

Serre の保型性予想をめぐって - 計算機的保型形式論入門 - Part II

【Sage ユーザーのための改訂版】

横山 俊一 (九大数理) 2012 年 4 月 15 日

On Serre's modularity conjecture: a brief introduction to the theory of modular forms using computer algebra systems - Part II

【Revised version for Sage users】

Shun'ichi Yokoyama (Kyushu University) April 15th, 2012

1 概要

まず始めにお断りしておくが、本稿は既刊のプロシーディングス

- 木田雅成, 原田昌晃, 横山俊一 (編)「Magma で広がる数学の世界」, 九大数理 MI レクチャーノートシリーズ vol. 29

に所収の拙稿

- 「Serre の保型性予想をめぐって - 計算機的保型形式論入門 -」(pp. 107-133)

を一部改訂したものである。数式処理システム Sage の活用例として、現在実装されている範囲で Sage で計算出来るもの(3章まで)は全て Sage の言葉で書き直した。未実装の部分は今後の課題として4章に纏めた。

本稿では、Serre の保型性予想 (cf. [12], 以下「Serre 予想」と略記する) という代数的整数論乃至数論幾何の分野における非常に trendy な話題について、計算機によるデモンストレーションを交えながら紹介する (因みに筆者が修士時代から研究テーマとして扱っているものである)。この予想に関する詳細は後述するが、簡潔に言えば代数的対象物である「Galois 表現」に対し、解析的对象物である「保型形式」が一一に対応しているであろう、という予想であり、最も基本的な有理数体上の場合が 2007 年に Khare-Wintenberger [8] によって解決されたばかりである。本予想は様々な形で一般化が期待されており、各々研究が進められているものの、未だ一般化された予想の定式化すら不十分といったケースも少なくない。そのため、計算機による数値実験を重ねて両者の対応を考察することが定式化・精密化への第一歩となると期待されている。本稿ではそのような背景を踏まえ、予想の数値実験に纏わる計算例をいくつか紹介したい。

まず 2 章では古典的保型形式を題材に Sage によるデモンストレーションを行う。続いて 3 章では、既に解決された有理数体上の Serre 予想に纏わる計算実験を行う。予備知識としては必要最小限の古典的保型形式論 (例えば Serre [11] の 7 章) があれば十分であるが、より進んだ内容に興味を持たれた方には Diamond-Shurman [4], Miyake [9] または Shimura [13] などをお薦めする。

一方 4 章ではプラットフォームを Magma に移し、まず 3 章の一般化として基礎体が虚二次体の場合を取り上げ、対応する保型形式として有力視されている Bianchi 保型形式を紹介すると共に、簡単な計算例を紹介する。そして最後に補足として、上記 2 種類の保型形式以外

の重要な例である Hilbert 保型形式の簡単な計算例を紹介する. Hilbert 保型形式は総実代数体上の Serre 予想において Galois 表現に対応する保型形式として大変注目されている.

なお, 本稿の目的上, Galois 表現や楕円曲線に纏わる基礎知識については大部分を割愛せざるを得なかった. これらについては適宜紹介している参考文献で補って頂きたい.

筆者の最大の目標は, 4 章で行われている Magma 上の計算を全て Sage 単独で実現することである. 現在 Sage コミュニティによってこの計画は進行中であり, 数年内に数論幾何システム Purple Sage (PSage) 安定版としてリリースされると予想される. しかしながら未だ完成のメドは立っておらず, 独自にパッケージを得られないものかと画策している. 読者からのコメント・アドバイスを切望する次第である.

謝辞

本稿(改訂版)を執筆するきっかけを下さいました高山信毅氏(神戸大学 / JST CREST)及び濱田龍義氏(福岡大学 / JST CREST)に感謝御礼申し上げます.

目次

| | | |
|-----|------------------------------------|----|
| 1 | 概要 | 1 |
| 2 | デモンストレーション | 3 |
| 3 | 有理数体上の Serre の保型性予想とその検証 | 8 |
| 4 | Sage ToDo | 12 |
| 4.1 | 虚二次体上の Serre の保型性予想とその検証 | 12 |
| 4.2 | 付録「Hilbert 保型形式とその計算」 | 19 |

2 デモンストレーション

まずは最も基本的な古典的保型形式を題材として, Sage による計算に慣れ親しんでいこう. 最初に保型形式の空間を構成する. 例えば $M_{12}(\Gamma_0(1)) = M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ は

```
> m = ModularForms(Gamma0(1),12)
> m
Modular Forms space of dimension 2 for Modular Subgroup
SL(2,Z) of weight 12 over Rational Field
```

となる. ここに $\Gamma_0(N)$ は合同部分群 (congruence subgroup)

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

である (更に合同式条件の行列を $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ としたものを $\Gamma_1(N)$ と書く). 保型形式のオプションは数種類用意されており, デフォルト値は

```
ModularForms(group=1, weight=2, base_ring=None, use_cache=True, prec=6)
```

となっている (ユーザーが自由に変更可). また, 空間の基底は q -展開の形で計算される.

```
> m.basis()
[
  q - 24*q^2 + 252*q^3 - 1472*q^4 + 4830*q^5 + 0(q^6),
  1 + 65520/691*q + 134250480/691*q^2 + 11606736960/691*q^3 +
  274945048560/691*q^4 + 3199218815520/691*q^5 + 0(q^6)
]
```

係数だけを取り出すことも容易である.

```
> f = m.basis()[1]; f
1 + 65520/691*q + 134250480/691*q^2 + 11606736960/691*q^3 +
274945048560/691*q^4 + 3199218815520/691*q^5 + 0(q^6)
> f.coefficients([1,3,4])
[65520/691, 11606736960/691, 274945048560/691]
```

Sequence に関しては Magma のそれとは異なり, インデックスが 0 から始まることに注意が必要である. 従って n 番目の要素を取り出したい場合は $n-1$ のインデックスで引いて来なければならない.

さて上の基底は $M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ の cuspidal subspace $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ の基底である. 尖点形式の空間は Sage では

```
> s = CuspForms(Gamma0(1),12)
> s
Cuspidal subspace of dimension 1 of Modular Forms space of dimension 2
for Modular Group SL(2,Z) of weight 12 over Rational Field
```

として実現出来る。因みに上の出力で保型形式の空間の次元が含まれているが, Sage の保型形式のパッケージでは, 保型形式の次元の計算は dimension formula と或る種の bound method を用いて高速に求める事が出来る¹.

```
> m500 = ModularForms(Gamma1(500),500)
> m500.dimension()
3742950
```

このようなデータは, ループとリストの機能を使うことによって効率的に整理することが出来る。必要なデータを書き出したり読み出したりするのが非常に容易であることも Sage のメリットと言えよう。

