ARGOS seminar on intersections of modular correspondences, Astérisque **312** (2007) の紹介 (2)

服部 新
北大理学研究院 3-601
shin-h@math.sci.hokudai.ac.jp

平成 19 年 10 月 19 日

※ B. H. Gross, K. Keating, *On the intersection of modular correspondences*, Invent. Math **112** (1993), 225-245 の解説本

1 今回示したこと

定理 1.1 (定理 C) *p を素数, Q を $\mathbb{Z}$ 上の positive definite ternary quadratic space で,*

- *$Q \otimes_{\mathbb{Z}} \mathbb{Z}_p$ は anisotropic*
- *任意の素数 $l \neq p$ に対し, $Q \otimes_{\mathbb{Z}} \mathbb{Z}_l$ は isotropic*

とすると,

$$\sum_{[E,E']:supersingular/\bar{\mathbb{F}}_p} \frac{\mathrm{R}_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} = 4 \prod_{l|\Delta(Q), l\neq p} \beta_l(Q)$$

ただし $u_E = \frac{1}{2}\sharp\mathrm{Aut}(E)$.

証明の概略. D を $\{p, \infty\}$ で分岐する $\mathbb{Q}$ 上の quaternion algebra, $\mathcal{O}_D$ をその (任意の)maximal order とする. $\bar{\mathbb{F}}_p$ 上の supersingular elliptic curve の同型類全体は

$$D \setminus (D \otimes \mathbb{A}_f)^\times / (\mathcal{O}_D \otimes \hat{\mathbb{Z}})^\times$$

と同一視できる. $\mathcal{O}_D$ の genus の各 proper class は, 適当な supersingular elliptic curve E, E' を取ると, $\mathrm{Hom}(E, E')$ の形の lattce で代表される. 同じ proper class を定めるペアの同型類 $[E, E']$ は E, E' が $\mathbb{F}_p$ 上定義されているときは 1 個, そうでないときは 2 個ある. また,

$$\sharp\mathrm{SO}((\mathrm{Hom}(E,E'), \deg)) = \begin{cases} \sharp\mathrm{Aut}(E)\sharp\mathrm{Aut}(E') & \text{if } E, E' \text{ が } \mathbb{F}_p \text{ 上 defined} \\ \frac{1}{2}\sharp\mathrm{Aut}(E)\sharp\mathrm{Aut}(E') & \text{otherwise} \end{cases}.$$

が示せる. これらを使って定理の左辺を書き直すと

$$\sum_{[E,E']:\mathrm{supersingular}/\bar{\mathbb{F}}_p} \frac{\mathrm{R}_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} = \sum_{[L]\in \text{proper classin gen}(\mathcal{O}_D)} 4\frac{\mathrm{R}_L(Q)}{\sharp\mathrm{SO}(L)}$$

を得るので, Minkowski-Siegel の公式を適用すれば主張が従う.

2 quadratic spaceの用語集 (2)

- 一般に, (M,Q) を R 上の quadratic space とするとき,

$$\mathrm{O}(M,Q) := \{g : (M,Q) \to (M,Q) \mid \text{isometry}\}$$
$$\mathrm{SO}(M,Q) := \{g \in \mathrm{O}(M,Q) \mid \det(g) = 1\}$$

とおく (誤解のない場合は Q は略す). $g \in \mathrm{O}(M,Q)$ のとき, M の basis を取って行列表示すると,

$$^{\mathrm{t}}gB_Qg = B_Q$$

から $\det(g)^2 = 1$ を得る.

- $\mathbb{Q}$ 上の quadratic space (V,Q) に対し, V の $\mathbb{Z}$-lattice とは, V の部分 $\mathbb{Z}$-加群 Λ で $\mathbb{Q}$ 上 V を生成するもののこと (つまり, こう書いた場合は, Q が Λ を保つことは仮定しない). 一方, V の Q を保つ $\mathbb{Z}$-lattice と言った場合は, $Q(\Lambda) \subseteq \mathbb{Z}$ も仮定することにする.

- 定義から,

$$\mathrm{O}(V \otimes \mathbb{A}_f) = \{g = (g_l)_l \in \mathrm{GL}(V \otimes \mathbb{A}_f) \mid \forall g_l \in \mathrm{O}(V \otimes \mathbb{Q}_l)\}.$$

- $g = (g_l)_l \in \mathrm{GL}(V \otimes \mathbb{A}_f)$ は V の $\mathbb{Z}$-lattice 全体のなす集合に,

$$g(\Lambda) := \bigcap_{l<\infty} V \cap g_l(\Lambda_l)$$

で作用する.

