = \frac{1}{\sqrt{t}} \theta(1/t)$$

が成り立つ。

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt$$

であることに注意すると、 $\text{Re} > 1$ で

$$\xi(s) = \frac{1}{2} \int_0^{\infty} (\theta(t) - 1) t^{s/2-1} dt$$

となることがわかる。さて、この積分表示を

$$\xi(s) = \frac{1}{2} \int_0^1 (\theta(t) - 1) t^{s/2-1} dt + \frac{1}{2} \int_1^{\infty} (\theta(t) - 1) t^{s/2-1} dt$$

と 2 つに分け、最初を変数変換 $t \rightarrow t^{-1}$ と Poisson の和公式を使うと

$$\begin{aligned} \frac{1}{2} \int_0^1 (\theta(t) - 1) t^{s/2-1} dt &= -s^{-1} + \frac{1}{2} \int_0^1 \theta(t) t^{s/2-1} dt \\ &= -s^{-1} + \frac{1}{2} \int_1^{\infty} \theta(1/t) t^{-s/2-1} dt = -s^{-1} + \frac{1}{2} \int_1^{\infty} \theta(t) t^{1/2-s/2-1} dt \end{aligned}$$

$$= -s^{-1} - (1-s)^{-1} + \frac{1}{2} \int_1^\infty (\theta(t) - 1) t^{1/2-s/2-1} dt$$

となるから, まとめて $\operatorname{Re}(s) > 1$ で

$$\xi(s) = -s^{-1} - (1-s)^{-1} + \frac{1}{2} \int_1^\infty (\theta(t) - 1) (t^{s/2} + t^{(1-s)/2} t^{-1}) dt$$

となる. これにより (1) は容易にわかる. このように, ”良い Dirichlet 級数” は ”良い変換式” を持つ関数による積分表示を持つことが期待される. この ”良い変換式” を持つ関数のひとつが以下の節で述べるで述べるモジュラー形式と呼ばれるものである.

1 モジュラー群

モジュラー形式を述べる前に, モジュラー群の定義をしておこう.

$$GL_2(\mathbf{R})^+ = \{\alpha \in M_2(\mathbf{R}) ; \det \alpha > 0\},$$

$$SL_2(\mathbf{R}) = \{\alpha \in M_2(\mathbf{R}) ; \det \alpha = 1\},$$

$$SL_2(\mathbf{Z}) = SL_2(\mathbf{R}) \cap M_2(\mathbf{Z})$$

とおく. $\mathbf{H} = \{x + iy \in \mathbf{C} ; y > 0\}$ を複素上半平面という. $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{R})^+$ と $z \in \mathbf{H}$ に対して

$$\alpha z = (az + b)(cz + d)^{-1}$$

とおくと, $\alpha z \in \mathbf{H}$ となり, $GL_2(\mathbf{R})^+$ の $\mathbf{H}$ への作用が定義される.

注意. $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{R})^+$ に対して $j(\alpha, z) = cz + d$ とおくと, $j(\alpha, z) \neq 0$ であり, $\beta \in GL_2(\mathbf{R})^+$ に対して

$$j(\alpha\beta, z) = j(\alpha, \beta z)j(\beta, z)$$

となる.

$\mathbf{H}$ 上の体積要素 $dv(z)$ を

$$dv(z) = \frac{dx dy}{y^2}$$

で定義する.

$$\operatorname{Im}(\alpha z) = \frac{\det \alpha \operatorname{Im} z}{|j(\alpha, z)|^2}$$

に注意すると, $dv(z)$ は $\mathbf{H}$ 上の $GL_2(\mathbf{R})^+$ -不変な測度を定義することがわかる.

Γ が $SL_2(\mathbf{R})$ の離散部分群, すなわち $SL_2(\mathbf{R})$ における 1_2 のある近傍 W をとれば $W \cap \Gamma = 1_2$ となるとき, Γ を Fuchs 群という. Fuchs 群は $\mathbf{H}$ に不連続に作用する. また, $SL_2(\mathbf{Z})$ の指数有限部分群をモジュラー群という. モジュラー群は Fuchs 群である. 例えば $SL_2(\mathbf{Z})$ はモジュラー群である. Γ が Fuchs 群のとき, $\mathbf{H}$ の連結な閉集合 $\mathcal{F}$ が Γ に関する基本領域 (fundamental domain) であるとは,

$$(1) \mathbf{H} = \cup_{\gamma \in \Gamma} \gamma \mathcal{F},$$

$$(2) \gamma \in \Gamma \text{ かつ } \gamma \neq \pm 1_2 \text{ ならば } \gamma \mathcal{F}^\circ \cap \mathcal{F}^\circ = \phi$$

を満たすものをいう. ここで $\mathcal{F}^\circ$ は $\mathcal{F}$ の内点の集合を表す. さらに,

$$v_\Gamma = \int_{\mathcal{F}} dv(z)$$

とおく. $dv(z)$ の $GL_2(\mathbf{R})^+$ 不変性より, 右辺は $\mathcal{F}$ のとり方によらない. Fuchs 群 Γ が $v_\Gamma < \infty$ となるとき, 第 1 種 Fuchs 群という.

例 $\Gamma = SL_2(\mathbf{Z})$ のとき,

$$\mathcal{F} = \{z = x + iy \in \mathbf{H} ; -1/2 \leq x \leq 1/2, |z| \geq 1\}$$

は $SL_2(\mathbf{Z})$ の基本領域である. $\mathcal{F}$ の $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ による像

$$\mathcal{F}' = \{z \in \mathbf{H} ; |z| \leq 1, |z+1| \geq 1, |z-1| \geq 1\}$$

も基本領域である. このとき

$$v_{SL_2(\mathbf{Z})} = \frac{\pi}{3}$$

となる. 一般にモジュラー群 Γ に対して

$$v_\Gamma = \frac{\pi}{3} [SL_2(\mathbf{Z}) : \Gamma]$$

となるから, モジュラー群は第 1 種 Fuchs 群である. モジュラー群でない第 1 種 Fuchs 群は例えば定符号 4 元数環の単数群から得られる.

Γ を第 1 種の Fuchs 群とする. $\gamma \in \Gamma$ が放物元 (parabolic element) とは γ のトレイスの絶対値 $|\text{tr}(\gamma)| = 2$ であるときをいう. $z \in \mathbf{C} \cup \{\infty\}$ が Γ の尖点 (cusp) であるとは, ある Γ の放物元 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の固定点, すなわち $\gamma z = z$ であるときをいう. 簡単な計算により Γ の尖点 (cusp) z は $c = 0$ のとき $z = \infty$, そうでないとき $z = \frac{a-d}{2c}$ の形をしていることがわかる.

さて, P_Γ を Γ の尖点全体からなる集合, $U_l^* = \{z \in \mathbf{H} \cup \{\infty\} ; \text{Im}(z) > l\}$ とおく. $\mathbf{H}^* = \mathbf{H} \cup P_\Gamma$ に次のような位相を導入する.

(1) $z \in \mathbf{H}$ のとき, $\mathbf{H}^*$ における近傍系として, $\mathbf{H}$ における z の近傍系をとる.

(2) $z \in P_\Gamma$ のとき, $\mathbf{H}^*$ における近傍系として, $\{\sigma^{-1}U_l^* ; l > 0\}$ をとる. ここで, σ は $\sigma z = \infty$ となる $SL_2(\mathbf{R})$ の元である.

この位相により, $\mathbf{H}^*$ はハウスドルフ空間となる. このとき, Γ の $\mathbf{H}$ への作用を $\mathbf{H}^*$ への作用に自然に延長することができ, $\Gamma \backslash \mathbf{H}^*$ にコンパクトリーマン面の構造を導入することができる. さらに, $\Gamma \backslash \mathbf{H} \subset \Gamma \backslash \mathbf{H}^*$ とみなすことができる.

例 (1) 以下, モジュラー群の例をあげよう.

$$\Gamma(N) = \{\gamma \in SL_2(\mathbf{Z}) ; \gamma \equiv 1_2 \pmod{N}\}$$

は $SL_2(\mathbf{Z})$ の正規部分群でその指数は $SL_2(\mathbf{Z}/N\mathbf{Z})$ の位数に等しいので, モジュラー群である. これを, レベル N の主合同部分群 (principal congruence subgroup) という. 一般に, $SL_2(\mathbf{Z})$ の部分群 Γ が $SL_2(\mathbf{Z})$ の合同部分群 (congruence subgroup) であるとは, ある正の整数 N が存在して $\Gamma(N) \subset \Gamma$ となるときをいう. 合同部分群はモジュラー群であるが, 合同部分群ではないモジュラー群も存在する.

(2)

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) ; c \equiv 0 \pmod{N} \right\}$$

は合同部分群である.

(3)

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) ; a \equiv d \equiv 1 \pmod{N} \right\}$$

は合同部分群である.

2 モジュラー形式

f を $\mathbf{H}$ 上定義された $\mathbf{C}$ に値を持つ関数とする. $\alpha \in GL_2(\mathbf{R})^+$ と $k \in \mathbf{Z}_{>0}$ に対して

$$f|_k \gamma(z) = (\det \alpha)^{k/2} j(\alpha, z)^{-k} f(\alpha z)$$

と定義する. このとき,

$$f|_k \alpha \beta(z) = (f|_k \alpha)|_k \beta(z)$$

が成り立つ. Γ をモジュラー群とし, $\chi : \Gamma \longrightarrow \mathbf{C}^1$ を有限位数の指標とする. $f : \mathbf{H} \longrightarrow \mathbf{C}$ が重さ k , 指標 χ の Γ に関する (正則) モジュラー形式であるとは, 以下の条件を満たすものをいう:

(1) f は $\mathbf{H}$ 上の正則関数

(2) $f|_k \gamma(z) = \chi(\gamma) f(z)$ がすべての $\gamma \in \Gamma$ について成り立つ

(3) すべての $\alpha \in SL_2(\mathbf{Z})$ と $\epsilon > 0$ に対して $f|_k \alpha(z)$ は $\{x + iy \in \mathbf{H} ; y > \epsilon\}$ 上で有界.

$\mathfrak{M}_k(\Gamma, \chi)$ で重さ k , 指標 χ の Γ に関する (正則) モジュラー形式の全体からなる集合を表す. とくに, χ が単位指標のとき, $\mathfrak{M}_k(\Gamma, \chi)$ を $\mathfrak{M}_k(\Gamma)$ と表す. $\mathfrak{M}_k(\Gamma, \chi)$ は有限次元 $\mathbf{C}$ -ベクトル空間となる. Γ' を Γ に含まれるモジュラー群で χ の Γ' への制限を同じ χ で表すと, $\mathfrak{M}_k(\Gamma, \chi) \subset \mathfrak{M}_k(\Gamma', \chi)$ となる.

モジュラー形式のフーリエ展開を考えよう.

定理 2.1. Γ をモジュラー群とし, χ を Γ の指標とする. $f \in \mathfrak{M}_k(\Gamma, \chi)$ とする. このとき, すべての $\gamma \in SL_2(\mathbf{Z})$ に対してある実数 $h = h_\gamma$ が存在して

$$f|_k \gamma(z) = \sum_{m=0}^{\infty} a_{f,\gamma}(m) \mathbf{e}(mz/h)$$

と表される. ここで, $a_{f,\gamma}(m)$ は f と γ と m によって決まる複素数である. 特に, Γ を合同部分群とし, ある正の整数 N が存在して, $\Gamma(N) \subset \Gamma$ かつ χ は $\Gamma(N)$ で 1 となるとする. このとき, すべての $\gamma \in SL_2(\mathbf{Z})$ に対して

$$f|_k \gamma(z) = \sum_{m=0}^{\infty} a_{f,\gamma}(m) \mathbf{e}(mz/N)$$

と表される.

証明の概略. まず, $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$ であるから,

$$f(x + iy + N) = f(x + iy)$$

となり, x の周期関数となる. よって, x の関数として次のようにフーリエ展開される:

$$f(x + iy) = \sum_{m=-\infty}^{\infty} b_{f,\gamma}(m, y) \mathbf{e}(mx/N).$$

ここで, $b_{f,\gamma}(m, y)$ は f, γ と m によって決まる y の関数である. ここで, f の正則性 (1) から,

$$b_{f,\gamma}(m, y) = a_{f,\gamma}(m) \mathbf{e}(imy/N)$$

となることがわかる. ここで, $a_{f,\gamma}(m)$ は f と γ によって決まる複素数である. さらに, 有界性 (3) より, $m < 0$ ならば $a_{f,\gamma} = 0$ となり, 定理が証明された.

注意. 条件 (1), (2) だけからでは, 定理に述べるようなフーリエ展開ができない.

$f \in \mathfrak{M}_k(\Gamma, \chi)$ が尖点形式 (cusp form) であるとは, すべての $\gamma \in SL_2(\mathbf{Z})$ に対して, $a_{f,\gamma}(0) = 0$ を満たすときをいう. $\mathfrak{S}_k(\Gamma, \chi)$ で尖点形式からなる $\mathfrak{M}_k(\Gamma, \chi)$ の部分空間を表す. χ を N を法とする Dirichlet 指標とすると,

$$\Gamma_0(N) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \chi(d) \in \mathbf{C}^1$$

は $\Gamma_0(N)$ の指標を定義する. これを同じ記号 χ で表す. このとき,

$$\mathfrak{M}_k(\Gamma_1(N)) = \oplus_{\chi} \mathfrak{M}_k(\Gamma_0(N), \chi)$$

が成り立つ．ここで， χ は N を法とするすべての Dirichlet 指標を渡る．また， $f \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ に対して

$$f(z) = \sum_{m=0}^{\infty} a(m) \mathbf{e}(mz)$$

と表される． $f(z)$ のフーリエ係数 $a(m)$ の評価式については次の事が知られている．

定理 2.2. $k \geq 2$ とする．このとき，ある定数 $M > 0$ が存在して

$$|a(m)| \leq M m^{k-1}$$

がすべての $m \geq 1$ に対して成り立つ．特に， $f(z)$ が尖点形式のとき

$$|a(m)| \leq M m^{(k-1)/2}$$

がすべての $m \geq 1$ に対して成り立つ．

$f, g \in \mathfrak{M}_k(\Gamma, \chi)$ に対して， f, g の Petersson 内積 $\langle f, g \rangle_\Gamma$ を

$$\langle f, g \rangle_\Gamma = \int_{\Phi_\Gamma} f(z) \overline{g(z)} y^k dv(z)$$

で定義する． Φ_Γ は Γ に関する基本領域である． f または g が $\mathfrak{S}_k(\Gamma, \chi)$ に属するとき， $\langle f, g \rangle_\Gamma < \infty$ となる．さらに， f, g の正規化された Petersson 内積 $\langle f, g \rangle_\Gamma$ を

$$\langle f, g \rangle = v_\Gamma^{-1} \langle f, g \rangle_\Gamma$$

で表す．次に，2つのモジュラー群 Γ_i ($i = 1, 2$) について $f_i \in \mathfrak{M}_k(\Gamma_i)$ をとったとき， Γ_1 と Γ_2 に含まれるモジュラー群 Γ' (例えば， $\Gamma_1 \cap \Gamma_2$) をとり， f_1, f_2 の正規化された Petersson 内積 $\langle f_1, f_2 \rangle$ を

$$\langle f_1, f_2 \rangle = v_{\Gamma'}^{-1} \langle f_1, f_2 \rangle_{\Gamma'}$$

で表す．ここで， f_1, f_2 を $\mathfrak{M}_k(\Gamma')$ の元とみなしている．この定義は， Γ' のとり方によらない．

以下， $\langle f, g \rangle$ の性質について列挙する．

(1) $\langle g, f \rangle = \overline{\langle f, g \rangle}$ ．

(2) $\alpha \in GL_2(\mathbf{R})^+$ が $[\Gamma : \Gamma \cap \alpha^{-1} \Gamma \alpha], [\alpha^{-1} \Gamma \alpha : \Gamma \cap \alpha^{-1} \Gamma \alpha] < \infty$ を満たすとき， $f, g \in \mathfrak{S}_k(\Gamma)$ に対して

$$\langle f|_k \alpha, g \rangle = \langle f, g|_k \alpha' \rangle$$

となる．ここで $\alpha' = (\det \alpha) \alpha^{-1}$ である．

3 モジュラー形式に付随する Dirichlet 級数

$f(z) = \sum_{m=0}^{\infty} a(m)\mathbf{e}(mz)$ を $\mathfrak{M}_k(\Gamma_0(N), \chi)$ の元としたとき, $f(z)$ に付随する Dirichlet 級数 $L(s, f)$ を

$$L(s, f) = \sum_{m=1}^{\infty} \frac{a(m)}{m^s}$$

で定義する. 定理 2.2 より, $L(s, f)$ は s の実部が十分大きなところで広義一様絶対収束し, s の正則関数となる. $L(s, f)$ の解析的性質を知るために,

$$\Lambda_N(s, f) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s) L(s, f)$$

とおく. このとき, 次の積分表示を得る.

命題 3.1. $\operatorname{Re}(s)$ が十分大きいとき,

$$\Lambda_N(s, f) = \int_0^{\infty} t^s (f(it/\sqrt{N}) - a(0)) t^{-1} dt$$

が成り立つ.

定理 3.2. $\mathbf{H}$ 上の関数

$$f(z) = \sum_{m=0}^{\infty} a(m)\mathbf{e}(mz), g(z) = \sum_{m=0}^{\infty} b(m)\mathbf{e}(mz)$$

は $\mathbf{H}$ 上の任意のコンパクト部分集合で一様絶対収束し, ある実数 $\nu > 0$ が存在して,

$$f(z) = O(\operatorname{Im}(z)^{-\nu}), g(z) = O(\operatorname{Im}(z)^{-\nu}) \quad (\operatorname{Im}(z) \rightarrow 0)$$

が成り立つとする. このとき次の (A), (B) は同値となる.

$$(A) \quad w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \text{ とおくとき,}$$

$$g(z) = f|_k w_N(z).$$

(B) (B-1) $\Lambda_N(s, f)$ と $\Lambda_N(s, g)$ は全 s -平面に有理型に解析接続されて

(B-2) 関数等式

$$\Lambda_N(s, f) = i^k \Lambda_N(k-s, g)$$

を満たし,

(B-3) $\Lambda_N(s, f) + \frac{a(0)}{s} + \frac{i^k b(0)}{k-s}$ は全 s -平面で正則かつ, 任意の帯状領域

$$\{s \mid \alpha \leq \operatorname{Re}(s) \leq \beta\}$$

で有界となる.

上の結果を $SL_2(\mathbf{Z})$ に関するモジュラー形式に応用しよう. まず, $SL_2(\mathbf{Z})$ は $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ と $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ で生成されることに注意する. これより, 次の系を得る.

定理 3.2 の系. 定理 3.2 の仮定のもとで次は同値となる.

M. $f(z) \in \mathfrak{M}_k(SL_2(\mathbf{Z}))$.

F. $\Lambda_1(s, f)$ は全 s -平面に有理型に解析接続されて 関数等式

$$\Lambda_1(s, f) = i^k \Lambda_1(k - s, f)$$

を満たし,

$$\Lambda_1(s, f) + \frac{a(0)}{s} + \frac{i^k a(0)}{k - s}$$

は全 s -平面で正則かつ, 任意の帯状領域

$$\{s \mid \alpha \leq \operatorname{Re}(s) \leq \beta\}$$

で有界となる. 特に, $f(z)$ が尖点形式ならば, $\Lambda_1(s, f)$ は正則であり, この逆も成り立つ.

さて, 上のようなことが一般の $\Gamma_0(N)$ に関するモジュラー形式について成り立つであろうか? もう少し詳しくいうと, 定理 3.2 におけるフーリエ級数 $f(z)$, および $g(z)$ に付随する Dirichlet 級数が条件 (B) を満たせば, $f(z)$ および $g(z)$ は $\Gamma_0(N)$ に関するモジュラー形式となるであろうか? これは, 一般には成り立たない. しかしながら, ひとつの関数等式ではなく十分にたくさんの関数等式を満たせば同様のことが成り立つ. これが Weil の逆定理である. これを紹介するために, $f(z) = \sum_{m=0}^{\infty} a(m)\mathbf{e}(mz) \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ と Dirichlet 指標 ψ に対して, ψ で捻った f の Dirichlet 級数 $L(s, f, \chi)$ を

$$L(s, f, \psi) = \sum_{m=1}^{\infty} \frac{a(m)\psi(m)}{m^s}$$

で定義する. 前と同じように, $L(s, f, \psi)$ は s の実部が十分大きなところで広義一様絶対収束し, s の正則関数となる. $L(s, f, \psi)$ の解析的性質を知るために,

$$\Lambda_N(s, f, \psi) = \left(\frac{2\pi}{m\sqrt{N}}\right)^{-s} \Gamma(s) L(s, f, \psi),$$

$$C_{\chi, \psi} = \frac{\chi(M_\psi)\psi(N)W(\psi)^2}{M_\psi}$$

とおく. ただし, M_ψ は ψ の導手で, $W(\psi)$ は ψ の Gauss 和を表す.

命題 3.3 $f(z)$ を上のとおりとし, $g(z) = f|_k w_N(z)$ とおく. このとき, 原始指標 ψ に対して次が成り立つ.

(B $_\psi$) $\Lambda_N(s, f, \psi)$ と $\Lambda_N(s, g, \psi)$ は全 s -平面に有理型に解析接続されて 関数等式

$$\Lambda_N(s, f, \psi) = i^k C_{\chi, \psi} \Lambda_N(k - s, g, \bar{\psi})$$

を満たし, 任意の帯状領域で有界となる.

さて, 命題 3.3 のある意味での逆が成り立つ. これが Weil の逆定理とよばれるものである.

定理 3.4. (A. Weil) χ を N を法とする *Dirichlet* 指標で $\chi(-1) = (-1)^k$ を満たすとする. 2 つの複素数列 $\{a(m)\}_{m=1}^\infty, \{b(m)\}_{m=1}^\infty$ で

$$a(m) = O(m^\nu), b(m) = O(m^\nu) \quad (\nu > 0)$$

を満たすものに対して

$$f(z) = \sum_{m=0}^{\infty} a(m) \mathbf{e}(mz), g(z) = \sum_{m=0}^{\infty} b(m) \mathbf{e}(mz)$$

とおく. このとき, 次の (1), (2) が満たされるならば, $f(z) \in \mathfrak{M}_k(\Gamma_0(N), \chi), g(z) \in \mathfrak{M}_k(\Gamma_0(N), \bar{\chi})$ かつ $g(z) = f|_k w_N(z)$ となる.

(1) $\Lambda_N(s, f), \Lambda_N(s, g)$ は定理 3.2 の B を満たす.

(2) すべての原始指標 ψ でその導手 M_ψ が N を割らない奇素数となるものに対して $\Lambda_N(s, f, \psi), \Lambda_N(s, g, \bar{\psi})$ は命題 3.3 の B $_\psi$ を満たす.

さらに, ある $\delta > 0$ が存在して, $L(s, f)$ が $s = k - \delta$ で絶対収束するならば $f \in \mathfrak{S}_k(\Gamma_0(N), \chi)$ となる.

さて, 定理 3.4 の応用例をあげよう. F を 2 次体とする. d を F の判別式とし, $(\frac{d}{*})$ を Kronecker 指標とする. 最初に F を虚 2 次体とする. このとき, 正の整数 ν と F の整イデアル $\mathfrak{N}$ に対して, Hecke 指標 ξ で

$$\xi((a)) = (a|a|^{-1})^\nu \quad (a \equiv 1 \pmod{\mathfrak{N}})$$

を満たすものをとる. このとき,

$$f(z) = \sum_{\mathfrak{N}} \xi(\mathfrak{N}) N_F(\mathfrak{N})^{\nu/2} \mathbf{e}(N_F(\mathfrak{N})z)$$

とおくと, $f(z) \in \mathfrak{S}_{\nu+1}(\Gamma_0(N), \chi)$ である.. ここで, $\chi(m) = (\frac{d}{m}) \xi((m)), N = |d| N_F(\mathfrak{N})$ である. これを示すために

$$f(z) = \sum_{m=1}^{\infty} a(m) \mathbf{e}(mz)$$

とフーリエ展開し, N を割らない奇素数 p を導手とする Dirichlet 指標 ψ に対して

$$L(s, f, \psi) = \sum_{m=1}^{\infty} \frac{a(m)\psi(m)}{m^s}$$

とおくと, $L(s, f, \psi)$ は Hecke の L -関数 $L(s, \xi(\psi \circ N_F))$ を用いて

$$L(s, f, \psi) = L(s - \nu/2, \xi(\psi \circ N_F))$$

と表される. ここで $\psi \circ N_F(\mathfrak{A}) = \psi(N_F(\mathfrak{A}))$ である. このとき, Hecke の L -関数の解析的性質 (第 1 節参照) と Weil の逆定理により, $f(z) \in \mathfrak{S}_{\nu+1}(\Gamma_0(N), \chi)$ となる. また, このことより

$$L(s, f) = L(s - \nu/2, \xi)$$

と表される.

特に, E を導手が M の虚 2 次体 F に虚数乗法を持つ $\mathbf{Q}$ 上の楕円曲線とする. このとき, E の Hasse zeta 関数 $L(s, E)$ はある Hecke 指標 ξ を用いて

$$L(s, E) = L(s - \nu/2, \xi)$$

と表されることが知られている ([村瀬, 2006] 参照.) これと, 上のことを組み合わせるとある $f(z) \in \mathfrak{S}_{\nu+1}(\Gamma_0(N), \chi)$ が存在して,

$$L(s, E) = L(s, f)$$

となる. ここで, N, χ は ξ に対して上に述べたように決まる正の整数と指標である. このとき,

$$L(s - \nu/2, \xi) = \prod_p (1 - a(p)p^{-s} + p^{-2s+\nu}\chi(p))^{-1}$$

の形をしていることが簡単な計算でわかる. これと, E の Hasse zeta 関数の Euler 因子を比較することにより, $\nu = 1$ かつ $\chi = 1$ となることがわかる. さらに, $N = M$ であることもわかる. すなわち, $f \in \mathfrak{S}_2(\Gamma_0(N))$ となる. これは, Shimura-Taniyama 予想の特別な場合である.

次に, F を実 2 次体とする. このとき, 任意の F の整イデアル $\mathfrak{A}$ に対して, Hecke 指標 ξ で

$$\xi((a)) = a|a|^{-1} \quad (a \equiv 1 \pmod{\mathfrak{A}})$$

または

$$\xi((a)) = a'|a'|^{-1} \quad (a \equiv 1 \pmod{\mathfrak{A}})$$

を満たすものをとる. このとき,

$$f(z) = \sum_{\mathfrak{A}} \xi(\mathfrak{A}) e(N_F(\mathfrak{A})z)$$

とおくと, $f(z) \in \mathfrak{S}_1(\Gamma_0(N), \chi)$ である. ここで, $\chi(m) = (\frac{d}{m})\xi((m))$, $N = |d|N_F(\mathfrak{A})$ である.

4 Hecke環

前節でモジュラー形式に付随する Dirichlet 級数を定義し、解析的な性質、とくに有理型性と関数等式について論じた。しかしながら、それが必ずしも Euler 積をもつとは限らず（この論説における意味での）L-関数とはならない。この節と次の節では、モジュラー形式に付随する Dirichlet 級数が Euler 積をもつための条件を論じよう。そのために、モジュラー形式のなす空間にある可換環を作用させその固有値とフーリエ係数の関係を調べてみる。この環が Hecke 環とよばれるものであり、その作用が Hecke 作用素とよばれるものである。

まず、この節において Hecke 環を定義しよう。2つの半群 $\Delta_0(N), \Delta_0^*(N)$ を

$$\Delta_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid c \equiv 0 \pmod{N}, (a, N) = 1, ad - bc > 0 \right\},$$

$$\Delta_0^*(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid c \equiv 0 \pmod{N}, (d, N) = 1, ad - bc > 0 \right\}$$

で定義する。以下しばらく簡単のため $\Delta = \Delta_0(N), \Delta^* = \Delta_0^*(N), \Gamma = \Gamma_0(N)$ とおく。このとき、

$$\mathcal{R}_N = \mathcal{R}(\Gamma, \Delta) = \left\{ \sum_{\alpha \in \Delta} a_\alpha \Gamma \alpha \Gamma; \text{finite sum}; a_\alpha \in \mathbf{C} \right\}$$

とおく。すなわち、 $\mathcal{R}_N$ は $\Gamma \alpha \Gamma$ ($\alpha \in \Delta$) で生成される $\mathbf{C}$ -自由加群である。 $\mathcal{R}_N$ に積を次のように定義する。まず、 $\Gamma \alpha \Gamma, \Gamma \beta \Gamma \in \mathcal{R}_N$ を $\Gamma \alpha \Gamma = \cup_i \Gamma \alpha_i, \Gamma \beta \Gamma = \cup_i \Gamma \beta_i$ と剰余類分解したとき、

$$\Gamma \alpha \Gamma \cdot \Gamma \beta \Gamma = \sum_{\gamma} c_\gamma \Gamma \gamma \Gamma$$

と定義する。ここで $c_\gamma = \#\{(i, j) \mid \Gamma \alpha_i \beta_j = \Gamma \gamma\}$ とおく。これを、線形に拡張して、 $\mathcal{R}_N$ に積が定義される。この積により、 $\mathcal{R}_N$ は単位元 $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Gamma$ をもつ $\mathbf{C}$ 上の多元環となる。同様にして、 $\mathbf{C}$ -多元環 $\mathcal{R}_N^* = \mathcal{R}(\Gamma, \Delta^*)$ が定義される。以下に $\mathcal{R}_N$ のいくつかの性質を列挙する。

補題 4.1. (1) 任意の $\alpha \in \Delta$ に対してある正の整数 l, m で $l|m$ かつ $(l, N) = 1$ となるものが存在して、

$$\Gamma \alpha \Gamma = \Gamma \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma$$

となる。

(2) 任意の $\alpha \in \Delta^*$ に対してある正の整数 l, m で $l|m$ かつ $(l, N) = 1$ となるものが存在して、

$$\Gamma \alpha \Gamma = \Gamma \begin{pmatrix} m & 0 \\ 0 & l \end{pmatrix} \Gamma$$

となる.

$l|m$ かつ $(l, N) = 1$ のとき, Δ の元 $T(l, m)$ および $T(n)$ を

$$T(l, m) = \Gamma \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma, \quad T(n) = \sum_{ml=n, l|m, (l, N)=1} T(l, m)$$

で定義する. これより, 特に, $T(p) = T(1, p), T(n, n) = \Gamma \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \Gamma$ である. 同様に Δ^* の元 $T^*(m, l)$ および $T^*(n)$ が定義される.

定理 4.2. $\mathcal{R}_N$ および $\mathcal{R}_N^*$ は可換環となる.

命題 4.3. $T(1, p^e)$ は次のような剰余類分解をもつ.

$$T(1, p^e) = \begin{cases} \bigcup_{\substack{0 \leq f \leq e, 0 \leq m < p^f \\ (m, p^f, p^{e-f})=1}} \Gamma \begin{pmatrix} p^{e-f} & m \\ 0 & p^f \end{pmatrix}, & (p \nmid N) \\ \bigcup_{0 \leq m < p^e} \Gamma \begin{pmatrix} 1 & m \\ 0 & p^e \end{pmatrix}, & (p|N). \end{cases}$$

命題 4.4. (1) $(lm, l'm') = 1$ のとき, $T(l, m)T(l', m') = T(ll', mm')$ となる. 特に, $(m, n) = 1$ のとき, $T(m)T(n) = T(mn)$ となる.
(2) $T(al, am) = T(a, a)T(l, m)$

命題 4.5

$$T(p)T(1, p^e) = T(1, p^{e+1}) + \begin{cases} (p+1)T(p, p) & p \nmid N, e = 1, \\ pT(p, p)T(1, p^{e-1}) & p \nmid N, e > 1, \\ 0 & p|N \end{cases}$$

となる. 特に,

$$T(p)T(p^e) = \begin{cases} T(p^{e+1}) + pT(p, p)T(p^{e-1}) & p \nmid N, \\ T(p^{e+1}) & p|N \end{cases}$$

となる.

さて, 命題 4.3 と命題 4.4 より次のことがわかる.

命題 4.6. $l|m, (l, N) = 1$ のとき, $T(l, m)$ は次の剰余類分解をもつ.

$$T(l, m) = \bigcup_{\substack{ad=lm, 0 \leq b < d \\ (a, b, d)=l, (a, N)=1}} \Gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

とくに

$$T(n) = \bigcup_{\substack{ad=n, 0 \leq b < d \\ (a, N)=1}} \Gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

注意. Δ^* の元 $T^*(m, l), T^*(n)$ についても命題 4.3, 4.4, 4.5, 4.6 と同様のことが言える.

定理 4.7. $\mathcal{R}_N$ は $\mathbb{C}$ 上 $T(p), T(p, p)$ ($p \nmid N$), $T(q)$ ($q|N$) で生成され, これらの生成元は $\mathbb{C}$ 上代数的独立である. 同様なことが $\mathcal{R}_N^*$ についても成り立つ.

$\tilde{\mathcal{R}}_N$ で $\mathbb{C}$ 上 $T(p), T(p, p)$ ($p \nmid N$) で生成される $\mathcal{R}_N$ の部分環を表す.

5 Hecke 作用素と Euler 積

この節では, 前節で定義した Hecke 環の元をモジュラー形式の空間に作用させよう. この節でも $\Gamma = \Gamma_0(N)$ とおく. χ を N を法とする Dirichlet 指標とするとき, 2 節に述べたように, χ によって定まる Γ の指標を同じ χ で表す. また, $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_0(N)$ に対して $\chi'(\alpha) = \overline{\chi(a)}$ と定める. 同様にして, $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_0^*(N)$ に対して, $\chi^{*'}(\alpha) = \overline{\chi(d)}$ と定める.

さて, $\mathcal{R}_N$ の元 $\Gamma\alpha\Gamma$ を $\Gamma\alpha\Gamma = \bigcup_{\nu} \Gamma\alpha_{\nu}$ と剰余類分解し, $f(z) \in \mathfrak{M}_k(\Gamma, \chi)$ に対して

$$f|\Gamma\alpha\Gamma(z) = (\det \alpha)^{k/2-1} \sum_{\nu} \overline{\chi'(\alpha)} f|_k \alpha_{\nu}(z)$$

と定義する. 同様にして, $\mathcal{R}_N^*$ の元 $\Gamma\alpha\Gamma = \bigcup_{\nu} \Gamma\alpha_{\nu}$ に対して $f|\Gamma\alpha\Gamma(z)$ を上の定義における $\chi'(\alpha_{\nu})$ を $\chi^{*'}(\alpha_{\nu})$ に換えて定義する. これらの定義は代表元 $\{\alpha_{\nu}\}$ のとり方によらない. また, 上のどちらの場合にも, $f|\Gamma\alpha\Gamma(z) \in \mathfrak{M}_k(\Gamma, \chi)$ となることがわかる. これらにより, $\mathcal{R}_N$ および $\mathcal{R}_N^*$ の $\mathfrak{M}_k(\Gamma, \chi)$ への作用が定義される. この作用を Hecke 作用素とよぶ. 以下, Hecke 作用素の性質について述べよう.

命題 5.1. $f(z) = \sum_{n=0}^{\infty} c(n)\mathbf{e}(nz) \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ に対して,

$$f|T(m)(z) = \sum_{n=0}^{\infty} b(n)\mathbf{e}(nz)$$

とおくとき

$$b(n) = \sum_{0 < a|(m, n)} \chi(a) a^{k-1} c(mn/a^2)$$

となる. 特に, $b(1) = c(m)$ となる.

系. 上の定理で $m = p$ とおく.

- (1) $p|n$ のとき, $b(n) = c(pn)$ である.
(2) $p \nmid n$ のとき $b(n) = c(pn) + p^{k-1}\chi(p)c(p^{-1}n)$ である.

定理 5.2. (1) $f(z) \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ とすると, $(lm, N) = 1$ のとき,

$$f|T^*(m, l) = \overline{\chi(lm)}f|T(l, m)$$

となる. また, $(n, N) = 1$ に対して

$$f|T^*(n) = \overline{\chi(n)}f|T(n)$$

となる.

- (2) $(lm, N) = 1$ のとき, すべての $f, g \in \mathfrak{S}_k(\Gamma_0(N), \chi)$ に対して

$$\langle f|T(l, m), g \rangle = \langle f, g|T^*(m, l) \rangle$$

となる. すなわち, *Petersson* 内積に関して $T^*(m, l)$ は $T(l, m)$ の随伴作用素である. また, $(n, N) = 1$ のとき, すべての $f, g \in \mathfrak{S}_k(\Gamma_0(N), \chi)$ に対して

$$\langle f|T(n), g \rangle = \langle f, g|T^*(n) \rangle$$

となる. すなわち, *Petersson* 内積に関して $T^*(n)$ は $T(n)$ の随伴作用素である.

系. $(n, N) = 1$ のとき, $T(n)$ は $\mathfrak{S}_k(\Gamma_0(N), \chi)$ の正規作用素である. すなわち, すべての $f \in \mathfrak{S}_k(\Gamma_0(N), \chi)$ に対して

$$f|T(n)T^*(n) = f|T^*(n)T(n)$$

となる. 特に χ が単位指標のとき, $T^*(n) = T(n)$ すなわち, $T(n)$ は自己共役作用素である.

定義 S を $\mathcal{R}_N$ または $\mathcal{R}_N^*$ の部分環とする. このとき, $f \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ が S -Hecke 固有形式であるとはすべての $T \in S$ の同時固有関数となることをいう. 特に, $\mathcal{R}_N$ -Hecke 固有形式を単に Hecke-固有形式という. また, $\mathfrak{M}_k(\Gamma_0(N), \chi)$ の部分空間 M が S -安定とはすべての $T \in S$ の作用に対して M が閉じていることをいう.

Hecke 作用素は互いに可換であり, $(n, N) = 1$ のとき $T(n)$ は正規作用素であるから, 線形代数の一般論より次のことが成り立つ.

定理 5.3. M を $\tilde{\mathcal{R}}_N$ -安定な $\mathfrak{S}_k(\Gamma_0(N), \chi)$ の部分空間とすると, M は $\tilde{\mathcal{R}}_N$ -固有形式からなる基底をもつ. 特に, $\mathfrak{S}_k(\Gamma_0(N), \chi)$ は $\tilde{\mathcal{R}}_N$ -固有形式からなる基底をもつ.

さて, $f(z) = \sum_{m=0}^{\infty} a(m)e(mz) \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ を $\tilde{\mathcal{R}}_N$ -固有形式とすると, すべての $(m, N) = 1$ に対して

$$f|T(m) = \lambda(m)f \quad (\lambda(m) \in \mathbb{C})$$

と表される．よって，命題 5.1 より $a(m) = \lambda(m)a(1)$ となる．よって，

$$\tilde{L}(s, f) = \sum_{\substack{m=1 \\ (m, N)=1}}^{\infty} \frac{a(m)}{m^s}$$

とおくとき

$$\tilde{L}(s, f) = a(1) \sum_{\substack{m=1 \\ (m, N)=1}}^{\infty} \frac{\lambda(m)}{m^s}$$

となる． $\tilde{L}(s, f)$ を詳しく調べよう．まず，命題 4.4 より $(m, n) = 1$ ならば

$$\lambda(mn) = \lambda(m)\lambda(n)$$

となるから $\operatorname{Re}(s)$ が十分大きいとき

$$\tilde{L}(s, f) = \prod_{p \nmid N} L_p(s, f)$$

となる．ここで

$$L_p(s, f) = \sum_{m=0}^{\infty} \lambda(p^e) p^{-es}$$

とおいた．さらに，

$$f|T(p, p) = \chi(p)p^{k-2}f$$

と命題 4.5 より

$$\lambda(p)\lambda(p^e) = \lambda(p^{e+1}) + \chi(p)p^{k-1}\lambda(p^{e-1})$$

となるから，

$$\sum_{m=0}^{\infty} \lambda(p^e) p^{-es} = (1 - \lambda(p)p^{-s} + p^{-2s+k-1}\chi(p))^{-1}$$

となる．さらに， $f(z)$ は $\mathcal{R}_N$ -Hecke 固有形式であるとしよう．このとき，やはり命題 4.5, 5.1 より

$$L(s, f) = a(1) \prod_p L_p(s, f)$$

となる．さらに， $\lambda(p)$ を $T(p)$ の固有値とすると命題 4.5 より $p|N$ に対して

$$\lambda(p^{e+1}) = \lambda(p^e)\lambda(p)$$

となるから

$$\sum_{m=0}^{\infty} \lambda(p^e) p^{-es} = (1 - \lambda(p)p^{-s})^{-1}$$

となるが $\chi(p) = 0$ に注意すると, これも $p \nmid N$ のときと同じく $(1 - \lambda(p)p^{-s} + p^{-2s+k-1}\chi(p))^{-1}$ と表される. これらをまとめると次のことが成り立つ.

定理 5.4. $f(z) = \sum_{m=0}^{\infty} a(m)\mathbf{e}(mz) \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ を $\tilde{\mathcal{R}}_N$ -固有形式とすると,

$$\tilde{L}(s, f) = a(1) \prod_{p \nmid N} (1 - \lambda(p)p^{-s} + p^{-2s+k-1}\chi(p))^{-1}$$

となる. さらに, $f(z)$ が $\mathcal{R}_N$ -固有形式とすると,

$$L(s, f) = a(1) \prod_p (1 - \lambda(p)p^{-s} + p^{-2s+k-1}\chi(p))^{-1}$$

となる. このとき, 特に $a(1) \neq 0$ である.

上に述べた議論を逆にたどることにより, 次のこともわかる.

定理 5.5. $f(z) = \sum_{m=0}^{\infty} a(m)\mathbf{e}(mz) \in \mathfrak{M}_k(\Gamma_0(N), \chi)$ とする. f に付随する *Dirichlet* 級数が

$$L(s, f) = c \prod_p (1 - t(p)p^{-s} + p^{-2s+k-1}\chi(p))^{-1}$$

の形に表されるとする. ただし, c は零でない複素数で, $t(p)$ は各素数に対して決まる複素数である. このとき, $f(z)$ は $\mathcal{R}_N$ -固有形式であり, すべての p に対して

$$f|T(p) = t(p)f$$

となる.

以上により, $\mathcal{R}_N$ -固有形式がモジュラー形式の整数論にとって重要であることがわかった. しかしながら, $\mathfrak{S}_k(\Gamma_0(N), \chi)$ は $\mathcal{R}_N$ -固有形式からなる基底をもつとは限らない.

例. $\mathcal{R}_N$ -固有形式からなる基底をもつとは限らない例を述べるために, まず次のことに注意する.

N, l を正の整数とする. $f(z) = \sum_{m=1}^{\infty} a(m)\mathbf{e}(mz) \in \mathfrak{S}_k(\Gamma_0(N), \chi)$, $a(1) = 1$ とする. このとき $l'|l$ なる任意の正の整数に対して $f_{l'}(z) = f(l'z)$ とおくと, $f_{l'}(z) \in \mathfrak{S}_k(\Gamma_0(lN), \chi)$ となる. Hecke-作用素の作用をみるために, しばらくの間, $\alpha \in \Delta_0(N)$ に対して $\Gamma_0(N)\alpha\Gamma_0(N)$ の $\mathfrak{S}_k(\Gamma_0(N), \chi)$ への作用を $T^{(N)}$, $\Gamma_0(lN)\alpha\Gamma_0(lN)$ の $\mathfrak{S}_k(\Gamma_0(lN), \chi)$ への作用を $T^{(lN)}$ で表す. すると, $(n, lN) = 1$ のとき,

$$f|T^{(N)}(n)(z) = \lambda(n)f(z)$$

ならば,

$$f_{l'}|T^{(lN)}(n)(z) = \lambda(n)f_{l'}(z)$$

となる. 特に, $f(z)$ が $\tilde{\mathcal{R}}_N$ -Hecke 固有形式ならば $f_{l'}(z)$ は $\tilde{\mathcal{R}}_{lN}$ -Hecke 固有形式である.

さて, $f(z) = \sum_{m=1}^{\infty} a(m)\mathbf{e}(mz) \in \mathfrak{S}_k(SL_2(\mathbf{Z}))$, $a(1) = 1$ は Hecke-固有形式であるとする. このとき, $f(z), f(pz), f(p^2z), f(p^3z)$ で生成される $\mathfrak{S}_k(\Gamma_0(p^3))$ の部分空間を M とおくと, M は $\mathcal{R}_{p^3}$ -安定である. $T'(p) = T^{(p^3)}(p)$ とおく.

$$f_{p^i}(z) = \sum_{m=1}^{\infty} a(p^{-i}m)\mathbf{e}(mz)$$

であり,

$$f_{p^i}|T'(p)(z) = \sum_{m=1}^{\infty} a(p^{-i+1}m)\mathbf{e}(mz)$$

だから, $i \geq 1$ ならば

$$f_{p^i}|T'(p)(z) = f_{p^{i-1}}(z)$$

である. また, $c(pm) = c(p)c(m) - p^{k-1}c(mp^{-1})$ に注意すると,

$$f|T'(p)(z) = c(p)f(z) - p^{k-1}f_p(z)$$

となり, まとめると $T'(p)$ の作用は

$$(f|T'(p), f_p|T'(p), f_{p^2}|T'(p), f_{p^3}|T'(p)) = (f, f_p, f_{p^2}, f_{p^3}) \begin{pmatrix} c(p) & 1 & 0 & 0 \\ -p^{k-1} & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

と表される. この表現行列はあきらかに対角化できない. すなわち, M は $T'(p)$ の固有関数からなる基底を持たない. よって, $\mathfrak{S}_k(\Gamma_0(p^3))$ 自身もそうである.

上の例のような現象が起きるのは, レベルの低いモジュラー形式も含めて Hecke 環の作用を考えたからである. それ故, それらを取り除いた部分空間を考えれば話がうまくいくのではないかと考えられる. 実際, それが可能であり, これが新形式 (new form) の理論と呼ばれるものである. これを, 述べるために m_χ を χ の導手としたとき,

$$\mathfrak{S}_k(\Gamma_0(N), \chi)^{(1)} = \langle \cup_{M \neq N, m_\chi | M, M|N} \cup_{l | \frac{N}{M}} \{f(lz) \mid f(z) \in \mathfrak{S}_k(\Gamma_0(M), \chi)\} \rangle$$

を旧形式 (old form) の空間という. また, $\mathfrak{S}_k(\Gamma_0(N), \chi)^{(0)}$ で $\mathfrak{S}_k(\Gamma_0(N), \chi)^{(1)}$ の Petersson 内積に関する直交補空間を表し, 新形式 (new form) の空間という. また, $f(z) = \sum_{m=1}^{\infty} a(m)\mathbf{e}(mz) \in \mathfrak{S}_k(\Gamma_0(N), \chi)$ が原始形式であるとは次の条件を満たすときをいう.

- (1) $f(z)$ は $\mathfrak{S}_k(\Gamma_0(N), \chi)^{(0)}$ に属する.
- (2) $f(z)$ は $\tilde{\mathcal{R}}_N$ -Hecke 固有形式であり, $a(1) = 1$ である.

定理 5.6. (1) $\mathfrak{S}_k(\Gamma_0(N), \chi)$ の原始形式は $\mathcal{R}_N$ -Hecke 固有形式である.

(2) $\mathfrak{S}_k(\Gamma_0(N), \chi)^{(0)}$ は原始形式からなる基底を持つ.

6 モジュラー形式のL関数の代数性

”はじめに”で述べたように, m が正の偶数のとき, $\frac{\zeta(m)}{\pi^m}$ は有理数となる. このような現象が, モジュラー形式のL関数の場合でも起こることを, 主として [Shimura, 1976] に基づき解説する. $\mathfrak{S}_k(\Gamma_0(N), \chi)$ における原始形式 f に対して, $T(m) \in \mathcal{R}_N$ の固有値を $\lambda(m)$ とおき, K_f で $\mathbf{Q}$ 上すべての $\lambda(m)$ で生成される体を表す. また, Dirichlet 指標 ψ に対して K_ψ で $\mathbf{Q}$ 上すべての ψ の値で生成される体を表す. このとき K_f は $\mathbf{Q}$ 上の有限次拡大体になることが知られている. さて, 次のことが知られている.

命題 6.1. $f(z) = \sum_{m=1}^{\infty} a(m)\mathbf{e}(mz)$ を $\mathfrak{S}_k(\Gamma_0(N), \chi)$ の元とする. このとき, $\sigma \in \text{Aut}(\mathbf{C})$ に対して $f^\sigma(z) = \sum_{m=1}^{\infty} a(m)^\sigma \mathbf{e}(mz)$ とおくと, $f^\sigma \in \mathfrak{S}_k(\Gamma_0(N), \chi^\sigma)$ となる. ここで $\chi^\sigma(m) = \chi(m)^\sigma$ である. 特に, f が原始形式なら, f^σ もそうである.

さて, Dirichlet 指標 ψ に対して

$$A(m, f, \psi) = \frac{L(m, f, \psi)}{W(\psi_0)(2\pi i)^m}$$

とおく. ここで ψ_0 は ψ に付随する原始指標で, $W(\psi_0)$ は Gauss 和を表す.

定理 6.2. f を $\mathfrak{S}_k(\Gamma_0(N), \chi)$ における原始形式とする. このとき, 二つの原始指標 ψ, ψ' と正の整数 $m, m' < k$ で $\psi(-1)\psi'(-1) = (-1)^{m-m'-1}$ を満たすものに対して

$$C(m, m'; f, \psi, \psi') = \frac{A(m, f, \psi)A(m, f, \psi')\sqrt{-1}^{k-1}}{\pi W(\chi)\langle f, f \rangle}$$

とおくと, 任意の $\sigma \in \text{Aut}(\mathbf{C})$ に対して

$$C(m, m'; f, \psi, \psi')^\sigma = C(m, m'; f^\sigma, \psi^\sigma, \psi'^\sigma)$$

となる. 特に $C(m, m'; f, \psi, \psi') \in K_f K_\psi K_{\psi'}$ となる.

定理 6.3. f を $\mathfrak{S}_k(\Gamma_0(N), \chi)$ における原始形式とする. このとき, 二つの原始指標 ψ, ψ' と正の整数 $m, m' < k$ で $\psi(-1)\psi'(-1) = (-1)^{m-m'-1}$ かつ $L(m', f, \psi') \neq 0$ を満たすものに対して

$$B(m, m'; f, \psi, \psi') = \frac{A(m, f, \psi)}{A(m', f, \psi')}$$

とおくと, 任意の $\sigma \in \text{Aut}(\mathbf{C})$ に対して

$$B(m, m'; f, \psi, \psi')^\sigma = B(m, m'; f^\sigma, \psi^\sigma, \psi'^\sigma)$$

となる. 特に $B(m, m'; f, \psi, \psi') \in K_f K_\psi K_{\psi'}$ となる.

上の定理より次の重要な結果が得られる.

定理 6.3. f を $\mathfrak{S}_k(\Gamma_0(N), \chi)$ における原始形式とする. このとき, ある二つの零でない複素数 $\Omega^{(+)}, \Omega^{(-)}$ が存在して, 原始指標 ψ と正の整数 $m < k$ で $\psi(-1) = j(-1)^m$ ($j = \pm 1$) を満たすものに対して $\frac{A(m, f, \psi)}{\Omega^{(j)}} \in K_f K_\psi$ となる. このような複素数 $\Omega^{(+)}, \Omega^{(-)}$ はそれぞれ $K_f^\times$ 倍を除いて一意に定まる.

注意 1. 上の定理において m は有限個の範囲しか動かないが ψ は無限個動き得る.

注意 2. 上の $\Omega^{(\pm)}$ には次のような幾何学的意味がある. E を $\mathbf{Q}$ 上定義された導手が N の楕円曲線とし, 一意化写像

$$\phi : (\Gamma_0(N) \backslash \mathbf{H}^*) \longrightarrow E$$

があるとしよう. このとき, ある原始形式 $f \in \mathfrak{S}_2(\Gamma_0(N))$ でその Fourier 係数が有理数であるものが存在して

$$\phi^* \omega = c_E f(z) 2\pi i dz \quad (c_E \in \mathbf{Q}^\times)$$

となる. ここで, ω は Neron の微分形式である. このとき, E の 1 次ホモロジー群 $H_1(E, \mathbf{Z})$ の部分群 $H_1(E, \mathbf{Z})^{(\pm)}$ を

$$H_1(E, \mathbf{Z})^{(\pm)} = \{c \in H_1(E, \mathbf{Z}) \mid c^\rho = \pm c\}$$

で定義する. ここで, ρ は複素共役写像によって $H_1(E, \mathbf{Z})$ に誘導される写像である. このとき, $H_1(E, \mathbf{Z})^{(\pm)}$ は $\mathbf{Z}$ 上の 1 次元自由加群である. その生成元を $\gamma^{(\pm)}$ とし,

$$\Omega_E^{(\pm)} = \int_{\gamma^{(\pm)}} \omega$$

とおくと, $\Omega^{(+)}, \Omega^{(-)}$ としてそれぞれ $\Omega_E^{(+)}, \Omega_E^{(-)}$ を取ることができる.

References

- [Miyake, 1989] T. Miyake, Modular forms, Springer, 1989.
- [村瀬, 2006] 村瀬篤, 楕円曲線, 「整数論札幌夏の学校」報告集, 2006
- [Shimura, 1967] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Iwanami Shoten and Princeton University press, 1971.
- [Shimura, 1976] G. Shimura, The special values of the zeta functions associated with cusp forms, Comm. Pure Appl. Math. 29(1976), 783-804.
- [Shimura, 2000] G. Shimura, Arithmeticity in the theory of automorphic forms, Mathematical Surveys and Monographs 82(2000), Amer. Math. Soc.
- [Yoshida, 2003] H. Yoshida, Absolute CM-Period, Mathematical Surveys and Monographs, 106(2003), Amer. Math. Soc.
- H. Katsurada, Muroran Institute of Technology, 27-1 Mizumoto, Muroran, 050-8585, Japan (hidenori@mmm.muroran-it.ac.jp)

楕円曲線入門*

村瀬 篤 (京都産業大学・理学部)

- I. 体上の楕円曲線
- II. $\mathbf{C}$ 上の楕円曲線
- III. Tate module とガロア表現
- IV. 補注
- 参考文献
- 文献案内

I. 体上の楕円曲線

§1. Introduction

(1) 体 k 上の楕円曲線とは、

$$\begin{cases} E: & k \text{ 上の絶対既約、smooth かつ種数 } 1 \text{ の曲線} \\ \mathcal{O}: & E(k) \text{ の点} \end{cases}$$

の組のことをいう。

(2) 重要な性質

(i) $\mathcal{O}$ を単位元とするアーベル群の構造が入る。

(ii) Weierstrass の標準形

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in k)$$

を持つ。

§2. Weierstrass 方程式

(1) 射影空間と平面曲線

- 体 $K(k \subset K \subset \bar{k})$ に対し、 $\mathbf{P}^n(K) = (K^{n+1} - \{(0, \dots, 0)\}) / \sim$ とおく。ここに、

$$(x_0, \dots, x_n) \sim (x'_0, \dots, x'_n) \iff \exists \lambda \in K^\times \text{ such that } x'_i = \lambda x_i \ (i = 0, \dots, n).$$

各類を $[x_0 : \dots : x_n]$ で表す。

* 整数論札幌夏の学校講義時 (2006 年 8 月 29 日) に配布した資料に加筆・修正したもの

- 同次多項式 $F(X, Y, Z) \in k[X, Y, Z]$ に対し、

$$C = \{[x : y : z] \in \mathbf{P}^2(\bar{k}) \mid F(x, y, z) = 0\}$$

を、 F を定義方程式とする k 上の射影的平面曲線という (以後、単に曲線という)。 F が $\bar{k}$ 上既約であるとき、 C は絶対既約であるという。

- 体 K ($k \subset K \subset \bar{k}$) に対し、

$$C(K) = \{[x : y : z] \in \mathbf{P}^2(K) \mid F(x, y, z) = 0\}$$

とおく。 $\text{Aut}(K/k)$ は $C(K)$ に自然に作用する。

- C が smooth であるとは、 C の各点 P に対し、

$$\left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z} \right)_P \neq (0, 0, 0)$$

が成り立つことをいう。

- smooth な曲線 C に対し、種数 $g(C) \in \mathbf{Z}_{\geq 0}$ が定まる (後述)。 C の定義方程式が d 次ならば、 $g(C) = (d-1)(d-2)/2$ である。

(2) 楕円曲線と Weierstrass 方程式

- 絶対既約かつ smooth な k 上の曲線 E で $g(E) = 1$ であるものと $E(k)$ の点 $\mathcal{O}$ を、 k 上の楕円曲線という。
- k 上の楕円曲線は、次の Weierstrass 方程式で定義される曲線 E と isomorphic である (“isomorphic” については補注を参照のこと)。

$$F(X, Y, Z) = (Y^2Z + a_1XYZ + a_3YZ^2) - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) \quad (a_i \in k).$$

ただし、判別式 $\Delta(E)$ (後述) は 0 でないとする。以後この節では、この形の曲線を考える。

- k の標数が 2 でも 3 でもないとき、適当なアフィン変換をほどこすことにより、Weierstrass 方程式として、 $Y^2Z - (X^3 + AXZ^2 + BZ^3)$ の形のものがとれる。このとき、 $\Delta(E) = -16(4A^3 + 27B^2)$ である。
- E は、アフィン部分 $\{[x : y : 1] \mid f(x, y) = 0\}$ と、“無限遠点” $\mathcal{O} = [0 : 1 : 0]$ からなる。ここに、 f は F のアフィン化である：

$$f(x, y) := F(x, y, 1) = (y^2 + a_1xy + a_3y) - (x^3 + a_2x^2 + a_4x + a_6).$$

(3) 判別式 $\Delta(E)$ と smoothness

- F の係数 a_i ($i = 1, \dots, 6$) から、 E の判別式 $\Delta = \Delta(E)$ を次のように定める。

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & c_4 &= b_2^2 - 24b_4, \\ b_4 &= a_1a_3 + 2a_4, & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ b_6 &= a_3^2 + 4a_6, & \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \end{aligned}$$

- E が smooth $\iff \Delta(E) \neq 0$.

(4) 不変量 $j(E)$

- $j(E) := \frac{c_4^3}{\Delta(E)}$.
- k 上の楕円曲線 E, E' に対し、

$$j(E) = j(E') \iff E, E' \text{ は } \bar{k} \text{ 上 isomorphic.}$$

(5) 加法の幾何的定義 (chord-tangent method)

- $P, Q \in E$ に対し、 ℓ を P, Q を結ぶ直線とする ($P = Q$ のときは P における接線)。 E と ℓ は重複度をこめて 3 点で交わる。それらを $P, Q, R = P * Q$ とする。 $P + Q = (P * Q) * \mathcal{O}$ により、 E の加法を定める。 $\mathcal{O}$ はこの加法について単位元であり、 $P = [x : y : 1]$ の逆元は $[x : -y - a_1x - a_3 : 1]$ である。また、 $k \subset K \subset \bar{k}$ に対し、 $E(K)$ は E の部分群をなす。

§3. Riemann-Roch の定理

この節では、 C を絶対既約かつ smooth な k 上の曲線とする。 $F \in k[X, Y, Z]$ を C の定義多項式とする。

(1) 因子群

- k 上の曲線 C に対し、 C 上の点の整数係数の形式的有限和のなす集合を

$$\text{Div}(C) := \left\{ \sum_{P \in C} n_P (P) \mid n_P \in \mathbf{Z}, \ n_P = 0 \ (\forall' P) \right\}$$

と書く。 $\text{Div}(C)$ は自然な加法により、アーベル群をなす。 $\text{Div}(C)$ を、 C の因子群という。零元を $\mathbf{0}$ と書く。

- 因子 $D = \sum_{P \in C} n_P (P)$ に対し、 $\deg(D) := \sum_{P \in C} n_P$ とおく。
- $\text{Div}^0(C) := \{D \in \text{Div}(C) \mid \deg(D) = 0\}$ は $\text{Div}(C)$ の部分群をなす。

(2) 有理関数とその因子

- 体 $k \subset K \subset \bar{k}$ に対し、

$$K(C) := \left\{ \frac{G(X, Y, Z)}{H(X, Y, Z)} \mid G, H \in K[X, Y, Z] \text{ は同次多項式, } \deg(G) = \deg(H), \ F \nmid H \right\} / \sim_F$$

を、 C の K 上の関数体という。ここに、

$$\frac{G}{H} \sim_F \frac{G'}{H'} \iff F \mid (GH' - HG').$$

- $\varphi = \frac{G}{H} \in K(C)$ と $P \in C$ に対し、

$$\text{ord}_P(\varphi) := I_P(F, G) - I_P(F, H)$$

とおく。ここに、同次多項式 $F' \in K[X, Y, Z]$ に対し、 $I_P(F, F') \in \mathbf{Z}_{\geq 0}$ を次のように定める。もし、 $F'(P) \neq 0$ ならば、 $I_P(F, F') = 0$ とする。そうでないとき、 P のアフィン近傍 (アフィン座標を u, v とする) を取り、そこでの F, F' のアフィン化を $f(u, v), f'(u, v)$ とするとき、 $I_P(F, F') = \dim_K K[u, v]_{(u, v)} / (f, f')$ とおく。ここに、 $K[u, v]_{(u, v)}$ は $K[u, v]$ の極大イデアル (u, v) による局所化である。

- $\varphi \in K(C)$ に対し、

$$\text{div}(\varphi) := \sum_{P \in C} \text{ord}_P(\varphi)(P)$$

とおく。このとき、 $\text{div}(\varphi) \in \text{Div}^0(C)$ である。

(3) effective な因子

- 因子 $D = \sum_{P \in C} n_P(P)$ に対し、 $n_P \geq 0 (\forall P)$ であるとき、 D は effective (または positive) であるといい、 $D \geq 0$ と書く。

(4) $L(D)$

- 因子 D に対し、

$$L(D) := \{\varphi \in \bar{k}(C)^\times \mid D + \text{div}(\varphi) \geq 0\} \cup \{0\}$$

とおく。 $L(D)$ は、 $\bar{k}$ 上の有限次元ベクトル空間である。

(5) Riemann-Roch の定理、種数

- Riemann(-Roch) の定理: k 上の曲線 C に対し、0 以上の整数 $g(C)$ が存在し、次を満たす。任意の因子 D に対し、不等式

$$\dim_{\bar{k}} L(D) \geq \deg(D) - g(C) + 1$$

が成立する。また、 $\deg(D) > 2g(C) - 2$ ならば、等号が成立する。

- $g(C)$ を C の種数 (genus) という。
- Weierstrass 方程式で定義される曲線で smooth なものは種数 1 である。

§4. Abel の定理

(1) 線形同値、 $\text{Pic}(C), \text{Pic}^0(C)$

- $D, D' \in \text{Div}(C)$ に対し、 $D - D' = \text{div}(\varphi)$ となるような $\varphi \in \bar{k}(C)^\times$ が存在するとき、 D, D' は線形同値であるといい、 $D \sim D'$ と書く。 $\text{Pic}(C) = \text{Div}(C)/\sim$ は自然な加法によりアーベル群をなす。 $\text{Pic}^0(C) = \text{Div}^0(C)/\sim$ は $\text{Pic}(C)$ の部分群をなす。 $D \in \text{Div}(C)$ の $\text{Pic}(C)$ における類を $\overline{D}$ と書く。

(2) Abel の定理

- Abel の定理: k 上の楕円曲線 E に対し、写像

$$E \ni P \mapsto \overline{(P) - (\mathcal{O})} \in \text{Pic}^0(E)$$

は、 E から $\text{Pic}^0(E)$ への全単射を与える。

- これより、 E に加法の構造が入る。すなわち、 $P, Q \in E$ に対し

$$(P) - (\mathcal{O}) + (Q) - (\mathcal{O}) \sim (P \oplus Q) - (\mathcal{O})$$

となる $P \oplus Q \in E$ が一意的に存在する。この加法は明らかに結合法則を満たす。一方、 E が Weierstrass 方程式で定義される曲線るとき、加法 $\oplus$ と chord-tangent method による加法 $+$ は一致する。

§5. 等分点

E を k 上の楕円曲線とする。 k の標数を p とする ($p \geq 0$)。

- (1) 正整数 m に対し、 $P \mapsto mP = \underbrace{P + \cdots + P}_{m \text{ 個}}$ は E の (全射) 準同型を定める。この準同型の核を $E[m]$ と書く。すなわち、 $E[m] := \{P \in E \mid mP = \mathcal{O}\}$ 。
- (2) $p = 0$ または $p > 0, p \nmid m$ のとき、 $E[m]$ はアーベル群として、 $(\mathbf{Z}/m\mathbf{Z})^2$ に同型である。
- (3) $p > 0$ のとき、 $E[p^r]$ は $\mathbf{Z}/p^r\mathbf{Z}$ または $\{0\}$ に同型である。
- (4) $\sigma \in \text{Gal}(\bar{k}/k)$ に対し、 $\sigma(mP) = m\sigma(P)$ であるから、 $\text{Gal}(\bar{k}/k)$ は $E[m]$ に作用する。(2) の条件が満たされるとき、 $E[m]$ のアーベル群としての基をとると、この作用はガロア表現 $\rho: \text{Gal}(\bar{k}/k) \rightarrow \text{GL}_2(\mathbf{Z}/m\mathbf{Z})$ を定める。
- (5) 次の 3 条件を満たす bilinear pairing $e_m: E[m] \times E[m] \rightarrow \mu_m = \{\zeta \in \bar{k}^\times \mid \zeta^m = 1\}$ が存在する (Weil pairing; 構成法については、補注を見よ)。
 - (i) $e_m(P, P) = 1$ ($P \in E[m]$)。
 - (ii) $e_m(P, E[m]) = 1 \implies P = \mathcal{O}$ 。
 - (iii) $\sigma(e_m(P, Q)) = e_m(\sigma P, \sigma Q)$ ($\sigma \in \text{Gal}(\bar{k}/k), P, Q \in E[m]$)。
- (6) Weil pairing の存在より、

$$\zeta^{\det \rho(\sigma)} = \zeta^\sigma \quad (\sigma \in \text{Gal}(\bar{k}/k), \zeta \in \mu_m)$$

が示される。

II. $\mathbf{C}$ 上の楕円曲線

§1. 楕円関数、Abel の定理

- $\mathbf{R}$ 上 1 次独立な $\omega_1, \omega_2 \in \mathbf{C}$ に対し、lattice $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ を考える。
- $\mathbf{C}(\Lambda) := \{f: \mathbf{C} \text{ 上の有理型関数}, f(z + \omega) = f(z) \ (\omega \in \Lambda)\}$ (Λ を周期とする楕円関数体)。
- $\text{Div}(\mathbf{C}/\Lambda) := \left\{ D = \sum_{w \in \mathbf{C}/\Lambda} n_w(w) \mid n_w \in \mathbf{Z}, n_w = 0 \ (\forall' w) \right\}, \quad \deg D := \sum_w n_w.$
- $\text{Div}^0(\mathbf{C}/\Lambda) := \{D \in \text{Div}(\mathbf{C}/\Lambda) \mid \deg D = 0\}.$
- $f \in \mathbf{C}(\Lambda)^\times$ に対し、 $\text{div}(f) := \sum_{w \in \mathbf{C}/\Lambda} \text{ord}_w(f)(w) \in \text{Div}(\mathbf{C}/\Lambda)$, ここに $\text{ord}_w(f)$ は f の w における位数。このとき、 $\text{div}(f) \in \text{Div}^0(\mathbf{C}/\Lambda)$ である。
- $\text{sum}: \text{Div}^0(\mathbf{C}/\Lambda) \rightarrow \mathbf{C}/\Lambda$ を、 $\text{sum}(\sum_w n_w(w)) := \sum_w n_w w$ で定める。
- Abel の定理:

$$1 \longrightarrow \mathbf{C}^\times \longrightarrow \mathbf{C}(\Lambda)^\times \xrightarrow{\text{div}} \text{Div}^0(\mathbf{C}/\Lambda) \xrightarrow{\text{sum}} \mathbf{C}/\Lambda \longrightarrow 1 \quad (\text{exact}).$$

§2. Weierstrass の $\mathcal{P}$ 関数

- $\mathcal{P}(z; \Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left\{ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right\}, \quad \mathcal{P}'(z; \Lambda) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^3}.$
(以後、 Λ は fix し、しばしば記号から省略する。)
- $\mathbf{C}(\Lambda) = \mathbf{C}(\mathcal{P}(z), \mathcal{P}'(z))$ が成り立つ。
- $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}z^{2k}$ 、ここに $G_k := \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-k}.$
- $z \in \mathbf{C} - \Lambda$ に対し、

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2\mathcal{P}(z) - g_3,$$

ここに $g_2 = 60G_4, g_3 = 140G_6.$

- $E: Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ は $\mathbf{C}$ 上の楕円曲線である。また、

$$\mathbf{C}/\Lambda \ni z \mapsto [\mathcal{P}(z) : \mathcal{P}'(z) : 1] \in \mathbf{P}^2(\mathbf{C})$$

は、複素 Lie 群としての同型写像である。

- $\mathbf{C}$ 上の楕円曲線 E に対し、lattice Λ が存在し、

$$\mathbf{C}/\Lambda \ni z \mapsto [\mathcal{P}(z; \Lambda) : \mathcal{P}'(z; \Lambda) : 1]$$

は複素 Lie 群としての同型写像である。 Λ は $\mathbf{C}^\times$ 倍を除いて一意的に定まる。

§3. $\mathbf{C}$ 上の楕円曲線の等分点の構造

- $(E, \mathcal{O})$ を $\mathbf{C}$ 上の楕円曲線とする。正整数 m に対し、 $E[m] := \{P \in E \mid mP = \mathcal{O}\}$ を E の m 等分点のなす群とする。 $E \simeq \mathbf{C}/\Lambda$ となる lattice Λ をとる。このとき、

$$E[m] \simeq m^{-1}\Lambda/\Lambda \simeq (\mathbf{Z}/m\mathbf{Z})^2$$

である。

III. Tate module とガロア表現

$(E, \mathcal{O})$ を $\mathbf{Q}$ 上の楕円曲線とする。また、 l を素数とする。

§1. Tate module

- l 倍写像 $E[l^{n+1}] \rightarrow E[l^n]$ に関する射影的極限 $T_l(E) = \varprojlim E[l^n]$ を E の Tate module という。すなわち、

$$T_l(E) := \{(x_n)_{n \geq 1} \mid x_n \in E[l^n], lx_{n+1} = x_n \ (n \geq 1)\}.$$

- $T_l(E)$ の位相を、任意の $n \geq 1$ に対し自然な射影 $T_l(E) \rightarrow E[l^n]$ が連続になるような最弱の位相とする。ただし、 $E[l^n]$ の位相は discrete topology をとるものとする。このとき、 $0 \in T_l(E)$ の基本近傍系として $\{l^n T_l(E)\}$ をとることができる。
- $T_l(E)$ はコンパクトアーベル群であり、 $\mathbf{Z}_l$ が連続的に作用する。
- $T_l(E)$ は、局所コンパクトアーベル群として、 $\mathbf{Z}_l^2$ に同型である。

§2. ガロア表現

- $G_{\mathbf{Q}} = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ は $T_l(E) \simeq \mathbf{Z}_l^2$ に作用する。これより、ガロア表現

$$\rho_{E,l}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Z}_l)$$

が得られる。

- また、 $G_{\mathbf{Q}}$ は $V_l(E) := T_l(E) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l \simeq \mathbf{Q}_l^2$ に作用する。これよりガロア表現 $\rho_{E,l}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Q}_l)$ が得られる。

§3. ガロア表現の性質

(1) $\det \rho_{E,l}$ について:

- $\chi_l: G_{\mathbf{Q}} \rightarrow \mathbf{Z}_l^\times$ を $\zeta^\sigma = \zeta^{\chi_l(\sigma)}$ ($\zeta \in \mu_{l^\infty}, \sigma \in G_{\mathbf{Q}}$) で定めると、 $\det \rho_{E,l} = \chi_l$ が成立する。

(2) 特性多項式について:

- 以後、 E は素数 p において good reduction $E^{(p)}$ を持つとする。 $E^{(p)}$ は、有限体 $\mathbf{F}_p$ 上の楕円曲線である。
- $l \neq p$ とする。このとき、 p の $G_{\mathbf{Q}}$ における惰性群は $V_l(E)$ に自明に作用する。
- p の $G_{\mathbf{Q}}$ における Frobenius 元を 1 つ取り、 σ_p とする。このとき、特性多項式 $\det(1 - \rho_{E,l}(\sigma_p)X)$ は Frobenius 元の取り方によらず、

$$1 - a_p X + pX^2$$

に等しい。ここに、 $a_p := p + 1 - |E^{(p)}(\mathbf{F}_p)|$ とおく。

(3) ガロア表現の像 (Serre; 1968, 1972)

- $\text{End}(E) = \mathbf{Z}$ とする。

任意の l に対し、 $\rho_{E,l}(G_{\mathbf{Q}})$ は $\text{Aut}(T_l(E))$ の指数有限部分群である。

ほとんどすべての l に対し、 $\rho_{E,l}(G_{\mathbf{Q}}) = \text{Aut}(T_l(E))$ である。

(4) Faltings (1983)

- $\text{Hom}_{\mathbf{Q}}(E, E') \otimes_{\mathbf{Z}} \mathbf{Z}_l \cong \text{Hom}_{G_{\mathbf{Q}}}(T_l(E), T_l(E'))$.

IV. 補注:

1. 有理写像, morphism, isomorphic

- 体 k 上の曲線 C, C' に対し、写像 $\phi: C \rightarrow C'$ で次の形のものを C から C' への有理写像という:

$$\phi = [\varphi_0 : \varphi_1 : \varphi_2],$$

ここに、 $\varphi_i \in \bar{k}(C)$ ($i = 0, 1, 2$) であり、各 $\varphi_i \in \bar{k}(C)$ が $P \in C$ において regular であるとき、 $\phi(P) = [\varphi_0(P) : \varphi_1(P) : \varphi_2(P)] \in C'$ を満たすものとする。

- 有理写像 $\phi = [\varphi_0, \varphi_1, \varphi_2]: C \rightarrow C'$ が $P \in C$ で regular とは、 $g \in \bar{k}(C)$ で次の 2 条件を満たすものがあるときをいう。

(1) 各 $i = 0, 1, 2$ に対し、 $g\varphi_i$ は P で regular である。

(2) $((g\varphi_i)(P))_{i=0,1,2} \neq (0, 0, 0)$.

- 有理写像 $\phi: C \rightarrow C'$ が各点 $P \in C$ で regular であるとき、 ϕ を C から C' への morphism という。morphism ϕ は、定数写像であるか、または全射である。
- C から C' への morphism ϕ と C' から C への morphism ϕ' で、 $\phi' \circ \phi$ (resp. $\phi \circ \phi'$) が C (resp. C') の恒等写像であるものが存在するとき、 C と C' は isomorphic であるという。

2. Weierstrass の標準形

k 上の楕円曲線 $(E, \mathcal{O})$ が、Weierstrass 方程式で定義される曲線と isomorphic であることを示す。

- $\mathcal{O} \in E(k)$ であることから、 $L(n(\mathcal{O}))$ は k 上定義されることに注意する。
- Riemann-Roch の定理より、 $\dim L(2(\mathcal{O})) = 2, \dim L(3(\mathcal{O})) = 3$ である。これより、 $x, y \in k(E)$ で、 $L(2(\mathcal{O}))$ の k -基底が $\{1, x\}$ 、 $L(3(\mathcal{O}))$ の k -基底が $\{1, x, y\}$ となるものがある。
- 再び、Riemann-Roch の定理より、 $\dim L(6(\mathcal{O})) = 6$ であるから、 $1, x, y, x^2, xy, x^3, y^2 \in L(6(\mathcal{O}))$ は k 上一次従属である。また、一次関係式において、 x^3, y^2 の係数はともに 0 でない。従って、 x, y を適当に定数倍することにより、 x, y は Weierstrass 方程式を満たすことがわかる。写像 $P \in E \mapsto [x(P) : y(P) : 1] \in \mathbf{P}^2(\bar{k})$ が求めるものである ($\mathcal{O}$ は $[0 : 1 : 0]$ に移ることに注意)。

3. Weil paring の構成

- $x, y \in E[m]$ とする。 $mt = x$ となる $t \in E$ をとる。Abel の定理より、

$$\sum_{u \in E[m]} (t + u) - \sum_{u \in E[m]} (u) = \operatorname{div}(g_x)$$

を満たす $g_x \in \bar{k}(E)^\times$ が存在する。このとき、

$$e_m(x, y) = \frac{g_x(z + y)}{g_x(z)}$$

は $z \in E$ の取り方によらず、しかも μ_m に属する。

参考文献

- [C] Cassels, J. W. S., *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193-291.
- [K] Knapp, A. W., *Elliptic curves*, Princeton University Press, 1992.
- [M] Milne, J. S., *Elliptic curves*, online course notes, <http://www.jmilne.org/math/CourseNotes/math679.html>.
- [S1] Silverman, J. H., *The arithmetic of elliptic curves*, Springer, 1986.
- [S2] Silverman, J. H., *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.
- [T] Tate, J., *The arithmetic of elliptic curves*, Inv. Math. **23** (1974), 179-206.