続いて Hecke 作用素を計算してみる。例として $M_2(\Gamma_0(41))$ を考え, T_2 を計算してみよう。

```
> m41 = ModularForms(Gamma0(41),2); m41
Modular Forms space of dimension 4 for Congruence Subgroup Gamma0(41)
of weight 2 over Rational Field
> T2 = m41.hecke_operator(2); T2
Hecke operator T_2 on Modular Forms space of dimension 4
for Congruence Subgroup Gamma0(41) of weight 2 over Rational Field
> ch2 = T2.charpoly(var='x'); ch2
x^4 - 2*x^3 - 8*x^2 + 14*x + 3
> T2.matrix()
[ 0  3 -2  0]
[ 1 -2  0  0]
[ 0 -2  1  0]
[ 0  0  0  3]
> factor(ch2)
(x - 3) * (x^3 + x^2 - 5*x - 1)
```

指標付きの空間の構成も容易である。

```
> G = (DirichletGroup(13).0)^2
> G.order()
6
> M = ModularForms(G,2); M
Modular Forms space of dimension 3, character [zeta6] and weight 2
over Cyclotomic Field of order 6 and degree 2
> f = M.T(2).charpoly('x'); f
x^3 + (-2*zeta6 - 2)*x^2 - 2*zeta6*x + 14*zeta6 - 7
> f.factor()
(x - 2*zeta6 - 1) * (x - zeta6 - 2) * (x + zeta6 + 1)
```

¹例えば [14] Chapter 6 を参照.

続いてニューフォームの空間を計算してみよう. 例えば $S_2(\Gamma_0(45))$ を考えてみる.

```
> Newforms(45,2)
[q + q^2 - q^4 - q^5 + O(q^6)]
```

$\dim(S_2^{new}(\Gamma_0(45))) = 1$ ということは $\dim(S_2^{old}(\Gamma_0(45))) = 2$ となるはずである. これを確認してみよう. まず $M \mid 45$, $M \neq 1, 45$ の候補は $M = 3, 5, 9, 15$ であり, このうち $S_2(M) \neq 0$ となるものは $M = 15$ の時のみである (上の計算と同様にして簡単に確かめられる). このただ一つの基底

```
[
  q - q^2 - q^3 - q^4 + q^5 + q^6 + 3*q^8 + q^9 + O(q^10)
]
```

を f_{15} とおくと, オールドフォームは

$$\alpha_d : S_2(15) \rightarrow S_2(45)$$

で $f(q) \in S_2(15)$ を $f(q^d) \in S_2(45)$ へ移す degeneracy map なる写像を用いて

$$S_2^{old}(45) = \text{Im}(\alpha_1) \cup \text{Im}(\alpha_3)$$

と表現されるので, その次元は 2 であることが確認出来る. ちなみに $S_2(45)$ の基底の q -展開を見ると

```
[
  q - q^4 - q^10 - 2*q^13 - q^16 + 4*q^19 + O(q^20),
  q^2 - q^5 - 3*q^8 + 4*q^11 - 2*q^17 + O(q^20),
  q^3 - q^6 - q^9 - q^12 + q^15 + q^18 + O(q^20)
]
```

となり, 一番下の基底は $\alpha_3(f_{15})$ に他ならない.

因みにニューフォームは Sage ではラベル付けされており, 上の例は

```
> Newform('45a', names='a')
q + q^2 - q^4 - q^5 + O(q^6)
```

で得ることが出来る.

次に楕円曲線に付随する保型形式について調べる. 以下は導手 11 の楕円曲線 E を与え, それに付随する保型形式が $S_2(\Gamma_0(11))$ から得られることを確認したものである.

```
> E = EllipticCurve([0,-1,1,-10,-20]); E
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20 over Rational Field
> E.conductor()
11
> f1 = E.modular_form(); f1
q - 2*q^2 - q^3 + 2*q^4 + q^5 + O(q^6)
> s11 = CuspForms(Gamma0(11),2)
> f2 = s11.basis()[0]; f2
q - 2*q^2 - q^3 + 2*q^4 + q^5 + O(q^6)
```

保型形式の合同判別定理として知られている Sturm の定理 [16] を用いると, $S_2(\Gamma_0(11))$ の Sturm bound は 2 であるから, 明らかに f_1 と f_2 は一致していることが分かる.

最後に, modular symbol と呼ばれる重要な対象物を取りあげておく. 上半平面にカスプを合わせたものをレベル N の合同部分群で割って compact Riemann 面 $X_0(N)$ を得たとき, modular symbol とはカスプ間をつなぐ $X_0(N)$ 上の path の事とイメージして頂いて差し支えない. これらは保型形式の空間を効率よく計算する為に有用な道具として用いられる.

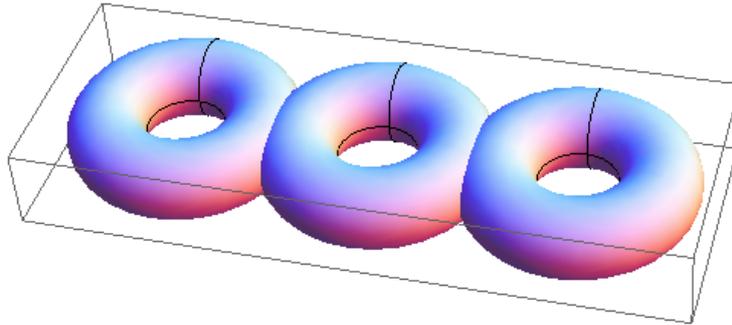


Figure. Compact Riemann 面 $X_0(39)$.

例を一つ挙げよう. $X_0(39)$ の 1 次ホモロジー群 $H_1(X_0(39), \mathbb{Z})$ は $\mathbb{Z}^{\oplus 6}$ に同型であり, 幾何的には上図のような種数 3 の compact Riemann 面を与える. これは $S_2(\Gamma_0(39))$ の modular symbol の空間の次元が 6 であり, 1 つのトーラスは 2 つの path で張られ², それらが 3 つ連結して出来ていると解釈出来る. 計算してみると, 確かに modular symbol の空間の基底は 6 つ得られる.

```
> MS = ModularSymbols(39,2,base_ring=QQ).cuspidal_subspace(); MS
Modular Symbols subspace of dimension 6 of Modular Symbols
space of dimension 9 for Gamma_0(39) of weight 2 with sign
0 over Rational Field
> MS.basis()
((3,4) - (13,2) + (13,3), (3,11) - (13,2) + (13,3),
(3,19) - (13,2) + (13,3), (3,22) - (13,2) + (13,3),
(3,25) - (13,2) + (13,3), (13,1) - (13,2))
```

勿論 modular symbol の空間にも Hecke 作用素の作用を考えることが出来る.

```
> MS.T(2).matrix()
[ 0  1 -1 -1  1 -1]
[ 1 -1 -2  1  1 -1]
[ 0  0 -1  0  1 -1]
[-1  1 -1  0  1 -1]
[ 0  0  0  0  1  0]
[ 0  0 -2  0  1 -1]
```

²トポロジーなどの分野では, この 2 つの path はメリディアン (経線: meridian) とロンジチュード (緯線: longitude) などと呼ばれている.

```

> ch2 = M.T(2).charpoly('x'); ch2
x^6 + 2*x^5 - 5*x^4 - 4*x^3 + 11*x^2 - 6*x + 1
> ch2.factor()
(x - 1)^2 * (x^2 + 2*x - 1)^2

