様式 C-19

科学研究費補助金研究成果報告書

平成２１年　４月１７日現在

研究種目：若手研究（B）
研究期間：2007 年度　～　2008 年度
課題番号：１９７４０００６
研究課題名（和文）アーベル多様体の代数幾何学的・数論的研究と暗号理論への応用
研究課題名（英文）Algebro-geometrical and number-theoretical study of Abelian Varieties and its applications to cryptography
研究代表者
小池　健二（KOIKE　KENJI）
山梨大学・教育人間科学部・准教授
研究者番号：２０３６２０５６

研究成果の概要：虚２次体が作用する４次元アーベル多様体の族を考え、その族の中でアーベル曲面の直積に退化した場合の Weil class を対角成分と直積成分で、具体的に表現した。６点で分岐する射影直線の巡回３重被覆は、種数４の代数曲線の族になるが、その族に対し周期写像を考察した。周期領域は４次元Ｉ型領域で、IV 型領域とも同型である。この同型をモジュラー群の作用込で具体的に調べ、テータ関数の Thomae の公式を導いた。また、モジュラー群の合同部分群による商群も考察した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	500,000	0	500,000
2008 年度	500,000	150,000	650,000
年度			
年度			
年度			
総　計	1,000,000	150,000	1,150,000

研究分野：数物系科学
科研費の分科・細目：数学・代数学
キーワード：代数幾何

１．研究開始当初の背景
(1) Hodge 予想は代数幾何学の重要な未解決問題である。３次超曲面、Fermat 超曲面、Abel 多様体等に関しては、正しい事が検証された例が散発的に存在するが、代数性が証明されていない Hodge サイクルの例も数多く構成されている。典型的な例としては、Weil が構成した、ある種の虚数乗法を持つアーベル多様体上の非自明なサイクル（Weil - Hodge クラス）がある。特殊な場合には Weil - Hodge クラスの代数性が証明されているが、より一般の場合に検証する事は一つの問題となっている。

(2) 楕円曲線のモジュライから楕円保形関数が得られるように、アーベル多様体のモジュライを考える事により、Siegel保型形式が得られるが、高次元の保型関数は、一変数の場合程は研究されていない。例えばSiegel保型形式に成す次数付き環の構造は、高次の場合は知られていない。しかしながら近年、代数曲線、K3曲面、3次超曲面等のモジュライ空間を、IV型領域や複素超球(I型領域)上の算術商として構成する研究が進展し、それに伴いBo

rcherdsの無限積を用いて多変数保形関数が構成等されている。

２．研究の目的
(1) ４次元アーベル多様体の Weil - Hodge クラスの代数性を複数の虚２次体の場合について検証する。

(2) 配置空間等に付随したアーベル多様体の PEL - family やＫ３曲面の族を考え、そのモジュライ空間上の保型関数を構成する。

３．研究の方法
(1) 虚２次体に対する Weil 型の４次元アーベル多様体の具体的な族を考え、アーベル曲面の直積に退化したファイバーで、Weil - Hodge クラスを表現するような、代数的サイクルの構成を試み、その変形を考察する。

(2) ６点で分岐する射影直線の巡回３重被覆は、種数４の代数曲線の族になる。この族に対し、周期写像の逆写像として、Ｉ型領域上の保型関数を構成する。対応するＩ型領域は４次元で、曲線は３次元族であるが、曲線の周期に対しては Thomae 型の公式を導く事により、曲線のパラメータである分岐点の cross-ratio とテータ関数の関係を記述出来ると考えられる。

４．研究成果
(1) 行列

$$\Omega = \left[\begin{array}{cc|cc} \tau_1 & \tau_2 & 0 & \tau_4 \\ \tau_2 & \tau_3 & -\tau_4 & 0 \\ \hline 0 & -\tau_4 & N\tau_1 & N\tau_2 \\ \tau_4 & 0 & N\tau_2 & N\tau_3 \end{array}\right]$$

は条件

$\mathrm{Im}\,\tau_1 > 0$,
$(\mathrm{Im}\,\tau_1)(\mathrm{Im}\,\tau_3)-(\mathrm{Im}\,\tau_2)^2-(\mathrm{Im}\,\tau_4)^2/N > 0$