文献案内

楕円曲線に関する文献は膨大にある (たとえば [S1] の文献表を参照のこと)。ここでは、この講義を準備するのに参照したうちの一部を紹介する。[S1] は標準的入門書である。[S2] は [S1] の続篇である。[T] は、証明はほとんどついていないものの、自由な筆致で書かれており楽しい。[S1] との併読をお勧めする。[K] は保型形式との関連を意識して書かれている。また、楕円曲線の chord-tangent method による加法が結合法則を満たすことの幾何的な完全な証明を与えている。[C] は古典的 survey である。[M] は、online text で未完成な部分もあるが、[S1] を補うのに便利である。

古典的岩澤理論

北川浩二

2006.8.31

文責 須田智彦

1 円分 $\mathbb{Z}_p$ 拡大

簡単のため p は奇素数とする. $\mu_{p^n} = \{1 \text{ の } p^n \text{ 乗根} \in \overline{\mathbb{Q}}\}$, $\mu_{p^\infty} = \bigcup_{n=1}^{\infty} \mu_{p^n}$ とおくと

$$\text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

$$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$$

となる. $\Delta \subset \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ を上の同型で $\mathbb{F}_p^\times$ に対応する部分群とし, $\mathbb{Q}_\infty$ を $\mathbb{Q}(\mu_{p^\infty})$ の Δ -不変体とすれば

$$\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = 1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$$

となる. $\mathbb{Q}_\infty$ を $\mathbb{Q}$ の円分 $\mathbb{Z}_p$ 拡大という.

有限次代数体 F に対して, $F_\infty = F\mathbb{Q}_\infty$ とおき, F_∞/F を円分 $\mathbb{Z}_p$ 拡大という. 一般に $\text{Gal}(N/F) \simeq \mathbb{Z}_p$ となる Galois 拡大 N/F を $\mathbb{Z}_p$ 拡大というが, 円分 $\mathbb{Z}_p$ 拡大は $\mathbb{Z}_p$ 拡大である. 実際, $\mathbb{Q}_n$ を $\mathbb{Q}(\mu_{p^{n+1}})$ の Δ -不変体とすると, ある $e \geq 0$ により $F \cap \mathbb{Q}_\infty = \mathbb{Q}_e$ となるので,

$$\text{Gal}(F_\infty/F) \simeq \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_e) \simeq p^e\mathbb{Z}_p \simeq \mathbb{Z}_p$$

が成り立つ. $\mathbb{Z}_p$ 拡大での素点の分解について次のことが成り立つ:

命題 1.1 N/F を $\mathbb{Z}_p$ 拡大とすると, p の上の素点以外は全て不分岐である (レポート問題 1). 分岐する素点は少なくとも 1 つあり, 円分 $\mathbb{Z}_p$ 拡大なら p の上の素点は全て分岐する.

$\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大は 1 個しかないが, 一般には次のように予想されている.

Leopoldt 予想. $\tilde{F}$ を F のすべての $\mathbb{Z}_p$ 拡大の合併体とすれば $\text{Gal}(\tilde{F}/F) \simeq \mathbb{Z}_p^{t+1}$ である. ただし, $2t$ は F の虚素点の個数とする^{*1}.

^{*1} 正確に述べておく. F の最大不分岐アーベル拡大を K とすると $\text{Gal}(K/F) \simeq \text{Cl}(F)$ であるが, いくつかの素点は分岐してもよいとするなら最大アーベル拡大は有限次とはならない. L を p の上にある素点以外は分岐しないような F の最大アーベル p 拡大としよう. 命題 1.1 より $\tilde{F} \subset L$ である. 乗法群

$$E = \{F \text{ の単数 } \varepsilon \mid \text{任意の素点 } \mathfrak{p} \mid p \text{ に対し } \varepsilon \equiv 1 \pmod{\mathfrak{p}}\}$$

を, $\mathbb{Z}_p$ -加群 $\Pi_{\mathfrak{p} \mid p} \{x \in F_{\mathfrak{p}}^\times \mid x \equiv 1 \pmod{\mathfrak{p}}\}$ に対角的に埋め込むと, 閉包 $\overline{E}$ も $\mathbb{Z}_p$ -加群になる. ここで $r =$

F_∞/F を円分 $\mathbb{Z}_p$ 拡大とし, $\Gamma = \text{Gal}(F_\infty/F)$ とおく. F_∞ の部分体で F 上 p^n 次のものがただ 1 つ存在するからそれを F_n とおく. A_n を F_n のイデアル類群 $\text{Cl}(F_n)$ の p -Sylow 群とし, F_n の p -Hilbert 類体を H_n とする. このとき, $m > n$ に対し,

$$\begin{array}{ccccc} A_m & \longrightarrow & \text{Gal}(H_m/F_m) & & A_m \longrightarrow \text{Gal}(H_m/F_m) \\ \text{Nr} \downarrow & \circlearrowleft & \downarrow \text{Res} & & i \uparrow \quad \circlearrowleft \quad \uparrow \text{trans} \\ A_n & \longrightarrow & \text{Gal}(H_n/F_n) & & A_n \longrightarrow \text{Gal}(H_n/F_n) \end{array}$$

という可換図式が得られる. ここで, 横方向は類体論の相互写像による同型, Res は定義域の制限, trans は移送^{*2}である. 特に, $\{A_n, \text{Nr}\}$ は Γ -加群の射影系であり, $\{A_n, i\}$ は Γ -加群の帰納系である. そこで,

$$A_\infty^\leftarrow = \varprojlim A_n = \varprojlim \text{Gal}(H_n/F_n) = \text{Gal}(H_\infty/F_\infty),$$

$$A_\infty^\rightarrow = \varinjlim A_n$$

とおく. $H_\infty = \cup_n H_n$ は F_∞ の最大不分岐 p -アーベル拡大である. $A_\infty^\leftarrow$ は $\text{pro-}p \Gamma$ 加群であり, 特にコンパクトである. $A_\infty^\rightarrow$ は離散的 Γ 加群となる. これらを調べるのには, 「完備化された Γ の群環 Λ 」を考えるとよい.

2 岩澤代数

Γ を $\mathbb{Z}_p$ に同型な乗法的位相群とし, $u \in \Gamma$ を位相的生成元, つまり $\overline{\langle u \rangle} = \Gamma$ となるものとする. $\Gamma_n = \Gamma/\Gamma^{p^n}$ とおけばこれは位数 p^n の巡回群で $u \bmod \Gamma^{p^n}$ が生成元となる.

$K/\mathbb{Q}_p$ を有限次拡大とし, $\mathfrak{o}$ を K の整数環, π を $\mathfrak{o}$ の素元とする. $\omega_n(T) = (1+T)^{p^n} - 1$ と置くと

$$\mathfrak{o}[\Gamma_n] \simeq \mathfrak{o}[T]/(\omega_n); u \bmod \Gamma^{p^n} \mapsto 1+T \bmod (\omega_n)$$

であるから, 完備群環 $\mathfrak{o}[[\Gamma]] := \varprojlim \mathfrak{o}[\Gamma_n]$ は

$$\begin{aligned} \mathfrak{o}[[\Gamma]] &\simeq \varprojlim \mathfrak{o}[T]/(\omega_n) \\ &= \varprojlim \mathfrak{o}[T]/(\pi, T)^n \quad (\because \omega_n \in (\pi, T)^n) \\ &= \varprojlim \mathfrak{o}[T]/(T^n) \\ &= \mathfrak{o}[[T]] \end{aligned}$$

$\text{rank}_{\mathbb{Z}_p}(\overline{E})$ とおくと, $\text{Gal}(L/F) \simeq \mathbb{Z}_p^{[F:\mathbb{Q}]-r} \oplus (\text{有限 } p \text{ 群})$ と表せる. Dirichlet 単数定理により $\text{rank}_{\mathbb{Z}}(E) = s+t-1$ であった (s は実素点の個数, $2t$ は虚素点の個数) が, r も $s+t-1$ になるだろうというのが Leopoldt 予想である. この予想は F が $\mathbb{Q}$ または虚二次体上のアーベル拡大の場合成立する (Ax-Brumer の定理).

^{*2} 一般に次のようにして定義される: H をアーベル群 G の指数有限の部分群とする. G/H の代表系 $g_1, \dots, g_h$ を選び, $b \in g_i H$ に対し $\bar{b} = g_i$ とする. $x \in G$ に対し

$$\text{trans}(x) = \prod_{i=1}^h g_i x \overline{g_i x}^{-1}$$

とする. これは代表系の選び方によらず定まり, G から H への準同型になっている.

となる. $\Lambda = \mathfrak{o}[[T]]$ を岩澤代数という. これは 2 次元局所環 (極大イデアルは $\mathfrak{m} = (\pi, T)$) であるが, Λ 上の有限生成加群は PID 上の有限生成加群と同様の構造定理が成り立つのでそれを説明する.

補題 2.1 (割り算定理) $f(T) \in T^n \Lambda^\times + \pi \Lambda_n$, $\Lambda_n = \{r(T) \in \mathfrak{o}[T] \mid \deg r < n\}$ とする. このとき任意の $g \in \Lambda$ に対し, ただ 1 つ $q \in \Lambda$ が存在して

$$g \in fq + \Lambda_n$$

となる.

証明. Gauss 記号の類似を定めておく: $a = \sum_{i=-\infty}^{\infty} a_i T^i \in \mathfrak{o}((T))$ に対し $[a] = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$ とする. $u = [T^{-n}f] \in \Lambda^\times$ とすれば, $T^n u - f \in \pi \Lambda_n$ である. $g \in \Lambda$ に対し,

$$g_0 = [T^{-n}g], \quad g_i = [(1 - T^{-n}fu^{-1})g_{i-1}]$$

と帰納的に定めていくと, $g_i \in \pi^i \Lambda$ だから無限和 $g_0 + g_1 + \cdots$ が Λ に存在する. それと u^{-1} の積を q とすれば条件を満たす:

$$fq - g = T^n(g_0 + g_1 + \cdots) - g - (T^n - fu^{-1})(g_0 + g_1 + \cdots) \in \Lambda_n$$

一意性は $0 \neq q \in \Lambda$, $r \in \Lambda_n$ が $fq + r = 0$ を満たすとして矛盾を導けばよい. あらかじめ π のべきで割っておくことにより, q, r のどちらかは π で割れないとして良い. fq の $n-1$ 次までの項は π で割れるので, r は π で割れる. f は π で割れないので, q は π で割れ, これは矛盾である. $\square$

$\sigma(T) \in \mathfrak{o}[T]$ が特殊多項式 (distinguished polynomial) であるとは,

$$\sigma(T) \in T^n + \pi \Lambda_n$$

となることをいう. $\omega_n(T)$ は特殊多項式である.

定理 2.2 (Weierstrass の予備定理) $0 \neq f(T) \in \Lambda$ に対し, 一組の $m \in \mathbb{Z}_{\geq 0}$, 特殊多項式 $\sigma(T)$ が存在して,

$$f \in \pi^m \sigma \Lambda^\times$$

となる.

証明. あらかじめ π のべきで割っておくことにより, $f \in T^n \Lambda^\times + \pi \Lambda_n$ としてよい. 割り算定理で $g = T^n$ とすれば

$$fq = T^n + r \quad (q \in \Lambda, r \in \Lambda_n)$$

とできるが, このとき $T^n + r$ は特殊多項式, $q \in \Lambda^\times$ となる. 一意性も割り算定理の一意性から導かれる. $\square$

Λ -加群の準同型 $h : N \rightarrow M$ に対し, $\text{Ker } h, M/\text{Im } h$ が共に有限であるとき, h は擬同型であるといい, $N \sim M$ と書く. これは対称律が成り立たないので同値関係ではない*3. M, N が torsion Λ 加群なら $M \sim N \implies N \sim M$ である (レポート問題 2).

定理 2.3 (構造定理) M を有限生成 Λ 加群とすると, 一組の $r \in \mathbb{Z}_{\geq 0}, n_i, m_j \in \mathbb{N}$, 既約な特殊多項式 f_j が存在して,

$$M \sim \Lambda^r \oplus \Pi_i \Lambda/(\pi^{n_i}) \oplus \Pi_j \Lambda/(f_j^{m_j})$$

となる. r を M の Λ -rank, $\mu(M) = \sum_i n_i$ を M の μ -不変量, $\text{ch}(M) = \Pi_j f_j^{m_j}$ を M の特性多項式, $\lambda(M) = \deg(\text{ch}(M))$ を M の λ -不変量という.

証明の概略 (Serre).

1. $M \sim \text{tor } M \oplus M/\text{tor } M$.
2. n_i, m_j, f_j が存在して $\text{tor } M \sim \Pi_i \Lambda/(\pi^{n_i}) \oplus \Pi_j \Lambda/(f_j^{m_j})$.
3. Λ 加群 N に対し双対を $N^* = \text{Hom}_\Lambda(N, \Lambda)$ と定める.

N が有限生成で torsion free なら $N \sim N^{**}$ であり, N^{**} は自由である. $\square$

定理 2.4 (漸近公式) M を有限生成 torsion Λ 加群とする (M の Λ -rank は 0). このとき, n と独立な定数 ν があって, 充分大きな n について

$$\#(M/\omega_n M) = p^{\lambda(M)n + \mu(M)p^n + \nu}$$

となる.

3 岩澤加群

Λ はコンパクト, Hausdorff な位相を備えている. コンパクトな Λ 加群で作用が連続なものを岩澤加群という. 有限生成 Λ 加群は自然な位相によりコンパクトである.

F_∞/F を円分 $\mathbb{Z}_p$ 拡大とすれば, $X = A_\infty^-$ は岩澤加群であったが, 実は次が成り立つ:

命題 3.1 X は有限生成 torsion Λ 加群である.

証明には次の補題を使う.

補題 3.2 M を岩澤加群とする. ある $f \in \mathfrak{m}$ が存在して M/fM が有限となるなら M は有限生成 torsion Λ 加群である.

*3 例えば, $\mathfrak{m} \sim \Lambda$ だが $\Lambda \not\sim \mathfrak{m}$ である. h が擬同型であることと, 全ての高さ 1 以下の素イデアル $\mathfrak{p}$ に対し局所化 $h_{\mathfrak{p}} : N_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}}$ が同型となること, は同値である. 推移律はこのことからわかる.

証明. 中山の補題^{*4}により M は有限生成となり構造定理が使えるが, $|\Lambda/(f)| = \infty$ なので Λ 自由部分は現れない. $\square$

p の上の F の素イデアルがただ一つでそれが F_∞ で完全分岐するときは $X/\omega_n X = A_n$ となり命題が示される. 一般には, X の適当な部分加群を取って, ω_n の番号をずらしたりして間接的に命題が示される. $\square$

ここで, 漸近公式を使うと

$$\#A_n = p^{\lambda(X)n + \mu(X)p^n + \nu} \quad (n \gg 0)$$

がわかる^{*5}. 次の様な予想が知られている:

岩澤 μ 予想. $\mu(X) = 0$ である.

これは F が $\mathbb{Q}$ 上のアーベル拡大のときは成立する (Ferrero-Washington の定理).

$F = \mathbb{Q}(\mu_p)$ とする. $\Delta \simeq \text{Gal}(F/\mathbb{Q})$ は X に作用する. Teichmüller 指標を $\omega: \mathbb{F}_p^\times \rightarrow \mathbb{Z}_p^\times$ とし,

$$\varepsilon_i = \frac{1}{p-1} \sum_{a \in \Delta} \omega^{-i}(a) a \in \mathbb{Z}_p[\Delta]$$

と定めると, ε_i はべき等元で

$$X = \bigoplus_{i=0}^{p-2} \varepsilon_i X$$

となる. 一方, 複素共役を ρ とすれば,

$$X = X^+ \oplus X^-, \quad (X^\pm = \{x \in X \mid x^\rho = \pm x\})$$

となり

$$X^+ = \bigoplus_{i: \text{偶数}} \varepsilon_i X, \quad X^- = \bigoplus_{i: \text{奇数}} \varepsilon_i X$$

である.

定理 3.3 (Iwasawa) X^- は Λ -torsion であるが, $\mathbb{Z}_p$ 上自由である.

X^+ については, 次の予想がある:

Vandiver 予想. $X^+ = 0$ である.

^{*4} 中山の補題. 岩澤加群 M に対して

$$\mathfrak{m}M = M \iff M = 0$$

$$M/\mathfrak{m}M \text{ が有限} \iff M \text{ が有限生成}$$

^{*5} F の類数が p で割れず, $F/\mathbb{Q}$ で p は不分解, F_∞/F で分岐素点は完全分岐, という条件が満たされれば $A_n = 0$ である. 例えば $\mathbb{Q}$ は条件を満たす.

この予想は $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ の類数が p で割れない, ということと同値であり, いくつかの p について成立することが確かめられている^{*6}. さらに, Vandiver 予想より弱い次の予想もある:

Greenberg 予想. X^+ は有限である.

4 p 進 L 関数

χ を Dirichlet 指標とし, $k \in \mathbb{Z}$ に対して $\chi_k = \chi\omega^{-k}$ とする.

定理 4.1 (Kubota-Leopoldt) $\chi \neq 1$ のとき, 連続関数 $L_p(s, \chi) : \mathbb{Z}_p \rightarrow \mathbb{Q}_p(\text{Im } \chi)$ で

$$L_p(1-k, \chi) = (1 - \chi_k(p)p^{k-1})L(1-k, \chi_k), \quad (k \in \mathbb{N})$$

を満たすものがある. $\chi(-1) = -1$ なら $L_p(s, \chi) = 0$ である.

定理 4.2 (Iwasawa) $\chi(-1) = 1$ で $\chi = \omega^k$ ($k \neq 0$) ならば, $G_p(\chi, T) \in \mathbb{Z}_p[[T]]$ が存在して,

$$G_p(\chi, u^s - 1) = L_p(s, \chi) \quad (u = 1 + p)$$

となる. このようにベキ級数に $u^s - 1$ を代入して得られる関数を岩澤関数という.

Stickelberger 元と呼ばれる $\theta_n \in \mathbb{Z}_p[\text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})]$ が存在し, $\theta_n A_n = 0$ となる^{*7}. $\{\theta_n\}_n$ の極限として $\mathbb{Z}_p[\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]$ の元を得るが, これを使って p 進 L 関数の存在を明示的に証明することができる.

5 主予想

定理 5.1 (Mazur-Wiles) $3 \leq i \leq p-2$ である奇数 i に対し,

$$\text{ch}(\varepsilon_i X) \in G_p(\omega^{1-i}, T)\Lambda^\times$$

となる.

この式で, 左辺はイデアル類群から決まる代数的, 数論的なもの, 右辺は L 関数の値から決まる p 進解析的なものである. Mazur-Wiles による証明は保型形式を本質的に使うが, Euler 系という概念を使った証明も得られている.

円分 $\mathbb{Z}_p$ 拡大以外の無限次 Galois 拡大で具体的に記述できるものはあるか (レポート問題 3).

^{*6} Buhler, Cradall, Ernvall, Metsänkylä, Shokrollahi, *Irregular primes and cyclotomic invariants to 12 million*, J.Symbolic Comput. **31** (2001), 89-96

^{*7} **Stickelberger の定理.** $G = \text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ とおくと, $\mathbb{Z}[G] \cap \theta \mathbb{Z}[G] \subset \text{ann}(C\ell(\mathbb{Q}(\mu_m)))$ である. ただし

$$\theta = \sum_{1 \leq a < m, (a, m)=1} \frac{a}{m} \cdot \sigma_a^{-1} \in \mathbb{Q}[G] \quad (\sigma_a : \zeta_m \mapsto \zeta_m^a)$$

文献案内

基本的な教科書

S.Lang, *Cyclotomic Fields I and II combined version*, GTM121, Springer-Verlag, 1990.

L.Washington, *Introduction to Cyclotomic fields*, Second Edition, GTM83, Springer-Verlag, 1996.

次の厚い本にも岩澤加群の章と岩澤理論の章がある.

J. Neukirch, A. Schmidt, K. Winberg, *Cohomology of Number Fields*, Springer-Verlag, 2000.

創始者の全集

Kenkichi Iwasawa, *Collected Papers*, Springer-Verlag, 2001.

日本語では, 次の本の 10 章が参考になる.

黒川信重・栗原将人・斎藤毅, 数論 3 (岩澤理論と保型形式), 岩波講座現代数学の基礎, 岩波書店, 1998.

GALOIS 変形理論

山上 敦士 (京産大理)

0. Introduction

本稿の目的は, 有限次代数体 F の代数的閉包 $\bar{F}$ をとり, その絶対 Galois 群 $\text{Gal}(\bar{F}/F)$ の (主に 2 次元の) 表現の変形理論 (deformation theory) について紹介することである.

まず最初に, F を有理数体 $\mathbb{Q}$ として, Galois 表現の deformation の例を見てみることにする.

p を素数とする. $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ を p -進整数環とし, $\mathbb{F}_p := \mathbb{Z}_p/p\mathbb{Z}_p$ をその剰余体とする. このとき, $\mathbb{F}_p$ は標数 p の素体となる. $\mathbb{Q}$ 上の楕円曲線 E に対し, E の p 冪等分点への Galois 作用から生じる Galois 表現

$$\rho_{E,p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_p)$$

を考える. $\rho_{E,p}$ と mod p 写像 $\text{GL}_2(\mathbb{Z}_p) \rightarrow \text{GL}_2(\mathbb{F}_p)$ との合成を

$$\bar{\rho} := \rho_{E,p} \pmod{p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$$

とおく. このとき, $\rho_{E,p}$ は mod p 表現 $\bar{\rho}$ の $\mathbb{Z}_p$ への deformation となっている.

一般に, $\mathbb{F}_p$ を剰余体にもつ局所 pro-artinian $\mathbb{Z}_p$ -algebra A を係数とする Galois 表現

$$\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(A)$$

について, A の極大 ideal $\mathfrak{m}_A$ による剰余写像 $\text{GL}_2(A) \rightarrow \text{GL}_2(\mathbb{F}_p)$ と合成した表現

$$\rho \pmod{\mathfrak{m}_A} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$$

が

$$\rho \pmod{\mathfrak{m}_A} = \bar{\rho}$$

となるとき, ρ は $\bar{\rho}$ の A への deformation であるという.

Galois 表現を用いた整数論の研究においては, 対象となる mod p 表現 $\bar{\rho}$ がもつ様々な数論的性質のうち, どのような性質が $\bar{\rho}$ の deformation たちに引き継がれているのかという, いわば deformation における数論的性質の伝播性なるものが鍵となる.

とくに, 保型形式の岩澤理論などといった保型形式にまつわる研究においては, 対象となる Galois 表現が「保型形式に付随する」という

Date: 2006 年 8 月 31 日, 9 月 1 日発表.

modularity と呼ばれる性質の deformation における伝播性が重要な焦点となる.

その際, $\bar{\rho}$ の無数に存在しうる deformation たちを一つひとつ帰納的に調べ尽くすのではなく, それらを支配する *universal deformation ring* $R_{\bar{\rho}}$ と, $\bar{\rho}$ の $R_{\bar{\rho}}$ への *universal deformation* ρ なるものを構成し, ρ の数論的性質を追究するという演繹的な手法が常套手段である (universal deformation の定義については Section 1 で詳しく述べる).

この手法を用いることで, Wiles [13]-Taylor-Wiles [11] により, Fermat の最終定理が解決されたことは, Galois 表現の deformation theory がいかに整数論の研究において強力なものであるかを示す顕著な例といえる.

本稿では, まず Section 1 において, deformation と universal deformation の定義を与える. そして, universal deformation の具体的な構成に必要な pseudo-representation なるものの定義と性質を Section 2 で紹介し, Section 3 において, 実際に pseudo-representation を用いた universal deformation の構成法を紹介する.

一方, Section 4 では, 先に与えられた deformation たちを用いて, それらだけを支配する universal deformation ring を構成する方法を紹介する.

最後に, Section 5 において, modularity をもつ Galois 表現の具体例を示すという趣旨で, とくに Hilbert cusp form に付随する Galois 表現を紹介する. その中で, Hilbert cusp form に対する Hecke algebra を modular な deformation を支配する universal deformation ring とみなせることが期待できる根拠として, Hilbert cusp form のなす空間とそれに作用する Hecke algebra の間の duality について紹介する.

Acknowledgement. 「整数論札幌夏の学校」での講演の機会を与えていただき出張旅費の援助をしていただいた, 前田芳孝先生はじめ北海道大学のご関係の先生の皆様方, また, 講演内容に関していくつかの suggestion をしていただいた UCLA の肥田晴三先生, そして, この度出張にまつわる様々な手続きに際してお世話になった金子ひろ子さんはじめ北海道大学理学部数学分室事務室の皆様方に, 心より感謝申し上げます.

CONTENTS

0. Introduction	1
1. Definition of deformations	3
2. Pseudo-representations	4
3. Construction of universal couple	9
4. Parametrization of given deformations	20
5. Modular Galois representations	23
5.1. Definition of Hilbert cusp forms	24

5.2. Hecke algebras and duality	28
5.3. Modular Galois representations	33
References	35

1. Definition of deformations

この Section では, [5, Section 2.3] に沿う形で deformation と universal deformation の定義をする.

p を素数とする. K を p -進数体 $\mathbb{Q}_p$ の有限次拡大体とし, $\mathcal{O}$ を K の整数環, $\mathfrak{m}_{\mathcal{O}}$ を $\mathcal{O}$ の極大 ideal とする. $\mathbb{F} := \mathcal{O}/\mathfrak{m}_{\mathcal{O}}$ を $\mathcal{O}$ の剰余体とすると, $\mathbb{F}$ は標数 p の有限体となる.

Definition 1.1. (1) 単位的可換環 A が artin 環のなす射影系の射影的極限として表されるとき, A を *pro-artinian* と呼ぶ.

(2) 群 G が有限群のなす射影系の射影的極限として表されるとき, G を *profinite group* という. profinite group G には, profinite 位相を入れておく.

$\mathbb{F}$ を剰余体にもつ局所 pro-artinian $\mathcal{O}$ -algebra を object とし, $\mathcal{O}$ -algebra 準同型を morphism とする圏を $\mathrm{CL}_{\mathcal{O}}$ とおく. A が $\mathrm{CL}_{\mathcal{O}}$ の object であるとき, $A \in \mathrm{CL}_{\mathcal{O}}$ と書き $\mathfrak{m}_A$ をその極大 ideal とする. $\mathbb{F}$ が有限体であることから, A に profinite 位相を入れることができる. 以下, 扱う表現や準同型は断らない限りすべて, しかるべき位相に関して連続なものとする.

Definition 1.2 ([5, Section 2.3]). n を正の整数とする. G を profinite group とし,

$$\bar{\rho} : G \rightarrow \mathrm{GL}_n(\mathbb{F})$$

を $\mathbb{F}$ -係数の n 次元表現 とする.

(1) $A \in \mathrm{CL}_{\mathcal{O}}$ について, A -係数の n 次元表現

$$\rho : G \rightarrow \mathrm{GL}_n(A)$$

が $\bar{\rho}$ の A への deformation であるとは, $\mathbb{F}$ -係数の表現として,

$$\rho \pmod{\mathfrak{m}_A} = \bar{\rho}$$

であることをいう.

(2) $A \in \mathrm{CL}_{\mathcal{O}}$ への二つの n 次元連続 ρ, ρ' が *equivalent* であるとは, ある $x \in \mathrm{GL}_n(A)$ があって, 任意の $g \in G$ に対して

$$\rho(g) = x\rho'(g)x^{-1}$$

となることであり, このとき $\rho \sim \rho'$ とかく. さらに, x として

$$x \equiv \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \pmod{\mathfrak{m}_A}$$

なるものを選べるとき, *strictly equivalent* であるといい, $\rho \approx \rho'$ とかく. このとき, もし ρ が $\bar{\rho}$ の A への deformation であれば, ρ' も $\bar{\rho}$ の A への deformation となることに注意.

(3) $R \in \text{CL}_{\mathcal{O}}$ と $\bar{\rho}$ の R への deformation

$$\boldsymbol{\rho} : G \rightarrow \text{GL}_n(R)$$

の組 $(R, \boldsymbol{\rho})$ が $\bar{\rho}$ の *universal couple* であるとは, 任意の $\bar{\rho}$ の deformation

$$\rho : G \rightarrow \text{GL}_n(A)$$

に対して, $\mathcal{O}$ -algebra 準同型 $\varphi : R \rightarrow A$ で

$$\varphi \circ \boldsymbol{\rho} \approx \rho$$

となるものがただ一つ存在することをいう. このとき, R を $\bar{\rho}$ に対する *universal deformation ring*, $\boldsymbol{\rho}$ を $\bar{\rho}$ に対する *universal deformation* という. この universality により, もし $\bar{\rho}$ に対する universal couple $(R, \boldsymbol{\rho})$ が存在するならば, 同型の差を除き一意に存在することがわかる. その意味で, $\bar{\rho}$ の universal deformation ring を $R_{\bar{\rho}}$ とかくことがある.

Remark 1.1. Definition 1.2 (1) の意味での “deformation” を “lift” といい, (2) で定義された strict equivalence class を “deformation” と呼ぶことがある.

Theorem 1.1 ([10, Proposition 1]). もし $\bar{\rho}$ が絶対既約, すなわち, 係数を $\mathbb{F}$ の代数的閉包 $\bar{\mathbb{F}}$ まで拡大しても既約性を保つならば, $\bar{\rho}$ に対する universal couple は存在する.

Mazur の原論文 [10] におけるこの存在定理の証明は, $\bar{\rho}$ の deformation からなる $\text{CL}_{\mathcal{O}}$ 上の関手が表現可能であることを証明する抽象的な可換環論を用いたものであるが, 本稿では, とくに Section 3 において, universal couple の具体的な構成法を示したい.

2. Pseudo-representations

ここでは, 次節で紹介する $n = 2$ の場合での universal couple の具体的な構成法に必要な pseudo-representation について, [5, Section 2.2.1] に沿って紹介する.

この Section に限り, G は抽象的な群であり, A は $\mathbb{F}$ を剰余体にもつ局所環であるとする. G の単位元を 1_G , A の極大 ideal を $\mathfrak{m}_A$ とか

く. さらに, G は位数 2 の元 c をもつとして, $\text{char}(\mathbb{F})$ は 2 でないと仮定する.

$$\rho : G \rightarrow \text{GL}_2(A)$$

を, c に関して odd, すなわち $\det \rho(c) = -1$ を満たす A -係数の 2 次元表現とする. ρ の表現空間を $V = V(\rho) := A^2$ とおく. また, $\text{mod } \mathfrak{m}_A$ 表現

$$\bar{\rho} := \rho \pmod{\mathfrak{m}_A} : G \rightarrow \text{GL}_2(\mathbb{F})$$

の表現空間を $\bar{V} = V(\bar{\rho}) := \mathbb{F}^2$ とおく.

$2 \in A^\times$ だから, c に対する V の固有空間分解

$$V = \frac{1-c}{2}V \oplus \frac{1+c}{2}V$$

が生じる. 同様に $2 \in \mathbb{F}^\times$ だから, c に対する $\bar{V}$ の固有空間分解

$$\bar{V} = \frac{1-c}{2}\bar{V} \oplus \frac{1+c}{2}\bar{V}$$

も生じる. ここで, $V_\pm := \frac{1 \pm c}{2}V$, $\bar{V}_\pm := \frac{1 \pm c}{2}\bar{V}$ (以下, $\pm$ は複号同順) とおくと,

$$\bar{V}_\pm = V_\pm / \mathfrak{m}_A V_\pm$$

を得る. $\det \rho(c) = -1$ だから $\dim_{\mathbb{F}} \bar{V}_\pm = 1$ であり, ある $\bar{v}_\pm \in \bar{V}_\pm$ が存在して, $\bar{V}_\pm = \mathbb{F}\bar{v}_\pm$ となる. $v_\pm \in V_\pm$ として $v_\pm \pmod{\mathfrak{m}_A} = \bar{v}_\pm$ なるものをとると, A -module 準同型

$$A \rightarrow V_\pm, \quad a \mapsto av_\pm$$

は A -同型となるので, A -module としての分解

$$V = Av_- \oplus Av_+$$

を得る. この分解のもとで, $\sigma \in G$ に対する $\rho(\sigma)$ の A -係数の表現行列を

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

とかくことにする. このとき,

$$\rho(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

となることに注意. ここで,

$$x : G \times G \rightarrow A, \quad (r, s) \mapsto b(r)c(s)$$

とおくと, 次の三つの条件が成立することがわかる:

$$\begin{aligned}
 (W1) \quad & a(rs) = a(r)a(s) + x(r, s), \quad d(rs) = d(r)d(s) + x(s, r), \\
 & x(rs, tu) = a(r)a(u)x(s, t) + a(u)d(s)x(r, t) \\
 & \quad + a(r)d(t)x(s, u) + d(s)d(t)x(r, u); \\
 (W2) \quad & a(1_G) = d(1_G) = d(c) = 1, \quad a(c) = -1, \\
 & x(r, s) = x(s, t) = 0 \quad (\text{if } s = 1_G \text{ or } s = c); \\
 (W3) \quad & x(r, s)x(t, u) = x(r, u)x(t, s).
 \end{aligned}$$

Definition 2.1 ([5, Section 2.2.1]). A を $\mathbb{F}$ を剰余体にもつ局所環とし, G を群, $c \in G$ を位数 2 の元とする. $\text{char}(\mathbb{F})$ は 2 と相異なるものとする. このとき,

(1) 写像たち

$$a : G \rightarrow A, \quad d : G \rightarrow A, \quad x : G \times G \rightarrow A$$

が上の三つの条件 (W1)-(W3) を満たすとき, 組 $\tau = \{a, d, x\}$ を (G, c) の A への *pseudo-representation* という.

(2) 写像たち

$$\begin{aligned}
 \text{Tr}(\tau) : G &\rightarrow A, \quad r \mapsto a(r) + d(r), \\
 \det(\tau) : G &\rightarrow A, \quad r \mapsto a(r)d(r) - x(r, r)
 \end{aligned}$$

をそれぞれ, τ の *trace*, *determinant* とよぶ.

Remark 2.1. (1) $2 \in A^\times$ だから,

$$\begin{aligned}
 a(r) &= \frac{1}{2}(\text{Tr}(\tau)(r) - \text{Tr}(\tau)(rc)), \quad d(r) = \frac{1}{2}(\text{Tr}(\tau)(r) + \text{Tr}(\tau)(rc)), \\
 x(r, s) &= a(rs) - a(r)a(s)
 \end{aligned}$$

となり, $\tau = \{a, d, x\}$ は $\text{Tr}(\tau)$ の値で決まることがわかる.

(2) $\det(\tau)$ は $A^\times$ に値をもつ G 上の群準同型である.

上で見たように, 2 次元表現 ρ から自然に pseudo-representation が構成できる (これを τ_ρ とかくことにする). このとき,

$$\text{Tr}(\rho) = \text{Tr}(\tau_\rho)$$

となることに注意. 逆に, pseudo-representation から trace が一致する 2 次元表現を構成することができる:

Proposition 2.1 (Wiles [12] (cf. [5, Proposition 2.16])). A を $\mathbb{F}$ を剰余体にもつ局所環とし, G を群, $c \in G$ を位数 2 の元とする. $\text{char}(\mathbb{F})$ は 2 と相異なるものとする. $\tau = \{a, d, x\}$ を A への (G, c) の pseudo-representation として, 次の二つの条件のうち, どちらか一方は満たされていると仮定する:

(i) 任意の $r, s \in G$ に対して $x(r, s) = 0$ である;

(ii) ある $(r, s) \in G \times G$ が存在して $x(r, s) \in A^\times$ となる.
このとき, ある A -係数の 2 次元表現

$$\rho : G \rightarrow \mathrm{GL}_2(A)$$

で, 次の等式を満たすものが存在する:

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(\tau), \quad \det(\rho) = \det(\tau), \quad \rho(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

もし, A と G が位相的であり a, d, x が連続写像であるときは, 上の ρ として連続な表現を得ることができる.

Proof. (i) 任意の $r, s \in G$ に対して $x(r, s) = 0$ であるとき: (W1) により

$$a(rs) = a(r)a(s), \quad d(rs) = d(r)d(s)$$

であり, (W2) により

$$a(1_G) = 1, \quad d(1_G) = 1$$

となるので, a と d は $A^\times$ に値をもつ G 上の群準同型である. よって,

$$\rho : G \rightarrow \mathrm{GL}_2(A), \quad g \mapsto \begin{pmatrix} a(g) & 0 \\ 0 & d(g) \end{pmatrix}$$

と定義すれば, ρ は 2 次元表現であり (W2) により

$$\rho(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

となる. さらに, $g \in G$ に対し $x(g, g) = 0$ であることから,

$$\begin{aligned} \mathrm{Tr}(\rho)(g) &= a(g) + d(g) = \mathrm{Tr}(\tau)(g), \\ \det(\rho)(g) &= a(g)d(g) = \det(\tau)(g) \end{aligned}$$

を得る.

(ii) ある $(r, s) \in G \times G$ が存在して $x(r, s) \in A^\times$ となるとき: $g, h \in G$ を任意の元とする.

$$b(g) := \frac{x(g, s)}{x(r, s)}, \quad c(h) := x(r, h)$$

とおけば (W3) により,

$$b(g)c(h) = \frac{x(g, s)x(r, h)}{x(r, s)} = \frac{x(r, s)x(g, h)}{x(r, s)} = x(g, h)$$

となる. ここで,

$$\rho(g) := \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$$

とおくと (W2) により,

$$\rho(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(1_G) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

となる. さらに,

$$\rho(g)\rho(h) = \begin{pmatrix} a(g)a(h) + b(g)c(h) & a(g)b(h) + b(g)d(h) \\ c(g)a(h) + d(g)c(h) & d(g)d(h) + c(g)b(h) \end{pmatrix}$$

において (W1) により,

$$\begin{aligned} a(g)a(h) + b(g)c(h) &= a(g)a(h) + x(g, h) = a(gh), \\ d(g)d(h) + c(g)b(h) &= d(g)d(h) + x(h, g) = d(gh), \\ c(g)a(h) + d(g)c(h) &= x(r, g)a(h) + d(g)x(r, h) \\ &= a(1_G)a(h)x(r, g) + a(1_G)d(g)x(r, h) \\ &= x(r, gh) = c(gh), \\ a(g)b(h) + b(g)d(h) &= x(r, s)^{-1}(a(g)b(h)x(r, s) + b(g)d(h)x(r, s)) \\ &= x(r, s)^{-1}(a(g)d(1_G)x(h, s) + d(h)d(1_G)x(g, h)) \\ &= x(r, s)^{-1}x(gh, s) = b(gh) \end{aligned}$$

となるので,

$$\rho(gh) = \rho(g)\rho(h)$$

であることがわかる. よって,

$$\rho : G \rightarrow \mathrm{GL}_2(A)$$

は表現であり,

$$\begin{aligned} \mathrm{Tr}(\rho)(g) &= a(g) + d(g) = \mathrm{Tr}(\tau)(g), \\ \det(\rho)(g) &= a(g)d(g) - b(g)c(g) = a(g)d(g) - x(g, g) = \det(\tau)(g) \end{aligned}$$

となる. さらに, G と A が位相的であるとき, a, d, x が連続ならば ρ も連続となることは構成法からわかる. $\square$

Remark 2.2. 2次元表現 $\rho : G \rightarrow \mathrm{GL}_2(A)$ が先に与えられて, ρ から構成される pseudo-representation τ_ρ が Proposition 2.1 の条件 (i) と (ii) のいずれか一方を満たすとき, Proposition 2.1 により新たに 2次元表現 $\rho' : G \rightarrow \mathrm{GL}_2(A)$ が構成される. これら二つの表現 ρ と ρ' の関係については次節で考察する.

3. Construction of universal couple

以下, Section 1 の記号を用いることにする. G を位数 2 の元 c をもつ profinite group, $A \in \text{CL}_\mathcal{O}$ とし, $\text{char}(\mathbb{F})$ は 2 と相異なるものとする. この Section では [5, Section 2.3.2] と [8, Section 1.1.4] に沿う形で, $\mathbb{F}$ -係数の 2 次元表現

$$\bar{\rho} : G \rightarrow \text{GL}_2(\mathbb{F})$$

に対する universal couple を pseudo-representation の理論を用いて構成したい.

この構成に用いられる手法は, 抽象的な存在定理である Theorem 1.1 の仮定に加えて, さらにいくつか条件が課されるものではあるが, Section 5.3 で紹介する Hecke 環を係数とした modular な Galois 表現を構成する際には, 非常に有用なものである.

以下, 次の二つの条件を仮定する:

- (i) $\bar{\rho}$ は絶対既約, すなわち, 係数を $\mathbb{F}$ の代数的閉包 $\bar{\mathbb{F}}$ まで拡大しても既約性が保たれる;
- (ii) $\bar{\rho}$ は c に関して odd, すなわち, $\det \rho(c) = -1$ である.

Lemma 3.1 ([5, (2.8) and (2.13)]). 上記の記号のもと, 次の二つの全単射が得られる:

- (1) $\{\rho : G \rightarrow \text{GL}_2(A) : \text{表現} \mid \rho \pmod{\mathfrak{m}_A} = \bar{\rho}\} / \approx$
 $\xrightarrow{\sim} \{\rho : G \rightarrow \text{GL}_2(A) : \text{表現} \mid \rho \pmod{\mathfrak{m}_A} \sim \bar{\rho}\} / \sim, [\rho]_{\approx} \mapsto [\rho]_{\sim}$
- (2) $\{\rho : G \rightarrow \text{GL}_2(A) : \text{表現} \mid \rho \pmod{\mathfrak{m}_A} \sim \bar{\rho}\} / \sim$
 $\xrightarrow{\sim} \{\tau : A \text{ への } (G, c) \text{ の pseudo-representation} \mid$
 $\tau \pmod{\mathfrak{m}_A} = \tau_{\bar{\rho}}\}, [\rho]_{\sim} \mapsto \tau_{\rho}.$

Remark 3.1. (1) Lemma 3.1 (1) の全単射性は, G を抽象的な群, A を単に $\mathbb{F}$ を剰余体にもつ局所環とした弱い仮定のもとでも成立する.

(2) Lemma 3.1 (1) により, $\bar{\rho}$ が絶対既約のときには, Lemma 3.1 (1) の右辺を deformation の定義に採用できる.

(3) Lemma 3.1 (2) の全単射性は, G を抽象的な群とした弱い仮定のもとでも成立する.

Proof. (1) もし $\rho \pmod{\mathfrak{m}_A} = \bar{\rho}$ であれば, 当然 $\rho \pmod{\mathfrak{m}_A} \sim \bar{\rho}$ であり, その一方で, もし $\rho \approx \rho'$ であれば, 明らかに $\rho \sim \rho'$ であるので, 写像 $[\rho]_{\approx} \mapsto [\rho]_{\sim}$ は well-defined である.

全射性: $[\rho]_{\sim}$ を右辺から取れば, ある $\bar{x} \in \text{GL}_2(\mathbb{F})$ が存在し,

$$\bar{x} \cdot \rho \pmod{\mathfrak{m}_A} \cdot \bar{x}^{-1} = \bar{\rho}$$

となる. $\text{mod } \mathfrak{m}_A$ 写像 $\text{GL}_2(A) \rightarrow \text{GL}_2(\mathbb{F})$ は全射なので, $\bar{x}$ の持ち上げ $x \in \text{GL}_2(A)$ が存在し,

$$\rho' := x\rho x^{-1} : G \rightarrow \text{GL}_2(A)$$

とおけば

$$\rho' \pmod{\mathfrak{m}_A} = \bar{\rho}$$

となり,

$$[\rho']_{\sim} = [\rho]_{\sim}$$

なので, 全射性が示された.

単射性: 二つの表現 ρ と ρ' が,

$$\rho \pmod{\mathfrak{m}_A} = \bar{\rho} = \rho' \pmod{\mathfrak{m}_A}, \quad \rho \sim \rho'$$

を満たすと仮定する. ある $x \in \mathrm{GL}_2(A)$ が存在して,

$$x\rho x^{-1} = \rho'$$

となるので, $\bar{x} := x \pmod{\mathfrak{m}_A} \in \mathrm{GL}_2(\mathbb{F})$ とおき, 両辺を $\pmod{\mathfrak{m}_A}$ すると,

$$\bar{x}\bar{\rho}\bar{x}^{-1} = \bar{\rho}$$

を得る. $\bar{\rho}$ は絶対既約なので, Schur の補題 (cf. [5, Proposition 2.5(2)])

により, ある $\bar{a} \in \mathbb{F}^\times$ が存在して $\bar{x} = \begin{pmatrix} \bar{a} & 0 \\ 0 & \bar{a} \end{pmatrix}$ とかける. $\bar{a}$ の持ち上げ $a \in A^\times$ を取ると,

$$(a^{-1}x) \pmod{\mathfrak{m}_A} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

であり, かつ

$$(a^{-1}x)\rho(a^{-1}x)^{-1} = \rho'$$

となるので,

$$\rho \approx \rho'$$

であることがわかり, 単射性が示された.

(2) もし $\rho \sim \rho'$ であれば $\mathrm{Tr}(\rho) = \mathrm{Tr}(\rho')$ であり, $\mathrm{char}(\mathbb{F})$ は 2 と相異なると仮定しているから, Remark 2.1 (1) により $\tau_\rho = \tau_{\rho'}$ となる. したがって, 写像 $[\rho]_{\sim} \mapsto \tau_\rho$ は well-defined である.

この写像の全単射性を証明するために, Carayol [1] による次の定理を証明を省略して認めることにする:

Theorem 3.2 ([1, Théorème 1] (cf. [8, Proposition 1.25])). G を群, A を $\mathbb{F}$ を剰余体にもつ完備な局所環, n と n' を正の整数とする. 二つの表現

$$\rho : G \rightarrow \mathrm{GL}_n(A), \quad \rho' : G \rightarrow \mathrm{GL}_{n'}(A)$$

について, もし $\bar{\rho} := \rho \pmod{\mathfrak{m}_A}$ が絶対既約であり $\mathrm{Tr}(\rho) = \mathrm{Tr}(\rho')$ であるならば, $n = n'$ かつ

$$\rho \sim \rho'$$

である.

全射性: (G, c) の A への pseudo-representation $\tau = \{a, d, x\}$ が

$$\tau \pmod{\mathfrak{m}_A} = \tau_{\bar{\rho}}$$

を満たすとする. Section 2 の前半と同様に, $\bar{\rho}$ の表現空間の c に関する固有空間分解に沿った $\bar{\rho}$ の表現行列を

$$\bar{\rho}(g) = \begin{pmatrix} \bar{a}(g) & \bar{b}(g) \\ \bar{c}(g) & \bar{d}(g) \end{pmatrix} \quad (g \in G)$$

とかき

$$\bar{x}(g, h) := \bar{b}(g)\bar{c}(h) \quad (g, h \in G)$$

とおけば, $\tau_{\bar{\rho}} = \{\bar{a}, \bar{d}, \bar{x}\}$ となる. $\bar{\rho}$ は絶対既約だから, ある $r, s \in G$ が存在して $\bar{b}(r), \bar{c}(s) \in \mathbb{F}^\times$ となり $\bar{x}(r, s) \in \mathbb{F}^\times$ である. このとき, $x \pmod{\mathfrak{m}_A} = \bar{x}$ なので,

$$x(r, s) \in A^\times$$

であることがわかる. したがって, Proposition 2.1 により, ある 2 次元表現

$$\rho : G \rightarrow \mathrm{GL}_2(A)$$

で

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(\tau)$$

を満たすものが存在する. このとき,

$$\begin{aligned} \mathrm{Tr}(\rho \pmod{\mathfrak{m}_A}) &= \mathrm{Tr}(\rho) \pmod{\mathfrak{m}_A} = \mathrm{Tr}(\tau) \pmod{\mathfrak{m}_A} \\ &= \mathrm{Tr}(\tau \pmod{\mathfrak{m}_A}) = \mathrm{Tr}(\tau_{\bar{\rho}}) = \mathrm{Tr}(\bar{\rho}) \end{aligned}$$

となるので, Theorem 3.2 により

$$\rho \pmod{\mathfrak{m}_A} \sim \bar{\rho}$$

が得られるので, 全射性は示された.

単射性: 二つの表現 ρ と ρ' が

$$\rho \pmod{\mathfrak{m}_A} \sim \bar{\rho} \sim \rho' \pmod{\mathfrak{m}_A}, \quad \tau_\rho = \tau_{\rho'}$$

を満たすとする. このとき,

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(\tau_\rho) = \mathrm{Tr}(\tau_{\rho'}) = \mathrm{Tr}(\rho')$$

となり, $\bar{\rho}$ が絶対既約なので $\rho \pmod{\mathfrak{m}_A}$ も絶対既約となるから, Theorem 3.2 により,

$$\rho \sim \rho'$$

となる. よって, 単射性が示された. □

Definition 3.1 ([8, Section 1.1.4]). 群 G , 局所環 A , 表現 $\bar{\rho} : G \rightarrow \mathrm{GL}_2(\mathbb{F})$ は Lemma 3.1 のものとする. $\bar{\rho}$ から構成される pseudo-representation を $\tau_{\bar{\rho}} = \{\bar{a}, \bar{d}, \bar{x}\}$ とおく. このとき, $R_{\tau_{\bar{\rho}}} \in \mathrm{CL}_{\mathcal{O}}$ と $R_{\tau_{\bar{\rho}}}$ への (G, c) の pseudo-representation $T = \{A, D, X\}$ の組 $(R_{\tau_{\bar{\rho}}}, T)$ が $\tau_{\bar{\rho}}$ に対する *universal couple* であるとは, 任意の (G, c) の $A \in \mathrm{CL}_{\mathcal{O}}$ への pseudo-representation τ で

$$\tau \pmod{\mathfrak{m}_A} = \tau_{\bar{\rho}}$$

を満たすものに対し, $\mathcal{O}$ -algebra 準同型 $\varphi_{\tau} : R_{\tau_{\bar{\rho}}} \rightarrow A$ で

$$\tau = \varphi_{\tau} \circ T$$

を満たすものがただ一つ存在することである. このとき, T を $\tau_{\bar{\rho}}$ に対する *universal pseudo-representation* という.

Theorem 3.3 ([8, Theorem 1.26]). G を位数 2 の元 c をもつ profinite group, $A \in \mathrm{CL}_{\mathcal{O}}$ とし, $\mathrm{char}(\mathbb{F})$ は 2 と相異なるものとする. $\mathbb{F}$ -係数の 2 次元表現

$$\bar{\rho} : G \rightarrow \mathrm{GL}_2(\mathbb{F})$$

は絶対既約であり, $\det \bar{\rho}(c) = -1$ を満たすとする.

このとき, $\bar{\rho}$ に対する universal couple $(R_{\bar{\rho}}, \rho)$ が存在し, さらに ρ から構成される pseudo-representation τ_{ρ} は, $\bar{\rho}$ から得られる pseudo-representation $\tau_{\bar{\rho}}$ の universal pseudo-representation となる.

Remark 3.2. Mazur [10] による universal deformation は, 完備な Noether 局所環のなす圏で論じられているため, profinite group G として “ p -finiteness condition” を満たすものを扱っていることに注意.

Proof. (1) まず $\tau_{\bar{\rho}}$ の universal pseudo-representation $(R_{\tau_{\bar{\rho}}}, T)$ を構成する. $\tau_{\bar{\rho}} = \{\bar{a}, \bar{d}, \bar{x}\}$ とおく.

(i) G が有限群であるとき: $\mathbb{F}$ の元の個数を q とし, $\mathcal{O}^{\times}$ 内の 1 の $q-1$ 乗根全体のなす部分群を $\mu_{q-1}(\mathcal{O})$ とおくと, $\mathrm{mod} \mathfrak{m}_{\mathcal{O}}$ 写像 $\mathcal{O}^{\times} \rightarrow \mathbb{F}^{\times}$ は有限群の同型

$$\mathrm{mod} \mathfrak{m}_{\mathcal{O}} : \mu_{q-1}(\mathcal{O}) \xrightarrow{\sim} \mathbb{F}^{\times}$$

を誘導する. この逆写像を

$$\varphi : \mathbb{F}^{\times} \xrightarrow{\sim} \mu_{q-1}(\mathcal{O})$$

とかき, $\varphi(0) := 0$ とすることで, $\mathbb{F}$ 上の写像

$$\varphi : \mathbb{F} \rightarrow \mu_{q-1}(\mathcal{O}) \cup \{0\}$$

に延長しておく. $\mathcal{O}$ -係数の形式的冪級数環

$$\Lambda = \Lambda_G := \mathcal{O}[[A_g, D_h, X_{(g,h)} \mid g, h \in G]]$$

を考える. $g, h \in G$ に対して, Λ の元

$$\begin{aligned} A(g) &:= A_g + \varphi(\bar{a}(g)), \\ D(g) &:= D_g + \varphi(\bar{d}(g)), \\ X(g, h) &:= X_{(g, h)} + \varphi(\bar{x}(g, h)) \end{aligned}$$

を定義し, Λ の ideal I を次の元たちで生成されるものとする: r, s, t, u を G の元として,

$$\begin{aligned} \text{(w1)} \quad & A(rs) - (A(r)A(s) + X(r, s)), \quad D(rs) - (D(r)D(s) + X(s, r)), \\ & X(rs, tu) - (A(r)A(u)X(s, t) + A(u)D(s)X(r, t) \\ & \quad + A(r)D(t)X(s, u) + D(s)D(t)X(r, u)); \\ \text{(w2)} \quad & A(1_G) - 1 (= A_{1_G}), \quad D(1_G) - 1 (= D_{1_G}), \\ & D(c) - 1 (= D_c), \quad A(c) + 1 (= A_c), \\ & X(r, s), \quad X(s, t) \quad (\text{if } s = 1_G \text{ or } s = c); \\ \text{(w3)} \quad & X(r, s)X(t, u) - X(r, u)X(t, s). \end{aligned}$$

このとき, 商環 $R_{\tau_{\bar{\rho}}} := \Lambda/I$ は $\text{CL}_{\mathcal{O}}$ の object となり, 関係式 (w1)-(w3) により, 三つの写像

$$\begin{aligned} A : G &\rightarrow R_{\tau_{\bar{\rho}}}, \quad g \mapsto A(g) \pmod{I}, \\ D : G &\rightarrow R_{\tau_{\bar{\rho}}}, \quad h \mapsto D(h) \pmod{I}, \\ X : G \times G &\rightarrow R_{\tau_{\bar{\rho}}}, \quad (g, h) \mapsto X(g, h) \pmod{I} \end{aligned}$$

が (G, c) の $R_{\tau_{\bar{\rho}}}$ への pseudo-representation $T = \{A, D, X\}$ を定めることがわかる. $\mathbb{F}^\times$ において,

$$\begin{aligned} (A(g) \pmod{I}) \pmod{\mathfrak{m}_{R_{\tau_{\bar{\rho}}}}} &= \bar{a}(g), \\ (D(h) \pmod{I}) \pmod{\mathfrak{m}_{R_{\tau_{\bar{\rho}}}}} &= \bar{d}(h), \\ (X(g, h) \pmod{I}) \pmod{\mathfrak{m}_{R_{\tau_{\bar{\rho}}}}} &= \bar{x}(g, h) \end{aligned}$$

であるから,

$$T \pmod{\mathfrak{m}_{R_{\tau_{\bar{\rho}}}}} = \tau_{\bar{\rho}}$$

となる. 任意の (G, c) の $B \in \text{CL}_{\mathcal{O}}$ への pseudo-representation $\tau = \{a, d, x\}$ で

$$\tau \pmod{\mathfrak{m}_B} = \tau_{\bar{\rho}}$$

なるものに対し, B において $g, h \in G$ に対し,

$$\begin{aligned} a(g) - \varphi(\bar{a}(g)) &\in \mathfrak{m}_B, \\ d(h) - \varphi(\bar{d}(h)) &\in \mathfrak{m}_B, \\ x(g, h) - \varphi(\bar{x}(g, h)) &\in \mathfrak{m}_B \end{aligned}$$

なので, $\mathcal{O}$ -algebra 準同型

$$\begin{aligned}\varphi_\tau : \Lambda &\rightarrow B, & A_g &\mapsto a(g) - \varphi(\bar{a}(g)), \\ & & D_h &\mapsto d(h) - \varphi(\bar{d}(h)), \\ & & X_{(g,h)} &\mapsto x(g, h) - \varphi(\bar{x}(g, h))\end{aligned}$$

が定まる. さらに, τ が pseudo-representation の性質 (W1)-(W3) を満たすことから,

$$\varphi_\tau(I) = 0$$

となることがわかるので, φ_τ は $R_{\tau_{\bar{\rho}}}$ を経由する:

$$\varphi_\tau : R_{\tau_{\bar{\rho}}} \rightarrow B.$$

また, $g, h \in G$ に対し,

$$\begin{aligned}\varphi_\tau(A(g)) &= a(g), \\ \varphi_\tau(D(h)) &= d(h), \\ \varphi_\tau(X(g, h)) &= x(g, h)\end{aligned}$$

となるので,

$$\varphi_\tau \circ T = \tau$$

である. 他に, $\mathcal{O}$ -algebra 準同型

$$\varphi'_\tau : R_{\tau_{\bar{\rho}}} \rightarrow B$$

で

$$\varphi'_\tau \circ T = \tau$$

なるものがあれば, $R_{\tau_{\bar{\rho}}}$ の $\mathcal{O}$ 上の生成系である

$$A_g \pmod{I}, D_h \pmod{I}, X_{(g,h)} \pmod{I}$$

たちに対して,

$$\begin{aligned}\varphi'_\tau(A_g) &= a(g) - \varphi(\bar{a}(g)) = \varphi_\tau(A_g), \\ \varphi'_\tau(D_h) &= d(h) - \varphi(\bar{d}(h)) = \varphi_\tau(D_h), \\ \varphi'_\tau(X_{(g,h)}) &= x(g, h) - \varphi(\bar{x}(g, h)) = \varphi_\tau(X_{(g,h)})\end{aligned}$$

であるので,

$$\varphi'_\tau = \varphi_\tau$$

となる. よって, $(R_{\tau_{\bar{\rho}}}, T)$ は $\tau_{\bar{\rho}}$ に対する universal couple である.

(ii) G が profinite group であるとき: G の指数有限な開正規部分群からなる集合 $\mathcal{N}$ をうまく選ぶことで,

$$G = \varprojlim_{N \in \mathcal{N}} G/N$$

とみなせる. $\bar{\rho}$ は連続なので, $\text{Ker}(\bar{\rho})$ は G の指数有限な開正規部分群であり, $\bar{\rho}$ は $G/\text{Ker}(\bar{\rho})$ を経由することから, $N \in \mathcal{N}$ に対し $N \cap \text{Ker}(\bar{\rho})$

を考えることで, G の表現 $\bar{\rho}$ を扱う際には $\mathcal{N}$ の元はすべて $\text{Ker}(\bar{\rho})$ の部分群であると仮定してよい. このとき, $\det(\bar{\rho}(c)) = -1$ であるため, 各 G/N において cN は位数 2 の元であることに注意.

任意の $N \in \mathcal{N}$ に対して $\bar{\rho}$ は G/N を経由するので, $\text{Tr}(\bar{\rho}) = \text{Tr}(\tau_{\bar{\rho}})$ を有限群 G/N 上の trace とみなせる. $\text{char}(\mathbb{F})$ は 2 と相異なるので, Remark 2.1 (1) により, $\tau_{\bar{\rho}}$ を G/N 上の pseudo-representation とみなすことができる.

(i) により, G/N の pseudo-representation $\tau_{\bar{\rho}}$ の universal couple $(R_{\tau_{\bar{\rho}}}^N, T_N = \{A_N, D_N, X_N\})$ が構成される. $\mathcal{N}$ において $N \subset N'$ のとき, 全射な $\mathcal{O}$ -algebra 準同型

$$\begin{aligned} \pi_{N,N'} : \Lambda_{G/N} &\rightarrow \Lambda_{G/N'}, & A_{gN} &\mapsto A_{gN'}, \\ & & D_{hN} &\mapsto D_{hN'}, \\ & & X_{(gN,hN)} &\mapsto X_{(gN',hN')} \end{aligned}$$

により, 全射な $\mathcal{O}$ -algebra 準同型

$$\pi_{N,N'} : R_{\tau_{\bar{\rho}}}^N \rightarrow R_{\tau_{\bar{\rho}}}^{N'}$$

が誘導され,

$$\pi_{N,N'} \circ T_N = T_{N'}$$

を満たす. このとき,

$$R_{\tau_{\bar{\rho}}} := \varprojlim_{N \in \mathcal{N}} R_{\tau_{\bar{\rho}}}^N$$

とおけば, $R_{\tau_{\bar{\rho}}}$ は $\text{CL}_{\mathcal{O}}$ の object であり, pseudo-representation の性質 (W1)-(W3) は $N \in \mathcal{N}$ に関して射影極限を取る操作と可換であるから, A_N, D_N, X_N ごとに射影極限を取ることで, (G, c) の $R_{\tau_{\bar{\rho}}}$ への pseudo-representation

$$\begin{aligned} T &= \{A, D, X\} \\ &:= \varprojlim_{N \in \mathcal{N}} T_N = \{\varprojlim_{N \in \mathcal{N}} A_N, \varprojlim_{N \in \mathcal{N}} D_N, \varprojlim_{N \in \mathcal{N}} X_N\} \end{aligned}$$

が得られ,

$$T \pmod{\mathfrak{m}_{R_{\tau_{\bar{\rho}}}}} = \tau_{\bar{\rho}}$$

が成立する. 任意の (G, c) の $B \in \text{CL}_{\mathcal{O}}$ への pseudo-representation $\tau = \{a, d, x\}$ で

$$\tau \pmod{\mathfrak{m}_B} = \tau_{\bar{\rho}}$$

なるものに対し, $\bar{\rho}$ は絶対既約であるから Proposition 2.1 により, B -係数の 2 次元表現

$$\rho : G \rightarrow \text{GL}_2(B)$$

で,

$$\text{Tr}(\rho) = \text{Tr}(\tau)$$

を満たすものが構成される.

(ii-1) B が artinian のとき: 剰余体 $\mathbb{F}$ が有限体であるため, B は有限環となる. したがって $\mathrm{GL}_2(B)$ は有限群であり, ρ は連続だから, $\mathrm{Ker}(\rho)$ は G の指数有限な開正規部分群となる. よって, ある $N \in \mathcal{N}$ で ρ が G/N を経由するものが存在し τ を G/N の pseudo-representation とみなせると仮定してよい. このとき, $(R_{\tau_{\bar{\rho}}}^N, T_N)$ の universality により, ある $\mathcal{O}$ -algebra 準同型

$$\varphi_{\tau}^N : R_{\tau_{\bar{\rho}}}^N \rightarrow B$$

で,

$$\varphi_{\tau}^N \circ T_N = \tau$$

なるものがただ一つ存在する. 自然な $\mathcal{O}$ -algebra 全射準同型

$$\pi_N : R_{\tau_{\bar{\rho}}} \rightarrow R_{\tau_{\bar{\rho}}}^N$$

との合成写像を

$$\varphi_{\tau} := \varphi_{\tau}^N \circ \pi_N : R_{\tau_{\bar{\rho}}} \rightarrow B$$

とおくと,

$$\varphi_{\tau} \circ T = \tau$$

が成立する. さらに, 他に $\mathcal{O}$ -algebra 準同型

$$\varphi'_{\tau} : R_{\tau} \rightarrow B$$

で

$$\varphi'_{\tau} \circ T = \tau$$

なるものが存在すれば, $R_{\tau_{\bar{\rho}}}^N$ の $\mathcal{O}$ 上の生成系である $A_{gN}, D_{hN} \cdot X_{(gN, hN)}$ たちは $N \in \mathcal{N}$ に関して射影極限を取ったとき, $R_{\tau_{\bar{\rho}}}$ の $\mathcal{O}$ 上の位相的生成系をなすので, $R_{\tau_{\bar{\rho}}}$ 上で

$$\varphi'_{\tau} = \varphi_{\tau}$$

を得る. よって, $(R_{\tau_{\bar{\rho}}}, T)$ は $\tau_{\bar{\rho}}$ の universal couple である.

(ii-2) B が pro-artinian のとき: B の開 ideal のなす集合 $\mathcal{A}$ をうまく選ぶことで, 任意の $\mathfrak{a} \in \mathcal{A}$ に対し $B/\mathfrak{a}$ は artinian であり, かつ

$$B = \varprojlim_{\mathfrak{a} \in \mathcal{A}} B/\mathfrak{a}$$

とみなせると仮定してよい. $\mathfrak{a} \in \mathcal{A}$ に対し, B -係数の表現である ρ と $\mathrm{mod} \mathfrak{a}$ 写像との合成を

$$\rho_{\mathfrak{a}} := \rho \pmod{\mathfrak{a}} : G \rightarrow \mathrm{GL}_2(B/\mathfrak{a})$$

とおくと, $\rho_{\mathfrak{a}}$ は連続であり $\mathrm{GL}_2(B/\mathfrak{a})$ は有限群であるから, ある $N(\mathfrak{a}) \in \mathcal{N}$ で $N(\mathfrak{a}) \subset \mathrm{Ker}(\rho_{\mathfrak{a}})$ となるものが存在すると仮定してよい. このとき, $\rho_{\mathfrak{a}}$ は有限群 $G/N(\mathfrak{a})$ を経由し, $\mathrm{Tr}(\rho_{\mathfrak{a}}) = \mathrm{Tr}(\tau \pmod{\mathfrak{a}})$ は $G/N(\mathfrak{a})$ の $B/\mathfrak{a}$ への pseudo-representation とみなせる.

universal couple $(R_{\tau_{\bar{\rho}}}^{N(\mathfrak{a})}, T_{N(\mathfrak{a})} = \pi_{N(\mathfrak{a})} \circ T)$ の universality により, ある $\mathcal{O}$ -algebra 準同型

$$\varphi_{\tau}^{N(\mathfrak{a})} : R_{\tau_{\bar{\rho}}}^{N(\mathfrak{a})} \rightarrow B/\mathfrak{a}$$

で,

$$\varphi_{\tau}^{N(\mathfrak{a})} \circ \pi_{N(\mathfrak{a})} \circ T = \tau \pmod{\mathfrak{a}}$$

なるものがただ一つ存在する. $\mathcal{A}$ において $\mathfrak{a} \subset \mathfrak{a}'$ のとき, $\mathcal{N}$ において $N(\mathfrak{a}) \subset N(\mathfrak{a}')$ となると仮定してよいので, $\mathfrak{a} \in \mathcal{A}$ に関して射影極限を取ることににより, $\mathcal{O}$ -algebra 準同型

$$\varphi_{\tau} := \varprojlim_{\mathfrak{a} \in \mathcal{A}} \varphi_{\tau}^{N(\mathfrak{a})} \circ \pi_{N(\mathfrak{a})} : R_{\tau_{\bar{\rho}}} \rightarrow B$$

が定まり,

$$\varphi_{\tau} \circ T = \tau$$

を満たす. $\mathcal{O}$ 上の位相的生成系における値が τ で定まっているので, $\mathcal{O}$ -algebra 準同型

$$\varphi : R_{\tau_{\bar{\rho}}} \rightarrow B$$

で

$$\varphi \circ T = \tau$$

なるものは φ_{τ} と一致する. よって, $(R_{\tau_{\bar{\rho}}}, T)$ は $\tau_{\bar{\rho}}$ の universal couple である.

(2) 次に (1) で構成した $\tau_{\bar{\rho}}$ に対する universal couple $(R_{\tau_{\bar{\rho}}}, T)$ を用いて, $\bar{\rho}$ の universal couple $(R_{\bar{\rho}}, \rho)$ を構成する.

$R_{\tau_{\bar{\rho}}}$ を $R_{\bar{\rho}}$ とかくことにして, Proposition 2.1 により, universal couple $(R_{\bar{\rho}}, T)$ から $R_{\bar{\rho}}$ -係数の表現

$$\rho' : G \rightarrow \mathrm{GL}_2(R_{\bar{\rho}})$$

で,

$$\mathrm{Tr}(\rho') = \mathrm{Tr}(T)$$

なるものが構成される. このとき,

$$\mathrm{Tr}(\rho' \pmod{\mathfrak{m}_{R_{\bar{\rho}}}}) = \mathrm{Tr}(T \pmod{\mathfrak{m}_{R_{\bar{\rho}}}}) = \mathrm{Tr}(\tau_{\bar{\rho}}) = \mathrm{Tr}(\bar{\rho})$$

であり, $\bar{\rho}$ は絶対既約であるので, Theorem 3.2 により,

$$\rho' \pmod{\mathfrak{m}_{R_{\bar{\rho}}}} \sim \bar{\rho}.$$

したがって, Lemma 3.1 (1) により, ある表現

$$\rho : G \rightarrow \mathrm{GL}_2(R_{\bar{\rho}})$$

で,

$$\rho \pmod{\mathfrak{m}_{R_{\bar{\rho}}}} = \bar{\rho}, \quad \rho \sim \rho'$$

なるものが存在する.

任意の $\bar{\rho}$ の $B \in \mathrm{CL}_{\mathcal{O}}$ への deformation

$$\rho : G \rightarrow \mathrm{GL}_2(B)$$

に対し, ρ から構成される pseudo-representation τ_{ρ} は

$$\tau_{\rho} \pmod{\mathfrak{m}_B} = \tau_{\bar{\rho}}$$

を満たすから, $(R_{\bar{\rho}}, T)$ の universality により, $\mathcal{O}$ -algebra 準同型

$$\varphi_{\tau_{\rho}} : R_{\bar{\rho}} \rightarrow B$$

で,

$$\varphi_{\tau_{\rho}} \circ T = \tau_{\rho}$$

なるものがただ一つ存在する. このとき,

$$\mathrm{Tr}(\varphi_{\tau_{\rho}} \circ \rho) = \mathrm{Tr}(\varphi_{\tau_{\rho}} \circ T) = \mathrm{Tr}(\tau_{\rho}) = \mathrm{Tr}(\rho)$$

なので, Theorem 3.2 により,

$$\varphi_{\tau_{\rho}} \circ \rho \sim \rho$$

となり,

$$(\varphi_{\tau_{\rho}} \circ \rho) \pmod{\mathfrak{m}_B} = \rho \pmod{\mathfrak{m}_B} = \bar{\rho}$$

であるから, Lemma 3.1 (1) により,

$$\varphi_{\tau_{\rho}} \circ \rho \approx \rho.$$

よって, $(R_{\bar{\rho}}, \rho)$ は $\bar{\rho}$ に対する universal couple である. $\square$

とくに, G を代数体 F の絶対 Galois 群 $\mathrm{Gal}(\bar{F}/F)$ とすれば, Galois 表現の場合の universal deformation が構成されたことになる:

Corollary 3.4 (cf. [5, Proposition 2.30]). F を少なくとも一つ実素点 $\infty_{\mathbb{R}}$ をもつ有限次代数体とし, $c \in \mathrm{Gal}(\bar{F}/F)$ を $\infty_{\mathbb{R}}$ から生じる複素共役とする. 有限体 $\mathbb{F}$ の標数 p は 2 と相異なるものとする. 絶対既約な 2 次元 Galois 表現

$$\bar{\rho} : \mathrm{Gal}(\bar{F}/F) \rightarrow \mathrm{GL}_2(\mathbb{F})$$

は, $\{p, \infty\}$ の外で不分岐, すなわち, F の p を割らない素 ideal $\mathfrak{l}$ に対し, $\mathfrak{l}$ での惰性群 $I_{\mathfrak{l}} \subset \mathrm{Gal}(\bar{F}/F)$ 上で $\bar{\rho}$ は自明であり, 複素共役 c に関して odd, すなわち, $\det(\bar{\rho}(c)) = -1$ であると仮定する. このとき, Noether 的な $\mathrm{CL}_{\mathcal{O}}$ の object $R_{\bar{\rho}}$ と, $\bar{\rho}$ の $R_{\bar{\rho}}$ への $\{p, \infty\}$ の外で不分岐な deformation

$$\rho : \mathrm{Gal}(\bar{F}/F) \rightarrow \mathrm{GL}_2(R_{\bar{\rho}})$$

で, 次の性質を満たすものが存在する:

任意の $\bar{\rho}$ の $A \in \mathrm{CL}_{\mathcal{O}}$ への $\{p, \infty\}$ の外で不分岐な deformation

$$\rho : \mathrm{Gal}(\bar{F}/F) \rightarrow \mathrm{GL}_2(A)$$

に対し, $\mathcal{O}$ -algebra 準同型 $\varphi_\rho : R_{\bar{\rho}} \rightarrow A$ で

$$\varphi_\rho \circ \rho \approx \rho$$

なるものがただ一つ存在する. すなわち, $(R_{\bar{\rho}}, \rho)$ は $\bar{\rho}$ の $\{p, \infty\}$ の外で不分岐な deformation たちを支配する universal couple である.

Proof. $F_{\{p, \infty\}}$ を F の $\{p, \infty\}$ の外で不分岐な最大 Galois 拡大とすると, $\bar{\rho}$ は Galois 群 $\text{Gal}(F_{\{p, \infty\}}/F)$ を経由する. よって, Theorem 3.3 により, $\{p, \infty\}$ の外で不分岐な universal couple $(R_{\bar{\rho}}, \rho)$ が存在することはわかる. さらに, $R_{\bar{\rho}}$ が Noether 的であることを示すために, 次の Lemma を証明を省略して認めることにする:

Lemma 3.5 ([5, Lemmas 2.28 and 2.29]). (1) $A \in \text{CL}_{\mathcal{O}}$ に対して, (affine scheme $\text{Spec}(A)_{/\mathcal{O}}$ の閉点 $\mathfrak{m}_A$ における *cotangent space* とよばれる) $t_{A/\mathcal{O}}^* := \mathfrak{m}_A/(\mathfrak{m}_A^2 + \mathfrak{m}_{\mathcal{O}})$ が $\mathbb{F}$ 上有限次元であれば, A は Noether 的である.

(2) 一般に, profinite group G の絶対既約な $\mathbb{F}$ -係数の n 次元表現

$$\bar{\rho} : G \rightarrow \text{GL}_n(\mathbb{F})$$

に対して universal couple $(R_{\bar{\rho}}, \rho)$ が存在したとき, $\mathbb{F}$ 上のベクトル空間としての同型

$$t_{R_{\bar{\rho}}/\mathcal{O}} := \text{Hom}_{\mathbb{F}}(t_{R_{\bar{\rho}}/\mathcal{O}}^*, \mathbb{F}) \cong H_{\text{ct}}^1(G, \text{ad}(\bar{\rho}))$$

が得られる (左辺の空間は $\text{Spec}(R_{\bar{\rho}})_{/\mathcal{O}}$ の閉点 $\mathfrak{m}_{R_{\bar{\rho}}}$ における *tangent space* とよばれるものである). ここで, G -加群 $\text{ad}(\bar{\rho})$ は, 集合としては $\mathbb{F}$ -係数の $n \times n$ 行列全体 $M_n(\mathbb{F})$ であり, G の作用が

$$g \cdot M = \bar{\rho}(g)M\bar{\rho}(g)^{-1} \quad (g \in G, M \in M_n(\mathbb{F}))$$

で与えられるもので, これには離散位相を入れておく. また, 連続な 1 次元 cohomology $H_{\text{ct}}^1(G, \text{ad}(\bar{\rho}))$ は, 連続な 1-cocycle 全体のなす集合

$$\begin{aligned} Z_{\text{ct}}^1(G, \text{ad}(\bar{\rho})) &:= \{u : G \rightarrow \text{ad}(\bar{\rho}) : \text{continuous} \mid \\ &\quad u(gh) = g \cdot u(h) + u(g), g, h \in G\} \end{aligned}$$

と, 連続な 1-coboundary 全体のなす集合

$$\begin{aligned} B_{\text{ct}}^1(G, \text{ad}(\bar{\rho})) &:= \{u \in Z_{\text{ct}}^1(G, \text{ad}(\bar{\rho})) \mid u(g) = M - g \cdot M \ (g \in G) \\ &\quad \text{with some } M \in \text{ad}(\bar{\rho})\} \end{aligned}$$

を用いて,

$$H_{\text{ct}}^1(G, \text{ad}(\bar{\rho})) := Z_{\text{ct}}^1(G, \text{ad}(\bar{\rho}))/B_{\text{ct}}^1(G, \text{ad}(\bar{\rho}))$$

と定義されるものである.

Lemma 3.5 により,

$$\dim_{\mathbb{F}} H_{\text{ct}}^1(\text{Gal}(F_{\{p,\infty\}}/F), \text{ad}(\bar{\rho})) < \infty$$

を示せば, $R_{\bar{\rho}}$ が Noether 的であることがわかる.

$$\bar{\rho} : \text{Gal}(F_{\{p,\infty\}}/F) \rightarrow \text{GL}_2(\mathbb{F})$$

に対して, $H := \text{Ker}(\bar{\rho})$ とおくと Inflation-restriction sequence により, 完全列

$$\begin{aligned} 0 \rightarrow H_{\text{ct}}^1(\text{Gal}(F_{\{p,\infty\}}/F)/H, \text{ad}(\bar{\rho})^H) &\rightarrow H_{\text{ct}}^1(\text{Gal}(F_{\{p,\infty\}}/F), \text{ad}(\bar{\rho})) \\ &\rightarrow H_{\text{ct}}^1(H, \text{ad}(\bar{\rho}))^{\text{Gal}(F_{\{p,\infty\}}/F)/H} \end{aligned}$$

を得る. (一般に, H -加群 M に対して, M^H は M の H -不変な元全体のなす部分加群を表すことにする.) H に対応する $F_{\{p,\infty\}}/F$ の有限次の中間体を F_H/F とおくと, $\text{ad}(\bar{\rho})$ に H は自明に作用するので, 次の完全列が得られる:

$$\begin{aligned} 0 \rightarrow H_{\text{ct}}^1(\text{Gal}(F_H/F), \text{ad}(\bar{\rho})) &\rightarrow H_{\text{ct}}^1(\text{Gal}(F_{\{p,\infty\}}/F), \text{ad}(\bar{\rho})) \\ &\rightarrow \text{Hom}_{\text{ct}}(H_p^{\text{ab}}, \text{ad}(\bar{\rho}))^{\text{Gal}(F_H/F)}. \end{aligned}$$

ここで, H_p^{ab} は H の abel 化 H^{ab} の p -part を表す. O_F を F の整数環とし, $O_p := O_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ とおく. また, Cl_F を F の ideal 類群とすれば, 類体論により, 完全列

$$O_p^{\times} \rightarrow \text{Gal}(F_{\{p,\infty\}}/F)^{\text{ab}} \rightarrow \text{Cl}_F \rightarrow 0$$

が得られる. よって, H_p^{ab} は $\mathbb{Z}_p$ 上 finite rank であるので,

$$\dim_{\mathbb{F}} H_{\text{ct}}^1(\text{Gal}(F_{\{p,\infty\}}/F), \text{ad}(\bar{\rho})) < \infty$$

となることがわかる. □

4. Parametrization of given deformations

Section 3 に引き続き, Section 1 と同じ記号を用いることにする. とくに, 扱う表現や環準同型などは, しかるべき位相に関して連続であることを仮定していることに注意.

