

東大理学部 市川尚志 (Takashi Ichikawa)

ここで、 $(X$ 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、 $X(\overline{\mathbb{F}}_p)$ 上の対応 $\chi^{(m)}$ で $\chi^{(m)} \bmod \bar{p}$ が $X_0^{\circ}(\overline{\mathbb{F}}_p)$ ($X_0^{\circ} : X_0 = X \otimes \mathbb{F}_p$
 の ordinary locus) 上 Frob_g を与えるものを構成する。 $\chi^{(m)}$ 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、 $\chi^{(m)} \bmod \bar{p}$ が $X_0(\overline{\mathbb{F}}_p)$ 上全体で Frob_g を与えるこ

ことがわかる。この結果から [5], p103 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。

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

$$X^0(\overline{\mathbb{Z}}_p) = \{x \in X(\overline{\mathbb{Z}}_p) \mid x \bmod \overline{p} \in X_0(\overline{\mathbb{F}}_p)\}$$

とおく。canonical lifting の理論より $\bmod \overline{p}$ が全単射

$$X^0(\overline{\mathbb{Z}}_p) \cap \mathcal{S}^{(m)} \xrightarrow{\sim} X_0(\overline{\mathbb{F}}_g)$$

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、 $\bmod \overline{p}$ は $\mathcal{S}^{(m)}$ から $X_0(\overline{\mathbb{F}}_g)$ への全単射を与えられていることもわかる。

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

が成り立つことが証明される。これは $X^{(m)}$ 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 $X^{(m)}$ を定義し、その固定点集合 $\mathcal{S}^{(m)}$

と $X_0(\mathbb{F}_q)$ の関係を調べる。§4 では $\mathcal{S}^{\text{inv}}$ の一意性を扱う。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 $g \geq n$ を固定し、 $n \geq 3$ と仮定する。 $d = (d_1, \dots, d_g)$ を $d_1 = 1$, $d_i | d_{i+1}$ ($i = 1, \dots, g-1$) を満たす g 個の自然数 d_i からなる横 vector とする。この d に対し自然数 d と行列 D を以下のように定める：

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

$\gamma: \mathbb{Z}^{2g} \times \mathbb{Z}^{2g} \rightarrow \mathbb{Z}$ ($\mathbb{Z}$: 有理整数環) を行列 $\begin{pmatrix} 0 & -D \\ D & 0 \end{pmatrix}$ により定義した双一次形式とする。すなわち

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

$$\text{ただし } e_i = (0, \dots, 0, \overset{i}{1}, 0, \dots, 0).$$

$\mathcal{S}$ を $\mathbb{Z}[1/d]$ 上の scheme とし、 A を $\mathcal{S}$ 上次元 g を持つ abelian scheme とする。 A の $\mathcal{S}$ 上の偏極、すなわち A から tA (A の dual abelian scheme) への $\mathcal{S}$ 上の同種写像 θ が type d であるとは、 $\text{Ker}(\theta)$ が $\prod_{1 \leq i \leq g} (\mathbb{Z}/d_i\mathbb{Z})^2$ と $\mathcal{S}$ 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、 $\text{Ker}(\theta)$ 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 d なるばその次数は d である。

この A と θ に対し, A の S 上の n 階構造

$$\sigma = \{ \sigma_i \in {}_n A(S) \mid 1 \leq i \leq 2g \}$$

(ただし ${}_n A := \text{Ker}(n: A \rightarrow A)$) が (θ に関して) similitude-

symplectic とは, $\mu_n(S)$ ($\mu_n := \text{Ker}(n: G_m \rightarrow G_m)$) の元 ζ で

$$e_n(\sigma_i, \theta(\sigma_j)) = \zeta^{\langle i, e_j \rangle} \quad (1 \leq i, j \leq 2g)$$

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

$\mathbb{Z}[1/d]$ 上の scheme S に対し, $X(S)$ を S 上 g 次元の abelian scheme A , A/S の type d の偏極 θ , θ に関して similitude-symplectic となる A/S の n 階構造 σ から成る三つ組 (A, θ, σ) の S -同型類のなる集合とする。この時 X は $\mathbb{Z}[1/d]$ 上の scheme のなる圏から集合のなる圏への反変関手を決める。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 に関して similitude-symplectic だから, $g=1$ (従って $d=(1)$) の時, $X(S)$ 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 $\mathbb{Z}[1/d]$ 上の scheme S に対し, $Y(S)$ 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 σ から成る三つ組 (A, θ, σ) の S -同型類のなる集合とすると, Y は $\mathbb{Z}[1/d]$ 上の scheme のなる圏から集合のなる圏への反変関

