数理解析研究所講究録
第658巻 1988年 111-128

Abel多様体のCanonical Subgroupについて

東大理学部　市川尚志（Takashi Ichikawa）

序　この小論では、Abel多様体のcanonical subgroupの大域的構成に関する筆者の結果について述べる。偏極、階構造付きの（g次元）Abel多様体のmoduli空間Xと、Xについて良い性質を持つ素数pをとると、上記の構成は"$X(\mathbb{Z}_p)$上の対応で$X(\overline{\mathbb{F}}_p)$上の$q=p^m$乗Frobenius写像$\mathrm{Frob}_q$の持ち上げとなるものの構成"に対応している。このような持ち上げのp進解析的な構成は、$g=1$の時Dwork[2]によってなされているが、それは$X(\mathbb{Z}_p)$上全体で定義されていなかった。

ここでは、（X上のある正規な有限被覆上に構成された）大域的なcanonical subgroup達を用いることにより、一般のgに対し、$X(\mathbb{Z}_p)$上の対応$\mathcal{X}^{(m)}$で$\mathcal{X}^{(m)} \bmod p$が$X_0^o(\overline{\mathbb{F}}_p)$（$X_0^o$：$X_0 = X \otimes \mathbb{F}_p$のordinary locus）上$\mathrm{Frob}_q$を与えるものを構成する。$\mathcal{X}^{(m)}$の剛性は、それが代数幾何的に定義されることから従う。さらに$g=1$の時は、$\mathcal{X}^{(m)} \bmod p$が$X_0(\overline{\mathbb{F}}_p)$上全体で$\mathrm{Frob}_q$を与えるこ

とがわかる。この結果から[5], p.103 における Lubin の予想"混標数を持つ局所環上の楕円曲線は（特に supersingular reduction を持つ時）、潜在的に canonical subgroup を持つ"が肯定的に解かれる。

$\mathcal{X}^{(m)}$ が Frob_q の持ち上げと見なせることから、$\mathcal{X}^{(m)}$ による $X(\overline{\mathbb{Z}}_p)$ の固定点集合 $\mathcal{S}^{(m)}$ と Frob_q による $X_0(\overline{\mathbb{F}}_p)$ の固定点集合 $X_0(\mathbb{F}_q)$ の間に密接な関係が存在することが予想されるが、これについては次のことが成りたつ。まず

$$X^{\circ}(\overline{\mathbb{Z}}_p) = \{ x \in X(\overline{\mathbb{Z}}_p) \mid x \bmod \bar{p} \in X_0^{\circ}(\overline{\mathbb{F}}_p) \}$$

とおくと、canonical lifting の理論より $\bmod \bar{p}$ が全単射

$$X^{\circ}(\overline{\mathbb{Z}}_p) \cap \mathcal{S}^{(m)} \xrightarrow{\sim} X_0^{\circ}(\mathbb{F}_q)$$

を導くことが証明される。これは Dwork[2] の結果（$g=1$）の一般化になっている。また $g=1$ の時には、$\bmod \bar{p}$ は $\mathcal{S}^{(m)}$ から $X_0(\mathbb{F}_q)$ への全単射を与えないにもかかわらず

$$\#(\mathcal{S}^{(m)}) = \#(X_0(\mathbb{F}_q))$$

が成りたつことが証明される。これは $\mathcal{X}^{(m)}$ が与える canonical subgroup が、数論的に意味のあるものであることを示している。

以下では、まず§1で moduli 空間 X を正確に定義し、§2で canonical subgroup の大域的な構成を行う。§3で§2の結果を用いて $X(\overline{\mathbb{Z}}_p)$ 上の対応 $\mathcal{X}^{(m)}$ を定義し、その固定点集合 $\mathcal{S}^{(m)}$

と $X_0(\mathfrak{H}_g)$ の関係を調べる。§4では $S^{(m)}$ の一意化を扱う。証明は概略を述べるにとどめた。

§1. Canonical model

この章では、symplectic代数群から定まる志村のcanonical modelについて復習する。

自然数 g と n を固定し，$n \geqq 3$ と仮定する。$\mathbb{d} = (d_1, \cdots, d_g)$ を $d_1 = 1$, $d_i | d_{i+1}$ $(i = 1, \cdots, g-1)$ を満たす g 個の自然数 d_i からなる横vectorとする。この $\mathbb{d}$ に対し自然数 d と行列 D を以下のように定める：

$$d = \prod_{1 \leq i \leq g} d_g \quad , \quad D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_g \end{pmatrix} 。$$

