数理解析研究所講究録
第775巻 1992年 154-166

Supersingular Abelian Varieties の算術的理論

大阪大学教養部 伊吹山 知義 (Tomoyoshi Ibukiyama)

§0. 序

幾何学的不変量が数論的不変量に関係していることは、よくあることである。特にNéron Severi群が非常に大きい時などは、数論的概念の占める割合が大きいように思われる。Supersingular elliptic curve の理論は、その1例で、Deuring等により、数論との対応が非常によくわかっている。これがどの程度Supersingular Abelian Varieties に一般化されるかを述べるのが、本稿の目的である。内容的には、多少桂利行氏の原稿と重複が生じるかもしれないが、その点は御容赦願いたい。また、誰による結果かは、その都度、明示することにしたい。

§1. 整数論的手法の例.

本稿の主テーマにはいる前に、簡単な例をあげて、整数論的方法の有効性について述べてみたい。Aを閉体上のアーベ

ル多様体とする。A'をAと isogeny なアーベル多様体とする。さて、$\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ とすると、$\mathrm{End}^0(A)$ は有限次元の半単純環であり、$\mathrm{End}(A)$ はその整数環である。今 $\mathrm{End}(A)$ が極大整数環でかつ類数が1とすると次のことがなりたつ。

AからA'への isogeny φ で、$\varphi^{-1}\mathrm{End}(A')\varphi \subset \mathrm{End}(A)$ なるものが存在する。

つまり、isogeny を上手に選べば、$\mathrm{End}(A')$ はその isogeny を通じて皆 $\mathrm{End}(A)$ にもちあがる。証明は非常に簡単で、次の通りである。$\mathrm{Hom}(A, A')$ は 右 $\mathrm{End}(A)$-加群であり、$\mathrm{End}(A)$ の類数1より、$\mathrm{Hom}(A, A') = \varphi\,\mathrm{End}\,A$ なるφがある。$\lambda \in \mathrm{End}(A')$ なら $\lambda\varphi \in \varphi\,\mathrm{End}\,A$ となる。//

たとえば、Eが supersingular elliptic curve の時、$A = E^n$ とおくと、$n \geq 2$ なら上の仮定はみたされている。(類数が1であることは、強近似定理による。) また $n=2$ なら、$A' \sim E^2$ (isogeny) なる A' について、$\mathrm{End}(A')$ を皆具体的に書くことができる。(cf. [1]) これらを代数幾何のみを用いて示すのはむつかしいのではないかと思う。

§2. Supersingular elliptic curve

この節では、supersingular elliptic curve について、古典的に知られている結果について述べる。内容を、後の拡張のことを考えて箇条書きにする。結果は Deuring, Eichler

等による。

以下、Eで標数$p>0$の閉体上のsupersingular elliptic curveをあらわし、End(E), Aut(E)で群多様体としての準同型環及び自己同型群をあらわす。

(1) $\mathrm{End}^0(E)=\mathrm{End}(E)\otimes\mathbb{Q}=B$とおくと、Bは$p$と$\infty$でちょうど分岐する定符号4元数環であり、$\mathrm{End}(E)=\mathcal{O}$とおくと$\mathcal{O}$はBの極大整数環である。

(2) 閉体上のsupersingular elliptic curvesの同型類は、Bの類数Hと個数が等しい。また(当然であるが)Eの主偏極は唯1つである。

(3) $\mathrm{Aut}(E)\cong\mathbb{Z}/2$ or $\mathbb{Z}/4$ or $\mathbb{Z}/6$である。

(4) Eは皆$\mathbb{F}_{p^2}$上のmodelを持つ。また、$\mathbb{F}_p$上のmodelを持つものの閉体上の同型類の個数は、$2T-H$である。但しここでHはBの類数、TはBのtype number, すなわちB内の極大整数環の同型類の個数である。

(5) $\mathbb{F}_{p^2}$上のsupersingular elliptic curveで、$\mathbb{F}_{p^2}$-有理点の個数が、$1+p^2+2p$及び$1+p^2-2p$のものが、それぞれ存在する。(この個数はWeilの評価式の最大及び最小である。)

以上でH及びTの値はよく知られているが省略する。

§3. 一般化の準備

前節の内容は、その一部は完全に一般次元に拡張され、またその一部は部分的拡張がなされている。そのために必要な数論的概念について説明したい。前節の4元数環Bにからむ数論的不変量は、実際には代数群$B^\times$の概念であり、$B^\times$は$\otimes\mathbb{C}$で考えれば$GL_2(\mathbb{C})$である。これは(semi-simple partをとれば) A_1型でもありC_1型でもある。よってこれの一般化としては、たとえば $GL_n(B) = M_n(B)^\times$ 及び、quaternion hermitian group G_n:

$$G_n = \{g \in M_n(B) \;;\; g^t\bar{g} = n(g)1_n,\ n(g) \in \mathbb{Q}^\times\}$$