手を決める。いま $n \geq 3$ だから, Mumford [7] の結果より, $\mathcal{Y}$ は $\mathbb{Z}[\frac{1}{nd}]$ 上のある有限型 scheme Y によつて表現される。従つて $\mathcal{Y}$ の部分関手である $\mathcal{X}$ は Y の開部分 scheme によつて表現される。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 $\mathcal{X}$ は formally smooth となるから, それを表現する scheme X は $\mathbb{Z}[\frac{1}{nd}]$ 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 φ 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

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

を満たす $v(g) \in R^\times$ 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 $\hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$ 。

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

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

この時

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

$$\frac{G(A_+)}{G(\mathbb{Q})_+ \backslash K_n} \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}} \right)^*$$

となるから、 $X \otimes \mathbb{C}$ は $\#((\mathbb{Z}/n\mathbb{Z})^*)$ - 個の連結成分 $\frac{H}{\Gamma_g}$ 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 ($\zeta: 1$ の原始 n 乗根の 1 つ) を持ち、Galois 群 $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 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、 $\wp = p^m$ 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。 $f^m: A_0 \rightarrow A_0^{(p)}$ を $\wp$ 乗写像、すなわち $f^m(x) = x^{\wp}$ ($x \in A_0$) で定義される準同型写像とし、 G_0 をその核 $\text{Ker}(f^m)$ 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 $\wp^{\dim(A_0)}$ 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

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

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一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 が唯一存在する。

k 上の Abelian 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 $(p(A_0))^{\circ}$ になる。よって R が henselian (例えば完備) である時, A の R 上の位数 m を持つ canonical subgroup が唯一存在し, 実際それは pA の 1 を含む連結成分 $(pA)^{\circ}$ で与えられる。

ここで $X = X(g, d, n)$ は関手 X を表現する scheme ならば, X 上の abelian scheme A , A/X の type d の偏極 θ , θ に関して similitude-symplectic となる A/X の n 階構造 ϕ の三つ組 (A, θ, ϕ) で universal なものが唯一存在する。以下 n を p で割りきれないことを仮定する。 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 $p(A(\bar{K}))$ の元がすべて K 上有理的になるものとする。 $\pi: Y \rightarrow X$ 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 s に対し、 $\mathcal{A}_s = \mathcal{A} \times_X \mathcal{S}_{\text{pec}}(k(s))$ は $k(s)$ 上の ordinary Abelian 多様体となる ([8], 定理 3.1)。よって

$$(\mathcal{f}(\mathcal{A}_s))^{\circ} = \text{Ker}(f^m: \mathcal{A}_s \rightarrow \mathcal{A}_s^{(q)}).$$

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

$$(\mathcal{f}(\mathcal{A}_R))^{\circ} \otimes_R k(s) = (\mathcal{f}(\mathcal{A}_s))^{\circ}.$$

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

G_K で

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

となるものが唯一つ存在する。 $G = G(Z)$ を G_K の $\mathcal{f}(\mathcal{A}_Y)$ の中の Zariski 閉包とすると、 Y の任意の affine 開部分集合 U に対し $\mathcal{f}(\mathcal{A}_U) = \mathcal{S}_{\text{pec}}(A)$, $G_K = \mathcal{S}_{\text{pec}}(B)$ とする時

$$G \times_Y U = \mathcal{S}_{\text{pec}}(\text{Im}(A \rightarrow B))$$

となる。明らかに G は Y 上の有限群 scheme となる。この時

予想 1. G は Y 上平坦。

もしこの予想が正しいければ、 Z を Y の被約な閉部分 scheme

として

$$G \times_Y Z = \text{Ker}(f^m: \mathcal{A}_Z \rightarrow \mathcal{A}_Z^{(g)})$$

が成り立つから、 G は $\mathcal{A}_Y$ 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 と一致することでもすぐわかる。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、 $f(\mathcal{A}_Y)$ は y で étale だから G もさうなる。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, 存在する $\mathcal{A}_y$ 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 にあって Y 上平坦で

$$G \times_Y \text{Spec}(k(y)) = \text{Ker}(f^m: \mathcal{A}_y \rightarrow \mathcal{A}_y^{(g)})$$

を満たす。

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

$$G \times_Y Z = \text{Ker}(f^m: \mathcal{A}_Z \rightarrow \mathcal{A}_Z^{(g)})$$