```

なお modular symbol を用いず計算したものと比較すると、両者の固有値は一致していることが分かる.

```

> S39 = CuspForms(39,2)
> S39.T(2).matrix()
[ 0 2 -1]
[ 1 -2 1]
[ 0 -1 1]
> ch2h = S39.T(2).charpoly('x'); ch2h
x^3 + x^2 - 3*x + 1
> ch2h.factor()
(x - 1) * (x^2 + 2*x - 1)

```

再び modular symbol の計算に戻り、固有形式の q -展開を計算しておこう.

```

> MS.decomposition()
[
Modular Symbols subspace of dimension 2 of Modular Symbols
space of dimension 9 for Gamma_0(39) of weight 2 with sign
0 over Rational Field,
Modular Symbols subspace of dimension 4 of Modular Symbols
space of dimension 9 for Gamma_0(39) of weight 2 with sign
0 over Rational Field
]
> MS4 = MS.decomposition()[1]
> MS4.q_eigenform(10,'a')
q + a*q^2 + q^3 + (-2*a - 1)*q^4 + (-2*a - 2)*q^5 + a*q^6
+ (2*a + 2)*q^7 + (a - 2)*q^8 + q^9 + 0(q^10)

```

modular symbol について更に詳しく知りたいという場合は [14] を参照願いたい. この文献では一般化した modular symbol についても詳しく取り扱われている.

3 有理数体上の Serre の保型性予想とその検証

まずは Galois 表現 (正確には mod l Galois 表現) の定義から始めよう. l を素数とする.

定義 3.1. ρ が \mathbb{Q} 上の 2 次元 mod l Galois 表現であるとは, 連続準同型

$$\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

のことである. 但し $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (\mathbb{Q} の絶対 Galois 群) とし, $G_{\mathbb{Q}}$ には Krull topology を, $\mathrm{GL}_2(\overline{\mathbb{F}}_l)$ には discrete topology を入れて考える.

さて, 保型形式には性質を特徴付けるタイプ (N, k, ε) という概念があったが, Galois 表現にも同様にタイプ $(N(\rho), k(\rho), \varepsilon(\rho))$ を定義することが出来る. しかしその定義はやや複雑であるので, ここではレベルだけを紹介する. 残る重さと指標の定義については, Serre の原論文 [12] を参照願いたい.

定義 3.2. V を 2 次元 $\overline{\mathbb{F}}_l$ -ベクトル空間とし, L/\mathbb{Q} を有限次 Galois 拡大とする. $\rho: \mathrm{Gal}(L/\mathbb{Q}) \rightarrow \mathrm{GL}(V)$ のレベル $N(\rho)$ は

$$N(\rho) = \prod_{p \neq l} p^{n(p, \rho)}$$

で定義される. ここで $n(p, \rho)$ は

$$n(p, \rho) = \sum_{i \geq 0} \frac{1}{(G_0 : G_i)} \dim(V/V_i)$$

で与えられる. なお $G_0 \supset G_1 \supset \dots \supset G_i \supset \dots$ は有限次 Galois 拡大 L/\mathbb{Q} の Galois 群 $\mathrm{Gal}(L/\mathbb{Q})$ の高次下付き分岐群, V_i は V の G_i -固定部分空間を表す.

上から分かるように, ρ のレベルは ρ の l 以外の素数における分岐の様子を反映している. 逆に ρ の l での分岐の様子を反映しているのが重さ (Serre weight と呼ばれる) である.

mod l Galois 表現 ρ で $\det \rho(c) = -1$ を満たすとき, ρ は奇 (odd) であるという (但し c は複素共役). この ρ に対して

$$a_p = \mathrm{Tr}(\rho(\mathrm{Frob}_p))$$

と定義する. ここに Frob_p は Frobenius 写像 (p 乗写像) である.

それでは Serre 予想のステートメントを述べよう. 本来ならばこれは現在「予想」ではないので「Khare-Wintenberger の定理」と書くべきであろうが, ここでは「予想」のまま記すことにしたい.

予想 3.3. 任意の既約かつ奇な 2 次元 mod l Galois 表現

$$\rho: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

はタイプ $(N(\rho), k(\rho), \varepsilon(\rho))$ の (古典的) 尖点形式から来る. 即ちある尖点形式

$$f = \sum_{n \geq 1} b_n q^n \quad (q = e^{2\pi iz/N}) \in S_{k(\rho)}(\Gamma, \varepsilon(\rho))$$

が存在し (ここで Γ はレベル $N(\rho)$ の合同部分群) 素数 $p \nmid lN(\rho)$ に対して次が成り立つ

$$\boxed{a_p \equiv b_p} \quad , \quad \det(\rho(\text{Frob}_p)) \equiv \varepsilon(p)p^{k-1} \pmod{l}.$$

上の予想は 1987 年に発表された “refined version” 乃至 “precise form” である. Serre 予想自体はそれより十数年ほど前に Serre 自身の別の論文に登場しており, そこでは上の「タイプ」を指定しないものが述べられている (これは “weak version” 乃至 “vague form” と呼ばれている). さらに refined version の発表後, 上の「タイプ」のうち指標に関する若干の補正が必要であることが, これまた Serre 自身によって指摘された. 因みに Khare-Wintenberger によって証明されたのもこの補正を仮定したものである. また, これとは異なる Serre 予想の定式化を Edixhoven [5] も行っており, こちらの流儀を採用するとこのような補正は必要無くなる. 但し Edixhoven 版の Serre 予想はその一部が未解決のままである.

Serre 予想の証明には, 帰納法のアイディアを用いた現代数論の最新のテクニックが使われている. 例えば報告集 [17] には Serre 予想に纏わる (関係する) 非常に詳細な解説が収められており, 非専門家向けの分かりやすい記事もあるので, こちらを参照されたい.

それでは計算例に入る. まずは最も良く知られた簡単な例から始めよう. $f(x) = x^3 - x + 1 \in \mathbb{Q}[x]$ とし, K/\mathbb{Q} を f を最小多項式に持つ最小分解体とする. このとき $\text{Gal}(K/\mathbb{Q}) \simeq S_3$ が成り立つ.

```
> L.<v> = NumberField(x^3-x+1)
> L.galois_group(names='y')
Galois group of Galois closure in y of Number Field in v
with defining polynomial x^3 - x + 1
```

これでは分からないので, Pari 型で出力してみると S_3 であることが分かる. Sage の統合ソフトウェアとしてのメリットは, こういった所からも窺える.

```
> Gal = L.galois_group(type='pari'); Gal
Galois group PARI group [6, -1, 2, "S3"] of degree 3 of
the Number Field in v with defining polynomial x^3 - x + 1
```

そこで埋め込み $\rho: S_3 \rightarrow \text{GL}_2(\mathbb{F}_{23})$ を与え³, 自然な射影 $\pi: G_{\mathbb{Q}} \rightarrow \text{Gal}(K/\mathbb{Q})$ と合成して Galois 表現

$$\rho: G_{\mathbb{Q}} \rightarrow \text{Gal}(K/\mathbb{Q}) \simeq S_3 \rightarrow \text{GL}_2(\mathbb{F}_{23})$$

を構成する. この Galois 表現 ρ に関しては, $\text{Tr}(\rho(\text{Frob}_p))$ の値は f の mod p での分解の型によって定まることが分かっており, 計算すると以下ようになる. 後は f の mod p での分解の型を調べれば良く, これは \mathbb{F}_p 係数での多項式の因数分解に他ならない.