の2つが考えられる。ところで$M_n(B)$の類数は$n \geqq 2$なら1であり(強近似定理)この事実は、n個($n \geqq 2$)のsupersingular elliptic curvesの直積は、curvesをどう選んでも同型というDeligne-Ogus-Serre-Shiodaの定理に、反映されている。これ以外の部分では、G_nの方が中心的役割を果たす。さて、とりあえず、類数とtype numberについて説明したい。

B^n内のlattice Lを考える。Bの極大整数環$\mathcal{O}$を1つ固定する。Lがleft $\mathcal{O}$-moduleであるとき、Lを$\mathcal{O}$-latticeと呼ぶ。さて、次のようなleft $\mathcal{O}$-latticesの集合$\mathcal{L}(L)$

を考えよう。

$$\mathcal{L}(L) = \{ M \subset B^n ;\ M \text{は left } \mathcal{O}\text{-lattice で、すべての素数 } v \text{ に対し } M \otimes \mathbb{Z}_v = (L \otimes \mathbb{Z}_v) g_v \text{ for some } g_v \in G_v \}$$

ここで $\mathbb{Z}_v$ は v 進整数環、G_v は G_n のアデール化の v-part すなわち、

$$G_v = \{ g \in GL_n(B \otimes \mathbb{Q}_v) ;\ g\,{}^t\bar{g} = n(g) 1_n,\ n(g) \in \mathbb{Q}_v^{\times} \}$$

である。$\mathbb{Q}_v$ は v 進数体である。（標数の p と区別したいので v と書いた。）上のような集合 $\mathcal{L}(L)$ のことを、L の属する種 (genus) という。このうち、極大 $\mathcal{O}$-lattice と呼ばれる lattices の集合は 2 つの genus にわかれることが知られている。（Shimura による）1 つは $\mathcal{O}^n$ を含む種 $\mathcal{L}(\mathcal{O}^n)$ であり、principal genus と呼ばれる。他の 1 つは、これと区別するために、non principal genus と呼ぶ。両者共幾何学的意味を持つ。さて一般の $\mathcal{L}(L)$ に戻ろう。$\mathcal{L}(L)$ にはあきらかに右から G が作用しているが、この G-orbit は有限個しかない。これを $\mathcal{L}(L)$ の類数という。

$$\mathcal{L}(L) \text{ の類数} = \#(\mathcal{L}(L)/G_n)$$

この量は、勿論 $\mathcal{L}(L)$ のとり方には、よっている。但し、principal genus 及び non principal genus の類数は、極大整数環 $\mathcal{O}$ の選び方にはよらない。

次にBのtype numberの拡張を考える。Bのtype numberはBの極大整数環の同型類の個数のことであったが、Skolem-Noetherの定理より、極大整数環の$B^\times$-共役類の個数といっても同じことである。我々は$B^\times$の拡張としてG_nを考えているのであるから、一般化は次のように定義すればよい。

$\mathcal{L}(\mathcal{O}^n)/G_n$の代表系を$L_1, \cdots, L_H$とする。$M_n(B)$の部分環$R_i$を各$i=1 \sim H$に対し、

$$R_i = \{ g \in M_n(B) \ ; \ L_i g \subset L_i \}$$

と定義する。(R_iは実は皆極大整数環であり、$n \geqq 2$なら、皆$M_n(\mathcal{O})$と同型になる。) R_iとR_jは、あるG_nの元gに対し$g^{-1}R_i g = R_j$となるときG_n-共役という。

$\{R_1, \cdots, R_H\}$のG_n-共役類の個数をG_nのtype numberと呼ぶ。

$$G_n\text{のtype number} = \#\left(\{R_1, \cdots, R_H\}/\underset{G_n\text{-共役}}{\sim}\right)$$

もう1つだけ記号を準備しておく。任意の$\mathcal{O}$-lattice Lに対して、Lのmetricを変えない自己同型のなす群を$\mathrm{Aut}(L)$とかく。すなわち

$$\mathrm{Aut}(L) = \{ g \in G_n \ ; \ Lg = L \}$$

なお、以上の諸概念は、アデールを用いた方が説明がすっきりするが、当研究集会の性格を考慮に入れて、敢えてアデールなしで済ませた。

§4. Supersingular abelian varieties

Eを supersingular elliptic curve，nを$n \geqq 2$なる自然数とする。n次元アーベル多様体Aは，$A \cong E^n$のとき，superspecial，$A \sim E^n$ (isogeny) のとき supersingular という。この節の目的は§2の内容が上のようなAについて，どの程度拡張されているかを述べることにある。あえて定理とは書かずに，§2の番号にあわせて，順に箇条書きにしてみたい。moduli に関することはあとで述べる。