$\psi : \mathbb{Z}^{2g} \times \mathbb{Z}^{2g} \to \mathbb{Z}$（$\mathbb{Z}$：有理整数環）を行列 $\begin{pmatrix} 0 & -D \\ D & 0 \end{pmatrix}$ によって定義される双1次形式とする。すなわち

$$\psi(e_i, e_j) = e_i \begin{pmatrix} 0 & -D \\ D & 0 \end{pmatrix} {}^t e_j \quad (1 \leqq i, j \leqq 2g)$$

$$\text{ただし} \quad e_i = (0, \cdots, 0, \overset{i}{\check{1}}, 0, \cdots, 0) 。$$

S を $\mathbb{Z}[1/nd]$ 上の scheme とし，A を S 上次元 g を持つ abelian scheme とする。A の S 上の偏極，すなわち A から ${}^tA$（：A のdual abelian scheme）への S 上の同種写像 θ が type $\mathbb{d}$ であるとは，$\mathrm{Ker}(\theta)$ が $\prod_{1 \leqq i \leqq g} (\mathbb{Z}/d_i\mathbb{Z})^2$ と S 上同型になることと定義する。また θ の次数が d であるとは，$\mathrm{Ker}(\theta)$ の位数が d^2 になることとし

て定義する。明らかに θ が type $\mathbb{d}$ ならばその次数は d である。このAと θ に対し、Aの S 上の n 階構造

$$\delta = \{ \delta_i \in {}_nA(S) \mid 1 \leq i \leq 2g \}$$

（ただし ${}_nA := \mathrm{Ker}(n: A \to A)$）が（$\theta$ に関して）similitude-symplectic とは，$\mu_n(S)$（$\mu_n := \mathrm{Ker}(n: \mathbb{G}_m \to \mathbb{G}_m)$）の元 ζ で

$$e_n(\delta_i, \theta(\delta_j)) = \zeta^{\psi(e_i, e_j)} \quad (1 \leq i, j \leq 2g)$$

（ただし $e_n: {}_nA \times {}_n({}^tA) \to \mu_n$ を Weil pairing とする）を満たすものが存在することであるとして定義する。

$\mathbb{Z}[1/nd]$ 上の scheme S に対し，$\underline{X}(S)$ を S 上 g 次元の abelian scheme A，A/S の type $\mathbb{d}$ の偏極 θ，θ に関して similitude-symplectic となる A/S の n 階構造 δ から成る3つ組 (A, θ, δ) の S－同型類のなす集合とする。この時 $\underline{X}$ は $\mathbb{Z}[1/nd]$ 上の sheme のなす圏から集合のなす圏への反変関手を定める。任意の楕円曲線Eは標準的な主偏極 θ を持ち，Eの任意の階構造は θ に関し similitude-symplectic だから，$g=1$（従って $\mathbb{d}=(1)$）の時，$\underline{X}(S)$ は S 上の n 階構造を持つ楕円曲線の S－同型類の集合となる。

さて $\mathbb{Z}[1/nd]$ 上の scheme S に対し，$\underline{Y}(S)$ を S 上 g 次元の abelian scheme A，A/S の次数 d の偏極 θ，A/S の n 階構造 δ から成る三つ組 (A, θ, δ) の S－同型類のなす集合とすると，$\underline{Y}$ は $\mathbb{Z}[1/nd]$ 上の scheme のなす圏から集合のなす圏への反変関

手を定める。いま$n \geq 3$だから，Mumford [7] の結果より，$\underline{Y}$は$\mathbb{Z}[1/nd]$上のある有限型scheme Yによって表現される。従って$\underline{Y}$の部分関手である$\underline{X}$はYの閉部分schemeによって表現される。このschemeを以下$X = X(g, d, n)$で表わす。Grothendieckの結果（[9]，定理2.4.1）より関手$\underline{X}$はformally smoothとなるから，それを表現するscheme Xは$\mathbb{Z}[1/nd]$上smoothとなる。

Xの定義より，複素多様体$X(\mathbb{C})$（$\mathbb{C}$：複素数体）は，商空間

$$G(\mathbb{Q})_+ \backslash H \times G(A_f) / K_n$$

と標準的に同型になる。ただし

H：次数gのSiegel上半空間。

G：交代双1次形式ψより定義されるsimilitude-symplectic代数群。すなわち単位元を持つ可換環Rに対し，$G(R)$は$GL(2g; R)$の元gで

$$(\psi \otimes R)(gv, gw) = \nu(g)\,(\psi \otimes R)(v, w) \quad (v, w \in R^{2g})$$