を満たすとき、Siegel 上半空間に属する。
４次元複素線形空間$\mathbf{C}^4$の単位ベクトル γ_1, γ_2, γ_3, γ_4及び、Ωの列ベクトル γ_5, γ_6, γ_7, γ_8が生成する格子が定める４次元アーベル多様体Ａ(Ω)には、非自明な準同型

$(z_1, z_2, z_3, z_4) \to (-Nz_3, -Nz_4, z_1, z_2)$

があり、これは$\sqrt{-N}$乗法を与え、これによりＡ(Ω)は Weil type になる事が分かる。

このアーベル多様体の族に対し、以下の結果を得た。
$\gamma_1,\cdots,\gamma_8$を$H_1(A(\Omega),\mathbf{Z})$の基底と考え、その双対基底となる$H^1_{dR}(A(\Omega),\mathbf{R})$の元を$\omega_1,\cdots,\omega_8$とする。このときＡ(Ω)の Weil-Hodge class は、

$$\Phi_1 = N\omega_{1256} - \omega_{3456} - N\omega_{2367} + N\omega_{1467} + N\omega_{2358} - N\omega_{1458} - N^2\omega_{1278} + N\omega_{3478}$$

及び

$$\Phi_2 = -\omega_{2356} + \omega_{1456} - N\omega_{1267} + \omega_{3467} + N\omega_{1258} - \omega_{3458} + N\omega_{2378} - N\omega_{1478}$$

の有理数係数１次結合となる。ただし

$\omega_{ijkl} = \omega_i \wedge \omega_j \wedge \omega_k \wedge \omega_1$

であるとする。
$\tau_4 = 0$ のときは、Ａ(Ω) はアーベル曲面の直積$B_1 \times B_2$ であるが(B_1は周期行列

$$\tau = \begin{vmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{vmatrix}$$

が定めるアーベル曲面であり、B_2は$N\tau$が定めるアーベル曲面)、このとき、

$\Phi_1 = [\Delta_+]+[\Delta_-]+2(N+1)([B_1] + N[B_2])$

となる。ここで、Δ_+は

$B_1 \to B_1 \times B_2, \quad z \to (z, Nz)$

の像であり、Δ_-は

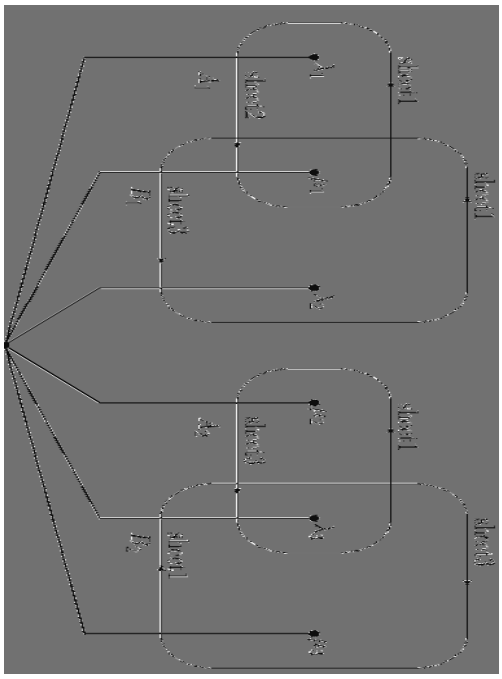
$B_1 \to B_1 \times B_2, \quad z \to (z, -Nz)$

の像である。

(2) λ_i, μ_i (i=1,2,3) をパラメータとする代数曲線 C : $y^3 = f(x)g(x)^2$,
$f(x)=(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$
$g(x)=(x-\mu_1)^2(x-\mu_2)^2(x-\mu_3)^2$,
は、射影直線の６点で分岐する巡回３重被覆であり、種数４の代数曲線となる。$H^{1,0}(C)$の基底として

$\phi_1 = dx/y, \quad \phi_2 = xdx/y,$
$\phi_3 = g(x)dx/y^2, \quad \phi_4 = xg(x)dx/y^2,$