(1) Aが supersingular ならば勿論$\mathrm{End}^0(A) \cong M_n(B)$である。しかし$\mathrm{End}(A)$は一般には極大整数環ではない。たとえば，$n=2$なら極大整数環以外に2種類あらわれる。（手法は§1に述べた通り。）$n \geqq 3$は知られていない。

(2) 主偏極 superspecial abelian variety (E^n, Θ)の同型類の個数は，$\mathcal{L}(\mathcal{O}^n)$の類数$H$に等しい。(cf. [1])

(3) (E^n, Θ)と上の(2)で自然に対応する$L \in \mathcal{L}(\mathcal{O}^n)$に対し主偏極アーベル多様体としての自己同型群を$\mathrm{Aut}(E^n, \Theta)$と書くと

$$\mathrm{Aut}(E^n, \Theta) \cong \mathrm{Aut}(L)$$

である。また，$n=2$ならば$\mathrm{Aut}(E^2, \Theta)$は皆具体的にわかる。(cf. [1])

(4) Eとして$\mathbb{F}_{p^2}$上定義されたものを取っておけば，主偏極アーベル多様体(E^n, Θ)はいつでも$\mathbb{F}_{p^2}$-rational である。また，(E^n, Θ)のうちで，$\mathbb{F}_p$上定義された model (A, C)

を持つものの，閉体上の同型類の個数は $2T-H$ である。但しここで T は G_n の type number である。(cf.[2])

(5) $p \neq 2$ ならば，$\mathbb{F}_{p^2}$ 上定義された genus 3 の curve で $\mathbb{F}_{p^2}$-有理点の個数が $1+p^2+6p$ のものが存在する。(cf.[3]) これは Weil の評価式の最大値である。(genus 2 の curve は Serre の結果がある。)

さて，$n \geqq 2$ の時と $n=1$ の時の1つの違いは，$n \geqq 2$ の時には，moduli の次元があることである。主偏極アーベル多様体の moduli を $\mathcal{A}_{n,1}$ とするとき，supersingular abelian varieties のなす $\mathcal{A}_{n,1}$ 内の locus は，一般に既約ではない。既約成分の個数については既に桂氏も書いているので，ここではくり返さないが，少し他の面について述べてみたい。今 $n=2$ とすると上記の locus の既約成分の個数は，non principal genus の類数に等しく，また各既約成分の normalization は $\mathbb{P}^1$ に等しいことが知られている。(Katsura-Oort) ところで，その各成分には superspecial なものがのっていて，こちらは principal genus の類数個あるのであるから，全体の各成分にどのようにのっているのか気になるところである。実はこれが数論的な判定条件になるばかりではなく，もっと面白いこともわかる。これらを説明するには今少し数論的概念に深入りせねばならない。

今，$n=2$とし，$\mathcal{L}, \mathcal{L}'$を$B^2$のprincipal及びnon-principal genusとする。$L\in\mathcal{L}$，$L'\in\mathcal{L}'$とし，すべての素数vに対し

$$U_v = \{ g\in G_v ; (L\otimes \mathbb{Z}_v) g = L\otimes \mathbb{Z}_v \}$$

$$U_v' = \{ g\in G_v ; (L'\otimes \mathbb{Z}_v) g = L'\otimes \mathbb{Z}_v \}$$

とおく。G_AをG_2のadele化とする。G_Aの部分群$\mathcal{U}, \mathcal{U}'$を，$G_\infty$を$G_A$の$\infty$成分として，

$$\mathcal{U} = G_\infty \cdot \prod_v U_v \ , \quad \mathcal{U}' = G_\infty \cdot \prod_v U_v'$$

とおく。G_Aをそれぞれについて次のようにdouble cosetに分解する。

$$G_A = \coprod_{i=1}^{H} \mathcal{U} g_i G \ , \quad G_A' = \coprod_{i=1}^{H'} \mathcal{U}' g_i' G$$