を満たす$\nu(g) \in R^\times$が存在するものから成る。

$A_f := \hat{\mathbb{Z}} \otimes \mathbb{Q}$（$\mathbb{Q}$：有理数体），ただし$\hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$。

$G(\mathbb{Q})_+ := \{ g \in G(\mathbb{Q}) \mid \nu(g) > 0 \}$。

$K_n := \{ g \in G(\hat{\mathbb{Z}}) \mid g \equiv I \mod n\hat{\mathbb{Z}} \}$。

この時

$$G(\mathbb{Q})_+ \backslash H \times G(A_f) / K_n = \coprod_{g \in G(\mathbb{Q})_+ \backslash G(A_f)/K_n} \Gamma_g \backslash H \quad (\Gamma_g := gK_ng^{-1} \cap G(\mathbb{Q})_+)$$

$$G(\mathbb{Q})_+ \backslash G(A_f) / K_n \cong (\mathbb{Z}/n\mathbb{Z})^\times ,$$

となるから，$X \otimes \mathbb{C}$ は $\#((\mathbb{Z}/n\mathbb{Z})^\times)$ 一個の連結成分 $\Gamma_g \backslash H$ から成っている。Xの定義より，これら連結成分は自然な $\mathbb{Q}(\zeta)$ −構造（ζ：1の原始n乗根の1つ）を持ち，Galois群 $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ の $\pi_0(X \otimes \mathbb{Q}(\zeta))$（：$X \otimes \mathbb{Q}(\zeta)$ の連結成分のなす集合）への作用は，この群の $\mu_n(\mathbb{Q}(\zeta))$ への自然な作用から定まる。特に $X \otimes \mathbb{Q}$ は既約になる。この事実とXが $\mathbb{Z}[1/nd]$ 上 smooth であることから，Xが正則（従って正規），整型 scheme になることがわかる。

§2 Canonical subgroup

素数 p を固定し，k を標数 p の体，R を局所環で k を剰余体に持つものとする。自然数 m を固定し，$q = p^m$ とおく。R 上の abelian scheme A をとり，A の special fiber $A \otimes_R k$ を A_0 と書く。$f^m : A_0 \to A_0^{(q)}$ を q 乗写像，すなわち $f^m(x) = x^q$ ($x \in A_0$) で定義される準同型写像とし，G_0 をその核 $Ker(f^m)$ として定義される A_0 の部分群 scheme とする。この時，G_0 は k 上有限でその位数は $q^{\dim(A_0)}$ となる。A の R 上の部分群 scheme G は，R 上有限かつ平坦で，条件

$$(G \to A)\otimes_R k = (G_0 \to A_0)$$

を満たす時，AのR上の位数mを持つcanonical subgroupと呼ばれる。一般のabelian schemeについては，そのcanonical subgroupは存在しないこともあり，また存在する時でも唯1つとは限らないことが知られている（Yui[12]）。しかし以下に見るように，完備なR上のある種のabelian schemeにはcanonical subgroupが唯1つ存在する。

k上のAbel多様体A_0がordinaryであるとは，${}_p(A_0)$の$\bar{k}$-有理点（$\bar{k}$：kの代数閉包）のなす群の位数が$p^{\dim(A_0)}$になることである（一般には$p^{\dim(A_0)}$以下になる）。この時，G_0は${}_p(A_0)$の1を含む連結成分$({}_p(A_0))^0$になる。よってRがhenselian（例えば完備）である時，AのR上の次数mを持つcanonical subgroupが唯1つ存在し，実際それは${}_pA$の1を含む連結成分$({}_pA)^0$で与えられる。

さて$X = X(g, dl, n)$は関手$\underline{X}$を表現するschemeだから，X上のabelian scheme $\mathcal{A}$，$\mathcal{A}/X$のtype dlの偏極θ，θに関してsimilitude-symplecticとなる$\mathcal{A}/X$のn階構造δの三つ組$(\mathcal{A}, \theta, \delta)$でuniversalなものが唯1つ存在する。以下$n$を$p$で割りきれないと仮定する。$X$の関数体を$K(X)$で表わし，$K$を$K(X)$の1つの有限次拡大体で${}_p(\mathcal{A}(\bar{K}))$の元がすべて$K$上有理的になるものとする。$\pi : Y \to X$を$X$の$K$の中での正規化とすると，$X$