F を少なくとも一つ実素点 $\infty_{\mathbb{R}}$ をもつ有限次代数体とし, $\infty_{\mathbb{R}}$ から生じる複素共役を $c \in \text{Gal}(\bar{F}/F)$ とかくことにする. O_F を F の整数環とする. 有限体 $\mathbb{F}$ の標数 p は 2 と相異なるものとする. S をすべての無限素点と p を割るすべての有限素点を含んだ F の素点からなる有限集合として,

$$\bar{\rho} : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(\mathbb{F})$$

を絶対既約で S の外で不分岐であり, c に関して odd な表現とする. F_S を F の S の外で不分岐な最大 Galois 拡大とすれば, $\bar{\rho}$ は $\text{Gal}(F_S/F)$ を経由する:

$$\bar{\rho} : \text{Gal}(F_S/F) \rightarrow \text{GL}_2(\mathbb{F}).$$

S に含まれない F の素 ideal $\mathfrak{l}$ に対し, $\mathfrak{l}$ の剰余次数を $q_{\mathfrak{l}}$ とおくと, 剰余体 $O_F/\mathfrak{l}$ の代数的閉包上での $q_{\mathfrak{l}}$ 乗写像 $x \mapsto x^{q_{\mathfrak{l}}}$ から持ち上げられた *arithmetic Frobenius element* $\text{Frob}_{\mathfrak{l}} \in \text{Gal}(F_S/F)$ が定まる. Chebotarev density theorem (cf. [4, Theorem 1.3.1]) により, $\{\text{Frob}_{\mathfrak{l}}\}_{\mathfrak{l} \notin S}$ は $\text{Gal}(F_S/F)$ において, profinite 位相に関し dense であることが知られている.

さて, $\text{CL}_{\mathcal{O}}$ の object の族 $\{A_i\}_{i \in I}$ と, それらを係数とする $\bar{\rho}$ の deformation の族

$$\rho_i : \text{Gal}(F_S/F) \rightarrow \text{GL}_2(A_i) \quad (i \in I)$$

を用意する. このとき, $\{\rho_i\}_{i \in I}$ から得られる情報を用いて, 少なくとも deformation の族 $\{\rho_i\}_{i \in I}$ は支配できるという小さな意味での $\bar{\rho}$ の universal couple (R, ρ) を構成することができる:

Theorem 4.1. 直積環 $\prod_{i \in I} A_i$ の Noether 的な部分環である $R \in \text{CL}_{\mathcal{O}}$ と, $\bar{\rho}$ の R への deformation

$$\rho : \text{Gal}(F_S/F) \rightarrow \text{GL}_2(R)$$

で, 各 $i \in I$ に対し,

$$p_i \circ \rho \approx \rho_i$$

を満たすものが存在する. ここで, $p_i : \prod_{i \in I} A_i \rightarrow A_i$ は i 番目の projection を表す.

Proof. $\prod_{i \in I} A_i$ の部分環

$$R' := \{(a_i)_{i \in I} \in \prod_{i \in I} A_i \mid a_i \pmod{\mathfrak{m}_{A_i}} = a_j \pmod{\mathfrak{m}_{A_j}} \text{ in } \mathbb{F} \text{ for any } i, j \in I\}$$

は, $\mathfrak{m}_{R'} := \prod_{i \in I} \mathfrak{m}_{A_i}$ を極大 ideal とし $\mathbb{F}$ を剰余体にもつ完備な局所 $\mathcal{O}$ -subalgebra である. 各 $i \in I$ に対して,

$$\rho_i \pmod{\mathfrak{m}_{A_i}} = \bar{\rho}$$

であるから, 直積表現

$$\rho' := \prod_{i \in I} \rho_i : \text{Gal}(F_S/F) \rightarrow \text{GL}_2\left(\prod_{i \in I} A_i\right)$$

は値を $\text{GL}_2(R')$ にもち,

$$\rho' \pmod{\mathfrak{m}_{R'}} = \bar{\rho}, \quad p_i \circ \rho' = \rho_i \quad (i \in I)$$

を満たす. ここで, R' の部分環

$$\mathcal{O}[(\mathrm{Tr}(\rho_i(\mathrm{Frob}_l)))_{i \in I} \mid l \notin S : \text{prime}]$$

を R' の中で完備化したものを R とおけば, R は $\mathfrak{m}_R := R \cap \mathfrak{m}_{R'}$ を極大 ideal とし $\mathbb{F}$ を剰余体にもつ完備な局所 $\mathcal{O}$ -subalgebra となる.

Chebotarev density theorem により $\{\mathrm{Frob}_l\}_{l \notin S}$ は $\mathrm{Gal}(F_S/F)$ の中で dense であり, ρ_i たちは連続なので,

$$\mathrm{Tr}(\rho') : \mathrm{Gal}(F_S/F) \rightarrow R'$$

は R に値をもつ. Remark 2.1 (1) により $\mathrm{Tr}(\rho')$ から作られる pseudo-representation から, Proposition 2.1 により, R -係数の表現

$$\rho'' : \mathrm{Gal}(F_S/F) \rightarrow \mathrm{GL}_2(R)$$

で,

$$\mathrm{Tr}(\rho'') = \mathrm{Tr}(\rho')$$

なるものが構成される. このとき,

$$\mathrm{Tr}(\rho''(\mathrm{mod} \mathfrak{m}_R)) = \mathrm{Tr}(\bar{\rho})$$

であるから, Theorem 3.2 により,

$$\rho''(\mathrm{mod} \mathfrak{m}_R) \sim \bar{\rho}.$$

このことから,

$$\rho : \mathrm{Gal}(F_S/F) \rightarrow \mathrm{GL}_2(R)$$

で,

$$\rho \sim \rho'', \quad \rho(\mathrm{mod} \mathfrak{m}_R) = \bar{\rho}$$

なるものが得られる. とくに,

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(\rho')$$

であり, ρ を $\mathrm{GL}_2(R')$ に値をもつものとみなせば, Theorem 3.2 により,

$$\rho \sim \rho' \quad (\text{over } R').$$

一方で,

$$\rho(\mathrm{mod} \mathfrak{m}_R) = \bar{\rho} = \rho'(\mathrm{mod} \mathfrak{m}_{R'})$$

だから, Lemma 3.1 (i) により,

$$\rho \approx \rho' \quad (\text{over } R')$$

となる (Remark 3.1 (1) にある通り, R' が局所環であるので Lemma 3.1 (1) を適用できることに注意). 各 $i \in I$ に対し,

$$p_i \circ \rho' = \rho_i$$

だから,

$$p_i \circ \rho \approx p_i \circ \rho' = \rho_i \quad (\text{over } A_i)$$

を得る. さて, [2, Theorem (2.3)] において, 完備な局所 $\mathcal{O}$ -algebra のなす圏における $\bar{\rho}$ に対する universal couple $(\mathcal{R}, \rho)$ が構成されており, さらに, もし

$$\dim_{\mathbb{F}} H_{\text{ct}}^1(\text{Gal}(F_S/F), \text{ad}(\bar{\rho})) < \infty$$

ならば, $\mathcal{R}$ は Noether 的であることが示されている. 今の状況では, Corollary 3.4 の証明の中で示したように, この有限次元性は満たされているので, $\mathcal{R}$ は Noether 的である. $(\mathcal{R}, \rho)$ の universality により, $\mathcal{O}$ -algebra 準同型

$$\varphi : \mathcal{R} \rightarrow R$$

で,

$$\varphi \circ \rho \approx \rho$$

なるものがただ一つ存在する. S に含まれない F の素 ideal $\mathfrak{l}$ に対して,

$$\begin{aligned} \varphi(\text{Tr}(\rho(\text{Frob}_{\mathfrak{l}}))) &= (\text{Tr}(\varphi \circ \rho))(\text{Frob}_{\mathfrak{l}}) \\ &= (\text{Tr}(\rho))(\text{Frob}_{\mathfrak{l}}) \\ &= \text{Tr}(\rho(\text{Frob}_{\mathfrak{l}})) \\ &= \text{Tr}(\rho'(\text{Frob}_{\mathfrak{l}})) \\ &= (\text{Tr}(\rho_i(\text{Frob}_{\mathfrak{l}})))_{i \in I} \end{aligned}$$

であり, $\{(\text{Tr}(\rho_i(\text{Frob}_{\mathfrak{l}})))_{i \in I}\}_{\mathfrak{l} \notin S}$ は R の $\mathcal{O}$ 上の位相的生成元であるから, φ は全射であることがわかる. よって, R も Noether 的であり, くに $R \in \text{CL}_{\mathcal{O}}$ となる. $\square$

5. Modular Galois representations

この Section では, [8, Section 2.3] に沿って, Hilbert cusp form に付随する Galois 表現たちを紹介し, その中で, Hilbert cusp form に対する Hecke algebra を modular な deformation を支配する universal deformation ring とみなせることが期待できる根拠として, Hilbert cusp form のなす空間とそれに作用する Hecke algebra の間の duality について紹介する.

$\mathbb{R}$ と $\mathbb{C}$ をそれぞれ実数体と複素数体とする. F を有限次総実代数体, $\mathcal{O}$ を F の整数環とする. F から $\overline{\mathbb{Q}}$ への embedding 全体のなす集合を I とおく. I を自由基底とする $\mathbb{Z}$ -自由加群を $\mathbb{Z}[I]$ と表すことにする. p を素数とし, 以下, 二つの体の embedding

$$i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p, \quad i_{\infty} : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$$

を固定する. ここで, $\overline{\mathbb{Q}}_p$ は p -進数体 $\mathbb{Q}_p$ の代数的閉包を表す. これら二つの embedding により, 代数的数を p -進的な対象とみなしたり, 複素数として扱ったりする.

5.1. Definition of Hilbert cusp forms

この Subsection では, F 上の Hilbert cusp form を adelic に定式化する. そのために, いくつか記号を準備したい.

$\kappa = (\kappa_1, \kappa_2) \in \mathbb{Z}[I]^2$ を一つ取り, $i = 1, 2$ に対して $\kappa_i = \sum_{\sigma \in I} \kappa_{i,\sigma} \sigma$ とおく. $\mathbf{1} := \sum_{\sigma \in I} \sigma \in \mathbb{Z}[I]$ とする. $g = (g_\sigma = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix})_{\sigma \in I} \in \mathrm{GL}_2(\mathbb{R})^I$ と, 複素上半平面 $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ の I を添字集合とした直積空間 $\mathfrak{H}^I$ の点 $z = (z_\sigma)_{\sigma \in I}$ に対して,

$$\det(g)^{\kappa_1 - \mathbf{1}} := \prod_{\sigma \in I} \det(g_\sigma)^{\kappa_{1,\sigma} - 1},$$

$$j(g, z)^{\kappa_2 - \kappa_1 + \mathbf{1}} := \prod_{\sigma \in I} (c_\sigma z_\sigma + d_\sigma)^{\kappa_{2,\sigma} - \kappa_{1,\sigma} + 1}$$

とおき,

$$J_\kappa(g, z) := \det(g)^{\kappa_1 - \mathbf{1}} j(g, z)^{\kappa_2 - \kappa_1 + \mathbf{1}}$$

と定義する. $\mathbf{i} := (\sqrt{-1}, \dots, \sqrt{-1}) \in \mathfrak{H}^I$ とおく. 一次分数変換による $g = (g_\sigma = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix})_{\sigma \in I} \in \mathrm{GL}_2(\mathbb{R})_+^I$ の $z = (z_\sigma)_{\sigma \in I} \in \mathfrak{H}^I$ 上への作用を

$$g \cdot z = (g_\sigma \cdot z_\sigma)_{\sigma \in I} := \left(\frac{a_\sigma z_\sigma + b_\sigma}{c_\sigma z_\sigma + d_\sigma} \right)_{\sigma \in I} \in \mathfrak{H}^I$$

と表すことにし,

$$C_{\mathbf{i}} := \{g \in \mathrm{GL}_2(\mathbb{R})_+^I \mid g \cdot \mathbf{i} = \mathbf{i}\}$$

と定義する. ここで, $\mathrm{GL}_2(\mathbb{R})_+$ は正の行列式をもつ $\mathbb{R}$ -係数の 2×2 行列全体のなす群を表す.

$\mathbb{A}$ を $\mathbb{Q}$ 上の adèle 環とし, $F_{\mathbb{A}} := \mathbb{A} \otimes_{\mathbb{Z}} O$ で F 上の adèle 環を表すことにする. F_∞ を $F_{\mathbb{A}}$ の infinite part, $F_{\mathbb{A}}^{(\infty)}$ を finite part とする. また, $u \in \mathrm{GL}_2(F_{\mathbb{A}})$ の infinite part を $u_\infty \in \mathrm{GL}_2(F_\infty) = \mathrm{GL}_2(\mathbb{R})^I$, finite part を $u^{(\infty)} \in \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)})$ とかくことにする. $\hat{\mathbb{Z}} := \prod_{p:\text{prime}} \mathbb{Z}_p$ とし, $\hat{O} := \prod_{\mathfrak{l}:\text{prime}} O_{\mathfrak{l}} = \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} O$ とおく.

$\mathfrak{N}$ を O の ideal とする. F の絶対差積 ∂ に対し, $\delta \in \hat{O}$ で $\delta \hat{O} = \partial \hat{O}$ なるものを一つ選び,

$$\hat{\Gamma}_0(\mathfrak{N}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{O}) \mid c \in \mathfrak{N} \hat{O} \right\}$$

とおき,

$$S_0(\mathfrak{N}) := \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}^{-1} \hat{\Gamma}_0(\mathfrak{N}) \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$$

と定義する. $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_+)$ を連続な二つの character

$$\varepsilon_1, \varepsilon_2 : \hat{O}^\times \rightarrow \mathbb{C}^\times$$

と, Hecke character

$$\varepsilon_+ : F_{\mathbb{A}}^\times / F^\times \rightarrow \mathbb{C}^\times$$

の組とし, これらについて, $z \in \hat{O}^\times$ に対し,

$$\varepsilon(z) = \varepsilon_1(z)\varepsilon_2(z)$$

を満たし, $x_\infty = (x_{\infty, \sigma})_{\sigma \in I} \in F_\infty^\times = (\mathbb{R}^\times)^I$ に対して,

$$\varepsilon_+(x_\infty) = x_\infty^{-(\kappa_1 + \kappa_2) + \mathbf{1}} := \prod_{\sigma \in I} x_{\infty, \sigma}^{-(\kappa_{1, \sigma} + \kappa_{2, \sigma}) + 1}$$

を満たすと仮定する. ε_1 と ε_2 は連続であり, $\hat{O}^\times$ は profinite group なので, これらの character は finite order となり, $i = 1, 2$ に対し, F の ideal $\mathfrak{c}(\varepsilon_i)$ を ε_i の conductor, すなわち, F の ideal $\mathfrak{c}$ で ε_i が $1 + \mathfrak{c}\hat{O}$ 上 trivial になるようなもののうち maximal なものとし,

$$\mathfrak{c}(\varepsilon) := \mathfrak{c}(\varepsilon_1)\mathfrak{c}(\varepsilon_2)$$

と定義する. このとき, ε_+ を $\hat{O}^\times$ に制限した際に生じる conductor を $\mathfrak{c}(\varepsilon_+)$ と表せば,

$$\mathfrak{c}(\varepsilon) \subset \mathfrak{c}(\varepsilon_+)$$

となることがわかる. さらに,

$$\varepsilon^- := \varepsilon_1 \cdot \varepsilon_2^{-1} : \hat{O}^\times \rightarrow \mathbb{C}^\times$$

とおき, $\mathfrak{c}(\varepsilon^-)$ をその conductor とする. もし, $\mathfrak{N} \subset \mathfrak{c}(\varepsilon^-)$ ならば, ε^- は $1 + \mathfrak{N}\hat{O}$ 上 trivial なので,

$$\varepsilon : S_0(\mathfrak{N}) \rightarrow \mathbb{C}^\times, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \xrightarrow{\text{def}} \varepsilon_2(ad - bc)\varepsilon^-(a_{\mathfrak{N}})$$

は $S_0(\mathfrak{N})$ の character となることがわかる. ここで, $a_{\mathfrak{N}} \in O_{\mathfrak{N}} := \prod_{\mathfrak{l} \nmid \mathfrak{N}} O_{\mathfrak{l}}$ は $a \in \hat{O}$ の $\mathfrak{N}$ -part を表す. 以下,

$$\mathfrak{N} \subset \mathfrak{c}(\varepsilon^-)$$

を仮定しておく. まず, $\mathbb{C}$ -係数の Hilbert cusp form を定義する:

Definition 5.1 ([8, Section 2.3.2]). 上述の設定のもとで, 関数 $f : \text{GL}_2(F_{\mathbb{A}}) \rightarrow \mathbb{C}$ が $\mathbb{C}$ -係数の weight $\kappa = (\kappa_1, \kappa_2)$, level $\mathfrak{N}$, character $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_+)$ の Hilbert cusp form であるとは, 次の三つの条件を満たすことをいう:

(SA1) $\alpha \in \text{GL}_2(F)$, $x \in \text{GL}_2(F_{\mathbb{A}})$, $u \in S_0(\mathfrak{N})C_{\mathfrak{i}}$, $z \in F_{\mathbb{A}}^\times$ に対して,

$$f(\alpha x u z) = \varepsilon_+(z)\varepsilon(u^{(\infty)})f(x)J_{\kappa}(u_{\infty}, \mathfrak{i})^{-1}$$

を満たす.

(SA2) 任意の $z \in \mathfrak{H}^I$ に対し, $u \in \mathrm{GL}_2(\mathbb{R})^I$ で $u \cdot \mathbf{i} = z$ となるものを一つ取っておく. このとき, 任意の $g \in \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)})$ に対し, 関数

$$f_g : \mathfrak{H}^I \rightarrow \mathbb{C}, \quad z \xrightarrow{\mathrm{def}} f(gu)J_{\kappa}(u, \mathbf{i})$$

は $\mathfrak{H}^I$ 上で正則である.

(SA3) 任意の $g \in \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)})$ に対して,

$$\int_{F_{\mathbb{A}}/F} f\left(\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} g\right) du = 0$$

を満たす. ここで, du は $F_{\mathbb{A}}/F$ 上の additive Haar measure である.

weight κ , level $\mathfrak{N}$, character ε の $\mathbb{C}$ -係数の Hilbert cusp form 全体のなす空間を $S_{\kappa}(\mathfrak{N}, \varepsilon; \mathbb{C})$ と表すことにする.

Remark 5.1. 条件 (SA1) により, $\kappa_1 + \kappa_2 \notin \mathbb{Z}\mathbf{1}$ であれば, $S_{\kappa}(\mathfrak{N}, \varepsilon; \mathbb{C}) = 0$ となることがわかる. 以下, Hilbert cusp form を論じるときは, $\kappa_1 + \kappa_2 \in \mathbb{Z}\mathbf{1}$ を仮定し, $\kappa_1 + \kappa_2 = [\kappa]\mathbf{1}$ とおくことにする.

Remark 5.2. (1) 条件 (SA3) は次の条件と同値である:

(SA3)' 任意の $g \in \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)})$ に対して, 関数

$$\tilde{f}_g : \mathfrak{H}^I \rightarrow \mathbb{C}, \quad z = (z_{\sigma})_{\sigma \in I} \xrightarrow{\mathrm{def}} f_g(z) \left| \prod_{\sigma \in I} \mathrm{Im}(z_{\sigma})^{\frac{\kappa_{2,\sigma} - \kappa_{1,\sigma} + 1}{2}} \right|$$

は z に依存しない有界性をもつ.

(2) 条件 (SA3)' の「 z に依存しない有界性をもつ」の部分に「 $\mathrm{Im}(z) \rightarrow \infty$ とした時に多項式増大度をもつ」としたものを (MA3)' とする. このとき, 関数 $f : \mathrm{GL}_2(F_{\mathbb{A}}) \rightarrow \mathbb{C}$ が三つの条件 (SA1), (SA2), (MA3)' を満たせば, f は weight κ , level $\mathfrak{N}$, character ε の $\mathbb{C}$ -係数の Hilbert modular form であるという.

Remark 5.3. $g \in \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)})$ に対し, 条件 (SA2) に現れる $\mathfrak{H}^I$ 上の正則関数 f_g は, classical な意味での weight $(\kappa_{2,\sigma} - \kappa_{1,\sigma} + 1)_{\sigma \in I}$, character $\varepsilon^{-1}(g^{-1}(\cdot)g)$, modular group

$$\Gamma_{0,g}(\mathfrak{N}) := gS_0(\mathfrak{N})g^{-1}\mathrm{GL}_2(\mathbb{R})_+^I \cap \mathrm{GL}_2(F)$$

を level にもつ Hilbert cusp form となっている.

Hilbert cusp form $f \in S_{\kappa}(\mathfrak{N}, \varepsilon; \mathbb{C})$ は adelic な Fourier 展開をもつことが知られている:

Proposition 5.1 ([8, Proposition 2.26]). $f \in S_{\kappa}(\mathfrak{N}, \varepsilon; \mathbb{C})$ は, 次の Fourier 展開をもつ: $x \in F_{\mathbb{A}}, y \in F_{\mathbb{A}}^{\times}$ について, とくに, $y_{\infty} = (y_{\sigma})_{\sigma \in I} \in$

$F_\infty^\times = (\mathbb{R}^\times)^I$ において,

$$f\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) = |y|_{\mathbb{A}} \sum_{0 \ll \xi \in F} \mathbf{a}_\infty(\xi y, f) \left(\prod_{\sigma \in I} (\sigma(\xi) y_\sigma)^{-\kappa_{1,\sigma}} \right) \\ \times e_F(\sqrt{-1} \xi y_\infty) e_F(\xi x).$$

Fourier 係数を与えている写像

$$F_{\mathbb{A}}^\times \rightarrow \mathbb{C}, \quad y \mapsto \mathbf{a}_\infty(y, f)$$

は, $(\hat{O}^\times \times F_\infty) \cap F_{\mathbb{A}}^\times$ で support されており, 任意の $u \in \hat{O}^\times$ に対して,

$$\mathbf{a}_\infty(uy, f) = \varepsilon_1(u) \mathbf{a}_\infty(y, f)$$

を満たす. ここで, $|\cdot|_{\mathbb{A}}$ は adèle norm, 記号 $0 \ll \xi \in F$ は ξ が総正であることを表している. また, 写像 $e_F : F_{\mathbb{A}}/F \rightarrow \mathbb{C}^\times$ は

$$e_F(x_\infty) := e^{2\pi\sqrt{-1}\sum_{\sigma \in I} x_\sigma} \quad (x_\infty = (x_\sigma)_{\sigma \in I} \in F_\infty = \mathbb{R}^I)$$

により定まる additive character である.

以上の設定のもとで, adelic な Fourier 係数に関する条件を課すことで, $\mathbb{C}$ 内の $\mathbb{Q}$ -algebra を係数にもつ Hilbert cusp form や, p -進的な係数をもつ Hilbert cusp form も定義しておく:

Definition 5.2 ([8, Section 2.3.3]). (1) $R \subset \mathbb{C}$ を $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_+)$ の値と F の Galois 閉包 F^{Gal} の整数環 O^{Gal} を含む $\mathbb{Q}$ -algebra とする. このとき, R -係数の weight κ , level $\mathfrak{N}$, character ε の Hilbert cusp form のなす空間を

$$S_\kappa(\mathfrak{N}, \varepsilon; R) := \{f \in S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C}) \mid \mathbf{a}_\infty(y, f) \in R \text{ for any } y \in F_{\mathbb{A}}^\times\}$$

と定義する.

(2) R を $\overline{\mathbb{Q}}_p$ -algebra とする. 固定した embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ を用いて, R -係数の weight κ , level $\mathfrak{N}$, character ε の Hilbert cusp form のなす空間を

$$S_\kappa(\mathfrak{N}, \varepsilon; R) := S_\kappa(\mathfrak{N}, \varepsilon; \overline{\mathbb{Q}}) \otimes_{\overline{\mathbb{Q}}, i_p} R$$

と定義する.

(3) $K \subset \overline{\mathbb{Q}}_p$ を $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_+)$ の値と O^{Gal} を含む $\mathbb{Q}_p$ の有限次拡大体とし, $\mathcal{O}$ を K の整数環とする. $\mathbb{C}_p$ を $\overline{\mathbb{Q}}_p$ の p -進完備化とし, $R \subset \mathbb{C}_p$ を $\mathcal{O}$ -algebra とする. このとき, R -係数の weight κ , level $\mathfrak{N}$, character ε の Hilbert cusp form のなす空間を

$$S_\kappa(\mathfrak{N}, \varepsilon; R) := \{f \in S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C}_p) \mid y_p^{-\kappa_1} \mathbf{a}_\infty(y, f) \in R \text{ for any } y \in F_{\mathbb{A}}^\times\}$$

と定義する. ここで $y_p^{-\kappa_1}$ は, 各 $\sigma \in I$ に対し F の p を割る素 ideal $\mathfrak{p}_\sigma$ を, $i_p(\sigma(F)) \subset \overline{\mathbb{Q}}_p$ の $\mathbb{C}_p$ 内での p -進完備化が $\sigma(F)_{\sigma(\mathfrak{p}_\sigma)}$ と一致するも

のとしておいて,

$$y_p^{-\kappa_1} := \prod_{\sigma \in I} y_{\mathfrak{p}_\sigma}^{-\kappa_1, \sigma}$$

とおいたものである.

Remark 5.4. (1) Definition 5.2 (3) の記号で, 各 $y \in F_{\mathbb{A}}^\times$ に対し,

$$\mathbf{a}_p(y, f) := y_p^{-\kappa_1} \mathbf{a}_\infty(y, f)$$

と定義し, f の p -adic Fourier coefficient とよぶ. この p -adic Fourier coefficient なるものは, 本来は幾何的に定式化されるものである (cf. [7, Section 4.2.10]).

(2) p -adic Fourier coefficient に関して, q -expansion principle が成立することが知られている. すなわち, R を Definition 5.2 (1)-(3) のいずれかのものとし, $f \in S_\kappa(\mathfrak{N}, \varepsilon; R)$ について, もし, すべての $y \in \hat{O} \cap (F_{\mathbb{A}}^{(\infty)})^\times$ に対し $\mathbf{a}_p(y, f) = 0$ ならば, $f = 0$ である (cf. [8, Section 2.3.3]).

5.2. Hecke algebras and duality

この Subsection では, [8, Sections 2.3.2, 2.3.3, 2.3.4] に沿って, Section 5.1 で定義した Hilbert cusp form の空間に作用する Hecke algebra を定義し, Hecke operator による Fourier coefficient の振る舞いや, Hilbert cusp form の空間と Hecke algebra の duality について紹介する. 以下で用いる記号は, 引き続き前節のものとする.

2×2 行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対し,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\iota := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

とおく (ι は 2×2 行列のなす環 M_2 の *main involution* とよばれるものである). まず, F の整 ideal $\mathfrak{N}$ に対し, 二つの semi-group を用意する:

$$\Delta_0(\mathfrak{N}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\hat{O}) \cap \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)}) \mid a_{\mathfrak{N}} \in O_{\mathfrak{N}}^\times, c \in \mathfrak{N}\hat{O} \right\},$$

$$\begin{aligned} \Delta_0^*(\mathfrak{N}) &:= \Delta_0(\mathfrak{N})^\iota \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\hat{O}) \cap \mathrm{GL}_2(F_{\mathbb{A}}^{(\infty)}) \mid d_{\mathfrak{N}} \in O_{\mathfrak{N}}^\times, c \in \mathfrak{N}\hat{O} \right\}. \end{aligned}$$

Definition 5.2 (3) に現れる p -進整数環 $\mathcal{O}$ を用いて, $\mathbb{Q}$ 上のある有限次拡大体に含まれる p -進付値環 $\mathcal{W} := i_\infty(i_p^{-1}(\mathcal{O})) \subset \mathbb{C}$ を定める. F の各素 ideal $\mathfrak{q}$ に対する素元 $\varpi_{\mathfrak{q}}$ を $\mathcal{W} \cap F$ から取っておく.

Hecke operator を定義するために, character $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_+)$ を $(F_{\mathbb{A}}^{(\infty)})^\times$ と $\Delta_0(\mathfrak{N})$ の上に, 次の手順で延長しておく:

(ex0) 任意の $w = \sum_{\sigma \in I} w_\sigma \in \mathbb{Z}[I]$ を,

$$O_p^\times := \prod_{\mathfrak{p}|p} O_{\mathfrak{p}}^\times \rightarrow \overline{\mathbb{Q}}_p^\times, \quad x = (x_{\mathfrak{p}})_{\mathfrak{p}|p} \mapsto x^w := \prod_{\sigma \in I} x_{\mathfrak{p}_\sigma}^{w_\sigma}$$

により, $O_p^\times$ の character とみなす. さらに, $\oplus_{\mathfrak{p}|p} \varpi_{\mathfrak{p}}^{\mathbb{Z}}$ 上では trivial とすることで $\prod_{\mathfrak{p}|p} F_{\mathfrak{p}}^\times$ 上に延長したものを,

$$\prod_{\mathfrak{p}|p} F_{\mathfrak{p}}^\times \rightarrow \overline{\mathbb{Q}}_p^\times, \quad x \mapsto x^{w_p}$$

と表す. とくに, 各 $\mathfrak{p}|p$ の $F/\mathbb{Q}$ における分岐指数を $e_{\mathfrak{p}}$ としたとき, ある $u_{\mathfrak{p}} \in O_{\mathfrak{p}}^\times$ を用いて, $p = u_{\mathfrak{p}} \varpi_{\mathfrak{p}}^{e_{\mathfrak{p}}}$ とかけるから, p^{w_p} は p -adic unit であることに注意.

(ex1) $\hat{O}^\times$ 上の character である ε_1 と ε_2 を, $\oplus_{\mathfrak{q}} \varpi_{\mathfrak{q}}^{\mathbb{Z}}$ 上では trivial とすることで,

$$\varepsilon_1, \varepsilon_2 : (F_{\mathbb{A}}^{(\infty)})^\times \rightarrow \mathbb{C}^\times$$

に延長する. 一方, ε_+ については, $(F_{\mathbb{A}}^{(\infty)})^\times$ 上に $\varepsilon_+ = \varepsilon_1 \cdot \varepsilon_2$ と延長しておく. また, $a \in (F_{\mathbb{A}}^{(\infty)})^\times$ に対し,

$$\varepsilon^-(a) := \varepsilon_1(a) \cdot \varepsilon_2(a)^{-1}$$

とおき, $F_{\mathbb{A}}^{(\infty)}$ -係数の対角行列全体のなす群

$$T_{\text{GL}}(F_{\mathbb{A}}^{(\infty)}) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in F_{\mathbb{A}}^{(\infty)} \right\}$$

上の character

$$\varepsilon : T_{\text{GL}}(F_{\mathbb{A}}^{(\infty)}) \rightarrow \mathbb{C}^\times, \quad \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mapsto \varepsilon_2(ad) \varepsilon^-(a_{\mathfrak{N}})$$

を定義しておく.

(ex2) v で ∞ か p を表し, 記号 $B^\times$ は $v = \infty$ (resp. $v = p$) のとき $\mathbb{C}^\times$ (resp. $\mathcal{O}^\times$) を表すものとする. また, F の整 ideal $\mathfrak{N} \cap (v)$ を $v = \infty$ (resp. $v = p$) のとき $\mathfrak{N}$ (resp. $\mathfrak{N} \cap (p)$) を表すものとする. $\hat{O}$ -係数の対角行列全体のなす群を

$$T_{\text{GL}}(\hat{O}) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \hat{O} \right\}$$

とし, $T_{\text{GL}}(\hat{O}) \cap S_0(\mathfrak{N} \cap (v))$ に制限した character ε を $\Delta_0(\mathfrak{N} \cap (v))$ と $\Delta_0^*(\mathfrak{N} \cap (v))$ の character ε_Δ^v に次のように延長する: $\delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_0(\mathfrak{N} \cap (v)) \cup \Delta_0^*(\mathfrak{N} \cap (v))$ に対し,

$$\varepsilon_\Delta^v(\delta) := \det(\delta)^{-1_v} \varepsilon_2(\det(\delta)) \varepsilon^-(a_{\mathfrak{N} \cap (v)}) \in B^\times.$$

ここで, $\det(\delta)^{-1_v}$ は $v = p$ (resp. $v = \infty$) のとき (ex0) で定義された p -adic unit (resp. 1) を表す.

(ex3) 以上の記号のもと, 群の積 $F_{\mathbb{A}}^{\times} S_0(\mathfrak{N} \cap (v))$ の character

$$\varepsilon_S = \varepsilon_S^v : F_{\mathbb{A}}^{\times} S_0(\mathfrak{N} \cap (v)) \rightarrow B^{\times},$$

$$zs \stackrel{\text{def}}{\mapsto} |z^{(\infty)}|_{\mathbb{A}}^{-2} z_v^{-2} \mathbf{1}_v \varepsilon_+(z) \varepsilon_{\Delta}^v(s) \quad (z \in F_{\mathbb{A}}^{\times}, s \in S_0(\mathfrak{N} \cap (v)))$$

を定義する. この character の well-defined 性は, $F_{\mathbb{A}}^{\times} \cap S_0(\mathfrak{N} \cap (v))$ 上で ε_{Δ}^v と写像

$$F_{\mathbb{A}}^{\times} / F^{\times} \rightarrow B^{\times}, \quad z \mapsto |z^{(\infty)}|_{\mathbb{A}}^{-2} z_v^{-2} \mathbf{1}_v \varepsilon_+(z)$$

が一致することにより保証されることに注意.

(ex4) とくに, $\varepsilon_{\Delta}^{\infty}$ は $\Delta_0(\mathfrak{N})$ 上で定義され, $(F_{\mathbb{A}}^{(\infty)})^{\times} \cap \Delta_0(\mathfrak{N})$ に制限すると, 写像

$$(F_{\mathbb{A}}^{(\infty)})^{\times} \cap \Delta_0(\mathfrak{N}) \rightarrow \mathbb{C}^{\times}, \quad z \mapsto \varepsilon_+(z_{\mathfrak{N}}) \varepsilon_2(\det(z^{(\mathfrak{N})}))$$

と一致するから, $\Delta_0^*(\mathfrak{N})$ を含む群の積 $(F_{\mathbb{A}}^{(\infty)})^{\times} \Delta_0(\mathfrak{N})$ の character

$$\underline{\varepsilon} : (F_{\mathbb{A}}^{(\infty)})^{\times} \Delta_0(\mathfrak{N}) \rightarrow \mathbb{C}^{\times},$$

$$z\delta \stackrel{\text{def}}{\mapsto} \varepsilon_+(z_{\mathfrak{N}}) \varepsilon_2(\det(z^{(\mathfrak{N})})) \varepsilon_{\Delta}^{\infty}(\delta) \quad (z \in (F_{\mathbb{A}}^{(\infty)})^{\times}, \delta \in \Delta_0(\mathfrak{N}))$$

は well-defined である. ここで, $z \in (F_{\mathbb{A}}^{(\infty)})^{\times}$ に対して, $z^{(\mathfrak{N})}$ は z の $\mathfrak{N}$ を割る素 ideal たちの外の部分を表す.

さて,

$$U(\hat{O}) := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \hat{O} \right\}$$

とおき, 各 $y \in \Delta_0(\mathfrak{N})$ に対して, $S_0(\mathfrak{N})$ による double coset の指数有限な左剰余類分解

$$S_0(\mathfrak{N}) y^t S_0(\mathfrak{N}) = \coprod_{u \in U(\hat{O}), t \in T_{\text{GL}}(F_{\mathbb{A}}^{(\infty)})} (ut) S_0(\mathfrak{N})$$

を取っておく. ここで, $t \in T_{\text{GL}}(F_{\mathbb{A}}^{(\infty)})$ は $\det(t) = \det(y)$ なるものを取っている. このとき, Hilbert cusp form $f \in S_{\kappa}(\mathfrak{N}, \varepsilon; \mathbb{C})$ に対して, $\text{GL}_2(F_{\mathbb{A}})$ 上の関数

$$f|[S_0(\mathfrak{N}) y^t S_0(\mathfrak{N})](g) := \sum_{u,t} \varepsilon_{\Delta}^{\infty}((ut)^t) f(gut)$$

$$= \underline{\varepsilon}(\det(y)) \sum_{u,t} \underline{\varepsilon}(ut)^{-1} f(gut) \quad (g \in \text{GL}_2(F_{\mathbb{A}}))$$

が u と t の選び方によらずに定まり,

$$f|[S_0(\mathfrak{N})y^t S_0(\mathfrak{N})] \in S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$$

となる.

Definition 5.3 ([8, Section 2.3.2]). F の各素 ideal $\mathfrak{q}$ に対し, 記号 $\begin{pmatrix} 1 & 0 \\ 0 & \varpi_{\mathfrak{q}} \end{pmatrix} \in \Delta_0(\mathfrak{N})$ で, $\mathfrak{q}$ -part は対角行列 $\begin{pmatrix} 1 & 0 \\ 0 & \varpi_{\mathfrak{q}} \end{pmatrix}$, その他の部分は trivial である元を表すことにする. $S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$ 上の Hecke operator として,

$$T(\varpi_{\mathfrak{q}}) := [S_0(\mathfrak{N}) \begin{pmatrix} 1 & 0 \\ 0 & \varpi_{\mathfrak{q}} \end{pmatrix} S_0(\mathfrak{N})]$$

とおく. また, 固定した二つの embedding $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ と $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ と可換な体の同型 $\overline{\mathbb{Q}}_p \xrightarrow{\sim} \mathbb{C}$ を一つ固定し, その同型を通して $\overline{\mathbb{Q}}_p^\times \xrightarrow{\sim} \mathbb{C}^\times$ とみなすことで,

$$T_p(\varpi_{\mathfrak{q}}) = \det \left(\begin{pmatrix} 1 & 0 \\ 0 & \varpi_{\mathfrak{q}} \end{pmatrix} \right)^{-\kappa_1} T(\varpi_{\mathfrak{q}})$$

とおく. また, $\mathfrak{q}|\mathfrak{N}$ であるときは, $\mathfrak{N}$ の prime-to- $\mathfrak{q}$ -part $\mathfrak{N}^{(\mathfrak{q})}$ が $\mathfrak{N}^{(\mathfrak{q})} \subset \mathfrak{c}(\varepsilon^-)$ となることを仮定して, 包含関係

$$S_\kappa(\mathfrak{N}^{(\mathfrak{q})}, \varepsilon; \mathbb{C}) \subset S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$$

に対して,

$$T(\varpi_{\mathfrak{q}})(S_\kappa(\mathfrak{N}^{(\mathfrak{q})}, \varepsilon; \mathbb{C})) \not\subset S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$$

となるので, $\mathfrak{q}$ での Hecke operator を区別するときは, $S_\kappa(\mathfrak{N}, \varepsilon; \mathbb{C})$ 上の Hecke operator $T(\varpi_{\mathfrak{q}})$ (resp. $T_p(\varpi_{\mathfrak{q}})$) を $U(\varpi_{\mathfrak{q}})$ (resp. $U_p(\varpi_{\mathfrak{q}})$) とかく.

とくに, $\kappa_1 = 0$ かもしれない $\mathfrak{q} \nmid p$ のときには,

$$T(\varpi_{\mathfrak{q}}) = T_p(\varpi_{\mathfrak{q}}), \quad U(\varpi_{\mathfrak{q}}) = U_p(\varpi_{\mathfrak{q}})$$

となることに注意.

Hecke operator と Fourier 展開との関係は次で与えられる:

Proposition 5.2 ([8, (2.3.16), (2.3.21)]). $\mathfrak{q}$ を F の素 ideal とする.

(1) $R \subset \mathbb{C}$ を ε の値と O^{Gal} を含む $\mathbb{Q}$ -algebra とする. R -係数の Hilbert cusp form $f \in S_\kappa(\mathfrak{N}, \varepsilon; R)$ に対し, もし $\mathfrak{q} \nmid \mathfrak{N}$ ならば,

$$\mathbf{a}_\infty(y, f|T(\varpi_{\mathfrak{q}})) = \mathbf{a}_\infty(y\varpi_{\mathfrak{q}}, f) + N_{F/\mathbb{Q}}(\mathfrak{q})\varepsilon_+(\varpi_{\mathfrak{q}})\mathbf{a}_\infty\left(\frac{y}{\varpi_{\mathfrak{q}}}, f\right) \quad (y \in F_{\mathbb{A}}^\times)$$

となる. ここで, $N_{F/\mathbb{Q}}$ は絶対ノルムを表す. 一方, $\mathfrak{q}|\mathfrak{N}$ ならば,

$$\mathbf{a}_\infty(y, f|T(\varpi_{\mathfrak{q}})) = \mathbf{a}_\infty(y\varpi_{\mathfrak{q}}, f) \quad (y \in F_{\mathbb{A}}^\times)$$

となる.

(2) $R \subset \mathbb{C}_p$ を $\mathcal{O}$ -algebra とする. R -係数の Hilbert cusp form $f \in S_\kappa(\mathfrak{N}, \varepsilon; R)$ に対し, もし $\mathfrak{q} \nmid p\mathfrak{N}$ ならば,

$$\mathbf{a}_p(y, f|T_p(\varpi_{\mathfrak{q}})) = \mathbf{a}_p(y\varpi_{\mathfrak{q}}, f) + N_{F/\mathbb{Q}}(\mathfrak{q})\varepsilon_+(\varpi_{\mathfrak{q}})\mathbf{a}_p\left(\frac{y}{\varpi_{\mathfrak{q}}}, f\right) \quad (y \in F_{\mathbb{A}}^\times)$$

となり, $\mathfrak{q}|p\mathfrak{N}$ ならば,

$$\mathbf{a}_p(y, f|T_p(\varpi_{\mathfrak{q}})) = \mathbf{a}_p(y\varpi_{\mathfrak{q}}, f) \quad (y \in F_{\mathbb{A}}^\times)$$

となる.

Definition 5.4. 以上の記号のもと,

$$p|\mathfrak{N} \quad \text{or} \quad [\kappa] \geq 0$$

と仮定し, R を Proposition 5.2 の (1) と (2) のいずれかのものとすれば, Proposition 5.2 により, R -係数の Fourier 展開は Hecke operator $T_p(\varpi_{\mathfrak{q}})$ たちの作用のもとで, 再び R -係数となることがわかる. このとき, R -係数の Hilbert cusp form の空間 $S_\kappa(\mathfrak{N}, \varepsilon; R)$ に作用する Hecke algebra を,

$$h_\kappa(\mathfrak{N}, \varepsilon; R) := R[T_p(\varpi_{\mathfrak{q}}) \mid \mathfrak{q} : \text{prime}] \subset \text{End}_R(S_\kappa(\mathfrak{N}, \varepsilon; R))$$

と定義する. 実は, $y \in \hat{O} \cap (F_{\mathbb{A}}^{(\infty)})^\times$ に対して, しかるべき $T_p(\varpi_{\mathfrak{q}})$ たちの $\mathbb{Z}$ -係数の多項式としてかけられる Hecke operator $T_p(y) \in h_\kappa(\mathfrak{N}, \varepsilon; R)$ を定義することができる. ここでは, $T_p(y)$ の定義は省略することにする. 詳しくは, [8, Section 2.3.4] を参照のこと.

Hilbert cusp form の空間とそれに作用する Hecke algebra の間の duality は, Fourier 係数を用いて次のように与えられる:

Theorem 5.3 ([8, Theorem 2.28]). 以上の記号のもと, A を $\mathcal{O}$ -algebra とする. A -係数の Hilbert cusp form の空間とそれに作用する Hecke algebra をそれぞれ

$$\begin{aligned} S_\kappa(\mathfrak{N}, \varepsilon; A) &:= S_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O}) \otimes_{\mathcal{O}} A, \\ h_\kappa(\mathfrak{N}, \varepsilon; A) &:= h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O}) \otimes_{\mathcal{O}} A \end{aligned}$$

と定義する. このとき, A -module としての同型

$$\text{Hom}_A(h_\kappa(\mathfrak{N}, \varepsilon; A), A) \xrightarrow{\sim} S_\kappa(\mathfrak{N}, \varepsilon; A), \quad \varphi \mapsto f_\varphi$$

で, 関係式

$$\mathbf{a}_p(y, f_\varphi) = \varphi(T_p(y)) \quad (y \in \hat{O} \cap (F_{\mathbb{A}}^{(\infty)})^\times)$$

を満たすものが存在する. Proposition 5.2 (2) により,

$$\mathbf{a}_p(1, f_\varphi|T_p(y)) = \mathbf{a}_p(y, f_\varphi)$$

となるので, とくに φ が A -algebra 準同型であるときには, f_φ として $\varphi(T_p(y))$ を $T_p(y)$ -固有値にもつ $h_\kappa(\mathfrak{N}, \varepsilon; A)$ に関する Hecke eigenform が対応することとなる.

Remark 5.5. $\mathfrak{m}_\mathcal{O}$ を $\mathcal{O}$ の極大 ideal とする. 自然な同一視

$$h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O}) = \varprojlim_n h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O}) \otimes_{\mathcal{O}} (\mathcal{O}/\mathfrak{m}_\mathcal{O}^n)$$

が成り立ち, 各 n に対し $h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O}) \otimes_{\mathcal{O}} (\mathcal{O}/\mathfrak{m}_\mathcal{O}^n)$ が有限環であることが知られている. よって, $h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O})$ に profinite 位相を入れることができる.

5.3. Modular Galois representations

この Subsection では, しかるべき mod p Galois 表現 $\bar{\rho}$ に対して, Hilbert cusp form に付随する deformation を支配する $\bar{\rho}$ の universal deformation ring として Hecke algebra をみなせることが期待されることについて少し触れながら, Hecke algebra の素 ideal による商環を係数とした Hilbert cusp form に付随する Galois 表現について, [8, Sections 2.3.4 and 2.3.8] に沿って紹介する. 引き続き, 前節の記号を用いることにする.

Definition 5.5. A を $\mathcal{O}$ -algebra とし, $f \in S_\kappa(\mathfrak{N}, \varepsilon; A)$ を $h_\kappa(\mathfrak{N}, \varepsilon; A)$ に関する Hecke eigenform とする. f の Hecke 固有値はすべて A に含まれていると仮定する. このとき,

$$\rho : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(A)$$

が f に付随する modular な Galois 表現であるとは, 次の二つの条件を満たすことである:

- (i) ρ は $p\mathfrak{N}$ と ∞ の外で不分岐である;
- (ii) $p\mathfrak{N}$ を割らない F の任意の素 ideal $\mathfrak{l}$ に対し, f の $T_p(\varpi_{\mathfrak{l}})$ -固有値は $\text{Tr}(\rho(\text{Frob}_{\mathfrak{l}}))$ と一致する.

ここで, $\mathcal{O}$ の剰余体を $\mathbb{F}$ として,

$$\bar{\rho} : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(\mathbb{F})$$

を, ある Hecke eigenform $\bar{f} \in S_\kappa(\mathfrak{N}; \varepsilon; \mathbb{F})$ に付随する mod p Galois 表現とする. Theorem 5.3 により, $h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O})$ の適当な完備局所化 $h_{\bar{\rho}}$ は, $\bar{\rho}$ の deformation のうち weight κ , level $\mathfrak{N}$, character ε の Hecke eigenform に付随するものたちを支配する modular な universal deformation ring とみなせることが期待できる. その際, 存在すべき $\bar{\rho}$ の $h_{\bar{\rho}}$ への universal deformation

$$\boldsymbol{\rho} : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(h_{\bar{\rho}})$$

は, $p\mathfrak{N}$ を割らない F の素 ideal $\mathfrak{l}$ に対し,

$$\text{Tr}(\boldsymbol{\rho}(\text{Frob}_{\mathfrak{l}})) = T_p(\varpi_{\mathfrak{l}})$$

を満たすべきものである.

Remark 5.6. しかるべき条件のもとで, このような modular な universal deformation ρ が構成され, $\bar{\rho}$ に対する変形条件を強めたある universal deformation ring と $h_{\bar{\rho}}$ が同一視されることが, Wiles [13]-Taylor-Wiles [11] や Fujiwara [3] などにより知られている.

以下, 実際に modular な Galois 表現が存在することを, 証明を省略して概観する (詳しくは, [8, Section 2.3.8] を参照のこと). $h_{\kappa}(\mathfrak{N}, \varepsilon; \mathcal{O})$ の素 ideal P に対し, 整域 $h_{\kappa}(\mathfrak{N}, \varepsilon; \mathcal{O})/P$ の商体を $k(P)$ とかくことにする. Theorem 5.3 において $A = k(P)$ とすれば, $k(P)$ -係数の Hecke eigenform f_P で, F の任意の素 ideal $\mathfrak{q}$ に対し, $T_p(\varpi_{\mathfrak{q}})$ -固有値が $T_p(\varpi_{\mathfrak{q}})(\bmod P)$ と一致するものが存在する. このとき, f_P に付随する modular な Galois 表現が存在する:

Theorem 5.4 ([8, Theorem 2.43]). 以上の記号のもと, $k(P)$ の標数は 2 でないと仮定する. また, すべての $\sigma \in I$ に対し $\kappa_{2,\sigma} - \kappa_{1,\sigma} \geq 0$ であると仮定し, $k := \kappa_2 - \kappa_1 + 1 \in \mathbb{Z}[I]$ とおく.

(1) このとき, 連続で semi-simple な Galois 表現

$$\rho_P : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(k(P))$$

で, 次の四つの条件を満たすものが存在する:

- (i) ρ_P は $p\mathfrak{N}$ と ∞ の外で不分岐である;
- (ii) $p\mathfrak{N}$ を割らない F の任意の素 ideal $\mathfrak{l}$ に対して,

$$\text{Tr}(\rho_P(\text{Frob}_{\mathfrak{l}})) = T_p(\varpi_{\mathfrak{l}}) \pmod{P}$$

を満たす. また, $\mathcal{N}_p$ を p -adic cyclotomic character とし, 類体論により ε_+ を Galois character とみなすことで,

$$\det(\rho_P) = \varepsilon_+ \mathcal{N}_p^{[\kappa]}$$

が得られる;

(iii) $\mathfrak{m}$ を P を含む $h_{\kappa}(\mathfrak{N}, \varepsilon; \mathcal{O})$ の極大 ideal とする. もし「 $\kappa_2 - \kappa_1 - 1 \geq 0$ かつ $T_p(p) \notin \mathfrak{m}$ である」かもしくは「 $k = 21$ かつ $T_p(\varpi_{\mathfrak{p}}) \notin \mathfrak{m}$ なる p を割る素 ideal $\mathfrak{p}$ がある」ならば,

$$\rho_P|_{D_{\mathfrak{p}}} \sim \begin{pmatrix} \epsilon_{\mathfrak{p}} & * \\ 0 & \delta_{\mathfrak{p}} \end{pmatrix}$$

とかける. この表示において, $D_{\mathfrak{p}}$ は $\mathfrak{p}$ における分解群, $\epsilon_{\mathfrak{p}}$ と $\delta_{\mathfrak{p}}$ は $D_{\mathfrak{p}}$ の character をそれぞれ表しており, とくに $\delta_{\mathfrak{p}}$ は,

$$\delta_{\mathfrak{p}}([y, F_{\mathfrak{p}}]) = U_p(y) \pmod{P} \quad (y \in F_{\mathfrak{p}}^{\times})$$

となるものである. ここで, F の素 ideal $\mathfrak{q}$ に対して $I_{\mathfrak{q}}$ を $\mathfrak{q}$ での惰性群としたうえで, 記号 $[\cdot, F_{\mathfrak{q}}]$ は

$$[\varpi_{\mathfrak{q}}, F_{\mathfrak{q}}] \pmod{I_{\mathfrak{q}}} = \text{Frob}_{\mathfrak{q}}$$

と正規化された Atrin symbol を表すものとする. また, Hecke operator $U_p(y)$ を

$$U_p(y) := [S_0(p^\infty \mathfrak{N}) \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} S_0(p^\infty \mathfrak{N})]$$

と定義した. とくに, Proposition 5.1 と Proposition 5.2 により,

$$\delta_{\mathfrak{p}}([u, F_{\mathfrak{p}}]) = (\varepsilon_1)_{\mathfrak{p}}(u) u^{-\kappa_1} \quad (u \in O_{\mathfrak{p}}^\times)$$

となることに注意;

(iv) $\mathfrak{N} = \mathfrak{N}_0 \mathfrak{c}(\varepsilon^-)$ とおく. もし, $\mathfrak{N}_0$ の prime-to- p -part $\mathfrak{N}_0^{(p)}$ が square free で $\mathfrak{c}(\varepsilon^-)$ と互いに素ならば, $\mathfrak{N}_0^{(p)}$ を割る F の任意の素 ideal $\mathfrak{q}$ に対して,

$$\rho_P|_{D_{\mathfrak{q}}} \sim \begin{pmatrix} \epsilon_{\mathfrak{q}} & * \\ 0 & \delta_{\mathfrak{q}} \end{pmatrix}$$

とかける. ここで, $\epsilon_{\mathfrak{q}}$ と $\delta_{\mathfrak{q}}$ は $\mathfrak{q}$ での分解群 $D_{\mathfrak{q}}$ の character であり, とくに $\delta_{\mathfrak{q}}$ は,

$$\delta_{\mathfrak{q}}([y, F_{\mathfrak{q}}]) = T_p(y) \pmod{P} \quad (y \in F_{\mathfrak{q}}^\times)$$

を満たす. このとき, $u \in O_{\mathfrak{q}}^\times$ について,

$$\delta_{\mathfrak{q}}([u, F_{\mathfrak{q}}]) = (\varepsilon_1)_{\mathfrak{q}}(u)$$

となることに注意.

(2) もし ρ_m が絶対既約であれば,

$$\rho_P : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O})/P)$$

のように ρ_P の値を $\text{GL}_2(h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O})/P)$ に取らせることができ, ρ_P は $h_\kappa(\mathfrak{N}, \varepsilon; \mathcal{O})/P$ 上の同値の差を除き一意に存在する.

References

- [1] H. Carayol, Formes modulaires et représentations galoisiennes à valeurs dans un anneau local compact, Contemporary Math. **165** (1994), 213-237.
- [2] B. de Smit and H. W. Lenstra, Jr, Explicit construction of universal deformation rings, in “Modular Forms and Fermat’s Last Theorem” (G. Cornell, J. H. Silverman and G. Stevens, Editors), Springer, 1997, 313-326.
- [3] K. Fujiwara, Deformation rings and Hecke algebras in totally real case, preprint, 1999.
- [4] H. Hida, *Elementary Theory of L-functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, 1993.
- [5] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, 2000.
- [6] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, Singapore, 2000.
- [7] H. Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, Springer, 2004.
- [8] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, Oxford Mathematical Monographs, Oxford Science Publications, 2006.

- [9] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1989.
- [10] B. Mazur, Deforming Galois representations, in “Galois Group over $\mathbb{Q}$ ”, MSRI publications **16** (1989), 385-437.
- [11] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, Ann. of Math. **141** (1995), 553-572.
- [12] A. Wiles, On ordinary Λ -adic representations associated to modular forms, Invent. Math. **94** (1988), 529-573.
- [13] A. Wiles, Modular elliptic curves and Fermat’s last theorem, Ann. of Math. **141** (1995), 443-551.

DEPARTMENT OF MATHEMATICS, KYOTO SANGYO UNIVERSITY, KYOTO, 606-8502, JAPAN

E-mail address: ayama30@cc.kyoto-su.ac.jp

コホモロジー論とモチーフ

伊藤 哲史¹

1. はじめに

本稿は2006年夏に北海道大学大学院理学研究院で行われた「整数論札幌夏の学校」における著者の講義²をもとにしている．講義の目的は，主に整数論を専攻とする学部生や大学院生を対象に，整数論における「モチーフ的な考え方」の重要性を解説することであった．

今日では，整数論のみならず，数学のありとあらゆる分野において細分化・専門化が進んでしまっている．多くの学生にとっては，“自分の分野”を勉強するのに精一杯で，関連する他分野のことになど構ってられないというのが実情かもしれない．しかし，早い段階で Grothendieck により創始された「モチーフ的な考え方」に触れておくことは様々な理論・対象を統一的な視点から眺め，具体的な問題に対する本質的なアプローチを探るためにも大切なことであると思われる．歴史的に見ても，整数論における深遠な理論・定理の中には，「モチーフ的な考え方」に強い影響を受けているものも多い．

表題のコホモロジーとは，位相幾何学において，図形の「形」を表す群やベクトル空間である． X を「 g 人乗りの浮き輪」



¹京都大学大学院理学研究科数学教室 (email: tetsushi@math.kyoto-u.ac.jp)

フランス高等科学研究所 (IHES) (email: tetsushi@ihes.fr)

2006年9月4日(月)～7日(木) (13:30～15:00)

²講義のタイトルは「コホモロジー論とモティーフ」だったが，“motive”の日本語表記としては「モチーフ」がより一般的だと思われるので，本稿では「モチーフ」で統一することにした．

とすると、 X の（特異）コホモロジーは次のようになる．

$$H^i(X, \mathbb{Z}) \cong \begin{cases} \mathbb{Z} & i = 0 \\ \mathbb{Z}^{\oplus 2g} & i = 1 \\ \mathbb{Z} & i = 2 \\ 0 & (\text{それ以外}) \end{cases}$$

i をコホモロジーの**次数**という³．図からも分かるように、 X 上には $2g$ 個の「1 次元的なサイクル」があり、それに対応して、 $H^1(X, \mathbb{Z})$ の階数は $2g$ となる．左辺の $\mathbb{Z}$ は**係数**であり、 $\mathbb{Z}$ の代わりに $\mathbb{Q}, \mathbb{C}$ などの群を係数としたコホモロジーを考えることもできる．閉曲面 X に対しては、その結果は上式の両辺の $\mathbb{Z}$ を $\mathbb{Q}, \mathbb{C}$ で置き換えたものに等しい⁴．また、より一般に、**局所系**や**層**を係数としたコホモロジーを考えることもできる．位相空間 X に対して、 $\mathbb{Q}$ 上のベクトル空間 $H^i(X, \mathbb{Q})$ の次元 $b_i(X)$ は、 X の i 次 **Betti 数**と呼ばれ、 X 上の「 i 次元的なサイクル」の「個数」を表す最も基本的な位相的不変量の一つである．

本稿のテーマの一つは、**エタールコホモロジー**である．これは、上に述べた位相幾何学におけるコホモロジーの代数幾何的類似であり、Hasse や Weil による有限体上の代数多様体のゼータ関数（**Hasse-Weil ゼータ関数**）の研究を踏まえて、Grothendieck によって 1960 年代に創始された理論である．位相幾何学において、コホモロジーが位相空間の「形」を表していたのと同様に、エタールコホモロジーも代数多様体の（抽象化された意味での）「形」を表していると考えられる．特筆すべきことは、エタールコホモロジーの理論は任意の代数多様体（より一般に任意のスキーム）に対して適用可能なことである．そして、 X を体 K 上の代数多様体とすると、 $\bar{K}$ 上の代数多様体 $X \otimes_K \bar{K}$ のエタールコホモロジー $H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$ は $\mathbb{Q}_\ell$ 上の有限次元ベクトル空間であり（ ℓ は K で可逆な素数． $\mathbb{Q}_\ell$ は $\mathbb{Q}$ の ℓ 進完備化），自然に K の絶対 Galois 群 $\text{Gal}(\bar{K}/K)$ が作用する．すなわち、

『エタールコホモロジーを用いることで、代数多様体から Galois 表現（ ℓ 進表現）を作ることができる』

のである．これは保型形式と Galois 表現の対応（Langlands 対応、非可換類体論の一種）への応用上も重要である．また、有限体の代数的閉包上の代数多様体のエタールコホモロジーを用いることで、**Weil 予想**（有限体上の代数多様体に対する Riemann

³次元ということもあるが、まぎらわしいので、本稿では「次数」で統一する．

⁴一般の位相空間 X に対しては、コホモロジー $H^i(X, \mathbb{Z})$ が捩れ元を持つことがあり、その結果は若干複雑になるが、**普遍係数定理**により計算される．詳しくは、[Hat] などの位相幾何学の教科書を参照．

予想の類似) という整数論の問題を, 位相幾何学的なアイデア・手法により研究することが可能になる.

本稿のもう一つのテーマは**モチーフ**である. これは, 代数多様体 (より一般にスキーム) のコホモロジーや, ゼータ関数, 代数的サイクルなどを統一的に扱うための土台となるもので, Grothendieck によって考案された概念である. Grothendieck は**スタンダード予想**と呼ばれる予想を提出し, その予想を用いて代数多様体を代数的サイクルによって “分解” することで, モチーフを「定義」した. そして, **Weil 予想が自然に導かれる**ことを示した. しかし, スタンダード予想自身は今日でも未解決であり, その意味で, モチーフの理論は現在もなお「未完成の理論」であるといえる.

本稿は (この「はじめに」を除くと) 次の 4 つの節からなり, 「整数論札幌夏の学校」における 4 日間の講義内容にほぼ対応している.

§2. 保型形式と Galois 表現

§3. Weil 予想とエタールコホモロジー

§4. Grothendieck の夢 — スタンダード予想とモチーフの理論, Weil 予想, Jannsen の定理

§5. 整数論における「モチーフ的な考え方」

講義の最終日には, 最近の話題として, Wiles による Fermat の最終定理の証明や, 最近の Taylor らによる佐藤 - テイト予想の (多くの場合の) 証明の中に, 「モチーフ的な考え方」がどのように使われるかを解説したが, これについては §5 で簡単に述べるにとどめた. 佐藤 - Tate 予想やそれに関連する話題については, [Tanoshimi] に詳しく書かれる予定であるので, 興味を持たれた読者はそちらを参照していただきたい. また, 本稿の終わりに本稿の内容と関連した演習問題と参考文献を挙げておいた. これをきっかけにさらに勉強・研究を進めていただければ幸いである.

最後に, 本稿で扱っていない事項について簡単に述べておく. 本稿で「エタールコホモロジー」といえば, ほとんどの場合, 代数的閉体上の代数多様体に対する定数層 $\mathbb{Q}_\ell$ (ℓ は基礎体で可逆な素数) を係数とするエタールコホモロジーのことである. 実は, エタールコホモロジーの理論は, 任意のスキームに対して展開できる. 体の Spec のエタールコホモロジーを考えることで Galois コホモロジーの理論と繋がり, 整数論への応用上も重要である. しかし, 本稿ではこれについては一切触れなかった⁵. これ以外にも本稿で触れていない (触れることができなかった) 重要なテーマとしては,

⁵これは, 位相幾何学におけるコホモロジーと, 体論における Galois コホモロジーはかなり雰囲気が異なるものであり, 一緒に述べない方が分かりやすいだろうと考えたからである.

次のようなものがある：エタール基本群の理論，エタール ℓ 進層の理論，「重さ」の理論，三角和への応用，偏屈層の理論，Hodge 理論との類似，有限 Chevalley 群の表現論への応用，保型表現に伴う Galois 表現・志村多様体・Langlands 対応への応用，代数的サイクル・Chow 群への応用，代数多様体の周期との関係，混合モチーフの理論，モチヴィックコホモロジー，ゼータ関数の特殊値・代数的 K 理論との関係など．これらについて興味をもたれた読者は，[EGA], [SGA] はもちろんのこと，興味に応じて [Corvallis], [AnnArbor], [Seattle], [Toronto], [A1] などの参考文献に進んでいただければ幸いである．

エタールコホモロジーやモチーフという広大なテーマをこのような小文で解説し尽くすことはもちろんできないし，そのようなことは目指していない．いろいろと不備もあると思うが，必要に応じて参考文献などで補っていただきたい．本稿が整数論や数論幾何を勉強している学生や，これから勉強しようという人々の助けに少しでもなれば幸いである．

2008 年 3 月 マリーの森⁶にて 著者記す．

謝辞．「整数論札幌夏の学校」の参加者の皆様には，講義中やそれ以外の時間を通して質問・コメントをいただきました．特に，肥田晴三氏（UCLA），田口雄一郎氏（九州大）からは，保型形式や Galois 表現に関する有意義なコメントをいただきました．また，谷口隆氏（愛媛大），千田雅隆氏（東北大）には講義ノートの詳細にとっていただき，本稿を執筆する際の参考にさせていただきました．また，最後になりましたが，講演の機会をいただいた前田芳孝先生（北海道大）に感謝するとともに，著者の遅筆により本稿の完成が大変遅れてしまったことをお詫びします．

⁶Le Bois-Marie. Grothendieck によるセミナー [SGA] が行われた場所．フランス高等科学研究所 (IHES) があるが，それ以外には何も無い．

2. 保型形式と GALOIS 表現

本節では、エタールコホモロジーやモチーフの理論への動機付けとして、保型形式と Galois 表現 (Artin 表現, ℓ 進表現, $\text{mod } \ell$ 表現) について簡単に復習し, 「保型形式に伴う ℓ 進表現」について述べる.

2.1. 保型形式の定義. ここでは, 保型形式の定義を簡単に復習する. (詳しくは, [Se5], [Sh], [Miy], [DiS] などの保型形式の教科書を参照.)

整数を成分とする行列式が 1 の 2 次正方行列全体を $SL_2(\mathbb{Z})$ とおく. 整数 $N \geq 1$ に対し, $SL_2(\mathbb{Z})$ の部分群 $\Gamma_0(N)$ を次のように定める.

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

$\mathbb{H} := \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$ を複素上半平面, $\varepsilon: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ を準同形 (**Dirichlet 指標**) とする. k を整数であつて, $\varepsilon(-1) = (-1)^k$ をみたすものとする⁷.

定義 2.1 (保型形式). $\Gamma_0(N)$ に関する (k, ε) -型の**保型形式**⁸とは, 複素上半平面 $\mathbb{H}$ 上の正則関数 f であつて,

$$\text{任意の } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \text{ に対し, } f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z)$$

をみたし, 無限遠点で正則なものをいう. N, k, ε をそれぞれ f の**レベル**, **重さ**, **指標**という.

「無限遠点で正則」の意味を説明しよう. $\gamma \in SL_2(\mathbb{Z})$ に対し

$$(f|_k \gamma)(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

とおく. $f|_k \gamma$ は再び $\mathbb{H}$ 上の正則関数となり $(f|_k \gamma)(z+N) = (f|_k \gamma)(z)$ をみたす. したがって,

$$(f|_k \gamma)(z) = \sum_{n=-\infty}^{\infty} \varphi(f, k, \gamma, n) e^{2\pi i n z / N}, \quad \varphi(f, k, \gamma, n) \in \mathbb{C}$$

という形に展開できる. 条件「 $n < 0 \Rightarrow \varphi(f, k, \gamma, n) = 0$ 」が任意の $\gamma \in SL_2(\mathbb{Z})$ に対してなりたつとき, f は**無限遠点で正則**であるという. さらに強く, 条件「 $n \leq 0 \Rightarrow$

⁷条件 $\varepsilon(-1) = (-1)^k$ をみたさない場合でも, 「保型形式」を定義することはできるが, その場合は $f(z) = 0$ となってしまう.

⁸ここでいう保型形式とは “modular form” の訳語である. “modular form” をモジュラー形式と訳し, より一般の群に対する “automorphic form” を保型形式と訳し分けることも多いが, 本稿では両者を特に区別せずに「保型形式」と呼ぶことにする.

$\varphi(f, k, \gamma, n) = 0$ 」が任意の $\gamma \in SL_2(\mathbb{Z})$ に対してなりたつとき、 f は**尖点的**であるという。

N' を N の約数で、 $N \neq N'$ とする。 f を $\Gamma_0(N')$ に関する保型形式とし、 $a \geq 1$ を aN' が N を割り切るような正整数とすると、 $f(az)$ は $\Gamma_0(N)$ に関する保型形式となる。 $\Gamma_0(N)$ に関する保型形式のうち、このようにしてレベルの小さい保型形式から得られる保型形式の線形結合で表される保型形式を**旧形式**という。 **Petersson 内積**

$$\langle f, g \rangle := \int_D f(z) \overline{g(z)} y^{k-2} dx dy$$

(D は $\Gamma_0(N)$ の $\mathbb{H}$ への作用の基本領域) によって旧形式の空間と直交している保型形式を**新形式**という。(レベル N で初めて現れる「新しい」保型形式という意味である。 §2.7 で述べる原始 Dirichlet 指標の類似である。)

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$ であるから、 $f(z+1) = f(z)$ がなりたつ。 したがって、 f は $q = \exp(2\pi iz)$ の関数として

$$f = \sum_{n=0}^{\infty} a_n q^n$$

という形に展開できる (q 展開)。 q の負べきの項が消えるのは、 f が無限遠点で正則であることの帰結である。 f が尖点的であれば、 $a_0 = 0$ である。 $a_1 = 1$ がなりたつとき、 f は**正規化されている**という。

保型形式の空間には **Hecke 作用素**と呼ばれる作用素が作用している。 Hecke 作用素は N を割らない素数 p に対する

$$T_p: f = \sum_n a_n q^n \mapsto T_p f := \sum_n a_{pn} q^n + \varepsilon(p) p^{k-1} \sum_n a_n q^{pn}$$

および N を割り切る素数 p に対する

$$U_p: f = \sum_n a_n q^n \mapsto U_p f := \sum_n a_{pn} q^n$$

がある。

保型形式の理論の中では、正規化されている尖点的な保型形式 $f = \sum_{n=1}^{\infty} a_n q^n$ であって、レベル N の新形式であり、さらに Hecke 作用素の同時固有関数となっているものが特に重要である。このとき、Hecke 作用素 T_p (または U_p) の固有値が、 f の q 展開における q^p の係数 a_p に等しいことが分かる。($T_p f$ や $U_p f$ の q 展開における q の 1 次の項の係数を見よ。) f の **L 関数**が Dirichlet 級数

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

によって定義される. f が Hecke 作用素の同時固有関数であることを用いると, $L(s, f)$ は **Euler 積**

$$L(s, f) = \prod_{p \text{ は } N \text{ を割らない}} \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s}} \cdot \prod_{p \text{ は } N \text{ を割り切る}} \frac{1}{1 - a_p p^{-s}}$$

を持つことが分かる. さらに $L(s, f)$ は s の実部 $\operatorname{Re}(s)$ が十分大きい領域で絶対収束し, 複素平面全体に正則関数として解析接続され, $s \leftrightarrow k - s$ という形の関数等式をみたす.

2.2. 保型形式の例 (1). Ramanujan の Δ 関数

$$\begin{aligned} \Delta &= q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + \cdots \end{aligned}$$

は最も基本的で重要な尖点的保型形式である. Δ はレベル 1, 重さ 12 の保型形式であり, レベル 1 の尖点的保型形式の中では最も重さが小さい. (尖点的でない保型形式としては Eisenstein 級数などがある.) モジュライ理論的には Δ は楕円曲線の「判別式」に対応しており, 整数論のみならず, 複素関数論, 代数幾何学, 数理論理学, 組み合わせ論などにも現れる重要な対象である. その q 展開の係数 $\tau(n)$ は Ramanujan の τ 関数と呼ばれており興味深い性質を持っている. (そのうちのいくつかは, Δ に伴う ℓ 進表現を用いることで鮮やかに説明・証明することができる ([Se3]).)

Ramanujan の τ 関数は, 定義は単純だが, その具体的な性質の証明は難しい. $L(s, \Delta)$ が Euler 積を持つことを用いて, $\tau(n)$ が関係式

- $n, m \geq 1$ が互いに素なら, $\tau(nm) = \tau(n)\tau(m)$.
- 素数 p , 整数 $a \geq 0$ に対し, $\tau(p^{a+2}) = \tau(p)\tau(p^{a+1}) - p^{11}\tau(p^a)$

をみたすことが示される (Mordell). 有名な **Ramanujan 予想**

$$\text{任意の素数 } p \text{ に対し, } |\tau(p)| \leq 2p^{11/2}$$

は二項係数の和に関する初等的な主張であるにも関わらず, 初等的証明はいまだに知られていない. (p のべきに現れる 11 は, Δ の重さ 12 から 1 を引いたものに等しい.) Ramanujan 予想の今日知られている唯一の証明は, 久賀 - 佐藤多様体を用いて Weil 予想に帰着させる Deligne によるものである. (§3.8 を参照.)

2.3. 保型形式の例 (2). もう一つ例を挙げよう.

$$\begin{aligned} f &= q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots \end{aligned}$$

重さ 2, レベル 11 の自明な指標に関する保型形式である⁹. f の q 展開を

$$f = \sum_{n=1}^{\infty} a_n q^n$$

とおく. 素数 $p \neq 11$ に対し, 楕円曲線

$$E : Y^2 Z + Y Z^2 = X^3 - X Z^2$$

の mod p 還元 $\mathbb{F}_p$ -有理点の個数を $\#E(\mathbb{F}_p)$ とおくと,

$$a_p(E) = 1 + p - \#E(\mathbb{F}_p)$$

がなりたつ. このことは, f に伴う Galois 表現が, 楕円曲線 E の ℓ 進 Tate 加群 (の双対) を用いて作られることを意味する. (例 2.9, 定理 2.10 を参照.) これは **谷山 - 志村予想** の特別な場合である. また **Hasse の定理** (例 3.6 を参照) を用いることで, f に対する Ramanujan 予想の類似 (**Ramanujan-Petersson 予想**)

$$\text{任意の素数 } p \text{ に対し, } |a_p| \leq 2\sqrt{p}$$

が得られる.

2.4. **Galois 表現の定義**. ここでは Galois 表現とその L 関数について簡単に述べる. (詳しくは, [Se4], [Se6], [Se7], [Tay3] など参照. 特に, Taylor による ICM 講演録 [Tay3] は, 最新の結果も踏まえて分かりやすく書かれている.)

以下, ℓ を素数とする.

定義 2.2 (Galois 表現). K を体とし, $\text{Gal}(\overline{K}/K)$ を K の絶対 Galois 群とする. E を複素数体 $\mathbb{C}$, ℓ 進体 ($\mathbb{Q}_\ell$ の有限次拡大), 有限体のいずれかとし, V を体 E 上の有限次元ベクトル空間とする. K の **Galois 表現** とは, 連続準同形

$$\rho: \text{Gal}(\overline{K}/K) \longrightarrow GL(V)$$

のことをいう. ここで, $\text{Gal}(\overline{K}/K)$ は Krull 位相に関するコンパクト位相群である. また, E が有限体か複素数体のときは, $GL(V)$ に離散位相を入れて考える. E が ℓ 進体のときは, $GL(V)$ に ℓ 進位相を入れて考える.

⁹ここでは無限積展開を持つ保型形式を挙げたが, 一般の保型形式はこのような無限積展開を持つわけではない.