ここでH，H'はそれぞれ$\mathcal{L}, \mathcal{L}'$の類数である。L，L'をうまく選べば，$v\neq p$については$U_v = U_v'$，$v=p$については$U_p\cap U_p'$が$G_p$のminimal parahoric群となるようにしておける。これを仮定し，$\mathcal{U}_0 = G_\infty \times \prod_{v\neq p} U_v \times (U_p\cap U_p')$とおく。また，

$$G_A = \coprod_{i=1}^{H_0} \mathcal{U}_0 g_i'' G$$

とする。（H_0は$\mathcal{U}_0$の類数ともいうべき量だが，この場合は対応するlatticeがあるわけではない。）さて，$\mathcal{U} g_i G$と$\mathcal{U}' g_i' G$の間には何の包含関係もないが，$\mathcal{U}_0 g_i'' G$は，どこかの$\mathcal{U}$-G-double coset及び$\mathcal{U}'$-G-double cosetに属するわけである。

<u>定理</u> (1) $\mathcal{U}'_{g_i}G$ に対応する既約成分に，$U_{g_j}G$ に対応する主偏極アーベル多様体 (E^2, Θ) がのっているための必要十分条件は，$\mathcal{U}'_{g_i}G$，$U_{g_j}G$ が共に共通の $\mathcal{U}''_{0g_i}G$ を1つは含むことである。

(2) 2次元主偏極 supersingular abelian surfaces の locus の arithmetic genus $= H_0 - H_1 - H_2 + 1$ である。

ここで $H_0 - H_1 - H_2 + 1$ という量は，U_0 に属する，weight 0 の保型形式のうちで new forms の次元であり，Jacquet–Langlands 対応の拡張を考える際に重要であった。(cf. [4])

なお，以上のような考察は，locus の連結性を示すためにも有効で実際 $n=2$ では，上と Bruhat-Tits theory 及び強近似定理で連結性が示せる。(Ekedahl) $n=3$ では locus の連結性は，ある種の Hecke operator の決める Brandt 行列の連結性と強近似定理に帰着する。(連結性は Ekedahl-Oort も得ているようであるが，私の証明とどういう関係かよく知らない。) なお，一般次元の locus のより深い構造については，まだ知られていない。この部分は最終的には G_n の数論により統制されるはずだと考えている。locus は smooth ではないので arith. genus 等のことはよくわからない。($n=2$ で

は、たまたまlocusが1次元なので、特異点があっても、arithmetic genusが定義される。）

もう1つ述べる。level 2のmoduli $\mathcal{A}_{2,1,2}$ から $\mathcal{A}_{2,1}$ へのcovering を考える。ここでlocusのcoveringを考えると、実は各 $L \in \mathcal{L}'/G_2$ に対し、Aut(L)は、対応する既約成分の分解群になっている。また、具体的にすべて求めることもできる。（cf. [5]）

§5. 手法上の注意

§4で述べたことをどのようにして証明するか、数論上のポイントに限って述べてみたい。数論上の手がかりは、G_n やlattice, Hecke operator 等にしかないのであるから、幾何学を全部これらの言葉に翻訳する必要がある。たとえば、Néron-Severi 群を End(A)の一部と同一視することにし、すべてをなるべく algebra または群論で考えるわけである。たとえば、定義体に関することであれば、Frobenius写像が問題になるが、これを algebra の元と思って、Weil criterion などを G_n の特殊な元の存在条件のようなものにおきかえる。その後は、跡公式等の手法で、具体的な計算を実行するわけである。実際には、このような過程で実は数論的手段も不足していることがわかり、新しく理論を作った部分もある。

たとえば、1つの種丈に対し、$\mathcal{L}/G=\{L_1,\cdots,L_H\}$ とするとき、$\mathrm{Aut}(L_i)$ を一斉によぶ方法は知られていなかった。これを原理的に解決し、また $n=2$ で実際に計算してみせたのが[5]である。このあたりは、今の所代数幾何的な手法では無理のようである。また、十分多くの $\mathbb{F}_{p^2}$ 有理点を持つ genus 3 の curve の存在証明も、ある種の mass が正になることを用いていて、存在定理であり、代数幾何的に構成するわけではない。

supersingular abelian varieties の理論では、まだまだ、数論が full に使われているとは言えない面もあり、今後も発展してゆくと思われる。

文献 (桂氏の稿も参照されたい。)

[1] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Compositio Math. 57 (1986)

[2] T. Ibukiyama and T. Katsura, On the field of definition of supersingular polarized abelian varieties and type numbers, preprint

[3] T. Ibukiyama, On rational points of curves of genus three over finite fields, preprint

[4] K. Hashimoto and T. Ibukiyama, On relations of dimensions of automorphic forms of $Sp(2, \mathbb{R})$ and its compact twist $Sp(2)$ (II) Adv. Stud. Pure Math. 7, 1985, 30-102

[5] T. Ibukiyama, On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula, Adv. Stud. Pure Math. 15, 1989, 301-349