は正規なので、πは全射でしかも有限射になる([1], 5.17)。

$\mathbb{F}_p$で位数pの有限体を表わし、$X_0 = X \otimes \mathbb{F}_p$, $Y_0 = Y \otimes \mathbb{F}_p$とおく。

ZをY_0の1つの既約成分とすると、going-down theorem (Xが正規であることに注意)より、$\pi(Z)$もX_0の既約(よってX_0の正則性から連結)成分になる。従って、Zの生成点ζに対し、$\mathcal{A}_\zeta = \mathcal{A} \times_X \mathrm{Spec}(k(\zeta))$は$k(\zeta)$上のordinary Abel多様体となる([8], 定理3.1)。よって

$$(g(\mathcal{A}_\zeta))^\circ = \mathrm{Ker}(f^m : \mathcal{A}_\zeta \to \mathcal{A}_\zeta^{(q)})。$$

またRを$\mathcal{O}_{Y,\zeta}$のhensel化とすると

$$(g(\mathcal{A}_R))^\circ \otimes_R k(\zeta) = (g(\mathcal{A}_\zeta))^\circ。$$

$K(R)$をRの商体とすると、$(g(\mathcal{A}_R))^\circ \otimes_R K(R)$は$g(\mathcal{A}_{K(R)})$の部分群になるから、$K$の性質より$g(\mathcal{A}_K)$の$K$上の部分群scheme G_Kで

$$G_K \otimes_K K(R) = (g(\mathcal{A}_R))^\circ \otimes_R K(R)$$

となるものが唯1つ存在する。$G = G(Z)$をG_Kの$g(\mathcal{A}_Y)$の中でのZariski閉包とすると、Yの任意のaffine開部分集合Uに対し$g(\mathcal{A}_U) = \mathrm{Spec}(A)$, $G_K = \mathrm{Spec}(B)$とする時

$$G \times_Y U = \mathrm{Spec}(\mathrm{Im}(A \to B))$$

となる。明らかにGはY上の有限群schemeとなる。この時

<u>予想1.</u> GはY上平坦。

もしこの予想が正しければ，Z を Y の被約な閉部分 scheme として

$$G \times_Y Z = \mathrm{Ker}(f^m : \mathcal{A}_Z \to \mathcal{A}_Z^{(q)})$$

が成り立つから，G は $\mathcal{A}_Y/Y$ の Z に関する大域的な canonical subgroup を与える。またこのような canonical subgroup が存在すれば，それは G と一致することもすぐわかる。今の所，上の予想は $g=1$ の場合（後述）を除いて示されていない。明らかに $y \in Y \setminus Y_0$ に対しては，$g(\mathcal{A}_Y)$ は y で étale だから G もそうなる。よって G/Y の平坦性は Y_0 の点について考えればよい。我々の結果は次の通り：

定理 2.1.

(1)　y を Y_0 の ordinary point，すなわち $\mathcal{A}_y$ が ordinary となる Y_0 の点とし，さらに y は Z に属しているとする。この時，G は y において Y 上平坦で

$$G \times_Y \mathrm{Spec}(k(y)) = \mathrm{Ker}(f^m : \mathcal{A}_y \to \mathcal{A}_y^{(q)})$$

を満たす。

(2)　$g=1$ の時予想1は正しい。よってこの時，G は $\mathcal{A}_Y/Y$ の有限，平坦な部分群 scheme で

$$G \times_Y Z = \mathrm{Ker}(f^m : \mathcal{A}_Z \to \mathcal{A}_Z^{(q)})$$

を満たす。

（略証）　$\mathcal{B}_K$ を $\mathcal{A}_K$ の G_K による商Abel多様体とすると，$\mathcal{B}_K$ の偏極 ρ_K，n 階構造 τ_K で

$$(\mathcal{B}_K, \rho_K, \tau_K) = (\mathcal{A}_K, \theta_K, \delta_K)/G_K$$

を満たすものが存在し，ρ_K が type $\mathfrak{d}$，τ_K が ρ_K に関して similitude-symplectic となる。よって $(\mathcal{B}_K, \rho_K, \tau_K)$ は射 $\varphi_K : \mathrm{Spec}(K) \to X$ を定める。予想 1 が成立することは，Y 上の偏極，n 階構造を持つ abelian scheme $(\mathcal{B}, \rho, \tau)$ で

$$(\mathcal{B}, \rho, \tau) \times_Y \mathrm{Spec}(K) = (\mathcal{B}_K, \rho_K, \tau_K)$$