ρ が**既約**とは、0 でも ρ 自身でもない部分表現が存在しないことをいう。また、表現 $\rho \otimes_E \bar{E}$ が既約のとき、 ρ は**絶対既約**であるという。

E が複素数体のとき、 ρ を **Artin 表現**という。 E が ℓ 進体のとき、 ρ を ℓ **進表現**という。 E が標数 ℓ の有限体のとき、 ρ を **mod ℓ 表現**という。Artin 表現や mod ℓ 表現の像は常に有限群である。したがって、Artin 表現や mod ℓ 表現を考えることと、有限次 Galois 拡大 L/K と埋め込み $\varphi: \text{Gal}(L/K) \hookrightarrow GL(V)$ の組 $(L/K, \varphi)$ を考えることは同値である。一般に、 ℓ 進表現の像は有限とは限らない。体同形 $\bar{\mathbb{Q}}_\ell \cong \mathbb{C}$ を固定し¹⁰、像が有限な ℓ 進表現を Artin 表現と同一視することも多い。

ρ を体 K の ℓ 進表現とする。 $\text{Gal}(\bar{K}/K)$ はコンパクト群なので、その ρ による像もコンパクトである。したがって、 V の基底をうまくとると、

$$\rho: \text{Gal}(\bar{K}/K) \longrightarrow GL_d(O_E) \subset GL_d(E)$$

となる。 $(V$ の次元を d とおいた。 O_E は E の整数環。) m_E を O_E の極大イデアルとすると、この写像の mod m_E を考えることで、mod ℓ 表現

$$\bar{\rho}: \text{Gal}(\bar{K}/K) \longrightarrow GL_d(O_E/m_E) = GL_d(\kappa_E)$$

が得られる。 $(\kappa_E = O_E/m_E$ は E の剰余体。) $\bar{\rho}$ を ρ の**剰余表現**という。一般に、 ρ が既約であっても $\bar{\rho}$ が既約とは限らない。また、 $\bar{\rho}$ は ρ から一意的に決まるとは限らないが (V の基底の取り方によるかもしれない)、半単純化 $\bar{\rho}^{\text{ss}}$ の同値類は ρ から一意的に決まる。これは、各 $\sigma \in \text{Gal}(\bar{K}/K)$ に対して、 $\bar{\rho}^{\text{ss}}(\sigma)$ の固有多項式が $\rho(\sigma)$ の固有多項式の mod m_E に等しいことから分かる¹¹。特に剰余表現 $\bar{\rho}$ の同値類は、もし既約であれば、 ρ から一意的に決まる。

整数論においては、代数体の Galois 表現が特に重要である。 K を代数体とし、簡単のため各素点 v に対し、 K 上の埋め込み $\bar{K} \hookrightarrow \bar{K}_v$ を固定する (K_v は v における K の完備化)。これにより、

$$\text{Gal}(\bar{K}_v/K_v) \subset \text{Gal}(\bar{K}/K)$$

と思えるから、 K の Galois 表現 ρ に対し、その $\text{Gal}(\bar{K}_v/K_v)$ への制限 $\rho_v := \rho|_{\text{Gal}(\bar{K}_v/K_v)}$ が考えられる。 v を有限素点とし、剰余体を $\kappa(v)$ とおくと、完全系列

$$1 \longrightarrow I_v \longrightarrow \text{Gal}(\bar{K}_v/K_v) \longrightarrow \text{Gal}(\bar{\kappa}(v)/\kappa(v)) \longrightarrow 1$$

¹⁰ $\bar{\mathbb{Q}}_\ell$ も $\mathbb{C}$ も連続濃度を持つ代数的閉体だから、Zorn の補題により、体としては同形である。

¹¹ $\bar{\rho}^{\text{ss}}$ の同値類は各 $\sigma \in \text{Gal}(\bar{K}/K)$ の固有多項式 $\det(T - \bar{\rho}^{\text{ss}}(\sigma))$ で決まる。標数 0 の体上の表現と異なり、各 σ の跡 $\text{Tr}(\bar{\rho}^{\text{ss}}(\sigma))$ だけでは $\bar{\rho}^{\text{ss}}$ の同値類は決まらないことに注意。

が得られる。 I_v を v における**惰性群**という。 $\kappa(v)$ の位数を q_v とおくと、 $\text{Gal}(\overline{\kappa(v)}/\kappa(v))$ は $\widehat{\mathbb{Z}}$ ($\mathbb{Z}$ の副有限完備化) と同形であり、 **幾何的 Frobenius 元**

$$\text{Frob}_v: x \mapsto x^{1/q_v} \quad (q_v \text{ 乗写像の逆写像})$$

により位相的に生成される¹²。 K_v の Galois 表現は、 惰性群 I_v への制限が自明となるとき**不分岐**であるといい、 そうでないとき**分岐**しているという。

2.5. Galois 表現の L 関数. 代数体 K の ℓ 進表現や Artin 表現 ρ に対し、 その L 関数 $L(s, \rho)$ が定まる。

定義 2.3 (Galois 表現の L 関数). K を代数体とし、

$$\rho: \text{Gal}(\overline{K}/K) \longrightarrow GL(V)$$

を ℓ 進表現または Artin 表現とする。 ρ が ℓ 進表現のときは (すなわち、 V が $\mathbb{Q}_\ell$ の有限次拡大 E 上の有限次元ベクトル空間のときは)、 体同形 $\overline{\mathbb{Q}_\ell} \cong \mathbb{C}$ を固定して、 $\rho(\sigma)$ ($\sigma \in \text{Gal}(\overline{K}/K)$) の固有値は複素数であると考え。 また、 ρ が ℓ 進表現のときは、 ρ は ℓ を割り切る素点で **de Rham** であると仮定する¹³。 このとき、 ρ の L 関数が Euler 積

$$L(s, \rho) = \prod_{v \text{ は有限素点}} L_v(s, \rho)$$

によって定義される。 **局所因子** $L_v(s, \rho)$ の定義は次の通りである。

- (1) ρ が Artin 表現か、 または ρ が ℓ 進表現で剰余体 $\kappa(v)$ の標数が ℓ と互いに素である場合。 惰性群 I_v により固定される元のなす部分空間を $V^{I_v} := \{v \in V \mid \rho(\sigma)v = v \ (\forall \sigma \in I_v)\}$ とおくと、 Frob_v は自然に V^{I_v} に作用する。 その固有値を $\alpha_{v,1}, \dots, \alpha_{v,d_v} \in \mathbb{C}$ ($d_v = \dim V^{I_v}$) とおき、 局所因子を

$$L_v(s, \rho) := \prod_{i=1}^{d_v} \frac{1}{1 - \alpha_{v,i} q_v^{-s}}$$

で定める。 (q_v は剰余体 $\kappa(v)$ の位数である。) これを簡単に、

$$L_v(s, \rho) = \det (1 - q_v^{-s} \text{Frob}_v; V^{I_v})^{-1}$$

とも書く。

¹²代数学の教科書では、 Frob_v の逆元 (単に **Frobenius 元**と呼ぶか、 または “幾何的” なものと区別して**数論的 Frobenius 元**と呼ぶ) を考えるものも多いが、 本稿ではすべて「幾何的 Frobenius 元」で統一して考える。 エタールコホモロジーから得られる Galois 表現を考える際には、 この方が自然である。 (§3.5 性質 8, 性質 9 を参照。)

¹³これは p 進 Hodge 理論 ($p = \ell$) から来る条件であり、「 ℓ を割り切る素点で**潜半安定**」とも同値である。 代数多様体のエタールコホモロジーから得られる Galois 表現はすべてこの条件をみたす。

- (2) ρ が ℓ 進表現で剰余体 $\kappa(v)$ の標数が ℓ に等しい場合¹⁴. ここでは詳しくは説明しないが, この場合は, Fontaine による D_{pst} -関手を用いることで, K_v の Weil-Deligne 表現 $D_{\text{pst}}(\rho_v)$ が得られ, それを用いて (1) と同様に局所因子 $L_v(s, \rho)$ が定まる:

$$L_v(s, \rho) := L_v(s, D_{\text{pst}}(\rho_v))$$

(詳しくは [Tay3] を参照.)

2.6. Galois 表現の L 関数の解析的性質 (予想). 整数論においては,

『“良い” L 関数は複素平面全体に解析接続され, 関数等式をみたすだろう.』

と広く信じられている. それでは, どのような Galois 表現が “良い” L 関数を生み出すのだろうか? 後で述べる Fontaine-Mazur 予想 (予想 5.1) を踏まえて, 次のように予想を定式化することができる.

予想 2.4. K を代数体とし, ρ を ℓ 進表現または Artin 表現とする. (ρ が ℓ 進表現のときは, 体同形 $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ を固定して考える.) ρ は絶対既約であり, 有限個の v の外で不分岐であると仮定する. さらに, ρ が ℓ 進表現のときは, ρ は ℓ を割り切る素点で de Rham であると仮定する. このとき, ρ の L 関数 $L(s, \rho)$ は (ρ が自明表現の場合の $s = 1$ における一位の極を除き) 複素平面全体に正則関数として解析接続される. さらに, $L(s, \rho)$ は (適当な形の) 関数等式をみたす¹⁵.

特に予想 2.4 の仮定は既約 Artin 表現に対しては自動的にみたされるから¹⁶, 予想 2.4 は次の古典的な予想を特別な場合として含む.

予想 2.5 (Artin 予想). K を代数体とし, $n \geq 1$ とする.

$$\rho: \text{Gal}(\overline{K}/K) \longrightarrow GL_n(\mathbb{C})$$

を既約 Artin 表現とする. このとき, $L(s, \rho)$ は ($n = 1$ で ρ が自明表現の場合の $s = 1$ における一位の極を除き) 複素平面全体に正則関数として解析接続される.

¹⁴歴史的にはこの場合を避けて議論することもあり. ℓ 進表現を個別に考えるのではなく, すべての素数 ℓ に関する ℓ 進表現の**整合系** (compatible system) を考え, 『整合系に対して L 関数が定まる』と考える (谷山豊). エタールコホモロジーを用いて作られる Galois 表現は整合系をなす (と期待されている). しかし, 現代においては, 『一つの ℓ のみから L 関数が定まる』と考えることが重要である. Wiles による Fermat の最終定理の証明には, ℓ として 3 や 5 といった特定の素数をとる技法 (いわゆる (3, 5)-トリック) が用いられた ([Wi]).

¹⁵ Γ -因子 (無限素点における局所因子) を定義して, Galois 表現 ρ のみを用いて関数等式の形を正確に予想することもできる ([Se6], [Tay3]).

¹⁶像が有限な Galois 表現 (Artin 表現や $\text{mod } \ell$ 表現) に対しては, 「有限個の v の外で不分岐」は自動的にみたされる.

$n = 1$ の場合は類体論の帰結である．一般の n でも， $L(s, \rho)$ が有理型関数として解析接続され，(適当な形の) 関数等式をみたすことが知られている．(**Brauer 誘導定理**を用いることで， $n = 1$ の場合 (類体論) に帰着できる.)

$n \geq 2$ のときは，この予想が証明されているケースは少ない．Langlands-Tunnell の定理により， $n = 2$ で ρ の像が可解群ならなりたつ．一般の n で ρ の像がベキ零群のときは，Arthur-Clozel によって $GL(n)$ の底変換定理の応用として証明されている ([AC]) ．また，最近では， $K = \mathbb{Q}$ ， $n = 2$ で ρ が「奇」な場合¹⁷の予想 2.5 が Khare-Wintenberger により証明されている． (§2.9 を参照.)

2.7. Galois 表現の例. Galois 表現とその L 関数の例をいくつか挙げよう．整数論に現れる “良い” L 関数の多くは，Galois 表現の L 関数として解釈される．

例 2.6 (自明表現と Riemann ゼータ関数). $K = \mathbb{Q}$ とし， ρ を自明表現とする． ρ はすべての素数 p で不分岐であり， $\rho(\text{Frob}_p)$ の固有値は 1 である．したがって，

$$L(s, \rho) = \prod_{p \text{ は素数}} \frac{1}{1 - p^{-s}}$$

が得られる．右辺の無限積を展開し，素因数分解の一意性を用いることで，

$$L(s, \rho) = \sum_{n=1}^{\infty} \frac{1}{n^s} =: \zeta(s)$$

が分かる ($\zeta(s)$ は **Riemann ゼータ関数**) ．特に， $\zeta(s)$ は複素平面全体に解析接続され， $s = 1$ における一位の極を除いて正則であり， $s \leftrightarrow 1 - s$ という形の関数等式をみたす．

例 2.7 (Dirichlet 指標と Dirichlet L 関数). 一般に，**円分体論** (すなわち $\mathbb{Q}$ の類体論) により，Dirichlet 指標を (1 次元) Galois 表現として解釈することができる． $N \geq 1$ とする．導手 N の**原始 Dirichlet 指標**とは，準同形

$$\chi: (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

であって， $(\mathbb{Z}/M\mathbb{Z})^\times$ (M は N の約数， $M \neq N$) を経由しないものをいう．このとき， χ の L 関数が

$$L(s, \chi) := \sum_{m \geq 1, m \text{ は } N \text{ と互いに素}} \frac{\chi(m)}{m^s} = \prod_{p \text{ は } N \text{ を割らない素数}} \frac{1}{1 - \chi(p)p^{-s}}$$

で定まる．一方， ζ_N を 1 の原始 N 乗根とすると，円分体論における同形

$$\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^\times, \quad \sigma \mapsto r(\sigma) \quad (\sigma(\zeta_N) = \zeta_N^{r(\sigma)})$$

¹⁷すなわち， $\det \rho(c) = -1$ の場合．ここで $c \in \text{Gal}(\mathbb{C}/\mathbb{R})$ は複素共役である．

があり¹⁸, 次の写像

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times \xrightarrow{a \mapsto a^{-1}} \mathbb{C}^\times$$

の合成を ρ とおけば¹⁹, ρ は 1 次元 Artin 表現で,

$$L(s, \rho) = L(s, \chi)$$

をみたく. **Kronecker-Weber の定理**より, $\mathbb{Q}$ のすべてのアーベル拡大はある $\mathbb{Q}(\zeta_N)$ に含まれるから, このようにして, $\mathbb{Q}$ のすべての 1 次元 Artin 表現が得られることが分かる.

例 2.8 (ℓ 進円分指標). K を体とし, ℓ を K で可逆な素数とする. $n \geq 1$ に対し, $\zeta_{\ell^n} \in \overline{K}$ を 1 の原始 ℓ^n 乗根とする. $\sigma \in \mathrm{Gal}(\overline{K}/K)$ に対し, $\sigma(\zeta_{\ell^n})$ もまた 1 の原始 ℓ^n 乗根なので, $\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{r_n(\sigma)}$ ($r_n(\sigma) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$) と書ける. $r_n(\sigma)$ は ζ_{ℓ^n} の選び方によらず, $m \geq n$ なら $r_m(\sigma) \bmod \ell^n = r_n(\sigma)$ をみたく. 写像 $\sigma \mapsto r_n(\sigma)$ の n に関する逆極限により, 準同形

$$\chi_\ell: \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathbb{Z}_\ell^\times = \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^\times \hookrightarrow \mathbb{Q}_\ell^\times = GL_1(\mathbb{Q}_\ell)$$

が得られる. χ_ℓ は K の 1 次元 ℓ 進表現であり, その像は一般には無限群である. χ_ℓ を K の ℓ 進円分指標という. K が代数体なら, ℓ を割らない有限素点 v において χ_ℓ は不分岐で, $\chi_\ell(\mathrm{Frob}_v) = q_v^{-1}$ をみたく (q_v は v の剰余体の位数). また, ℓ 進表現 $\rho: \mathrm{Gal}(\overline{K}/K) \rightarrow GL(V)$ と整数 $n \in \mathbb{Z}$ に対し, テンソル積 $\rho \otimes \chi_\ell^{\otimes n}$ のことを $\rho(n): \mathrm{Gal}(\overline{K}/K) \rightarrow GL(V(n))$ と書く. $\rho(n), V(n)$ をそれぞれ ρ, V の **Tate 捻り** という.

例 2.9 (楕円曲線の ℓ 進 Tate 加群). K を体とし, E を K 上の楕円曲線とする. $n \geq 1$ に対し, E の n 等分点のなす群を

$$E[n] = \{P \in E(\overline{K}) \mid \underbrace{P + \cdots + P}_{n \text{ 個}} = O\}$$

とおく. (右辺の “ $P + \cdots + P$ ” は $E(\overline{K})$ に定まる加法であり, $O \in E(K)$ は無限遠点 (加法に関する単位元) である.) n が K で可逆であれば, $E[n]$ は階数 2 の自由 $\mathbb{Z}/n\mathbb{Z}$ 加群である. ℓ を K で可逆な素数とし,

$$T_\ell E := \varprojlim E[\ell^n], \quad V_\ell E := (T_\ell E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

¹⁸ N を割らない素数 p に対し, 左辺における幾何的 Frobenius 元 Frob_p (の持ち上げの像) は, 右辺における p^{-1} に対応する. (p ではない!)

¹⁹最後の写像 $a \mapsto a^{-1}$ が “不自然” に思われるかもしれない. これは, Galois 表現の L 関数が幾何的 Frobenius 元 (p 乗写像の逆写像) により定義され, Dirichlet 指標の L 関数が (伝統的に) $\chi(p)$ で定義されることの「帳尻」をあわせるためのものである. もちろん, 数論的 Frobenius 元 (p 乗写像) を使って L 関数を定義することもできるのだが, エタールコホモロジーとの整合性を優先して, 本稿ではあえてそうしなかった.

とおくと, $T_\ell E, V_\ell E$ はそれぞれ $\mathbb{Z}_\ell, \mathbb{Q}_\ell$ 上の階数 2 の自由加群であり, $\text{Gal}(\overline{K}/K)$ が自然に作用する. $T_\ell E, V_\ell E$ を楕円曲線 E の ℓ 進 Tate 加群という. $V_\ell E$ の双対空間を

$$V = \text{Hom}_{\mathbb{Q}_\ell}(V_\ell E, \mathbb{Q}_\ell)$$

とおくと, V にも自然に $\text{Gal}(\overline{K}/K)$ が作用し, K の 2 次元 ℓ 進表現

$$\rho_{E,\ell}: \text{Gal}(\overline{K}/K) \longrightarrow GL(V)$$

が得られる. V は E の 1 次エタールコホモロジー $H^1(E \otimes_K \overline{K}, \mathbb{Q}_\ell)$ と同形である. K が位数 q の有限体 $\mathbb{F}_q$ であれば, q と互いに素な任意の素数 ℓ に対し,

$$\text{Tr}(\rho_{E,\ell}(\text{Frob}_q)) = 1 + q - \#E(\mathbb{F}_q)$$

がなりたつ. ($\#E(\mathbb{F}_q)$ は E の $\mathbb{F}_q$ -有理点の個数である. 例 3.9 を参照.)

2.8. なぜ Galois 表現を考えることが大切なのか. 古典的な整数論の問題のうちのいくつかは, Galois 表現の L 関数に関する問題に翻訳できる. 例えば,

『どのような奇素数 p が, $p = x^2 + y^2$ (x, y は正整数) と書けるか?』

という問題 (答え: 上のように書けることと, $p \equiv 1 \pmod{4}$ は同値) は二次形式 $x^2 + y^2$ が二次拡大 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ のノルムであること, すなわち $\alpha = x + y\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ に対して α とその共役 $\bar{\alpha}$ との積が

$$\alpha\bar{\alpha} = (x + y\sqrt{-1})(x - y\sqrt{-1}) = x^2 + y^2$$

となることと, $\mathbb{Q}(\sqrt{-1})$ の類数が 1 であることに注目すると, 次の写像の合成

$$\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) \cong \{\pm 1\} \hookrightarrow \mathbb{C}^\times$$

で定まる $\mathbb{Q}$ の 1 次元 Artin 表現 ρ に対し Frob_p の行き先 $\rho(\text{Frob}_p)$ を問う問題, すなわち,

『1 次元 Artin 表現 ρ の L 関数 $L(s, \rho)$ を決定せよ.』

という問題 (答え: $\sqrt{-1}$ は 1 の原始 4 乗根であるから, 円分体論から次が分かる. 導手 4 の非自明な (唯一の) 原始 Dirichlet 指標

$$\chi: (\mathbb{Z}/4\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times, \quad 1 \mapsto 1, \quad 3 \mapsto -1$$

に対し, $L(s, \rho) = L(s, \chi)$. 特に, 奇素数 p に対しては, $\rho(\text{Frob}_p) = 1$ と $p \equiv 1 \pmod{4}$ は同値) に翻訳できる.

整数論における重要な定理の中には、「素数」や「方程式」といった個々の対象を離れて、「Galois 表現」を統一的に考察することで、見通しよく説明・証明されるものも多い²⁰.

2.9. 保型形式に伴う Galois 表現. 例 2.7 で述べたように、 $\mathbb{Q}$ の類体論は、

$$\text{原始的 Dirichlet 指標 } \chi \leftrightarrow \mathbb{Q} \text{ の 1 次元 Artin 表現 } \rho$$

という一対一の対応として理解することができる²¹. Dirichlet 指標の「2次元版」である保型形式に、 $\mathbb{Q}$ の 2 次元 Galois 表現が対応することを述べる²².

一般に、 $\mathbb{Q}$ の 2 次元 Galois 表現 ρ が奇 (および、偶) であるとは、 $\det \rho(c) = -1$ (および、 $\det \rho(c) = 1$) となることをいう. ($c \in \text{Gal}(\mathbb{C}/\mathbb{R}) \subset \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ は複素共役である.)

定理 2.10 ([De1], [DeS], [Ca], [Sch], [Sa] など). $f = \sum_{n=1}^{\infty} a_n q^n$ を正規化されている尖点的な保型形式であって、Hecke 作用素の同時固有関数となっているものとする. f はレベル N の新形式であると仮定する. f の重さを k , 指標を ε とおく. ℓ を素数とし、体同形 $\overline{\mathbb{Q}}_{\ell} \cong \mathbb{C}$ を固定する. このとき、 $\mathbb{Q}$ の「奇」で絶対既約な 2 次元 ℓ 進表現

$$\rho_{f,\ell}: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(V)$$

(V は $\mathbb{Q}_{\ell}$ の有限次拡大 E 上の 2 次元ベクトル空間) が存在し、

$$L(s, f) = L(s, \rho_{f,\ell})$$

をみたす²³. $\rho_{f,\ell}$ を保型形式 f に伴う ℓ 進表現という. さらに、次がなりたつ.

(1) p を N と互いに素な素数とする. $p \neq \ell$ ならば、 $(\rho_{f,\ell})_p$ は不分岐で、

$$\text{Tr}(\rho_{f,\ell}(\text{Frob}_p)) = a_p, \quad \det(\rho_{f,\ell}(\text{Frob}_p)) = \varepsilon(p)p^{k-1}$$

がなりたつ. 特に、 $\rho_{f,\ell}$ の行列式表現 $\det \rho_{f,\ell}$ は $\tau \otimes \chi_{\ell}^{\otimes 1-k}$ に等しい. ここで、 χ_{ℓ} は ℓ 進円分指標であり (例 2.8), τ は例 2.7 の対応により ε に対応する 1 次元 ℓ 進

²⁰もちろん、整数論における重要な定理の中には、Galois 表現とは関係が無いものもある. (現在のところ関係が知られていないと言うべきか?)

²¹これは像が有限な場合である. この対応を、代数的 Hecke 指標と $\mathbb{Q}$ の 1 次元 ℓ 進表現の間の対応に拡張することもできる.

²²重さが 1 の保型形式に 2 次元 Artin 表現 (のうち「奇」なもの) が対応し、重さが 2 以上の保型形式に (像が無限な) ℓ 進表現が対応する.

²³ ℓ 進表現 $\rho_{f,\ell}$ (の同値類) が一意であることが、 $\rho_{f,\ell}$ が絶対既約であることと **Chebotarev 密度定理** からしたがう. (Chebotarev 密度定理から、 ℓ 進表現 ρ の半単純化 (の同値類) が、有限個を除くすべての素数 p に対する $\text{Tr} \rho(\text{Frob}_p)$ の値から一意に決まることが分かる ([Se4]).) また、 $\rho_{f,\ell}$ と $\rho_{g,\ell}$ が同値であれば $f = g$ となることが、保型形式に対する **重複度一定理** からしたがう.

表現 (Artin 表現) である. すなわち, N を割らない素数 p に対し, $\tau(\text{Frob}_p) = \chi(p)$ がなりたつ²⁴.

- (2) $p = \ell$ のとき, $(\rho_{f,\ell})_p$ は de Rham である. さらに, $\mathbb{Q}_p$ の代数的閉包の p 進完備化を $\mathbb{C}_p$ とおくと, $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ の作用と可換な $\mathbb{C}_p$ 上のベクトル空間としての同形

$$V \otimes_E \mathbb{C}_p \cong \mathbb{C}_p \oplus \mathbb{C}_p(1-k) \quad (\text{Hodge-Tate 分解})$$

が存在する. 左辺 $V \otimes_E \mathbb{C}_p$ に $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ は対角的に作用する. また, 右辺の $\mathbb{C}_p(1-k)$ は $\mathbb{C}_p$ の Tate 捻りである²⁵.

- (3) $k = 1$ のとき, $\rho_{f,\ell}$ の像は有限群である. また, N を割らない素数 p で $\rho_{f,\ell}$ は不分岐である. $\rho_{f,\ell}$ の同値類は ℓ によらない²⁶.

ここでは, 多くの数学者による (Eichler, 志村五郎, Deligne, Serre, Langlands, Carayol, Scholl, 斎藤毅らによる) 長年の結果の蓄積を一つの定理の形で書いた. $\rho_{f,\ell}$ が絶対既約であることの証明は Ribet による. 保型形式 f に対応する $GL_2(\mathbb{A}_{\mathbb{Q}})$ の保型表現 π と局所 Langlands 対応を用いることで, N を割り切る素数 p における対応を精密に述べるができる. また, これは証明からしたがうのだが, $\rho_{f,\ell}$ が単に (抽象的に) 存在するだけでなく, $k \geq 2$ の場合²⁷,

『 f に伴う ℓ 進表現 $\rho_{f,\ell}$ は, 久賀 - 佐藤多様体と呼ばれる $(k-1)$ 次元代数多様体 (モジュラー曲線上の楕円曲線族の自己ベキにより得られる代数多様体) の $(k-1)$ 次エタールコホモロジーを用いて作られる』

という点は重要である. これを用いて, Deligne は Ramanujan 予想 (および Ramanujan-Petersson 予想) を Weil 予想に帰着することにより証明した ([De1], [De2]. 本稿の §3.8 も参照).

²⁴ $\det \rho_{f,\ell} = \tau \otimes \chi_{\ell}^{\otimes 1-k}$ がなりたつことは, Chebotarev 密度定理の帰結である. f の重さ k と指標 ε は $\varepsilon(-1) = (-1)^k$ をみたすから (§2.1 を見よ), $\det \rho_{f,\ell}(c) = (-1)^k \cdot (-1)^{1-k} = -1$ となり, $\rho_{f,\ell}$ が「奇」であることが分かる.

²⁵ $\rho_{f,\ell}$ の $p = \ell$ における様子から f の「重さ k 」が復元できることになる. これは p 進 Hodge 理論の帰結である. 一般に, **Hodge-Tate 分解** とは次のような分解である: $\mathbb{Q}_p$ の有限次拡大 F 上の滑らかな射影的代数多様体 Y に対し, $\text{Gal}(\overline{F}/F)$ の作用と可換な $\mathbb{C}_p$ 上のベクトル空間としての同形 $H^m(Y \otimes_F \overline{F}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbb{C}_p \cong \bigoplus_{i+j=m} H^j(Y, \Omega^i) \otimes_F \mathbb{C}_p(-i)$ がある. $\text{Gal}(\overline{F}/F)$ は左辺には対角的に作用し, 右辺の H^j には自明に作用する.

²⁶正確に言うと, 体同形 $\mathbb{Q}_{\ell} \cong \mathbb{C}$ の選び方による可能性はある. しかし, f の q 展開の係数 a_n はすべてある代数体に含まれるから, これはそれほど深刻なことではない. また, 「 $\rho_{f,\ell}$ が Artin 表現である」ことから, 「重さ 1 の保型形式 f に対し, a_n は有限個の値しかとらない」という結論が得られる ([DeS]).

²⁷ $k = 1$ の場合の $\rho_{f,\ell}$ の構成は, 重さの大きい保型形式との間の合同性を用いるもので, 若干事情が異なる ([DeS]).

定理 2.10 は「保型形式 $\rightarrow$ Galois 表現」という対応であるが、逆方向の「Galois 表現 $\rightarrow$ 保型形式」という対応を考えることもできる²⁸。これは **Galois 表現の保型性予想**と呼ばれ、一般には難しい問題である。Wiles ([Wi]), Taylor-Wiles ([TW]) により創始された「 $R = T$ 定理」の発展により、最近では、 $\mathbb{Q}$ や総実代数体上の「奇」な 2 次元 Galois 表現の保型性予想に対しては、いくつかの結果が得られるようになってきた。 $\mathbb{Q}$ 上の楕円曲線 E の ℓ 進 Tate 加群により得られる 2 次元 ℓ 進表現は重さ 2 の保型形式に伴うというのが **谷山 - 志村予想**であり、Breuil-Conrad-Diamond-Taylor により完全に解決された ([BCDT])。与えられた $\mathbb{Q}$ の既約で「奇」な 2 次元 mod ℓ 表現 ρ は、保型形式に伴う ℓ 進表現の mod ℓ で得られるというのが **Serre 予想**であり、Taylor, Shepherd-Barron らによる部分的解決の後、Taylor による「潜保型性」や Kisin による「 $R^{\text{red}} = T$ 定理」を用いて、Khare-Wintenberger により解決された ([SBT], [KW])。Serre 予想に Buzzard-Taylor による p 進保型形式の“はりあわせ”(または“ p 進解析接続”)の議論を組み合わせることで、**強 Artin 予想**(既約で「奇」な $\mathbb{Q}$ の 2 次元 Artin 表現が、重さ 1 の保型形式に伴うという予想)が証明され、その帰結として ($n = 2$, $K = \mathbb{Q}$ で「奇」な場合の) Artin 予想 (予想 2.5) が証明された。 $(\mathbb{Q}$ の 2 次元 ℓ 進表現に対する保型性予想の現状については、[Kis] やそこで引用されている文献を参照。)

2.10. 非可換類体論へ。 $\mathbb{Q}$ の 2 次元非可換類体論を

$$\text{保型形式 } f \leftrightarrow \mathbb{Q} \text{ の 2 次元 } \ell \text{ 進表現 } \rho_{f,\ell}$$

という形で理解することができる。左辺は「 $GL_2(\mathbb{A}_{\mathbb{Q}})$ の保型表現」の特別な場合 (正則保型形式に対応する場合、「奇」な Galois 表現に対応する) である。最近では、より一般の代数体 K に対して、

$$GL_n(\mathbb{A}_K) \text{ の (代数的) 保型表現 } \pi \leftrightarrow K \text{ の } n \text{ 次元 (幾何的) } \ell \text{ 進表現 } \rho_{\pi,\ell}$$

という形の非可換類体論が研究されている。高次元志村多様体 (モジュラー曲線の一般化) のエタールコホモロジーを用いることで、いくつかの特別な場合 (K が総実代数体か CM 体で、 π が様々な技術的仮定をみたす場合) には、

$$GL_n(\mathbb{A}_K) \text{ の保型表現 } \pi \text{ に伴う } n \text{ 次元 } \ell \text{ 進表現 } \rho_{\pi,\ell}$$

が構成され、整数論的应用も得られている ([Tay3], [HT], [TY], [Tanoshimi])。

²⁸ $\mathbb{Q}$ の「偶」な 2 次元 Galois 表現は実解析的な保型形式 (Maass の波動形式) に伴うと期待されているが、現時点では「保型形式 $\leftrightarrow$ Galois 表現」の対応のいずれの方向も証明されていない。実解析的な保型形式に対しては、数論幾何的な手法が使えないことが一因である。

3. WEIL 予想とエタールコホモロジー

ここでは、数論幾何の発展の原動力となった **Weil 予想**（有限体上の代数多様体に対する Riemann 予想の類似）と、その解決に大きな役割を果たした**エタールコホモロジー**について述べる．

3.1. Hasse-Weil ゼータ関数. まず、古典的な Riemann 予想について思い出しておこう．Riemann ゼータ関数は Dirichlet 級数

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

で定義される関数である．右辺は s の実部が十分に大きいところで絶対収束し（実際には $\operatorname{Re}(s) > 1$ でよい），複素平面全体に有理型関数として解析接続され， $s = 1$ における 1 位の極を除いて正則である．また， $\zeta(s)$ は $s \leftrightarrow 1-s$ という形の関数等式をみたす． $\zeta(s)$ は負の偶数 ($s = -2, -4, -6, \dots$) で零点 (**自明な零点**) を持つ．有名な **Riemann 予想**

『 $\zeta(s)$ の零点は，自明な零点以外は直線 $\operatorname{Re}(s) = \frac{1}{2}$ 上にある』

は今日でも未解決である．

素因数分解の一意性から， $\zeta(s)$ は $\operatorname{Re}(s) > 1$ において Euler 積

$$\zeta(s) = \prod_{p \text{ は素数}} \frac{1}{1 - p^{-s}}$$

をもつ．スキーム $\operatorname{Spec} \mathbb{Z}$ の閉点は $\mathbb{Z}$ の極大イデアルに対応し， $(p) = p\mathbb{Z}$ (p は素数) という形をしているから，

$$\zeta(s) = \prod_{x \in |\operatorname{Spec} \mathbb{Z}|} \frac{1}{1 - \#(\kappa(x))^{-s}}$$

という形に書ける．ここで， $|\operatorname{Spec} \mathbb{Z}|$ はスキーム $\operatorname{Spec} \mathbb{Z}$ の閉点の集合である．（一般にスキーム X の閉点の集合を $|X|$ で表す．）また， $\kappa(x)$ は x における剰余体であり， $\#(\kappa(x))$ はその位数である．($x = (p)$ なら $\kappa(x) = \mathbb{F}_p$ ， $\#(\kappa(x)) = p$ である．)

定義 3.1. X を $\operatorname{Spec} \mathbb{Z}$ 上有限型のスキームとする．このとき， X の **Hasse-Weil ゼータ関数**を Euler 積

$$\zeta(s, X) := \prod_{x \in |X|} \frac{1}{1 - \#(\kappa(x))^{-s}}$$

で定義する．右辺は s の実部が十分大きいところで収束する．

$X = \operatorname{Spec} \mathbb{Z}$ のときに $\zeta(s, \operatorname{Spec} \mathbb{Z})$ が Riemann ゼータ関数になることを述べた．一般に $X = \operatorname{Spec} O_K$ (K は代数体, O_K は K の整数環) のとき, $\zeta(s, \operatorname{Spec} O_K)$ は K の **Dedekind ゼータ関数** に等しい．

任意の $\operatorname{Spec} \mathbb{Z}$ 上有限型のスキーム X に対し, $\zeta(s, X)$ は複素平面全体に有理型関数として解析接続され, さらに X が良い性質を持てば $\zeta(s, X)$ は関数等式をみたすと予想されている²⁹．この予想は, エタールコホモロジーから定まる Galois 表現を用いて, Galois 表現の L 関数の問題として精密に定式化することができる³⁰．しかし, (代数体の整数環の場合や, 本節でこれから述べる有限体上の代数多様体の場合を除いて) 証明されている例は極めて少ない． X が $\mathbb{Q}$ 上の楕円曲線 (の Néron モデル) の場合でさえ, この予想が証明されたのは最近のことである．(谷山 - 志村予想の帰結である.)

3.2. Weil 予想 (古典的定式化).

補題 3.2. 有限体 $\mathbb{F}_q$ 上の代数多様体 X に対し,

$$\zeta(s, X) = \exp \left(\sum_{m=1}^{\infty} \#X(\mathbb{F}_{q^m}) \frac{(q^{-s})^m}{m} \right)$$

がなりたつ．これは両辺を $T = q^{-s}$ に関する有理数係数の形式的べき級数と考えたときの等式である．

証明. 閉点 $x \in |X|$ における剰余体 $\kappa(x)$ の位数を q^{m_x} とおくと, $\#(\kappa(x))^{-s} = (q^{-s})^{m_x} = T^{m_x}$ だから, 左辺の $\log$ は

$$\begin{aligned} \log \zeta(s, X) &= \sum_{x \in |X|} \log \left(\frac{1}{1 - \#(\kappa(x))^{-s}} \right) = \sum_{x \in |X|} \log \left(\frac{1}{1 - T^{m_x}} \right) \\ &= \sum_{x \in |X|} \sum_{n=1}^{\infty} \frac{(T^{m_x})^n}{n} = \sum_{x \in |X|} \sum_{n=1}^{\infty} m_x \frac{T^{(m_x n)}}{(m_x n)} \\ &= \sum_{n=1}^{\infty} \left(\sum_{x \in |X|, m_x \text{ は } n \text{ の約数}} m_x \right) \frac{T^n}{n} \end{aligned}$$

と書ける．よって,

$$\sum_{x \in |X|, m_x \text{ は } n \text{ の約数}} m_x = \#X(\mathbb{F}_{q^n})$$

²⁹もちろん, Riemann 予想の類似を“期待”することもできるが, Riemann 予想は $\operatorname{Spec} \mathbb{Z}$ の場合でさえ証明されていないから, 一般的な「予想」を述べるのは性急すぎるかもしれない．

³⁰Hasse-Weil ゼータ関数と Galois 表現の L 関数の関係については §3.10 を参照．また, [Se6], [Tay3], [Tay1], [Tay2] を参照．

を示せばよい. これは, 各閉点 $x \in |X|$ に対し, $(\mathbb{F}_q$ 上共役な m_x 個の) $\mathbb{F}_{q^{m_x}}$ -有理点の組 $P_{x,1}, \dots, P_{x,m_x}$ が定まり, これにより一対一対応

$$\begin{aligned} |X| &\xleftrightarrow{1:1} \{X(\overline{\mathbb{F}}_q) \text{ の } \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\text{-軌道}\} \\ x &\longleftrightarrow \{P_{x,1}, \dots, P_{x,m_x}\} \end{aligned}$$

が得られることの帰結である. (閉点 $x \in |X|$ は, 各 $X(\mathbb{F}_{q^n})$ (n は m_x の倍数) に m_x 個ずつ寄与する.) $\square$

定義 3.3. 有限体 $\mathbb{F}_q$ 上の代数多様体 X に対し, 変数 T に関する形式的べき級数

$$Z(T, X) := \exp \left(\sum_{m=1}^{\infty} \#X(\mathbb{F}_{q^m}) \frac{T^m}{m} \right)$$

を X の **合同ゼータ関数** という. (X の合同ゼータ関数と Hasse-Weil ゼータ関数の間には $\zeta(s, X) = Z(q^{-s}, X)$ の関係がある.)

Weil は, 有限体上の Fermat 型の超曲面の有理点の個数を数えることで, 合同ゼータ関数を計算し, 次の予想に導かれた ([We]).

予想 3.4 (Weil 予想). 有限体 $\mathbb{F}_q$ 上の代数多様体 X の合同ゼータ関数 $Z(T, X)$ は次をみたす.

- (1) (**有理性**) $Z(T, X)$ は T に関する有理関数である. すなわち, T に関する 0 でない多項式の比で表される.
- (2) (**関数等式**) X が $\mathbb{F}_q$ 上の滑らかな射影的代数多様体とすると, $Z(T, X)$ は

$$Z\left(\frac{1}{q^n T}, X\right) = \pm q^{n\chi/2} \cdot T^\chi \cdot Z(T, X)$$

をみたす. ここで n は X の次元である. χ は X の **Euler 数** であり, 対角集合 $\Delta \subset X \times X$ の自己交点数で定義される: $\chi := \Delta \cdot \Delta$. (Euler 数については §3.6 を参照.)

- (3) (**Riemann 予想の類似**) $Z(T, X)$ は

$$\begin{aligned} Z(T, X) &= \frac{P_1(T) \cdot P_3(T) \cdots P_{2n-1}(T)}{P_0(T) \cdot P_2(T) \cdot P_4(T) \cdots P_{2n}(T)}, \\ P_i(T) &= \prod_j (1 - \alpha_{i,j} T), \quad |\alpha_{i,j}| = q^{i/2} \end{aligned}$$

という形に書ける. ($|\alpha_{i,j}| = q^{i/2}$ の正確な意味は次の通り: $\alpha_{i,j}$ は代数的数で, そのすべての共役の複素絶対値が $q^{i/2}$ に等しい.)

- (4) (**Betti 数の一致**) X が代数体 K 上の滑らかな射影的代数多様体 Y の標数 p 還元で得られると仮定する. (すなわち, Y の定義方程式の係数を $\text{mod } m_v$ (v は p の上にある K の有限素点, $m_v \subset O_K$ は対応する O_K の極大イデアル) したものが X の定義方程式であるとする.) 任意の体の埋め込み $K \hookrightarrow \mathbb{C}$ に対し, $Y(\mathbb{C})$ は複素多様体であるから, その特異コホモロジー $H^i(Y(\mathbb{C}), \mathbb{Q})$ が定義される. その次元 (Betti 数) は多項式 $P_i(T)$ の次数に等しい:

$$\dim_{\mathbb{Q}} H^i(Y(\mathbb{C}), \mathbb{Q}) = \deg P_i(T)$$

(1) から, 特に, $\zeta(s, X) = Z(q^{-s}, X)$ が s に関する有理型関数として $\mathbb{C}$ 全体に解析接続されることが分かる. (2) を Hasse-Weil ゼータ関数の言葉に翻訳すると, $T = q^{-s}$ であるから, $s \leftrightarrow n - s$ という形の関数等式が得られる. また, 複素数 q に対し, $|q^{-s}| = q^{-\text{Re}(s)}$ であるから, (3) は Hasse-Weil ゼータ関数の極や零点の実部に関する主張である.

楕円曲線の場合の予想 3.4 は Hasse によって 1930 年代には知られていた (例 3.6). (Hasse は 1933 年と 1934 年に 2 通り³¹の証明を与えている.) Weil は 1940 年代に代数曲線の場合や (2 通り³²の証明を与えている), アーベル多様体の場合を解決した. 最終的に, Artin, Grothendieck らによるエタールコホモロジーの基礎付けを経て, 予想 3.4 は Deligne によって解決された ([De2], [De3]). (Deligne もまた 2 通り³³の証明を与えている!)

例 3.5. X を n 次元射影空間 $\mathbb{P}^n$ とする. このとき,

$$\mathbb{P}^n(\mathbb{F}_{q^m}) = q^{mn} + q^{m(n-1)} + \cdots + q^m + 1 = \sum_{k=0}^n q^{km}$$

であるから,

$$Z(T, X) = \exp \left(\sum_{m=1}^{\infty} \sum_{k=0}^n q^{km} \frac{T^m}{m} \right) = \prod_{k=0}^n \exp \left(\sum_{m=1}^{\infty} \frac{(q^k T)^m}{m} \right) = \prod_{k=0}^n \frac{1}{1 - q^k T}$$

となる. $\mathbb{P}^n$ の Euler 数は $\chi = n + 1$ であり, 射影空間 $\mathbb{P}^n(\mathbb{C})$ の Betti 数は

$$\dim_{\mathbb{Q}} H^i(\mathbb{P}^n(\mathbb{C}), \mathbb{Q}) = \begin{cases} 1 & i = 0, 2, 4, \dots, 2n \\ 0 & \text{それ以外} \end{cases}$$

³¹標数 0 の体上に持ち上げて虚数乗法論を用いる証明と, 標数 p の体上の Frobenius 射を用いる証明である.

³²Jacobi 多様体を用いて代数曲線の場合をアーベル多様体の場合に帰着する方法と, 代数曲線のベキ $C \times C$ 上の Hodge 指数定理を用いる方法である. これらは Grothendieck による「スタンダード予想」の動機付けとなった.

³³[De2], [De3] の証明のアイデアは若干異なるが, 使われている道具 (エタールコホモロジー, Lefschetz ペンシル, 関数体上の L 関数の収束性など) には共通のことが多い. (Hasse や Weil に比べると) “2 通りの別証明” とまでは言えないかもしれない.

であるから, $P_{2k}(T) = 1 - q^k T$ ($k = 0, \dots, n$), $P_{2k+1}(T) = 1$ ($k = 0, \dots, n-1$) とおけば, 予想 3.4 が確かめられる³⁴.

例 3.6 (Hasse の定理). E を有限体 $\mathbb{F}_q$ 上の楕円曲線とする. $\mathbb{F}_q$ の標数が 2 でも 3 でもなければ, E は射影空間 $\mathbb{P}^2$ の中で 3 次式 (**Weierstrass 標準形**)

$$E: Y^2 Z = X^3 + aXZ^2 + bZ^3 \quad (a, b \in \mathbb{F}_q, 4a^3 + 27b^2 \neq 0)$$

で定義される滑らかな射影的代数曲線である. このとき, 代数的数 $\alpha, \beta \in \mathbb{C}$ が存在して, $\alpha\beta = q$ かつ, 任意の $m \geq 1$ に対して

$$\#E(\mathbb{F}_{q^m}) = 1 - (\alpha^m + \beta^m) + q^m$$

をみtas. (これは **Lefschetz 跡公式** を用いて解釈できる. 例 3.9 を参照.) これより, E の合同ゼータ関数は

$$Z(T, E) = \exp \left(\sum_{m=1}^{\infty} (1 - (\alpha^m + \beta^m) + q^m) \frac{T^m}{m} \right) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

と書ける. $\mathbb{C}$ 上の楕円曲線は「1 人乗りの浮き輪」であるから, その Betti 数を考慮すると, 予想 3.4 (1), (3) から, $P_1(T) = (1 - \alpha T)(1 - \beta T)$ となるはずである. したがって, 予想 3.4 (3) (Riemann 予想の類似) は

$$\begin{aligned} |\alpha| = |\beta| = q^{1/2} &\iff P(T) = 0 \text{ が重解か, または 2 個の異なる虚数解を持つ.} \\ &\iff (\alpha + \beta)^2 \leq 4q \end{aligned}$$

となるが, $\alpha + \beta = 1 + q - \#E(\mathbb{F}_q)$ に注意すると, 不等式

$$|1 + q - \#E(\mathbb{F}_q)| \leq 2\sqrt{q} \quad (\text{Hasse の不等式})$$

と同値であることが分かる. このように, 楕円曲線に対する Weil 予想は,

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$$

という整数論的な意味を持つ³⁵

³⁴厳密に言うと, 予想 3.4 (4) は $\mathbb{F}_q$ 上の射影空間 $\mathbb{P}^n$ の標数 0 への「すべての」持ち上げに対する主張であるから, 特定の持ち上げ (すなわち $\mathbb{P}^n(\mathbb{C})$ 自身) に対して等号を確かめただけでは, 予想 3.4 (4) を証明したことにはならない.

³⁵例えば, 素数 $p = 1,000,003$ に対し, $\mathbb{F}_p$ 上の楕円曲線 $E: Y^2 Z = X^3 + aXZ^2 + bZ^3$ を考える. $\mathbb{P}^2$ 上の $\mathbb{F}_p$ -有理点は $p^2 + p + 1 = 1,000,007,000,013$ 個もあるが, そのうち E を定義する 3 次方程式をみたすものが, 998,004 個以上 1,002,004 個以下であることが分かる. Hasse の定理をうまく用いることで, 有限体上の楕円曲線の有理点の個数を効率よく計算することができる.

3.3. **Weil 予想への位相幾何学的アプローチ.** Weil は、当時発達していた位相幾何学からのアイデアを取り入れることで、Weil 予想 (予想 3.4) に取り組んだ。Weil による大胆なアイデアを一言で言えば、

『Frobenius 射に対して Lefschetz 跡公式を用いる』

というものであった。([K12], 8 ページの footnote を参照.)

これについて説明しよう。 X を有限体 $\mathbb{F}_q$ 上の射影的代数多様体とする。 X は十分次元の大きい射影空間に含まれ ($X \subset \mathbb{P}^m$ とする), いくつかの $\mathbb{F}_q$ -係数の多項式の共通零点として表される。

$$X = \{[x_0 : \cdots : x_m] \in \mathbb{P}^m \mid F_1(x_0, \dots, x_m) = \cdots = F_r(x_0, \dots, x_m) = 0\}$$

($[x_0 : \cdots : x_m]$ は $\mathbb{P}^m$ の斉次座標。 $F_1, \dots, F_r$ は $(m+1)$ 変数で $\mathbb{F}_q$ に係数を持つ斉次多項式。) 斉次座標を q 乗する写像

$$[x_0 : \cdots : x_m] \mapsto [x_0^q : \cdots : x_m^q]$$

は X を自分自身にうつすから、これを $F: X \rightarrow X$ で表し、 X の **Frobenius 射** と呼ぶ。一方で、有限体の Galois 理論により $\mathbb{F}_q = \{a \in \overline{\mathbb{F}_q} \mid a^q = a\}$ であるから、 F の固定点の集合 $\text{Fix}(F)$ は、 X の $\mathbb{F}_q$ -有理点の集合 $X(\mathbb{F}_q)$ に一致する³⁶：

$$\text{Fix}(F) := \{x \in X \mid F(x) = x\} = X(\mathbb{F}_q).$$

同様に、 $\text{Fix}(F^m) = X(\mathbb{F}_{q^m})$ である。予想 3.4 のためには、 X の $\mathbb{F}_{q^m}$ -有理点の個数 $\#X(\mathbb{F}_{q^m})$ をうまくコントロールする必要があるが、そのためには Frobenius 射のベキの固定点集合の位数 $\#\text{Fix}(F^m)$ がコントロールできればよい。

位相幾何学における **Lefschetz 跡公式**を思い出そう。これは、大雑把に言えば、 M をコンパクト位相多様体、 $\varphi: M \rightarrow M$ を連続写像とし、 φ の固定点集合を $\text{Fix}(\varphi) := \{x \in M \mid \varphi(x) = x\}$ とおくと、

$$\#\text{Fix}(\varphi) = \sum_i (-1)^i \text{Tr}(\varphi^*; H^i(M))$$

がなりたつという定理である³⁷。ここで $H^i(M)$ は M の (特異) コホモロジーであり、 $\varphi^*: H^i(M) \rightarrow H^i(M)$ は φ から誘導される線形写像である。

³⁶ここで重要なことは、 $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ の位相的生成元 (q 乗写像) の $X(\overline{\mathbb{F}_q})$ への作用が、 $F: X \rightarrow X$ という代数多様体の間の射 (Frobenius 射) に “化ける” ことである。このようなことは有限体以外の基礎体では期待できない。

³⁷これはやや不正確である。正しい定理を述べるためには、 $\text{Fix}(\varphi)$ が孤立していることなどを仮定し (そうでないと「個数」に意味がない), 左辺を「重複度を込めた和」に置き換えるなどの修正が必要である。また、 M がコンパクトでなくても (あるいは位相多様体でなくても) なりたつ場合もある。詳しくは位相幾何学の教科書を参照。

X は有限体上の代数多様体であるから、もちろん、この定理を適用することはできない。ここで、大胆にも (!),

『Frobenius 射 $F: X \rightarrow X$ に対しても、何らかの意味で「Lefschetz 跡公式の類似」がなりたつ』

と“仮定”する。すなわち、 X の「コホモロジー」と呼ばれる有限次元ベクトル空間 $H^i(X)$ が存在して、

$$\# \text{Fix}(F^m) = \sum_i (-1)^i \text{Tr}((F^*)^m; H^i(X))$$

がなりたつとする。線形写像 $F^*: H^i(X) \rightarrow H^i(X)$ の固有値を $\alpha_{i,1}, \dots, \alpha_{i,k_i}$ とおくと、 $\# \text{Fix}(F^m) = X(\mathbb{F}_{q^m})$ であるから、

$$X(\mathbb{F}_{q^m}) = \sum_i (-1)^i \sum_j \alpha_{i,j}^m$$

が分かり、 X の合同ゼータ関数に関する公式

$$\begin{aligned} Z(T, X) &= \exp \left(\sum_{m=1}^{\infty} \sum_i (-1)^i \sum_j \alpha_{i,j}^m \frac{T^m}{m} \right) = \prod_{i,j} \left(\exp \left(\sum_{m=1}^{\infty} \frac{(\alpha_{i,j} T)^m}{m} \right) \right)^{(-1)^i} \\ &= \prod_{i,j} \left(\frac{1}{1 - \alpha_{i,j} T} \right)^{(-1)^i} = \prod_{i,j} (1 - \alpha_{i,j} T)^{(-1)^{i*}}. \end{aligned}$$

が得られる。こうして、「コホモロジー」の存在と、それに対して『Lefschetz 跡公式がなりたつ』という“仮定”から、合同ゼータ関数 $Z(T, X)$ が有理関数である (予想 3.4 (1)) という整数論的な命題が形式的に導かれてしまう。

それでは、ここで存在を“仮定”した、 X の「コホモロジー」とは一体何なのだろうか？もちろん、 X は位相多様体ではないから、位相幾何における定義をそのまま採用するわけにはいかない³⁸。Weil は代数曲線の Jacobi 多様体の Tate 加群を用いて、「代数曲線の H^1 」にあたるものを考察し、曲線の場合やアーベル多様体の場合の予想 3.4 を証明した。その目的のために、Weil が代数幾何学の基礎付けを行ったことは有名である³⁹。Grothendieck は [EGA] において「スキーム」を導入し、代数幾何学の徹底的な基礎付けを行った後、位相空間や層といった概念を抽象化し、スキームに対する (通常の Zariski 位相とは異なる) 「エタール位相」の概念を導入し、それを用

³⁸ X は Zariski 位相を持つから、もちろんその位相に関するコホモロジーを定義することはでき、代数幾何学への応用上重要である (連接層のコホモロジー ([Har])). しかし、これは X の「形」や整数論的性質を十分に表すものではなく、Weil 予想への応用上は不十分である。

³⁹ 歴史的には、 $\mathbb{C}$ 上の代数曲線 (Riemann 面) の Jacobi 多様体は位相的・複素解析的な方法で研究されていたが、Weil はそれらの理論を代数的に (有限体上で) 展開する必要があった。

いてコホモロジーを定義した ([SGA]). これが次に述べるエタールコホモロジーである. [EGA] の冒頭に壮大なプロジェクト開始当初に予定されていた「目次」を見ることができる⁴⁰. Grothendieck による [EGA] の目標の一つは, Weil のアイデアをさらに発展させて, Weil 予想を「自然に証明する」ことであった.

3.4. エタールコホモロジー (入門). ここでは, 整数論への応用を踏まえて, エタールコホモロジーがどういうもので, それがどう役に立つのか, ということに重点を置いて説明する. エタールコホモロジーの定義を説明したり, その基本的な性質を証明することは一切しない (できない) ので, 適宜文献を参照していただきたい. (文献については, §3.11 を参照.)

K と体とし, ℓ を K で可逆な素数とする. K 上の代数多様体 X に対し, i 次 ℓ 進エタールコホモロジー

$$H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$$

が定まる⁴¹. これは $\mathbb{Q}_\ell$ 上の有限次元ベクトル空間であり, K の絶対 Galois 群 $\text{Gal}(\bar{K}/K)$ が連続に作用する. これにより K の ℓ 進表現

$$\rho: \text{Gal}(\bar{K}/K) \longrightarrow GL(H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell))$$

が得られる. 本稿の「はじめに」にも述べたように,

『エタールコホモロジーを用いることで, 代数多様体から Galois 表現 (ℓ 進表現) を作ることができる』

という点は重要である.

各次数 i に対するエタールコホモロジーをまとめて,

$$H^*(X \otimes_K \bar{K}, \mathbb{Q}_\ell) := \bigoplus_i H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$$

と書く.

3.5. エタールコホモロジーの基本的性質. ここでは主に整数論への応用上重要な性質を説明することにし, 定理の主張の一般的な定式化は行わない. 次の性質はどれも

⁴⁰[EGA I] の 6 ページを見よ.

⁴¹ ℓ が K の標数と等しい場合でもエタールコホモロジーは定義され, ガロア表現を得ることができる. しかし, エタールコホモロジーに対する重要な定理の中には, ℓ が K で可逆な場合にしかなりたないものも多い. そこで, 本稿では「 ℓ が K で可逆である」という仮定の下で説明することにする. (詳しくは [SGA] を参照.)

「自然」に見えるかもしれないが、(その見かけに反して) 証明が極めて難しいものも数多く含まれている。

性質 1 (関手性): エタールコホモロジーは反変関手である。すなわち、 K 上の代数多様体の間の射 $f: X \rightarrow Y$ に対し、**引き戻し**と呼ばれる線形写像

$$f^*: H^i(Y \otimes_K \bar{K}, \mathbb{Q}_\ell) \longrightarrow H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$$

が誘導される。 f^* は $\text{Gal}(\bar{K}/K)$ の作用と可換である。また、 f が恒等射なら f^* は恒等写像で、 $f: X \rightarrow Y$, $g: Y \rightarrow Z$ に対して $(g \circ f)^* = f^* \circ g^*$ がなりたつ。

性質 2 (有限性): $H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$ は $\mathbb{Q}_\ell$ 上の有限次元ベクトル空間である。また、 X の次元を n とおくと、 $i < 0$ および $i > 2n$ では $H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) = 0$ である⁴²。

性質 3 (特異コホモロジーとの比較定理): $K = \mathbb{C}$ のとき、自然な同形

$$H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \cong H^i(X(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$$

が存在する。ここで右辺の $H^i(X(\mathbb{C}), \mathbb{Q})$ は位相空間 $X(\mathbb{C})$ の特異コホモロジーである。

性質 4 (代数的閉体の変更にに関する不変性): K' を $\bar{K}$ を含む代数的閉体とする (例えば K が代数体で、 $K' = \mathbb{C}$)。このとき、自然な同形

$$H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \cong H^i(X \otimes_K K', \mathbb{Q}_\ell)$$

が存在する。

性質 3, 性質 4 をあわせると、次が導かれる：代数体 K 上の X と任意の体の埋め込み $\bar{K} \hookrightarrow \mathbb{C}$ に対し、エタールコホモロジー $H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$ の $\mathbb{Q}_\ell$ 上の次元は、位相空間 $X(\mathbb{C})$ の Betti 数 $b_i(X(\mathbb{C}))$ に等しい⁴³。

X の次元を n とすると、 $\text{Gal}(\bar{K}/K)$ の作用と可換な自然な同形

$$H^0(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell, \quad H^{2n}(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(-n)$$

がある。(後者は**向き付け写像**と呼ばれている。 $\mathbb{Q}_\ell(-n)$ は Tate 捻りである (例 2.8 を参照)。) また、任意の i, j に対し、**カップ積**と呼ばれる双線形写像

$$H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \times H^j(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \longrightarrow H^{i+j}(X \otimes_K \bar{K}, \mathbb{Q}_\ell), \quad (\alpha, \beta) \mapsto \alpha \cdot \beta$$

⁴²これは $K = \mathbb{C}$ の場合、 $X(\mathbb{C})$ は $2n$ 次元の位相多様体になる (したがって、 $i < 0$ および $i > 2n$ ではその i 次特異コホモロジーが消える) ことの対応物であると考えられる。

⁴³Betti 数 $b_i(X(\mathbb{C}))$ が埋め込み $\bar{K} \hookrightarrow \mathbb{C}$ のとり方によらないことは自明ではない ([Se1])。一般に、 $\mathbb{C}$ 上の代数多様体 X, X' が互いに共役 ($\text{Aut}(\mathbb{C}/\mathbb{Q})$ の元でうつりあう) であっても、 $X(\mathbb{C}), X'(\mathbb{C})$ は同相とは限らない ([Se2])。

がある．カップ積は $\alpha \cdot \beta = (-1)^{ij} \beta \cdot \alpha$ をみたし，引き戻しと可換である．($f: X \rightarrow Y$ に対し， $f^*(\alpha \cdot \beta) = (f^*\alpha) \cdot (f^*\beta)$ がなりたつ.)

性質 5 (Poincaré 双対定理): X の次元を n とすると，カップ積と向き付け写像から定まる双線形形式

$$H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \times H^{2n-i}(X \otimes_K \bar{K}, \mathbb{Q}_\ell)(n) \longrightarrow \mathbb{Q}_\ell$$

は非退化である．

Poincaré 双対定理より， $\text{Gal}(\bar{K}/K)$ の作用と可換な同形

$$H^{2n-i}(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \cong (H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell))^*(-n)$$

が得られる ($*$ は双対空間を表す)．また， X の次元を n ， Y の次元を m としたとき，射 $f: X \rightarrow Y$ による引き戻し写像 f^*

$$f^*: H^{2n-i}(Y \otimes_K \bar{K}, \mathbb{Q}_\ell) \longrightarrow H^{2n-i}(X \otimes_K \bar{K}, \mathbb{Q}_\ell)$$

の双対写像

$$H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell)(n) \longrightarrow H^{2m-(2n-i)}(Y \otimes_K \bar{K}, \mathbb{Q}_\ell)(m)$$

の Tate 捻りで得られる写像を

$$f_*: H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \longrightarrow H^{i+2(m-n)}(Y \otimes_K \bar{K}, \mathbb{Q}_\ell)(m-n)$$

とおく．

性質 6 (Künneth 公式): X, Y に対し，直積からの射影をそれぞれ $p: X \times Y \rightarrow X$ ， $q: X \times Y \rightarrow Y$ とおく．このとき， $(\alpha, \beta) \mapsto (p^*\alpha) \cdot (q^*\beta)$ の和から導かれる写像

$$\left(\bigoplus_{i+j=k} H^i(X \otimes_K \bar{K}, \mathbb{Q}_\ell) \otimes H^j(Y \otimes_K \bar{K}, \mathbb{Q}_\ell) \right) \xrightarrow{\cong} H^k((X \times Y) \otimes_K \bar{K}, \mathbb{Q}_\ell)$$

は同形である．

引き続き， X の次元を n とおく． X の余次元 i の閉部分代数多様体の整数係数の形式和 $a_1 Z_1 + \cdots + a_r Z_r$ ($a_1, \dots, a_r \in \mathbb{Z}$ ， $Z_1, \dots, Z_r \subset X$ は余次元 i) のことを余次元 i の代数的サイクルといい，その全体を $C^i(X)$ とおく．

性質 7 (サイクル写像): サイクル写像と呼ばれる写像

$$\gamma_X: C^i(X) \longrightarrow H^{2i}(X \otimes_K \bar{K}, \mathbb{Q}_\ell)(i), \quad Z \mapsto \gamma_X(Z)$$

が存在し、次をみたす.

- $f: X \rightarrow Y$ に対し $f^* \circ \gamma_Y = \gamma_X \circ f^*$, $f_* \circ \gamma_X = \gamma_Y \circ f_*$.
- $Z \in C^i(X), W \in C^j(Y)$ に対し, $\gamma_{X \times Y}(Z \times W) = \gamma_X(Z) \otimes \gamma_Y(W)$.
- X が 1 点のときは, $C^0(X) = \mathbb{Z}$, $H^0(X \otimes_K \bar{K}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ である. $\gamma_X: \mathbb{Z} \rightarrow \mathbb{Q}_\ell$ は 1 を 1 にうつす.

$\gamma_X(Z)$ を Z の定める **コホモロジー類** という. Z が余次元 i , W が余次元 $n-i$ であれば, $Z \cdot W = \gamma_X(Z) \cdot \gamma_Y(W)$ がなりたつことが証明できる (左辺は Z と W の **交点数**. 右辺はコホモロジー類のカップ積に向き付け写像を合成したもの).

Galois 表現への応用上は, 次の性質が重要である.

性質 8 (標数 p 還元における不変性): X を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数多様体とし, 代数体上の滑らかな射影的代数多様体 Y の標数 p 還元として得られると仮定する. すなわち, Y の定義方程式の係数を $\text{mod } m_v$ (v は p の上にある K の有限素点, $m_v \subset O_K$ は対応する O_K の極大イデアル) したものが X の定義方程式であるとする. K の v における完備化を K_v とおく. ℓ を q と互いに素な素数とし, 体の埋め込み $\bar{K} \hookrightarrow \bar{K}_v$ を固定する. このとき, $\text{Gal}(\bar{K}_v/K_v)$ の作用と可換な同形

$$H^i(Y \otimes_K \bar{K}, \mathbb{Q}_\ell) \cong H^i(X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q, \mathbb{Q}_\ell)$$

が存在する.

この同形から, 特に, $\text{Gal}(\bar{K}_v/K_v)$ の左辺への作用は全射 $\text{Gal}(\bar{K}_v/K_v) \twoheadrightarrow \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ を経由するから, 惰性群 I_v の作用は自明であり, $H^i(Y \otimes_K \bar{K}, \mathbb{Q}_\ell)$ から得られる K の ℓ 進表現が v で不分岐であることが分かる. また, 一般に, Y を代数体 K 上の滑らかな射影的代数多様体とすると, Y のエタールコホモロジーから定まる ℓ 進表現が有限個を除くすべての v で不分岐⁴⁴であることも分かる.

性質 9 (有限体上の Frobenius 射): X を有限体 $\mathbb{F}_q$ 上の代数多様体とし, $\text{Frob}_q \in \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ を **幾何的 Frobenius 元** (q 乗写像の逆写像) とする. また, $F: X \rightarrow X$ を **Frobenius 射** とする. このとき, Frob_q と F が $H^i(X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q, \mathbb{Q}_\ell)$ に誘導する写像は等しい.

これが Frob_q を “幾何的” Frobenius 元と呼んだ理由である.

⁴⁴ Y の定義方程式の係数を $\text{mod } m_v$ したものが剰余体 $\kappa(v)$ 上の滑らかな代数多様体を定め (このような v において Y は **良い還元** を持つという), さらに剰余体 $\kappa(v)$ において ℓ が可逆であるとき, Y のエタールコホモロジーから定まる ℓ 進表現は v において不分岐である.

3.6. Lefschetz 跡公式. 上に述べた性質を用いることで、エタールコホモロジーに対する Lefschetz 跡公式が示される.

命題 3.7 (Lefschetz 跡公式). X を体 K 上の滑らかな射影的代数多様体とし, その次元を n とおく. 射 $\varphi: X \rightarrow X$ の固定点集合を $\text{Fix}(\varphi) := \{x \in X \mid \varphi(x) = x\}$ とおく. このとき,

$$\text{“}\#\text{Fix}(\varphi)\text{”} = \sum_{i=0}^{2n} (-1)^i \text{Tr}(\varphi^*; H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell))$$

がなりたつ.

証明を述べる前に, 左辺の “ $\#\text{Fix}(\varphi)$ ” について説明する. 写像 $X \rightarrow X \times X$, $x \mapsto (\varphi(x), x)$ の像を Γ_φ とおき, $\varphi: X \rightarrow X$ の **グラフ** という. また, 対角写像 $X \rightarrow X \times X$, $x \mapsto (x, x)$ の像を Δ とおく. このとき,

$$\text{“}\#\text{Fix}(\varphi)\text{”} := \Gamma_\varphi \cdot \Delta$$

と定義する. ここで, 右辺の $\Gamma_\varphi \cdot \Delta$ は 2 つの部分代数多様体 $\Gamma_\varphi, \Delta \subset X \times X$ の **交点数** であり, もし Γ_φ と Δ が **横断的に交わっていれば**, 共通部分 $\Gamma_\varphi \cap \Delta = \text{Fix}(\varphi)$ の位数と等しく, 「 φ の固定点の個数」を数えていることになる.

命題 3.7 は Γ_φ と Δ が横断的に交わっていなくてもなりたつ. 例えば, φ として恒等写像 $\text{id}: X \rightarrow X$ をとると, Δ の **自己交点数** に関する公式

$$\Delta \cdot \Delta = \sum_i (-1)^i \dim_{\mathbb{Q}_\ell} H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$$

が得られる⁴⁵. X が種数 g の滑らかな射影的代数曲線であれば, その H^1 の次元は (標数によらず) $2g$ に等しく,

$$\Delta \cdot \Delta = 2 - 2g$$

となる. これが, 予想 3.4 (2) において, $\Delta \cdot \Delta$ を **Euler 数** と呼んだ理由である.

$\alpha \in H^{2n}((X \times X) \otimes_K \overline{K}, \mathbb{Q}_\ell)(n)$ に対して, $X \times X$ の二つの成分を入れ替えたものを ${}^t\alpha$ とおき, α の **転置** という. また α は写像 (この写像も再び α で表す)

$$H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell) \longrightarrow H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell), \quad x \mapsto p_{2*}((p_1^*x) \cdot \alpha)$$

を引き起こす. (ここで, $p_1, p_2: X \times X \rightarrow X$ はそれぞれ第一, 第二成分への射影である.

$$p_{2*}: H^{i+2n}(X \otimes_K \overline{K}, \mathbb{Q}_\ell)(n) \longrightarrow H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$$

⁴⁵特に, 右辺は ℓ の選び方によらないことが分かる.

に注意.) Δ のコホモロジー類 $\gamma_{X \times X}(\Delta)$ は恒等写像を誘導し, φ のグラフ Γ_φ のコホモロジー類 $\gamma_{X \times X}(\Gamma_\varphi)$ の誘導する写像は φ^* に等しい. また, その転置 ${}^t\gamma_{X \times X}(\Gamma_\varphi)$ は φ_* を誘導する.

したがって, 命題 3.7 を示すためには, より一般的な次の命題を示せば十分である.
($\alpha = \gamma_{X \times X}(\Gamma_\varphi)$, $\beta = \gamma_{X \times X}(\Delta)$ とおけばよい)

命題 3.8 (Lefschetz 跡公式の一般化). $\alpha, \beta \in H^{2n}((X \times X) \otimes_K \overline{K}, \mathbb{Q}_\ell)(n)$ に対し, α, β が誘導する写像の合成を

$$\beta \circ \alpha: H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell) \longrightarrow H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$$

とおく. この写像の跡の交代和が次のようにして計算できる:

$$\alpha \cdot {}^t\beta = \sum_i (-1)^i \text{Tr}(\beta \circ \alpha; H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell))$$

(左辺は α と ${}^t\beta$ のカップ積で, 向き付け写像 $\alpha \cdot {}^t\beta \in H^{4n}((X \times X) \otimes_K \overline{K}, \mathbb{Q}_\ell)(2n) \cong \mathbb{Q}_\ell$ によって $\mathbb{Q}_\ell$ の元とみなす.)

証明. ([Kl], Proposition 1.3.6 を参照). Künneth 公式より

$$H^{2n}((X \times X) \otimes_K \overline{K}, \mathbb{Q}_\ell)(n) \cong \bigoplus_i H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell)(n) \otimes H^{2n-i}(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$$

であり, 定理の両辺は α, β に関して双線形なので, $\alpha = \alpha_j \otimes \alpha'_{2n-j}$, $\beta = \beta_k \otimes \beta'_{2n-k}$ と仮定してよい (添え字はコホモロジーの次数を表す). $x \in H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$ の行き先は

$$(\beta \circ \alpha)(x) = q_*(x \cdot \alpha_j) \cdot q_*(\alpha'_{2n-j} \cdot \beta_k) \cdot \beta'_{2n-k}$$

である. X から一点 P への射影を $q: X \rightarrow P$ とおいた. q_* の像は $H^*(P \otimes_K \overline{K}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ の元 (スカラー) である.

$j \neq k$ なら $q_*(\alpha'_{2n-j} \cdot \beta_k) = 0$ なので, 右辺は $\beta \circ \alpha = 0$ となる. また, 左辺については, ${}^t\beta = \beta'_{2n-k} \otimes \beta_k$ だから, $\alpha \cdot {}^t\beta = (\alpha_j \cdot \beta'_{2n-k}) \otimes (\alpha'_{2n-j} \cdot \beta_k) = 0$ となる ($j \neq k$ なら, $2n + (j - k) > 2n$ または $2n + (k - j) > 2n$ である). したがって, $0 = 0$ となって, 命題 3.8 の等式はなりたつ.

$j = k$ のときは, 命題 3.8 の等式の右辺の交代和において, $i = 2n - j$ の項のみが残る. $\beta \circ \alpha$ の像は β'_{2n-j} の定数倍に等しいから, 右辺は

$$\begin{aligned} (-1)^{2n-j} (q_*(\beta'_{2n-j} \cdot \alpha_j) \cdot q_*(\alpha'_{2n-j} \cdot \beta_j)) &= (q_*(\alpha_j \cdot \beta'_{2n-j}) \cdot q_*(\alpha'_{2n-j} \cdot \beta_j)) \\ &= (q \times q)_*(\alpha \cdot {}^t\beta) \end{aligned}$$

となり, 命題 3.8 の等式が得られる. □

X を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数多様体とし、その次元を n とおく． $m \geq 1$ とおく． Frobenius 射のべき $F^m: X \rightarrow X$ が接空間に零写像を誘導することから⁴⁶、 $X \times X$ の部分代数多様体として、Frobenius 射のグラフ Γ_F と対角集合 Δ が横断的に交わることが分かる．そして、Lefschetz 跡公式（命題 3.7）から

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}((F^*)^m; H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))$$

が分かる． (§3.4 の性質 9 より、右辺の F^* を Frob_q の作用に置き換えても同様．) このようにして、エタールコホモロジーの理論により、§3.3 で“仮定”として述べた

『Frobenius 射に対する Lefschetz 跡公式』

が実現される．

例 3.9. E を体 K 上の楕円曲線とする．例 2.9 において、 $\mathbb{Q}_\ell$ 上の 2 次元ベクトル空間

$$V = \operatorname{Hom}_{\mathbb{Q}_\ell}((\varprojlim E[\ell^n]) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell, \mathbb{Q}_\ell)$$

への $\operatorname{Gal}(\overline{K}/K)$ の作用から、 K の 2 次元 ℓ 進表現 $\rho_{E,\ell}$ が得られることを述べた（ ℓ は K で可逆な素数）． V は E の 1 次エタールコホモロジーと同形である：

$$V = H^1(E \otimes_K \overline{K}, \mathbb{Q}_\ell)$$

さらに、もし K が有限体 $\mathbb{F}_q$ であれば、Frobenius 射 F は $H^0(E \otimes_K \overline{K}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ に自明に作用し、 $H^2(E \otimes_K \overline{K}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(-1)$ に q 倍で作用する．したがって、Lefschetz 跡公式から

$$\#E(\mathbb{F}_q) = 1 - \operatorname{Tr}(F^*; V) + q$$

が得られる．そして、§3.5, 性質 9 を使うと、

$$\operatorname{Tr}(\rho_{E,\ell}(\operatorname{Frob}_q)) = 1 + q - \#E(\mathbb{F}_q)$$

が得られる．

3.7. Weil 予想 (エタールコホモロジーを用いた定式化). Weil 予想 (予想 3.4) に戻ろう．

エタールコホモロジーと Lefschetz 跡公式 (§3.6, 命題 3.7) を用いることで、§3.3 と同様の議論により、 X の合同ゼータ関数 $Z(X, T)$ に関する性質を示すことができる．その結果をまとめておこう． X を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数多様体とし、

⁴⁶これは、 $\mathbb{F}_q$ 上では $q = 0$ なので、 $f(x) = x^q$ の微分が $f'(x) = 0$ となることの帰結である．

その次元を n とおく. Frobenius 射 F のエタールコホモロジー $H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ への作用の固有値を $\alpha_{i,1}, \dots, \alpha_{i,k_i}$ とおくと, Lefschetz 跡公式 (§3.6, 命題 3.7) より

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n} (-1)^i (\alpha_{i,1}^m + \dots + \alpha_{i,k_i}^m)$$

がなりたつ. また,

$$P_i(T) := \det(1 - TF^*; H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)) = \prod_{j=1}^{k_i} (1 - \alpha_{i,j} T)$$

とおくと, X の合同ゼータ関数は

$$Z(T, X) = \prod_{i=0}^{2n} (P_i(T))^{(-1)^i} = \frac{P_1(T) \cdot P_3(T) \cdots P_{2n-1}(T)}{P_0(T) \cdot P_2(T) \cdot P_4(T) \cdots P_{2n}(T)}$$

をみtas. 特に, $Z(T, X)$ が有理関数であること (予想 3.4 (1)) が分かる. $Z(T, X)$ の関数等式 (予想 3.4 (2)) は, Poincaré 双対定理 (§3.4, 性質 5) から次のようにして導かれる. 同形

$$H^{2n-i}(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell) \cong (H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell))^*(-n)$$

から, 固有値の集合 $\{\alpha_{2n-i,1}, \dots, \alpha_{2n-i,k_{n-i}}\}$ と固有値の集合 $\{q^n \alpha_{i,1}^{-1}, \dots, q^n \alpha_{i,k_i}^{-1}\}$ は (重複度を込めて) 等しい. 特に $k_i = k_{2n-i}$ であり,

$$\left(\prod_{j=1}^{k_i} \alpha_{i,j} \right) \left(\prod_{j=1}^{k_{n-i}} \alpha_{2n-i,j} \right) = q^{nk_i}$$

となる. また,

$$P_i\left(\frac{1}{q^n T}\right) = \prod_{j=1}^{k_i} \left(1 - \frac{\alpha_{i,j}}{q^n T}\right) = (-1)^{k_i} \cdot \frac{\prod_{j=1}^{k_i} \alpha_{i,j}}{(q^n T)^{k_i}} \cdot P_{2n-i}(T)$$

が分かる. Euler 数が $\chi = k_0 - k_1 + \dots + k_{2n}$ となることに注意して,

$$Z\left(\frac{1}{q^n T}, X\right) = \pm q^{n\chi/2} \cdot T^\chi \cdot Z(T, X)$$

が得られる. また, Betti 数の一致 (予想 3.4 (4)) は §3.4 の性質 3, 性質 4, 性質 8 の帰結である.

こうして, Weil 予想は, 最も難しい Riemann 予想の類似 (予想 3.4 (3)) を除いて, エタールコホモロジーを用いて自然に証明される. 残された予想 3.4 (3) は, エタールコホモロジーへの Frob_q の作用の固有値に関する次の定理に帰着される.