を満たす。

(略証) β_K を A_K の G_K による商 Abel 多様体とする。

β_K の偏極 f_K , n 階構造 τ_K で

$$(\beta_K, f_K, \tau_K) = (A_K, \theta_K, \delta_K)/G_K$$

を満たすものが存在し, f_K が type dl, τ_K が f_K に関して similitude-symplectic となる。よって (β_K, f_K, τ_K) は射 $\varphi_K: \text{Spec}(K) \rightarrow X$ 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 (β, f, τ) で

$$(\beta, f, \tau) \times_Y \text{Spec}(K) = (\beta_K, f_K, \tau_K)$$

を満たすものが存在すること, すなわち射 $\varphi: Y \rightarrow X$ で

$\varphi \times_Y \text{Spec}(K) = \varphi_K$ 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るが, Z の ordinary point y については

$$(A_y)^\circ = \text{Ker}(f^m: A_y \rightarrow A_y^{(p)})$$

となることは Y の正則性から, φ_K は射 $\varphi_{O_y}: O_y \rightarrow X$ 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 $\pi: Y \rightarrow X$ 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 を素数 $0 < p$ 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 $G(\mathbb{Z})$ 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, $F_{\text{red}}: X(\overline{\mathbb{F}}_p) \rightarrow X(\overline{\mathbb{F}}_p)$ の持ち上げと見なせるものを構成する。

reduction homomorphism $\text{mod } \overline{p}: \overline{\mathbb{Z}}_p \rightarrow \overline{\mathbb{F}}_p$ が導く写像 $X(\overline{\mathbb{Z}}_p) \rightarrow X(\overline{\mathbb{F}}_p)$, $Y(\overline{\mathbb{Z}}_p) \rightarrow Y(\overline{\mathbb{F}}_p)$ を再び $\text{mod } \overline{p}$ 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

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

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

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

は $k(y)$ 上の Abelian 多様体 β_y , $\beta_y/k(y)$ の type d の偏極 f_y , f_y

に關して similitude-symplectic な $\beta_g/k(g)$ の n 階構造 τ_g から成る組を定める。Serre-Tate の結果 ([11], 定理 2, 系 2) より $(\beta_g, \rho_g, \tau_g)$ は $\bar{\mathbb{Z}}_p$ 上定義されるから、これは X の $\bar{\mathbb{Z}}_p$ -有理点を定める。これを $\pi(g)$ と書く。この時、 $X(\bar{\mathbb{Z}}_p) \times X(\bar{\mathbb{Z}}_p)$ の部分集合 $T^{(m)}$ を次のように定義する：

$$T^{(m)} = \bigcup_i \{(\pi(g), \pi(g)) \mid g \in \Gamma(\bar{\mathbb{Z}}_p)\}.$$

$T^{(m)}$ が Γ 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 より次が成り立つ。

命題 3.1

(1) x を $X(\bar{\mathbb{Z}}_p)$ の元で $x \bmod \bar{p} \in X(\bar{\mathbb{F}}_p)$ が ordinary point に存在ものとする。この時 $(x, x') \in T^{(m)}$ となる $X(\bar{\mathbb{Z}}_p)$ の元 x' が唯一存在し、 $x' \bmod \bar{p} = \text{Frob}_g(x \bmod \bar{p})$ が成り立つ。

(2) $g=1$ の時、任意の $(x, x') \in T^{(m)}$ に対し、 $x' \bmod \bar{p} = \text{Frob}_g(x \bmod \bar{p})$ が成り立つ。

もし予想 1 が正しいければ、任意の $(x, x') \in T^{(m)}$ に対し、 $x' \bmod \bar{p} = \text{Frob}_g(x \bmod \bar{p})$ が成り立つ。

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

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

とする。この時

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

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 $X(\bar{\mathbb{F}}_p)$ の部分集合 $X^\circ(\bar{\mathbb{F}}_p)$

を

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

として定義する。この時最初の結果は

定理 3.2 写像 $\text{mod } \bar{p} : X(\bar{\mathbb{F}}_p) \rightarrow X(\bar{\mathbb{F}}_p)$ は全単射

$$S^{(m)} \cap X^\circ(\bar{\mathbb{F}}_p) \xrightarrow{\sim} X_0^\circ(\bar{\mathbb{F}}_g)$$

を導く。特に

$$\#(S^{(m)} \cap X^\circ(\bar{\mathbb{F}}_p)) = \#(X_0^\circ(\bar{\mathbb{F}}_g))$$

である。

(略証) まず命題 3.1 (1) より, $\text{mod } \bar{p} \mid S^{(m)} \cap X^\circ(\bar{\mathbb{F}}_p)$ は