³詳しくは $(1\ 2) \in S_3$ を $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ へ, $(1\ 2\ 3) \in S_3$ を $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ へ移す.

| 分解の型 | ord(Frob _p) | Tr(ρ(Frob _p)) |
|-----------|-------------------------|---------------------------|
| 3つの1次式の積 | 1 | 2 |
| 1次式と2次式の積 | 2 | 0 |
| 既約 | 3 | -1 |

さて、この Galois 表現に付随する尖点形式は Ramanujan のデルタ

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

と呼ばれる重さ 12 (かつレベル 1) の尖点形式である。これは 2 章の序盤に計算した尖点形式の空間 $S_{12}(\Gamma_0(1)) = S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ の基底であって、少し計算範囲を伸ばせば

$$\begin{aligned} q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 - \\ 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} - 577738q^{13} + \\ 401856q^{14} + 1217160q^{15} + 987136q^{16} - 6905934q^{17} + 2727432q^{18} + \\ 10661420q^{19} - 7109760q^{20} - 4219488q^{21} - 12830688q^{22} + 18643272q^{23} \\ + 21288960q^{24} - 25499225q^{25} + 13865712q^{26} - 73279080q^{27} + \\ 24647168q^{28} + 128406630q^{29} - 29211840q^{30} - 52843168q^{31} - \\ 196706304q^{32} + 134722224q^{33} + 165742416q^{34} - 80873520q^{35} + \\ 167282496q^{36} - 182213314q^{37} - 255874080q^{38} - 145589976q^{39} + \\ 408038400q^{40} + 0(q^{41}) \end{aligned}$$

と展開される。この係数を mod 23 すれば

$$\begin{aligned} q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25} + \\ q^{26} + q^{27} - q^{29} - q^{31} + q^{39} + 0(q^{41}) \end{aligned}$$

となる。以上より、両者の係数を比較すれば一致している様子が観察出来る。

| | | | | | | | | | | | | | |
|----------|----|----|---|---|----|----|----|----|-----|----|----|----|-----|
| p | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | ... |
| ρ | -1 | -1 | 0 | 0 | 0 | -1 | 0 | 0 | * | -1 | -1 | 0 | ... |
| Δ | -1 | -1 | 0 | 0 | 0 | -1 | 0 | 0 | (1) | -1 | -1 | 0 | ... |

続いてもう少し複雑な例に移ろう。まず \mathbb{Q} 上の半安定⁴ (semi-stable) 楕円曲線を用意し、これに付随する Galois 表現を構成する。例として

$$E : y^2 + xy + y = x^3 + 1$$

を考え、 E の極小判別式 (minimal discriminant) を Δ_E とおく。このとき、 E に付随する 2 次元 mod l Galois 表現 $\rho_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{Aut}(E[l]) \simeq \mathrm{GL}_2(\mathbb{F}_l)$ のタイプは

$$N(\rho_{E,l}) = \prod_{p \neq l, l | \mathrm{ord}_p(\Delta_E)} p, \quad k(\rho_{E,l}) = \begin{cases} 2 & (l \mid \mathrm{ord}_l(\Delta_E)) \\ l+1 & (\text{otherwise}) \end{cases}, \quad \varepsilon(\rho_{E,l}) = 1$$

⁴至る所良い還元 (good reduction) または乗法的還元 (multiplicative reduction) を持つ曲線のこと。

で与えられる (cf. [12], Prop.5). ここまでを計算してみると

```
> E := EllipticCurve([1,0,1,0,1]); E
Elliptic Curve defined by y^2 + x*y + y = x^3 + 1 over
Rational Field
> D = E.discriminant(); D
-639
> D.factor()
-1 * 3^2 * 71
```

となり $\Delta_E = -3^2 \cdot 71$ が求まる. このとき E は $l = 3$ で分裂乗法的還元 (split multiplicative reduction), $l = 71$ で非分裂乗法的還元 (non-split multiplicative reduction) を持つ. 今 $E[3]$ 上の Galois 表現 $\rho_3 = \rho_{E,3}$ を考えると, 先程述べた事実から $(N(\rho_3), k(\rho_3), \varepsilon(\rho_3)) = (71, 4, 1)$ が分かる. ここで $\text{Tr}(\rho_3(\text{Frob}_p))$ を $p \leq 50$ の範囲で計算しておく (これは E の情報から得られる). 例えば $p = 31$ は次のようになり, 素数をわたるループをかければ良い.

```
> E = EllipticCurve(GF(31), [1,0,1,0,1])
> E.trace_of_frobenius()
-10
```

一方, タイプ $(71, 4, 1)$ を持つような尖点固有形式を求めなければならないが, これは $S_4^{\text{new}}(\Gamma_0(71))$ から得られる. 以上 2 つの計算結果を並べてみると, 各 p について両者の値は mod 3 で一致していることが分かる.

| | | | | | | | | | | | | | |
|--------|---|-----|-----|----|----|----|----|------|------|-----|-----|------|-----|
| p | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | ... |
| ρ | 1 | (1) | 2 | 2 | 0 | -2 | 0 | 0 | 0 | -2 | -10 | -6 | ... |
| f | 1 | (1) | -16 | -1 | 24 | 7 | 72 | -153 | -213 | 232 | 149 | -204 | ... |

(mod 3)

| | | | | | | | | | | | | | |
|--------|---|-----|----|----|----|----|----|----|----|----|----|----|-----|
| p | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | ... |
| ρ | 1 | (1) | -1 | -1 | 0 | 1 | 0 | 0 | 0 | 1 | -1 | 0 | ... |
| f | 1 | (1) | -1 | -1 | 0 | 1 | 0 | 0 | 0 | 1 | -1 | 0 | ... |

4 Sage ToDo

ここからは未だ Sage 上では実装されていない計算例を紹介する。内容的には3章の続きであるが、プラットフォームは Magma に移しておく。

4.1 虚二次体上の Serre の保型性予想とその検証

古典的保型形式は、2次元上半平面 \mathcal{H} とカスプ $\mathbb{P}^1(\mathbb{Q})$ の合併空間 $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ 上の正則関数として定義された。この一般化として、3次元上半空間上の実解析的関数を考えることが出来るが、これから定義する Bianchi 保型形式はこのような関数のことである。

まず、3次元双曲空間 (hyperbolic 3-space)

$$\mathcal{H}_3 = \mathbb{C} \times \mathbb{R}^+ = \{(z, r) \in \mathbb{C} \times \mathbb{R} \mid r > 0\} = \{(x, y, r) \in \mathbb{R}^3 \mid r > 0\}$$