定理 3.10 ([De2], [De3]). X を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数多様体とし, Frobenius 射 F のエタールコホモロジー $H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ への作用の固有値を $\alpha_{i,1}, \dots, \alpha_{i,k_i}$

とおくと、任意の j ($1 \leq j \leq k_i$) に対し、 $\alpha_{i,j}$ は代数的数で、そのすべての共役の複素絶対値は $q^{i/2}$ に等しい。

Deligne は定理 3.10 に対し、2通りの（少しだけ異なる）証明を与えた。（今日では [De2] は “Weil I”, [De3] は “Weil II” と呼ばれている。）特に “Weil II” において、Weil 予想はエタール ℓ 進層に一般化された形で証明されており、その結果はその後の数論幾何の発展の基礎となった⁴⁷。

Deligne による定理 3.10 の証明は、Grothendieck が当初期待していたもの（これについては次節で説明する）とは異なるものであった。残念ながらここでは Deligne の証明を紹介することはできないが、その証明は、関数体上の L 関数の収束性に関する解析数論の技法に、Lefschetz ペンシルのモノドロミーという位相幾何学的なアイデアを組み合わせた驚くべきものであるということを述べておこう。

3.8. Weil 予想の応用. Weil 予想（および Deligne の定理（定理 3.10））は、それ自身重要であるのみならず、多くの応用を持つ。そのうちのいくつかを挙げよう。

K を体とし、 X を K 上の滑らかな射影的代数多様体とする。 ℓ を K で可逆な素数とする。 X の ℓ 進 Betti 数をエタールコホモロジーの次元

$$b_{\ell,i}(X) := H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$$

で定義する。これが ℓ によらないことはエタールコホモロジーに関する基本的な問題である。§3.6 で $b_{\ell,i}(X)$ の交代和（Euler 数）が ℓ によらないことを述べたが、実は、定理 3.10 を用いることで、各 $b_{\ell,i}(X)$ が ℓ によらないことを証明することができる。（本稿では説明していないが）特殊化の議論により、標数が ℓ と異なる有限体の場合に帰着できる⁴⁸。 $K = \mathbb{F}_q$ とおく。 X の合同ゼータ関数は

$$Z(T, X) = \prod_{i=0}^{2n} (P_i(T))^{(-1)^i} = \frac{P_1(T) \cdot P_3(T) \cdots P_{2n-1}(T)}{P_0(T) \cdot P_2(T) \cdot P_4(T) \cdots P_{2n}(T)}$$

と書ける。関数 $Z(T, X)$ は ℓ によらずに（べき級数として）定義され、 T の関数として複素平面全体に一意的に解析接続される⁴⁹ことに注意しよう。定理 3.10 を用いると、関数 $Z(T, X)$ の極また零点のうち、その絶対値が $q^{-i/2}$ に等しいものの個数を重複度を込めて数えたものが $\deg P_i(T) = b_{\ell,i}(X)$ に等しいことが分かる。こうして、 $b_{\ell,i}(X)$

⁴⁷その後、Laumon, Katz による “ ℓ 進 Fourier 変換” を用いた別証明も得られている ([La], [Katz])。また、Kedlaya による “ p 進版 Weil II” もある ([Ked])。

⁴⁸ K の標数が 0 の場合は、 $\mathbb{C}$ に帰着する証明も可能である。 $K = \mathbb{C}$ の場合、 ℓ 進 Betti 数は $X(\mathbb{C})$ の（位相空間としての）Betti 数に等しいから、特に ℓ によらない。

⁴⁹ T に関する有理関数なので、これは当たり前である。

が ℓ によらないことが証明される⁵⁰．同様の議論で，Weil 予想を標数 0 の代数多様体の Betti 数の計算に応用することもできる．すなわち，標数 0 の体上の滑らかな射影的代数多様体 X に対し，その $\text{mod } p$ 還元の有理点の個数を計算し，合同ゼータ関数を求めることで， $X(\mathbb{C})$ の Betti 数を計算するのである．例えば，トーリック多様体の場合の Betti 数の計算が [Fu] にある．これ以外にも，ある種のベクトルバンドルのモジュライ空間や ([HN])，Calabi-Yau 多様体の Betti 数の計算に応用することもできる ([Ba])⁵¹．

§2.2, §2.9 でも述べたが，Weil 予想の著しい応用として，Ramanujan 予想の解決が挙げられる．これは，無限積の展開係数

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

で定義される Ramanujan の τ 関数が，任意の素数 p に対し

$$|\tau(p)| \leq 2p^{11/2}$$

をみたすというものであり，久賀 - 佐藤多様体と呼ばれる 11 次元代数多様体 X の標数 p 還元のコホモロジー環の合同ゼータ関数が

$$1 - \tau(p)T + p^{11}T^2$$

という因子を持つことを示すことによって証明される．もう少し正確にいうと， X の 11 次元エタールコホモロジー $H^{11}(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ には Ramanujan の Δ 関数に対応する 2 次元ベクトル空間⁵²が含まれており，そこでの幾何的 Frobenius 元 Frob_p の固有多項式 α_p, β_p が

$$(1 - \alpha_p T)(1 - \beta_p T) = 1 - \tau(p)T + p^{11}T^2$$

をみたすのである．定理 3.10 により $|\alpha_p| = |\beta_p| = p^{11/2}$ であるから，

$$|\tau(p)| = |\alpha_p + \beta_p| \leq 2p^{11/2}$$

となって，Ramanujan 予想が導かれる ([De1], [De2]) ．

これ以外にも，代数曲線や超平面の $\mathbb{F}_q$ -有理点の個数の良い評価（楕円曲線の場合の Hasse の定理（例 3.6）の一般化）や，三角和の評価，関数体上の佐藤-Tate 予想への応用もある．([De2], [De3], [La] を参照．関数体上の佐藤-Tate 予想については，[Yo] も参照．)

⁵⁰一般の代数多様体 X （滑らかでない，あるいは射影的でない）に対しても ℓ 進 Betti 数は定義できるが，一般には，それが ℓ によらないことは未解決である．これ以外にも，エタールコホモロジーに関しては，様々な未解決問題がある．Illusie による最近の論説 [Ill] を参照．

⁵¹手前味噌だが，Hodge 数の計算への応用については [It1], [It2] もある．

⁵²§2.9 の言葉を使うと，『 Δ に伴う ℓ 進表現が X の 11 次元エタールコホモロジーに現れる』となる．

3.9. **強 Lefschetz 定理.** Deligne は “Weil II” において次の定理を証明した⁵³.

定理 3.11 (強 Lefschetz 定理 ([De3])). K を体とし, ℓ を K で可逆な素数とする. X を K 上の滑らかな射影的代数多様体とする. X の次元を n とおく. X は射影的なので, (十分大きな次元の) 射影空間に含まれる: $X \subset \mathbb{P}^m$. $H \subset \mathbb{P}^m$ を超平面とし, 超平面切断 $H \cap X$ は滑らかであると仮定する. $\gamma_X(H \cap X) \in H^2(X \otimes_K \overline{K}, \mathbb{Q}_\ell)(1)$ とカップ積をとる写像を

$$L: H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell) \longrightarrow H^{i+2}(X \otimes_K \overline{K}, \mathbb{Q}_\ell)(1), \quad x \mapsto x \cdot \gamma_X(H \cap X)$$

とおく (L を **Lefschetz 作用素** という). 任意の $i \geq 1$ に対し, L を i 回繰り返して得られる次の写像は同形である:

$$L^i: H^{n-i}(X \otimes_K \overline{K}, \mathbb{Q}_\ell) \longrightarrow H^{n+i}(X \otimes_K \overline{K}, \mathbb{Q}_\ell)(i)$$

強 Lefschetz 定理と関係した定理として, **弱 Lefschetz 定理**がある. これは, 包含写像を $h: H \cap X \hookrightarrow X$ とおくと, 引き戻し写像

$$h^*: H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell) \longrightarrow H^i((H \cap X) \otimes_K \overline{K}, \mathbb{Q}_\ell)$$

は $i \leq n-2$ で同形であり, $i = n-1$ で単射であるという定理であり, 強 Lefschetz 定理よりもずっとやさしい (“Weil II” よりも前に, [SGA] ですでに証明されている). 強 Lefschetz 定理から弱 Lefschetz 定理 (の一部) が次のようにして導かれる (もちろんこれは論理的には正しい順序ではないが): サイクル写像の基本的性質により,

$$h_* \circ h^*: H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell) \longrightarrow H^{i+2}(X \otimes_K \overline{K}, \mathbb{Q}_\ell)(1)$$

は Lefschetz 作用素 L と等しいことが示される. したがって, もし定理 3.11 の L^i が同形なら, H^{n-i} 上で h^* は単射である⁵⁴.

3.10. **Hasse-Weil ゼータ関数と Galois 表現の L 関数.** Hasse-Weil ゼータ関数と Galois 表現の L 関数の関係についてまとめておこう. (Galois 表現の L 関数については定義 2.3 を参照. また, Hasse-Weil ゼータ関数については定義 3.1 を参照.)

⁵³定理 3.11 がなぜ Weil 予想 (定理 3.10) と関係するのか不思議に思う読者も多いと思う. 詳しくは原論文 [De3] を参照していただきたいが, その証明の方針をとて雑に述べると次の通り: 定理 3.11 はカップ積から定まるある双線形形式が非退化であることと同値である. Lefschetz ペンシルのモノドロミーを考えることで, あるエタール ℓ 進層が半単純であることに帰着される. これは, エタール ℓ 進層の圏が半単純であるという Deligne の定理から分かる (定理 3.10 (の一般化) を用いて, $(\text{Ext}^1$ と関係する) ある種の H^1 への幾何的 Frobenius 元の作用が 1 を固有値に持たないことを示すのがポイント). “Weil II” の偏屈層への一般化については [BBD] を参照.

⁵⁴ $i \leq n-2$ なら h^* が同形であることは, $X, H \cap X, U = X \setminus (H \cap X)$ のエタールコホモロジーを比較する長完全系列の存在と, (滑らかな) アフィン多様体 U の (コンパクト台付き) エタールコホモロジーが $i < n$ で消えることから分かる.

K を代数体とし、 X を K 上の滑らかな射影的代数多様体とする。 X の次元を n とおき、素数 ℓ を固定する。 X の i 次 ℓ 進エタールコホモロジー $H^i(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$ から K の ℓ 進表現が得られる。これを $\rho_{X,\ell}^i$ とおく。次の交代積を考えよう。

$$\zeta_{X,\ell}(s) := \prod_{i=0}^{2n} L(s, \rho_{X,\ell}^i)^{(-1)^i}$$

ここで、 $\zeta_{X,\ell,v}(s) = \prod_{i=0}^{2n} L_v(s, \rho_{X,\ell}^i)^{(-1)^i}$ とおくと、

$$\zeta_{X,\ell}(s) = \prod_{v \text{ は } K \text{ の有限素点}} \zeta_{X,\ell,v}(s)$$

と書ける。

$\text{Spec } O_K$ 上有限型のスキームで $\mathfrak{X} \otimes_{O_K} K = X$ をみたすものをとる⁵⁵。 $\mathfrak{X}$ の Hasse-Weil ゼータ関数を $\zeta(s, \mathfrak{X})$ とおく。 v における特殊ファイバー $\mathfrak{X}_v := \mathfrak{X} \otimes_{O_K} (O_K/m_v)$ の Hasse-Weil ゼータ関数を $\zeta(s, \mathfrak{X}_v)$ とおくと、

$$\zeta(s, \mathfrak{X}) = \prod_{v \text{ は } K \text{ の有限素点}} \zeta(s, \mathfrak{X}_v)$$

がなりたつ。

そして、有限個の v を除いて、等式

$$\zeta_{X,\ell,v}(s) = \zeta(s, \mathfrak{X}_v)$$

がなりたつ⁵⁶。

まとめておこう。

『エタールコホモロジーを用いることで、代数体 K 上の代数多様体 X から ℓ 進表現 $\rho_{X,\ell}^i$ を作ることができる。 ℓ 進表現の L 関数 $L(s, \rho_{X,\ell}^i)$ の交代積 $\zeta_{X,\ell}(s)$ は、高々有限個の v に関する因子を除いて、 X の O_K 上の整モデル $\mathfrak{X}$ の Hasse-Weil ゼータ関数 $\zeta(s, \mathfrak{X})$ に等しい。』

3.11. エタールコホモロジーに関する文献について。Weil 予想やエタールコホモロジーに関する文献は多い。日本語の教科書としては [Kato] の出版が予定されている。代数幾何学の標準的な教科書である [Har] (最近、和訳も出版された) には、付録に

⁵⁵このような $\mathfrak{X}$ を X の O_K 上の**整モデル**という。整モデルは一意的ではないが常に存在する。 X は有限個の K 係数の多項式で定義されるから、 X の定義方程式の分母を適当に払うことで、 O_K 係数の多項式で定義されていると仮定してよい。それらの多項式で定義された $\text{Spec } O_K$ 上のスキームを $\mathfrak{X}$ とおけばよい。

⁵⁶整モデル $\mathfrak{X}$ を“うまく”選べば、この等式が「すべての v でなりたつ」こともある。例えば、楕円曲線 (やアーベル多様体) の場合は **Néron モデル**がそのような整モデルを与える。

Weil 予想とエタールコホモロジーに関する簡単な解説が書かれている．また，[Hot] には，代数曲線に対する Weil 予想の「初等的証明」(Bombieri による ([Bo])) が解説されている．これ以外にも，英語で書かれた教科書としては，[FK], [Mil] などがある．([FK] の冒頭には Dieudonné による歴史的解説があり，興味深い．) アーベル多様体に対する Weil 予想の証明が書かれた文献としては [Mum] がある．しかし，エタールコホモロジーの理論の構成や定理の証明がきちんと書かれた文献は，いまだに原典 [SGA] (Weil 予想については [De2], [De3]) しかないようである．[SGA] には他の文献では省略されている部分 — コホモロジー論の基礎となる部分 — が丁寧に (丁寧すぎる程) 書かれており，その背後にある (理論の構築とはこうあるべきである，定義・定理・証明とはこうあるべきであるという) Grothendieck の思想が色濃く反映されている．すべてを読み通すのは不可能に近いが，(学生のうちに) 苦勞して読めば，苦勞した分だけ得るものがあることは間違いないので，本稿をここまで読み進めることができた読者は (!)，ぜひ [SGA], [De2], [De3] に挑戦していただきたい．

4. GROTHENDIECK の夢 — スタンダード予想とモチーフの理論, WEIL 予想, JANNSEN の定理

エタールコホモロジーを用いることで, Riemann 予想の類似 (予想 3.4 (3)) を除き, Weil 予想 (予想 3.4) は見通しよく証明されることを述べた. では, 残された Riemann 予想の類似 (予想 3.4 (3)) を証明するためには, どうすればよいだろうか? Grothendieck の大胆なアイデアは,

『Weil 予想は良い性質をもつコホモロジー理論と, 代数的サイクルに関する予想 (スタンダード予想) から **自然に導かれる** だろう.』

というものであった.

Grothendieck は, 存在が期待される良い性質をもつコホモロジー理論を **Weil コホモロジー** と呼び, その公理的な枠組みを与え, **スタンダード予想** と呼ばれる 2 つの予想 (予想 4.3, 予想 4.4) を提出した. これらの予想は, Weil による代数曲線やアーベル多様体の場合の証明や, Serre による Weil 予想の複素数体 $\mathbb{C}$ 上の類似の証明に触発されたものであった. そして, Weil コホモロジーの存在と 2 つのスタンダード予想を **仮定した上で**, Weil 予想が自然に証明されることを示した. さらに, 代数多様体のコホモロジーをすべて支配するような理論 — **モチーフの理論** — が存在することを示した.

本節では, Grothendieck による Weil 予想の証明のアイデアを紹介する. そして, Grothendieck が夢見た「モチーフの理論」について説明する. (詳しくは, [Groth], [Ma], [K1], [K12], [Seattle] を参照⁵⁷.)

4.1. Weil コホモロジーの “公理”. 基礎体として代数的閉体 K を, 係数体として標数 0 の体 L を固定する. L を係数体とした **Weil コホモロジー** とは, K 上の滑らかな射影的代数多様体 X に対して, L 上の次数付き代数 $H^*(X)$ を対応させる規則:

$$X \mapsto H^*(X) = \bigoplus_i H^i(X)$$

であって, $H^*(X)$ の積 (**カップ積** という) は $\alpha \in H^i(X)$, $\beta \in H^j(X)$ に対し $\alpha \cdot \beta = (-1)^{ij} \beta \cdot \alpha$ をみたす反変関手であり ($f: X \rightarrow Y$ に対し, 次数を保つ L 代数準同形写像 $f^*: H^*(X) \rightarrow H^*(Y)$ が定まる. f が恒等射なら f^* は恒等写像で, $f: X \rightarrow$

⁵⁷Grothendieck Circle のホームページ <http://www.grothendieckcircle.org/> から, Grothendieck に関する様々な文献をダウンロードすることができる. 未出版の原稿や, Grothendieck がモチーフについて述べた手紙を入手することもできる.

$Y, g: Y \rightarrow Z$ に対し $(g \circ f)^* = f^* \circ g^*$ をみたす), さらに以下の性質 1~6 をみたすものをいう.

性質 1 (有限性): 各 $H^i(X)$ は L 上の有限次元ベクトル空間である. X の次元が n なら, $i < 0$ または $i > 2n$ において $H^i(X) = 0$ である.

性質 2 (Poincaré 双対定理): X の次元を n とすると, 向き付け写像と呼ばれる同形 $H^{2n}(X) \xrightarrow{\cong} L$ が関手的に定まる. さらに, カップ積と向き付け写像から定まる双線形形式

$$H^i(X) \times H^{2n-i}(X) \longrightarrow H^{2n}(X) \cong L, \quad (\alpha, \beta) \mapsto \alpha \cdot \beta$$

は非退化である. X の次元を n, Y の次元を m としたとき, 射 $f: X \rightarrow Y$ による引き戻し写像 $f^*: H^i(Y) \longrightarrow H^i(X)$ の Poincaré 双対を

$$f_*: H^i(X) \longrightarrow H^{i+2(m-n)}(Y)$$

で表す.

性質 3 (Künneth 公式): X, Y に対し, 直積からの射影をそれぞれ $p: X \times Y \rightarrow X, q: X \times Y \rightarrow Y$ とおく. このとき, 写像

$$H^*(X) \otimes H^*(Y) \xrightarrow{\cong} H^*(X \times Y), \quad \alpha \otimes \beta \mapsto (p^*\alpha) \cdot (q^*\beta)$$

は同形である.

性質 4 (サイクル写像): X 上の余次元 i の代数的サイクルのなす群を $C^i(X)$ とおく. サイクル写像と呼ばれる写像

$$\gamma_X: C^i(X) \longrightarrow H^{2i}(X)$$

が存在し, 次をみたす.

- $f: X \rightarrow Y$ に対し $f^* \circ \gamma_Y = \gamma_X \circ f^*, f_* \circ \gamma_X = \gamma_Y \circ f_*$.
- $Z \in C^i(X), W \in C^j(Y)$ に対し, $\gamma_{X \times Y}(Z \times W) = \gamma_X(Z) \otimes \gamma_Y(W)$.
- X が 1 点のときは, $C^0(X) = \mathbb{Z}, H^0(X) = L$ である. $\gamma_X: \mathbb{Z} \rightarrow L$ は 1 を 1 にうつす.

性質 5 (弱 Lefschetz 定理): X の次元を n とおく. X は射影的なので, (十分大きな次元の) 射影空間に含まれる: $X \subset \mathbb{P}^m$. $H \subset \mathbb{P}^m$ を超平面とし, 超平面切断 $H \cap X$ は滑らかであると仮定する. 包含写像を $h: H \cap X \hookrightarrow X$ とおくと, 引き戻し写像

$$h^*: H^i(X) \longrightarrow H^i(H \cap X)$$

は $i \leq n-2$ で同形であり, $i = n-1$ で単射である.

性質 6 (強 Lefschetz 定理): 性質 5 と同様の仮定の下で, **Lefschetz 作用素**を次のように定める:

$$L: H^i(X) \longrightarrow H^{i+2}(X), \quad \alpha \mapsto L\alpha := \alpha \cdot \gamma_X(H \cap X)$$

($H \cap X$ は X の余次元 1 の代数的サイクルなので, $\gamma_X(H \cap X) \in H^2(X)$ である.) 任意の $i \geq 1$ に対し, 次の写像は同形である:

$$L^i: H^{n-i}(X) \xrightarrow{\cong} H^{n+i}(X).$$

$P^{n-i}(X) := \text{Ker}(L^{i+1}: H^{n-i}(X) \rightarrow H^{n+i+2}(X))$ を**原始部分**という. 性質 6 から, $i \leq n$ に対し, $H^i(X)$ は**原始分解**

$$H^i(X) = P^i(X) \oplus LH^{i-2}(X) = \bigoplus_{j \geq 0} L^j P^{i-2j}(X)$$

を持つことが分かる. 次数を 2 だけ下げる作用素

$$\Lambda: H^i(X) \longrightarrow H^{i-2}(X)$$

を次のように定義する. $0 \leq i \leq n$ のとき, 任意の $x \in H^i(X)$ は $x = \sum_{j \geq 0} L^j x_j$ ($x_j \in P^{i-2j}(X)$) と一意的に書ける. $\Lambda x = \sum_{j \geq 1} L^{j-1} x_j$ と定める. $n < i \leq 2n$ のとき, 任意の $x \in H^i(X)$ は $x = \sum_{j \geq i-n} L^j x_j$ ($x_j \in P^{i-2j}(X)$) と一意的に書ける. $\Lambda x = \sum_{j \geq i-n} L^{j-1} x_j$ と定める.

4.2. Weil コホモロジーの例. 今日では様々な種類のコホモロジー理論が §4.1 の公理をみたすことが知られている.

- (1) 基礎体 K を複素数体 $\mathbb{C}$ の部分体とする (例えば, $K = \mathbb{C}$ や $\overline{\mathbb{Q}}$). 係数体を $L = \mathbb{Q}$ とおく. $X(\mathbb{C})$ は複素多様体である (特に位相多様体である) から, その特異コホモロジー (**Betti コホモロジー**)

$$H^*(X(\mathbb{C}), \mathbb{Q}) = \bigoplus_i H^i(X(\mathbb{C}), \mathbb{Q})$$

を考えることができる. これは Weil コホモロジーの公理をみたす.

- (2) 基礎体 K を標数 0 の代数的閉体とし, 係数体を $L = K$ とおく. X 上の代数的 de Rham 複体の超コホモロジーにより, X の **de Rham コホモロジー**

$$H_{DR}^*(X/K) = \bigoplus_i H_{DR}^i(X/K)$$

が定まる. これは Weil コホモロジーの公理をみたす. ($K = \mathbb{C}$ であれば, これは Betti コホモロジーに “ $\otimes_{\mathbb{Q}} \mathbb{C}$ ” したものと同形である.)

- (3) 基礎体 K を任意の代数的閉体とし, ℓ を K で可逆な素数とする. 係数体を $L = \mathbb{Q}_\ell$ とおく. $\mathbb{Q}_\ell$ 上のベクトル空間としての同形 $\mathbb{Q}_\ell \cong \mathbb{Q}_\ell(1)$ を固定する. X の $(\ell$ 進) エタールコホモロジー

$$H^*(X, \mathbb{Q}_\ell) = \bigoplus_i H^i(X, \mathbb{Q}_\ell)$$

は Weil コホモロジーの公理をみたす. 性質 1~5 は [SGA] で証明されている. 性質 6 は Deligne が “Weil II” ([De3]) で証明している (§3.9 を参照).

- (4) 基礎体 K を標数 $p > 0$ の代数的閉体とし, L を Witt 環 $W(K)$ の商体とする⁵⁸. このとき, X のクリスタルコホモロジー

$$H_{\text{crys}}^*(X/W(K)) \otimes_{W(K)} L = \bigoplus_i H_{\text{crys}}^i(X/W(K)) \otimes_{W(K)} L$$

は Weil コホモロジーの公理をみたす. 性質 4 以外は Katz-Messing が, Deligne による “Weil II” の結果を用いて, ℓ 進エタールコホモロジーの場合に帰着して証明している ([KM]). 性質 4 は Gillet-Messing, Gros による ([GM], [Gros]).

4.3. スタンダード予想と Weil 予想. ここでは, 「Weil コホモロジー」を 1 つ固定して考える. §3.6 に述べた方法と同様にして, §4.1 の性質のみから, Lefschetz 跡公式が形式的に導かれる (性質 5, 性質 6 は不要である). そして, 合同ゼータ関数の有理性 (予想 3.4 (1)) と関数等式 (予想 3.4 (2)) が自然に証明される.

以下では, X を代数的閉体 K 上の滑らかな射影的代数多様体とし, X の次元を n とおく.

定義 4.1. X 上の余次元 i の代数的サイクル $\alpha, \beta \in C^i(X)$ が **数値的同値** であるとは, 任意の $\gamma \in C^{n-i}(X)$ との交点数が等しいことをいう: $\alpha \cdot \gamma = \beta \cdot \gamma$. また, $\alpha, \beta \in C^i(X)$ が **ホモロジー同値** であるとは, サイクル写像の像が等しいことをいう: $\gamma_X(\alpha) = \gamma_X(\beta)$.

予想 4.2. $\alpha, \beta \in C^i(X)$ が数値的同値であることと, ホモロジー同値であることは同値. 特に, 「ホモロジー同値」は Weil コホモロジーのとり方によらない⁵⁹.

Grothendieck は Riemann 予想の類似 (予想 3.4 (3)) を証明するために, スタンダード予想と呼ばれる予想を提出した.

⁵⁸ $L = \text{Frac } W(K)$ は標数 0 の完備離散付値体で, p が素元で, K が剰余体となるもの.

⁵⁹ α, β がホモロジー同値であれば数値的同値であることの証明はやさしい. 逆向きは一般には知られていない.

予想 4.3 (Lefschetz スタンダード予想). 原始分解から定まる作用素 $\Lambda: H^i(X) \rightarrow H^{i-2}(X)$ は代数的サイクルから来る. すなわち, $X \times X$ 上の余次元 $n-1$ の代数的サイクル $\alpha \in C^{n-1}(X \times X)$ が存在して, 各 i に対して, α が導く写像

$$H^i(X) \longrightarrow H^{i-2}(X), \quad x \mapsto p_{2*}((p_1^*x) \cdot \alpha)$$

は Λ に等しい.

予想 4.4 (Hodge スタンダード予想). $i \leq n/2$ とする. $\gamma_X: C^i(X) \rightarrow H^{2i}(X)$ の像で生成された $\mathbb{Q}$ 上のベクトル空間を $A^i(X)$ とおく⁶⁰. $\mathbb{Q}$ 上のベクトル空間 $A^i(X) \cap P^{2i}(X)$ ($P^{2i}(X)$ は原始部分) に定まる双線形形式

$$(A^i(X) \cap P^{2i}(X)) \times (A^i(X) \cap P^{2i}(X)) \longrightarrow \mathbb{Q}, \quad (x, y) \mapsto (-1)^i (L^{n-2i}x \cdot y)$$

は正定値である. すなわち, $x \in A^i(X) \cap P^{2i}(X)$, $x \neq 0$ に対し, $(-1)^i (L^{n-2i}x \cdot x) > 0$.

予想 4.4 は Hodge 理論における不等式を代数的サイクルの言葉で述べたものであり, $n \leq 2$ なら解決されている. また, K の標数が 0 なら, $K = \mathbb{C}$ の場合に帰着して Hodge 理論を用いて証明することができる. 一方で, 予想 4.3 は ($K = \mathbb{C}$ でも) 未解決である. 予想 4.3 と予想 4.4 から, 予想 4.2 が導かれることが知られている.

Grothendieck は, Weil や Serre の結果を踏まえて, 「Weil コホモロジーの存在」と「スタンダード予想 (予想 4.3, 予想 4.4)」から Riemann 予想の類似 (予想 3.4 (3)) が導かれることを示した. (詳しくは [Groth], [Kl], [Kl2] を参照.)

定理 4.5 (Weil コホモロジーの存在 + スタンダード予想 $\Rightarrow$ Weil 予想). $K = \overline{\mathbb{F}}_q$ とする. §4.1 の“公理”をみたす Weil コホモロジーを一つ固定し (存在を仮定する), さらに K 上の滑らかな射影的代数多様体に対して予想 4.3 と予想 4.4 がなりたつと仮定する. このとき, $\mathbb{F}_q$ 上の滑らかな射影的代数多様体 X に対し, Frobenius 射 F の $H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q)$ への作用は半単純である⁶¹. さらに, F の固有値 α は代数的数で, そのすべての共役の複素絶対値は $q^{i/2}$ に等しい.

こうして Riemann 予想の類似 (予想 3.4 (3)) の主張は

- §4.1 の“公理” (性質 1~6) をみたす「Weil コホモロジー」の存在
- 2つのスタンダード予想 (予想 4.4, 予想 4.4)

に帰着された. 1968 年にスタンダード予想を提出した論文 [Groth] の 198 ページにおいて, Grothendieck は次のように述べている:

⁶⁰すなわち, $A^i(X)$ は $C^i(X) \otimes \mathbb{Q}$ をホモロジー同値で割った群である

⁶¹すなわち, 対角化可能な行列で表されるということ.

『特異点解消問題と並んで、スタンダード予想の解決は代数幾何学における最も急を要する課題であると思われる。』

しかしながら、今日でも、スタンダード予想は（両方とも）未解決である． Weil 予想は Deligne によって解決されたが ([De2], [De3]), その証明は Grothendieck が当初想定していたものとは異なり、スタンダード予想を用いないものであった⁶²．

Grothendieck 自身は、Weil 予想の証明を目指して Weil コホモロジーの枠組みを与えたものの、自らが創始したエタールコホモロジーがその“公理”を満たすことは証明できなかった．（実際、[SGA] においては、エタールコホモロジーに関する強 Lefschetz 定理は未解決問題として残っている．）§4.2 でも述べたように、エタールコホモロジーは Weil コホモロジーの“公理”をみたす．しかし、皮肉なことに、その証明には、Deligne による “Weil II” ([De3]) の結果が用いられる．Grothendieck の当初の期待とは逆に、Weil 予想（の Deligne による一般化）の帰結として、Weil コホモロジーの存在が証明されたのである．

4.4. Grothendieck 理論の夢 — モチーフの圏 “ $\mathcal{M}_K$ ”，半単純性． 代数多様体のコホモロジーは様々な種類の分解を持つ．もちろん、コホモロジーの次数による分解

$$H^*(X) = \bigoplus_i H^i(X)$$

は常に存在する．もし X が $X = Y \times Z$ という形に直積に分解されていれば、Künneth 公式による分解

$$H^i(X) = \bigoplus_{j+k=i} H^j(Y) \otimes H^k(Z)$$

がある．また、一般に強 Lefschetz 定理 (§4.1, 性質 6) から導かれる原始分解

$$H^i(X) = \bigoplus_{j \geq 0} L^j P^{i-2j}(X)$$

がある．こうした“分解”はすべての「Weil コホモロジー」でなりたつ． X 自身が何らかの意味で（コホモロジー理論によらない形で）“分解”していて、上で見たコホモロジーの分解はその表れである、と考えることはできないだろうか？

⁶² q と互いに素な素数 ℓ に対し、 ℓ 進エタールコホモロジーは Weil コホモロジーである．この場合、定理 4.5 の一つ目の主張、すなわち、Frobenius 射 F のエタールコホモロジー $H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ への作用が半単純であることは未解決である．

Grothendieck は、スタンダード予想（予想 4.3, 予想 4.4）の仮定の下に、モチーフの圏⁶³ $\mathcal{M}_K$ と反変関手

$$h: (K \text{ 上の滑らかな射影的代数多様体}) \longrightarrow \mathcal{M}_K$$

を構成し、 $X \mapsto h(X)$ が“普遍的なコホモロジー理論”の一種であることを示した。そして、(良い性質をみたす) コホモロジー理論 $X \mapsto H^*(X)$ は、この関手 h を経由することを（スタンダード予想の仮定の下で）示した。

Grothendieck によるモチーフの圏 $\mathcal{M}_K$ の構成は、次の通りである。まず、 K 上の滑らかな射影的代数多様体を対象とし、射が

$$\mathrm{Hom}(h(X), h(Y)) = C_{\mathrm{neq}}^m(X \times Y, \mathbb{Q})$$

で与えられるような圏 $\mathcal{M}'$ を考える。 X, Y に対応する対象を $h(X), h(Y) \in \mathcal{M}'$ で書いた。 n は X の次元であり、 $C_{\mathrm{neq}}^n(X \times Y, \mathbb{Q})$ は $X \times Y$ 上の余次元 n の $\mathbb{Q}$ -係数の代数的サイクルのなす群 $C^n(X \times Y) \otimes_{\mathbb{Z}} \mathbb{Q}$ を数値的同値で割った群である。 $\mathcal{M}'$ における射の合成は代数的対応の合成で定める。すなわち、 X, Y, Z (X の次元を n , Y の次元を m とおく) に対し、 $p_{12}: X \times Y \times Z \longrightarrow X \times Y$, $p_{23}: X \times Y \times Z \longrightarrow Y \times Z$, $p_{13}: X \times Y \times Z \longrightarrow X \times Z$ とおき、 $\alpha \in C_{\mathrm{neq}}^n(X \times Y, \mathbb{Q})$ と $\beta \in C_{\mathrm{neq}}^m(Y \times Z, \mathbb{Q})$ の合成を

$$\beta \circ \alpha = (p_{13})_*(p_{12}^* \alpha \cdot p_{23}^* \beta) \in C_{\mathrm{neq}}^m(X \times Z, \mathbb{Q})$$

で定める。(エタールコホモロジーと同様に、 C_{neq}^n に対しても f^*, f_* などの写像が定義できる。) この圏 $\mathcal{M}'$ に、自己準同形環 $\mathrm{Hom}(h(X), h(X))$ のベキ等元による像を付け加え、さらに対象の「Tate 捻り」(ℓ 進エタールコホモロジーの世界で Tate 捻りに対応するもの) を付け加えたものが $\mathcal{M}_K$ である。(詳しくは [Jan] を参照。)

Grothendieck は（スタンダード予想を仮定して）この圏 $\mathcal{M}_K$ が半単純アーベル圏であることを示した。これにより、任意の $h(X) \in \mathcal{M}_K$ は単純な対象の和 $h(X) = \bigoplus_i \alpha_i$ に“分解”されることが分かる。代数多様体 X を“分解”することでモチーフ α_i が得られ⁶⁴、 X のコホモロジー論的な性質はすべてこのモチーフ α_i たちがコントロールすることになる。これは極めて著しい性質である。Grothendieck がこれは“奇跡”であると言ったという記録が残っている⁶⁵。

⁶³ 今日では数値的同値モチーフ (neq motives, numerical equivalence motives) の圏と呼ばれている。

⁶⁴ 広辞苑第五版によると、モチーフには「音楽形式を構成する最小単位」という意味がある。著者にはフランス語の “motif” に込められた微妙な意味を読み取ることはできないが（安っぽい辞書を引くと、「motif = モチーフ」とだけ書かれていることもある）、代数多様体のコホモロジーの奏でる音楽を構成する「単位」という意味を込めたのかもしれない。

⁶⁵ [K12], 5 ページ, 13 行目に Kleiman による記述がある。

4.5. **Jannsen の定理.** はたして “奇跡” は起こるのだろうか. 圏 $\mathcal{M}_K$ 自身はスタンダード予想を仮定しなくても定義可能である. また, 「数値的同値」以外の同値関係 (例えば, Weil コホモロジーを一つ固定したときの「ホモロジー同値」) を用いて $\mathcal{M}_K$ と類似の圏を構成することもできる.

Grothendieck がスタンダード予想を提出してから 20 年以上が経過した 1992 年に, Jannsen は, **スタンダード予想を仮定せずに** 次の定理を示した.

定理 4.6 ([Jan]). 「数値的同値」から定義された圏 $\mathcal{M}_K$ は半単純アーベル圏である.

Jannsen によるこの定理の証明は Lefschetz 跡公式を用いた鮮やかなものであり, 非常に短い. (論文自体もたったの 6 ページである!) Jannsen は, さらに, (数値的同値とは限らない同値関係から定義された) 圏が半単純アーベル圏であるためには, その圏が数値的同値から作られることが必要十分であることを示している. したがって, もし “奇跡” を信じるならば, $\mathcal{M}_K$ が正しいモチーフの圏を与えていることになる.

スタンダード予想は現在もなお未解決であり, したがって, Grothendieck の夢がすべて実現されたわけではない. しかし, Jannsen の定理により, 少なくとも「モチーフの圏」と呼ばれるべき圏 $\mathcal{M}_K$ は得られたことになる⁶⁶.

著者は 2008 年 1 月 3 日から 12 日にかけてインドの Tata 研究所で行われた国際研究集会「代数的サイクル, モチーフ, 志村多様体」に参加し, Jannsen 氏から論文 [Jan] についての話を直接伺うことができるという幸運を得た. 本節の最後に, Jannsen 氏の言葉を引用しよう.

『私が論文 [Jan] を書いたのは, 心理的な理由によるものでした. それ以前には, 多くの人々がモチーフのことを “いわゆるモチーフと呼ばれているもの” (so-called motives) と呼んでいました. しかし, 私の論文が出版されてから, そう呼ぶ人はいなくなりました.』

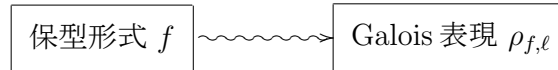
⁶⁶Jannsen の定理は応用上は不十分であることが多い. ℓ 進エタールコホモロジーが, 関手 h を経由することは証明できない. (そのためには予想 4.2 — これはスタンダード予想の帰結である — を仮定する必要がある) また, Jannsen の定理から, エタールコホモロジーへの Frobenius 作用の半単純性を導くことはできない. $\mathcal{M}_K$ が「正しい」モチーフの圏であることは疑いようはないが, スタンダード予想が解決されていない現状では, 応用上は, $\mathcal{M}_K$ よりももっと扱いやすい圏を使わざるをえないこともある.

5. 整数論における「モチーフ的な考え方」

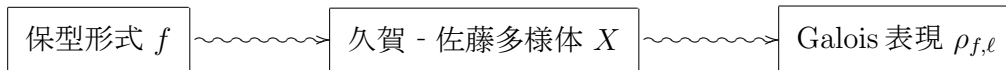
5.1. **保型形式とモチーフ.** §2.9 では, 保型形式に伴う Galois 表現について述べた. すなわち, (適当な条件をみたす) 尖点的保型形式 $f = \sum_{n=1}^{\infty} a_n q^n$ と素数 ℓ に対して, $\mathbb{Q}$ の 2 次元 ℓ 進表現 $\rho_{f,\ell}: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL(V)$ が存在し,

$$L(s, f) = L(s, \rho_{f,\ell})$$

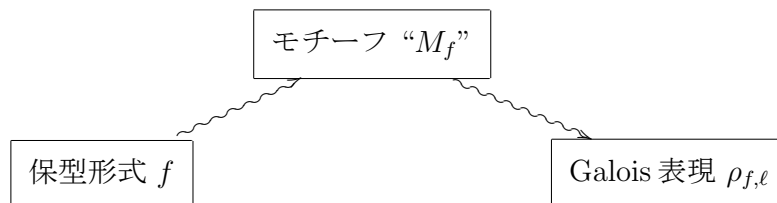
をみたす (定理 2.10) :



しかも, f の重さが $k \geq 2$ であれば, この対応は, **久賀 - 佐藤多様体** と呼ばれる $(k-1)$ 次元代数多様体 X の $(k-1)$ 次エタールコホモロジーから, Hecke 環の作用によって「 f に対応する部分」を切り取ることで作られる:



さて, §4.4 で述べた「モチーフの理論」の考え方を使って, この対応をもう少し推し進めてみよう. 久賀 - 佐藤多様体 X 上には Hecke 作用素が代数的対応として作用するから, その作用により X のモチーフ “ $h(X) \in \mathcal{M}_K$ ” を分解し, f に対応する部分モチーフ “ $M_f \in \mathcal{M}_K$ ” (保型形式 f のモチーフ) を取り出すことはできないだろうか? そして, Galois 表現 $\rho_{f,\ell}$ を, モチーフ “ M_f ” のエタールコホモロジー $H^*(M_f, \mathbb{Q}_\ell)$ として理解することはできないだろうか?



実際, これは (適当な修正の下で⁶⁷⁾ 可能であり, 保型形式のモチーフは Scholl によって構成されている.

久賀 - 佐藤多様体 X そのものよりも, X を “分解” して得られるモチーフ “ M_f ”こそが保型形式 f に対応すべきであるという考え方は重要である. 一般に, 保型形式 f

⁶⁷ スタンダード予想は未解決なので, モチーフのエタールコホモロジーを定義するためには, 「数値的同値」を「ホモロジー同値」に置き換えて論じる必要がある. 詳しくは [Sch] を参照.

に伴う Galois 表現をエタールコホモロジーを用いて構成する方法は複数あるが⁶⁸, その場合でも, 背後にあるモチーフ “ M_f ” そのものは一意的である (に違いない!) と期待することができる⁶⁹.

5.2. Fontaine-Mazur 予想. それでは, 逆に, Galois 表現 ρ から出発して, それに対応するモチーフや保型形式を作り出すことはできないだろうか? この問題に関して, Fontaine と Mazur は次の著しい予想を提出した ([FM]⁷⁰).

予想 5.1 (Fontaine-Mazur 予想). K を代数体とする. ℓ を素数とし, ρ を絶対既約な n 次元 ℓ 進表現とする. ρ が滑らかな射影的代数多様体のエタールコホモロジー (の適当な Tate 捻り) の部分商として得られることと, ρ が次の 2 つの条件

- (1) ρ が分岐する素点は有限個.
- (2) ℓ を割り切る素点 v に対し, ρ_v は de Rham.

をみたすことは同値である.

予想 5.1 の特筆すべきところは, (勝手に与えられた) ρ に対し, それが代数多様体のエタールコホモロジーから得られるためには, 条件 (1),(2) “だけ” で十分であることを (大胆にも) 予想したことにある. 特に, Weil 予想 (予想 3.4) を用いると, 条件 (1),(2) “だけ” から, 有限個を除くすべての有限素点 v に関する主張

『「重さ」と呼ばれる整数 w が存在して, 有限個を除くすべての有限素点 v に対し, v における幾何的 Frobenius 元 Frob_v の固有値は代数的数であり, そのすべての共役の複素絶対値は $q_v^{w/2}$ に等しい (q_v は v の剰余体の位数)』

が導かれてしまう⁷¹.

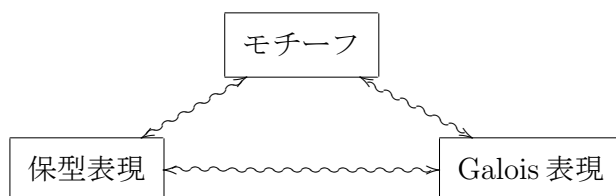
⁶⁸例えば志村曲線やある種のユニタリ型志村多様体が使える場合もある. 総実代数体への底変換 (持ち上げ) を使って構成することが可能な場合もある. また, f が虚数乗法を持つ場合には, さらに別の構成も可能である.

⁶⁹実際, 適当な予想 (Tate 予想など ([Tat])) を仮定すれば, “ M_f ” のモチーフとしての一意性を証明することもできる.

⁷⁰Fontaine-Mazur 予想については, [Tay1], [Tay3], [Kis] も参照.

⁷¹これは極めて非自明である. 各 v に対してこのような整数 w が存在することも自明ではないし, 仮に存在したとしても, そのような w が v によらないことも自明ではない! $\text{Gal}(\bar{K}/K)$ には, 各素点 v に対して (位相群としては比較的単純な) $\text{Gal}(\bar{K}_v/K_v)$ が含まれているが, これらはばらばらに含まれているのではなく, 非常に強い規則をもっていると考えることができる. これは, $\text{Gal}(\bar{K}/K)$ に対する非可換類体論あるいは非可換相互法則の一つの見方ということもできる.

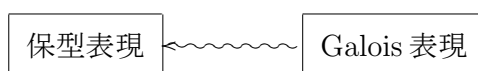
予想 5.1 に Langlands による予想を組み合わせることで、条件 (1),(2) をみたす ρ に、 $GL_n(\mathbb{A}_K)$ の尖点的な保型表現 π が対応することが予想される。したがって、



という図式が期待されることになる。

もちろん、この図式が実現されているケースは（エタールコホモロジーにより「代数多様体から Galois 表現を作る」ことが可能になったことを除けば）それほど多くはない⁷²。しかし、この図式を念頭に置きながら具体的な問題を考察することは、個々の問題への本質的なアプローチを探る上でも大切なことである。

5.3. 最近の話題 「Galois 表現からモチーフを作る」。最近では、Wiles ([Wi]) や Taylor-Wiles ([TW]) により創始された「 $R = T$ 定理」の発展により、いくつかの場合に「Galois 表現の保型性」、すなわち、



という方向の対応が得られるようになってきた。その議論の中では、「 $R = T$ 定理」に加えて、

『与えられた $\text{mod } \ell$ 表現に対し、それをエタールコホモロジー（の一部）として実現するような代数多様体（モチーフ）を構成する』

という手法が用いられる（例えば、[Wi], [SBT], [Tay1], [HSBT] を参照.）。これは、本稿で今まで述べてきた方向とは逆の、「Galois 表現からモチーフを作る」という“新しい”方向であるが、方程式論的に見ると、少なくとも 19 世紀の Hermite や Klein の研究にさかのぼる“古い”手法でもある⁷³。与えられた Galois 表現 ρ を調べるために、“都合の良いモチーフ”を作ればよいという発想は⁷⁴、今後、ますます重要になってくるかもしれない。

⁷²もちろん、類体論によって、「階数 1」の場合はこの対応が実現されている。

⁷³[SBT], 284 ページを見よ。[Se8] も参照。

⁷⁴佐藤 - Tate 予想は楕円曲線（やその自己ベキ）に対する主張であるが、その証明の中で、高次元 Calabi-Yau 超曲面のエタールコホモロジーが補助的に用いられているのは、その一例であろう ([HSBT])。

6. 演習問題

問 1. K を体とし, $\rho: \text{Gal}(\overline{K}/K) \rightarrow GL_n(\mathbb{C})$ を連続準同形とする. ただし, $\text{Gal}(\overline{K}/K)$ には Krull 位相を入れ, $GL_n(\mathbb{C})$ には普通の (位相多様体としての) 位相を入れる. このとき, ρ の像は有限群であり, ρ は Artin 表現となる (すなわち, $GL_n(\mathbb{C})$ に離散位相を入れたときに連続となる) ことを示せ.

問 2. E を ℓ 進数体 $\mathbb{Q}_\ell$ の有限次拡大とする. K を体とし, $\rho: \text{Gal}(\overline{K}/K) \rightarrow GL_n(E)$ を ℓ 進表現とする. (すなわち, $\text{Gal}(\overline{K}/K)$ には Krull 位相を入れ, $GL_n(E)$ には ℓ 進位相を入れる.) このとき, ある $g \in GL_n(E)$ が存在して, $g \cdot \rho(\text{Gal}(\overline{K}/K)) \cdot g^{-1}$ が $GL_n(O_E)$ に含まれることを示せ. (O_E は E の整数環である.)

問 3. K を体とし, $\rho: \text{Gal}(\overline{K}/K) \rightarrow GL_n(\overline{\mathbb{Q}_\ell})$ を連続準同形とする. ただし, $\text{Gal}(\overline{K}/K)$ には Krull 位相を入れ, $GL_n(\overline{\mathbb{Q}_\ell})$ には ℓ 進位相を入れる. このとき, $\mathbb{Q}_\ell$ の有限次拡大 E が存在して, ρ の像は $GL_n(E)$ に含まれることを示せ. (ヒント: Baire のカテゴリー一定理を用いよ.)

問 4. 代数体の ℓ 進表現 ρ であって, 無限個の有限素点で分岐するものを構成せよ. (このような ρ は代数多様体のエタールコホモロジー (やその Tate 捻り) の部分商として作ることとはできない.)

問 5. $a \in \mathbb{Q}$ を有理数とする. 代数体の ℓ 進表現 ρ であって, 有限個を除くすべての素点 v で不分岐で, Frob_v の固有値は代数的数で, そのすべての共役の複素絶対値が q_v^a (q_v は v の剰余体の位数) に等しいものを構成せよ. ($a \notin \frac{1}{2}\mathbb{Z}$ であれば, このような ρ は代数多様体のエタールコホモロジー (やその Tate 捻り) の部分商として作ることとはできない.)

問 6. 重さ 2, レベル 11 の保型形式

$$f = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{n=1}^{\infty} a_p q^n$$

の q 展開の係数 a_p を小さな素数 p に対して具体的に計算せよ. また, 楕円曲線 $E: Y^2Z + YZ^2 = X^3 - XZ^2$ に対し, $a_p = 1 + p - \#E(\mathbb{F}_p)$ を確かめよ. (計算機が使える人は, $p \leq 10,000$ 位まで計算してみてください.)

問 7. p を素数とし, q を p のべきとする. $\mathbb{F}_q$ 上の楕円曲線は, $1 + q - \#E(\mathbb{F}_q) \equiv 0 \pmod{p}$ をみたすとき, **超特異** という. E を代数体 K 上の楕円曲線とする. $E \bmod v$ が超特異でない有限素点 v が無限個存在することを示せ. (余力のある人は, $K = \mathbb{Q}$ の時に, 谷山-志村予想を用いた別証明も考えてみてください.) (未解決問題: Ramanujan の τ 関数について, $\tau(p)$ が p で割れない素数 p は無限個存在するか?)

問 8. 群 G , 正標数の体 E と, n 次元表現 $\rho, \rho': G \rightarrow GL_n(E)$ であって, $\text{Tr}(\rho(\sigma)) = \text{Tr}(\rho'(\sigma))$ ($\forall \sigma \in G$) だが, 半単純化 $\rho^{ss}, (\rho')^{ss}$ が同値でない例を挙げよ.

問 9. 次の代数曲線に対し合同ゼータ関数を計算せよ.

- (1) $\mathbb{F}_p$ 上のアフィン空間 $\mathbb{A}^n$, $\mathbb{A}^n \setminus \{0\}$ (0 は原点), 射影空間 $\mathbb{P}^n$, 直積 $\mathbb{P}^n \times \mathbb{P}^m$.
- (2) $\mathbb{F}_p$ 上の楕円曲線 $Y^2Z = X^3 + XZ^2$. (小さい素数 p で具体的に)
- (3) $\mathbb{F}_p$ 上の超楕円曲線 $Y^2Z^3 = X^5 - XZ^4$. (小さい素数 p で具体的に)

問 10. $\mathbb{F}_q$ 上の滑らかな射影的代数多様体 X, Y に対して Weil 予想がなりたてば, 直積 $X \times Y$ に対してもなりたつことを示せ.

問 11. X を $\mathbb{F}_q$ 上の n 次元の滑らかな射影的代数多様体とする. χ を X の Euler 数とする (χ は対角集合 $\Delta \subset X \times X$ の自己交点数). X の合同ゼータ関数 $Z(T, X)$ は, 次の形の関数等式をみたす:

$$Z\left(\frac{1}{q^n T}, X\right) = \pm q^{n\chi/2} \cdot T^\chi \cdot Z(T, X)$$

符号が $+1$ である X の例と, -1 である X の例を挙げよ.

問 12. X を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数曲線とする. X の種数を g とおく. X に対する Weil 予想 (Riemann 予想の類似) を用いて, $\mathbb{F}_q$ -有理点の個数 $\#X(\mathbb{F}_q)$ が不等式

$$|1 + q - \#X(\mathbb{F}_q)| \leq 2g\sqrt{q} \quad (\text{Hasse-Weil の不等式})$$

をみたすことを示せ. また, 逆に, すべての $n \geq 1$ に対して Hasse-Weil の不等式

$$|1 + q^n - \#X(\mathbb{F}_{q^n})| \leq 2g\sqrt{q^n}$$

がなりたてば, X は Weil 予想 (Riemann 予想の類似) をみたすことを示せ.

問 13. X を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数曲線とする. 等式 $\#X(\mathbb{F}_q) = q+1+2g\sqrt{q}$ がなりたつとき, X を**極大曲線**という.

- (1) $q = p^r$ (p は素数, r は奇数) のとき, $\mathbb{F}_q$ 上に極大曲線は存在しないことを示せ.
- (2) $q = p^r$ (p は素数, $r \geq 1$) とし, X を $\mathbb{F}_q$ 上の極大曲線とする. このとき, X の種数 g は, $g \leq q(q-1)/2$ をみたすことを示せ.
- (3) $q = p^r$ (p は素数, $r \geq 1$) とする. $Y^qZ + YZ^q = X^{q+1}$ で定まる $\mathbb{F}_q$ 上の射影的代数曲線を X とおく (**Hermite 曲線**).
 - (a) X は滑らかな代数曲線であることを示せ. また, その種数を求めよ.
 - (b) $\#X(\mathbb{F}_q)$ を求めよ. また, X は極大曲線であることを示せ.
 - (c) X の $\mathbb{F}_q$ 上の合同ゼータ関数 $Z(T, X)$ を求めよ.

問 14. X を $\mathbb{Q}$ 上の滑らかな射影的代数多様体とする. $f(T) \in \mathbb{Z}[T]$ を整数係数多項式とし, 有限個を除くすべての素数 p に対して $\#X(\mathbb{F}_p) = f(p)$ がなりたつと仮定する. このとき, $X(\mathbb{C})$ の奇数次の Betti 数は 0 であり, $X(\mathbb{C})$ の $2m$ 次の Betti 数は $f(T)$ における T^m の係数に等しいことを示せ.

問 15. X, Y を代数体 K 上の滑らかな射影的代数多様体とする. K の有限素点 v を 1 つ固定し, X, Y は v で良い還元を持つと仮定する. さらに, すべての n に対して $\#X(\mathbb{F}_{q^n}) = \#Y(\mathbb{F}_{q^n})$ が成り立つと仮定する (v における剰余体を $\mathbb{F}_q$ とおいた). このとき, $X(\mathbb{C}), Y(\mathbb{C})$ の Betti 数が等しいことを示せ. また, これは Hodge 数に対してはなりたたないことを示せ (反例を挙げよ).

問 16. X, Y を代数体 K 上の滑らかな射影的代数多様体とする. 有限個を除くすべての有限素点 v に対し, $\#X(\kappa(v)) = \#Y(\kappa(v))$ なら ($\kappa(v)$ は v の剰余体), $X(\mathbb{C}), Y(\mathbb{C})$ の Hodge 数が等しいことを示せ. (Hodge 分解から, $X(\mathbb{C}), Y(\mathbb{C})$ の Betti 数が等しいことも分かる.)

問 17. 体 K 上の $K3$ 曲面 X は, $X \otimes_K \bar{K}$ の Picard 数が 22 であるとき**超特異**であるという (超特異 $K3$ 曲面は標数 0 の体上には存在しない). (q によらない) 自然数 N が存在して, 任意の有限体 $\mathbb{F}_q$ と, 超特異 $K3$ 曲面 $X, Y/\mathbb{F}_q$ に対し, $\#X(\mathbb{F}_{q^N}) = \#Y(\mathbb{F}_{q^N})$ となることを示せ. (ヒント: $K3$ 曲面の Betti 数は, $b_0 = 1, b_1 = 0, b_2 = 22, b_3 = 0, b_4 = 1$ である.)

問 18 (Weil). C を有限体 $\mathbb{F}_q$ 上の滑らかな射影的代数曲線とする. $X = (C \times C) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ とおき, $\Delta \subset X$ を対角集合, $\Gamma \subset X$ を Frobenius 射 $F: C \rightarrow C$ のグラフとする. C の種数を g とおく.

- (1) $\Delta \cdot \Delta = 2 - 2g$, $\Gamma \cdot \Gamma = q(2 - 2g)$ を示せ.
- (2) 交点数 $\Delta \cdot \Gamma$ が C の $\mathbb{F}_q$ -有理点の個数 $\#C(\mathbb{F}_q)$ に等しいことを示せ.
- (3) X は Hodge スタンダード予想をみたすことが知られている. これを用いて, Hasse-Weil の不等式

$$|1 + q - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}$$

を示せ.

問 19 (Jannsen). X を代数的閉体 K 上の n 次元の滑らかな射影的代数多様体とし, K で可逆な素数 ℓ を固定する. $X \times X$ 上の余次元 n の代数的サイクルのなす群を数値的同値で割った群を $C_{\text{neq}}^n(X \times X)$ とおく. また, $E = \mathbb{Q}, \mathbb{Q}_\ell$ に対し, $C^n(X \times X) \otimes_{\mathbb{Z}} E$ を数値的同値で割った群を $C_{\text{neq}}^n(X \times X, E)$ とおき, (ℓ 進エタールコホモロジーから定まる) ホモロジー同値で割った群を $C_{\text{hom}}^n(X \times X, E)$ とおく. (スタンダード予想を仮定すれば $C_{\text{hom}}^n = C_{\text{neq}}^n$ だが, ここでは仮定しない.) 代数的対応の合成で積を入れることにより, $C_{\text{neq}}^n(X \times X, E), C_{\text{hom}}^n(X \times X, E)$ は E 上の代数になる.

- (1) $C_{\text{neq}}^n(X \times X)$ は有限生成自由アーベル群であることを示せ. $C_{\text{neq}}^n(X \times X, \mathbb{Q})$ は $\mathbb{Q}$ 上の有限次元ベクトル空間であることを示せ. また, $C_{\text{neq}}^n(X \times X, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = C_{\text{neq}}^n(X \times X, \mathbb{Q}_\ell)$ を示せ.
- (2) $C_{\text{hom}}^n(X \times X, \mathbb{Q}_\ell)$ は $\mathbb{Q}_\ell$ 上の有限次元ベクトル空間であることを示せ.
- (3) K の標数が 0 のとき, $C_{\text{hom}}^n(X \times X, \mathbb{Q})$ は $\mathbb{Q}$ 上有限次元であり, その次元は ℓ によらないことを示せ. (補足: K が正標数のときは, $C_{\text{hom}}^n(X \times X, \mathbb{Q})$ が $\mathbb{Q}$ 上有限次元であることは知られていない. その次元が ℓ によらないかどうかとも知られていない.)
- (4) $\alpha \in C_{\text{hom}}^n(X \times X, \mathbb{Q}_\ell)$ をベキ零元とする. このとき, α のエタールコホモロジー $H^i(X, \mathbb{Q}_\ell)$ への作用はベキ零であることを示せ.
- (5) $I \subset C_{\text{hom}}^n(X \times X, \mathbb{Q}_\ell)$ をベキ零な両側イデアルとする. I の自然な全射 $C_{\text{hom}}^n(X \times X, \mathbb{Q}_\ell) \rightarrow C_{\text{neq}}^n(X \times X, \mathbb{Q}_\ell)$ による像が 0 であることを示せ. (ヒント: Lefschetz 跡公式を用いよ.)
- (6) $C_{\text{neq}}^n(X \times X, \mathbb{Q}_\ell)$ が $\mathbb{Q}_\ell$ 上の半単純代数であることを示せ. また, $C_{\text{neq}}^n(X \times X, \mathbb{Q})$ が $\mathbb{Q}$ 上の半単純代数であることを示せ. (ヒント: Jacobson 根基 $J \subset C_{\text{hom}}^n(X \times X, \mathbb{Q}_\ell)$ の像が 0 であることを示せ.)

問 20. $PSL_2(\mathbb{F}_5) = SL_2(\mathbb{F}_5)/\{\pm 1\}$ は交代群 A_5 と同形であることを示せ. また, 任意の単射準同形 $i: PSL_2(\mathbb{F}_5) \hookrightarrow PSL_2(\overline{\mathbb{Q}})$ に対し, 以下の図式が可換になる $i': SL_2(\mathbb{F}_5) \rightarrow SL_2(\overline{\mathbb{Q}})$ が一意的に存在することを示せ. また, この i' は単射であることを示せ.

$$\begin{array}{ccc} SL_2(\mathbb{F}_5) & \xrightarrow{i'} & SL_2(\overline{\mathbb{Q}}) \\ \downarrow & & \downarrow \\ PSL_2(\mathbb{F}_5) & \xrightarrow{i} & PSL_2(\overline{\mathbb{Q}}) \end{array}$$

問 21 楕円曲線の等分点から得られる Galois 表現について, 次を示せ.

- (1) $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_5)$ を $\mathbb{Q}$ の mod 5 表現で, $\det \rho$ が mod 5 円分指標であるとする. このとき, $\mathbb{Q}$ 上の楕円曲線 E の同形類であって, $E[5]$ への $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の作用が ρ と同値になるものが無限個存在することを示せ. (ヒント: モジュラー曲線 $X(5)$ の適当な Galois 捻りが $\mathbb{P}_{\mathbb{Q}}^1$ と同形になることを示せ. 1 次分数変換により, $\text{Aut}(\mathbb{P}_{\mathbb{Q}}^1) \cong PSL_2(\overline{\mathbb{Q}})$ であることに注意.)
- (2) (1) は $\mathbb{Q}$ の mod 3 表現 $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_3)$ に対してもなりたつことを示せ.
- (3) (Dieulefait) $p \geq 7$ を素数とする. $\mathbb{Q}$ の mod p 表現 $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_p)$ であって, $\det \rho$ が mod p 円分指標であり, どんな $\mathbb{Q}$ 上の楕円曲線 E に対しても $E[p]$ と ρ が同値にならないものが存在することを示せ.

問 22 (L 関数の有理型解析接続 (1)). Brauer 誘導定理とは、次のような定理である.

定理 G を有限群とし, ρ を G の $\mathbb{C}$ 上の有限次元表現とする. このとき, 可解部分群 $H_1, \dots, H_r \subset G$ (H_i には重複があるかもしれない) および, H_i の 1 次元表現 $\chi_i: H_i \rightarrow \mathbb{C}^\times$ と $m_i \in \mathbb{Z}$ が存在して, 任意の $\sigma \in G$ に対し, 次がなりたつ:

$$\mathrm{Tr}(\rho(\sigma)) = \sum_{i=1}^r m_i \mathrm{Tr}((\mathrm{Ind}_{H_i}^G \chi_i)(\sigma))$$

これを用いて, 任意の Artin 表現 $\rho: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_n(\mathbb{C})$ に対し, L 関数 $L(s, \rho)$ が有理型関数として複素平面全体に解析接続されることを示せ. (ヒント: L 関数は誘導表現によって不変である. すなわち, L/K を代数体の有限次拡大とし, $\rho: \mathrm{Gal}(\overline{L}/L) \rightarrow GL(V)$ を有限次元 Galois 表現 (Artin 表現または ℓ 進表現) とすると, $L(s, \rho) = L(s, \mathrm{Ind}_{\mathrm{Gal}(\overline{L}/L)}^{\mathrm{Gal}(\overline{L}/K)} \rho)$ がなりたつ.)

問 23 (L 関数の有理型解析接続 (2)). 素数 ℓ と体同形 $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ を固定する. また, 実数 $t \in \mathbb{R}$ を固定する. 代数体 K の ℓ 進表現 ρ に対して, 次の条件 (※) を考える.

(※) 任意の 1 次元 Artin 表現 χ に対し, $L(s, \rho \otimes \chi)$ は有理型関数として複素平面全体に解析接続され, $\mathrm{Re}(s) \geq t$ において正則で零点を持たない.

さて, $\mathbb{Q}$ の ℓ 進表現 ρ が次をみたすとする.

Galois 拡大 $F/\mathbb{Q}$ が存在し, 任意の部分拡大 $F \supset F' \supset \mathbb{Q}$ で F/F' が可解拡大であるものに対し, ρ の制限 $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F')}$ は (※) をみたす.

このとき, $L(s, \rho)$ は有理型関数として複素平面全体に解析接続され, $\mathrm{Re}(s) \geq t$ において正則で零点を持たないことを示せ. (ヒント: Brauer 誘導定理を用いよ.)

参考文献

- [A1] André, Y., *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, Panoramas et Synthèses, 17. Société Mathématique de France, Paris, 2004.
- [AC] Arthur, J., Clozel, L., *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies, 120. Princeton University Press, Princeton, NJ, 1989.
- [Ba] Batyrev, V., *Birational Calabi-Yau n -folds have equal Betti numbers*, New trends in algebraic geometry (Warwick, 1996), 1–11, London Math. Soc. Lecture Note Ser., 264, Cambridge Univ. Press, Cambridge, 1999.
- [BBD] Beilinson, A. A., Bernstein, J., Deligne, P., *Faisceaux pervers*, Analysis and topology on singular spaces, I (Luminy, 1981), 5–171, Astérisque, 100, Soc. Math. France, Paris, 1982.
- [Bo] Bombieri, E., *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, no. 430, (1972/1973).
- [BCDT] Breuil, C., Conrad, B., Diamond, F., Taylor, R., *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.
- [Ca] Carayol, H. *Sur les représentations ℓ -adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) 19 (1986), no. 3, 409–468.
- [CHT] Clozel, L., Harris, M., Taylor, R., *Automorphy for some ℓ -adic lifts of automorphic mod ℓ representations*, preprint, 2006. (<http://www.math.harvard.edu/~rtaylor/>)
- [De1] Deligne, P., *Formes modulaires et représentations ℓ -adiques*, Séminaire Bourbaki, no. 355, (1968/69).
- [De2] Deligne, P., *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. No. 43 (1974), 273–307.
- [De3] Deligne, P., *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. No. 52 (1980), 137–252.
- [DeS] Deligne, P., Serre, J.-P., *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup. (4) 7 (1974), 507–530.
- [DiS] Diamond, F., Shurman, J., *A first course in modular forms*, Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.
- [FK] Freitag, E., Kiehl, R., *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 13. Springer-Verlag, Berlin, 1988.
- [FM] Fontaine, J.-M., Mazur, B., *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.
- [Fu] Fulton, W. *Introduction to toric varieties*, Annals of Mathematics Studies, 131. Princeton University Press, Princeton, NJ, 1993.
- [GM] Gillet, H., Messing, W., *Cycle classes and Riemann-Roch for crystalline cohomology*, Duke Math. J. 55 (1987), no. 3, 501–538.

- [Gros] Gros, M., *Classes de Chern et classes de cycles en cohomologie de Hodge-Witt logarithmique*, Mém. Soc. Math. France (N.S.) No. 21 (1985).
- [Groth] Grothendieck, A., *Standard conjectures on algebraic cycles*, Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), pp. 193–199, Oxford Univ. Press, London.
- [HN] Harder, G., Narasimhan, M. S., *On the cohomology groups of moduli spaces of vector bundles on curves*, Math. Ann. 212 (1974/75), 215–248.
- [HSBT] Harris, M., Shepherd-Barron, N., Taylor, R., *A family of Calabi-Yau varieties and potential automorphy*, preprint, 2006. (<http://www.math.harvard.edu/~rtaylor/>)
- [HT] Harris, M., Taylor, R., *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, 151. Princeton University Press, Princeton, NJ, 2001.
- [Har] Hartshorne, R., *Algebraic geometry*, Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. (邦訳: R. ハーツホーン (高橋宣能, 松下大介訳), 『代数幾何学 1–3』, シュプリンガーフェアラーク東京, 2004–2005 年.)
- [Hat] 服部晶夫, 『位相幾何学』, 岩波基礎数学選書, 岩波書店, 1991 年.
- [Hot] 堀田良之, 『可換環と体』, 岩波書店, 2006 年.
- [Il] Illusie, L., *Miscellany on traces in ℓ -adic cohomology: a survey*, Jpn. J. Math. 1 (2006), no. 1, 107–136.
- [It1] Ito, T., *Birational smooth minimal models have equal Hodge numbers in all dimensions*, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), 183–194, Fields Inst. Commun., 38, Amer. Math. Soc., Providence, RI, 2003.
- [It2] Ito, T., *Stringy Hodge numbers and p -adic Hodge theory*, Compos. Math. 140 (2004), no. 6, 1499–1517.
- [Jan] Jannsen, U., *Motives, numerical equivalence, and semi-simplicity*, Invent. Math. 107 (1992), no. 3, 447–452.
- [Kato] 加藤和也, 『Weil 予想とエタールコホモロジー』, 岩波書店 (出版予定) .
- [Katz] Katz, N., *L -functions and monodromy: four lectures on Weil II*, Adv. Math. 160 (2001), no. 1, 81–132.
- [KM] Katz, N., Messing, W., *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. 23 (1974), 73–77.
- [Ked] Kedlaya, K., *Fourier transforms and p -adic ‘Weil II’*, Compos. Math. 142 (2006), no. 6, 1426–1450.
- [KW] Khare, C., Wintenberger, J.-P., *Serre’s modularity conjecture I,II*, preprint, 2007. (<http://www.math.utah.edu/~shekhar/papers.html>)
- [Kis] Kisin, M., *The Fontaine-Mazur conjecture for GL_2* , preprint, 2005. (<http://www.math.uchicago.edu/~kisin/preprints.html>)
- [Kl] Kleiman, S. L., *Algebraic cycles and the Weil conjectures*, Dix exposés sur la cohomologie des schémas, pp. 359–386. North-Holland, Amsterdam; Masson, Paris, 1968.

- [Kl2] Kleiman, S. L., *The standard conjectures*, Motives (Seattle, WA, 1991), 3–20, Proc. Sympos. Pure Math., 55, Part 1, Amer. Math. Soc., Providence, RI, 1994.
- [La] Laumon, G., *Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil*, Inst. Hautes Études Sci. Publ. Math. No. 65 (1987), 131–210.
- [Ma] Manin, Ju. I., *Correspondences, motifs and monoidal transformations*, Mat. Sb. (N.S.) 77 (119) (1968) 475–507.
- [Mil] Milne, J. S., *Étale cohomology*, Princeton Mathematical Series, 33. Princeton University Press, Princeton, N.J., 1980.
- [Miy] Miyake, T., *Modular forms*, Springer-Verlag, Berlin, 1989.
- [Mum] Mumford, D., *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Oxford University Press, London, 1970.
- [Sa] Saito, T., *Modular forms and p -adic Hodge theory*, Invent. Math. 129 (1997), no. 3, 607–620.
- [Sch] Scholl, A. J., *Motives for modular forms*, Invent. Math. 100 (1990), no. 2, 419–430.
- [Se1] Serre, J.-P., *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier, Grenoble 6 (1955–1956), 1–42.
- [Se2] Serre, J.-P., *Exemples de variétés projectives conjuguées non homéomorphes*, C. R. Acad. Sci. Paris 258 (1964), 4194–4196.
- [Se3] Serre, J.-P., *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Séminaire Delange-Pisot-Poitou (1967–68), No. 14.
- [Se4] Serre, J.-P., *Abelian ℓ -adic representations and elliptic curves*, McGill University lecture notes, Benjamin, Inc., New York-Amsterdam 1968. (邦訳 : J.-P. セール (鈴木治郎訳), 『楕円曲線と ℓ 進アーベル表現』, ピアソン・エデュケーション, 1999 年.)
- [Se5] Serre, J.-P., *A course in arithmetic*, Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. (邦訳 : J.-P. セール (弥永健一訳), 『数論講義』, 岩波書店, 1979 年.)
- [Se6] Serre, J.-P., *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou, (1969/70), No. 19.
- [Se7] Serre, J.-P., *Représentations ℓ -adiques*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), pp. 177–193. Japan Soc. Promotion Sci., Tokyo, 1977.
- [Se8] Serre, J.-P., *Extensions icosaédriques*, Seminar on Number Theory, 1979–1980, Exp. No. 19, 7 pp., Univ. Bordeaux I, Talence, 1980.
- [SBT] Shepherd-Barron, N. I., Taylor, R., *mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc. 10 (1997), no. 2, 283–298.
- [Sh] Shimura, G., *Introduction to the arithmetic theory of automorphic functions*, Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

- [Tat] Tate, J., *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 93–110.
- [Tay1] Taylor, R., *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu 1 (2002), no. 1, 125–143.
- [Tay2] Taylor, R., *On the meromorphic continuation of degree two L -functions*, Doc. Math. 2006, Extra Vol., 729–779.
- [Tay3] Taylor, R., *Galois representations*, Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002), 449–474, Higher Ed. Press, Beijing, 2002.
- [Tay4] Taylor, R., *Automorphy for some ℓ -adic lifts of automorphic mod ℓ representations. II*, preprint, 2006 (<http://www.math.harvard.edu/~rtaylor/>).
- [TW] Taylor, R., Wiles, A., *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (1995), no. 3, 553–572.
- [TY] Taylor, R., Yoshida, T., *Compatibility of local and global Langlands correspondences*, J. Amer. Math. Soc. 20 (2007), no. 2, 467–493.
- [We] Weil, A., *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55, (1949), 497–508.
- [Wi] Wiles, A., *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443–551.
- [Yo] Yoshida, H., *On an analogue of the Sato conjecture*, Invent. math. 19 (1973), 261–277.
- [EGA] Grothendieck, A., *Éléments de géométrie algébrique. I–IV*, Inst. Hautes Études Sci. Publ. Math. No. 4 (1960), No. 8 (1961), No. 11 (1961), No. 17 (1963), No. 20 (1964), No. 24 (1965), No. 28 (1966), No. 32 (1967).
- [SGA] *Séminaire de Géométrie Algébrique du Bois Marie (SGA) 1–7 & 4 $\frac{1}{2}$* .
(Grothendieck Circle : <http://www.grothendieckcircle.org/>)
- [Corvallis] *Automorphic forms, representations and L -functions* (Corvallis, Ore., 1977), Proc. Sympos. Pure Math., 33, Part 1 & 2, Amer. Math. Soc., Providence, R.I., 1979.
- [AnnArbor] *Automorphic forms, Shimura varieties, and L -functions*, Vol. I & II (Ann Arbor, MI, 1988), Perspect. Math., 10, Academic Press, Boston, MA, 1990.
- [Seattle] *Motives* (Seattle, WA, 1991), Proc. Sympos. Pure Math., 55, Part 1 & Part 2, Amer. Math. Soc., Providence, RI, 1994.
- [Toronto] *Harmonic analysis, the trace formula, and Shimura varieties*, Clay Math. Proc., 4, Amer. Math. Soc., Providence, RI, 2005.
- [Tanoshimi] 数学のたのしみ, 『佐藤-テイト予想の解決と展望』, 日本評論社, 2008 年 (出版予定)

$\mathcal{L}$ -INVARIANT OF TENSOR POWER OF HILBERT MODULAR FORMS

HARUZO HIDA

CONTENTS

1. Galois deformation and $\mathcal{L}$ -invariant	7
1.1. Greenberg's Selmer Groups	8
1.2. Greenberg's $\mathcal{L}$ -invariant	12
2. Factorization of $\mathcal{L}$ -invariant	13
2.1. Factorization	14
2.2. Multiplicative $\mathcal{L}$ -invariant	14
2.3. Proof of Theorem 0.4	16
3. Proof of Conjecture 0.3 under potential modularity	17
3.1. Potential version implies Conjecture 0.3	17
3.2. Proof of Corollary 0.6	17
4. $\mathcal{L}$ -invariants of CM fields	18
4.1. CM Iwasawa modules	18
4.2. Anticyclotomic Iwasawa modules	19
4.3. The $\mathcal{L}$ -invariant of CM fields	20
References	22

INTRODUCTION ¹

The author's study of $\mathcal{L}$ -invariant of automorphic p -adic L -functions described in [HMI] is sketched in [H07a], and the series of lectures at Hokkaido university was based on [H07a] and is given under the title: " $\mathcal{L}$ -invariant of p -adic L -functions". In this half expository and half research note, we illustrate progress made after the lectures in Sapporo and publication of [H07a]; so, the material of [H07a] is also covered here but briefly. Formulation of our results aside, some results described here are at least not in print before, for example, Corollary 0.6 and Proposition 3.1.

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the field of all algebraic numbers. For each prime ℓ , we pick a field embedding i_ℓ of $\overline{\mathbb{Q}}$ into an algebraic closure $\overline{\mathbb{Q}_\ell}$ of the ℓ -adic field. This gives rise to a choice of the decomposition subgroup $D_\ell = \text{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$ and its inertia subgroup I_ℓ in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We fix a prime $p > 2$ and a p -adic absolute value $|\cdot|_p$ on $\overline{\mathbb{Q}}$. Then $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}$ under $|\cdot|_p$. We write $W = \{x \in K \mid |x|_p < 1\}$ for the p -adic integer ring of a sufficiently large extension $K/\mathbb{Q}_p$ inside $\mathbb{C}_p$. We write $\overline{\mathbb{Q}_p}$ for the field of all numbers in $\mathbb{C}_p$ algebraic over $\mathbb{Q}_p$. Start with a strictly compatible system $\{\rho_l\}$ of semi-simple Galois representations $\rho_l : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_n(T_l)$ for primes l of the coefficient field $T \subset \overline{\mathbb{Q}}$. Thus $V_l = T_l^n$ is a Galois module via ρ_l . We assume that ρ does not contain the trivial representation as a subquotient. We write S for the finite set of common ramification primes of ρ_l ; so, ρ_l is unramified outside $S \cup \{\infty, \ell\}$, where ℓ is the residual characteristic of l .

The author is partially supported by the NSF grant: DMS 0244401, DMS 0456252 and DMS 0753991.

¹This introduction is a follow-up of the lectures delivered at the conference on L -functions at Kyushu university on February in 2006, the lectures at Harvard University, Spring 2006, in the eigenvariety semester and at Hokkaido university, summer 2006, as a series lectures at Sapporo summer school organized by Yoshitaka Maeda. The author would like to thank Yoshitaka Maeda for the invitation to speak at the summer school.

We write $\mathfrak{p} = \{\xi \in O_T \mid |\xi|_p < 1\}$ for the integer ring O_T of T , and take a sufficiently large discrete valuation ring W containing $O_{T,\mathfrak{p}}$ as our coefficient ring; so, we regard $\rho_{\mathfrak{p}}$ to have values in $GL_n(W)$. Often we just write ρ for $\rho_{\mathfrak{p}}$ which acts on $V = K^n$ for the quotient field K of W .

We always assume that ρ is ordinary in the following sense: ρ restricted to $D_p = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is upper triangular with diagonal characters $\mathcal{N}^{a_j}$ on an open subgroup of the inertia group I_p for the p -adic cyclotomic character $\mathcal{N}$ ordered from top to bottom as $a_1 \geq a_2 \geq \cdots \geq 0 \geq \cdots \geq a_n$. Thus

$$\rho|_{I_p} = \begin{pmatrix} \mathcal{N}^{a_1} \psi_1 & * & \cdots & * \\ 0 & \mathcal{N}^{a_2} \psi_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathcal{N}^{a_n} \psi_n \end{pmatrix}$$

for finite order characters ψ_j ($j = 1, 2, \dots, n$), and we have a decreasing filtration $\mathcal{F}^{i+1}\rho \subset \mathcal{F}^i\rho$ stable under D_p such that the Tate twists of the graded piece $gr^i(\rho)(-i) := (\mathcal{F}^i\rho/\mathcal{F}^{i+1}\rho)(-i)$ is unramified after finite base-change.