を満たすものが存在すること，すなわち射 $\varphi : Y \to X$ で $\varphi \times_Y \mathrm{Spec}(K) = \varphi_K$ を満たすものが存在することと同値である。（Y が一般の正則 scheme の時，射 φ_K の Y への延長可能性は Grothendieck [3] で論じられている。）一般の g について φ の存在は示されていないが，Z の ordinary point y については

$$(\mathcal{A}_y)^{\circ} = \mathrm{Ker}(f^m : \mathcal{A}_y \to \mathcal{A}_y^{(q)})$$

となることと Y の正規性から，φ_K は射 $\varphi_{\mathcal{O}_y} : \mathcal{O}_y \to X$ に延長できることがわかる。また $g=1$ の時は，X が affine scheme であることから φ_K が φ に延長できることがわかる。

定理 2.1, (2) と $\pi : Y \to X$ の全射性から次の結果が従う。これは [5], p.103 における Lubin の予想を肯定的に解いている。

系 2.2. Rを混標数 0 と p を持つ局所環，EをR上の楕円曲線とする。この時 E は潜在的に canonical subgroup を持つ。すなわち R の有限次拡大 R' で $E \otimes_R R'$ が canonical subgroup を持つものが存在する。

§3. $X(\overline{\mathbb{Z}}_p)$ 上の1つの対応

記号を今までの通りとする。$\mathbb{Z}_p$ を p 進整数環，$\mathbb{Q}_p$ を p 進数体とし，$\overline{\mathbb{Q}}_p$ で $\mathbb{Q}_p$ の代数閉包を，$\overline{\mathbb{Z}}_p$ で $\mathbb{Z}_p$ の $\overline{\mathbb{Q}}_p$ の中での整閉包を表わす。この時 §2 で定義した群 scheme $G(Z)$ を用いて，$X(\overline{\mathbb{Z}}_p)$ 上の対応

$$\chi^{(m)} = (T^{(m)} \subset X(\overline{\mathbb{Z}}_p) \times X(\overline{\mathbb{Z}}_p))$$

で，q 乗写像 $\mathrm{Frob}_q : X(\overline{\mathbb{F}}_p) \to X(\overline{\mathbb{F}}_p)$ の持ち上げと見なせるものを構成する。

reduction homomorphism $\mathrm{mod}\,\overline{p} : \overline{\mathbb{Z}}_p \to \overline{\mathbb{F}}_p$ が導く写像 $X(\overline{\mathbb{Z}}_p) \to X(\overline{\mathbb{F}}_p)$, $Y(\overline{\mathbb{Z}}_p) \to Y(\overline{\mathbb{F}}_p)$ を再び $\mathrm{mod}\,\overline{p}$ で表わす。$\{Z_i\}_i$ を Y_0 の既約成分全体の成す集合とする。各 i に対し

$$Y(\overline{\mathbb{Z}}_p)_i = \{ y \in Y(\overline{\mathbb{Z}}_p) \mid y \bmod \overline{p} \in Z_i \}$$

とおき，$G_i = G(Z_i)$ とする。$Y(\overline{\mathbb{Z}}_p)_i$ の各元 y に対し，$G_{i\,y} = G_i \times_Y \mathrm{Spec}(k(y))$ とおくと

$$(B_y, \rho_y, \tau_y) = (A_y, \theta_y, \sigma_y)/G_{i\,y}$$

は $k(y)$ 上の Abel 多様体 B_y，$B_y/k(y)$ の type $\mathfrak{d}$ の偏極 ρ_y，ρ_y

に関して similitude-symplectic な $B_y/k(y)$ の n 階構造 τ_y から成る3つ組を定める。Serre-Tate の結果（[11], 定理2, 系2）より (B_y, ρ_y, τ_y) は $\overline{\mathbb{Z}}_p$ 上定義されるから, これは X の $\overline{\mathbb{Z}}_p$ − 有理点を定める。これを $\pi_i(y)$ と書く。この時, $X(\overline{\mathbb{Z}}_p) \times X(\overline{\mathbb{Z}}_p)$ の部分集合 $T^{(m)}$ を次のように定義する：

$$T^{(m)} = \bigcup_i \{(\pi(y), \pi_i(y)) \mid y \in Y(\overline{\mathbb{Z}}_p)\}。$$