には次のような計量 (= hyperbolic metric) が入る。

$$ds^2 = \frac{dx^2 + dy^2 + dr^2}{r^2}$$

さらに \mathcal{H}_3 には $\mathrm{SL}_2(\mathbb{C})$ が次のように作用する。

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}), \quad g(z, r) = \left(\frac{(az + b)(\bar{c}z + \bar{d}) + a\bar{c}r^2}{|cz + d|^2 + |c|^2r^2}, \frac{r}{|cz + d|^2 + |c|^2r^2} \right)$$

この作用はカスプ $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ に伸び、 $\mathcal{H}_3^* = \mathcal{H}_3 \cup \mathbb{P}^1(\mathbb{C})$ 上の作用となることに注意しよう⁵。

さて、古典的保型形式論における modular 群に相当するものとして、基礎体 $K = \mathbb{Q}(\sqrt{-d})$ の整数環 \mathcal{O}_K を行列の成分に持つ $\mathrm{PSL}_2(\mathbb{C})$ の部分群 $\mathrm{PSL}_2(\mathcal{O}_K)$ を考えるのは自然であろう。この群を Bianchi 群と呼ぶ。それでは、 $\mathrm{PSL}_2(\mathcal{O}_K)$ の合同部分群を定義しよう。

定義 4.1. \mathcal{I} を \mathcal{O}_K のイデアルとする。 Γ は $\mathrm{PSL}_2(\mathcal{O}_K)$ の有限指数の部分群であって

$$\Gamma(\mathcal{I}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\mathcal{I}} \right\}$$

を含むものとする。このとき Γ は レベル \mathcal{I} の合同部分群 (congruence subgroup) であるという。特に次の2つが重要である。

- $\Gamma_0(\mathcal{I}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{\mathcal{I}} \right\}$.
- $\Gamma_1(\mathcal{I}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{\mathcal{I}} \right\}$.

⁵この作用は一見複雑に見えるが、実は modular 群の作用 (一次分変換) の自然な一般化になっている。まず \mathbb{H} をハミルトンの四元数体 (Hamilton's quaternion) とし、その標準 \mathbb{R} -基底を $\{1, i, j, k\}$ とすると、写像 $h: \mathcal{H}_3 \rightarrow \mathbb{H}$ を $h((z, r)) = p = z + rj$ と定義することによって、 \mathcal{H}_3 を \mathbb{H} の部分集合とみなすことが出来る。これによって p に上の g を作用させると $g(p) = (ap + b)/(cp + d)$ が成り立つ。しかも $-I \in \mathrm{SL}_2(\mathbb{C})$ は \mathcal{H}_3 に自明に作用することから、 $\mathrm{PSL}_2(\mathbb{C})$ が \mathcal{H}_3 上に一次分変換で作用していることが分かる。

続いて係数加群 (coefficient module) を導入する. R を 1 を含む可換環とし, $E_k(R)$ を k 次の 2 変数 R -係数斉次多項式のなす空間とする. この空間の R -基底は

$$\{X^{k-i}Y^i \mid 0 \leq i \leq k\}$$

で与えられる. ここで Steinberg の仕事 [15] によって, \mathbb{C} 上の $\mathrm{SL}_2(K)$ の既約表現は次の形で与えられることが知られている.

$$E_{k_1, k_2}(\mathbb{C}) = E_{k_1}(\mathbb{C}) \otimes \overline{E}_{k_2}(\mathbb{C})$$

ここに 2 つ目の overline は複素共役を表す. また, l を \mathcal{O}_K で分解する素数とする ($l = \lambda\bar{\lambda}$ と分解しているとする) と, 先程の [15] と Brauer-Nesbitt の仕事 [1] によって, \mathbb{F}_l 上の $\mathrm{SL}_2(\mathcal{O}_K/l)$ の既約表現は次の形で与えられることが知られている.

$$E_{k_1, k_2}(\mathbb{F}_l) = E_{k_1}(\mathbb{F}_l) \otimes \overline{E}_{k_2}(\mathbb{F}_l)$$

ここに 2 つ目の overline は mod $\bar{\lambda}$ reduction の意味, つまり $\mathrm{SL}_2(\mathcal{O}/(\bar{\lambda}))$ が作用していることを表している.

それでは Bianchi 保型形式を定義する.

定義 4.2. f がレベル \mathcal{I} , 重さ (k_1, k_2) の Bianchi 保型形式 (Bianchi modular form) であるとは, f が 1 次元コホモロジー $H^1(\Gamma(\mathcal{I}), E_{k_1, k_2}(\mathbb{C}))$ に属するコホモロジー類であることをいう.

同様に mod l Bianchi 保型形式も定義される.

定義 4.3. f がレベル \mathcal{I} , 重さ (k_1, k_2) の mod l Bianchi 保型形式であるとは, f が 1 次元コホモロジー $H^1(\Gamma(\mathcal{I}), E_{k_1, k_2}(\overline{\mathbb{F}_l}))$ に属するコホモロジー類であることをいう.

なお, 上述のコホモロジーの cuspidal part を Bianchi 尖点形式 (Bianchi cuspform) と呼ぶ.

それでは虚二次体 $K = \mathbb{Q}(\sqrt{-d})$ 上の Serre 予想のステートメントを述べる. 都合上 $\mathrm{PSL}_2(\mathcal{O}_K)$ の代わりに $\mathrm{SL}_2(\mathcal{O}_K)$ を用いることにし, 記号は以下の通りとする.

- R : 1 を含む可換環.
- $\alpha = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$, 但し π は \mathcal{O}_K の素元.
- $\Gamma \subset \mathrm{SL}_2(\mathcal{O}_K)$: 合同部分群.
- $\Gamma_\alpha = \Gamma \cap \alpha^{-1}\Gamma\alpha$, $\Gamma^\alpha = \Gamma \cap \alpha\Gamma\alpha^{-1}$.
- V : 右 $R[\mathrm{Mat}_2(\mathcal{O}_K)_{\det \neq 0}]$ -加群.

この時, コホモロジー $H^m(\Gamma, V)$ 上の Hecke 作用素は, 次のように $\Gamma_\alpha, \Gamma^\alpha$ のコホモロジーを經由して定義される.

$$H^m(\Gamma, V) \xrightarrow{\text{restriction}} H^m(\Gamma_\alpha, V) \xrightarrow{\tilde{\alpha}} H^m(\Gamma^\alpha, V) \xrightarrow{\text{transfer}} H^m(\Gamma, V)$$

ここで真ん中の写像 $\tilde{\alpha}$ は, コサイクル $c \in H^m(\Gamma_\alpha, V)$ を用いて

$$c \mapsto (g \mapsto c(\alpha^{-1}g\alpha)\det(\alpha)\alpha^{-1})$$

で定義される. もう少し explicit に書き出してみると

$$(T_\pi c)(g) = \sum_{1 \leq i \leq m} c(\gamma_{j(i)}^{-1}g\gamma_i)\det(\gamma_i)\gamma_i^{-1}$$

となる. ここで γ_i は

$$\Gamma\alpha\Gamma = \bigsqcup_{1 \leq i \leq m} \gamma_i\Gamma$$

で定まり, 添え字 $j(i)$ は任意の $g, \gamma_i \in \Gamma$ に対して唯一つ定まる.

また, 以上の操作を α の代わりに $\beta = \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}$ で行って定義される Hecke 作用素を S_π とおく.