この作用での Λ の $\mathrm{O}(V \otimes \mathbb{A}_f)$-orbit を Λ の **genus** といい, $\mathrm{gen}(\Lambda)$ で表す.

注 2.1 実際は, $\mathrm{SO}(V \otimes \mathbb{A}_f)$-orbit と同じになることが示せる (各素点 l で, $\tau_l \in \mathrm{O}(V \otimes \mathbb{Q}_l)$ で $\det(\tau_l) = -1$ となる元 (折り返し写像) を作れるので).

- Λ の $\mathrm{O}(V)$-orbit を Λ の **class**,

  Λ の $\mathrm{SO}(V)$-orbit を Λ の **proper class** という.

- Λ と Λ' が同じ class/proper class に入っているとき, Λ と Λ' は **equivalent**/**proper equivalent** であるという.

- Λ の genus の中には有限個の proper class しかないことが示せる.

- 完全系列

$$1 \to \mathrm{SO}(V) \to \mathrm{O}(V) \xrightarrow{\det} \{\pm 1\}$$

から, 各 class は高々2 つの proper class の disjoint union であることがわかる.

-

$$\mathrm{O}(\Lambda) := \{g \in \mathrm{O}(V) \mid g(\Lambda) \subseteq \Lambda\}$$
$$\mathrm{SO}(\Lambda) := \{g \in \mathrm{SO}(V) \mid g(\Lambda) \subseteq \Lambda\}$$

とおく. このとき,

Λ の proper class と class が一致 $\iff \mathrm{SO}(\Lambda) \neq \mathrm{O}(\Lambda)$.

- Λ を V の Q を保つ $\mathbb{Z}$-lattice とする. このとき, $g \in \mathrm{O}(V \otimes \mathbb{A}_f)$ なら, lattice $g\Lambda$ も Q を保つ.

3 Minkowski-Siegelの公式

M, N を $\mathbb{Z}$ 上の positive definite quadratic space で rank= m, n のものとする.

$$w(N) := \frac{1}{2} \sum_{N':\text{proper class} \in \text{gen}(N)} \frac{1}{\sharp \mathrm{SO}(N')},$$

$$m(M,N) := \frac{1}{2w(N)} \sum_{N':\text{proper class} \in \text{gen}(N)} \frac{\mathrm{R}_{N'}(M)}{\sharp \mathrm{SO}(N')}$$

$$\epsilon_{m,n} := \begin{cases} \frac{1}{2} & \text{if } n = m+1 \text{ または } n = m > 1 \\ 1 & \text{otherwise} \end{cases}$$

$$\alpha_\infty(M,N) := \pi^{\frac{1}{4}m(2n-m+1)} \Big(\prod_{i=0}^{m-1} \Gamma(\frac{n-i}{2})^{-1} \Big) (\det(N))^{\frac{-m}{2}} (\det(M))^{\frac{n-m-1}{2}}$$

とおく. このとき,

$$m(M,N) = \epsilon_{m,n} 2^{-\frac{m(m-1)}{2}} \alpha_\infty(M,N) \prod_l \alpha_l(M,N)$$

が成立.

4 supersingular elliptic curve

素数 p を fix. l を素数, $W = W(\bar{\mathbb{F}}_p)$, σ を W 上の Frobenius とする.
以下 E,E' などを $\bar{\mathbb{F}}_p$ 上の supersingular elliptic curve とする.

- $l \neq p$ に対し, $T_l(E) := \varprojlim_n E[l^n](\bar{\mathbb{F}}_p)$: l-進 Tate 加群 ($\simeq \mathbb{Z}_l^2$)
- $T_p(E) := \mathrm{D}_*(E[p^\infty])$: E の p-divisible 群 $E[p^\infty]$ の covariant Dieudonné 加群 ($\simeq W^2$)
  - $T_p(E)$ には σ-semilinear map Φ が付随している (Dieudonné 加群の「Frobenius」. だが, 今は covariant Dieudonné 理論を考えているので, Φ は $E[p^\infty]$ の Verschiebung V に対応している. Dieudonné 加群の「Vershibung」Ψ ($E[p^\infty]$ の Frobenius F に対応) の方は, $T_p(E)$ が W-自由加群であり $\Phi\Psi = \Psi\Phi = p$ であることから Ψ の情報を Φ から復元できるため, 考える必要はない)
- Φ は条件 $pT_p(E) \subsetneq \Phi(T_p(E)) \subsetneq T_p(E)$ を満たす ($\Phi(T_p(E)) = T_p(E)$ なら Φ が同型, ゆえ V が同型. $pT_p(E) = \Phi(T_p(E))$ なら Ψ が同型, ゆえ F が同型. どちらも supersinglar に反する). さらに, $T_p(E)$ の basis e_0, e_1 を適当に取ると, $\Phi(e_0, e_1) = (e_0, e_1) \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$ と書けることもわかる.
- $V_p(E) = \mathbb{Q}_p \otimes T_p(E)$ にも Φ(と Ψ) を延長させて考える. $L \subseteq V_p(E)$: $\mathbb{Z}_p$-lattice で, 条件 $pL \subsetneq \Phi(L) \subsetneq L$ を満たすものを考える. このとき, L の basis e_0', e_1' を適当に取ると, $\Phi(e_0', e_1') = (e_0', e_1') \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$ と書けることがわかる.