$T^{(m)}$ が Y の関数体 K のとり方によらないことは容易にわかる。定理 2.1 より次が成りたつ。

<u>命題 3.1</u>

(1)　x を $X(\overline{\mathbb{Z}}_p)$ の元で $x \bmod \overline{p} \in X(\overline{\mathbb{F}}_p)$ が ordinary point になるものとする。この時 $(x, x') \in T^{(m)}$ となる $X(\overline{\mathbb{Z}}_p)$ の元 x' が唯1つ存在し，$x' \bmod \overline{p} = \mathrm{Frob}_q(x \bmod \overline{p})$ が成りたつ。

(2)　$g=1$ の時, 任意の $(x, x') \in T^{(m)}$ に対し，$x' \bmod \overline{p} = \mathrm{Frob}_q(x \bmod \overline{p})$ が成りたつ。

もし予想1が正しければ, 任意の $(x, x') \in T^{(m)}$ に対し，$x' \bmod \overline{p} = \mathrm{Frob}_q(x \bmod \overline{p})$ が成りたつ。

$S^{(m)}$ を対応 $\mathcal{X}^{(m)}$ で固定される $X(\overline{\mathbb{Z}}_p)$ の部分集合, すなわち

$$S^{(m)} = \{x \in X(\overline{\mathbb{Z}}_p) \mid (x, x) \in T^{(m)}\}$$

とする。この時

予想 2. $\#(\mathcal{S}^{(m)}) = \#(X_0(\mathbb{F}_q))$。

以下では、この予想を支持する2つの結果を述べる。

X_0° を X_0 の ordinary locus, すなわち任意の標数 p の体 F に対し

$$X_0^\circ(F) = \{ z \in X_0(F) : \text{ordinary point} \}$$

を満たす X_0 の開部分集合とする。そして $X(\overline{\mathbb{Z}}_p)$ の部分集合 $X^\circ(\overline{\mathbb{Z}}_p)$ を

$$X^\circ(\overline{\mathbb{Z}}_p) = \{ x \in X(\overline{\mathbb{Z}}_p) \mid x \bmod \overline{p} \in X_0^\circ(\overline{\mathbb{F}}_p) \}$$

として定義する。この時最初の結果は

定理 3.2. 写像 $\bmod \overline{p} : X(\overline{\mathbb{Z}}_p) \to X(\overline{\mathbb{F}}_p)$ は全単射

$$\mathcal{S}^{(m)} \cap X^\circ(\overline{\mathbb{Z}}_p) \xrightarrow{\sim} X_0^\circ(\mathbb{F}_q)$$

を導く。特に

$$\#(\mathcal{S}^{(m)} \cap X^\circ(\overline{\mathbb{Z}}_p)) = \#(X_0^\circ(\mathbb{F}_q))$$

である。

(略証) まず命題 3.1.(1) より, $\bmod \overline{p} \mid \mathcal{S}^{(m)} \cap X^\circ(\overline{\mathbb{Z}}_p)$ は $\mathcal{S}^{(m)} \cap X^\circ(\overline{\mathbb{Z}}_p)$ から $X_0^\circ(\mathbb{F}_q)$ への写像を与える。この写像の全射性は、ordinary Abel多様体の canonical lifting の存在 (cf. [10]) による。すなわち $X_0^\circ(\mathbb{F}_q)$ の元 z に対し、(A_z, θ_z, ϕ_z) の canonical lifting に対応

する $X^0(\mathbb{Z}_p)$ の元を x とすると、$x \in \mathcal{S}^{(m)}$, $x \bmod \bar{p} = z$ となる。またこの写像の単射性は、Messing の結果（[6], Appendix, 系 1.2）"有限体上の ordinary Abel 多様体 A_0 の lifting A は、φ_0 が A_0 の Frobenius 自己準同型となる自己準同型 φ を持つ時 A_0 の canonical lifting となる" から従う。

さて2番目の結果は、次のように予想2が $g=1$ の時に正しいことを示している。

<u>定理 3.3</u>　$g=1$ の時，$\#(\mathcal{S}^{(m)}) = \#(X_0(\mathbb{F}_q))$。

<u>注意</u>　$g=1$ の時、命題 3.1, (2) より $\bmod \bar{p} \mid \mathcal{S}^{(m)} \cap X(\mathbb{Z}_p)$ は $\mathcal{S}^{(m)} \cap X(\mathbb{Z}_p)$ から $X_0(\mathbb{F}_q)$ への写像を与えるが、これは全射ではない。例えば $\mathbb{F}_p$ 上の楕円曲線 E_0 でその Frobenius 自己準同型 f が $f^2 = p$ を満たすものをとり（Honda [4] よりこのような E_0 は存在する），z を $X_0(\mathbb{F}_q)$ の元で $A_z \cong E_0 \otimes \mathbb{F}_q$ となるものとすると，虚数乗法の理論より z は $\bmod \bar{p}\,(\mathcal{S}^{(m)} \cap X(\mathbb{Z}_p))$ に属さないことがわかる。