定義 4.4. \mathbb{F} を標数 l の体とする (l は 0 または素数). $f \in H^1(\Gamma(\mathcal{I}), E(\mathbb{F}))$ が固有形式 (eigenform) であるとは, 任意の $n \geq 1$ に対してある $c_n \in \mathbb{C}$ が存在して

$$T_n(f) = c_n f$$

と書けることをいう.

予想 4.5. 絶対既約な mod l Galois 表現 $\rho : G_K \rightarrow \text{GL}_2(\mathbb{F})$ は mod l Bianchi 尖点形式から来る. 即ち, ある $f \in H_{cusp}^1(\Gamma(\mathcal{I}), E(\mathbb{F}))$ が存在し, ρ が不分岐な任意の素点 $\lambda \nmid l\mathcal{I}$ に対して次が成り立つ.

$$\boxed{\text{Tr}(\rho(\text{Frob}_\lambda)) = a_\lambda}, \det(\rho(\text{Frob}_\lambda)) = b_\lambda N(\lambda) .$$

ここで a_λ, b_λ はそれぞれ T_λ, S_λ の固有値

$$T_\lambda f = a_\lambda f, \quad S_\lambda f = b_\lambda f$$

を表し, $N(\lambda)$ は \mathbb{Q} 上の λ のノルムである. また $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$ とする.

補足 4.6. 上の形の予想は, 有理数体上の予想における “weak version” にあたる. では同様に “refined version” を提唱出来ないか? と考えるのは自然であるが, 対応が示唆されているのは今の所レベルだけであり, 重さについては定式化がなされていない (有理数体上の場合とは違い, 重さは 2 つの整数のペア (k, l) であるから, Galois 表現の Serre weight とは (このままでは) 比較出来ない). そのためレベルだけを指定した “intermediate version” として予想の定式化が考えられている.

それでは計算例に移ろう。Bianchi 保型形式の計算プログラムは Grunewald や Şengün によってプロトタイプが公開され、現在でも研究され続けているが、Magma のバージョン 2.16 (本稿執筆時の最新バージョンは 2.18) から標準パッケージとして搭載され、容易に扱えるようになった。とはいえこちらも完全版ではなく、多くの伸びしろを残した状態で機能拡充の余地がある。現時点では尖点形式 (重さの指定は不可) に関するものとその Hecke 作用素絡みの計算が可能となっている。

まずは Bianchi 尖点形式 $H_{cusp}^1(\Gamma_0(\mathcal{O}_{-d}), E_2(\mathbb{C}))$ を構成する。Magma 標準搭載のパッケージでは重さ 2 のものしか扱えないため、引数は基礎体 $K = \mathbb{Q}(\sqrt{-d})$ とレベルの情報を持つイデアル \mathcal{I} の 2 つである。なお \mathcal{O}_{-d} は K の整数環を表す。

```
> P<x> := PolynomialRing(Rationals());
> K := NumberField(x^2+14);
> OK := Integers(K);
> level := 1*OK;
> M := BianchiCuspForms(K, level);
> M;
Cuspidal space of Bianchi modular forms over Number Field
  with defining polynomial x^2 + 14 over the Rational Field
  Level = Ideal of norm 1 generated by ( [1, 0] )
  Weight = 2
> time Dimension(M);
0
Time: 4.980
```

なお Verbose Output の設定を最初に変更しておく、BianchiCuspForms コマンドを実行した際に何が計算されたかのログが追加出力される。

```
> SetVerbose("Bianchi",2);
Found perfect form.
Finding 3-dimensional cells.
  Found 9 3-dimensional cells.
Finding 2-dimensional cells.
  Found 23 2-dimensional cells.
Finding 1-dimensional cells.
  Found 14 1-dimensional cells.
```

Magma のパッケージでは perfect form や Voronoi 多面体といった組み合わせ論的アイデアを用いて Bianchi 保型形式の計算を行っている。これは 2 章の最後で少し紹介した modular symbol の理論の一般化のアイデアによるもので、A. Ash や P. Gunnells などによって行われたコホモロジー類の計算と Hecke action の考察に基づいて設計されている。

続いて素イデアル $\mathfrak{p} \mid (3)$ を考え、レベル $\mathcal{I} = \mathfrak{p}^2$ を持つ Bianchi 保型形式を与えてみる。基礎体は上と同じものを使う。

```

> level := (Factorization(3*OK)[1][1])^2;
> Norm(level);
9
> time M9 := BianchiCuspForms(K, level);
Time: 7.300
> M9;
Cuspidal space of Bianchi modular forms over Number Field
  with defining polynomial z^2 + 14 over the Rational Field
  Level = Ideal of norm 9 generated by ( [9, 0], [5, 2] )
  Weight = 2
> Dimension(M9);
1

```

ここで素イデアル $\mathfrak{q} \mid (23)$ を考え、上の空間 M_9 に Hecke 作用素 $T_{\mathfrak{q}}$ を作用させると次のようになる。

```

> Q:=Factorization(23*OK); Q;
[
  <Prime Ideal of OK
  Two element generators:
    [23, 0]
    [3, 1], 1>,
  <Prime Ideal of OK
  Two element generators:
    [23, 0]
    [20, 1], 1>
]
> HeckeOperator(M9, Q[1,1]);
[8]

```

\mathfrak{q} を別の素イデアル $\mathfrak{q}' \mid (23)$ に取りかえてみよう。

```

> Q[2,1];
Prime Ideal of OK
Two element generators:
  [23, 0]
  [20, 1]
> HeckeOperator(M9, Q[2,1]);
[-8]

```

さて、先程も述べたが、Magma 搭載のパッケージでは重さの指定が出来ない。重さ 2 (正確には重さ (2, 2) のこと) 以外の尖点形式を扱うには Grunewald-Şengün によるアルゴリズムを用いる。行列計算がメインとなるため計算時間を要するが、アイデアは本節で説明した内容そのものであり、コードを追うのは容易であろう。但しソースコードは非常に長く、掲載するのは得策ではないと思われるので、計算結果の例を挙げるにとどめておく。例として基礎体を $K = \mathbb{Q}(\sqrt{-2})$ として $T(\mathcal{P}) \curvearrowright H^1(\Gamma_0(\mathcal{I}), E_{3,3}(\mathbb{C}))$, $N(\mathcal{I}) = 3$, $N(\mathcal{P}) < 100$ を計算すると以下のようなになる。

| \mathcal{P} | eigenvalue | |
|--------------------|------------|--------|
| $1 \pm \sqrt{-2}$ | -14 | 6 |
| $3 \pm \sqrt{-2}$ | -46 | -26 |
| $3 \pm 2\sqrt{-2}$ | -574 | 226 |
| $1 \pm 3\sqrt{-2}$ | 434 | 134 |
| $3 \pm 4\sqrt{-2}$ | -1246 | 994 |
| $5 \pm 3\sqrt{-2}$ | -3502 | -1882 |
| $3 \pm 5\sqrt{-2}$ | -238 | -5018 |
| $7 \pm 3\sqrt{-2}$ | -5134 | 8006 |
| $1 \pm 6\sqrt{-2}$ | 9506 | 386 |
| $9 \pm \sqrt{-2}$ | 11186 | -2234 |
| $9 \pm 2\sqrt{-2}$ | 5474 | -10046 |
| $5 \pm 6\sqrt{-2}$ | -9982 | 8738 |