をとり、$H_1(C,\mathbf{Z})$の基底として、次の図の様なサイクルをとる。



これ等の基底に関して、周期行列は

$$\begin{aligned}&\begin{bmatrix}{}^t\Omega_2 & {}^t\Omega_1\end{bmatrix}\\ &=\begin{bmatrix}\int_{B_1}\varphi_1 & \cdots & \int_{B_4}\varphi_1 & \int_{A_1}\varphi_1 & \cdots & \int_{A_4}\varphi_1\\ \vdots & & \vdots & \vdots & & \vdots\\ \int_{B_1}\varphi_4 & \cdots & \int_{B_4}\varphi_4 & \int_{A_1}\varphi_4 & \cdots & \int_{A_4}\varphi_4\end{bmatrix}\\ &=\begin{bmatrix}{}^tZ_2 & -\omega^tZ_2 & {}^tZ_1 & \omega^{2t}Z_1\\ {}^tW_2 & -\omega^{2t}W_2 & {}^tW_1 & \omega^tW_1\end{bmatrix}\end{aligned}$$

となり、$\Omega = \Omega_2\Omega_1^{-1}$は

$$\Omega=\frac{1}{1-\omega}\begin{bmatrix}Z+{}^tZ & -\omega^2Z-\omega^tZ\\ -\omega Z-\omega^{2t}Z & Z+{}^tZ\end{bmatrix}$$

により与えられる。ここでωは１の３乗根であり、$Z = Z_2Z_1^{-1}$はⅠ型領域

$$\mathbb{H}_{3,2}=\{Z\in \mathrm{GL}_2(\mathbb{C}) \ ; \ \omega^{2t}\bar{Z}+\omega Z<0\}$$

に属す。この領域には Eisenstein 整数環上の離散ユニタリ群

$$\Gamma=\{g\in \mathrm{GL}_4(\mathbb{Z}[\omega]) \ ; \ {}^tgJg=J\}$$
$$\left(J=\begin{bmatrix}0 & \omega^2E_2\\ \omega E_2 & 0\end{bmatrix}\right)$$

が作用する。この群が

(i) *translations*

$$\begin{bmatrix}I & B\\ 0 & I\end{bmatrix},\quad B=\begin{bmatrix}(1-\omega)m_1 & -m_4-\omega m_3\\ m_3+\omega m_4 & (1-\omega)m_4\end{bmatrix}$$
$$(m_1,\cdots,m_4\in\mathbb{Z}),$$

により生成される事を示した。
また、２次形式
が定める IV 型領域

$$\mathbb{D}_T=\{\eta\in\mathbb{P}^3 \ ; \ {}^t\eta T\eta>0,\ {}^t\eta T\eta=0\}$$

$$\begin{bmatrix}A & 0\\ 0 & {}^t\bar{A}^{-1}\end{bmatrix},\quad A\in \mathrm{GL}_2(\mathbb{Z}[\omega]),$$

(iii) *involutions*

$$H=\begin{bmatrix}0 & 0 & \omega^2 & 0\\ 0 & 0 & 0 & \omega^2\\ \omega & 0 & 0 & 0\\ 0 & \omega & 0 & 0\end{bmatrix},\qquad K=\begin{bmatrix}0 & 0 & \omega^2 & 0\\ 0 & 1 & 0 & 0\\ \omega & 0 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

に作用する整数環上の直交群

$$T=\mathrm{U}\oplus\mathrm{U}(3)\oplus\mathrm{A}_2,\quad \mathrm{U}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},$$
$$\mathrm{U}(3)=\begin{bmatrix}0 & 3\\ 3 & 0\end{bmatrix},\quad \mathrm{A}_2=\begin{bmatrix}-2 & 1\\ 1 & -2\end{bmatrix}$$

の生成元も決定し、同型写像

$$\Phi:\mathbb{D}_T^+\longrightarrow\mathbb{H}_{2,2},$$
$$[1:w_2:\cdots:w_4]\mapsto\begin{bmatrix}(1-\omega)w_2 & -\omega w_3-w_4\\ w_3+\omega w_4 & (1-\omega)w_4\end{bmatrix}$$
$$\Gamma'(L)=\{g\in\Gamma(L) \ ; \ g(\mathbb{D}_T^+)=\mathbb{D}_T^+\}$$

がΓの指数２の部分群と、直交群の間の作用と互換性があるモジュラー同型である事を示した。
以下では曲線 C の分岐点を

$$\mu_1 = 0,\quad \mu_2 = 1,\quad \mu_3 = \infty$$

と正規化して考え、対応する C 上の点をP_0, P_1, P_∞で表す。アーベル・ヤコビ写像の基点としてP_0をとると、リーマン定数は

$$\Delta = 2P_0 + 2P_1 - P_\infty$$

で与えられる。
C の自己同型ρの symplectic 表現を、上記の$H_1(C,\mathbf{Z})$の基底に関して具体的に計算して、得られた symplectic 行列をテータ関数の変換公式に適用して、ρ-不変な characteristics で、テータ零値が恒等的に消えないものを求めると、