（定理 3.3 の略証）　$\mathcal{S}^{(m)}$ と $X_0(\mathbb{F}_q)$ の個数を比べるために、étale cohomology 群に関する base change theorem

$$H_c^i(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell) \cong H_c^i(X_{\bar{\mathbb{F}}_p}, \mathbb{Q}_\ell)$$

（$H_c^i(\cdot, \mathbb{Q}_\ell)$：compact な台を持つ i 次 ℓ 進（$\ell \neq p$）étale cohomology

群）を用いる。$(\mathcal{E}, \delta)$ を X 上の n 階構造を持つ楕円曲線で universal なものとする。Z を

$$(\mathcal{E}_x, \delta_x) \mapsto ((\mathcal{E}_x, \delta_x), (\mathcal{E}_x, \delta_x)/H) \quad (x \in X_{\varpi})$$

（ただし H は条件

$H \cap p^i(\mathcal{E}_x)$ と ${}^tH \cap p^i(\mathcal{E}_x/H)$ が任意の $i=1, \cdots, m$ に対し位数 p^i を満たす $\mathcal{E}_x$ の位数 q の部分群全体を走る）から定まる X_{ϖ} の代数的対応とし、Z が $H_c^i = H_c^i(X_{\bar{\varpi}}, \mathbb{Q}_\ell) = H_c^i(X_{\bar{\mathbb{F}}_p}, \mathbb{Q}_\ell)$ 上に導く Hecke 作用素を $T'(q)$ とする。この時，Lefshetz の跡公式を用いて

$$\sum_{i=0}^{2} (-1)^i \operatorname{Tr}(T'(q) \mid H_c^i(X_{\bar{\varpi}}, \mathbb{Q}_\ell))$$
$$= (Z \cdot \Delta) \quad (\Delta \subset X_{\bar{\varpi}} \times X_{\bar{\varpi}} : \text{diagonal})$$
$$= 2\,\#(\mathcal{S}^{(m)})。$$

また合同関係式 $T'(q) \mid H_c^i(X_{\bar{\mathbb{F}}_p}, \mathbb{Q}_\ell) = F^m + (T(p,p) \circ V)^m$ より

$$\sum_{i=0}^{2} (-1)^i \operatorname{Tr}(T'(q) \mid H_c^i(X_{\bar{\mathbb{F}}_p}, \mathbb{Q}_\ell)) = 2\,\#(X_0(\mathbb{F}_q))$$

となることがわかる。

§4. $\mathcal{S}^{(m)}$ の一意化

g を自然数，$\mathbb{d}$ を §1 の通りとし，p を素数とする。p で割り切れない 3 以上の自然数 n に対し，$X_n = X(g, \mathbb{d}, n)$ とおく。これは type $\mathbb{d}$ の偏極とそれに関して similitude-symplectic となる n 階構造を持つ Abel 多様体の fine moduli 空間である。H,

$G(A_f)$, $G(\mathbb{Q})_+$, K_n を §1 の通りとし，

$$\mathcal{H} = G(\mathbb{Q})_+ \backslash H \times G(A_f)$$

とおくと，§1 で見たように $X_n(\mathbb{C}) = \mathcal{H}/K_n$ である。$\pi_n : \mathcal{H} \to X_n(\mathbb{C})$ を自然な射影とする。自然数 m に対し，$\mathcal{S}_n(p^m) = \mathcal{S}^{(m)}$ を対応 $\mathcal{X}^{(m)}$ で固定される $X_n(\overline{\mathbb{F}}_p)$ の部分集合とする。すなわち

$$\mathcal{S}_n(p^m) = \{ x \in X_n(\overline{\mathbb{F}}_p) \mid (x, x) \in T^{(m)} \}。$$