このうち、例えば一番上の $T(1 \pm \sqrt{-2})$ の Hecke 作用素は

```
[
      -14      0      0      0
[      16*w + 1      6      0      0
[1/2*(-97*w + 512)      0      6      16]
[      0      0      0      -14]
```

と計算されるので、この特性多項式を求めて

```
[
  <$ .1 - 6, 2 >,
  <$ .1 + 14, 2 >
]
```

となり、固有値のリスト $[6, -14]$ が得られる。なお、上の w という文字は

```
> K<w> := QuadraticField(-2);
```

から来ている。

この方面の研究で現在最も進んでいる例としては A_5 -拡大の場合の計算例が [10] にあり、ここでも実際に Galois 表現との対応例（と予想されるもの）を考察している。ここでは

- Galois 表現の連続性から、 L が K の有限次拡大体の時ある a が存在して、埋め込み

$$\rho : \text{Gal}(L/K) \hookrightarrow \text{GL}_2(\mathbb{F}_{p^a})$$

が構成出来る。

- $A_5 \simeq \text{SL}_2(\mathbb{F}_4)$ である。
- 更に $\text{GL}_2(\mathbb{F}_4) \hookrightarrow \text{GL}_2(\overline{\mathbb{F}}_2)$ と埋め込める。

ことを使って, mod 2 Galois 表現

$$\rho: \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_2)$$

を構成出来るので, 従って mod 2 コホモロジーを計算することで対応する Bianchi 保型形式を探ることが出来るだろう, というアイデアをとっている.

なお, 上の [10] で対応が示唆されているのは $K = \mathbb{Q}(\sqrt{-1})$ の場合で

$$f(x) = x^5 + (-1 + 2\sqrt{-1})x^4 + (-6 + 2\sqrt{-1})x^2 + (-4 - 7\sqrt{-1})x - 3\sqrt{-1} \in K[x]$$

で K 上定義される Galois 表現 (A_5 -Galois 拡大, $N(\rho) = (2 - \sqrt{-1})^2(2 + \sqrt{-1})^3$) と, mod 2 Bianchi 保型形式

$$H^1(\Gamma_0((2 - \sqrt{-1})^2(2 + \sqrt{-1})^3), \mathbb{F}_2)$$

であり, 次項に示すように 1 つめの eigenvalue system と一致している. ここで w は $x^2 + x + 1 \in \mathbb{F}_4[x]$ の根とする.

| \mathcal{P} | $N(\mathcal{P})$ | $\text{Tr}(\rho(\text{Frob}_{\mathcal{P}}))$ | eigenvalue | |
|------------------|------------------|--|------------|-------|
| $3 + 2\sqrt{-1}$ | 13 | 1 | 1 | 1 |
| $3 - 2\sqrt{-1}$ | 13 | w^2 | w^2 | w |
| $4 + \sqrt{-1}$ | 17 | w | w | w^2 |
| $4 - \sqrt{-1}$ | 17 | 0 | 0 | 0 |
| $6 + \sqrt{-1}$ | 37 | 1 | 1 | 1 |
| $6 - \sqrt{-1}$ | 37 | w | w | w^2 |
| $5 + 4\sqrt{-1}$ | 41 | w^2 | w^2 | w |
| $5 - 4\sqrt{-1}$ | 41 | w | w | w^2 |
| $7 + 2\sqrt{-1}$ | 53 | 1 | 1 | 1 |
| $7 - 2\sqrt{-1}$ | 53 | 1 | 1 | 1 |
| $6 + 5\sqrt{-1}$ | 61 | w | w | w^2 |
| $6 - 5\sqrt{-1}$ | 61 | w | w | w^2 |
| $8 + 3\sqrt{-1}$ | 73 | w^2 | w^2 | w |
| $8 - 3\sqrt{-1}$ | 73 | w | w | w^2 |
| $8 + 5\sqrt{-1}$ | 89 | 0 | 0 | 0 |
| $8 - 5\sqrt{-1}$ | 89 | w^2 | w^2 | w |
| $9 + 4\sqrt{-1}$ | 97 | 1 | 1 | 1 |
| $9 - 4\sqrt{-1}$ | 97 | w^2 | w^2 | w |

一方, Bianchi 保型形式を古典的保型形式に倣って modular symbol の形で表現出来ないかという方面の研究も考えられる (先ほども少し触れた generalized modular symbol の計算). これについては Cremona [2] によって, 双曲空間の mosaic 細工 (hyperbolic tessellation) を用いた先行研究があり, その後 Cremona の学生数人⁶によって, 特別な基礎体の場合に対する考察がなされている.

⁶E. Whitley (1990), J. Bygott (1999), M. Lingham (2005) の 3 名. Whitley と Bygott は Exeter で, Lingham は Nottingham にて Ph.D. を取得している. Whitley は類数 1 の虚二次体を, Bygott は $K = \mathbb{Q}(\sqrt{-5})$ を, Lingham は $K = \mathbb{Q}(\sqrt{-23})$, $\mathbb{Q}(\sqrt{-31})$ をそれぞれ考察している.

4.2 付録「Hilbert 保型形式とその計算」

最後に付録として、古典的保型形式からの一般化として最も良く知られている Hilbert 保型形式についてその計算例と共に紹介する。なお、ここでは簡単な定義やその性質について触れるのみとし、一切の詳細は省いている。必要に応じて適宜文献を参照されたい。

Hilbert 保型形式 (Hilbert modular form) とは、簡潔には上半平面に属する $n = \deg(F/\mathbb{Q})$ 個の複素変数を持ち、総実代数体 (totally real field) F の元を成分に持つ 2×2 行列に対して、古典的保型形式とほぼ同様の関係式を満足するものである。多変数化によって難しくなったように感じるかもしれないが、要するに基礎体を \mathbb{Q} から総実代数体 F へ、群作用を $\mathrm{PSL}_2(\mathbb{Z})$ から $\mathrm{GL}_2^+(\mathcal{O}_F)$ へ一般化したものである。

なお、Hilbert 保型形式は総実代数体上の Serre 予想において Galois 表現の対応物として有力視されている。今現在 Serre 予想の一般化の中では最も解決に近いと思われており、代数幾何的手法を用いて研究が進んでいる。

それでは実際に Hilbert 保型形式を計算してみよう。まず総実代数体を $F = \mathbb{Q}(\sqrt{43})$ と定義し、 F 上の Hilbert 尖点形式を構成する。

```
> P<x> := PolynomialRing(Rationals());
> F := NumberField(x^2-43);
> level := 1*Integers(F);
> H := HilbertCuspForms(F, level);
> H;
Cuspidal space of Hilbert modular forms over Number Field with defining
polynomial x^2 - 43 over the Rational Field
  Level = Ideal of norm 1 generated by ( [1, 0] )
  Weight = [ 2, 2 ]
```