$S^{(m)} \cap X^\circ(\bar{\mathbb{F}}_p)$ から $X_0^\circ(\bar{\mathbb{F}}_g)$ 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 $X_0^\circ(\bar{\mathbb{F}}_g)$ の元 z に対し, $(A_z, \theta_z, \delta_z)$ の canonical lifting に対応

する $X^0(\bar{\mathbb{F}}_p)$ 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 Abelian 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。

定理 3.3 $g=1$ の時, $\#(\mathcal{S}^{(m)}) = \#(X_0(\mathbb{F}_g))$ 。

注意 $g=1$ の時, 命題 3.1, (2) より $\bmod \bar{p} : \mathcal{S}^{(m)} \rightarrow X(\bar{\mathbb{F}}_p)$ は $\mathcal{S}^{(m)} \cap X(\bar{\mathbb{F}}_p)$ から $X_0(\mathbb{F}_g)$ への写像を与えが, 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 $f^2 = p$ を満たすものを取り (Honda (4) よりこのような E_0 は存在する), z を $X_0(\mathbb{F}_g)$ の元で $A_z \equiv E_0 \otimes \mathbb{F}_g$ となるものとする, 虚数乗法の理論より z は $\bmod \bar{p} : (\mathcal{S}^{(m)} \cap X(\bar{\mathbb{F}}_p))$ に属さないことがわかる。

(定理 3.3 の略証) $\mathcal{S}^{(m)}$ と $X_0(\mathbb{F}_g)$ 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 次元 ($\ell \neq p$) étale cohomology

群)を用いる。 (ε, δ) 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

$$(\varepsilon_x, \delta_x) \mapsto ((\varepsilon_x, \delta_x), (\varepsilon_x, \delta_x)/H) \quad (x \in X_{\overline{\mathbb{Q}}})$$

(ただし H は厚)

$H \cap p^i(\varepsilon_x) \subset {}^t H \cap p^i(\varepsilon_x/H)$ が任意の $i=1, \dots, m$ に対し位数 p^i を満たす ε_x の位数 q の部分群全体を走り)から定まる $X_{\overline{\mathbb{Q}}}$ の代数的対応とし、 Z が $H_c^i = H_c^i(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell) = H_c^i(X_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$ 上に導く Hecke 作用素を $T(q)$ とする。この時、Lefschetzの跡公式を用いて

$$\begin{aligned} & \sum_{i=0}^2 (-1)^i \operatorname{Tr}(T(q) | H_c^i(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)) \\ &= (Z \cdot \Delta) \quad (\Delta \subset X_{\overline{\mathbb{Q}}} \times X_{\overline{\mathbb{Q}}} : \text{diagonal}) \\ &= 2 \#(\mathcal{S}^{(m)}). \end{aligned}$$

また合同関係式 $T(q) | H_c^i(X_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell) = F^m + (T(p, p) \circ V)^m$ より

$$\sum_{i=0}^2 (-1)^i \operatorname{Tr}(T(q) | H_c^i(X_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)) = 2 \#(X_0(\mathbb{F}_q))$$

となることがわかる。

§ 4. $\mathcal{S}^{(m)}$ の一意化

g を自然数、 d を§1の通りとし、 p を素数とする。 p で割り切れないうちの自然数 n に対し、 $X_n = X(g, d, n)$ と置く。

これは type d の偏極とそれに関して similitude-symplectic となる n 階構造を持つ Abelian 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. $\pi_n: \mathcal{H} \rightarrow X_n(\mathbb{C})$ 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 $\chi^{(m)}$ で固定される $X_n(\bar{\mathbb{Z}}_p)$ の部分集合とする. すなわち

$$\mathcal{S}_n(p^m) = \{x \in X_n(\bar{\mathbb{Z}}_p) \mid (x, x) \in T^{(m)}\}.$$

($\mathcal{S}_n(p^m) \subset X_n(\mathbb{Q})$ が成り立つと思われる.) $X_n(\bar{\mathbb{Z}}_p)$ 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 $\mathbb{Q}_p \hookrightarrow \mathbb{C}$ を ι とすると, ι は $X_n(\bar{\mathbb{Z}}_p) \subset X_n(\mathbb{C})$ 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出来る. よってこの時々の集合を $\mathcal{H}(p^\infty)$ と書くと, 自然な射影 $\pi_n|_{\mathcal{H}(p^\infty)}: \mathcal{H}(p^\infty) \rightarrow \mathcal{S}_n(p^\infty)$ は全単射

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

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.

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

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

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

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

とすると、今の所得されている結果は次の通り：

命題 4.1.

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

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

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

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

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.