

Some Remarks on Abelian Varieties

東大 理 塩田徹治

§0. アーベル多様体に関する次の問題を考える:

問題1. アーベル多様体 A とその部分アーベル多様体 B_1, B_2 が与えられたとき、商アーベル多様体 A/B_i について、
$$B_1 \simeq B_2 \implies A/B_1 \simeq A/B_2 \quad ?$$

問題2. A, A' を代数体 K 上定義されたアーベル多様体とし、 K の素イデアル $\mathfrak{p}$ について、 A, A' の reduction mod $\mathfrak{p}$ をそれぞれ $A(\mathfrak{p}), A'(\mathfrak{p})$ とかく。このとき、もし $A \neq A'$ (K の代数的閉体の上で) ならば、 $A(\mathfrak{p}) \simeq A'(\mathfrak{p})$ となる $\mathfrak{p}$ は高々有限個にかぎられるか?

問題1の特別な場合として、楕円曲線 E, E', E'' について次の問を答えることができる ("Cancellation problem"):

問題3. $E \times E' \simeq E \times E'' \implies E' \simeq E'' \quad ?$

問題4. $E \times E \simeq E \times E' \implies E \simeq E' \quad ?$

さて 答はいずれも一般には否定的である! それを示す

のが本稿の目的である。明らかに、問題3又は4の反例は、問題1の反例を与えるから、我々は主として直積型のアーベル曲面、即ち $A = E \times E'$ (E, E' : 楕円曲線) の形のものを考える。問題2に関しても、このよりの A, A' から反例を見出すことができる。

まずアーベル曲面 $A = E \times E'$ のピカール数 ρ について、次の事実を思い出す (cf. [1], Appendix)

$$\rho(A) = \begin{cases} 2 & E \not\sim E' \\ 3 & E \sim E', \quad \text{End}(E) = \mathbb{Z} \\ 4 & E \sim E', \quad \text{End}(E) \simeq \mathbb{Z}^2 \\ 6 & E \sim E', \quad \text{End}(E) \simeq \mathbb{Z}^4 \end{cases}$$

ここで、 $\sim$ は同種、 $\text{End}(E)$ は E の自己準同型環をあらわす。

命題 もし $\rho(E \times E') \leq 3$ ならば、問題3 (及び4) は正しい。

証明は省略する。一般の場合の結果は次の通り:

標数	問題3	問題4
0	No	Yes
$p > 0$	No	$\Leftarrow$ No

標数 $p > 0$ のとき、4の反例を supersingular な E を用いて構成する。標数0 (複素体上) の場合、特異アーベル曲面の理論 ([2]) を応用して、単に反例を与えるのみならず、問題3の完全な理解が可能である。

§ 1. まず問題 4 の標数 $p > 0$ における反例をあげる:

例 I $p \equiv 3 \pmod{4}$, $k = \mathbb{F}_{p^2}$ とし, 次の楕円曲線を考える

$$(1) \quad E: Y^2 = X^3 - X$$

$$(2) \quad E': Y^2 = (X+1)(X^2 - 4X - 4)$$

このとき $E \times E \simeq E \times E' \quad (k \text{ 上})$ であるが,

$p > 7$ ならば $E \not\simeq E' \quad (k \text{ の閉包 } \bar{k} \text{ 上でも})$ である。

次に, 問題 2 の反例:

例 II 上の楕円曲線 E および E' を Gauss の数体 $\mathbb{Q}(\sqrt{-1})$

の上で考え, アーベル曲面

$$(3) \quad A = E \times E, \quad A' = E \times E'$$

を考える。このとき

$$(4) \quad A \not\simeq A' \quad (\mathbb{C} \text{ 上})$$

$$(5) \quad A \bmod p \simeq A' \bmod p, \quad \forall p \equiv 3 \pmod{4}.$$

これを示すために, まず上の E を一般の体 k 上で考える。

E に無限遠点を原点^oとして群の構造を考えると, 2 等分点は

$$V: (X, Y) = (0, 0) \quad \text{及び} \quad W: (X, Y) = (1, 0) \quad \text{で生成される。}$$