この尖点形式は上半平面に属する 2 個の複素変数を持っていることが読み取れる。なお空間の次元は \mathbb{C} 上 10 次元である。

```
> Dimension(H);
10
```

続いて基礎体を $F = \mathbb{Q}(\sqrt{2})$ に、レベルを $\mathcal{I}(19) \subset \mathcal{O}_F$ に取りかえてから、空間の次元の計算にかかる時間を計測してみよう。

```
> F := NumberField(x^2-2);
> OF := RingOfIntegers(F);
> level := Factorization(19*OF)[1][1];
> H19 := HilbertCuspForms(F, level);
> time Dimension(H19);
16
Time: 0.820
```

ところで Hilbert 保型形式の計算には “quaternion order” と呼ばれるものが internal に使われている。計算に際して時間を要するのはこの部分であり、Hilbert 保型形式のレベルに

よるものではない。そのため、一度基礎体を固定して異なるレベルで同様の計算を行う場合は、QuaternionOrder コマンドを用いてセーブしておき、必要な時に呼び出すようにしておけば計算時間を大幅に短縮出来る。例えば直前の次元の計算を行う場合は次のようにすれば良い。

```
> Q0 := QuaternionOrder(H19); Q0;
Order of Quaternion Algebra with base ring F
with coefficient ring Maximal Order of Equation Order with defining
polynomial x^2 - 2 over its ground order
> H19Q := HilbertCuspForms(F, level : QuaternionOrder:=Q0 );
> time Dimension(H19Q);
16
Time: 0.100
```

計算時間が 1/8.2 と格段に抑えられていることが読み取れる。

続いて Hecke 作用素の計算に入ろう。直前で計算した H19 (乃至 H19Q) に対して Hecke 作用素 T_2 を作用させてみる。

```
> T2 := Factorization(2*OF)[1][1];
> HeckeOperator(H19, T2);
[ 0 0 0 0 1 0 1 0 0 0 1 0 0 0 0 0]
[ 0 0 0 0 0 1 0 1 0 0 1 0 0 0 0 0]
[ 0 0 0 0 0 0 0 0 1 0 1 0 0 0 3 0]
[ 0 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0]
[ 1 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0]
[-1 0 -1 0 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 0 -1 -1 0 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 0 1 0 0 0 0 0 2 0 0 0 0 0 0 0 0]
[ 0 0 1 0 0 0 0 0 0 0 0 2 0 0 0 0]
[-1 -1 -1 0 -1 -1 -1 -1 -1 -1 -1 -1 0 -1 -1 -1]
[ 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0]
[ 0 0 0 0 0 0 0 0 2 0 0 0 1 0 0 0]
[ 0 0 0 0 0 0 0 0 0 1 0 1 0 2 0 0]
[ 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 2]
[ 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0]
[ 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1]
```

最後は固有形式の計算を行う。ここでは例として Hilbert 保型形式 H19 のニューフォームが $\mathbb{Q}(\sqrt{2})$ 上の楕円曲線で導手が 19 のものから来ており、それが \mathbb{Q} 上の楕円曲線から得られていることを見てみよう。まず H19 の分割を行う。

```
> decomp := NewformDecomposition(NewSubspace(H19)); decomp;
[*
  New cuspidal space of Hilbert modular forms of dimension 1
  over Number Field with defining polynomial x^2 - 2
  over the Rational Field
```

```

Level = Ideal of norm 361 generated by ( [19, 0] )
New at Ideal of norm 361 generated by ( [19, 0] )
Weight = [ 2, 2 ],
New cuspidal space of Hilbert modular forms of dimension 1
over Number Field with defining polynomial x^2 - 2
over the Rational Field
Level = Ideal of norm 361 generated by ( [19, 0] )
New at Ideal of norm 361 generated by ( [19, 0] )
Weight = [ 2, 2 ],
New cuspidal space of Hilbert modular forms of dimension 6
over Number Field with defining polynomial x^2 - 2
over the Rational Field
Level = Ideal of norm 361 generated by ( [19, 0] )
New at Ideal of norm 361 generated by ( [19, 0] )
Weight = [ 2, 2 ],
New cuspidal space of Hilbert modular forms of dimension 8
over Number Field with defining polynomial x^2 - 2
over the Rational Field
Level = Ideal of norm 361 generated by ( [19, 0] )
New at Ideal of norm 361 generated by ( [19, 0] )
Weight = [ 2, 2 ]

```

*]

このうち 2 番目の 1 次元空間に注目する.

```

> f := Eigenform(decomp[2]);
> primes := [P : P in PrimesUpTo(50,F) | IsOdd(Norm(P)) and IsPrime(Norm(P))];
> for P in primes do
>   Norm(P), HeckeEigenvalue(f,P);
> end for;
7 -1
7 -1
17 -3
17 -3
23 0
23 0
31 -4
31 -4
41 -6
41 -6
47 -3
47 -3

```

一方, レベル 19 の古典的保型形式 (つまり導手 19 の \mathbb{Q} 上の楕円曲線から来る) から全くと同じ固有値のリストが得られる.

```

> fQ := Newforms(CuspForms(19))[1][1];
> for P in primes do
>   p := Norm(P);
> p, Coefficient(fQ, p);

```

```
> end for;
7 -1
7 -1
17 -3
17 -3
23 0
23 0
31 -4
31 -4
41 -6
41 -6
47 -3
47 -3
```

参考文献

- [1] R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2), **42** (1941), 556-590.
- [2] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math., **51** (1984), 275-324.
- [3] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, Second Edition (1997).
- [4] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag (2005).
- [5] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), 563-594.
- [6] J. Franke, *Harmonic analysis in weighted l_2 -spaces*, Ann. Sci. École Norm. Sup. (4), **31** (1998), 181-279.
- [7] R. S. Kulkarni, *An arithmetic-geometric method in the study of the subgroups of the modular group*, Amer. J. Math., **113** (6) (1991), 1053-1133.
- [8] C. Khare, J.-P. Wintenberger, *Serre's modularity conjecture I,II*, 2007, preprint.
- [9] T. Miyake, *Modular forms*, Springer-Verlag, Berlin (1989), Translated from the Japanese by Yoshitaka Maeda.
- [10] M. H. Şengün, *A numerical study of mod p Bianchi modular forms and Galois representations*, preprint.
- [11] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York (1973).

- [12] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Mathematical Journal **54** (1987), 179-230.
- [13] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, **11**, Tokyo (1971).
- [14] W. Stein, *Modular Forms: A Computational Approach*, with an appendix by P. Gunnells, AMS Graduate Studies in Mathematics, Vol. 79 (2007).
- [15] R. Steinberg, *Tensor Product theorems*, in The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), vol. 47 of Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, 1987, 331-338.
- [16] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes in Math. **1240** (1984), 275-280.
- [17] T. Saito, G. Yamashita and S. Yasuda, *Recent progressions on $R=T$* , volume 1 and 2, Proceedings available at: <http://www.kurims.kyoto-u.ac.jp/~gokun/R=T.html>.

Shun'ichi Yokoyama
Graduate School of Mathematics, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail Address: s-yokoyama@math.kyushu-u.ac.jp