（$\mathcal{S}_n(p^m) \subset X_n(\overline{\mathbb{Q}})$ が成り立つと思われる。）$X_n(\overline{\mathbb{F}}_p)$ の部分集合 $\mathcal{S}_n(p^\infty)$ を

$$\mathcal{S}_n(p^\infty) = \bigcup_m \mathcal{S}_n(p^m)$$

で定義する。体としての埋めこみ $\iota : \mathbb{Q}_p \hookrightarrow \mathbb{C}$ を1つとると，ι は $X_n(\overline{\mathbb{F}}_p) \subset X_n(\mathbb{C})$ を定める。この時 $\mathcal{H}$ の部分集合 $\mathcal{H}_n(p^\infty)$ を

$$\mathcal{H}_n(p^\infty) = \{ z \in \mathcal{H} \mid \pi_n(z) \in \mathcal{S}_n(p^\infty) \}$$

で定義する。

予想1が正しいと仮定すると，$\mathcal{H}_n(p^\infty)$（$n \geq 3$, $p \nmid n$）が n によらないことを困難なく示すことができる。よってこの時その集合を $\mathcal{H}(p^\infty)$ と書くと，自然な射影 $\pi_n | \mathcal{H}(p^\infty) : \mathcal{H}(p^\infty) \to \mathcal{S}_n(p^\infty)$ は全単射

$$\mathcal{H}(p^\infty)/\sim \;\cong\; \mathcal{S}_n(p^\infty) \qquad (n \geq 3,\ p \nmid n)$$

を導く。ただし $\mathcal{H}(p^\infty)$ の二つの元 z, z' に対し，記号 $z \sim z'$ は $z = z'g$ となる $g \in K_n$ が存在することを表わす。

$$X_n^\circ(\overline{\mathbb{Z}}_p) = \{x \in X_n(\overline{\mathbb{Z}}_p) \mid x \bmod \bar{p} \ \text{ordinary point}\},$$

$$\mathcal{S}_n^\circ(p^m) = \mathcal{S}_n(p^m) \cap X_n^\circ(\overline{\mathbb{Z}}_p),$$

$$\mathcal{S}_n^\circ(p^\infty) = \mathcal{S}_n(p^\infty) \cap X_n^\circ(\overline{\mathbb{Z}}_p) = \bigcup_m \mathcal{S}_n^\circ(p^m),$$

$$\mathcal{H}_n^\circ(p^\infty) = \{z \in \mathcal{H} \mid \pi_n(z) \in \mathcal{S}_n^\circ(p^\infty)\},$$

とすると、今の所得られている結果は次の通り：

命題 4.1

(1) $\mathcal{H}_n^\circ(p^\infty)$ $(n \geqq 3,\ p \nmid n)$ は n によらない。よってこれを $\mathcal{H}^\circ(p^\infty)$ とおくと

$$\mathcal{H}^\circ(p^\infty)/\sim \ \cong \ \mathcal{S}_n^\circ(p^\infty)。$$

(2) $g=1$ と仮定する。この時 $\mathcal{H}_n(p^\infty)$ $(n \geqq 3,\ p \nmid n)$ は n によらない。よってこれを $\mathcal{H}(p^\infty)$ とおくと

$$\mathcal{H}(p^\infty)/\sim \ \cong \ \mathcal{S}_n(p^\infty)。$$

文献

[1] M. Atiyah and I. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass., 1969.

[2] B. Dwork, p-adic cycles, Inst. Hautes Etudes Sci Publ. Math. 37 (1969), 27-116.

[3] A. Grothendieck, Un Theoreme sur les Homomorphismes de Schemas Abeliens, Inv. Math. 2 (1966), 59-78.

[4] T. Honda, Isogeny classes of abelian varieties over finite fields, J. Math. Soc. Japan 20, no. 1-2 (1968), 83-95.

[5] J. Lubin, Canonical subgroups of formal groups, Trans, Amer. Math. Soc. 251 (1979), 103-127.

[6] W. Messing, The crystals associated to Barsotti-Tate groups: with applications to abelian schemes, Lecture Notes in Math. 264, Springer-Verlag, 1972.

[7] D. Mumford, Geometric Invariant Theory, Ergebnisse 34, Springer-Verlag, 1965.

[8] P. Norman and F. Oort, Moduli of abelian varieties, Ann. of Math. 112 (1980), 413-439.

[9] F. Oort, Finite group schemes, local moduli for abelian varieties and lifting problems, Algebraic geometry, Oslo 1970, Wolters-Noordhoff, 1972.

[10] J. P. Serre and J. Tate, Elliptic curves and formal groups, Mimeographed notes from Woods Hole Summer Institute, 1964.

[11] J. P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. 88 (1968), 492-517.

[12] N. Yui, Elliptic curves and canonical subgroups of formal groups, J. reine angew. Math. 303/304 (1978), 319-331.