簡単な計算により, 点 V 又は W による E 上の平行移動はそれぞれ

$$(X, Y) \rightarrow (-1/X, Y/X^2),$$

$$(X, Y) \rightarrow (X+1)/(X-1), -2Y/(X-1)^2)$$

で与えられる。従って、これらによる商曲線 $E/\langle v \rangle$, $E/\langle w \rangle$ について、 $E/\langle v \rangle \simeq E$, $E/\langle w \rangle \simeq E'$ が容易に確かめられる。
一方、不変量を見ると

$$j(E) = 2^6 \cdot 3^3, \quad j(E') = (2 \cdot 3 \cdot 11)^3$$

だから、 $E \simeq E' (\bar{k} \text{上})$ と成るのは、 $p=3$ または 7 に限る。

さて、よく知られているように、

$$E : \text{supersingular} \iff p \equiv 3 \pmod{4}.$$

しかも、このとき、 $k \ni \sqrt{-1}$ とする (i.e. $k \supset \mathbb{F}_p$) と、 E の k 上
有理的 $\mathbb{F}_p$ 自己同型環 $\text{End}_k(E)$ は rank 4 の加群となる。

そこで、例 I を証明するには、次の事が成立てば十分である：

アーベル曲面 $E \times E$ の $\mathbb{F}_p$ 自己同型 (群の意味でも) で

点 $(v, 0)$ と点 $(0, w)$ に写すものが存在する。

実際、これを認めると、 $E \times E$ と、これらの 2 等分点で割って

$$(E/\langle v \rangle) \times E \simeq E \times (E/\langle w \rangle) \quad (\bar{k} \text{上})$$

従って、 $E \times E \simeq E \times E' (\bar{k} \text{上})$ を得る。

補題 一般に E と、標数 p の supersingular 楕円曲線、
 $\ell \neq p$ と素数、 $v, w \in E$ の ℓ 等分点の群 E_ℓ の生成元とする。
2 のとき、 $\text{Aut}(E \times E) \ni f$ で、 $f(v, 0) = (0, w)$ と成るもの
が存在する。さらに、 $\text{End}_k(E) \simeq \mathbb{Z}^4$ かつ、 v, w が k 上
有理的なら、 f として k -有理的なものも与えられる。

証明. E の準同型 φ は $\mathbb{Z}/\ell$ 分裂の群 E_ℓ に制限する $\varphi|_{E_\ell}$ により、自然に群の準同型

$$\gamma: \text{End}_k(E) \rightarrow \text{End}(E_\ell)$$

が与えられる。 $\text{Ker}(\gamma) \ni \varphi \iff \varphi(x) = 0, \forall x \in E_\ell \iff \varphi = \ell \cdot \psi,$

$\exists \psi \in \text{End}_k(E)$, 故に

$$\bar{\gamma}: \text{End}_k(E)/\ell \cdot \text{End}_k(E) \hookrightarrow \text{End}(E_\ell).$$

ところで仮定より、 $\mathbb{Z}/\ell$ (素数) 上 4 次元のベクトル空間だから、 $\bar{\gamma}$ は同型、従って $\bar{\gamma}$ は全射となる。

そこで v, w は E_ℓ の $(\mathbb{Z}/\ell$ 上の) 基底であるから、 $\text{End}(E_\ell)$ の元 $v \mapsto w, w \mapsto 0$ なるものが存在する。上の注意から

$$\exists \varphi \in \text{End}_k(E) \quad \varphi(v) = w, \quad \varphi(w) = 0.$$

同様に

$$\exists \psi \in \text{End}_k(E), \quad \psi(v) = 0, \quad \psi(w) = v.$$

そこで $E \times E$ の自己同型 f_1, f_2 を次の形に定義する:

$$f_1(x, y) = (x, y + \varphi(x))$$

$$f_2(x, y) = (x + \psi(y), y).$$

このとき $f_1(v, 0) = (v, w) = f_2(0, w)$ 故に $f = f_2^{-1} \circ f_1$

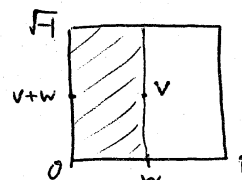
とあると、 f は補題の条件を満たす。 証終。

以上で、例 I が示された。例 II については、あと (4) を示せば十分である。

複素数体 $\mathbb{C}$ 上で、楕円曲線 (1), (2) は、夫々、次の複素トーラスと同視される。

$$E \simeq \mathbb{C} / (\mathbb{Z} + \mathbb{Z}\sqrt{1}) ,$$

$$E' \simeq \mathbb{C} / (\mathbb{Z} + \mathbb{Z}2\sqrt{1}) .$$



実際、前者は、 $\text{Aut}(E) \ni \sqrt{1}$ から明らか、後者は、 $E' \simeq E / \langle w \rangle$ となること（および $E / \langle v \rangle \simeq E$ ）から命ずる。