- これらの Tate 加群に対し,

$$\mathrm{Hom}(T_l(E), T_l(E')) := \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E), T_l(E')) \text{ if } l \neq p$$
$$\mathrm{Hom}(T_p(E), T_p(E')) := \mathrm{Hom}_{\mathbb{Z}_p,\Phi}(T_p(E), T_p(E'))$$

  と定める. End や Aut も同様. (Ψ との可換性は, Φ との可換性から自動的に出るので, 考えなくて良い)

- このとき,

$$\mathrm{End}(T_l(E)) := \begin{cases} \mathrm{End}_{\mathbb{Z}_l}(T_l(E)) \simeq \mathrm{M}_2(\mathbb{Z}_l) & \text{if } l \neq p \\ \mathrm{End}_{\mathbb{Z}_p,\Phi}(T_p(E)) \simeq \mathcal{O}_{D_p} \end{cases},$$

  但し D_p は $\mathbb{Q}_p$ 上の division quaternion algebra で, $\mathcal{O}_{D_p}$ はその (unique) maximal order.

  - 証明. $g = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ が $\Phi = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$ と可換になることは, $g = \begin{pmatrix} x & pz^\sigma \\ z & x^\sigma \end{pmatrix}$, 但し $x, z \in W(\mathbb{F}_{p^2})$, と書けることと同値. このような g 全体のなす $\mathbb{Z}_p$-algebra を R と書くと, $g \in R$ に対し $\det(g) = xx^\sigma - pzz^\sigma$ で, $W(\mathbb{F}_{p^2})$ は不分岐だから $\det(g) \neq 0$ である. このことから, $D_p = R \otimes \mathbb{Q}_p$ は $\mathbb{Q}_p$ 上の division quaternion algebra で, reduced norm が det で与えられることがわかる. R は不分岐二次拡大の整数環と D_p の素元 (=Nrd の付値が 1 になる元, たとえば $\begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$) を含むから, maximal order $\mathcal{O}_{D_p}$ と一致.

- 全ての supersingular elliptic curve/$\bar{\mathbb{F}}_p$ は isogenous であることが知られている (Tate の定理の帰結).

- したがって, $\mathbb{Q} \otimes \mathrm{Hom}(E, E') \simeq \mathbb{Q} \otimes \mathrm{End}(E)$ であり, 右辺は $\mathbb{Q}$ 上階数 4 だったので, 同型

$$\mathbb{Z}_l \otimes \mathrm{Hom}(E, E') \simeq \mathrm{Hom}(T_l(E), T_l(E')) \text{ for } \forall l$$

  を得る.

- これと右辺の local description から, $\mathbb{Q} \otimes \mathrm{End}(E)$ は $\{p, \infty\}$ で分岐する $\mathbb{Q}$ 上の quaternion algebra D で, $\mathrm{End}(E)$ はその maximal order $\mathcal{O}_D$ になっていることがわかる.

  - Weil pairing から, 上の同型は deg を Nrd に移すことがわかる. 二次形式の近似定理から, $(\mathrm{End}(E), \deg)$ と $(\mathcal{O}_D, \mathrm{Nrd})$ が同一視できることもわかる.

- $\forall l$ に対し, $V_l(E) := \mathbb{Q}_l \otimes T_l(E)$ とおく. これは $\mathbb{Q}_l$ 上階数 2 の自由加群.

  さらに,

$$T^p(E) := \prod_{l \neq p} T_l(E),$$
$$V^p(E) := \mathbb{Q} \otimes T^p(E),$$
$$T_f(E) := T^p(E) \times T_p(E),$$
$$V_f(E) := V^p(E) \times V_p(E)$$

  とおく.

  これらはそれぞれ, $\hat{\mathbb{Z}}^p$, $\mathbb{A}_f^p = \mathbb{Q} \otimes \hat{\mathbb{Z}}^p$, $\hat{\mathbb{Z}}^p \times W$, $\mathbb{A}_f^p \times \mathrm{Frac}(W)$ 上階数 2 の自由加群.