Let $E_\ell(X) = \det(1 - \rho_{\mathfrak{q}}(\text{Frob}_\ell)|_{V_{I_\ell}} X) \in T[X]$ (assuming $\mathfrak{q} \nmid \ell$), where $V_{I_\ell} = H_0(I_\ell, V_{\mathfrak{q}})$. We assume that $E_\ell(X)$ is independent of the choice of $\mathfrak{q} \nmid \ell$ (strict compatibility). Decompose

$$E_p(X) = \prod_{j=1}^{n'} (1 - \alpha_j X) \quad \text{for } n' = \dim V_{I_p}.$$

By potential unramifiedness of $gr^i(\rho)(-i)$, we have $\text{ord}_p(\alpha_j) \in \mathbb{Z}$ (if we assume to have the étale-crystalline comparison isomorphism producing $E_p(X)$ as the characteristic polynomial of the crystalline Frobenius map on the crystalline part of V ; another strict compatibility). Let us define

$$\beta_j = \begin{cases} \alpha_j & \text{if } \text{ord}_p(\alpha_j) \geq 1, \\ p\alpha_j^{-1} & \text{if } \text{ord}_p(\alpha_j) \leq 0 \end{cases}$$

and put $e = |\{j \mid \beta_j = p\}|$.

$$\mathcal{E}(\rho) = \prod_{j=1}^n (1 - \beta_j p^{-1}) \quad \text{and} \quad \mathcal{E}^+(\rho) = \prod_{j=1, \beta_j \neq p}^n (1 - \beta_j p^{-1}).$$

Then the complex L -function is defined by $L(s, \rho) = \prod_\ell E_\ell(\ell^{-s})^{-1}$. We assume that the value at 1 is critical for $L(s, \rho)$. We suppose to have an algebraicity result that for a well defined period $\Omega(\rho(1)) \in \mathbb{C}^\times$ such that $\frac{L(s, \rho \otimes \varepsilon)}{\Omega(\rho(1))} \in \overline{\mathbb{Q}}$ for all finite order characters $\varepsilon : \mathbb{Z}_p^\times \rightarrow \mu_{p^\infty}(\overline{\mathbb{Q}})$. Then we should have

Conjecture 0.1. *Suppose that $s = 1$ is critical for ρ and that D_p acts on $gr^0(\rho)$ trivially. Then there exist a power series $\Phi^{an}(X) \in W[[X]]$ and a p -adic L -function $L_p^{an}(s, \rho) = \Phi_p^{an}(\gamma^{1-s} - 1)$ interpolating $L(1, \rho \otimes \varepsilon)$ for p -power order character ε such that $\Phi_p^{an}(\varepsilon(\gamma) - 1) \sim \mathcal{E}(\rho \otimes \varepsilon) \frac{L(1, \rho \otimes \varepsilon)}{\Omega(\rho(1))}$ with the modifying p -factor $\mathcal{E}(\rho)$ as above (putting $\mathcal{E}(\rho \otimes \varepsilon) = 1$ if $\varepsilon \neq 1$). The L -function $L_p^{an}(s, \rho)$ has zero of order $e + \text{ord}_{s=1} L(s, \rho)$ for a nonzero constant $\mathcal{L}^{an}(\rho) \in \mathbb{C}_p^\times$ (called the analytic $\mathcal{L}$ -invariant), we have*

$$\lim_{s \rightarrow 1} \frac{L_p^{an}(s, \rho)}{(s-1)^e} = \mathcal{L}^{an}(\rho) \mathcal{E}^+(\rho) \frac{L(1, \rho)}{\Omega(\rho(1))},$$

where “ $\lim_{s \rightarrow 1}$ ” is the p -adic limit.

When $e > 0$, we call that $L_p^{an}(s, \rho)$ has an *exceptional zero* at $s = 1$. The problem of $\mathcal{L}$ -invariant is to compute explicitly the $\mathcal{L}$ -invariant $\mathcal{L}^{an}(\rho)$.

Here are some examples of successful computation of the invariant and cases awaiting further study. Start with a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z}) \rightarrow \overline{\mathbb{Q}}^\times$ with $\chi(-1) = -1$. Then $\Omega(\rho(1)) = 2\pi i$. If we suppose $\chi = \left(\frac{-D}{\cdot}\right)$ for a square free positive integer D , the modifying Euler factor

vanishes at $s = 1$ if the Legendre symbol $\left(\frac{-D}{p}\right) = 1 \Leftrightarrow (p) = \mathfrak{p}\bar{\mathfrak{p}}$ ($\mathfrak{p} \neq \bar{\mathfrak{p}}$) in $\mathbb{Q}[\sqrt{-D}]$ with $\mathfrak{p}$ induced by i_p . By a work of Kubota–Leopoldt and Iwasawa, we have a p -adic analytic L -function $L_p^{an}(s, \chi) = \Phi^{an}(\gamma^{1-s} - 1)$ for a power series $\Phi^{an}(X) \in \Lambda = W[[X]]$ and $\gamma = 1 + p$ such that for $\mathcal{E}(\chi\mathcal{N}^m) = (1 - \chi(p)p^{m-1})$

$$L_p^{an}(m, \chi) = \Phi^{an}(\gamma^{1-m} - 1) = \mathcal{E}(\chi\mathcal{N}^m)L(1 - m, \chi) \sim \mathcal{E}(\chi\mathcal{N}^m)\frac{L(m, \chi)}{(2\pi i)^m}$$

for all positive integer m as long as $|n^m - n|_p < 1$ for all n prime to p . If we have an exceptional zero at 1, it appears that we lose the exact connection of the p -adic L -value and the corresponding complex L -value. However, the conjecture says we can recover the complex L -value via an appropriate derivative of the p -adic L -function as long as we can compute $\mathcal{L}^{an}(\rho)$. We may regard χ as a Galois character $\text{Gal}(\mathbb{Q}[\mu_N]/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \{\pm 1\}$, and we remark that $\chi(Frob_p) = 1$ to have the exceptional zero. For our later use, for the class number h of $\mathbb{Q}[\sqrt{-D}]$, we write ϖ for a generator of $\bar{\mathfrak{p}}^h$; so, $\bar{\mathfrak{p}}^h = (\varpi)$ for $\varpi \in \mathbb{Q}[\sqrt{-D}]$.

Here is another example. Start with an elliptic curve $E/\mathbb{Q}$, which yields a compatible system $\rho_E := \{T_\ell E\}$ given by the ℓ -adic Tate module $T_\ell E$. Suppose that E has split multiplicative reduction at p . In this case, $E_p(X) = (1 - X)$, $\mathcal{E}(\rho_E) = 0$ and $\mathcal{E}^+(\rho) = 1$. Then by the solution of the Shimura–Taniyama conjecture by Wiles et al, this L -function has p -adic analogue constructed by Mazur such that we have $\Phi_E^{an}(X) \in \Lambda$ with $\Phi_E^{an}(\varepsilon(\gamma) - 1) = \mathcal{E}(\rho_E \otimes \varepsilon)\frac{G(\varepsilon^{-1})L(1, E, \varepsilon)}{\Omega_E}$ for all p -power order character $\varepsilon : \mathbb{Z}_p^\times \rightarrow W^\times$; in other words, $L_p^{an}(s, E) = \Phi_E^{an}(\gamma^{1-s} - 1)$. Here Ω_E is the period of the Néron differential of E . Thus if $Frob_p$ has eigenvalue 1 on $T_\ell E$, the exceptional zero appears at $s = 1$ as in the case of Dirichlet character. The $Frob_p$ has eigenvalue 1 if and only if E has multiplicative reduction mod p .

The $\mathcal{L}$ -invariant in the cases where $\rho = \chi = \left(\frac{-D}{\cdot}\right)$ as above and $\rho = \rho_E$ for E with split multiplicative reduction is computed in the 1970s to 90s, and the results are

Theorem 0.2. *Let the notation and the assumption be as above.*

- (1) $\mathcal{L}^{an}(\chi) = \frac{\log_p(q)}{\text{ord}_p(q)} = -\frac{\log_p(q)}{h}$ for $q \in \mathbb{C}_p$ given by $q = \varpi/\bar{\varpi}$ ($\bar{\mathfrak{p}}^h = (\varpi)$) and the class number h of $\mathbb{Q}[\sqrt{-D}]$;
- (2) For E split multiplicative at p , writing $E(\mathbb{C}_p) = \mathbb{C}_p^\times/q^\mathbb{Z}$ for the Tate period $q \in \mathbb{Q}_p^\times$, we have $\mathcal{L}^{an}(\rho_E) = \frac{\log_p(q)}{\text{ord}_p(q)}$.

Here $\log_p$ is the Iwasawa logarithm and $|x|_p = p^{-\text{ord}_p(x)}$.

The first assertion is due to Gross–Koblitz [GsK] and Ferrero–Greenberg [FG], and the second was conjectured by Mazur–Tate–Teitelbaum [MTT] and proven by Greenberg–Stevens [GS] and different proofs given by some others later. In the first formula of the theorem, the sign “−” of $-\frac{\log_p(q)}{h}$ is correct as explained in [G] (10) (and if we evaluate the value at $s = 0$, the minus sign should be removed as was done in [FG]).

To present more examples of occurrences of exceptional zero, let G be a classical group split over $\mathbb{Z}_p$ with simple derived group. Write $\mathfrak{s}(R)$ for the Lie algebra of $G(R)$ for a $\mathbb{Z}_p$ -algebra R . Starting with an ordinary p -adic Galois representation $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow G(W)$, there is a systematic way to create many Galois representations whose eigenvalues of $Frob_p$ contain 1. Indeed, let ρ act on the Lie algebra $\mathfrak{s}(W)$ by adjoint action. As an example, take a symmetric or skew symmetric integral nondegenerate $(n + 1) \times (n + 1)$ matrix J , and let G be an algebraic group given by

$$G(R) = \{x \in GL_{n+1}(R) \mid {}^t x J x = \nu(x) J \text{ for } \nu(x) \in R^\times\}.$$

Then we have $\mathfrak{s}(R) = \{x \in M_{n+1}(R) \mid Jx = -{}^t x J\}$. Then the adjoint action is given by

$$Ad(\rho)(\sigma)(x) = \rho(\sigma)x\rho(\sigma)^{-1}$$

for $x \in \mathfrak{s}(W)$. The action of $Ad(\rho)(Frob_p)$ on $\mathfrak{s}(W)$ has eigenvalue 1 with multiplicity $\lfloor \frac{n+1}{2} \rfloor$. If $\rho(Frob_\infty)$ for a complex conjugation $Frob_\infty$ is conjugate to the n -th symmetric power $\text{Sym} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)^{\otimes n}$ (that is, ρ is totally odd), $Ad(\rho)$ critical at $s = 1$. Let $\rho_1 : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(W)$ be a Galois representation associated to an elliptic Hecke eigenform f with $\text{Tr}(\rho_0(Frob_\ell)) = \lambda_\ell$ if $f|T(\ell) = \lambda_\ell f$. Then $\rho_n = \text{Sym}(\rho_1)^{\otimes n}$ has values in $G(W)$ for G defined for $J = \text{Sym} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right)^{\otimes n}$ and $\rho_n(Frob_\infty) \sim \text{Sym} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)^{\otimes n}$. Thus $Ad(\rho_n)$ is critical at $s = 1$, and $Ad(\rho_n)(Frob_p)$ has eigenvalue 1 with multiplicity $\lfloor \frac{n+1}{2} \rfloor$. As is well known,

$$Ad(\rho_n) \cong \bigoplus_{0 < j \leq n; j: \text{odd}} ad_j(\rho_1),$$

where $ad_j(\rho_1) = \text{Sym}(\rho_1)^{\otimes 2j} \otimes \det(\rho_1)^{-j}$. The Galois representation $ad_j(\rho_1)$ is critical at $s = 1$, and $ad_j(\rho_1)(Frob_p)$ has eigenvalue 1 with multiplicity 1.

To give one more example, let $\rho_F : \text{Gal}(\overline{\mathbb{Q}}/F) \rightarrow GL_2(W)$ be a Galois representation associated to a p -ordinary Hilbert Hecke eigenform (belonging to a discrete series at ∞) over a totally real field F . We make $Ad(\rho_F)$ and consider the induced representation $\text{Ind}_F^{\mathbb{Q}} Ad(\rho_F)$ whose eigenvalues for $Frob_p$ contains 1 with multiplicity g for the number g of prime factors of p in F . The system $\text{Ind}_F^{\mathbb{Q}} Ad(\rho_F)$ is critical at $s = 1$. More generally, for $\rho_{F,n} = \text{Sym}(\rho_F)^{\otimes n}$, $Ad(\rho_{F,n})$ is critical at $s = 1$, and $\text{Ind}_F^{\mathbb{Q}} Ad(\rho_{F,n})(Frob_p)$ has eigenvalue 1 with multiplicity $g \lfloor \frac{n+1}{2} \rfloor$. Similarly as above, $ad_j(\rho_F)$ for odd j is critical at $s = 1$, and $\text{Ind}_F^{\mathbb{Q}} ad_j(\rho_F)(Frob_p)$ has eigenvalue 1 with multiplicity g . We mainly study this example in this note.

Arithmetic $\mathcal{L}$ -invariant. Returning to a general ordinary representation $\rho = \rho_p$, we describe an arithmetic way of constructing p -adic L -function due to Iwasawa and others. We define the Selmer group via Galois cohomology

$$\text{Sel}(\rho) \subset H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty), \rho \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

for the $\mathbb{Z}_p$ -extension $\mathbb{Q}_\infty/\mathbb{Q}$ inside $\mathbb{Q}(\mu_{p^\infty})$ by the subgroup of cohomology classes unramified outside p whose image in $H^1(I_p, (\rho/\mathcal{F}^+\rho) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$ vanishes. Here $\mathcal{F}^+\rho$ is the middle filtration $\mathcal{F}^1\rho$ and I_p is each inertia group at p . The Galois group $\Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ acts on $H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty), \rho \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ and hence on $\text{Sel}(\rho)$, making it as a discrete module over the group algebra $W[[\Gamma]] = \varprojlim_n W[\Gamma/\Gamma^{p^n}]$. Identifying Γ with $1 + p\mathbb{Z}_p$ by the cyclotomic character, we may regard $\gamma \in \Gamma$. Then $W[[\Gamma]] \cong \Lambda$ by $\gamma \mapsto 1 + X$. By the classification theory of compact Λ -modules of finite type, the Pontryagin dual $\text{Sel}^*(\rho)$ has a Λ -linear map into $\prod_{f \in \Omega} \Lambda/f\Lambda$ (for a finite set $\Omega \subset \Lambda$) with finite kernel and finite cokernel. The power series $\Phi_\rho = \prod_{f \in \Omega} f(X)$ is uniquely determined up to unit multiple. We then define $L_p^{\text{arith}}(s, \rho) = \Phi_\rho(\gamma^{1-s} - 1)$. Greenberg gave a recipe of defining $\mathcal{L}(\rho)$ for this $L_p^{\text{arith}}(s, \rho)$ and verified in 1994 (see [G]) the conjecture for this $L_p^{\text{arith}}(s, \rho)$ except for the nonvanishing of $\mathcal{L}(\rho)$ (under some restrictive conditions). For the adjoint square $Ad(\rho_F)$ with ρ_F associated to a Hilbert modular form, the conjecture (except for the nonvanishing of $\mathcal{L}(\rho)$) was again proven in my paper [H07b] under another set of conditions (see also [H00]). If there exists an analytic p -adic L -function $L_p^{\text{an}}(s, \rho) = \Phi_\rho^{\text{an}}(\gamma^{1-s} - 1)$ interpolating complex L -values, the main conjecture of Iwasawa's theory confirms $\Phi_\rho = \Phi_\rho^{\text{an}}$ up to unit multiple; so, $\mathcal{L}(\rho) = \mathcal{L}^{\text{an}}(\rho)$ (up to units) under the main conjecture, and thus, we may take Conjecture 0.1 to be a conjecture also for the arithmetic $\mathcal{L}$ -invariant.

The $\mathcal{L}$ -invariant of Hilbert modular forms. Let F be a totally real field with integer ring O , and we fix an algebraic closure $\overline{F}$. Suppose now that $\rho_F : \text{Gal}(\overline{F}/F) \rightarrow GL_2(W)$ is associated to a cuspidal Hilbert modular Hecke eigenform of weight $k \geq 2$ over a totally real field F (for simplicity, in these notes, we assume that all Hilbert modular forms have parallel integer weight; see, [H07b] for more general cases). We assume p -ordinarity of ρ_F and

(AI) $\rho_{F,n}$ is absolutely irreducible as a representation into $GL_{n+1}(K)$.

This condition holds either if $n = 1$ or if $\text{Im}(\rho_F)$ contains an open subgroup of $SL_2(\mathbb{Z}_p)$ (see [D]). Thus (AI) for $n > 1$ excludes the case of complex multiplication. Here ρ_F is said to have complex multiplication if $\rho_F \otimes \chi \cong \rho_F$ for a nontrivial character χ of $\text{Gal}(\overline{F}/F) \rightarrow \overline{\mathbb{Q}_p}^\times$. We hereafter assume

If $n > 1$, ρ_F does not have complex multiplication.

By a result of Ribet, if $F = \mathbb{Q}$ and ρ_F is without CM, $\text{Im}(\rho_F)$ contains an open subgroup of $SL_2(\mathbb{Z}_p)$. If $F \neq \mathbb{Q}$, Ribet's result should extend to this case, but what is known at this moment is that $\text{Im}(\rho_F)$ contains a conjugate of $SL_2(\mathbb{Z}_p)$ for almost all l for the compatible system $\{\rho_{F,l}\}_l$ (see [D]).

As before, for each prime ideal l of F with residual characteristic ℓ , we fix a field embedding $i_l : \overline{F} \hookrightarrow \overline{\mathbb{Q}_\ell}$ so that the l -adic place of F is induced by the ℓ -adic absolute value $|i_l(x)|_\ell$. We have the corresponding decomposition subgroup $D_l \subset \text{Gal}(\overline{F}/F)$ and its inertia group I_l . Following Greenberg's recipe, we try to compute $\mathcal{L}(\text{Ind}_F^\mathbb{Q} \text{Ad}(\rho_{F,n}))$ for all positive integers n . By ordinarity, we have $\rho_F|_{\text{Gal}(\overline{\mathbb{Q}_p}/F_p)} \cong \begin{pmatrix} \beta_p & * \\ 0 & \alpha_p \end{pmatrix}$ with two distinct diagonal characters α_p and β_p factoring through $I_p \rightarrow \text{Gal}(F_p[\mu_{p^\infty}]/F_p)$ for the inertia group I_p for all $p|p$. By p -ordinarity and $k \geq 2$ combined with the result in [B], the following assertion (DS) holds

(DS) $\alpha_p^i \neq \beta_p^j$ for all pairs of integers $(i, j) \neq (0, 0)$.

As before, let

$$G_n(R) = \{x \in GL_{n+1}(R) \mid {}^t x J_n x = \nu(x) J_n \text{ for } \nu(x) \in R^\times\}$$

for $J_n = \text{Sym} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{\otimes n}$. Then $\rho_{F,n}$ has values in $G_n(W)$. Let S be the set of ramifying primes of the compatible system of $\rho_{F,n}$. Then $\rho_{F,n}$ ramifies at places of S , at all prime factors of p and at all archimedean places of F . Write S_p for the set of all prime factors of p . We consider the universal nearly ordinary deformation $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow G_n(R)$ over K with values in the pro-Artinian local K -algebra R . This means that for any Artinian local K -algebra A with maximal ideal $\mathfrak{m}_A$ and each Galois representation $\rho_A : \text{Gal}(\overline{\mathbb{Q}}/F) \rightarrow GL_2(A)$ such that

(K1) unramified outside S , ∞ and p ;

(K2) for $\mathfrak{p} \in S_p$, $\rho_A|_{D_p} \cong \begin{pmatrix} \alpha_{0,A,p} & * & \cdots & * \\ 0 & \alpha_{1,A,p} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{n,A,p} \end{pmatrix}$ with $\alpha_{j,A,p} \equiv \beta_p^{n-j} \alpha_p^j \pmod{\mathfrak{m}_A}$ and $\alpha_{j,A,p}|_{I_p}$

($j = 0, 1, \dots, n$) factoring through the restriction map $D_p \twoheadrightarrow \text{Gal}(F_p^{ur}[\mu_{p^\infty}]/F_p^{ur})$ for the maximal unramified extension F_p^{ur}/F_p ;

(K3) $\nu \circ \rho_A = \nu \circ \rho_{F,n} = \det(\rho_F)^n$ in A ;

(K4) $\rho_A \equiv \rho_{F,n} \pmod{\mathfrak{m}_A}$,

there exists a unique K -algebra homomorphism $\varphi : R \rightarrow A$ such that $\varphi \circ \rho \approx \rho_A$. Here $\rho \approx \rho'$ if and only if $\rho' = x\rho x^{-1}$ for $x \in G_n(A)$ whose image in $G_n(A/\mathfrak{m}_A)$ is trivial. The representation ρ is said to be *strictly* equivalent to ρ' if $\rho \approx \rho'$. If it is necessary to indicate the relevance to n , we write (R_n, ρ_n) for (R, ρ) .

Write now

$$\rho_n|_{D_p} \cong \begin{pmatrix} \delta_{0,p} & * & \cdots & * \\ 0 & \delta_{1,p} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \delta_{n,p} \end{pmatrix}$$

with $\delta_{j,p} \equiv \beta_p^{n-j} \alpha_p^j \pmod{\mathfrak{m}_n}$ (for $\mathfrak{m}_n = \mathfrak{m}_{R_n}$). Let W be the integer ring of K and Γ_p be the maximal torsion-free quotient of $\text{Gal}(F_p^{ur}[\mu_{p^\infty}]/F_p^{ur})$. Then the character $\delta_{j,p}(\beta_p^{n-j} \alpha_p^j)^{-1}$ restricted to I_p factors through Γ_p , giving rise to an algebra structure of R_n over $W[[\Gamma_p]]$. Take the product $\Gamma = \prod_{p|p} \Gamma_p^{n+1}$ of $n+1$ copies of Γ_p over all prime factors p of p in F . We write general elements of Γ as $x = (x_{j,p})_{j,p}$ with $x_{j,p}$ in the j -th component Γ_p in Γ ($j = 0, 1, \dots, n$). Consider the character $\widehat{\delta} : \Gamma \rightarrow R_n^\times$ given by $\widehat{\delta}(x) = \prod_{j=0}^n \prod_{p|p} \delta_{j,p}(x_{j,p})$. Choosing a generator γ_p of the topologically cyclic group Γ_p , we identify $W[[\Gamma]]$ with a power series ring $W[[X_{j,p}]]_{j,p}$ by associating the generator

$\gamma_{\mathfrak{p}}$ of the j -th component: $\Gamma_{\mathfrak{p}}$ of Γ with $1 + X_{j,\mathfrak{p}}$. The character $\widehat{\delta} : \Gamma \rightarrow R_n^\times$ extends uniquely to an algebra homomorphism $\widehat{\delta} : W[[X_{j,\mathfrak{p}}]]_{j,\mathfrak{p}} \rightarrow R_n$ by the universality of the (continuous) group ring $W[[\Gamma]]$. Thus R_n is naturally an algebra over $K[[X_{j,\mathfrak{p}}]]_{j,\mathfrak{p}}$. Choose a subset $I \subset \{0, 1, \dots, n\}$ which is a complete representative set under the involution $\tau : j \mapsto n - j$ for $0 \leq j \leq n$ removing all fixed points of the involution; so, $I \cong (\{0, 1, \dots, n\} - \{0, 1, \dots, n\}^{(\tau)}) / \langle \tau \rangle$. If n is odd, we may choose I to be the subset of odd integers, and if n is even, $I = \{0, 1, \dots, \frac{n-2}{2}\}$ is a choice. By (K4), $\delta_j \delta_{n-j} = 1$; thus, the variables X_j and X_{n-j} are dependent, and if $n = 2m$ is even, $X_m = 0$; so, there are at most $|I| = \lfloor \frac{n+1}{2} \rfloor$ independent variables for each $\mathfrak{p}$.

Conjecture 0.3. *The universal ring R_n is isomorphic to the power series ring $K[[X_{i,\mathfrak{p}}]]_{\mathfrak{p}|p, i \in I}$ of e variables for $e = g \lfloor \frac{n+1}{2} \rfloor$ ($g = |S_p|$).*

When $n = 0$, taking $\rho_{F,0}$ to be the trivial representation, the conjecture is trivially true. By the results of Wiles, Taylor-Wiles, Fujiwara, Kisin and Skinner-Wiles, the conjecture for $n = 1$ holds at least if either $F = \mathbb{Q}$ (see [Ki], [Ki1] and [Ki2]) or the residual representation $\overline{\rho}_F = (\rho \bmod \mathfrak{m}_W)$ is absolutely irreducible over $\text{Gal}(\overline{F}/F[\mu_p])$ (see [Fu], [Fu1] and [Ch]).

We have two possibilities for each $\mathfrak{p} \in S_p$: $\beta_{\mathfrak{p}}/\alpha_{\mathfrak{p}} = \mathcal{N}$ or not. We call the first case the multiplicative case. If the multiplicative cases occur, the weight k is forced to be 2 (unless we consider multiple weights). If $\mathfrak{p}$ is multiplicative for ρ_F , it is known by Carayol that

$$\rho_F|_{D_{\mathfrak{p}}} \cong \begin{pmatrix} \mathcal{N} & \xi \\ 0 & 1 \end{pmatrix} \otimes \eta$$

for a finite order character η of $D_{\mathfrak{p}}$. Here $\xi : D_{\mathfrak{p}} \rightarrow K(1)$ is a inhomogeneous 1-cocycle given by $\xi(\sigma) = \varprojlim_n (\sqrt[n]{q_{\mathfrak{p}}})^{\sigma-1}$ for an non-unit $q_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times \cap \mathcal{O}_{\mathfrak{p}}$. We call the number $q_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times$ the *Tate period* of ρ_F at $\mathfrak{p}$. We order multiplicative prime factors (for ρ_F) of p as $\mathfrak{p}_1, \dots, \mathfrak{p}_b$ and other non-multiplicative prime factors of p as $\mathfrak{p}_{b+1}, \dots, \mathfrak{p}_g$; so, $\rho_F|_{D_{\mathfrak{p}_j}}$ is potentially Barsotti-Tate if $j > b$ (in the sense that, after finite extension, it is the Galois representation of the Tate module of a Barsotti-Tate group).

Here is a theorem:

Theorem 0.4. *Let $Q_i = N_{F_{\mathfrak{p}_i}/\mathbb{Q}_p}(q_{\mathfrak{p}_i})$ for $i \leq b$ and m be a odd positive integer. If Conjecture 0.3 holds true for two positive integers $n = n_1$ and n_2 with $m - 2 \leq n_1 \leq m - 1$ and $m \leq n_2 \leq m + 1$, then we have*

$$\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F)) = \left(\prod_{i=1}^b \frac{\log_p(Q_i)}{\text{ord}_p(Q_i)} \right) \mathcal{L}(m)$$

for the constant $\mathcal{L}(m) \in K^\times$ defined in Definition 2.1. We have $\mathcal{L}(m) = 1$ if $b = g$, and the value $\mathcal{L}(1)$ when $b < g$ is given by

$$\mathcal{L}(1) = \det \left(\frac{\partial \delta_{\mathfrak{p}_i,1}([p, F_{\mathfrak{p}_i}])}{\partial T_j} \right)_{i>b, j>b} \Big|_{T_1=T_2=\dots=T_g=0} \prod_{i>b} \frac{\log_p(\gamma_{\mathfrak{p}_i})}{[F_{\mathfrak{p}_i} : \mathbb{Q}_p] \alpha_{\mathfrak{p}_i}([p, F_{\mathfrak{p}_i}])}$$

for the local Artin symbol $[p, F_{\mathfrak{p}_i}]$, where $T_j = X_{1,\mathfrak{p}_j}$ and we regard $\gamma_{\mathfrak{p}_i}$ as an element of $\mathbb{Z}_p^\times$ by the cyclotomic character $\mathcal{N}$ to have $\log_p(\gamma_{\mathfrak{p}_i}) \in \mathbb{Q}_p$.

This theorem is proven in [H07b] in a far more general setting. In this note, though the definitions and the results will be stated in full generality, we will give the proof (often) under the following three simplifying assumptions:

- (H1) $k \geq 2$ is a parallel weight;
- (H2) p totally splits in $F/\mathbb{Q}$;
- (H3) ρ_F is unramified outside p and ∞ .

Here are some examples showing usefulness of this theorem: Take a totally imaginary quadratic extension M/F in which all prime factors $\mathfrak{p}|p$ in F splits as $\mathfrak{P}\overline{\mathfrak{P}}$. Write $\mathcal{O}_M$ for the integer ring of M . Take a set $\Sigma_p = \{\mathfrak{P}|p\}$ so that $\Sigma_p \cup \overline{\Sigma}_p$ is the set of all prime factors of p in M . Write h for the class number of M and choose $\varpi(\mathfrak{P}) \in M$ so that $\mathfrak{P}^h = (\varpi(\mathfrak{P}))$ for $\mathfrak{P} \in \overline{\Sigma}_p$. For any Galois

character $\psi : \text{Gal}(\overline{\mathbb{Q}}/M) \rightarrow W^\times$ of M with $\psi(\sigma) \neq \psi^c(\sigma)$ for $\psi^c(\sigma) = \psi(c\sigma c^{-1})$ and a complex conjugation $c \in \text{Gal}(\overline{\mathbb{Q}}/F)$, we have $\text{Ad}(\text{Ind}_M^F \psi) = \chi \oplus \text{Ind}_M^F \psi^{1-c}$ for $\chi = \left(\frac{M/F}{\cdot}\right)$, and we can easily show $\mathcal{L}(\chi) = \mathcal{L}(\text{Ad}(\text{Ind}_M^F \psi))$. The arithmetic p -adic L -function $L_p^{\text{arith}}(s, \chi)$ for $\chi = \left(\frac{M/F}{\cdot}\right)$ constructed à la Iwasawa has an exceptional zero of order $\geq e$ for $e = |\Sigma_p|$. Since we can compute explicitly the universal deformation ρ of $\rho = \text{Ind}_M^F \psi$, we get from the theorem

Corollary 0.5. *We have $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \chi) = (-1)^e \frac{\det(\log_p(N_{\mathfrak{p}'}(\varpi(\mathfrak{P})^{(1-c)})))_{\mathfrak{p}, \mathfrak{p}' \in \Sigma_p}}{\prod_{\mathfrak{p} \in \Sigma_p} h \cdot f(\mathfrak{P})}$, where $N_{\mathfrak{p}}$ is the local norm $N_{M_{\mathfrak{p}}/\mathbb{Q}_p}$ and $f(\mathfrak{P})$ is the residual degree $\dim_{\mathbb{F}_p}(O_M/\mathfrak{P})$.*

A proof of this is given in [HMI] Corollary 5.39, though there are two small errors in the formula of [HMI] Corollary 5.39 and we need to add $(-1)^e$ in front and divide by the value there by $f(\mathfrak{P})$. The above value is the corrected one. We will revisit briefly the proof of this corollary in Section 3 and correct the errors.

If E/F is an elliptic curve with split multiplicative reduction at a prime factor $\mathfrak{p}|p$, we write $E_{/F_p}(\overline{F}_{\mathfrak{p}}) \cong \overline{F}_{\mathfrak{p}}^\times / q_{\mathfrak{p}}^{\mathbb{Z}}$ with the Tate period $q_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times$. Then we have directly from the theorem the following

Corollary 0.6. *Let E/F be an elliptic curve over F without complex multiplication. Assume that the field $F(E[p])$ of rationality of the p -torsion points of E is nonsoluble over F and that p is unramified in $F/\mathbb{Q}$. Then Conjecture 0.3 holds true, and the $\mathcal{L}$ -invariant formula for $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{ad}_1(\rho_E))$ in Theorem 0.4 is valid. In particular, if E is multiplicative at all p -adic places of F , then the $\mathcal{L}$ -invariant $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{ad}_1(\rho_E))$ is given by $\prod_{\mathfrak{p}} \frac{\log_p(N_{\mathfrak{p}}(q_{\mathfrak{p}}))}{\text{ord}_p(N_{\mathfrak{p}}(q_{\mathfrak{p}}))}$, where $N_{\mathfrak{p}}$ is the local norm $N_{F_{\mathfrak{p}}/\mathbb{Q}_p}$.*

It is a celebrated theorem of Serre that $\text{Gal}(F(E[p])/F)$ is full (that is, $\text{Gal}(F(E[p])/F) \cong GL_2(\mathbb{F}_p)$) for almost all primes p ; so, the $\mathcal{L}$ -invariant formula in the corollary is valid for almost all ordinary p . Though this corollary treats the adjoint square $\text{Ad}(\rho_E) = \text{ad}_1(\rho_E)$, the expression of the $\mathcal{L}$ -invariant is exactly the same as the analytic one $\mathcal{L}^{\text{an}}(E)$ for $L_p^{\text{an}}(s, E)$ proven by Greenberg-Stevens when $F = \mathbb{Q}$ (Mok [M] has generalized the method of Greenberg-Stevens for $L_p^{\text{an}}(s, E)$ for E over some totally real fields F). An analytic version (for $F = \mathbb{Q}$) of this corollary is given in [Ci]. This corollary will be proven in Section 3 reducing it to the potentially modularity theorem of E (proven by Taylor) and Fujiwara's $R = T$ theorem [Fu1], and a similar result is stated in [H08a] and [H08b].

1. GALOIS DEFORMATION AND $\mathcal{L}$ -INVARIANT

Assuming the three simplifying assumptions (H1–3), we recall briefly a version (given in [HMI] Definition 3.85) of Greenberg's formula of the $\mathcal{L}$ -invariant for $V := \text{ad}_m(\rho_F)$ for odd m (if m is even, $\text{ad}_m(\rho_F)$ is not critical at $s = 1$). This definition is equivalent to the one in [G] if we apply it to $\text{Ind}_F^{\mathbb{Q}} V$ as proved in [HMI]. Under the vanishing $\text{Sel}_F(\text{ad}_m(\rho_F)) = 0$ (which follows from Conjecture 0.3 for $n = m$), Greenberg found a unique subspace $\mathbf{H} \subset H^1(\mathbb{Q}, \text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F))$ of dimension g . By Shapiro's lemma, we have $H^1(\mathbb{Q}, \text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F)) \cong H^1(F, \text{ad}_m(\rho_F))$, and one can give a definition of the image $\mathbf{H}_F$ of $\mathbf{H}$ in $H^1(F, \text{ad}_m(\rho_F))$ without reference to the induction $\text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F)$ as we recall the precise definition later in 1.2. The space $\mathbf{H}_F$ is represented by cocycles $c : \text{Gal}(\overline{F}/F) \rightarrow \text{ad}_m(\rho_F)$ such that

- (1) c is unramified outside p ;
- (2) $c|_{D_{\mathfrak{p}}}$ at each $\mathfrak{p}|p$ has values in $\mathcal{F}_{\mathfrak{p}}^- \text{ad}_m(\rho_F)$.

Here $\mathcal{F}_{\mathfrak{p}}^- \text{ad}_m(\rho_F) = \mathcal{F}_{\mathfrak{p}}^0 \text{ad}_m(\rho_F)$, $\mathcal{F}_{\mathfrak{p}}^+ \text{ad}_m(\rho_F) = \mathcal{F}_{\mathfrak{p}}^1 \text{ad}_m(\rho_F)$, and $\mathcal{F}^j \text{ad}_m(\rho_F)$ is the decreasing filtration on $\text{ad}_m(\rho_F)$ such that an open subgroup of $I_{\mathfrak{p}}$ acts by $\mathcal{N}^j$ on $\frac{\mathcal{F}_{\mathfrak{p}}^j \text{ad}_m(\rho_F)}{\mathcal{F}_{\mathfrak{p}}^{j+1} \text{ad}_m(\rho_F)}$.

Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$ -extension, and write F_∞/F for the composite of F and $\mathbb{Q}_\infty$. By the condition (2), $(c|_{D_{\mathfrak{p}'}}} \bmod \mathcal{F}_{\mathfrak{p}'}^+ ad_m(\rho_F))$ with a prime $\mathfrak{p}'|p$ may be regarded as a homomorphism $a : D_{\mathfrak{p}'} \rightarrow K$ because $\mathcal{F}_{\mathfrak{p}'}^- ad_m(\rho_F)/\mathcal{F}_{\mathfrak{p}'}^+ ad_m(\rho_F)$ is isomorphic to the trivial $D_{\mathfrak{p}'}$ -module K . Since $F_{\mathfrak{p}} = \mathbb{Q}_p$, a becomes unramified everywhere over the cyclotomic $\mathbb{Z}_p$ -extension F_∞/F . In other words, the cohomology class $[c]$ is in $\text{Sel}_{F_\infty}(ad_m(\rho_F))$ but not in $\text{Sel}_F(ad_m(\rho_F))$, and we have

$$\mathbf{H}_F \cong \text{Sel}_F^{cyc}(ad_m(\rho_F)) := \text{Res}^{-1}(\text{Sel}_{F_\infty}(ad_m(\rho_F)))$$

for the restriction map $\text{Res} : H^1(F, ad_m(\rho_F)) \rightarrow H^1(F_\infty, ad_m(\rho_F))$ (see the definition of various Selmer groups given in the following section).

Take a basis $\{c_{\mathfrak{p}}\}_{\mathfrak{p}|p}$ of $\mathbf{H}_F$ over K . Write $a_{\mathfrak{p}} : D_{\mathfrak{p}'} \rightarrow K$ for $c_{\mathfrak{p}} \bmod \mathcal{F}_{\mathfrak{p}'}^+ ad_m(\rho_F)$ regarded as a homomorphism (identifying $\mathcal{F}_{\mathfrak{p}'}^- ad_m(\rho_F)/\mathcal{F}_{\mathfrak{p}'}^+ ad_m(\rho_F)$ with the trivial $D_{\mathfrak{p}'}$ -module K). We now have two $g \times g$ matrices ($g = |S_p|$) with coefficients in K :

$$A_m = (a_{\mathfrak{p}_i}([p, F_{\mathfrak{p}_j}]))_{i,j} \quad \text{and} \quad B_m = (\log_p(\gamma_{\mathfrak{p}_i})^{-1} a_{\mathfrak{p}_i}([\gamma_{\mathfrak{p}_j}, F_{\mathfrak{p}_j}]))_{i,j}.$$

As we will see in (1.7) (because we have $B = \prod_{0 < m \leq n, M: \text{odd}} B_m$ by Lemma 1.1 for B in (1.7)), Conjecture 0.3 for $\rho_{F,n}$ with $n = m$ or $n = m + 1$ implies that B_m is invertible. Then Greenberg's $\mathcal{L}$ -invariant is defined by

$$(1.1) \quad \mathcal{L}(\text{Ind}_F^{\mathbb{Q}} ad_m(\rho_F)) = \det(A_m B_m^{-1}).$$

The determinant $\det(A_m B_m^{-1})$ is independent of the choice of the basis $\{c_{\mathfrak{p}}\}_{\mathfrak{p}}$.

1.1. Greenberg's Selmer Groups. We recall the definition of Selmer groups. Let S be a finite set of primes of F . Write $F^{(S)}/F$ for the maximal extension unramified outside S , p and ∞ . Put $\mathfrak{G} = \text{Gal}(F^{(S)}/F)$ and $\mathfrak{G}_M = \text{Gal}(F^{(S)}/M)$. Let V be a potentially ordinary representation of $\mathfrak{G}$ on a K -vector space V . Thus V has decreasing filtration $\mathcal{F}_{\mathfrak{p}}^i V$ stable under $\text{Gal}(\overline{F}_{\mathfrak{p}}/F_{\mathfrak{p}})$ such that an open subgroup of $I_{\mathfrak{p}}$ (for each prime factor $\mathfrak{p}|p$) acts on $\mathcal{F}_{\mathfrak{p}}^i V/\mathcal{F}_{\mathfrak{p}}^{i+1} V$ by the i -th power $\mathcal{N}^i$ of the p -adic cyclotomic character $\mathcal{N}$. We fix a W -lattice T in V stable under $\mathfrak{G}$.

Write $D = D_{\mathfrak{p}} \subset \mathfrak{G}$ for the decomposition group of each prime factor $\mathfrak{p}|p$. Put $\mathcal{F}_{\mathfrak{p}}^+ V = \mathcal{F}_{\mathfrak{p}}^1 V$ and $\mathcal{F}_{\mathfrak{p}}^- V = \mathcal{F}_{\mathfrak{p}}^0 V$. Writing $\mathcal{F}_{\mathfrak{p}}^\bullet T = T \cap \mathcal{F}_{\mathfrak{p}}^\bullet V$ and $\mathcal{F}_{\mathfrak{p}}^\bullet V/T = \mathcal{F}_{\mathfrak{p}}^\bullet V/\mathcal{F}_{\mathfrak{p}}^\bullet T$, we have a 3-step filtration stable under $D_{\mathfrak{p}}$ for $A = V, T$ or V/T :

$$(\text{ord}) \quad A \supset \mathcal{F}_{\mathfrak{p}}^- A \supset \mathcal{F}_{\mathfrak{p}}^+ A \supset \{0\}.$$

Its dual $V^*(1) = \text{Hom}_K(V, K(1))$ again satisfies (ord).

Let M/F be a subfield of $F^{(S)}$, and put $\mathfrak{G}_M = \text{Gal}(F^{(S)}/M)$. We write $\mathfrak{p}$ for a prime of M over p and $\mathfrak{q}$ for general primes outside p of M . We write $I_{\mathfrak{p}}$ and $I_{\mathfrak{q}}$ for the inertia subgroup in $\mathfrak{G}_M$ at $\mathfrak{p}$ and $\mathfrak{q}$, respectively. We put

$$L_{\mathfrak{p}}(A) = \text{Ker}(\text{Res} : H^1(M_{\mathfrak{p}}, A) \rightarrow H^1(I_{\mathfrak{p}}, \frac{A}{\mathcal{F}_{\mathfrak{p}}^+(A)})),$$

and

$$L_{\mathfrak{q}}(A) = \text{Ker}(\text{Res} : H^1(M_{\mathfrak{q}}, A) \rightarrow H^1(I_{\mathfrak{q}}, A)).$$

Then we define the Selmer submodule in $H^1(M, A)$ (for $A = V, V/T$) by

$$(1.2) \quad \text{Sel}_M(A) = \text{Ker} \left(H^1(\mathfrak{G}_M, A) \rightarrow \prod_{\mathfrak{q}} \frac{H^1(M_{\mathfrak{q}}, A)}{L_{\mathfrak{q}}(A)} \times \prod_{\mathfrak{p}} \frac{H^1(M_{\mathfrak{p}}, A)}{L_{\mathfrak{p}}(A)} \right).$$

The classical Selmer group of V is given by $\text{Sel}_M(V/T)$, equipped with the discrete topology. We define the “minus”, the “locally cyclotomic” and the “strict” Selmer groups $\text{Sel}_M^-(A)$, $\text{Sel}_M^{cyc}(A)$ and

$\text{Sel}_M^{st}(A)$, respectively, replacing $L_{\mathfrak{p}}(A)$ by

$$\begin{aligned} L_{\mathfrak{p}}^-(A) &= \text{Ker}(\text{Res} : H^1(M_{\mathfrak{p}}, V) \rightarrow H^1(I_{\mathfrak{p}}, V/\mathcal{F}_{\mathfrak{p}}^-(A))) \supset L_{\mathfrak{p}}(A) \\ L_{\mathfrak{p}}^{cyc}(A) &= \text{Ker}(\text{Res} : L_{\mathfrak{p}}^-(A) \rightarrow H^1(I_{\mathfrak{p}, \infty}, V/\mathcal{F}_{\mathfrak{p}}^+(A))) \subset L_{\mathfrak{p}}^-(A) \\ L_{\mathfrak{p}}^{st}(A) &= \text{Ker}(\text{Res} : L_{\mathfrak{p}}^-(A) \rightarrow H^1(M_{\mathfrak{p}}, V/\mathcal{F}_{\mathfrak{p}}^+(A))) \subset L_{\mathfrak{p}}(A), \end{aligned}$$

where $I_{\mathfrak{p}, \infty}$ is the inertia group of $\text{Gal}(\overline{M}_{\mathfrak{p}}/M_{\mathfrak{p}}[\mu_{p^\infty}])$. Then we have

$$\text{Sel}_F^{cyc}(A) = \text{Res}_{F_\infty/F}^{-1}(\text{Sel}_{F_\infty}(A)).$$

Under the simplifying assumption (H2), $\text{Sel}_F^{cyc}(A) = \text{Sel}_F^-(A)$. It is easy to verify that the above Selmer groups do not depend on the choice of S as long as S contains all the ramification primes of V . We assume that $\rho_{F, n}$ is unramified outside p and ∞ ; so, $S = \{p\}$.

Lemma 1.1. *We have*

$$\text{Sel}_F^{cyc}(Ad(\rho_{n,0})) \cong \bigoplus_{0 < m \leq n, m: \text{odd}} \text{Sel}_F^{cyc}(ad_m(\rho_F)) \cong \text{Hom}_K(\mathfrak{m}_n/\mathfrak{m}_n^2, K),$$

where $\mathfrak{m}_n$ is the maximal ideal of R_n . If n is odd and Conjecture 0.3 holds either for n or for $n+1$, we have $\text{Sel}_F(ad_m(\rho_F)) = 0$ for all odd m with $0 < m \leq n$ and $\dim_K \text{Sel}_F^{cyc}(ad_m(\rho_F)) = g$ for all odd $0 < m \leq n$.

Proof. We repeat the proof in [H07b] assuming the conditions (H1–3). Let $V = Ad(\rho_{F, n})$. Then we have the filtration:

$$V \supset \mathcal{F}_{\mathfrak{p}}^- V \supset \mathcal{F}_{\mathfrak{p}}^+ V \supset \{0\},$$

where taking a basis so that the semi-simplification of $\rho_{F, n}|_{D_{\mathfrak{p}}}$ is diagonal with the diagonal characters $\beta_{\mathfrak{p}}^n, \beta_{\mathfrak{p}}^{n-1}\alpha_{\mathfrak{p}}, \dots, \alpha_{\mathfrak{p}}^n$ in this order from top to bottom, $\mathcal{F}_{\mathfrak{p}}^- V$ is made up of upper triangular matrices and $\mathcal{F}_{\mathfrak{p}}^+ V$ is made up of upper nilpotent matrices, and on $\mathcal{F}_{\mathfrak{p}}^- V/\mathcal{F}_{\mathfrak{p}}^+ V$, $D_{\mathfrak{p}}$ acts trivially (getting eigenvalue 1 for $Frob_{\mathfrak{p}}$). We consider the space $Der_K(R_n, K)$ of continuous K -derivations. Let $K[\varepsilon] = K[t]/(t^2)$ for the dual number $\varepsilon = (t \bmod t^2)$. Then writing each K -algebra homomorphism $\phi : R_n \rightarrow K[\varepsilon]$ as $\phi(r) = \phi_0(r) + \partial_{\phi}(r)\varepsilon$ and sending ϕ to $\partial_{\phi} \in Der_K(R_n, K)$, we have $\text{Hom}_{K\text{-alg}}(R_n, K[\varepsilon]) \cong Der_K(R_n, K) = \text{Hom}_K(\mathfrak{m}_n/\mathfrak{m}_n^2, K)$. By the universality of (R_n, ρ_n) , we have

$$\text{Hom}_{K\text{-alg}}(R_n, K[\varepsilon]) \cong \frac{\{\rho : \text{Gal}(\overline{F}/F) \rightarrow G_n(K[\varepsilon]) | \rho \text{ satisfies (K1–4)}\}}{\approx}$$

by $\text{Hom}_{K\text{-alg}}(R_n, K[\varepsilon]) \ni \phi \mapsto \rho_{\phi} = \phi \circ \rho_n = \rho_{F, n} + \varepsilon \partial_{\phi} \rho_n$. Pick $\rho = \rho_{\phi}$ as above. Write $\rho(\sigma) = \rho_{F, n}(\sigma) + \rho_1(\sigma)\varepsilon$ with $\rho_1(\sigma) = \frac{\partial \rho}{\partial t} = \partial_{\phi} \rho_n(\sigma)$. Then $c_{\rho} = (\partial_{\phi} \rho_n) \rho_{F, n}^{-1}$ can be easily checked to be an inhomogeneous 1-cocycle having values in $M_{n+1}(K) \supset V$. Here $\sigma \in \text{Gal}(\overline{F}/F)$ acts on $x \in M_{n+1}(K)$ by $x \mapsto \rho_{F, n}(\sigma) x \rho_{F, n}(\sigma)^{-1}$.

Since $\nu \circ \rho = \nu \circ \rho_{F, n}$ by (K3), we have $\det(\rho) = \det(\rho_{F, n})$, which implies $\text{Tr}(c_{\rho}) = 0$; so, c_{ρ} has values in $\mathfrak{sl}_{n+1}(K)$. For $X \in GL_{n+1}(R_n)$ with ${}^t X J_n X = J_n$, write $\overline{X} = (X \bmod \mathfrak{m}_n) \in GL_{n+1}(K)$. Since ${}^t \rho_n J_n \rho_n = \det(\rho_0)^n J_n = {}^t \rho_{F, n} J_n \rho_{F, n}$, we have ${}^t \rho_{F, n}^{-1} {}^t \rho_n J_n \rho_n \rho_{F, n}^{-1} = J_n$. Let $X = \rho_n \rho_{F, n}^{-1}$. Differentiating the identity: ${}^t X J_n X = J_n$ by $\partial \in Der_K(R_n, K)$, we have

$$({}^t \partial X J_n) \overline{X} + {}^t \overline{X} (J_n \partial X) = 0 \Leftrightarrow {}^t (\partial X \cdot \overline{X}^{-1}) J_n + J_n (\partial X \cdot \overline{X}^{-1}) = 0,$$

which is equivalent to $c_{\rho}(\sigma) \in \mathfrak{s}_n(K) = V$. By the reducibility conditions in (K2), $[c_{\rho}]$ vanishes in $\frac{H^1(M_{\mathfrak{p}}, V)}{L_{\mathfrak{p}}^-(V)}$. Since $F_{\mathfrak{p}} = \mathbb{Q}_p$, $(c_{\rho} \bmod \mathcal{F}_{\mathfrak{p}}^+ V)$ is unramified at $\mathfrak{p}$ over F_{∞} . Thus the cohomology class $[c_{\rho}]$ of c_{ρ} is in $\text{Sel}_F^{cyc}(V)$. We see easily that $\rho \approx \rho' \Leftrightarrow [c_{\rho}] = [c_{\rho'}]$.

We argue in a reverse way starting with a cocycle c giving an element of $\text{Sel}_F^{cyc}(V)$ to construct a deformation $\rho_c = \rho_{F, n} + \varepsilon(c\rho_{F, n})$ with values in $G_n(K[\varepsilon])$; thus,

$$\frac{\{\rho : \text{Gal}(\overline{F}/F) \rightarrow G_n(K[\varepsilon]) | \rho \text{ satisfies the conditions (K1–4)}\}}{\approx} \cong \text{Sel}_F^{cyc}(V).$$

Recall that the isomorphism $\text{Der}_K(R_n, K) \cong \text{Sel}_F^{\text{cyc}}(V)$ is given by

$$\text{Der}_K(R_n, K) \ni \partial \mapsto [c_\partial] \in \text{Sel}_F^{\text{cyc}}(V)$$

for the cocycle $c_\partial = c_\rho = (\partial \rho_n) \rho_{F,n}^{-1}$, where $\rho = \rho_{F,n} + \varepsilon(\partial \rho_n)$.

Since the algebra structure of R_n over $W[[X_{j,p}]]_{\mathfrak{p}|p}$ is given by $\delta_{j,p}(\beta_{\mathfrak{p}}^{n-j} \alpha_{\mathfrak{p}}^j)^{-1}$ and $\delta_{n-j,p} \delta_{j,p} = \det(\rho_F)^n$, the K -derivation $\partial = \partial_\phi : R_n \rightarrow K$ corresponding to a $K[\varepsilon]$ -deformation ρ is a $W[[X_{j,p}]]$ -derivation for $j \in I$ if and only if $\partial \rho_n|_{I_{\mathfrak{p}}}$ is upper nilpotent, which is equivalent to $[c_\partial] \in \text{Sel}_F(V)$. Since $V \cong \bigoplus_{0 < m \leq n, m: \text{odd}} \text{ad}_m(\rho_F)$ as global Galois modules, we have

$$\text{Sel}_F(V) \cong \bigoplus_{0 < m \leq n, m: \text{odd}} \text{Sel}_F(\text{ad}_m(\rho_F)).$$

Assume n to be odd. Let n' be either n or $n+1$. Suppose Conjecture 0.3 for n' . Thus we have $\text{Sel}_F(\text{Ad}(\rho_{F,n'})) \cong \text{Der}_{W[[X_{i,p}]]_{i \in I, \mathfrak{p}|p}}(R_{n'}, K) = 0$ by Conjecture 0.3 for n' . By $\text{Sel}_F(\text{Ad}(\rho_{F,n'})) \cong \bigoplus_{0 < m \leq n', m: \text{odd}} \text{Sel}_F(\text{ad}_m(\rho_F))$, we conclude $\text{Sel}_F(\text{ad}_m(\rho_F)) = 0$ for all odd positive $m \leq n$. Then as seen in [G] (see below (1.4) and Lemma 1.4), the vanishing $\text{Sel}_F(\text{ad}_m(\rho_F)) = 0$ implies

$$\dim_K \text{Sel}_F^{\text{cyc}}(\text{ad}_m(\rho_F)) = \dim_K \mathbf{H}_F = g.$$

□

Question 1.2. *It is curious that we have a canonical isomorphism $\mathfrak{m}_n/\mathfrak{m}_n^2 \cong \mathfrak{m}_{n+1}/\mathfrak{m}_{n+1}^2$ by Lemma 1.1 for any given odd n . A natural question is if this isomorphism extends to a canonical isomorphism $R_n \cong R_{n+1}$.*

Write V for either the representation space of $\text{ad}_m(\rho_F)$ or that of $\text{Ad}(\rho_{F,n})$. For each prime $\mathfrak{q} \in S \cup \{\mathfrak{p}|p\}$, we put

$$(1.3) \quad \overline{L}_{\mathfrak{q}}(V) = \begin{cases} \text{Ker}(H^1(F_j, V) \rightarrow H^1(F_j, \frac{V}{\mathcal{F}_{\mathfrak{p}_j}^+(V)})) \subset L_{\mathfrak{p}_j}(V) & \text{if } \mathfrak{q} = \mathfrak{p}_j \text{ with } j \leq b, \\ L_{\mathfrak{q}}(V) & \text{otherwise} \end{cases}$$

Once $\overline{L}_{\mathfrak{q}}(V)$ is defined, put $\overline{L}_{\mathfrak{q}}(V^*(1)) = \overline{L}_{\mathfrak{q}}(V)^\perp$ under the local Tate duality between $H^1(F_{\mathfrak{q}}, V)$ and $H^1(F_{\mathfrak{q}}, V^*(1))$, where $V^*(1) = \text{Hom}_K(V, \mathbb{Q}_{\mathfrak{p}}(1))$ as Galois modules. Then define the balanced Selmer group $\overline{\text{Sel}}_F(V)$ (resp. $\overline{\text{Sel}}_F(V^*(1))$) by the same formula as in (1.2) replacing $L_{\mathfrak{p}}(V)$ (resp. $L_{\mathfrak{p}}(V^*(1))$) by $\overline{L}_{\mathfrak{p}}(V)$ (resp. $\overline{L}_{\mathfrak{p}}(V^*(1))$). By definition, $\overline{\text{Sel}}_F(V) \subset \text{Sel}_F(V)$. Often we have $\overline{L}_{\mathfrak{p}}(V) = L_{\mathfrak{p}}(V)$ and hence $\text{Sel}_F(V) = \overline{\text{Sel}}_F(V)$. The fact $\overline{L}_{\mathfrak{p}_j}(V) = L_{\mathfrak{p}_j}(V)$ for $V = \text{ad}_m(\rho_F)$ and $\text{Ad}(\rho_{F,n})$ follows from the following F -version of the argument in [G] page 160:

Lemma 1.3. *Let $V = \text{Ad}(\rho_{F,n})$ or $\text{ad}_m(\rho_F)$. Then we have $\overline{L}_{\mathfrak{p}}(V) = L_{\mathfrak{p}}(V)$.*

For K -vector space V with Galois action as above, we have $\overline{\text{Sel}}_F(V) = \text{Sel}_F(V)$.

Proof. Since we have $\overline{L}_{\mathfrak{p}}(V) = L_{\mathfrak{p}}(V)$ by definition if $\mathfrak{p} = \mathfrak{p}_j$ with $j > b$; so, we may assume that $j \leq b$. Write $H^\bullet(M)$ for $H^\bullet(F_{\mathfrak{p}}, M)$ for $D_{\mathfrak{p}}$ -modules M . We need to show the image $\overline{L}_{\mathfrak{p}}(V)$ of $H^1(\mathcal{F}_{\mathfrak{p}}^+ V)$ in $H^1(V)$ is equal to $L_{\mathfrak{p}}(V) := \text{Ker}(r : H^1(V) \rightarrow H^1(I_{\mathfrak{p}}, \overline{V}))$ for $\overline{V} = V/\mathcal{F}^+ V$. We can factor the map r as $r = \text{Res} \circ \gamma$ for $\gamma : H^1(V) \rightarrow H^1(\overline{V})$ and $\text{Res} : H^1(\overline{V}) \rightarrow H^1(I_{\mathfrak{p}}, \overline{V})$. Since $\text{Ker}(\gamma) = \overline{L}_{\mathfrak{p}}(V)$, we need to show that $\text{Im}(\gamma) \cap \text{Ker}(\text{Res}) = 0$.

Writing $Y = \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^2 V$ and $\overline{Y} = \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V$, we have exact sequences of $D_{\mathfrak{p}}$ -modules: $Y \hookrightarrow V/\mathcal{F}_{\mathfrak{p}}^2 V \twoheadrightarrow V/\mathcal{F}_{\mathfrak{p}}^- V$ and $\overline{Y} \hookrightarrow \overline{V} \twoheadrightarrow V/\mathcal{F}_{\mathfrak{p}}^- V$. Since $H^0(V/\mathcal{F}_{\mathfrak{p}}^- V) = 0$, by the long exact sequences of the above two short exact sequences, we find that the natural maps $H^1(Y) \rightarrow H^1(V/\mathcal{F}_{\mathfrak{p}}^2 V)$ and $H^1(\overline{Y}) \rightarrow H^1(\overline{V})$ are injective. Identify $H^1(\overline{Y})$ with its image in $H^1(\overline{V})$. We have

$$\text{Im}(\gamma) \cap H^1(\overline{Y}) = \text{Im}(\overline{\gamma} : H^1(Y) \rightarrow H^1(\overline{Y})) \subset H^1(\overline{V}).$$

In the proof of the same lemma given in my paper [H07b] as Lemma 1.4, there is a typographical error in the statement of the above identity and the left-hand-side: “ $\text{Im}(\gamma) \cap H^1(\overline{Y})$ ” is wrongly written as “ $\text{Im}(\gamma)$ ” in the proof (at page 15) of [H07b] Lemma 1.4.

By the inflation-restriction sequence (and by (H2)),

$$\text{Ker}(\text{Res}) = H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, \overline{V}^{I_{\mathfrak{p}}}) = \overline{V}^{I_{\mathfrak{p}}} / (Frob_{\mathfrak{p}} - 1)\overline{V}^{I_{\mathfrak{p}}} \subseteq \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V.$$

Similarly

$$\begin{aligned} \text{Ker}(\text{Res}_Y : H^1(\overline{Y}) \rightarrow H^1(I_{\mathfrak{p}}, \overline{Y})) &= H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, \overline{Y}^{I_{\mathfrak{p}}}) \\ &= \overline{Y}^{I_{\mathfrak{p}}} / (Frob_{\mathfrak{p}} - 1)\overline{Y}^{I_{\mathfrak{p}}} \subseteq \mathcal{F}_{\mathfrak{p}}^- Y / \mathcal{F}_{\mathfrak{p}}^+ Y = \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V. \end{aligned}$$

Thus inside $H^1(\overline{V})$, $\text{Ker}(\text{Res}) = \text{Ker}(\text{Res}_Y) \subset H^1(\overline{Y})$. We may replace V by Y in our argument, and we shall show that

$$\text{Im}(\overline{\gamma} : H^1(Y) \rightarrow H^1(\overline{Y})) \cap \text{Ker}(\text{Res} : H^1(\overline{Y}) \rightarrow H^1(I_{\mathfrak{p}}, \overline{Y})) = 0.$$

Write $t(\mathfrak{p})$ for $\dim \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V$ (thus, $t(\mathfrak{p}) = 1$ or $\lfloor \frac{n+1}{2} \rfloor$ according as $V = ad_m(\rho_F)$ or $Ad(\rho_{F,n})$). We have the long exact sequence attached to the short one $\mathcal{F}_{\mathfrak{p}}^+ Y \hookrightarrow Y \twoheadrightarrow \overline{Y}$:

$$0 \rightarrow \overline{Y} = H^0(\overline{Y}) \rightarrow H^1(\mathcal{F}_{\mathfrak{p}}^+ Y) \rightarrow H^1(Y) \xrightarrow{\overline{\gamma}} H^1(\overline{Y}) \rightarrow H^2(\mathcal{F}_{\mathfrak{p}}^+ Y) \rightarrow H^2(Y) = 0.$$

By the non-splitting of the short sequence, $H^0(\overline{Y})$ injects into $H^1(\mathcal{F}_{\mathfrak{p}}^+ Y)$. By the local Tate duality,

$$\dim_K H^2(Y) = \dim_K H^0(\text{Hom}_K(Y, K(1))) = 0 \text{ and } \dim_K H^2(\mathcal{F}_{\mathfrak{p}}^+ Y) = t(\mathfrak{p}).$$

This shows that $\dim_K H^1(Y) = 2t(\mathfrak{p})d$ and $\dim_K \text{Im}(\overline{\gamma}) = t(\mathfrak{p})d$ for $d = [F_{\mathfrak{p}}, \mathbb{Q}_p]$ ($d = 1$ by (H2)), because by Kummer’s theory, assuming $d = 1$ for simplicity,

$$H^1(K(1)) = K \otimes_{\mathbb{Z}_p} \varprojlim_n F_{\mathfrak{p}}^{\times} / (F_{\mathfrak{p}}^{\times})^{p^n} \cong K^2$$

and $H^1(K) \cong \text{Hom}((F_{\mathfrak{p}})^{\times}, K) \cong K^2$. By the inflation-restriction sequence, we have

$$L_{\mathfrak{p}}(\overline{Y}) := \text{Ker}(H^1(\overline{Y}) \rightarrow H^1(I_{\mathfrak{p}}, \overline{Y})) \cong H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, \overline{Y}^{I_{\mathfrak{p}}}) \cong \overline{Y}.$$

Thus $\dim L_{\mathfrak{p}}(\overline{Y}) + \dim \text{Im}(\overline{\gamma}) = \dim H^1(I_{\mathfrak{p}}, \overline{Y})$. Thus we need to show $L_{\mathfrak{p}}(\overline{Y}) + \text{Im}(\overline{\gamma}) = H^1(I_{\mathfrak{p}}, \overline{Y})$. By the local Tate duality, noting $Y^*(1) \cong Y$, this statement is equivalent to

$$\text{Ker}(\delta : H^1(\mathcal{F}_{\mathfrak{p}}^+ Y) \rightarrow H^1(Y)) \cap L_{\mathfrak{p}}(\overline{Y})^{\perp} = 0.$$

Here $L_{\mathfrak{p}}(\overline{Y})^{\perp} = H_{f_l}^1(\mathcal{F}_{\mathfrak{p}}^+ Y) = \overline{Y} \otimes_{\mathbb{Z}_p} \varprojlim_n O_{\mathfrak{p}}^{\times} / (O_{\mathfrak{p}}^{\times})^{p^n} \subset H^1(\overline{Y}(1))$, because $\overline{Y}^*(1) = \overline{Y}(1) = K(1)^{t(\mathfrak{p})}$. Since $\text{Ker}(\delta)$ gives rise to the subspace spanned by extension class of $K(1)^{t(\mathfrak{p})} = \mathcal{F}_{\mathfrak{p}}^+ Y \hookrightarrow Y \twoheadrightarrow \overline{Y} \cong K^{t(\mathfrak{p})}$, as already noted, it is given by the cocycles in $\xi_q \otimes \overline{Y}$ for the Tate period q of $\rho_F|_{D_{\mathfrak{p}}}$ at $\mathfrak{p} = \mathfrak{p}_j$. Let us recall ξ_q : $\xi_q(\sigma) = \varprojlim_n (\sqrt[n]{q})^{\sigma-1}$ which has values in $\mathbb{Z}_p(1) \subset K(1)$ and is a inhomogeneous 1-cocycle (see [H08a] Section 4). In particular, $(\overline{Y} \otimes \xi_q) \cap H_{f_l}^1(\mathcal{F}_{\mathfrak{p}}^+ Y)$ is given by

$$(q \otimes \overline{Y}) \cap (\overline{Y} \otimes_{\mathbb{Z}_p} \varprojlim_n O_{\mathfrak{p}}^{\times} / (O_{\mathfrak{p}}^{\times})^{p^n})$$

inside $\overline{Y} \otimes_{\mathbb{Z}_p} \varprojlim_n F_{\mathfrak{p}}^{\times} / (F_{\mathfrak{p}}^{\times})^{p^n}$, which is trivial (because q is a nonunit). $\square$

Lemma 1.4. *Let V be $Ad(\rho_{F,n})$ or $ad_m(\rho_F)$. If V is critical at $s = 1$,*

$$(V) \quad \text{Sel}_F(V) = 0 \Rightarrow H^1(\mathfrak{G}, V) \cong \prod_{\mathfrak{q} \in S} \frac{H^1(F_{\mathfrak{q}}, V)}{L_{\mathfrak{q}}(V)} \times \prod_{\mathfrak{p} | p} \frac{H^1(F_{\mathfrak{p}}, V)}{L_{\mathfrak{p}}(V)}.$$

Proof. Since $\overline{\text{Sel}}_F(V) \subset \text{Sel}_F(V)$, the assumption implies $\overline{\text{Sel}}_F(V) = 0$. Then the Poitou-Tate exact sequence tells us the exactness of the following sequence:

$$\overline{\text{Sel}}_F(V) \rightarrow H^1(\mathfrak{G}, V) \rightarrow \prod_{l \in S \sqcup \{\mathfrak{p}|p\}} \frac{H^1(F_l, V)}{\overline{L}_l(V)} \rightarrow \overline{\text{Sel}}_F(V^*(1))^*.$$

It is an old theorem of Greenberg (which assumes criticality at $s = 1$) that

$$\dim \overline{\text{Sel}}_F(V) = \dim \overline{\text{Sel}}_F(V^*(1))^*$$

(see [G] Proposition 2 or [HMI] Proposition 3.82); so, we have the assertion (V). In [HMI], Proposition 3.82 is formulated in terms of $\overline{\text{Sel}}_{\mathbb{Q}}(\text{Ind}_F^{\mathbb{Q}} V)$ and $\overline{\text{Sel}}_{\mathbb{Q}}(\text{Ind}_F^{\mathbb{Q}} V^*(1))$ defined in [HMI] (3.4.11), but this does not matter because we can easily verify $\overline{\text{Sel}}_{\mathbb{Q}}(\text{Ind}_F^{\mathbb{Q}} ?) \cong \overline{\text{Sel}}_F(?)$ by Shapiro's lemma (similarly to [HMI] Corollary 3.81). $\square$

1.2. Greenberg's $\mathcal{L}$ -invariant. Let $V = \text{Ad}(\rho_{n,F})$ and $\text{ad}_m(\rho_F)$, and assume (H2-3). Here is Greenberg's definition of $\mathcal{L}(V)$: The long exact sequence of $\mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V \hookrightarrow V / \mathcal{F}_{\mathfrak{p}}^+ V \twoheadrightarrow V / \mathcal{F}_{\mathfrak{p}}^- V$ gives a homomorphism, noting $F_{\mathfrak{p}} = \mathbb{Q}_p$,

$$H^1(F_{\mathfrak{p}}, \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V) = \text{Hom}(\mathfrak{G}_{\mathbb{Q}_p}^{ab}, \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V) \xrightarrow{\iota_{\mathfrak{p}}} H^1(F_{\mathfrak{p}}, V) / L_{\mathfrak{p}}(V).$$

Note that

$$\text{Hom}(G_{\mathbb{Q}_p}^{ab}, \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V) \cong (\mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V)^2 \cong K^2$$

canonically by $\phi \mapsto (\frac{\phi([\gamma_{\mathfrak{p}}, F_{\mathfrak{p}}])}{\log_p(\gamma_{\mathfrak{p}})}, \phi([p, F_{\mathfrak{p}}]))$. Here $[x, F_{\mathfrak{p}}] = [x, \mathbb{Q}_p]$ is the local Artin symbol (suitably normalized). Since

$$L_p(\mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V) = \text{Ker}(H^1(F_{\mathfrak{p}}, \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V) \xrightarrow{\text{Res}} H^1(I_{\mathfrak{p}}, \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V)),$$

the image of $\iota_{\mathfrak{p}}$ is isomorphic to $\mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V \cong K$. By (V), we have a unique subspace $\mathbf{H}_F$ of $H^1(\mathfrak{G}, V)$ projecting down onto

$$\prod_{\mathfrak{p}} \text{Im}(\iota_{\mathfrak{p}}) \hookrightarrow \prod_{\mathfrak{p}} \frac{H^1(F_{\mathfrak{p}}, V)}{L_{\mathfrak{p}}(V)}.$$

Thus

$$(1.4) \quad \mathbf{H}_F = \prod_{\mathfrak{p}|p} \mathbf{H}_{F,\mathfrak{p}} \quad \text{with} \quad \mathbf{H}_{F,\mathfrak{p}} \cong \text{Im}(\iota_{\mathfrak{p}}).$$

Then by the restriction, $\mathbf{H}_F$ gives rise to a subspace L of

$$\prod_{\mathfrak{p}} \text{Hom}(G_{F_{\mathfrak{p}}}^{ab}, \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V) \cong \prod_{\mathfrak{p}} (\mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V)^2$$

isomorphic to $\prod_{\mathfrak{p}} (\mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V)$. If a cocycle c representing an element in $\mathbf{H}_F$ is unramified, it gives rise to an element in $\text{Sel}_F(V)$. By the vanishing of $\text{Sel}_F(V)$ (Lemma 1.1), this implies $c = 0$; so, the projection of L to the first factor $\prod_{\mathfrak{p}} \frac{\mathcal{F}_{\mathfrak{p}}^- V}{\mathcal{F}_{\mathfrak{p}}^+ V}$ (via $\phi \mapsto (\phi([\gamma_{\mathfrak{p}}, F_{\mathfrak{p}}]) / \log_p(\gamma_{\mathfrak{p}}))_{\mathfrak{p}}$) is surjective. Thus this subspace L is a graph of a K -linear map

$$(1.5) \quad \mathcal{L} : \prod_{\mathfrak{p}} \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V \rightarrow \prod_{\mathfrak{p}} \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V.$$

We then define $\mathcal{L}(V) := \det(\mathcal{L}) \in K$.

Fix n , and consider $(R, \rho) = (R_n, \rho_n)$. Suppose Conjecture 0.3: $R_n \cong K[[X_{i,\mathfrak{p}}]]_{i \in I, \mathfrak{p}|p}$. Let

$$(1.6) \quad \mathcal{J} := \det \left(\frac{\partial \delta_{i,\mathfrak{p}}([p, F_{\mathfrak{p}}])}{\partial X_{i',\mathfrak{p}'}} \right)_{\mathfrak{p}, \mathfrak{p}', i, i' \in I},$$

and put $\mathcal{J}_A = \varphi(\mathcal{J})$ for any algebra homomorphism $\varphi : R \rightarrow A$. The following result is a generalization of [HMI] Theorem 3.73:

Theorem 1.5. *Assume Conjecture 0.3 for a positive integer n and (H2-3). If P is the maximal ideal of R_n , we have*

$$\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{Ad}(\rho_{F,n})) = \mathcal{J}_{R/P} \left(\prod_{\mathfrak{p}|p, j \in I} (\beta_{\mathfrak{p}}^{n-j} \alpha_{\mathfrak{p}}^j)([p, F_{\mathfrak{p}}]) \right)^{-1} \left(\prod_{\mathfrak{p}} \log_p(\gamma_{\mathfrak{p}}) \right)^{\lfloor (n+1)/2 \rfloor}.$$

In particular, $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{Ad}(\rho_{F,n}))(\prod_{\mathfrak{p}} \log_p(\gamma_{\mathfrak{p}}))^{-\lfloor (n+1)/2 \rfloor} = \mathcal{J}_{R/P}$ up to units in W .

Proof. Let $\partial_{i,\mathfrak{p}} = \frac{\partial}{\partial X_{i,\mathfrak{p}}} \big|_{X=0} \in \text{Der}_K(R_0, K)$ and $V = \text{Ad}(\rho_{F,n})$. The space $\mathbf{H}_F$ in (1.4) is spanned by $\{(\partial_{i,\mathfrak{p}} \rho) \rho_{F,n}^{-1}\}_{i \in I}$ by Lemma 1.1. Writing $\rho|_{D_{\mathfrak{p}}}$ upper triangular, $\mathcal{F}_{\mathfrak{p}}^+ V$ is made up of upper nilpotent matrices in $\mathfrak{s}(K)$ and $\mathcal{F}_{\mathfrak{p}}^- V$ is made up of upper triangular matrices. Thus $(\partial_{i,\mathfrak{p}} \rho) \rho_{F,n}^{-1} \bmod \mathcal{F}_{\mathfrak{p}}^+ V$ can be identified with $\text{diag}[c_{i,j,\mathfrak{p},\mathfrak{p}'}]_{i,j \in I}$ for $c_{i,j,\mathfrak{p},\mathfrak{p}'} = (\partial_{i,\mathfrak{p}} \delta_{j,\mathfrak{p}'})(\beta_{\mathfrak{p}}^{n-j} \alpha_{\mathfrak{p}}^j)^{-1}$. Indeed by (1.5) (and also (1.1)), we have $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} V) = \det(A) \det(B)^{-1}$ for

$$\det(A) = \det \left((c_{i,j,\mathfrak{p},\mathfrak{p}'}([p, F_{\mathfrak{p}}]))_{\mathfrak{p},\mathfrak{p}',i,j \in I} \right) = \mathcal{J}_{R/P} \left(\prod_{\mathfrak{p}|p, j \in I} (\beta_{\mathfrak{p}}^{n-j} \alpha_{\mathfrak{p}}^j)([p, F_{\mathfrak{p}}]) \right)^{-1}$$

and $B = \prod_{\mathfrak{p}} \det \left((c_{i,j,\mathfrak{p},\mathfrak{p}'}(\gamma_{\mathfrak{p}}) \log_p(\gamma_{\mathfrak{p}})^{-1})_{\mathfrak{p},\mathfrak{p}',i,j \in I} \right)$. Since

$$\delta_{j,\mathfrak{p}}(\beta_{\mathfrak{p}}^{n-j} \alpha_{\mathfrak{p}}^j)^{-1}(\gamma_{\mathfrak{p}}) = 1 + X_{j,\mathfrak{p}},$$

$c_{i,j,\mathfrak{p},\mathfrak{p}'}(\gamma_{\mathfrak{p}}) = \delta_{i,j} \delta_{\mathfrak{p},\mathfrak{p}'}$ for Kronecker symbols $\delta_{i,j}$ and $\delta_{\mathfrak{p},\mathfrak{p}'}$. Thus we conclude

$$(1.7) \quad \det(B) = \left(\prod_{\mathfrak{p}} \log_p(\gamma_{\mathfrak{p}}) \right)^{-\lfloor (n+1)/2 \rfloor}$$

as desired. $\square$

If one restricts $c \in \mathbf{H}_F$ to $\mathfrak{G}_{\infty} := \text{Gal}(F^{(S)}/F_{\infty})$, its ramification is exhausted by $\Gamma = \text{Gal}(F_{\infty}/F)$ (because of the definition of $\text{Sel}_F^{\text{cyc}}(\rho_{2n,n})$ and $\mathbf{H}_F$) giving rise to a class $[c] \in \text{Sel}_{F_{\infty}}(V)$. The kernel of the restriction map: $H^1(\mathfrak{G}, V) \rightarrow H^1(\mathfrak{G}_{\infty}, V)$ is given by $H^1(\Gamma, H^0(\mathfrak{G}_{\infty}, V)) = 0$ because $H^0(\mathfrak{G}_{\infty}, V) = 0$. Thus the image of $\mathbf{H}_F$ in $\text{Sel}_{F_{\infty}}(V/T)$ gives rise to the order g exceptional zero of $L^{\text{arith}}(s, \text{ad}_n(\rho_F))$ at $s = 1$. We have reproved the first half of the following result in [G] Proposition 1.

Proposition 1.6. *Let m be an odd positive integer. Suppose Conjecture 0.3 for m or $m+1$. Then for the number g of prime factors of p in F , we have*

$$\text{ord}_{s=1} L_p^{\text{arith}}(s, \text{ad}_m(\rho_F)) \geq g.$$

Further, we have $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F)) = 0 \iff \text{ord}_{s=1} L_p^{\text{arith}}(s, \text{ad}_m(\rho_F)) > g$.

The last assertion follows from [G] Proposition 3.