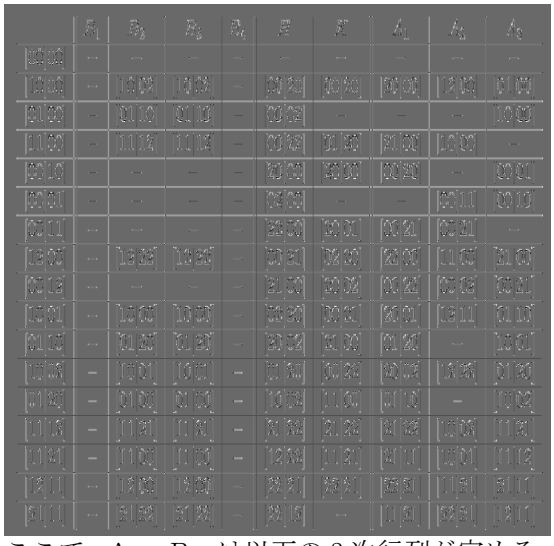
[0, 0|0, 0], [1, 0|0, 0], [0, 1|0, 0], [1, 1|0, 0]
, [0, 0|1, 0], [0, 0|0, 1], [0, 0|1, 1],
[1, 2|0, 0], [0, 0|1, 2], [1, 0|0, 1], [0, 1|1, 0]
, [1, 0|0, 2], [0, 1|2, 0], [1, 1|1, 2],
[1, 1|2, 1], [1, 2|1, 1], [2, 1|1, 1],
及び

[2,0|0,0], [2,0|0,0], [2,2|0,0], [0,0|2,0], [0,0|0,2], [0,0|2,2], [2,1|0,0], [0,0|2,1], [2,0|0,2], [0,2|2,0], [2,0|0,1], [0,2|1,0], [2,2|2,1], [2,2|1,2], [2,1|2,2], [1,2|2,2]

の 33 個を得る。ここで、

$(a_1, a_2, a_1, a_2)/3$　　$(b_1, b_2, -b_1, -b_2)/3$

を$[a_1, a_2|b_1, b_2]$と表した。テータ零値として異なるものは、前半の 17 個になる。またリーマン定数に対応する characteristics は[1,1|2,1]である。これ等の characteristics に上述の Γ の生成元を作用させると次の表を得る。



ここで、A_i, B_i は以下の 2 次行列が定める translation と unimodular 変換である。

$$B_1 = \begin{bmatrix} 1-\omega & 0 \\ 0 & 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0 & -1 \\ \omega & 0 \end{bmatrix},$$
$$B_3 = \begin{bmatrix} 0 & -\omega \\ 1 & 0 \end{bmatrix}, \quad B_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1-\omega \end{bmatrix},$$
$$A_1 = \begin{bmatrix} -\omega & 0 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

最後に、Thomae 型の公式を得たので、いくつか例を述べる。

$$\frac{\lambda_2(\lambda_2-1)}{(\lambda_3-\lambda_1)(\lambda_3-\lambda_2)} = \frac{[01|00]^8}{[00|00]^8}$$

$$\frac{(\lambda_2-1)(\lambda_2-\lambda_3)}{\lambda_3(\lambda_3-\lambda_1)} = \frac{[12|00]^8}{[10|00]^8}$$

$$\frac{(\lambda_3-\lambda_1)(\lambda_3-\lambda_2)}{\lambda_3(\lambda_3-1)} = \frac{[00|00]^8}{[01|00]^8}$$

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① 小池健二、志賀弘典、An extended Gauss AGM and corresponding Picard modular forms、Journal of Number Theory、Vol. 128、pp. 2097-2126、2008 年、査読有

〔その他〕
講演２件

① 小池健二、埼玉大学代数幾何学講演会、「Picard curves and theta constants I, II」、2008 年９月８日、埼玉大学

② 小池健二、香川セミナー、「算術幾何平均と超幾何関数」、2007 年７月２８日、香川大学

６．研究組織
(1)研究代表者

小池　健二（KOIKE　KENJI）
山梨大学・教育人間科学部・准教授
研究者番号：２０３６２０５６

(2)研究分担者

該当無し

(3)連携研究者

該当無し