故に、(3) で定義されるアーベル曲面は、いわゆる特異アーベル曲面になる：すなわち、 $\rho(A) = \rho(A') = 4$ 。

一般に、 $\mathbb{C}$ 上の特異アーベル曲面 A に対し、 A 上の代数的サイクルの群 S_A は、 $H_2(A, \mathbb{Z})$ の rank 4 の部分加群であるから、その直交補空間として、“超越的サイクル”の群 T_A が定義され rank 2 である。今 T_A の底 $\{t_1, t_2\}$ で

$$\text{Im} \left(\int_{t_1} \omega / \int_{t_2} \omega \right) > 0$$

となるもの ω とする。ここに ω は A 上の正則 π 2-form である。

そして、 T_A の変換行列

$$Q_A = \begin{pmatrix} t_1 t_1 & t_1 t_2 \\ t_1 t_2 & t_2 t_2 \end{pmatrix}$$

を考えると、これは、 T_A の上のような基底の変換により

$$Q \rightarrow {}^t \gamma Q \gamma, \quad \exists \gamma \in \text{SL}_2(\mathbb{Z}),$$

となる。従って、次の対応が得られた：

$$A \mapsto \{Q_A\} \bmod \text{SL}_2(\mathbb{Z}).$$

特異アーベル曲面の理論 [2] により, これは 特異アーベル曲面の同型類の集合から 正定値偶整 = 元二次形式の狭義同値類の集合の上への 1対1の対応を与える。

さて, 問題の A, A' については [2] p. 265~により, 直ちに

$$Q_A \sim \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad Q_{A'} \sim \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$$

が分る。従って A と A' は $(\mathbb{C})$ 上同型であり得ない。故に

(4) が示され, 例 II の証明は終る。

§2. 標数 0 の時. 問題 3 (および 4) を与える。§0 で述べた命題により, $p(E \times E') \leq 3$ のときは, 正しいから,

$p(E \times E') = 4$, 即ち $E \times E'$ は特異アーベル曲面の時を与えなければよい。このとき, E と E' は同種で, 虚数乗法をもつ楕円曲線である。共通する虚数乗法の二次体を K とかく。

K の整数環を $\mathcal{O}$, その導写 f の order を $\mathcal{O}_f$ とかく (i.e. $\mathcal{O}_f$ は $\mathcal{O}$ の指数 f の唯一つの部分環)。すなわち

$$\text{End}(E) = \mathcal{O}_f, \quad \text{End}(E') = \mathcal{O}_{f'},$$

$$(f, f') = d.$$

とかく。この時,

定理 上のように E, E' が与えられたとき,

$$E \times E'' \simeq E \times E'$$

とある楕円曲線 E'' の同型類の個数は有限で: 次の公式で
与えられる:

$$\begin{aligned} N &= h(\mathcal{O}_{f'}) / h(\mathcal{O}_d) \\ &= (f'/d) \cdot [\mathcal{O}_d^\times : \mathcal{O}_{f'}^\times]^{-1} \prod_{p|f'd} \left(1 - \frac{\chi(p)}{p}\right). \end{aligned}$$

ここで $h(\mathcal{O}_{f'})$ は $\mathcal{O}_{f'}$ の類数, $\mathcal{O}_{f'}^\times$ は $\mathcal{O}_{f'}$ の単位の群, $\chi(p) = \left(\frac{K}{p}\right)$ は K の Legendre 記号である.

(証明は: §1 の最後で述べた特異アベリ曲面に関する結果により, 二次体の理論に帰着する. 詳しくことは [3] を参照されたい.)

特に $E = E'$ のときは $f = f'$ 上の $N = 1$. 即ち問題4が ① の場合成立する. ($p(E \times E) \leq 3$ のときは: §0 命題によって やはりよい). 他方 $N > 1$ とする例を与えることも容易で: これは問題3の反例を与える.

なお, こういう問題を考えた動機は, Kummer 曲面に関連した問題に由来するが, それについては [3] を見られたい.

Reference

- [1] T. Shioda, Algebraic cycles on certain K3 surfaces in char. p , Proc. Int. Conf. on Manifolds, Univ. Tokyo Press, 1975.
- [2] — and N. Mitani, Singular abelian surfaces and binary quadratic forms, in Springer Lecture Note 412, 1974
- [3] —, Some remarks on abelian varieties, (to appear)