2. FACTORIZATION OF $\mathcal{L}$ -INVARIANT

We continue to assume (H2-3) in the proofs given in this section. We recall the factorization (given in [H07b]) of $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F))$ for odd m into the product of local invariants over potentially multiplicative places and the global invariant from the contribution of the potentially crystalline part. This potentially crystalline part gives $\mathcal{L}(m)$ for $\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} \text{ad}_m(\rho_F))$ in Theorem 0.4.

2.1. Factorization. We keep notation introduced in the previous section; so, V is either $ad_m(\rho_F)$ or $Ad(\rho_{n,0})$.

Proposition 2.1. *Let V be either $ad_m(\rho_F)$ with odd $m \geq 1$ or $Ad(\rho_{F,n})$. Suppose $b > 0$, and fix an index k with $1 \leq k \leq b$. Let $a \in \prod_{i=1}^g \text{Hom}(D_{\mathfrak{p}_i}, \mathcal{F}_{\mathfrak{p}_i}^- V / \mathcal{F}_{\mathfrak{p}_i}^+ V)$ be induced by $c \in \mathbf{H}_{F,\mathfrak{p}_k}$ (so, $c \in \mathbf{H}_F$ restricts down trivially to $\frac{H^1(F_{\mathfrak{p}_i}, V)}{L_{\mathfrak{p}_i}(V)}$ for all $i \neq k$). Then we have $a(\gamma_{\mathfrak{p}_i}) = 0$ for all $i \neq k$ and $a([p, F_{\mathfrak{p}_{k'}}]) = 0$ for all $k' \neq k$ with $k' \leq b$.*

Proof. If $i > b$, $L_{\mathfrak{p}_i}(V)$ is made of classes of cocycles becoming unramified modulo those with values in $\mathcal{F}_{\mathfrak{p}_i}^+ V$; so, even if $c|_{D_{\mathfrak{p}_i}}$ vanishes in $\frac{H^1(F_{\mathfrak{p}_i}, V)}{L_{\mathfrak{p}_i}(V)}$ (that is, $c|_{D_{\mathfrak{p}_i}} \in L_{\mathfrak{p}_i}(V)$), we cannot pull out much information on the value $a([p, F_{\mathfrak{p}_i}])$ because of the ambiguity modulo unramified cocycles with values in $\mathcal{F}_{\mathfrak{p}_i}^- V / \mathcal{F}_{\mathfrak{p}_i}^+ V$. Anyway, $a(\gamma_{\mathfrak{p}_i}) = 0$ because $\gamma_{\mathfrak{p}_i} \in I_{\mathfrak{p}_i}$.

For $i \leq b$ with $i \neq k$, by Lemma 1.3, $\overline{L}_{\mathfrak{p}_i}(V)$ is made of cocycles of $D_{\mathfrak{p}_i}$ with values in $\mathcal{F}_{\mathfrak{p}_i}^+ V$, and the condition that $c|_{D_{\mathfrak{p}_i}} \in \overline{L}_{\mathfrak{p}_i}(V)$ implies the vanishing of $a(\sigma) = c(\sigma) \bmod \mathcal{F}_{\mathfrak{p}_i}^+ V$ for all $\sigma \in D_{\mathfrak{p}_i}$. This shows the assertion. $\square$

By the above proposition, we get immediately the following fact.

Corollary 2.2. *Let the notation be as in Proposition 2.1. Then the linear endomorphism $\mathcal{L}$ in (1.5) acting on $\prod_{\mathfrak{p}} \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V$ preserves the following exact sequence:*

$$0 \rightarrow \prod_{i>b} \mathcal{F}_{\mathfrak{p}_i}^- V / \mathcal{F}_{\mathfrak{p}_i}^+ V \rightarrow \prod_{\mathfrak{p}} \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V \rightarrow \prod_{k \leq b} \mathcal{F}_{\mathfrak{p}_k}^- V / \mathcal{F}_{\mathfrak{p}_k}^+ V \rightarrow 0,$$

and $\mathcal{L}$ acting on the quotient $\prod_{k \leq b} \mathcal{F}_{\mathfrak{p}_k}^- V / \mathcal{F}_{\mathfrak{p}_k}^+ V$ sends $\mathcal{F}_{\mathfrak{p}_k}^- V / \mathcal{F}_{\mathfrak{p}_k}^+ V$ into itself for each $k \leq b$.

Definition 2.1. Let $V = ad_m(\rho_F)$. Define $\mathcal{L}(m)$ by

$$\det \left(\mathcal{L}|_{\prod_{i>b} \mathcal{F}_{\mathfrak{p}_i}^- V / \mathcal{F}_{\mathfrak{p}_i}^+ V} \right) \in K.$$

Similarly, define $\mathcal{L}_k(ad_m(\rho_F))$ for $k \leq b$ by the determinant of the linear operator induced by $\mathcal{L}$ on $\mathcal{F}_{\mathfrak{p}_k}^- V / \mathcal{F}_{\mathfrak{p}_k}^+ V = \prod_{\mathfrak{p}} \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V / \prod_{i \neq k} \mathcal{F}_{\mathfrak{p}_i}^- V / \mathcal{F}_{\mathfrak{p}_i}^+ V$.

Corollary 2.3. *Let the notation be as above. Then we have*

$$\mathcal{L}(\text{Ind}_F^{\mathbb{Q}} ad_m(\rho_F)) = \mathcal{L}(m) \prod_{k=1}^b \mathcal{L}_k(ad_m(\rho_F))$$

for odd $n \geq 1$.

2.2. Multiplicative $\mathcal{L}$ -invariant. We now relate $\mathcal{L}_k(ad_m(\rho_F))$ to the p -adic logarithm of the tate period of ρ_F if $k \leq b$. Let $\rho_{n,m} = \text{Sym}(\rho_F)^{\otimes n} \otimes \det(\rho_F)^{-m}$; so, $ad_m(\rho_F) = \rho_{2m,m}$. We start with

Lemma 2.4. *Suppose that $\rho_F|_{D_{\mathfrak{p}}} \cong \begin{pmatrix} \mathcal{N} & \xi_q \\ 0 & 1 \end{pmatrix}$ for $\xi_q(\sigma) = \varprojlim_n (p^n \sqrt{q})^{\sigma-1}$ with a nonunit $q \in F_{\mathfrak{p}}^{\times}$. Then if $0 \leq m \leq n$, we have $\mathcal{F}_{\mathfrak{p}}^- \rho_{n,m} / \mathcal{F}_{\mathfrak{p}}^2 \rho_{n,m} \cong \rho_F$ as $D_{\mathfrak{p}}$ -modules.*

Proof. Write $M(m) = M \otimes \mathcal{N}^m$ for a $D_{\mathfrak{p}}$ -module M . Identify $\rho_0|_{D_{\mathfrak{p}}}$ with $\begin{pmatrix} \mathcal{N} & \xi_q \\ 0 & 1 \end{pmatrix}$ choosing a basis (x, y) of ρ_0 . Then the matrix expression of $\rho_{F,n}$ on $D_{\mathfrak{p}}$ with respect the basis $(x^n, x^{n-1}y, \dots, y^n)$ is given by

$$\begin{pmatrix} \mathcal{N}^n & n\mathcal{N}^{n-1}\xi_q & * & \cdots & * \\ 0 & \mathcal{N}^{n-1} & (n-1)\mathcal{N}^{n-2}\xi_q & \cdots & * \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \mathcal{N} & \xi_q \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

Thus we get an extension $K(m+1) \hookrightarrow \mathcal{F}_{\mathfrak{p}}^m \rho_{F,n} / \mathcal{F}_{\mathfrak{p}}^{m+2} \rho_{F,n} \twoheadrightarrow K(m)$ of $D_{\mathfrak{p}}$ -modules on which $D_{\mathfrak{p}}$ acts by $\begin{pmatrix} \mathcal{N}^{m+1} & (m+1)\mathcal{N}^m \xi_q \\ 0 & \mathcal{N}^m \end{pmatrix}$. We have the following commutative diagram of exact rows:

$$\begin{array}{ccccc} K(1) & \xrightarrow{\hookrightarrow} & \frac{\mathcal{F}_{\mathfrak{p}}^m \rho_{F,n}}{\mathcal{F}_{\mathfrak{p}}^{m+2} \rho_{F,n}} \otimes \det(\rho_0)^{-m} & \twoheadrightarrow & K \\ \parallel \downarrow & & \downarrow \wr & & \downarrow \parallel \\ K(1) & \xrightarrow{\hookrightarrow} & \frac{\mathcal{F}_{\mathfrak{p}}^m \rho_{n,m}}{\mathcal{F}_{\mathfrak{p}}^{m+2} \rho_{n,m}} & \twoheadrightarrow & K, \end{array}$$

because $\begin{pmatrix} m+1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \mathcal{N} & (m+1)\xi_q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m+1 & 0 \\ 0 & 1 \end{pmatrix} \cong \begin{pmatrix} \mathcal{N} & \xi_q \\ 0 & 1 \end{pmatrix}$. This proves the desired assertion. $\square$

Here is the first main result:

Theorem 2.5. *Suppose Conjecture 0.3 for n . Then we have $\mathcal{L}_k(Ad(\rho_{F,n})) = \left(\frac{\log_p(Q_k)}{\text{ord}_p(Q_k)} \right)^{\lfloor (n+1)/2 \rfloor}$ for $k \leq b$, where $Q_k = N_{F_{\mathfrak{p}_k}/\mathbb{Q}_p}(q_k)$ for the Tate period q_k of ρ_F at $\mathfrak{p}_k$.*

Proof. Fix $k \leq b$, and write $\mathfrak{p} = \mathfrak{p}_k$. Since $Ad(\text{Sym}^{\otimes n}(\rho_0 \otimes \eta)) \cong Ad(\rho_{F,n})$, by twisting ρ_F by a character, we may assume that $\rho_F|_{D_{\mathfrak{p}_k}} \cong \begin{pmatrix} \mathcal{N} & \xi_{q_k} \\ 0 & 1 \end{pmatrix}$. In this proof, we assume (H1-2).

Write $X_i = X_{i,\mathfrak{p}_j}$ if $i \in I$. For $\ell \in I$, define $\mathfrak{M}_{\ell}$ be the ideal generated by X_i for $i \neq \ell$ ($i, \ell \in I$) and X_{ℓ}^2 . We fix a ℓ with $0 \leq \ell \leq n$, and write $\mathfrak{M}$ for $\mathfrak{M}_{\ell}$ and $\tilde{K} = R_n/\mathfrak{M} \cong K[\varepsilon]$ with $\varepsilon^2 = 0$ by $X_{\ell} \mapsto \varepsilon$. Let $\bar{\rho} = (\rho_n \bmod \mathfrak{M})$, and write $\bar{\delta}_j$ for $\delta_{j,\mathfrak{p}} \bmod \mathfrak{M}$. We consider the exact sequence of $\tilde{K}[D_{\mathfrak{p}}]$ -modules:

$$0 \rightarrow \frac{\mathcal{F}_{\mathfrak{p}}^{j+1} \bar{\rho}}{\mathcal{F}_{\mathfrak{p}}^{j+2} \bar{\rho}} \rightarrow \frac{\mathcal{F}_{\mathfrak{p}}^j \bar{\rho}}{\mathcal{F}_{\mathfrak{p}}^{j+2} \bar{\rho}} \rightarrow \frac{\mathcal{F}_{\mathfrak{p}}^j \bar{\rho}}{\mathcal{F}_{\mathfrak{p}}^{j+1} \bar{\rho}} \rightarrow 0.$$

Writing $\tilde{K}(\psi)$ for the rank one free $\tilde{K}$ -module on which $D_{\mathfrak{p}}$ acts by a character $\psi : D_{\mathfrak{p}} \rightarrow \tilde{K}^{\times}$, this exact sequence gives the following exact sequence

$$0 \rightarrow \tilde{K}(\bar{\delta}_{j+1}) \rightarrow \frac{\mathcal{F}_{\mathfrak{p}}^j \bar{\rho}}{\mathcal{F}_{\mathfrak{p}}^{j+2} \bar{\rho}} \rightarrow \tilde{K}(\bar{\delta}_j) \rightarrow 0.$$

Twisting by $\bar{\delta}_{j+1}^{-1} \mathcal{N}$, we get another exact sequence of $\tilde{K}[D_{\mathfrak{p}}]$ -modules:

$$0 \rightarrow \tilde{K}(\mathcal{N}) \rightarrow M \rightarrow \tilde{K}(\bar{\delta}_j \bar{\delta}_{j+1}^{-1} \mathcal{N}) \rightarrow 0.$$

By Lemma 2.4, this sequence gives the top row of the following commutative diagram of $D_{\mathfrak{p}}$ -modules with exact rows:

$$\begin{array}{ccccc} \tilde{K}(\mathcal{N}) & \xrightarrow{\hookrightarrow} & M & \twoheadrightarrow & \tilde{K}(\bar{\delta}_j \bar{\delta}_{j+1}^{-1} \mathcal{N}) \\ \text{mod } X_{\ell} \downarrow & & \text{mod } X_{\ell} \downarrow & & \downarrow \text{mod } X_{\ell} \\ K(\mathcal{N}) & \xrightarrow{\hookrightarrow} & \rho_0|_{D_{\mathfrak{p}_k}} & \twoheadrightarrow & K. \end{array}$$

By our assumption (H2): $F_{\mathfrak{p}} = \mathbb{Q}_p$, $D_{\mathfrak{p}} = D_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, and by (2.3.4) of [GS1], this implies

$$\frac{\partial \delta_j \delta_{j+1}^{-1} \mathcal{N}}{\partial X_{\ell}}([q_k, \mathbb{Q}_p]) = 0.$$

In (2.3.4) of [GS1], the coefficient field of the Galois representation is assumed to be $\mathbb{Q}_p$, but the argument proving the theorem works well for general coefficient fields K as easily checked. Since $\mathcal{N}([q_k, \mathbb{Q}_p])$ is a constant in $\mathbb{Q}_p^{\times}$, we get

$$\frac{\partial \delta_j \delta_{j+1}^{-1}}{\partial X_{\ell}}([q_k, \mathbb{Q}_p]) = 0$$

which yields by the Leibnitz formula

$$\left(\delta_j^{-1} \frac{\partial \delta_j}{\partial X_\ell} - \delta_{j+1}^{-1} \frac{\partial \delta_{j+1}}{\partial X_\ell} \right) ([q_k, \mathbb{Q}_p]) = 0,$$

where $\delta_j = (\delta_j \bmod \mathfrak{m}_n) = \mathcal{N}^{n-j}$. Since this holds for $j = 0, 1, \dots, n$, we get

$$\left(\delta_0^{-1} \frac{\partial \delta_0}{\partial X_\ell} - \delta_n^{-1} \frac{\partial \delta_n}{\partial X_\ell} \right) ([q_k, \mathbb{Q}_p]) = 0.$$

Since $\delta_0 \delta_n = \mathcal{N}$ on $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ ($F_{\mathfrak{p}} = \mathbb{Q}_p$ by (H2)), we have

$$\delta_0^{-1} \frac{\partial \delta_0}{\partial X_\ell} = -\delta_n^{-1} \frac{\partial \delta_n}{\partial X_\ell},$$

and hence

$$\delta_n^{-1} \frac{\partial \delta_n}{\partial X_\ell} ([q_k, \mathbb{Q}_p]) = 0.$$

This in turn yields

$$\delta_j^{-1} \frac{\partial \delta_j}{\partial X_\ell} ([q_k, \mathbb{Q}_p]) = 0$$

for all $j = 0, 1, \dots, n$.

Write $q_k = p^a u$ for $a = \text{ord}_p(q_k)$ and $u \in \mathbb{Z}_p^\times$. Then $\log_p(u) = \log_p(q_k)$, and we have

$$\delta_i([q_k, \mathbb{Q}_p]) \equiv \delta_i([p, \mathbb{Q}_p])^a \delta_i([u, \mathbb{Q}_p]) \equiv \delta_i([p, \mathbb{Q}_p])^a (1 + X_i)^{-\log_p(u)/\log_p(\gamma_{\mathfrak{p}_i})} \bmod \mathfrak{M}.$$

Differentiating this identity with respect to X_ℓ , we get from $\delta_i([p, \mathbb{Q}_p]) = \mathcal{N}^{n-i}([p, \mathbb{Q}_p]) = 1$

$$a \frac{\partial \delta_\ell}{\partial X_\ell} \Big|_{X=0} ([p, \mathbb{Q}_p]) - \frac{\log_p(u)}{\log_p(\gamma_k)} = 0 \quad \text{and} \quad a \frac{\partial \delta_i}{\partial X_\ell} \Big|_{X=0} ([p, \mathbb{Q}_p]) = 0 \quad \text{if } i \neq \ell \ (i, \ell \in I).$$

Since $a \neq 0$, we have

$$\frac{\partial \delta_i}{\partial X_\ell} \Big|_{X=0} ([p, \mathbb{Q}_p]) = 0 \quad \text{if } i \neq \ell \ (i, \ell \in I), \text{ and } \frac{\partial \delta_\ell}{\partial X_\ell} \Big|_{X=0} ([p, \mathbb{Q}_p]) \log_p(\gamma_{\mathfrak{p}_k}) = \frac{\log_p(q_k)}{\text{ord}_p(q_k)}.$$

Since $\frac{\partial \rho_n}{\partial X_\ell} \Big|_{X=0} \rho_{F,n}^{-1}$ for odd ℓ with $0 < \ell \leq n$ gives a basis of the $\mathfrak{p}$ -part of $\mathbf{H}_F$ isomorphic to $\text{Im}(\iota_{\mathfrak{p}})$,

we find that $\mathcal{L}_k(\text{Ad}(\rho_{F,n})) = \left(\frac{\log_p(q_k)}{\text{ord}_p(q_k)} \right)^{\lfloor (n+1)/2 \rfloor}$. Since we have

$$\text{Sel}_F^{cyc}(\text{Ad}(\rho_{F,n})) \cong \bigoplus_{0 < m \leq n, m: \text{odd}} \text{Sel}_F^{cyc}(\text{ad}_m(\rho_F)),$$

we find

$$(2.1) \quad \mathcal{L}_k(\text{Ad}(\rho_{F,n})) = \prod_{0 < m \leq n, m: \text{odd}} \mathcal{L}_k(\text{ad}_m(\rho_F)) = \left(\frac{\log_p(q_k)}{\text{ord}_p(q_k)} \right)^{\lfloor (n+1)/2 \rfloor}$$

as desired. $\square$

2.3. Proof of Theorem 0.4. We now prove Theorem 0.4 (assuming (H1–2)). We note $\text{Ad}(\rho_{F,n_2}) \cong \text{Ad}(\rho_{F,n_1}) \oplus \text{ad}_m(\rho_F)$. Thus by definition, we have $\mathcal{L}_k(\text{Ad}(\rho_{F,n_2})) = \mathcal{L}_k(\text{Ad}(\rho_{F,n_1})) \mathcal{L}_k(\text{ad}_m(\rho_F))$. Then by Theorem 2.5, if $\log_p(q_k) \neq 0$ we have

$$\mathcal{L}_k(\text{ad}_m(\rho_F)) = \frac{\mathcal{L}_k(\text{Ad}(\rho_{F,n_2}))}{\mathcal{L}_k(\text{Ad}(\rho_{F,n_1}))} = \frac{\left(\frac{\log_p(q_k)}{\text{ord}_p(q_k)} \right)^{\lfloor (n_2+1)/2 \rfloor}}{\left(\frac{\log_p(q_k)}{\text{ord}_p(q_k)} \right)^{\lfloor (n_1+1)/2 \rfloor}} = \frac{\log_p(q_k)}{\text{ord}_p(q_k)}$$

as desired. If $\log_p(q_k) = 0$, the linear operator $\mathcal{L}|_{\text{gr}^0(\text{Ad}(\rho_{F,n_2}))}$ induced by $\mathcal{L}$ in Definition 2.1 on the quotient $\text{gr}^0(V) := \mathcal{F}_{\mathfrak{p}_k}^- V / \mathcal{F}_{\mathfrak{p}_k}^+ V = \prod_{\mathfrak{p}} \mathcal{F}_{\mathfrak{p}}^- V / \mathcal{F}_{\mathfrak{p}}^+ V / \prod_{i \neq k} \mathcal{F}_{\mathfrak{p}_i}^- V / \mathcal{F}_{\mathfrak{p}_i}^+ V$ for $V = \text{Ad}(\rho_{F,n_2})$ has only

eigenvalue 0. Since $ad_m(\rho_F)$ is a factor of $Ad(\rho_{F,n_2})$, the corresponding operator $\mathcal{L}|_{gr^0(ad_m(\rho_F))}$ on the 0-th graded piece $gr^0(ad_m(\rho_F)) := \mathcal{F}_{\mathfrak{p}_k}^- ad_m(\rho_F) / \mathcal{F}_{\mathfrak{p}_k}^+ ad_m(\rho_F)$ is induced by $\mathcal{L}|_{gr^0(Ad(\rho_{F,n_2}))}$; so, it has unique eigenvalue 0, and hence $\mathcal{L}_k(ad_m(\rho_F)) = 0 = \frac{\log_p(q_k)}{\text{ord}_p(q_k)}$. Then the desired formula in the theorem follows from the definition of $\mathcal{L}(m)$ in Definition 2.1. $\square$

3. PROOF OF CONJECTURE 0.3 UNDER POTENTIAL MODULARITY

We first prove Conjecture 0.3 for ρ_F if it is valid for the restriction ρ_L of ρ_F to $\text{Gal}(\overline{F}/L)$ for a totally real finite Galois extension L/F . Then by a result of Taylor, we show that this potential version of the conjecture holds under mild assumptions, which proves Corollary 0.6. In this section, we do not assume (H1–3).

3.1. Potential version implies Conjecture 0.3. Let $S_{p,L}$ be the set of prime factors of p in L for a number field L .

Proposition 3.1. *Let (R_L, ρ_L) be the universal couple for $\rho_{L,n}$ for a totally real extension L/F . If there exists a finite totally real Galois extension L/F such that $R_L \cong K[[X_{i,\mathfrak{p}}]]_{i \in I, \mathfrak{p} \in S_{p,L}}$ for the variable $X_{i,\mathfrak{p}}$ specified in Conjecture 0.3, then Conjecture 0.3 holds for $\rho_{F,n}$ and F .*

Proof. By assumption, we have $R_L \cong K[[X_{i,\mathfrak{p}}]]_{i \in I, \mathfrak{p} \in S_{p,L}}$. For $\sigma \in \text{Gal}(L/F)$, we take a lift $\tilde{\sigma} \in \text{Gal}(\overline{F}/L)$ inducing σ on L , for any deformation ρ of ρ_L with values in A , regarding ρ_F as having values in $G(A)$ through the K -algebra structure $K \hookrightarrow A$, we can define

$$\rho^\sigma(g) = \rho_{F,n}(\tilde{\sigma})^{-1} \rho(\tilde{\sigma} g \tilde{\sigma}^{-1}) \rho_{F,n}(\tilde{\sigma}).$$

The isomorphism class of ρ^σ is determined independently of the choice of the lift $\tilde{\sigma}$ and depends only on σ . Since ρ_L extends to $\rho_F : \text{Gal}(\overline{F}/F) \rightarrow G(W)$, $\rho_{L,n}^\sigma = \rho_{L,n}$, for $\rho_L = \rho|_{\text{Gal}(\overline{F}/L)}$, ρ_L^σ is another deformation of $\rho_{L,n}$ over $\text{Gal}(\overline{F}/L)$ satisfying (K1–4). Thus we have a unique ring automorphism $[\sigma] \in \text{Aut}(R_L)$ such that $\rho_L^\sigma \approx [\sigma] \circ \rho_L$. In this way, $\Delta := \text{Gal}(L/F)$ acts on R_L . Since $\delta_{i,\mathfrak{p}}^\sigma(g) = \delta_{i,\mathfrak{p}}(\tilde{\sigma} g \tilde{\sigma}^{-1})$ coincides with $\delta_{i,\mathfrak{p}\sigma}$, we have $[\sigma](X_{i,\mathfrak{p}}) = X_{i,\mathfrak{p}\sigma}$. Note that $H^2(\Delta, K) = 0$ (because Δ is finite and K is uniquely divisible). Then by the K -deformation version of Theorem 5.42 in [MFG], we have $R_F \cong R_L / \sum_{\sigma \in \Delta} R_L([\sigma] - 1)R_L$, where $\sum_{\sigma \in \Delta} R_L([\sigma] - 1)R_L$ is the ideal of R_L generated by $[\sigma](r) - r$ for all $r \in R_L$. Then it is clear that $R_F \cong K[[X_{i,\mathfrak{p}}]]_{i \in I, \mathfrak{p} \in S_p}$ as desired. $\square$

3.2. Proof of Corollary 0.6. We first state a general proposition and then prove the corollary reducing it to a special case of the proposition.

Let $\overline{\rho}_F = \rho_F \bmod \mathfrak{m}_W$ having values in $GL_2(\mathbb{F})$ for the residue field $\mathbb{F}$ of W . We consider the following conditions:

- (NS) $\text{Im}(\overline{\rho}_F)$ is a non-soluble subgroup in $GL_2(\mathbb{F})$;
- (DS) the semi-simplification of $\overline{\rho}_F$ restricted to $D_{\mathfrak{p}}$ is non-scalar.

We now give a sketch of a proof of Conjecture 0.3 for $n = 1$ under these two conditions:

Proposition 3.2. *Suppose (NS). Then we have $R_1 \cong K[[X_{1,\mathfrak{p}}]]_{\mathfrak{p}|p}$ as in Conjecture 0.3 for $n = 1$.*

This proposition implies Corollary 0.6 because for elliptic curve with ordinary reduction (including multiplicative one) at $\mathfrak{p}$, the two characters $(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ is given by $(1, \mathcal{N})$ over the inertia group $I_{\mathfrak{p}}$ which are distinct modulo $\mathfrak{m}_W$ if p is unramified in $F/\mathbb{Q}$ and p is odd. The condition (NS) follows from nonsolubility of the field of rationality of p -torsion points of the elliptic curve.

Proof. By the result of [Ta] and [Ta1], the Galois representation $\overline{\rho}_F$ is potentially modular in the sense that there exists a totally real Galois extension L/F in which p totally split and $\overline{\rho}_L$ is associated to a Hilbert cusp form of weight 2 and $\text{Im}(\rho_L)$ is still nonsoluble (in particular, it is absolutely irreducible over $L[\mu_p]$). Actually, in the above paper of Taylor, details of the proof are given for $F = \mathbb{Q}$, but we can adjust his argument to prove the result for general F (see [V] Theorem 2.2). Since any $\mathfrak{p} \in S_p$ splits totally in L/F , (DS) is also valid over L if it holds over F . Assuming (DS) over F , by a result

of Fujiwara (see [Fu1] and [HMI] Proposition 3.78) which requires absolute irreducibility of $\bar{\rho}_{L[\mu_p]}$ and (DS) over $D_{\mathfrak{P}}$ for all $\mathfrak{P} \in S_{p,L}$, we have Conjecture 0.3 for ρ_L . The assumption (DS) of [Fu1] is recently removed by [Ch] by considering framed deformation of upper triangular type. Thus we do not need to assume (DS) over F now. Then by the above proposition, the desired result follows. $\square$

Remark 3.1. Since the potential modularity for ρ_n is proven in [Ta2] under some assumptions, we expect that the above argument (or a modified version) would prove Conjecture 0.3 for general n in near future.

4. $\mathcal{L}$ -INVARIANTS OF CM FIELDS

This section is almost identical to Section 3 of [H07a]; however, we correct some minor errors there coming from the factor $[F_{\mathfrak{p}} : \mathbb{Q}_p]$ in Theorem 0.4 here missing from Theorem 0.4 in [H07a]. Since this factor does not matter under (H2), we do not assume (H1–3) in this section.

Let p be an odd prime. Let M/F be a totally imaginary quadratic extension of the base totally real field F . We study the adjoint square Selmer group when the Galois representation is an induction of a Galois character of $\mathfrak{G}_M := \text{Gal}(M^{(p)}/M)$. Put $\mathfrak{G}_F := \text{Gal}(M^{(p)}/F)$. For simplicity, we assume that $p > 2$ totally splits in $M/\mathbb{Q}$. We relate the Selmer group with a more classical Iwasawa module of a quadratic extension of F , and from the torsion property of the Selmer group already proven, we deduce some torsion property of such classical Iwasawa modules. In this section, our starting deformation (the origin of $\text{Spec}(R_1)$) is $\rho_F = \text{Ind}_M^F \lambda$ for a p -adic Galois character λ of $\text{Gal}(\bar{\mathbb{Q}}/M)$.

4.1. CM Iwasawa modules. Let O_M be the integer ring of M . We consider $Z = \varprojlim_n Cl_M(p^n)$ for the ray class group $Cl_M(p^n)$ of M modulo p^n . Let Δ be the maximal torsion subgroup of Z , and put $\Gamma_M = Z/\Delta$, which has a natural action of $\text{Gal}(M/F)$. We split $Z = \Delta \times \Gamma_M$. We define $\Gamma^+ = H^0(\text{Gal}(M/F), \Gamma_M)$ and $\Gamma^- = \Gamma_M/\Gamma^+$. Since $p > 2$, the action of $\text{Gal}(M/F)$ splits the extension $\Gamma^+ \hookrightarrow \Gamma_M \twoheadrightarrow \Gamma^-$, and we have a canonical decomposition $\Gamma_M = \Gamma^+ \times \Gamma^-$. Write $\pi^- : Z \rightarrow \Gamma^-$, $\pi^+ : \Gamma_M \rightarrow \Gamma^+$ and $\pi_\Delta : Z \rightarrow \Delta$ for the three projections. Take a character $\varphi : \Delta \rightarrow \bar{\mathbb{Q}}^\times$, and regard it as a character of Z through the projection: $Z \twoheadrightarrow \Delta$.

Let M_∞ be the composite of all $\mathbb{Z}_p$ -extensions of M . Then by class field theory, M_∞ is the subfield of the ray class field of M modulo p^∞ fixed by Δ . Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$ -extension. Let M_∞^{cyc} be the composite $M\mathbb{Q}_\infty/M$. Define M_∞^- (resp. M_∞^+) for the fixed subfield of Γ^- (resp. Γ^+). Since M_∞^{cyc} is abelian over F , we have $M_\infty^{cyc} \subset M_\infty^+$ and a projection $\pi_{cyc} : \Gamma^+ \rightarrow \text{Gal}(M_\infty^{cyc}/M) \subset 1 + p\mathbb{Z}_p$. The Leopoldt conjecture for F asserts that π_{cyc} is an isomorphism; in other words, $M_\infty^+ = M_\infty^{cyc}$. The extension M_∞^-/M is called the anticyclotomic tower over M . Thus if the Leopoldt conjecture holds for F , M_∞ is the composite of the cyclotomic $\mathbb{Z}_p$ -extension M_∞^{cyc} and the anticyclotomic $\mathbb{Z}_p^{[F:\mathbb{Q}]}$ -extension M_∞^- .

To introduce Iwasawa modules for the multiple $\mathbb{Z}_p$ -extensions $M_\infty^?/M$, we fix a CM type Σ , which is a set of embeddings of M into $\bar{\mathbb{Q}}$ such that $I_M = \Sigma \sqcup \Sigma c$ for the generator c of $\text{Gal}(M/F)$. Over $\mathbb{C}$, an abelian variety with complex multiplication by M has $\mathbb{C}$ -points isomorphic to $\mathbb{C}^\Sigma/\Sigma(\mathfrak{a})$ for a lattice $\mathfrak{a}$ in M (see [ACM] 5.2), where $\Sigma(\mathfrak{a}) = \{(\sigma(\mathfrak{a}))_{\sigma \in \Sigma} \in \mathbb{C}^\Sigma \mid \mathfrak{a} \in \mathfrak{a}\}$. By composing i_p , we write Σ_p for the set of p -adic places induced by $i_p \circ \sigma$ for $\sigma \in \Sigma$. We assume

$$(spt) \quad \Sigma_p \cap \Sigma_p c = \emptyset.$$

This is to guarantee the abelian variety of CM type Σ to have ordinary good reduction modulo p (whose Galois representation is hence ordinary at all $\mathfrak{p} \mid p$).

Writing $M(p^\infty)$ for the ray class field over M modulo p^∞ , we identify Z with $\text{Gal}(M(p^\infty)/M)$ via the Artin reciprocity law. Fix a character φ of Δ . We then define M_Δ by the fixed field of Γ in $M(p^\infty)$; so, $\text{Gal}(M_\Delta/M) = \Delta$.

Since φ is a character of Δ , φ factors through $\text{Gal}(M_\infty^? M_\Delta/M)$ for $?$ indicating one of $+$, $-$, cyc or “nothing”. When nothing is attached, it refers to the object for the full multiple $\mathbb{Z}_p$ -extension M_∞ . Let $L_\infty^?/M_\infty^? M_\Delta$ be the maximal p -abelian extension unramified outside Σ_p . Each $\gamma \in \text{Gal}(L_\infty/M)$

acts on the normal subgroup $X^\gamma = \text{Gal}(L_\infty^\gamma/M_\infty^\gamma M_\Delta)$ continuously by conjugation, and by the commutativity of X^γ , this action factors through $\text{Gal}(M_\Delta M_\infty^\gamma/M)$. Then we look into the compact p -profinite Γ^γ -module: $X^\gamma[\varphi] = X^\gamma \otimes_{\mathbb{Z}_p[\Delta], \varphi} W$, where $\Gamma^\gamma = \text{Gal}(M_\infty^\gamma/M)$. We study when $X^\gamma[\varphi]$ is a torsion Iwasawa module over $\Lambda^\gamma = W[[\Gamma^\gamma]]$. The module $X^\gamma[\varphi]$ is generally expected to be torsion of finite type over Λ^γ for the naturally defined multiple $\mathbb{Z}_p$ -extensions M_∞^γ .

The torsion property of $X^{cyc}[\varphi]$ over Λ^{cyc} is classically known (e.g., [HT2] Theorem 1.2.2). This implies

Theorem 4.1. *The modules $X[\varphi]$, $X^+[\varphi]$ and $X^{cyc}[\varphi]$ are torsion modules over the corresponding Iwasawa algebra Λ , Λ^+ and Λ^{cyc} , respectively.*

We refer this result to [HT2] Theorem 1.2.2 (which was originally due to R. Greenberg). We study the anticyclotomic Iwasawa module $X^-[\varphi]$ over Λ^- from our new view point of Galois deformation theory. As is well known, $X^-[\varphi]$ is a Λ^- -module of finite type, and under mild assumptions (including anticyclotomicity of φ), we will prove the torsion property of $X^-[\varphi]$ in Theorem 4.3.

The Σ -Leopoldt conjecture for abelian extensions of M is almost equivalent to the torsion property of $X^-[\varphi]$ over Λ^- for all possible φ (see [HT2] Theorem 1.2.2). Here, for an abelian extension L/M with integer ring O_L , the Σ -Leopoldt conjecture asserts the closure $\overline{O_L^\times}$ of $O_L^\times$ in $L_\Sigma = \prod_{\mathfrak{p} \in \Sigma_p} L_{\mathfrak{p}}$ satisfies

$$\dim_{\mathbb{Q}}(O_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}) = \dim_{\mathbb{Q}_p}(\overline{O_L^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

If $X^-[\varphi]$ is a torsion Λ^- -module, we can think of the characteristic element $\mathcal{F}^-(\varphi) \in \Lambda^-$ of the module $X^-[\varphi]$. The anticyclotomic main conjecture (cf. [HT] Conjecture 2.2) predicts the identity (up to units) of $\mathcal{F}^-(\varphi)$ and the projection of (the φ -branch of) the Katz p -adic L -function (constructed in [K] and [HT1]) under π^- .

4.2. Anticyclotomic Iwasawa modules. A character ψ of Δ is said *anticyclotomic* if $\psi(c\sigma c^{-1}) = \psi^{-1}(\sigma)$ for a complex conjugation $c \in \text{Gal}(\overline{\mathbb{Q}}/F)$. Fix an algebraic closure $\overline{F}$ of F . Regarding φ as a Galois character, we define $\varphi^-(\sigma) = \varphi(c\sigma c^{-1}\sigma^{-1})$ for $\sigma \in \text{Gal}(\overline{F}/M)$. Then $\psi := \varphi^-$ is anticyclotomic. Conversely, for any anticyclotomic character ψ , we can find φ with $\psi = \varphi^-$ (e.g., [HMI] Lemma 5.31).

We define a Galois character $\tilde{\varphi} : \mathfrak{G}_F \rightarrow W[[\Gamma^-]]$ by $\tilde{\varphi}(\sigma) = \varphi(\sigma)(\sigma|_{M_\infty^-})^{1/2}$, where $(\sigma|_{M_\infty^-})^{1/2}$ is the unique square root of $(\sigma|_{M_\infty^-})$ in Γ^- and $(\sigma|_{M_\infty^-}) \in \Gamma^-$ is regarded as a group element in $\Gamma^- \subset W[[\Gamma^-]]$. Note that $\tilde{\varphi}(\sigma) = \tilde{\varphi}(c\sigma c^{-1}\sigma^{-1}) = \psi(\sigma)\sigma|_{M_\infty^-}$. Then we consider $\text{Ind}_M^F(\tilde{\varphi}) : \text{Gal}(\overline{F}/F) \rightarrow GL_2(W[[\Gamma^-]])$. We write $\alpha_{M/F}$ for the quadratic character of $\text{Gal}(\overline{F}/F)$ identifying $\text{Gal}(M/F)$ with $\{\pm 1\}$.

Lemma 4.2. *We have*

- (1) $\det(\text{Ind}_M^F \chi) = \alpha_{M/F} \chi|_{F^\times}$ and $\text{Tr}(\text{Ind}_M^F \chi(Frob_l)) = \sum_{\mathfrak{b} \subset O_M, N_{M/F}(\mathfrak{b})=l} \chi(\mathfrak{b})$ for a prime l of F unramified for $\text{Ind}_M^F \chi$, identifying a character χ of $\text{Gal}(\overline{F}/M)$ with a character of $M_{\mathbb{A}(\infty)}^\times/M^\times$ by the Artin symbol,
- (2) $\text{Ad}(\text{Ind}_M^F(\tilde{\varphi})) \cong \alpha_{M/F} \oplus \text{Ind}_M^F(\tilde{\varphi}^-)$ as $\mathfrak{G}_F$ -modules.

Since $\text{Ind}_M^F(\tilde{\varphi})|_{\mathfrak{G}_M} = \tilde{\varphi} \oplus \tilde{\varphi}_c$ with $\tilde{\varphi}_c(\sigma) = \tilde{\varphi}(c\sigma c^{-1})$, we define $\mathcal{F}_{\mathfrak{p}}^+ \text{Ind}_M^F \tilde{\varphi} = \tilde{\varphi}$ for $\mathfrak{p} \in \Sigma_p$. In Section 1, we have already defined $\mathcal{F}_{\mathfrak{p}}^\pm \text{Ad}(\text{Ind}_M^F \tilde{\varphi})$ and the Selmer group $\text{Sel}_F(\text{Ad}(\text{Ind}_M^F \tilde{\varphi}) \otimes_{\mathbb{Z}_p} (W[[\Gamma^-]])^*)$. Since the image of $\mathcal{F}_{\mathfrak{p}}^+(\text{Ad}(\text{Ind}_M^F \tilde{\varphi}))$ in $\alpha_{M/F}$ is trivial in the above decomposition in Lemma 4.2 and the image of $\mathcal{F}_{\mathfrak{p}}^+(\text{Ad}(\text{Ind}_M^F \tilde{\varphi}))$ is given by $\mathcal{F}_{\mathfrak{p}}^+(\text{Ind}_M^F(\tilde{\varphi}^-))$, we get (cf. [HMI] Exercise 1.12 and Corollary 3.81)

$$\begin{aligned} \text{Sel}_F(\text{Ad}(\text{Ind}_M^F(\tilde{\varphi}) \otimes_{W[[\Gamma^-]]} (W[[\Gamma^-]])^*)) \\ = \text{Sel}_F(\alpha_{M/F} \otimes_{\mathbb{Z}_p} (W[[\Gamma^-]])^*) \oplus \text{Sel}_F(\text{Ind}_M^F(\tilde{\varphi}^-) \otimes_{W[[\Gamma^-]]} (W[[\Gamma^-]])^*) \\ = \text{Hom}(Cl_M^- \otimes_{\mathbb{Z}} W[[\Gamma^-]], \mathbb{Q}_p/\mathbb{Z}_p) \oplus \text{Sel}_M((\tilde{\varphi}^-) \otimes_{W[[\Gamma^-]]} W[[\Gamma^-]]^*), \end{aligned}$$

where Cl_M^- is the quotient of CL_M by the image of Cl_F (the order of Cl_M^- is equal to the order of the $\alpha_{M/F}$ -eigenspace of Cl_M up to a power of 2). By the definition of the Selmer group, we note that

$$(4.1) \quad \text{Sel}_M(\tilde{\varphi}^- \otimes_{W[[\Gamma^-]]} (W[[\Gamma^-]])^*) \cong \text{Hom}(X^-[\varphi^-], \mathbb{Q}_p/\mathbb{Z}_p),$$

which shows

Theorem 4.3. *Let the notation be as above. Then we have*

$$\text{Sel}_F^*(\text{Ad}(\text{Ind}_M^F(\tilde{\varphi}))) \cong (Cl_M^- \otimes_{\mathbb{Z}} W[[\Gamma^-]]) \oplus X^-[\varphi^-]$$

as $W[[\Gamma^-]]$ -modules. Moreover $X^-[\varphi^-]$ is a torsion $W[[\Gamma^-]]$ -module without exceptional zero if $\psi := \varphi^-$ satisfies the following conditions:

- (at1) The character ψ has order prime to p .
- (at2) The local character $\psi_{\mathfrak{p}}$ is non-trivial for all $\mathfrak{p} \in \Sigma_p$.
- (at3) The restriction ψ^* of ψ to $\text{Gal}(\overline{F}/M^*)$ for the composite M^* of M and the unique quadratic extension inside $F[\mu_p]$ is non-trivial.

This theorem is general enough to cover $X^-[\psi]$ for any anticyclotomic character ψ since such a ψ can be written as φ^- for a suitable choice of φ (e.g., [HMI] Lemma 5.31).

The first assertion follows from the argument given as above. The torsion property follows from the theorem of Taylor–Wiles and Fujiwara and has been proven in [HMI] Theorem 5.33. The condition (at2) is probably removable by the recent result in [Ch] but in this note, we do not work it out.

4.3. The $\mathcal{L}$ -invariant of CM fields. Choose a character $\varphi : \mathfrak{G}_M \rightarrow W^\times$ associated to an arithmetic Hecke character of M so that $\rho_F = \text{Ind}_M^F \varphi$ satisfies (DS). Since φ is a character of $\mathfrak{G}_M$, it is unramified outside p . Consider the universal couple $(\mathcal{R}_F, \varrho)$ deforming $\rho_F = \text{Ind}_M^F \varphi \bmod \mathfrak{m}_W$ among W -deformations ρ_A into $GL_2(A)$ for proartinian W -algebras A with residue field $W/\mathfrak{m}_W$ satisfying the following conditions

- (W1) ρ_A factors through $\mathfrak{G}_F$;
- (W2) $\rho_A|_{\text{Gal}(\overline{\mathbb{Q}_p}/F_p)} \cong \begin{pmatrix} * & * \\ 0 & \alpha_{A,p} \end{pmatrix}$ with $\alpha_{A,p} \equiv \alpha_p \bmod \mathfrak{m}_A$ and $\alpha_{A,p} \alpha_p^{-1}|_{I_p}$ factoring through the local cyclotomic Galois group $\text{Gal}(F_p[\mu_{p^\infty}]/F_p)$;
- (W3) $\det(\rho_A) = \det \rho$;
- (W4) $\rho_A \equiv \overline{\rho} \bmod \mathfrak{m}_A$,

We know $\mathcal{R}_F \cong \mathbb{T}$ by Fujiwara (see [HMI] Theorem 3.59). Since $\dim \text{Spf}(W[[\Gamma^-]]) = \dim \text{Spf}(\mathbb{T})$, $\text{Spf}(W[[\Gamma^-]])$ gives an irreducible component of $\text{Spf}(\mathcal{R}_F)$. Write $\mathbb{I} = W[[\Gamma^-]]$ simply. Let $\pi_{\mathbb{I}} : \mathbb{T} = \mathcal{R}_F \rightarrow \mathbb{I}$ be the projection (which factors through π^{cyc}). We would like to compute the $\mathcal{L}$ -invariant of the component $\mathbb{I}$. Thus we need to compute $\mathbf{a}(p_{\mathfrak{p}}) = \pi_{\mathbb{I}}(U(p_{\mathfrak{p}}))$. The following fact follows from the fact $\text{Ind}_M^F \phi|_{\mathfrak{G}_M} = \phi \oplus \phi^c$.

Lemma 4.4. *Let the notation be as above. Then we have $\mathbf{a}(p_{\mathfrak{p}}) = \tilde{\varphi}([p, M_{\mathfrak{p}}])$ for the prime factor $\mathfrak{p} \in \Sigma_p^c$ of p .*

Define the character $\kappa : \text{Gal}(\overline{F}/M) \rightarrow (\Lambda^-)^\times$ by $\kappa(\sigma) = (\sigma|_{M_\infty^-})^{1/2}$. Then $\tilde{\varphi} = \lambda\kappa$, and we write $\kappa_{\mathbb{I}} = \pi_{\mathbb{I}} \circ \kappa : \text{Gal}(\overline{F}/M) \rightarrow \mathbb{I}^\times$. Then, $\kappa_{\mathbb{I}}$ restricted to the inertia group $I_{\mathfrak{p}}$ at $\mathfrak{p}$ factors through the projection: $I_{\mathfrak{p}} \rightarrow \text{Gal}(\mathbb{Q}_p[\mu_{p^\infty}]/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$. Since the $W[[\Gamma_F]]$ -algebra structure of $\mathbb{I}$ is induced by the nearly ordinary character of $\text{Ind}_M^F \kappa_{\mathbb{I}}$ (restricted to the inertia group $I_{\mathfrak{p}}$), for $u_{\mathfrak{p}} \in O_{M,\mathfrak{p}}^\times$ ($\mathfrak{p} \in \Sigma_p^c$), we have

$$(4.2) \quad \kappa_{\mathbb{I}}([u_{\mathfrak{p}}, M_{\mathfrak{p}}]) = (1 + X_p)^{d_p \log_p(N_p(u_{\mathfrak{p}}))/\log_p(\gamma_p)},$$

where $d_{\mathfrak{p}} = [F_{\mathfrak{p}} : \mathbb{Q}_p]$, $\mathfrak{p} = \mathfrak{P} \cap O$, $N_{\mathfrak{p}} : M_{\mathfrak{P}} = F_{\mathfrak{p}} \rightarrow \mathbb{Q}_p$ is the norm map and $\gamma_{\mathfrak{p}}$ is the generator of $\Gamma_{\mathfrak{p}} := (1 + p\mathbb{Z}_p) \cap N_{\mathfrak{p}}(O_{\mathfrak{p}}^{\times})$. The factor $d_{\mathfrak{p}}$ in the right-hand-side is missing from [H07a] (3.2), which comes from the fact that

$$[\gamma_{\mathfrak{p}}, F_{\mathfrak{p}}]_{\mathbb{Q}_p^{ab}} = [N_{F_{\mathfrak{p}}/\mathbb{Q}_p}(\gamma_{\mathfrak{p}}), \mathbb{Q}_p] = [\gamma_{\mathfrak{p}}, \mathbb{Q}_p]^{d_{\mathfrak{p}}}$$

because $\gamma_{\mathfrak{p}}$ is the image in $\mathbb{Q}_p$ under $\mathcal{N}$ of the generator of the Galois group of the cyclotomic $\mathbb{Z}_p$ -extension of $F_{\mathfrak{p}}$. Choose an element $\varpi(\mathfrak{P}) \in M$ so that $\mathfrak{P}^h = (\varpi(\mathfrak{P}))$ for each $\mathfrak{P} \in \Sigma_p^c$, where $h = |Cl_M|$ (the class number of M). Then $p_{\mathfrak{P}}^h = u_{\mathfrak{P}} \varpi(\mathfrak{P})_{\mathfrak{P}}^{e(\mathfrak{p})}$ with $u_{\mathfrak{P}} \in O_{M, \mathfrak{P}}^{\times}$ for the absolute ramification index $e(\mathfrak{p})$ of $\mathfrak{p}$ (which is the absolute ramification index of $\mathfrak{P}$ also). Regarding $\kappa_{\mathbb{I}}$ as a character of $M_{\mathbb{A}(\infty)}^{\times}/M^{\times}$ by class field theory, we have $\kappa_{\mathbb{I}}(\varpi(\mathfrak{P})) = 1 = \kappa_{\mathbb{I}}(\varpi(\mathfrak{P})_{\mathfrak{l}})$ with the $\mathfrak{l}$ -component $\varpi(\mathfrak{P})_{\mathfrak{l}} \in M_{\mathfrak{l}}^{\times}$ for any prime $\mathfrak{l}$ outside p , because $\kappa_{\mathbb{I}}(O_{\mathfrak{l}}^{\times}) = 1$ and $\varpi(\mathfrak{P}) \in M^{\times}$. Then we have

$$\kappa_{\mathbb{I}}(p_{\mathfrak{P}}^h) = \kappa_{\mathbb{I}}(p_{\mathfrak{P}}^h \varpi(\mathfrak{P})^{-e(\mathfrak{p})}) = \kappa_{\mathbb{I}}(u_{\mathfrak{P}}) \prod_{\mathfrak{P}' | p, \mathfrak{P}' \neq \mathfrak{P}} \kappa_{\mathbb{I}}(\varpi(\mathfrak{P})_{\mathfrak{P}'}^{-e(\mathfrak{p})}),$$

where $\varpi(\mathfrak{P})_{\mathfrak{P}'}$ is the $\mathfrak{P}'$ -component of $\varpi(\mathfrak{P}) \in M^{\times} \subset M_{\mathbb{A}}^{\times}$. By (4.2), we get

$$\kappa_{\mathbb{I}}(p_{\mathfrak{P}}^h) = (1 + X_{\mathfrak{p}})^{\frac{d_{\mathfrak{p}} \log_p(N_{\mathfrak{p}}(\varpi(\mathfrak{P})_{\mathfrak{p}}^{e(\mathfrak{p})} u_{\mathfrak{P}}))}{\log_p(\gamma_{\mathfrak{p}})}} \prod_{\mathfrak{P}' \in \Sigma_p^c - \{\mathfrak{P}\}} (1 + X_{\mathfrak{p}'})^{\frac{e(\mathfrak{p}) d_{\mathfrak{p}} \log_p(N_{\mathfrak{p}'}(\varpi(\mathfrak{P})_{\mathfrak{P}'}^{e(\mathfrak{p})}))}{\log_p(\gamma_{\mathfrak{p}'})}},$$

where $\mathfrak{p}' = \mathfrak{P}' \cap O$. Here $\log_p$ is the Iwasawa p -adic logarithm defined over $\overline{\mathbb{Q}_p}^{\times}$ characterized by $\log_p(p) = 0$. In particular, we have

$$\log_p(N_{\mathfrak{p}}(u_{\mathfrak{P}})) = \log_p(N_{\mathfrak{p}}(p_{\mathfrak{P}}^h \varpi(\mathfrak{P})_{\mathfrak{P}}^{-e(\mathfrak{p})})) = -e(\mathfrak{p}) \log_p(N_{\mathfrak{p}}(\varpi(\mathfrak{P})_{\mathfrak{P}})).$$

Thus we have

Lemma 4.5. *Let the notation be as above. Then we have, for primes $\mathfrak{P}' \in \Sigma_p$ and $\mathfrak{p}' = \mathfrak{P}' \cap O$,*

$$\frac{\partial \kappa(p_{\mathfrak{P}})}{\partial X_{\mathfrak{p}'}} = \frac{\log_p(N_{\mathfrak{p}'}(\varpi(\mathfrak{P})_{\mathfrak{P}'}^{(c-1)}))}{h \cdot f(\mathfrak{p}) \log_p(\gamma_{\mathfrak{p}'})} \kappa(p_{\mathfrak{p}}) (1 + X_{\mathfrak{p}'})^{-1}.$$

We have $\mathbf{a}(p_{\mathfrak{p}}) = c_{\mathfrak{p}} \kappa(p_{\mathfrak{p}})$ for a nonzero constant $c_{\mathfrak{p}} \in W^{\times}$, because the nearly ordinary character of $\text{Ind}_M^F \tilde{\varphi}$ is κ times a character of $D_{\mathfrak{P}}$ with values in $W^{\times}$. We do not need to pay much attention to the constant $c_{\mathfrak{p}}$, because the formula of the $\mathcal{L}$ -invariant only involve

$$\left(\prod_{\mathfrak{p}|p} \mathbf{a}(p_{\mathfrak{p}})^{-1} \delta_{\mathfrak{p}}([\gamma_{\mathfrak{p}}, F_{\mathfrak{p}}]) \right) \det \left(\left(\frac{\partial \mathbf{a}(p_{\mathfrak{p}})}{\partial X_{\mathfrak{p}'}} \right)_{\mathfrak{p}, \mathfrak{p}'} \right)$$

in which the constant $c_{\mathfrak{p}}$ cancels out. Specializing the above formula to the locally cyclotomic point P , we get

Theorem 4.6. *Let the notation and the assumption be as above and as in Theorem 4.3, including (at1–4). Then we have, for any specialization $\tilde{\varphi}_P$ of $\tilde{\varphi}$ modulo a locally cyclotomic point $P \in \text{Spf}(\mathbb{I})(W)$,*

$$\mathcal{L}(\text{Ad}(\text{Ind}_M^F \tilde{\varphi}_P)) = (-1)^e \det \left(\left(\log_p(N_{\mathfrak{p}'}(\varpi(\mathfrak{P})_{\mathfrak{P}'}^{(1-c)})) \right)_{\mathfrak{P}, \mathfrak{P}' \in \Sigma_p^c} \right) \prod_{\mathfrak{p}|p} \frac{1}{h \cdot f(\mathfrak{p})},$$

where $e = |\Sigma_p|$, $\mathfrak{p} = O \cap \mathfrak{P}$ and $\mathfrak{p}' = O \cap \mathfrak{P}'$.

Note here $\text{ord}_p(\varpi(\mathfrak{P})_{\mathfrak{P}'}^{(1-c)}) = -h/e(\mathfrak{p})$, taking the valuation ord_p associated to $\overline{\mathfrak{P}} \in \Sigma$. By Lemma 4.2 (2) and Theorem 4.3, we see

$$\mathcal{L}(\text{Ad}(\text{Ind}_M^F \tilde{\varphi}_P)) = \mathcal{L}(\alpha_{M/F}),$$

and this is the reason for the independence of $\mathcal{L}(\text{Ad}(\text{Ind}_M^F \tilde{\varphi}_P))$ on the choice of the locally cyclotomic points P . If $F = \mathbb{Q}$, we have $\varpi(\mathfrak{P})\varpi(\mathfrak{P})^c = p^h$ and hence $\log_p(\varpi(\mathfrak{P})) = -\log_p(\varpi(\mathfrak{P})^c)$. Thus $\log_p(\varpi(\mathfrak{P})^{1-c}) = 2\log_p(\varpi(\mathfrak{P}))$, and therefore the above formula coincides with the classical analytic $\mathcal{L}$ -invariant formula for $\alpha_{M/F}$ of Ferrero–Greenberg.

For a given ordinary CM type (M, Σ_p) , we can choose ψ satisfying the assumptions of Theorems 4.3 and 4.6. Then through the above process, we can compute $\mathcal{L}(\alpha_{M/F})$ as follows:

Corollary 4.7. *Suppose that M/F is an ordinary CM-quadratic extension of M satisfying (spt). Choose a p -ordinary CM-type Σ of M . Then the $\mathcal{L}$ -invariant $\mathcal{L}(\alpha_{M/F})$ of Greenberg for the quadratic Galois character $\alpha_{M/F} = \left(\frac{M/F}{\cdot}\right)$ is given by*

$$(-1)^e \det \left(\left(\log_p(N_{\mathfrak{p}'}(\varpi(\mathfrak{P})_{\mathfrak{p}'}^{(1-c)})) \right)_{\mathfrak{p}, \mathfrak{p}' \in \Sigma_p^c} \right) \prod_{\mathfrak{p}|p} \frac{1}{h \cdot f(\mathfrak{p})},$$

where h is the class number of M , $e = |\Sigma_p|$, $\mathfrak{p} = \mathfrak{P} \cap O$ and $\varpi(\mathfrak{P})$ is a generator of $\mathfrak{P} \in \Sigma_p^c$. If the prime p does not split in $F/\mathbb{Q}$, the $\mathcal{L}$ -invariant of $\alpha_{M/F}$ does not vanish.

A regulator similar to the above determinant was introduced long ago in [FeG] (3.8) in the context of (classical) cyclotomic Iwasawa’s theory.

Suppose that p does not split in $F/\mathbb{Q}$. Then for $\varpi = \varpi(\mathfrak{P})$, $N_{\mathfrak{P}}(\varpi) = \prod_{\sigma \in \Sigma} \varpi^\sigma = \varpi^\Sigma$. Then we have $|\varpi^\Sigma|_p = 1$ and $|\varpi^{c\Sigma}|_p < 1$ and hence $N_{\mathfrak{P}}(\varpi^{1-c})$ cannot be of the form ζp^α for $\alpha \in \mathbb{Q}$ and a root of unity ζ . Thus $\log_p(N_{\mathfrak{P}}(\varpi^{1-c})) \neq 0$ as claimed in the corollary. Of course, by Baker’s argument (exploited by Brumer in the p -adic case), if $M/\mathbb{Q}$ is abelian, we can also confirm the nonvanishing of the determinant in the corollary.

REFERENCES

Books

- [ACM] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1998.
- [BCM] N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961–83
- [CRT] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics **8**, Cambridge Univ. Press, 1986
- [HMI] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, Oxford University Press, 2006
- [MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, 2000, Cambridge University Press

Articles

- [B] D. Blasius, Hilbert modular forms and Ramanujan conjecture, in “Noncommutative Geometry and Number Theory” Aspects of Mathematics **E 37**, 35–56 Vieweg, Wiesbaden, 2006.
- [Ch] Lin Chen, Framed deformation of Galois representation, preprint, 2008
- [Ci] Craig Citro, $\mathcal{L}$ -Invariants of Adjoint Square Galois Representations Coming from Modular Forms, International Mathematics Research Notices, 2008 Volume 2008: article ID rnn048, 12 pages
- [D] M. Dimitrov, Galois representations modulo p and cohomology of Hilbert modular varieties, Ann. Sci. École Norm. Sup. **38**, (2005), 505–551
- [FeG] L. Federer and B. H. Gross, Regulators and Iwasawa Modules, Inventiones Math. **62** (1981), 443–457
- [FG] B. Ferrero and R. Greenberg, On the behavior of p -adic L -functions at $s = 0$, Inventiones Math. **50** (1978), 91–102.
- [Fu] K. Fujiwara, Deformation rings and Hecke algebras in totally real case, preprint, 1999 (arXiv.math.NT/0602606)
- [Fu1] K. Fujiwara, Galois deformations and arithmetic geometry of Shimura varieties, International congress of Mathematicians, vol. II, 347–371, Zürich: European Mathematical Society, 2006
- [G] R. Greenberg, Trivial zeros of p -adic L -functions, Contemporary Math. **165** (1994), 149–174
- [GS] R. Greenberg and G. Stevens, p -adic L -functions and p -adic periods of modular forms, Inventiones Math. **111** (1993), 407–447
- [GS1] R. Greenberg and G. Stevens, On the conjecture of Mazur, Tate, and Teitelbaum, Contemporary Math. **165** (1994), 183–211

- [GsK] B. H. Gross and N. Koblitz, Gauss sums and the p -adic Γ -function, *Ann. of Math.* **109** (1979), 569–581.
- [H88] H. Hida, Modules of congruence of Hecke algebras and L -functions associated with cusp forms, *Amer. J. Math.* **110** (1988) 323–382
- [H00] H. Hida, Adjoint Selmer groups as Iwasawa modules, *Israel Journal of Math.* **120** (2000), 361–427 (a preprint version available at www.math.ucla.edu/~hida)
- [H04] H. Hida, Greenberg’s $\mathcal{L}$ -invariants of adjoint square Galois representations, *International Mathematics Research Notices*, **59** (2004), 3177–3189 (a preprint version available at www.math.ucla.edu/~hida)
- [H07a] H. Hida, $\mathcal{L}$ -invariant of p -adic L -functions, in “The conference on L -functions” pp.17–53, 2007, World Scientific (a preprint version available at www.math.ucla.edu/~hida)
- [H07b] H. Hida, On a generalization of the conjecture of Mazur–Tate–Teitelbaum, *International Mathematics Research Notices*, **2007**, Article ID rnm102, 49 pages. doi:10.1093/imrn/rnm102 (reprint available at www.math.ucla.edu/~hida)
- [H08a] H. Hida, $\mathcal{L}$ -invariants of Tate curves, to appear in the Tate anniversary volume from *Pure and Applied Math Quarterly*, 2008 (available at www.math.ucla.edu/~hida)
- [H08b] H. Hida, $\mathcal{L}$ -invariant of the symmetric powers of Tate curves, preprint, 2007, to appear in *Publications of RIMS* (available at www.math.ucla.edu/~hida)
- [HT] H. Hida and J. Tilouine, Katz p -adic L -functions, congruence modules and deformation of Galois representations, *LMS Lecture notes* **153** (1991), 271–293.
- [HT1] H. Hida and J. Tilouine, Anticyclotomic Katz p -adic L -functions and congruence modules, *Ann. Sci. Ec. Norm. Sup. 4th series* **26** (1993), 189–259.
- [HT2] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fields, *Inventiones Math.* **117** (1994), 89–147.
- [K] N. M. Katz, p -adic L -functions for CM fields, *Inventiones Math.* **49** (1978), 199–297.
- [Ki] M. Kisin, Overconvergent modular forms and the Fontaine-Mazur conjecture, *Inventiones Math.* **153** (2003), 373–454
- [Ki1] M. Kisin, Geometric deformations of modular Galois representations, *Inventiones Math.* **157** (2004), 275–328
- [Ki2] M. Kisin, Moduli of finite flat group schemes, and modularity, to appear in *Ann. of Math.*
- [M] C.-P. Mok, Exceptional zero conjectures for Hilbert modular forms, preprint, 2007
- [MTT] B. Mazur, J. Tate and J. Teitelbaum, On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Inventiones Math.* **84** (1986), 1–48.
- [Ta] R. Taylor, Remarks on a conjecture of Fontaine and Mazur. *Journal of the Institute of Mathematics of Jussieu* **1** (2002), 1–19
- [Ta1] R. Taylor, On the meromorphic continuation of degree two L -functions, preprint, 2001.
- [Ta2] R. Taylor, Automorphy for some l -adic lifts of automorphic mod l Galois representations. II, preprint, 2006
- [TW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.
- [V] C. Virdol, Zeta functions of twisted quaternionic Shimura varieties, preprint (available at <http://www.math.columbia.edu/~virdol/research.html>)
- [W] A. Wiles, Modular elliptic curves and Fermat’s last theorem, *Ann. of Math.* **141** (1995), 443–551

DEPARTMENT OF MATHEMATICS, UCLA, LOS ANGELES, CA 90095-1555, U.S.A.

第Ⅱ部

若手研究発表会

平方和 2 次形式に関する極大格子の種の類数について

平岡 敬浩 *

2006 年 7 月 30 日

1 概要

n を正の有理整数とし、 $V = \mathbb{Q}_n^1$ を n 次元行ベクトル空間とする。非退化対称双 1 次形式 $\varphi: V \times V \rightarrow \mathbb{Q}$ をとり、 $\varphi[x] = \varphi(x, x)$ とおく。以後、 φ は正定値とする。 V の標準基底 $\{e_i\}_{i=1}^n$ を固定し、 φ と対称行列 $\varphi_0 = [\varphi(e_i, e_j)]_{1 \leq i, j \leq n}$ を同一視する。 φ の直交群 G^φ を

$$G^\varphi = \{\alpha \in GL_n(\mathbb{Q}) \mid \alpha \varphi^t \alpha = \varphi\}$$

とおく。 $v \in \{p: \text{素数}\} \cup \{\infty\}$ と V 内の格子 L に対し、

$$G_v^\varphi = \{\alpha_v \in GL_n(\mathbb{Q}_v) \mid \alpha_v \varphi \alpha_v = \varphi\}$$

$$G_{\mathbb{A}}^\varphi = \{(\alpha_v) \in \prod_{v \in \mathbf{v}} G_v^\varphi \mid \text{殆どすべての } p \text{ に対して } L_p \alpha_p = L_p \text{ を満足する}\}$$

とおく。次に、格子 L の類 $k(L)$ と種 $\Lambda(L)$ を以下で定義する。

$$k(L) = LG^\varphi = \{La \mid a \in G^\varphi\}, \quad \Lambda(L) = LG_{\mathbb{A}}^\varphi = \{La \mid a \in G_{\mathbb{A}}^\varphi\} \quad (1.1)$$

ここで La ($a \in G_{\mathbb{A}}^\varphi$) とは、 $L_p a_p = (La)_p$ を満足する V 内の格子とする。このとき、次の proposition が成り立つ。

Proposition 1.1. $\Lambda(L)$ に対して

$$\Lambda(L) = \bigsqcup_{i=1}^{k(n)} k(L^{(i)})$$

を満足する有限個の格子 $L^{(i)}$, $i = 1, \dots, k(n)$ が存在する。

$\Lambda(L)$ の中の類の個数 $k(n)$ を L の種の類数とよぶ。類数の有限性は Minkowski の対称行列の簡約理論による。

ここから、 L の φ に関する極大性を仮定する。即ち、 L は φ が L 上で値を $\mathbb{Z}$ にとるもの

*Department of Mathematical Sciences, Ritsumeikan University, Kusatsu, Shiga 525-8577, Japan. E-mail adress : rp043954@se.ritsumeikan.ac.jp

の中で極大であるとする。ここで、次の事実が知られている (cf. [Shimura97, Lemma 5.9], [Shimura97, Lemma 8.10])。

φ に関する極大格子全体から成る集合は 1 個の種をなす。

このことから、 L の種の類数は L のとり方によらないことがわかる。

次に種 $\Lambda(L)$ の不変量 $\mathfrak{m}(L)$ を定義し、Shimura's mass formula について述べる。

$$\mathfrak{m}(L) = \sum_{i=1}^{k(n)} \sharp \Gamma(L^{(i)})^{-1}, \quad \Gamma(L) = \{\gamma \in G^\varphi \mid L\gamma = L\}$$

とおく。 $\mathfrak{m}(L)$ を L の種の mass とよぶ。mass の歴史的背景については [Shimura 06] を参照していただきたい。

$$C = \{\alpha \in G_{\mathbb{A}}^\varphi \mid L\alpha = L\}, \quad C^+ = (G_+^\varphi)_{\mathbb{A}} \cap C, \\ \Gamma^a = aCa^{-1} \cap G \quad (a \in G_{\mathbb{A}}^\varphi), \quad \Gamma_+^a = G_+^\varphi \cap \Gamma^a,$$

$$\mathfrak{m}(G^\varphi, C) = \sum_{G^\varphi aC \in \mathcal{B}} [\Gamma^a : 1]^{-1}, \quad \mathfrak{m}(G_+^\varphi, C^+) = \sum_{G_+^\varphi aC^+ \in \mathcal{B}_+} [\Gamma_+^a : 1]^{-1}.$$

とおく。ここで、 $\mathcal{B}$ (resp. $\mathcal{B}_+$) は $G^\varphi \backslash G_{\mathbb{A}}^\varphi / C$ (resp. $G_+^\varphi \backslash (G_+^\varphi)_{\mathbb{A}} / C^+$) の完全代表系とする。全単射

$$G^\varphi \backslash G_{\mathbb{A}}^\varphi / C \ni G^\varphi aC \mapsto \mathfrak{k}(La^{-1}) \in \Lambda(L)/G^\varphi (= \{k(L^{(i)}) \mid 1 \leq i \leq k\}),$$

をとることにより、 $\mathfrak{m}(G^\varphi, C) = \mathfrak{m}(L)$ が示され、さらに、[Shimura 99a, Lemma 5.6(1)] によって $\mathfrak{m}(G^\varphi, C) = 2^{-1} \mathfrak{m}(G_+^\varphi, C^+)$ が得られる。

ここから、 φ は平方和とする。この場合に Shimura's mass formula を適用すると次のようになる。

Proposition 1.2.

$$\mathfrak{m}(G_+^\varphi, C^+) = \prod_{k=1}^m (4k)^{-1} |B_{2k}| \cdot \begin{cases} 2 & \text{if } n \pm 1 \in 8\mathbb{Z}, \\ 3^{-1}(2^m - 1) & \text{if } n \pm 3 \in 8\mathbb{Z}, \end{cases} \quad (1.2)$$

$$\mathfrak{m}(G_+^\varphi, C^+) = (2m)^{-1} |B_m| \prod_{k=1}^{m-1} \begin{cases} 2 & \text{if } n \in 8\mathbb{Z}, \\ 3^{-1}(2^m - 1)(2^{m-1} - 1) & \text{if } n - 4 \in 8\mathbb{Z}, \end{cases} \quad (1.3)$$

$$\mathfrak{m}(G_+^\varphi, C^+) = 2^{n-1} (m-1)! (2\pi)^{-m} L(m, \psi) \prod_{k=1}^{m-1} (4k)^{-1} |B_{2k}| \quad \text{if } n \pm 2 \in 8\mathbb{Z}. \quad (1.4)$$

ここで、 $m = [n/2]$ とし、 ψ は 4 を法とする原始的 *Dirichlet* 指標、 B_{2k} は $2k$ 番目の *Bernoulli* 数とする。

これから、類数に関する具体例をいくつか述べる。そこで後に必要となる古典的結果を述べておく。

Proposition 1.3.

$$k(n) = 1, \quad 1 \leq n \leq 9$$

$$k(n) = 2, \quad n = 10, 12, 15, 16.$$

$1 \leq n \leq 9$ の場合は、[Shimura 02, Lemma 1.6] にまとめられている。 $n = 10, 12, 15$ の場合は Conway-Sloane(1988 年), $n = 16$ の場合は Witt(1941 年) による。そこで、 $k(11), k(13), k(14)$ を決めるために、以下の $\mathbb{Z}_n^1$ を含む格子 L_n, M_n を与える。

$$L_n = \sum_{i=1}^n \mathbb{Z}\varepsilon_i, \quad M_n = \sum_{i=1}^n \mathbb{Z}\delta_i$$

$$\varepsilon_i = \begin{cases} e_i & \text{if } i \equiv 1, 2, 3, 5 \pmod{8}, \\ f_i = 2^{-1}(e_i + e_{i-1} + e_{i-2} + e_{i-3}) & \text{if } i \equiv 4, 6, 8 \pmod{8}, \\ g_i = 2^{-1}(e_i + e_{i-2} + e_{i-4} + e_{i-6}) & \text{if } i \equiv 7 \pmod{8}, \end{cases}$$

$$\delta_i = \begin{cases} e_i & \text{if } i \text{ is odd or } i = 2, \\ f_i = 2^{-1}(e_i + e_{i-1} + e_{i-2} + e_{i-3}) & \text{otherwise.} \end{cases}$$

L_n はすべての n で平方和 φ に関して極大で、 M_n は $n \not\equiv 0 \pmod{8}$ のとき極大になる。また、 $n \leq 6$ のとき、両者は一致する。さらに、以下の格子を与える。

$$N_{13} = M_{10} + \mathbb{Z}e_{11} + \mathbb{Z}e_{12} + \mathbb{Z}h_{13},$$

$$N_{14} = M_{12} + \mathbb{Z}e_{13} + \mathbb{Z}h_{14},$$

$$h_{13} = 2^{-1}(e_1 + e_3 + e_5 + e_7 + e_9 + e_{11} + e_{12} + e_{13}),$$

$$h_{14} = 2^{-1}(e_1 + e_3 + e_5 + e_7 + e_9 + e_{11} + e_{13} + e_{14}),$$

とする。このとき、類数および類代表は以下で与えられる。

Proposition 1.4.

$$k(11) = 3, \{L^{(i)}\} = \{L^{(1)} = L_{11}, L^{(2)} = M_{11}, L^{(3)} = L_7 \oplus L_4.\}$$

$$k(13) = 4, \{L^{(i)}\} = \{L_{13}, M_{13}, L_7 \oplus L_6, N_{13}\}.$$

$$k(14) = 4, \{L^{(i)}\} = \{L_{14}, M_{14}, L_7 \oplus L_7, N_{14}\}.$$

この proposition は Shimura's mass formula により種 $\Lambda(L)$ の mass を求め、一方で、mass の定義に従って、各代表の自己同型群の位数を計算し、一致を観ることで得られる。その際、 $\Gamma(N_{13}), \Gamma(N_{14})$ の位数が問題となる。そこで、 $\Gamma(N_{13}) \subset H_{13}, \Gamma(N_{14}) \subset H_{14}$ を満たす群 H_{13}, H_{14} をうまくとることで、指数 $[H_{13} : \Gamma(N_{13})], [H_{14} : \Gamma(N_{14})]$ を mass との関係から決定できる。他の代表の自己同型群の位数については先に述べた古典的結果および [Martinet 03, Lemma 1.4.6] を用いる。

参考文献

- [Conway 88a] J. H. Conway and N. J. A. Sloane, *Low dimensional lattices. I. Quadratic forms of small determinant.*, Proc. Roy. Soc. London Ser. A418(1988), no. 1854, 17-41.
- [Conway 88b] J. H. Conway and N. J. A. Sloane, *Low dimensional lattices. IV. The mass formula.*, Proc. Roy. Soc. London Ser. A419(1988), no. 1857, 259-286.
- [Martinet 03] J. Martinet, *Perfect Lattices in Euclidean space*, Springer-Verlag, 2003.
- [Shimura97] G. Shimura, *Euler Products and Eisenstein Series*, CBMS Regional Conference Series in Mathematics, No.93, Amer. Math., 1997.
- [Shimura 99a] G. Shimura, “An exact mass formula for orthogonal groups.” *Duke Math. J.* **97** (1999), 1-66.
- [Shimura 99b] G. Shimura, “The number of representations of an integer by a quadratic form.” *Duke Math. J.* **100** (1999), 59-92.
- [Shimura 02] G. Shimura, “The representation of an integers as sums of squares.” *Amer. J. Math.* **124** (2002), 1059-1081.
- [Shimura 06] G. Shimura, “Quadratic Diophantine equations, the class number, and the mass formula.” *Bulletin of the American mathematical society* **14** (2006).
- [Witt 41] E. Witt, “Eine Identität zwischen Modulformen zweiten Grades.” *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 323-337.

実2次体上の直交群に対する Shimura mass formula

村田 学*

概要

平方和に関する実2次体上の maximal lattice に対して Shimura mass formula を適用し, その genus の mass を計算すること, およびこの mass の応用例について述べる.

1 Shimura mass formula の適用

V を実2次体 F 上 n 次元の行 vector 空間 F^n とし, φ を n 次単位行列 1_n とする ($n > 1$). $x, y \in V$ に対して $\varphi(x, y) = x\varphi \cdot {}^t y = x \cdot {}^t y$, $\varphi[x] = \varphi(x, x) = x \cdot {}^t x$ とおく.

$$G = G_+^\varphi = \{\alpha \in SL_n(F) \mid \alpha\varphi \cdot {}^t \alpha = \varphi\}$$

とおく. V の $\mathfrak{g}$ -lattice L を1つとり, L の属す G に関する genus の class の代表系 $\{L_i\}_{i=1}^h$ を1組とる. ここで $\mathfrak{g}$ は F の整数環とし, $\mathfrak{g}$ -lattice は F 上 V を張る有限生成 $\mathfrak{g}$ -submodule の意味で用いる. (genus や class の定義については [S04, §9.3] を参照.) このとき,

$$\mathfrak{m}(L) = \sum_{i=1}^h [\Gamma_i : 1]^{-1}$$

とおく. ここで $\Gamma_i = \{\gamma \in G_+^\varphi \mid L_i\gamma = L_i\}$ である. これは代表系 $\{L_i\}_{i=1}^h$ のとり方に依らずに L の属す genus によって定まる. $\mathfrak{m}(L)$ を L の属す (G に関する) genus の mass という.

$$\tilde{L} = \{x \in V \mid 2\varphi(x, y) \in \mathfrak{g} \text{ for every } y \in L\}$$

とおく. $\tilde{L}$ は V における $\mathfrak{g}$ -lattice であり, L が $\varphi[L] \subset \mathfrak{g}$ をみたすならば, $L \subset \tilde{L}$ である. L_v を F の有限素点 v での L の局所化とし, $\mathfrak{e}$ を $\tilde{L}_v \neq L_v$ となる有限素点 v の積とする.

いま, L を φ に関する $\mathfrak{g}$ -maximal lattice とする, すなわち, $\varphi[L] \subset \mathfrak{g}$ をみたす $\mathfrak{g}$ -lattice の中で maximal なものとする. L の属す genus は φ に関する $\mathfrak{g}$ -maximal lattice 全体からなる集合と一致する (cf. [S04, §9.7]). このとき, Shimura mass formula [S99a, Theorem 5.8] を適用することにより, $\mathfrak{m}(L)$ は次のように与えることができる:

*本稿は2006年「整数論札幌夏の学校」若手研究発表会での講演内容をもとにして書かれたものです。北海道での滞在と講演の機会を与えてくださいました前田芳孝先生に感謝の意を表します。

Theorem 1.1. L を φ に関する $\mathfrak{g}$ -maximal lattice とするとき, L の属す genus の mass は,

$$\mathfrak{m}(L) = \mathfrak{m}_n(\mathfrak{g})[\tilde{L} : L]^\mu \prod_{v|\mathfrak{e}} \lambda_v$$

と与えられる. ここで, $\mathfrak{m}_n(\mathfrak{g})$ は次のように定義される:

$$\mathfrak{m}_n(\mathfrak{g}) = 2D_F^{[\mu^*]} \prod_{k=1}^{[\mu]} \{D_F^{1/2}((2k-1)!(2\pi)^{-2k})^2 \zeta_F(2k)\} \\ \cdot \begin{cases} 2^{-2\mu} & \text{if } n \text{ is odd,} \\ D_F^{1/2}((n/2-1)!(2\pi)^{-n/2})^2 L(n/2, \psi_{K/F}) & \text{if } n \text{ is even.} \end{cases}$$

$\mu = (n-1)/2$ とし, D_F は F の判別式である. n が偶数のとき $K = F(\sqrt{(-1)^{n/2}})$ とし, $\psi_{K/F}$ を K/F に対応する F の Hecke character とする. 但し, $K = F$ の場合は $\psi_{K/F} = 1$ と約束する. また, λ_v は F の有限素点 v における φ の Witt 分解に応じて定まる定数である.

本稿では, F の有限素点 v での局所体 F_v 上の φ の Witt 分解を, φ を適当な $GL_n(F_v)$ の元 α_v によって,

$$\alpha_v \varphi \cdot {}^t \alpha_v = \begin{bmatrix} 0 & 0 & 1_{r_v} \\ 0 & \theta_v & 0 \\ 1_{r_v} & 0 & 0 \end{bmatrix}$$

の形に変形した行列のこととして用いる. 但し θ_v は $\theta_v[x] = 0 \implies x = 0$ をみたす F_v 成分の対称行列とする. (Witt 分解については [S04, Lemma 1.3] を参照.) φ と v に対してこのような θ_v は一意ではないが, その size t_v は一意的に定まる. この t_v を v での φ の core dimension という. 任意の有限素点 v に対して $t_v \leq 4$ であることが知られている (cf. [S04, Theorem 7.6(ii)]).

Theorem 1.1 により, $\mathfrak{m}(L)$ を求めることは次の2つの議論に帰着できる:

1つは F の Dedekind zeta 関数と $F(\sqrt{-1})/F$ に対応する Hecke character に付随する L 関数の特殊値の計算である. これらは $F(\sqrt{-1})/\mathbf{Q}$ が Abel 拡大であるため, Riemann zeta 関数と Dirichlet L 関数の特殊値に帰着させて求めることができる.

もう1つは, $\tilde{L}_v \neq L_v$ となる F の有限素点 v をすべてを見つけることである. これによって Theorem 1.1 における $[\tilde{L} : L]$ と $\mathfrak{e}$ が定められる. 各素点 v での指数 $[\tilde{L}_v : L_v]$ は [S99a, (3.2.1)] を用いて計算できるが, そのためには 1_n の F_v 上 Witt 分解を決定する必要がある. この Witt 分解を実行するために, 各有理素数 p に対して 1_n の $\mathbf{Q}_p$ 上 Witt 分解を与え, $v|p$ となる素点 v に対して, その Witt 分解にあらわれた高々4次の対称行列 θ_p を F_v 上でさらに分解することを考える. このようにして Witt 分解が求められる要因の1つは, 考える2次形式を $\mathbf{Q}$ 成分の対称行列によって与えているところにあることを注意しておく. 一般に, $\mathbf{Q}$ 上の (非退化) 2次形式については, 各素数 p に対しその不変量を計算して, $\mathbf{Q}_p$ 上の Witt 分解を求めることができる (例えば, J.-P. Serre の「数論講義」の第3, 4章を参照).

Theorem 1.1 を適用して実際に mass をみるために、具体例として、 $F = \mathbf{Q}(\sqrt{5})$, $\varphi = 1_4$ の場合を計算してみる。 1_4 は 2 と無限素点 ∞ でのみ分岐する $\mathbf{Q}$ 上 quaternion algebra B_0 の norm form と同値である。すなわち、 β を B_0 の適当な $\mathbf{Q}$ 上の基底によって行列表示したものが 1_4 となる。従って β の $\mathbf{Q}_p$ 上 Witt 分解をみればよいが、一般に quaternion algebra の norm form の core dimension は、その algebra が素点 v で分岐するとき $t_v = 4$ であり、不分岐のとき $t_v = 0$ となる。故に φ の $\mathbf{Q}_p$ 上 Witt 分解は p での B_0 の分岐に依存して決まり、その core dimension は $p = 2$ で $t_2 = 4$ 、それ以外の p で $t_p = 0$ となる。いま、局所体上の quaternion algebra はその任意の 2 次拡大体上で分解することが知られている。 F において 2 は素 ideal だから、 $B = B_0 \otimes_{\mathbf{Q}} F$ は 2 で (algebra として) 分解し、結果的にすべての素点で B は不分岐となる。これは φ の core dimension がすべての素点 v で $t_v = 0$ であることを意味する。この事実 [S99a, (3.2.1)] を適用して、 $[\tilde{L}_v : L_v] = 1$ が任意の素点 v で成り立つ。従って $[\tilde{L} : L] = 1$ と $\mathfrak{e} = \mathfrak{g}$ がわかる。故に $\zeta_F(2) = \zeta(2)L(2, \chi)$ (χ は F の Dirichlet 指標) とあわせて、 φ に関する $\mathfrak{g}$ -maximal lattice L の mass は、

$$\mathfrak{m}(L) = \mathfrak{m}_4(\mathfrak{g}) = 2 \cdot 5^3 (2\pi)^{-8} \zeta_F(2)^2 = 2^{-5} \cdot 3^{-2} \cdot 5^{-2}$$

と計算できる。

この議論から、任意の実 2 次体 F の 2 を割る素点 v について、

$$\begin{aligned} B \otimes_F F_v &\cong (B_0 \otimes_{\mathbf{Q}} \mathbf{Q}_2) \otimes_{\mathbf{Q}} F_v \\ &\cong \begin{cases} B_0 \otimes_{\mathbf{Q}} \mathbf{Q}_2 & (2 \text{ が } F \text{ において分解するとき}), \\ M_2(F_v) & (2 \text{ が } F \text{ において分解しないとき}) \end{cases} \end{aligned}$$

が成り立つことがわかる。その他の素点 v については上述同様に $t_v = 0$ なので、これで任意の実 2 次体の各有限素点における 1_4 の Witt 分解とその core dimension が決定できた。

一般の 1_n の F_v 上 Witt 分解については [M, Lemma 3.3] にある。これと L 関数の特殊値の計算とをあわせて Theorem 1.1 をより具体的な形にまとめた公式は、[M, Theorem 3.6] で得ている。また $F = \mathbf{Q}$, $\varphi = 1_n$ の場合に、maximal lattice の属す genus に対して mass formula が適用された公式は、[S99a, Examples 5.16] において与えられている。

2 応用例

$\varphi = 1_4$, $F = \mathbf{Q}(\sqrt{5})$ のとき、具体的に計算された mass を利用して、maximal lattice L の属す genus の類数は 1 であることが確かめられる。(以下の詳細については [M, §4] を参照。)

実際、 $\varepsilon = (1 + \sqrt{5})/2$ として、 L を

$$L = \sum_{i=1}^4 \mathfrak{g} \alpha_i = \mathfrak{g}^4 \alpha, \quad \alpha = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/2 & (1 + \varepsilon)/2 & \varepsilon/2 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 \end{bmatrix}$$

とすると, これは $[\tilde{L} : L] = 1$ をみたすので φ に関する $\mathfrak{g}$ -maximal lattice である. このとき $\Gamma = \{\gamma \in G \mid L\gamma = L\}$ の位数は $2^5 \cdot 3^2 \cdot 5^2$ になることが計算によってわかる. 一方, $\mathfrak{m}(L) = 2^{-5} \cdot 3^{-2} \cdot 5^{-2}$ であったので, mass の定義から, L の属す genus は 1 つの類のみからなっていないわけではない.

この結果をさらに利用して, F の総正な整数 q を 4 つの平方和で表現する L の元の個数

$$N(L, q) = \#\{x \in L \mid x \cdot {}^t x = q\}$$

に対する公式が次のようにして求められる.

§1 のときと同様に $\{L_i\}_{i=1}^h$ を $\mathfrak{g}$ -lattice L の属す G に関する genus の class の 1 組の代表系として,

$$R(L, q) = \sum_{i=1}^h [\Gamma_i : 1]^{-1} N(L_i, q)$$

とおく. これは代表系 $\{L_i\}_{i=1}^h$ のとり方に依らない. L が φ に関する $\mathfrak{g}$ -maximal lattice であるとき, 志村五郎先生 (Princeton 大学) によって与えられた公式 [S99b, Theorem 1.5] をこの場合に適用することにより, $R(L, q)\mathfrak{m}(L)^{-1}$ を計算できる. とくに $\varphi = 1_4$, $F = \mathbf{Q}(\sqrt{5})$ の場合, 上の結果から $h = 1$ なので, これと公式 [S99b, Theorem 1.5(II)] の適用により,

$$\begin{aligned} N(L, q) &= \frac{R(L, q)}{\mathfrak{m}(L)} \\ &= 120 \cdot \prod_{\mathfrak{p} \mid q} \left(\sum_{i=0}^{e_{\mathfrak{p}}} N(\mathfrak{p})^i \right) \end{aligned}$$

を得ることができる. ここで $q\mathfrak{g} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ とする.

参考文献

- [M] M. Murata, *Shimura's mass formula for an orthogonal group over real quadratic fields*, Acta Arith. **121** (2006), 125–148.
- [S99a] G. Shimura, *An exact mass formula for orthogonal groups*, Duke Math. J. **99** (1999), 1–66.
- [S99b] G. Shimura, *The number of representations of an integer by a quadratic form*, Duke Math. J. **100** (1999), 59–92.
- [S04] G. Shimura, *Arithmetic and analytic theories of quadratic forms and Clifford groups*, Mathematical Surveys and Monographs, **109**, Amer. Math. Soc., Providence, RI, 2004.

4 元数体による乗法をもつアーベル曲面に伴うガロア表現の像について

東京大学大学院数理科学研究科 新井 啓介

1 序文

k を標数 0 の体とする。 G_k で k の絶対ガロア群を表す。 E を k 上の楕円曲線とし、 p を素数とする。 E の p 進 Tate 加群 $T_p E$ への G_k の作用が定める表現を

$$\rho_{E/k,p} : G_k \longrightarrow \text{Aut}(T_p E) \cong \text{GL}_2(\mathbb{Z}_p)$$

で表す。代数体（すなわち $\mathbb{Q}$ の有限次拡大）上の虚数乗法をもたない楕円曲線に伴うガロア表現の像について、次の定理が成り立つ。

定理 1.1 (*[S]*) K を代数体、 E を虚数乗法をもたない K 上の楕円曲線、 p を素数とする。このとき、 $\rho_{E/K,p} : G_K \longrightarrow \text{GL}_2(\mathbb{Z}_p)$ の像は開である。即ち、 K, E, p に依存した整数 $n = n(K, E, p) \geq 1$ が存在して、 $\rho_{E/K,p}(G_K) \supseteq 1 + p^n M_2(\mathbb{Z}_p)$ となる。

私は、定理 1.1 において、べき n が楕円曲線 E に依存しないようにとれることを示した。即ち、次の定理を証明した。

定理 1.2 (*[A]*) K を代数体、 p を素数とする。このとき、 K, p に依存した整数 $n = n(K, p) \geq 1$ が存在して、虚数乗法をもたない K 上の任意の楕円曲線 E に対して、 $\rho_{E/K,p}(G_K) \supseteq 1 + p^n M_2(\mathbb{Z}_p)$ が成り立つ。

注 1.3 定理 1.2 において、 $n(K, p)$ の K, p による具体的な評価は、有限個の j 不変量を除けば分かっている。

私は、上記のような現象が、楕円曲線の高次元化である 2 次元以上のアーベル多様体でも見られるか、ということを考えた。そして、楕円曲線と見かけ上同じガロア表現をもつ QM アーベル曲面に対して、定理 1.2 と同様の定理を示した。

2 主定理

B を $\mathbb{Q}$ 上の不定符号 4 元数体、 $d = \text{disc}(B)$ を B の判別式とする。 B の maximal order R をひとつとして固定する。 d を割らない素数 p に対して、 $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ において、同型 $R_p \cong M_2(\mathbb{Z}_p)$ を固定する。 k を標数 0 の体とする。

定義 2.1 k 上の (R による) QM アーベル曲面とは、 k 上のアーベル曲面 A と、環の単射準同型 (1 を id に送る) $i : R \hookrightarrow \text{End}_k(A)$ の組 (A, i) のことをいう。

(A, i) を k 上の QM アーベル曲面とする。同型

$$i : R \cong \text{End}_k(A) \cong \text{End}(A) \quad (2.1)$$

を仮定する。 d を割らない素数 p をとる。すると、 A の p 進 Tate 加群 $T_p A$ は R_p 加群として自由でランク 1 である。そして、ガロア表現

$$\rho_{(A,i)/k,p} : G_k \longrightarrow \text{Aut}_{R_p}(T_p A) \cong R_p^\times \cong \text{GL}_2(\mathbb{Z}_p)$$

が得られる。

QM アーベル曲面に伴うガロア表現の像についても、定理 1.1 と同様に、次のことが知られている。

定理 2.2 ($[O]$) K を代数体、 (A, i) を K 上の QM アーベル曲面で、同型 (2.1) を仮定する。 d を割らない素数 p をとる。すると、 $\rho_{(A,i)/K,p}(G_K) \subseteq \text{GL}_2(\mathbb{Z}_p)$ は開である。即ち、 $R, p, K, (A, i)$ に依存した整数 $n = n(R, p, K, (A, i)) \geq 1$ が存在して、 $\rho_{(A,i)/K,p}(G_K) \supseteq 1 + p^n M_2(\mathbb{Z}_p)$ を満たす。

私は、定理 2.2 において、べき n が QM アーベル曲面 (A, i) に依存しないようにとれることを示した。次が主定理である。

定理 2.3 K を代数体とし、 d を割らない素数 p をとる。すると、 R, p, K に依存した整数 $n = n(R, p, K) \geq 1$ が存在して、同型 (2.1) が成り立つような K 上の任意の QM アーベル曲面 (A, i) に対して、 $\rho_{(A,i)/K,p}(G_K) \supseteq 1 + p^n M_2(\mathbb{Z}_p)$ となる。

証明は、以下のようにしてなされる。 X^R を R による QM アーベル曲面のモジュライとする。これは $\mathbb{Q}$ 上の proper smooth curve である (Shimura curve と呼ばれている)。 X^R の種数 g^R が 2 以上のとき ($d \notin \{6, 10, 14, 15, 21, 22, 33, 34, 46\}$ のとき) は、Faltings により証明された Mordell 予想を用いて示される。 $g^R \leq 1$ のときは、QM アーベル曲面にあるレベル構造を入れてモジュライを考え、その種数が 2 以上を示すことにより、証明することができる。

参考文献

- [A] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, preprint.
- [O] M. Ohta, *On l -adic representations of Galois groups obtained from certain two-dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 21 (1974), 299–308.
- [S] J.-P. Serre, *Abelian l -adic representations and elliptic curves*, Lecture at McGill University, New York-Amsterdam, W. A. Benjamin Inc. (1968).

on the p -adic absolute CM-period symbol.

Tomokazu Kashio, joint work with Hiroyuki Yoshida.

G. Shimura は虚数乗法を持つ多様体の幾何的周期について研究しその値から CM-period symbol p_K を定義した. これは保型形式の CM-point での値などにも現れ重要な情報である. しかし代数的数倍のあいまい性を持つなど一般には扱うのが難しい. そこで H. Yoshida は多重 Γ 函数の特殊値を用いて absolute CM-period symbol $g_{K/F}$ を定義し, CM-period symbol の値と一致することを予想した. これは次のように定式化される. F は総実体, K は CM 体とし K/F がアーベル拡大とする. この時 $\tau \in G := \text{Gal}(K/F)$ に対して

$$(1) \quad p_K(id, \tau) \equiv g_{K/F}(id, \tau) := \pi^{-\mu(\tau)/2} \exp \left(\frac{1}{|G|} \sum_{\chi \in \hat{G}_-} \frac{\chi(\tau) X^{id}(\chi)}{L(0, \chi)} \right) \bmod \overline{\mathbf{Q}}^\times.$$

但し $\hat{G}_-$ は G の奇指標全体, $\tau = id, \rho$ (複素共役写像), その他に対し $\mu(\tau) := 1, -1, 0$ と定義した. 記号 $X(\chi)$ は多重 Γ 函数で定義され L 函数の $s = 0$ での微分値を $J_F := \{\sigma : F \hookrightarrow \overline{\mathbf{Q}}\}$ 方向へ分解したものである. これには新谷公式を用いて次のように表せる.

$$(2) \quad L(0, \chi) = \sum_{\sigma \in J_F} X^\sigma(\chi).$$

なお吉田予想は古典的には Chowla-Selberg 公式と一致する. 即ち虚二次体 K 及び対応する Dirichlet 指標 χ に対し

$$(3) \quad \pi p_K(id, id)^2 \equiv \exp \left(\frac{L'(0, \chi)}{L(0, \chi)} \right) \bmod \overline{\mathbf{Q}}^\times.$$

これらの研究は自然に p 進へ拡張される. 即ち p 進多重 Γ 函数を用いて (logarithmic) p -adic absolute CM-period symbol $lg_{p,K/F}$ を定義しその性質を調べた [Kashio, Yoshida]. 我々の第一の予想は次の様に定式化できる. K/F は吉田予想と同じとする. 代数体 L に p 進位相を入れる素イデアルを $\mathfrak{p}_L$ と書く事にする. $\mathfrak{p}_F$ が K/F で完全分解するとき

$$(4) \quad \frac{1}{2} \log_p \left(\left(\frac{\mathfrak{p}_K^\rho}{\mathfrak{p}_K} \right)^{\tau^{-1}} \right) \equiv lg_{p,K/F}(id, \tau) := \frac{-\mu(\tau)}{2} \log_p(\mathfrak{p}_F) + \frac{1}{|G|} \sum_{\chi \in \hat{G}_-} \frac{\chi(\tau) X_p^{id}(\chi_{\bullet_F})}{L(0, \chi)} \bmod \mathbf{Q} \log_p(E_F).$$

ただし指標 χ の法を $\mathfrak{f}$ とした時, 整イデアル $\mathfrak{a}$ に対して指標 $\chi_{\bullet}$ は法を $\mathfrak{f}\mathfrak{a}$ とするイデアル類群の指標と見なしたことを意味する. またイデアル $\mathfrak{a}$ に対して単項化 $\mathfrak{a}^h = (\alpha)$ を行い $\log_p(\mathfrak{a}) := \frac{1}{h} \log_p(\alpha)$ と定義する. E_F は F の単数群と置いた. 上と同様に記号 X_p は p 進多重 Γ 函数で定義され新谷公式の p 進類似から得られる. 即ち

$$(5) \quad L_p(0, \chi\omega) = \sum_{\sigma \in J_F} X_p^\sigma(\chi_{(p)}).$$

ただし ω は Teichmüller 指標 (とイデアルノルムの合成) である. 我々の第一予想は古典的には Gross-Koblitz 公式と一致している. 即ち虚二次体 K で p が分解するとき

$$(6) \quad \log_p \left(\frac{\mathfrak{p}_K^\rho}{\mathfrak{p}_K} \right) = \frac{L'_p(0, \chi\omega)}{L(0, \chi)}.$$

なお第一予想において $\mathfrak{p}_F$ の完全分解性は先頭項を観察することを意味する. 我々はこの条件なしでも次の第二予想を得た. こちらは非先頭項を扱っており吉田予想の p 進類似と呼ぶにふさわしい. p は K まで不分岐としておく. この時

$$(7) \quad \log_p \left(\frac{p_{p,K}(id, \tau)}{p_{p,K}(\text{Frob}_{\bullet_F}, \tau)^{\text{Frob}_p^{f_F}}} \right) \equiv lg_{p,K/F}(id, \tau) \pmod{\log_p(\overline{\mathbf{Q}}^\times)}.$$

ただし $p_{p,K}$ は CM-period symbol の p 進類似であり, crystalline cohomology と etale cohomology の比較同型から定義されるものである. この比較同型は B_{crys} と書かれる巨大な環を係数とし $p_{p,K}$ はここに値をとる. Frob_p は B_{crys} へ作用する絶対 Frobenius 作用であり, $f_\bullet$ は素イデアル $\mathfrak{p}$ の次数を表す事とする. $\text{Frob}_\bullet$ は Galois 群の元で素イデアル $\mathfrak{p}$ での Frobenius を表す. 次の式から第一予想は第二予想の特別な形である.

$$(8) \quad \log_p \left(\frac{p_{p,K}(id, \tau)}{p_{p,K}(id, \tau)^{\text{Frob}_p^{f_K}}} \right) = \frac{1}{2} \log_p \left(\left(\frac{\mathfrak{p}_K^\rho}{\mathfrak{p}_K} \right)^{\tau^{-1}} \right).$$

吉田予想及び我々の二つの予想は Stark 予想や Gross 予想 (L -invariant 予想の一部) の様な (p 進) L 関数の先頭項予想と深く関係する. 簡単な例を挙げてみよう. 吉田予想は $K = \mathbf{Q}(i, \sqrt{2})$, $F = \mathbf{Q}$ の時は $\pmod{\overline{\mathbf{Q}}^\times}$ で次を述べる.

$$(9) \quad \Gamma(1/8)\Gamma(7/8)^{-1} \equiv \pi^{3/4} p_K(id, id)^{3/2} p_K(id, \sigma_3)^{1/2}, \quad \Gamma(3/8)\Gamma(5/8)^{-1} \equiv \pi^{1/4} p_K(id, id)^{1/2} p_K(id, \sigma_3)^{3/2}.$$

ただし $\text{Gal}(K/F) = (\mathbf{Z}/8\mathbf{Z})^\times$, $\sigma_n \leftrightarrow n \pmod{8}$ と置いた. 一方で $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ に対する Stark 予想 (この場合は Euler's reflection formula) は

$$(10) \quad \Gamma(1/8)\Gamma(7/8) = \pi\sqrt{2 - \sqrt{2}}, \quad \Gamma(3/8)\Gamma(5/8) = \pi\sqrt{2 + \sqrt{2}}.$$

即ち二つの予想はそれぞれ Γ 関数の値の商と積を対象とし並行的である. さて同様の比較を p 進で行おう. $\mathbf{Q}(i)/\mathbf{Q}$ に対する我々の第一予想と Gross 予想は一致して次を述べる.

$$(11) \quad \log_p(\Gamma_p(1/4)) = 1/2 \log_p(2\pi_K^\rho), \text{ if } p = a^2 + b^2, |a + bi|_p < 1, \pi_K := a + bi.$$

(一般には我々の第一予想は Gross 予想より真に強い予想となっている.) また第二予想は次を言う.

$$(12) \quad \log_p(\Gamma_p(\frac{1}{4})) \equiv \frac{1}{2} \log_p \frac{p_{p,K}(id, id)}{p_{p,K}(\text{Frob}_p, id)^{\text{Frob}_p}} \pmod{\log_p(\overline{\mathbf{Q}}^\times)} \quad (p \neq 2).$$

更に零点の位数に関して Gross の予想は $r(\chi) := \{\mathfrak{p} | (p), \chi(\mathfrak{p}) = 1\}$ と置いた時 $\text{ord}_{s=0} L(s, \chi\omega) = r(\chi)$ であった. 実は p 進新谷公式による分解 (不変量 X_p) を用いてこの部分的解が得られる.

$$(13) \quad r(\chi) \geq 2 \text{ なら } \text{ord}_{s=0} L(s, \chi\omega) \geq 2$$

この様に, 特に p 進の場合には非先頭項に関する不変量 ($X_p, lg_{p,K}$) から先頭項予想に関する結果を導く事ができるのである.

我々の研究は高次の微分への拡張が期待される. これには新谷公式の高次微分への拡張が必要となり, 先頭項予想との関わりも予想される. 特に二階微分に関しては部分的な結果を得ることができた. 即ちある条件下で次のような分解を行える.

$$(14) \quad L''(0, \chi) = \sum_{\sigma, \sigma' \in J_F} X^{\sigma, \sigma'}(\chi) + \text{補正項}, \quad L''_p(0, \chi\omega) = \sum_{\sigma, \sigma' \in J_F} X_p^{\sigma, \sigma'}(\chi_{(p)}) + \text{補正項}.$$

ここで記号 $X^{\sigma, \sigma'}(\chi)$, $X_p^{\sigma, \sigma'}(\chi_{(p)})$ は (p 進) 多重 Γ 関数を拡張した函数の特殊値で定義される. これらはそれぞれが数論的に意味を持つと考えられ興味深い函数である. 特に Gross 予想は各 $X_p^{\sigma, \sigma'}$ 部分へ”分解”されるであろう.

(In)divisibility of special values of zeta functions associated to quadratic fields

木村 巖 (富山大学理学部数学科)

$\mathbf{Z}$ を有理整数環、 $\mathbf{Q}$ を有理数体とする．その代数閉包 $\overline{\mathbf{Q}}$ を複素数体の中に固定し、以下代数体といえば $\overline{\mathbf{Q}}$ の部分体とする． O_k を k の整数環とする．但し、2 次体 $k = \mathbf{Q}(\sqrt{D})$ については、簡単のため $O_D = O_k$ とする．自然数 n について、 ζ_n を $\overline{\mathbf{Q}}$ 内の 1 の原始 n 乗根の一つとする．有限次代数体 k の Dedekind ゼータ関数を $\zeta_k(s)$ と書く．集合 S の濃度を $\#S$ と表す．

n を自然数、 k を有限次代数体として、 $w_n(k)$ を、

$$w_n(k) := \max\{m \in \mathbf{Z}_{\geq 0} \mid \exp(\text{Gal}(k(\zeta_m)/k)) \mid n\},$$

ここで $\exp(G)$ は有限群 G の exponent, と定義する．

実または虚の 2 次体 $k = \mathbf{Q}(\sqrt{D})$ (対応する Kronecker 指標 $\chi_D(\cdot) = (D/\cdot)$) と自然数 n に対して、 $\xi_n(D)$ を次のように定義する：

$$\xi_n(D) := \begin{cases} w_n(\mathbf{Q}(\sqrt{D}))L(1-n, \chi_D), & D < 0, \\ w_n(\mathbf{Q}(\sqrt{D}))\zeta_{\mathbf{Q}(\sqrt{D})}(1-n), & D > 0, \end{cases}$$

ここで、 $L(s, \chi)$ は Dirichlet L 関数． $\xi_n(D) \neq 0$ であるのは、“ $D < 0$ かつ n が奇数” または “ $D > 0$ かつ n が偶数” のときのみである．

Coates-Sinnot [4] により、正の基本判別式 $D > 0$ に対して $\xi_n(D) \in \mathbf{Z}$ である．また、負の基本判別式 $D < 0$, $D \neq -1, -8$ に対しても、奇数 n に対して、Kolster [6] の高次類数公式が知られている：

$$|\xi_n(D)| = 4h_n^-(D). \quad (1)$$

右辺は、全ての素数 p に対しての $\#H^2(O_D[1/p], \mathbf{Z}_p(n))/\#H^1(O_D[1/p], \mathbf{Z}_p(n))$ の積である．

基本判別式 D について、 $B_{2,D}$ を Kronecker 記号 $(D/\cdot)$ に関する一般化 Bernoulli 数とすると、 $D > 5$ ならば

$$\xi_2(\mathbf{Q}(\sqrt{D})) = w_{\mathbf{Q}(\sqrt{D})}\zeta_{\mathbf{Q}(\sqrt{D})}(-1) = B_{2,D}.$$

数値計算の結果を見ると、次の疑問が湧く：

疑問. 勝手な奇素数 p について、 $p \mid \xi_2(\mathbf{Q}(\sqrt{D}))$ となる基本判別式 $D > 0$ は無数に存在するか？

同じ記号で、 $p \nmid \xi_2(\mathbf{Q}(\sqrt{D}))$ となる $D > 0$ が無数に存在することは、Byeon [3] により示されている。

$\xi_2(\mathbf{Q}(\sqrt{D}))$ の値と、 O_D の代数的 K 群 $K_2(O_D)$ の位数との関係が、Mazur-Wiles [8] により示されている： $\xi_2(F) \sim_p \#K_2(O_F)$ 。但し、勝手な $a, b \in \mathbf{Q}$ と素数 p について、 $a \sim_p b$ は a/b が p 進単数であることとする。

$p = 3, 5$ については、上の疑問に、肯定的に答えることができる：

定理.

$$\#\{0 < D < X \mid 3 \mid \#K_2(O_D)\} \gg X^{\frac{7}{8}-\varepsilon}.$$

証明には、Browkin [1] 他による、「 $3 \mid \#K_2(O_D)$ が、 $3 \mid h(\mathbf{Q}(\sqrt{-3D}))$ または $D \equiv 6 \pmod{9}$ と同値」という事実と、Soundararajan [9] による、類数が 3 で割り切れる虚 2 次体の個数の評価を用いる。

定理. $\{\mathbf{Q}(\sqrt{D}) \mid 5 \mid \#K_2(O_D)\}$ は無限集合。

証明には、Lu [7] による、一般化 Bernoulli 数と 2 次体の類数との間の合同と、Yamamoto [10] の結果を用いる。

非可除性については、Bruinier [2] の次の結果がある：奇素数 p が、 $(p-1) \nmid 2n$ かつ $v_p(\zeta(1-2n)) = 0$ なら ($v_p(\cdot)$ は p 進加法付値)、基本判別式 $D > 0$ で、 $v_p(L(1-n, \chi_D)) = 0$ となるものが無数に存在する。虚 2 次体の場合も、同様の主張が成立する。

$\xi_n(D)$ は、 O_D のコホモロジー群 $H_{\text{ét}}^2(O_D[1/p], \mathbf{Z}_p(n))$ の位数と同じ p 進付値を持つことが知られている (Lichtenbaum 予想の étale 版、Mazur-Wiles [loc. cit.])。また、代数的 K 群 $K_{2n-2}(O_D)$ の p 部分の位数と等しいことも予想されている (Quillen-Lichtenbaum 予想)。

類数の (非) 可除性に関する Cohen-Lenstra 予想 [5] の類似を、この場合に考えることは興味ある問題である。

参考文献

- [1] Jerzy Browkin, *On the divisibility by 3 of $\#K_2O_F$ for real quadratic fields F* , Demonstratio Math. **18** (1985), no. 1, 153–159. MR 87c:11115
- [2] Jan Hendrik Bruinier, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), no. 3, 595–611. MR 2000d:11061

- [3] Dongho Byeon, *Indivisibility of special values of Dedekind zeta functions of real quadratic fields*, Acta Arith. **109** (2003), no. 3, 231–235. MR 1 980 259
- [4] J. Coates and W. Sinnott, *Integrality properties of the values of partial zeta functions*, Proc. London Math. Soc. (3) **34** (1977), no. 2, 365–384. MR MR0439815 (55 #12697)
- [5] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Springer, Berlin, 1984, pp. 33–62. MR 85j:11144
- [6] Manfred Kolster, *Higher relative class number formulae*, Math. Ann. **323** (2002), no. 4, 667–692. MR 2003i:11168
- [7] Hong Wen Lu, *Congruences for the class number of quadratic fields*, Abh. Math. Sem. Univ. Hamburg **52** (1982), 254–258. MR 85b:11096
- [8] B. Mazur and A. Wiles, *Class fields of abelian extensions of $\mathbf{Q}$* , Invent. Math. **76** (1984), no. 2, 179–330. MR 85m:11069
- [9] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690. MR 2001i:11128
- [10] Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76. MR 42 #1800

Siegel modular form of degree 2 and Abelian variety.

岡崎 武生

大阪大学大学院理学研究科

1 吉田予想と吉田リフト.

[志村-谷山予想] 全ての $\mathbb{Q}$ 上定義された楕円曲線 E に対して, 次の条件を満たす重さ 2 の楕円保型形式 f が存在する.

- $L(s, E) = L(s, f)$.
- E の conductor と f の level は一致する. □

この予想の根拠となった Eichler-Shimura 理論がありました.

[Eichler-Shimura 理論] $f = \sum_{n \in \mathbb{Z}_{>0}} a_n \exp(2\pi i n z)$ を重さ 2 の Hecke eigen cuspform とする. このとき,

- $\mathbb{Q}_f := \mathbb{Q}\langle a_n \mid n \in \mathbb{N} \rangle$ は有限次代数体である.
- $[\mathbb{Q}_f : \mathbb{Q}]$ 次元 Abel 多様体 A_f で $L(s, H^1(A_f, \mathbb{Q}_l)) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}_f/\mathbb{Q})} L(s, f^\sigma)$ となるものが存在する.

特に $\mathbb{Q}_f = \mathbb{Q}$ のときは A_f は楕円曲線である. □

さて, 志村-谷山予想の 2 次元版として, 京都大学の吉田敬之先生により

吉田予想 *root number = 1* をもつ $\mathbb{Q}$ 上定義された, 全ての *simple* な Abel 曲面 A に対して, $L(s, H^1(A, \mathbb{Q}_l)) = L(s, F, \text{spin})$, *up to finitely many bad primes* となる次数, 重さ 2 の Siegel 保型形式 F が存在する. □

と予想されました. この予想の根拠となったのが, 吉田リフトと呼ばれる Siegel 保型形式の構成法でした. その吉田リフトには次の 2 タイプがあります.

(I) 楕円保型形式の pair から構成:

$$S_2^{(1)}(\Gamma_0(p))^2 \ni f_1, f_2 \longmapsto Y_{f_1, f_2}^2 \in M_2^2(\Gamma_0(p)), \quad L(s, Y_{f_1, f_2}, \text{spin}) = L(s, f_1)L(s, f_2).$$

(II) 2 次体 $K = \mathbb{Q}(\sqrt{N})$ の Hilbert 保型形式から構成:

$$S_2(\Gamma_K) \ni f \longmapsto Y_f^2 \in M_2^2(\Gamma_0(N), \chi_N), \quad L(s, Y_f, \text{spin}) = L(s, f).$$

$$\Gamma_K = \begin{pmatrix} * & \sqrt{N^{-1}}* \\ \sqrt{N}* & * \end{pmatrix}, \quad * \in \mathfrak{o}_K.$$

吉田先生は, この type (I) の吉田リフトと, Eichler-Shimura 理論で得られる Abel 曲面とを用いて, 吉田予想の成立している Siegel 保型形式と Abel 曲面の pair の example を与えました. しかし, この吉田リフトには,

Yoshida's non-vanishing problem この吉田リフトはいつでも有効な構成法なのか？消えている事はないのか？

という問題がありました。この問題に対して、

Böcherer and Schulze-Pillot's result (1992) type (I) の吉田リフトは消えない。 $\square$

という事が証明されました。この定理により、我々は楕円保型形式 (trivial central character) から得られる Abel 曲面に対しては吉田予想が成立している事がわかります。

一方、東京大学の織田孝幸先生の予想 (1982) や Brylinski-Labesse (1984) の結果などより、次の事を予想するのは自然と思われます。

Conjecture 1 K を実 2 次体, ρ を $\text{Gal}(K/\mathbb{Q})$ の生成元とする. 重さ 2 の Hilbert eigen cuspform $f(z_1, z_2) = \sum_{\mathbf{n} \in \mathfrak{o}_K} a_{\mathbf{n}} \exp(2\pi i(N(\mathbf{n})z_1 + N(\mathbf{n})^\rho z_2))$ に対して, K 上定義された以下の条件をみたす Abel 多様体 A_f が存在する.

- $L(s, H^1(A_f, \mathbb{Q}_l)) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}_f/\mathbb{Q})} L(s, f^\sigma).$

- $\text{End}_{\mathbb{Q}}(A_f) \supset \mathbb{Q}_f.$ $\square$

REMARK 1 $\text{End}_{\mathbb{Q}}(A_f) \supset K$ ではない事に注意. 織田予想は一般次数の *totally real field* 上の Hilbert 保型形式に対してされている.

この Conjecture 1 を仮定すれば, 特に Hilbert 保型形式 f から, 次のタイプの Abel 曲面/ $\mathbb{Q}$ が得られます.

- i). 楕円曲線 E_f/K の Weil restriction $\text{Res}_{K/\mathbb{Q}} E_f.$
- ii). $S_2^{(1)}(\Gamma_0(N), \chi_N)$ から得られる Abel 曲面. (これは予想を仮定する必要はない. E-S.)
- iii). $[\mathbb{Q}_f : \mathbb{Q}] = 2$ で, ‘本当は’ $\mathbb{Q}$ 上定義されている Abel 曲面 $A_f.$

(genus 2 の hyper-elliptic curve $C : y^2 = x^5 + a$, ($a \in \mathbb{Q}^\times$) の Jacobian などは高い conductor を持つので full-modular 保型形式に対応しないが, 3 の例と考えられる.)

そこで次に吉田予想に更に根拠を与える為の自然な問題として, 吉田リフト type (II) は消えないか？を考えました.

2 主結果.

上の問題について次の答えが与えられます. $p|N$ に対して local Fircke involution を

$$i_p : S_2(\Gamma_K) \ni f(z_1, z_2) \longmapsto f\left(\frac{z_1}{p}, \frac{z_2}{p}\right) \in S_2(\Gamma_K)$$

で定義する. $i_p(f) = \pm f$ である.

Main Theorem 1 f が $i_p, p|N$ に関する eigen value が全て 1 ならば,

- 吉田リフト type (II) の像 Y_f は消えない.
- Y_f の Fourier 係数は $\mathbb{Q}_f$ に含まれる.

- f が *Doi-Naganuma lift of nebentypus* で得られるなら, Y_f は *cusppform* では無い.

$$S_2^{(1)}(\Gamma_K)^\vee \xrightarrow{Y} S_2^{(2)}(\Gamma_0(N), \chi_N), \\ S_2^{(1)}(\Gamma_0(N), \chi_N) \xrightarrow{DN} S_2(\Gamma_K)^N \xrightarrow{Y} N_2^{(2)}(\Gamma_0(N), \chi_N) \xrightarrow{\Phi} S_2^{(1)}(\Gamma_0(N), \chi_N).$$

$S_2(\Gamma_K)$ における *D-N lift* の像を $S_2(\Gamma_K)^N$ であらわし, 直交補空間を $S_2(\Gamma_K)^\vee$ としている. 下段最右の *map* は *Siegel* 作用素. $N_2^{(2)}$ は *Siegel non-cusppform* の空間. $g \in S_2^{(1)}(\Gamma_0(N), \chi_N)$ から出発して最後まで行き着く事が常に出来, $\Phi \circ Y \circ DN(g) = g + \bar{g}$ になっている. $\square$

更に,

Main Theorem 2 上定理では, $f \in S_2(\Gamma_K)^N$ の吉田リフトの像 Y_f は *non-cusppform* であったが, f が *Grössencharacter* でかけるなら, Y_f と同じ *spinor L-関数* をもつ *cusppform* F^C が存在する. $\square$

こういった現象の explicit な表示として, [4] に『 $y^2 = x^5 - x$ に対応した *Siegel cusppform* が存在し *Igusa-theta* の 4 積の形をしている.』という結果があります. なお, $y^2 = x^5 - x$ は $E : y^2 = x(x-1)(x-1-\sqrt{2})$ の *Weil restriction* なので $\mathbb{C}$ -simple ではない.

さて, 吉田予想と (拡張された) 織田予想を仮定すると *Siegel* 保型形式の standard L -関数に関する *Kudla-Rallis-Soudry* 結果 (1993) より, *Abel* 曲面の *Hasse-Weil* 関数の 2 次元 part の本質的な部分 $L'(s, H^2(A, \mathbb{Q}_l)) := \zeta(s-1)^{-2} L(s, H^2(A, \mathbb{Q}_l))$ に関して次の事が言えます.

$A/\mathbb{Q}$ が simple かつ root number = 1 ならば, $\text{ord}_{s=2} L(s, H^2(A, \mathbb{Q}_l)) \geq -1$ で

1. $\text{End}_{\mathbb{Q}}(A) = \mathbb{Q} \Rightarrow \text{ord}_{s=2} L(s, H^2(A, \mathbb{Q}_l)) > 0$.
2. $\text{ord}_{s=2} L(s, H^2(A, \mathbb{Q}_l)) = 0 \Rightarrow L(s, H^1(A, \mathbb{Q}_l))$ と同じ L -関数を持つ楕円保型形式の pair が *Hilbert* 保型形式 (虚 2 次体上も含む) が存在する.
3. $\text{ord}_{s=2} L(s, H^2(A, \mathbb{Q}_l)) = -1 \iff A$ は $S_2^{(1)}(\Gamma_0(N), \chi_N)$ から得られる *Abel* 曲面.

従って, 興味深い問題として, 『 $\text{End}_{\mathbb{Q}}(A) \neq \mathbb{Q}$ ならば, *Shimura curve* の *Jacobian* か 2 次体上の *Hilbert* 保型形式の motive と isogeneous か?』という問題が考えられます.

参考文献

- [1] Böcherer, S and Schulze-Pillot, R: *Siegel modular forms and theta series attached to quaternion algebras*, Nagoya Math. J. **121** (1991), 35-96. II, **147** (1997), 71-106.
- [2] S. Kudla, S. Rallis and D. Soudry: On the degree 5 L -function for $Sp(2)$, Invent. math. **107** (1992), 483-541.
- [3] Oda, T: Periods of Hilbert surfaces. Progress in math. **19**, Birkhäuser, (1982).
- [4] Okazaki, T: Proof of R. Salvati Manni and J. Top's conjectures on *Siegel* modular forms and *Abelian* surfaces, Amer. J. Math. **128**, (2006) 139-165.
- [5] Yoshida, H: *Siegel's* modular forms and the arithmetics of quadratic forms, Invent. math. **60** (1980), 193-248.

Certain Dirichlet series of Rankin-Selberg type associated with the Ikeda lifting ^{*†}

Hisa-aki Kawamura (Hokkaido University)

For any $n \in \mathbb{Z}_{>0}$, let $\mathfrak{H}_n$ be the Siegel upper-half space of degree n , that is,

$$\mathfrak{H}_n := \{ Z = X + \sqrt{-1} Y \in M_n(\mathbb{C}) \mid {}^t Z = Z, Y > 0 \text{ (positive definite)} \}.$$

For any $k \in \mathbb{Z}_{>0}$, let $S_k(\mathrm{Sp}_n(\mathbb{Z}))$ be the $\mathbb{C}$ -vector space consisting of all Siegel cusp forms of weight k with respect to the Siegel modular group

$$\mathrm{Sp}_n(\mathbb{Z}) = \left\{ \gamma \in \mathrm{GL}_{2n}(\mathbb{Z}) \mid {}^t \gamma \begin{pmatrix} \mathbf{0}_n & \mathbf{1}_n \\ -\mathbf{1}_n & \mathbf{0}_n \end{pmatrix} \gamma = \begin{pmatrix} \mathbf{0}_n & \mathbf{1}_n \\ -\mathbf{1}_n & \mathbf{0}_n \end{pmatrix} \right\}$$

of degree n . If $n > 1$, then for any $F \in S_k(\mathrm{Sp}_n(\mathbb{Z}))$, we can consider the so-called Fourier-Jacobi expansion

$$F\left(\begin{pmatrix} \tau' & z \\ {}^t z & \tau \end{pmatrix}\right) = \sum_{N=0}^{\infty} \phi_N(\tau, z) \exp(2\pi\sqrt{-1}N\tau'),$$

where $\tau \in \mathfrak{H}_{n-1}$, $z \in \mathbb{C}^{n-1}$ and $\tau' \in \mathfrak{H}_1$. Here we note that for each $N \in \mathbb{Z}_{>0}$, the N -th coefficient $\phi_N(\tau, z)$ is an element of the $\mathbb{C}$ -vector space $J_{k,N}^{\mathrm{cusp}}(\mathrm{Sp}_{n-1}(\mathbb{Z})^J)$ consisting of all holomorphic Jacobi cusp forms of weight k and index N with respect to the Jacobi modular group $\mathrm{Sp}_{n-1}(\mathbb{Z})^J = \mathrm{Sp}_{n-1}(\mathbb{Z}) \ltimes (\mathbb{Z}^{2n-2} \times \mathbb{Z})$ of degree $n-1$. Then we define a certain Dirichlet series of Rankin-Selberg type associated with F by

$$D_1(s; F) := \zeta(2s - 2k + 2n) \sum_{N=1}^{\infty} \langle \phi_N, \phi_N \rangle N^{-s} \quad (s \in \mathbb{C})$$

where $\zeta(s)$ is the Riemann ζ -function and we denote by $\langle *, * \rangle$ the Petersson inner product defined on the space $J_{k,N}^{\mathrm{cusp}}(\mathrm{Sp}_{n-1}(\mathbb{Z})^J)$. It can be viewed as a generalization of the Rankin-Selberg convolution series for elliptic cusp forms. Furthermore, T. Yamazaki ([Yam]) proved by using the Rankin-Selberg method with a certain non-holomorphic Eisenstein series of Klingen-Siegel type that $D_1(s; F)$ has the following analytic properties:

Fact 1 (cf. Theorems 3.4, 3.5 in [Yam]). (i) *The Dirichlet series $D_1(s; F)$ has a meromorphic continuation to the entire complex plane $\mathbb{C}$. More precisely, the function*

$$\mathbf{D}_1(s; F) := \pi^{k-n} (2\pi)^{-2s} \Gamma(s) \Gamma(s - k + n) D_1(s; F) \tag{1}$$

is holomorphic on $\mathbb{C}$ except for simple poles at $s = k$ and $s = k - n$ of same residue $\langle F, F \rangle$, where we denote by $\langle *, * \rangle$ the Petersson inner product defined on the space $S_k(\mathrm{Sp}_n(\mathbb{Z}))$.

(ii) *It satisfies a functional equation*

$$\mathbf{D}_1(s; F) = \mathbf{D}_1(2k - n - s; F).$$

^{*}This manuscript is based on the talk at the Summer School on Number Theory at Sapporo in 2006.

[†]This is a joint work with Professor Hidenori Katsurada at Muroran Institute of Technology.

On the other hand, let $n, k \in \mathbb{Z}_{>0}$ be both even satisfying that $k > n + 1$. Then we can consider the so-called Ikeda lifting of elliptic cusp forms:

Fact 2 (cf. Theorems 3.2, 3.3 in [Ike1]). *If $f \in S_{2k-n}(\mathrm{SL}_2(\mathbb{Z}))$ is a normalized Hecke eigenform, then there exists a Hecke eigenform $I_n(f) \in S_k(\mathrm{Sp}_n(\mathbb{Z}))$ whose standard L -function is equal to*

$$\zeta(s) \prod_{i=1}^n L(s + k - i, f),$$

where $L(s, f)$ is the Hecke L -function associated with f . In particular, if $n = 2$, then $I_2(f)$ coincides with the Saito-Kurokawa lifting of f .

Remark. Moreover, let $S_{k-(n-1)/2}^+(\Gamma_0^{(1)}(4))$ be the Kohnen's plus subspace of elliptic cusp forms of half-integral weight $k - (n - 1)/2$ with respect to the congruence subgroup

$$\Gamma_0^{(1)}(4) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{4} \right\}$$

of $\mathrm{SL}_2(\mathbb{Z})$, then the above $I_n(f)$ can be explicitly constructed by a Hecke eigenform $\tilde{f} \in S_{k-(n-1)/2}^+(\Gamma_0^{(1)}(4))$ corresponding to f under the Shimura correspondence (cf. [Koh]).

Then we obtain the following explicit formula for the Dirichlet series $D_1(s; I_n(f))$:

Theorem 1 (cf. [K-K1]). *If $f \in S_{2k-n}(\Gamma_1)$ is a normalized Hecke eigenform, then*

$$D_1(s; I_n(f)) = \langle \phi_1, \phi_1 \rangle \zeta(s - k + 1) \zeta(s - k + n) L(s, f), \quad (2)$$

where $\phi_1 \in J_{k,1}^{\mathrm{cusp}}(\mathrm{Sp}_{n-1}(\mathbb{Z})^J)$ is the first Fourier-Jacobi coefficient of $I_n(f)$.

Remark. We denote the usual gamma factors of $\zeta(s)$ and $L(s, f)$ by $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2} \Gamma(s/2)$ and $\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s} \Gamma(s)$, respectively. Then we easily see that the gamma factor in (1) is equal to a constant multiple of

$$\prod_{i=0}^{n/2-1} (s - k + 2i + 1) \Gamma_{\mathbb{R}}(s - k + 1) \Gamma_{\mathbb{R}}(s - k + n) \Gamma_{\mathbb{C}}(s),$$

and therefore the equation (2) agrees with the properties (i) and (ii) in Fact 1.

Furthermore, by comparing residues at $s = k$ on the both sides of (2), we also obtain

Corollary 1. *Under the same assumption as above, we have*

$$\frac{2^{2k} \pi^{k+n}}{(k-1)!(n-1)!} \cdot \frac{\langle I_n(f), I_n(f) \rangle}{\langle \phi_1, \phi_1 \rangle} = L(k, f) \zeta(n). \quad (3)$$

Remark. The equations (2) and (3) are generalizations of the well-known results for the Saito-Kurokawa lifting $I_2(f)$, which are obtained by W. Kohnen and N.-P. Skoruppa ([K-S]) (See also [Oda]).

Here we shall recall that the space $J_{k,1}^{\text{cusp}}(\text{Sp}_{n-1}(\mathbb{Z})^J)$ is isomorphic to a certain subspace of the $\mathbb{C}$ -vector space $S_{k-1/2}(\Gamma_0^{(n-1)}(4))$ consisting of all Siegel cusp forms of half-integral weight $k - 1/2$ with respect to the congruence subgroup

$$\Gamma_0^{(n-1)}(4) := \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{Sp}_{n-1}(\mathbb{Z}) \mid C \equiv \mathbf{0}_{n-1} \pmod{4} \right\}$$

of $\text{Sp}_{n-1}(\mathbb{Z})$. Namely, as is known by W. Kohnen, M. Eichler and D. Zagier ([E-Z]) in case $n = 1$ and by T. Ibukiyama for general n , we have

Fact 3 (cf. Theorems 1, 2 in [Ibu]). *For any $1 < n \in \mathbb{Z}_{>0}$ and $k \in \mathbb{Z}_{>0}$, let $S_{k-1/2}^+(\Gamma_0^{(n-1)}(4))$ be the generalized Kohnen's plus subspace of $S_{k-1/2}(\Gamma_0^{(n-1)}(4))$. If k is even, then there exists a $\mathbb{C}$ -linear isomorphism*

$$\Psi_{n-1} : J_{k,1}^{\text{cusp}}(\text{Sp}_{n-1}(\mathbb{Z})^J) \xrightarrow{\simeq} S_{k-1/2}^+(\Gamma_0^{(n-1)}(4)),$$

which is compatible with the actions of Hecke operators.

Then by using an analogous method to the proof of Theorem 5.4 in [E-Z], we also obtain the compatibility of Ψ_{n-1} with Petersson inner products as follows:

Theorem 2 (cf. [K-K2]). *Let $n > 1$ and k be a positive integer. If k is even, then for any $\phi \in J_{k,1}^{\text{cusp}}(\text{Sp}_{n-1}(\mathbb{Z})^J)$, we have*

$$\langle \phi, \phi \rangle = 2^{(2k-2)(n-1)} \langle \Psi_{n-1}(\phi), \Psi_{n-1}(\phi) \rangle, \quad (4)$$

where in the left-hand side of the above equation, we denote by $\langle *, * \rangle$ the Petersson inner product defined on the space $S_{k-1/2}^+(\Gamma_0^{(n-1)}(4))$ which is normalized by $[\text{Sp}_{n-1}(\mathbb{Z}) : \Gamma_0^{(n-1)}(4)]^{-1}$.

Therefore by combining the equations (3) and (4), we have

Corollary 2. *Under the same situation as above, we have*

$$\frac{2^{4k-2nk+2n-2} \pi^{k+n}}{(k-1)!(n-1)!} \cdot \frac{\langle I_n(f), I_n(f) \rangle}{\langle \Psi_{n-1}(\phi_1), \Psi_{n-1}(\phi_1) \rangle} = L(k, f) \zeta(n). \quad (5)$$

Now we shall recall the so-called Ikeda's conjecture on the Petersson inner product of the Ikeda lifting. Before stating it, we prepare the following notations of L -functions: for a normalized Hecke eigenform $f \in S_{2k-n}(\text{SL}_2(\mathbb{Z}))$, we put

$$\begin{aligned} \tilde{\xi}(s) &:= \Gamma_{\mathbb{C}}(s) \zeta(s), \\ \Lambda(s, f) &:= \Gamma_{\mathbb{C}}(s) L(s, f), \\ \tilde{\Lambda}(s, f, \text{Ad}) &:= \Gamma_{\mathbb{C}}(s) \Gamma_{\mathbb{C}}(s + 2k - n - 1) L(s, f, \text{Ad}), \end{aligned}$$

where $\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s} \Gamma(s)$ and we denote by $L(s, f, \text{Ad})$ the adjoint L -function associated with f , which is defined by

$$L(s, f, \text{Ad}) := \prod_{p: \text{prime}} \{(1 - p^{-s})(1 - \alpha_p^2 p^{-s})(1 - \alpha_p^{-2} p^{-s})\}^{-1},$$

where $\alpha_p \in \mathbb{C}$ is the p -th Satake parameter of f . Then T. Ikeda ([Ike2]) gave the following conjecture:

Ikeda Conjecture (cf. Conjecture 5.1 in [Ike2]). *Let $n, k \in \mathbb{Z}_{>0}$ be even satisfying that $k > n + 1$. Under the same situation as in Fact 2, then we have*

$$\Lambda(k, f) \prod_{i=1}^{n/2} \tilde{\Lambda}(2i-1, f, \text{Ad}) \tilde{\xi}(2i) = 2^{\alpha(n,k)} \frac{\langle f, f \rangle \langle I_n(f), I_n(f) \rangle}{\langle \tilde{f}, \tilde{f} \rangle}, \quad (6)$$

where $\alpha(n, k) = (n-1)(k - n/2 + 1)$.

Therefore by the equation (5), we can reduce the Ikeda conjecture to the following

Conjecture. *Under the same assumption as above, then we have*

$$\frac{\langle \Psi_{n-1}(\phi_1), \Psi_{n-1}(\phi_1) \rangle}{\langle \tilde{f}, \tilde{f} \rangle} = 2^{\beta(n,k)} \prod_{j=1}^{n/2-1} \tilde{\xi}(2j) \tilde{\Lambda}(2j+1, f, \text{Ad}), \quad (7)$$

where $\beta(n, k) = -(n-2)(3k - (n-1)/2)$.

We note that the situation of the above conjecture is more suitable to show. In fact, we can obtain by showing a certain explicit formula for the Rankin-Selberg convolution series associated with $\Psi_{n-1}(\phi_1)$ that the above conjecture is true, therefore so is the Ikeda conjecture (cf. [K-K2]).

References

- [E-Z] M. Eichler and D. Zagier, *The theory of Jacobi forms*, Progress in Math., vol. 55, Birkhäuser Boston Inc., Boston, Mass., 1985.
- [Ibu] T. Ibukiyama, *On Jacobi forms and Siegel modular forms of half integral weights*, Comment. Math. Univ. St. Paul. **41** (1992), no. 2, 109–124.
- [Ike1] T. Ikeda, *On the lifting of elliptic modular forms to Siegel cusp forms of degree $2n$* , Ann. Math. **154** (2001), no. 3, 641–681.
- [Ike2] ———, *Pullback of the lifting of elliptic cusp forms and Miyawaki’s conjecture*, Duke Math. J. **131** (2006), no. 3, 469–497.
- [K-K1] H. Katsurada and H. Kawamura, *A certain Dirichlet series of Rankin-Selberg type associated with the Ikeda lifting*, to appear in J. Number Theory.
- [K-K2] ———, *Ikeda’s conjecture on the Petersson inner product of the Ikeda lifting*, in preparation.
- [Koh] W. Kohnen, *Modular forms of half-integral weight on $\Gamma_0(4)$* , Math. Ann. **248** (1980), 249–266.
- [K-S] W. Kohnen and N.-P. Skoruppa, *A certain Dirichlet series attached to Siegel modular forms of degree two*, Invent. Math. **95** (1989), 541–558.
- [Oda] T. Oda, *On the poles of Andrianov L -functions*, Math. Ann. **256** (1981), 323–340.
- [Yam] T. Yamazaki, *Rankin-Selberg method for Siegel cusp forms*, Nagoya Math. J. **120** (1990), 35–49.

Department of Mathematics, Hokkaido University, Kita 10, Nishi 8, Kita-Ku, Sapporo 060-0810, Japan; KAWAMURA, Hisa-aki (kawamura@math.sci.hokudai.ac.jp)

Motif 理論変形考

望月哲史¹

このノートでは motif 理論変形についての考え方とそれを補う文献案内 (と謂っても文献表は筆者の見識と知識量に依存していて完全ではない) を述べたい。紙面の都合上述べられない詳細は、[Epi0] 等を参照して載きたい。

1 motif 理論とは、代数多様体上の (co)homology 論的手法の生成系を見つける作業の総称の事である。

1.1 従って、扱っている問題陣に応じて、複数の motif 理論が生じ得る。

1.1.1 例を挙げるならば、Weil cohomology 理論を理解する為の古典的 motif 理論 [Kle68]、Bloch-Kato-Milnor 予想、Beilinson-Lichtenbaum 予想を理解する為の $\mathbb{A}^1$ -homotopy 理論 [Voe98], [SV00], [Wei06]、そして又、B. Kahn と R. Sujatha の双有理 motif 理論等が挙げられる。広義の意味では、Gersten 分解の存在を導き出す Bloch-Ogus(-Gabber) 理論等 [BO74], [CHK97] も motif 理論の変種であるところでは考えたい。

1.2 数学全般分野の視点に於いては、慣習的に古典的 motif 理論を指して “the” motif 理論と考える傾向が或る。又、近年、専門家の間では、 $\mathbb{A}^1$ -homotopy 理論を以って motif 理論と考える傾向が或る。

2 motif 理論変形とは、複数の motif 理論間の関係の研究の総称である。

2.1 この様な研究は、幾多の motif 理論に跨った数学的現象の理解に有意義である。

2.2 筆者が特に問題にするのは、 $\mathbb{A}^1$ -homotopy 理論と $\mathbf{G}_a$ に付随する motif を理解出来る $\mathbb{P}^1$ -homotopy 理論との関係である。

2.2.1 将来的には、例えば、代数的 K -理論の $\mathbb{A}^1$ -homotopy 不変性の障害を加法的 K -理論等で量り Hodge 分解を利用して統制する Vorst 予想 [CHW06] 等の (広義の意味での) motif 理論的解釈を与える事を念頭において研究している。

2.2.1.1 Vorst 予想は典型的な、 $\mathbb{A}^1$ -homotopy 理論と $\mathbb{P}^1$ -homotopy 理論に跨った問題である。

3 motif 理論の問題にはどの様に表記されるか？が本質的な問題として関わってきている。

3.1 生成系と関係式を然るべく定めて、(高階) 圏を構成して、考察している (co)homology 理論はそこを経由する様にする。そして、その (co)homology 論的手法は凡てその選ばれた生成系と関係式の帰結として導き出す事によって motif 理論は記述される。

3.2 例えば、古典的 motif 理論は abel 圏を使って表現されるであろうと “予想” されていたが、筆者には “理想” 以上の数学的根拠を見出せない。

3.3 安定 homotopy 理論の文脈では、motivic homotopy 理論は、compact 生成三角化圏を用いて表示されるであろうと予想 (期待) された。

3.3.1 これは、Neeman-Brown 表現定理 [Nee96] に起因している期待である。この定理は、compact 生成三角化圏上の cohomological 関手が表現可能である事の必要十分条件は、直和との可換性である事を示している。

3.3.1.1 従って、一つの (直和と可換な) cohomology 理論を定める事は、然るべき compact 生成三角化圏の対象を定める事と同値である。

3.3.2 実際に、 $\mathbb{A}^1$ -motivic homotopy 理論は、compact 生成三角化圏を用いて表現された。[Voe98],

¹This research is supported by the 21 century COE program at Graduate School of Mathematical Sciences, the University of Tokyo.

[Jar00]

3.3.2.1 正則な多様体に対する代数的 K -理論や motivic cohomology 理論が、安定 A^1 -motivic homotopy 圏の中で表現された。[Voe98]

3.3.2.2 安定 A^1 -motivic homotopy 圏は、普遍的な Bloch-Ogus cohomology 理論が経由する圏であると考えられている。[Lev06]

3.3.3 一方で、三角化圏の理論は多くの情報を失っている事が知られている。

3.3.3.1 例えば、それを補う理論として、homotopy(余) 極限の振る舞いを考察出来る導来子の理論 [Gro90], [Hel88] や homotopy 理論の公理的特徴付け [DHKS04] が考えられた。

3.3.3.1.1 又、代数的 K -理論は導来圏からも [Sch02] 導来子からも [Toë03] 復元出来ないが、Dwyer-Kan 単体的局所化 [DK80] から完全に復元されることが知られている。[TV04]

3.3.3.1.1.1 Dwyer-Kan 単体的局所化とは圏とその部分圏の組に対して、 $\mathcal{S}$ -圏 (単体的集合で enrich された圏) を対応させる操作であり、その連結成分が古典的な Gabriel-Zisman 型の局所化 [GZ67] に対応している。

3.3.3.1.1.1.1 $\mathcal{S}$ -圏は高階の射が凡て可逆な ∞ -圏の model だと考えられている。[TV05]

3.4 以上の経緯を踏まえて、motivic homotopy 理論は、連結成分を取る前の model 圏 [Qui67], [Hov98] 或いは、DG-圏 [Kel99]、安定 $\mathcal{S}$ -圏 [Hel97], [HS98], [Toë03], [TV04]、等を用いて表現される方が豊かな構造を持っているであろうと信じられている。

3.4.1 結局 motif 理論の記述問題で重大な基礎付けは、各々の圏の class の formalism で、生成系と関係式で記述する一般論 (例えば、高階 topos 理論 [TV05] や homotopical 圏論 [DHKS04]) である。

3.4.1.1 例えば、model 圏の文脈では、[MV99], [Hir03], [Spi01]、DG-圏の文脈では、[Han95], [Dri04], [BV06] 等の理論が重要な役割を果たしている。安定 $\mathcal{S}$ -圏の文脈では、[TV05] がその方向を示唆しているが、motif 理論への応用はまだ書かれていない。

3.5 筆者の想定する motif 理論変形は安定 $\mathcal{S}$ -圏を用いて記述される。

3.5.1 その所以は、代数的 cycle 依りも被約でない代数的 cycle の如き或る種の接続層の同型類群 (或いは、或る種の擬接続複体の擬同型類群) である二変数代数的 K 理論を Hom 集合に作用した圏を基盤に考えるからである。[Wal96], [Sus03]

3.5.1.1 代数的 K -理論は単体的集合 (或いは圏) の homotopy 群として捉えられるので、非可換な設定での DG-圏の理論 (=安定 $\mathcal{S}$ -圏の理論) が必要になる。

3.5.1.1.1 Homotopy 群との次数を合わせる為に、代数的 K -理論の model としては un-deloooped 版 [GG87], [GSVW92] が必要になる。

4 安定 motivic homotopy 論の文脈で、motif とは、“brave new” $M\mathbb{Z}$ 加群である。[KM95], [Spi01], [RØ06]

4.1 “brave new” 代数的構造とは、高階 homotopy 構造を持つ圏に於ける代数的構造対象 (群対象、環対象、...) を意味する。

4.1.1 例えば、motif とは、位相的安定 homotopy 圏に於いて、Eilenberg-MacLane 環 spectrum 上の加群の圏が加法群の導来圏の model である事 [EKMM97] の代数幾何的類似である。

4.1.1.1 Røndigs-Østvær の定理は標数 0 の体上の motivic cohomology spectrum $M\mathbb{Z}$ 上の加群の homotopy 圏は A^1 -homotopy motivic 圏と同値である事を示す。

4.2 実質的に前層 F が $M\mathbb{Z}$ -作用を持つという事は、Voevodsky の意味で、 F が transfer 付きである事を暗に意味している。

4.2.1 古くから知られているように、可換群多様体は、函手として transfer 付きに拡張される事

が知られている。[Org04]

4.2.1.1 半 Abel 多様体の様な 1-motif [Del74] が $\mathbb{A}^1$ -homotopy 理論と相性がいいのは、更にこれらの群多様体が、 $\mathbb{A}^1$ -homotopy 不変だからである。[Org04]

4.2.2 G_a を同様に理解するには、 $\mathbb{A}^1$ -homotopy 理論とは異なる motif 理論が必要であり、丁度、Laumon の一般化された 1-motif を考える事 [Lau96] に対応している。

5 motif 理論の本質的な問題は扱っている問題陣の観察から然るべく生成系を選ぶ事である。

5.1 筆者の立場から、生成系を選ぶ動機となる数学的現象は、Weil 相互律と Gersten 予想である。

5.1.1 筆者が Weil 相互律に着目する所以は、加藤-染川の予言『半 abel 多様体の 1-motif の tensor 積の体での切断には、Weil 相互律が関係式として現れる。』[Som90] に起因している。

5.1.1.1 実際にこの予想は、一次元半 abel 多様体に対して正しい。[SV00], [Moc06]

5.1.2 Weil 相互律は、 $\mathbb{A}^1$ -homotopy 理論に於いては Gysin 写像の functoriality の帰結として導かれる。[Moc06]

5.1.2.1 $\mathbb{A}^1$ -homotopy 理論では Gysin 写像は、法錐変形の議論を用いて構成され、従って、 $\mathbb{A}^1$ -homotopy 不変性の公理が構成にふんだんに用いられている。[Dég04], [Dég06]

5.1.3 一方で、一般化された de Rham-Witt 複体 [HS04] の Weil 相互律も知られている。[Rül07]

5.1.3.1 de Rham-Witt 複体は $\mathbb{A}^1$ -homotopy 不変でないので、この現象を $\mathbb{A}^1$ -motivic homotopy 理論的な観点から解釈するのは一見困難に思われる。

5.1.3.1.1 筆者は、丁度、代数的 K 理論と homotopy 代数的 K 理論の関係の様に motif と $\mathbb{A}^1$ -homotopy 不変 motif の二つが存在していると解釈してこの問題を理解しようとする。

5.1.3.1.1.1 例えば、motivic functor と $\mathbb{A}^1$ -homotopy 不変 motivic functor の間の自然な射の homotopy fiber は純性定理の障害を表し、各種実現で、偏純性定理が成立している事の根拠を与えていると考える。

5.2 安定 $\mathbb{P}^1$ -motivic homotopy 圏は普遍的な Bloch-Ogus-Gabber cohomology 理論が経由する圏になるように定義したい。

5.2.1 $\mathbb{A}^1$ -homotopy 理論を支えている二大定理は次の主張であり、それは Gersten 分解の存在の帰結である。[BV06]

- $\mathbb{A}^1$ -homotopy 不変 transfer 付き Nisnevich 層の cohomology は又、 $\mathbb{A}^1$ -homotopy 不変 transfer 付き Nisnevich 層である。

- $\mathbb{A}^1$ -homotopy 不変 transfer 付き Nisnevich 層の cohomology は Zariski cohomology で計算出来る。

5.2.1.1 Bloch-Ogus-Gabber 公理を分析して、完全無限体なる基礎体を持つ motif 理論の motivic functor が Gersten 予想を導くのに備えているべき必要な公理は、étale 切除性と $\mathbb{P}^1$ -homotopy 不変性であるという事が判る。[Epi0]

5.2.1.1.1 étale 切除性は Nisnevich 位相と相性がいい。[MV99]

5.2.1.1.2 射影的 bundle 公式を持つ (co)homology 理論は、 $\mathbb{P}^1$ -homotopy 不変である。

5.2.1.1.2.1 例えば、代数的 K -理論 [Qui73], [TT90], [Tho93]、加法的代数的 K -理論 (=cyclic homology 理論) [Kel99]、motivic cohomology 理論 [Voe96], [SV00], [Voe00]、加法的高次 Chow 群 [KL07] はその様な理論である。

5.2.1.2 基礎体の仮定は、Noether の正規化定理の変種 “幾何的表示定理” を証明するのに必要である。[GS88], [Gab94], [CHK97]

5.2.1.2.1 基礎体がない場合の motif 理論を構成するには、基礎体無しの Noether の正規化定理に相当する議論をする必要がある。[GerCon], [Epi0]

参考文献

- [BO74] S. Bloch, A. Ogus, *Gersten's conjecture and the homology of schemes*, Ann. Sci. Ec. Norm. Sup., 4. sèr. **7** (1974), p.181-202.
- [BV06] A. Belilinson and V. Volgodsky, *A guide to Voevodsky's motives*, preprint math.AG/0604004 (2006).
- [CHK97] Jean-Louis Colliot-Thélène, T. Raymond Hoobler, Bruno Kahn, *The Bloch-Ogus-Gabber theorem*, In algebraic K -theory, Volume **16** of Fields Inst. Commun. (1997), p.31-94.
- [CHW06] G. Cortinàs, C. Hasemeyer and C. A. Weibel, *K -regularity, cdh -fibrant Hochschild homology and a conjecture of Vorst*, preprint available at <http://www.math.uiuc.edu/K-theory/0783> (2006).
- [Dég04] F. Déglise, *Interprétation motivique de la formule d'excès d'intersection*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), p. 41-46.
- [Dég06] F. Déglise, *Motifs génériques*, preprint available at <http://www.math.uiuc.edu/K-theory/0690> (2006).
- [Del74] P. Deligne, *Théorie de Hodge III*, Publ. Math. I.H.E.S. **44** (1974), p.5-78.
- [Dri04] V. Drinfeld, *DG quotients of DG categories*, J. Algebra **272** (2004), p.643-691.
- [DK80] W. Dwyer and D. Kan, *Simplicial localization of categories*, JPAA **17** (1980), p.267-284.
- [DHKS04] W. Dwyer, P. Hirschhorn, D. M. Kan and J. H. Smith, *Homotopy limit functors on model categories and homotopical categories*, Mathematical Surveys and Monographs, Vol. **113**, American Mathematical Society.(2004).
- [EKMM97] A. D. Elmendorf, I. Kriz, M. A. Mandell, J. P. May, *Rings, modules, and algebras in stable homotopy theory*, Mathematical Surveys and Monographs, Vol. **47**, American Mathematical Society. (1997).
- [Gab94] O. Gabber, *Gersten's conjecture for some complexes of vanishing cycles*, Manuscripta Math. **85** (1994), p.323-343.
- [GZ67] P. Gabriel, M. Zisman, *Calculus of fractions and homotopy theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band **35**, Springer-Verlag New York. (1967).
- [GG87] H. Gillet and D. Grayson, *The loop space of the Q -construction*, Illinois J. Math. **31** (1987), p.574-597.
- [GS88] M. Gros, N. Suwa, *La conjecture de Gersten pour les faisceaux de Hodge-Witt logarithmiques*, Duke Math. Journal, **57** (1988), p.615-628.
- [Gro90] A. Grothendieck, *Dérivateurs*, unpublished manuscript, a part which is available at <http://www.math.jussieu.fr/~maltsin/groth/Derivateurs.html> (1990).
- [GSVW92] T. Gunnarsson, R. Schwänzl, R. M. Vogt and F. Waldhausen, *An un delooped version of algebraic K -theory*, JPAA **79** (1992), p.255-270.
- [Han95] M. Hanamura, *Mixed motives and algebraic cycles I*, Math. Res. Lett. **2** (1995), p.811-821.
- [HS04] L. Hasselholt and I. Madsen, *On the de Rham-Witt complex in mixed characteristic*,

- Ann. Scient. Éc. Norm. Sup. IV, Ser. **37** (2004), p.1-43.
- [Hel88] A. Heller, *Homotopy theories*, Memories of the Amer. Math. Soc. **71** (1988).
- [Hel97] A. Heller, *Stable homotopy theories and stabilization*, JPAA **115** (1997), p.113-130.
- [HS98] A. Hirschowitz, C. Simpson, *Descente pour les n -champs*, preprint math.AG/9807049 (1998).
- [Hir03] P. Hirschhorn, *Model categories and their localizations*, Mathematical Surveys and Monographs, Vol. **99**, American Mathematical Society. (2003).
- [Hov98] M. Hovey, *Model categories*, Mathematical Surveys and Monographs, Vol. **63**, American Mathematical Society. (1998).
- [Jar00] J. F. Jardine, *Motivic symmetric spectra*, Doc. Math. **5** (2000), p.445-553.
- [Kel99] B. Keller, *On the cyclic homology of exact categories*, JPAA, Vol. **136** (1999), p.1-56.
- [Kle68] S. L. Kleiman, *Algebraic cycles and the Weil conjectures*, Dix exposés sur la cohomologie des schémas, North-Holland Amsterdam (1968), p.359-386.
- [KL07] A. Krishna and M. Levine, *Additive Chow groups of schemes*, preprint math.AG/0702138 (2007).
- [KM95] I. Kriz, J. P. May, *Operads, algebras, modules and motives*, Astérisque. No. **233** (1995).
- [Lau96] Laumon, *Transformation de Fourier generalisee*, preprint mat.AG/9603004 (1996).
- [Lev06] M. Levine, *Mixed motives and homotopy theory of schemes V*, available at <http://www.ihes.fr/IHES/Scientifique/asie/resume.html> (2006).
- [Moc06] S. Mochizuki, *Motivic interpretation of Milnor K -groups associated to Jacobian varieties*, thesis, available at <http://www.math.uiuc.edu/K-theory/0774> (2006).
- [GerCon] S. Mochizuki, *Gersten's conjecture for commutative discrete valuation rings*, preprint, available at <http://www.math.uiuc.edu/K-theory/0819> (2007).
- [Epi0] S. Mochizuki, *Deforming motivic theories Episode 0 ~ Revolution of an additive world ~*, preprint (2007).
- [MV99] F. Morel, V. Voevodsky, *$\mathbf{A}^1$ -homotopy theory of schemes*, Publ. Math. I.H.E.S. **90** (1999), p. 45-143.
- [Nee96] A. Neeman, *The Grothendieck duality theorem via Bousfield's techniques and Brown representability*, J. Amer. Math. Soc., **9**, (1996), p. 205-236.
- [Org04] F. Orgogozo, *Isomotifs de dimension inférieure ou égale à un*, manuscripta math. **115** (2004), p. 339-360.
- [Qui67] D. Quillen, *Homotopical algebra*, Lect. notes in Math. vol. **43** (1967).
- [Qui73] D. Quillen, *Higher algebraic K -theory I*, In Higher K -theories, Springer Lect. Notes Math. **341** (1973), p.85-147.
- [RØ06] O. Röndigs and P. A. Østvær, *Motives and modules over motivic cohomology*, C. R. Acad. Sci. Paris, Ser. I **342** (2006), p.751-754.
- [Rül07] Rülling, *The generalized de Rham Witt complex over a field is a complex of zero cycles*, J. Alg. Geom. **16** (2007), p.109-169.
- [Sch02] M. Schlichting, *A note on K -theory and triangulated categories*, Inv. Math. **150** (2002), p.111-116.
- [Som90] M. Somekawa, *On Milnor K -groups attached at semi-Abelian varieties*, K -theory, **4** (1990), p. 105-119.

- [Spi01] M. Spitzweck, *Operads, algebras and modules in model categories and motives*, thesis, (2001).
- [SV00] A. Suslin and V. Voevodsky, *Bloch-Kato conjecture and motivic cohomology with finite coefficients*, The Arithmetic and Geometry of Algebraic Cycles, Nato ASI series C, vol. **548**, Kluwer, (2000), p. 117-189.
- [Sus03] A. Suslin, *On the Grayson spectral sequence*, Tr. Mat. Inst. Stek. **241** (2003), p.218-253.
- [TT90] R. W. Thomason, T. Trobaugh, *Higher K-theory of schemes and of derived categories*, In The Grothendieck Festschrift, Vol III, (1990), p.247-435.
- [Tho93] R. W. Thomason, *Les K-groupes d'un fibré projectif*, Algebraic K-theory and algebraic topology, Nato ASI series C, vol. **407**, Kluwer, (1993), p. 243-248.
- [Toë03] B. Toën, *Homotopical and higher categorical structures in algebraic geometry*, preprint Math.AG/0312262 (2003).
- [TV04] B. Toën, G. Vezzosi, *A remark on K-theory and S-categories*, Topology **43** (2004), p.765-791.
- [TV05] B. Toën, G. Vezzosi, *Homotopical algebraic geometry I: topos theory*, Advances in Mathematics **193** (2005), p.257-372.
- [Voe96] V. Voevodsky, *Homology of schemes*, Selecta Math. (N.S.) **2** (1996), p.111-153.
- [Voe98] V. Voevodsky, *$\mathbf{A}^1$ -homotopy theory*, Procceding of the international congress of mathematicians, Berlin, (1998), p.579-604.
- [Voe00] V. Voevodsky, *Triangulated categories of motives over field*, in *Cycles, transfers, and motivic homology theories*, Annals of Mathematics Studies, vol **143**, Princeton University press, (2000), p. 188-254.
- [Wal96] M. E. Walker, *Motivic complex and the K-theory of automorphisms*, thesis, (1996).
- [Wei06] C. A. Weibel, *Axioms for the norm residue isomorphism*, preprint available at <http://www.math.uiuc.edu/K-theory/0809> (2006).