Torsion points of abelian varieties with values in infinite extensions over a p-adic field

九州大学大学院数理学府数理学専攻 D1　小関 祥康

平成 20 年 5 月 31 日

本稿は, 筑波大学にて行われた第十三回代数学若手研究集会において講演した内容に関して, 時間の関係上発表できなかった内容も補足として若干加えたうえで, まとめたものである.

1　導入

アーベル多様体とは楕円曲線の概念を高次元化したもので, 多様体でありながらも有理点全体が群の構造を持っているようなものであり, 数論幾何において重要な研究対象である.

定義 1. (1) スキーム S 上の群スキーム A が **アーベルスキーム** (*abelian scheme*) であるとは, S 上滑らか (smooth), 固有 (proper), かつ幾何学的に既約なファイバー達 (geometrically irreducible fibers) をもつときをいう. さらに, 体 K に対して $S = \mathrm{Spec}(K)$ であるとき, A を K 上の **アーベル多様体** (*abelian variety*) と呼ぶ. 特に一次元のアーベル多様体を **楕円曲線** (*elliptic curve*) と呼ぶ.
(2) 体 K 上のアーベル多様体 A と K の体拡大 L に対して, A の **L-有理点** 全体のなす群 $A(L)$ を

$$A(L) := \mathrm{Hom}_{K\text{-Sch}}(\mathrm{Spec}(L), A)$$

で定義する.

群スキームの定義から, $A(L)$ は群構造を持つが, アーベル多様体の性質から, これはアーベル群の構造を持つということが分かる.

粗い言い方を許していただけるなら, アーベル多様体というものは, 有理点の集合がアーベル群の構造を持っているような「良い」多様体である.

さて, A を体 K 上のアーベル多様体とする. K の代数拡大 L に関するアーベル群 $A(L)$ の構造については古くから考えられてきた. L が K の有限次拡大である場合, 次の定理がよく知られている.

定理 2. L は K 上の有限次拡大体とする.
(1) (Mordell-Weil の定理) K を素体上有限生成の体とする. このとき,

$$A(L) \simeq \mathbb{Z}^{\oplus r} \oplus W,$$

ただし, r は 0 以上の整数, W は有限群.
(2) (Mattuck) K を p-進数体 $\mathbb{Q}_p$ の有限次拡大体とする. このとき,

$$A(L) \simeq \mathbb{Z}^{\oplus \dim(A)\cdot[L:\mathbb{Q}_p]} \oplus W,$$

ただし, W は有限群.

ここで, p は素数, $\mathbb{Z}$ は整数全体である. 上の定理 (1) に関して, 有理数体 $\mathbb{Q}$ 上の楕円曲線の場合を Mordell が示し, ヤコビ多様体の場合を Weil, 代数体 (すなわち, $\mathbb{Q}$ の有限次拡大) 上のアーベル多様体の場合を Taniyama, そしてその他の場合は Lang と Néron によって示された. とくに, 上の定理のような体 K では, L が K の有限次拡大であれば $A(L)$ のねじれ部分群 $A(L)_{\mathrm{tors}}$ は有限群になることが分かる.

ここまでの話は全て L が K の有限次拡大体の場合であるが, では L が K の無限次の代数拡大の場合は $A(L)_{\mathrm{tors}}$ は有限になるのであろうかと考えることは自然であるように思う. 例えば K が代数体の場合は多くの結果が Greenberg, Ribet, Silverberg, Zarhin, ... etc によって多くの結果が知られている.

一方, K が $\mathbb{Q}_p$ の有限次拡大の場合については, 代数体の場合に比べると, あまり $A(L)_{\mathrm{tors}}$ の有限性は知られていない. そこで私はこの場合の $A(L)_{\mathrm{tors}}$ の有限性に関する研究を進めてきた.

2 アーベル多様体のねじれ有理点の有限性

以下, p を素数, K は p-進数体 $\mathbb{Q}_p$ の有限次拡大とし、A は K 上のアーベル多様体とする. また, K の整数環を $\mathcal{O}_K$ と書き, 剰余体を k で表す. $\bar{K}, \bar{k}$ でそれぞれ K, k の代数閉包を表す. また, 一般のアーベル群 M と自然数 $n \geq 1$ に対して, n 倍で 0 になる元全体のなす M の部分群を $M[n]$ と書き, $M[p^\infty]$ で位数が p 冪の元全体のなす M の部分群を表すものとする. この節では, 次の問題に関して, 修士論文 [O] にて得られた結果の一部を紹介する.

問題. L が K 上の代数拡大であるとき, $A(L)_{\mathrm{tors}}, A(L)[p^\infty]$ は有限群か?

これを A の reduction type で場合分けして考える. この問題に関してよく知られている結果の一つとして, Imai により示された次の定理がある.

定理 3 ([Im])**.** *A が K 上 good reduction を持つとき, $A(K(\mu_{p^\infty}))_{\mathrm{tors}}$ は有限. ここで, $K(\mu_{p^\infty})$ は K に 1 の p 冪根全てを添加した体を表す.*

得られた結果を紹介する前に, アーベル多様体の reduction type について, 本文中に必要なものについて復習する.

定義 4. A が K 上 **good reduction を持つ**とは, A がある $\mathcal{O}_K$ 上のアーベルスキーム $\mathcal{A}$ の生成ファイバー $\mathcal{A} \times_{\mathcal{O}_K} K$ と同型であるときをいう. また, このとき, $\mathcal{A} \times_{\mathcal{O}_K} k$ のことを A の **reduction** と呼び, $\tilde{A}$ と書く.

一般に, A が K 上 good reduction を持つとき,

$$\tilde{A}(\bar{k})[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{d(A)}, \quad 0 \leq d(A) \leq \dim(A)$$

が成り立つ.

定義 5. (1) $d(A) = \dim(A)$ のとき, A は K 上 **ordinary good reduction を持つ**という.
(2) $\dim(A) = 1$ とする (すなわち, A は楕円曲線). $d(A) = 0$ のとき, A は **supersingular good reduction をもつ**という.
(3) その他, A が楕円曲線のとき, A が **multiplicative reduction** を持つ, **split multiplicative reduction** を持つ, **non-split multiplicative reduction** を持つ, **虚数乗法**を持つ, といった言葉は, [Si] によるものとする.

2.1 A が K 上 ordinary good reduction を持つ場合

A は K 上 ordinary good reduction を持つと仮定する. まず, この節の冒頭に述べた問題に対して次の結果を得た.

定理 6 ([O]). *L は K の代数拡大とする.*
(1) L の剰余体が K の剰余体の potentially prime-to-p 拡大であるとき, $A(L)[p^\infty]$ は有限.
(2) L が有限体を剰余体に持つとき, $A(L)_{\mathrm{tors}}$ は有限. 特に $A(L)[p^\infty]$ も有限.

ここで, 体拡大 F_2/F_1 が **potentially prime-to-p 拡大**とは, ある F_1 の有限次拡大体 F_1' が存在して, F_2 が, F_1' の有限次拡大体で拡大次数が p と素なものたちの和集合であるときをいう.

局所体上で上の問題を考えることの利点の一つとして, 同様の有限性の性質を代数体上のアーベル多様体に関して簡単に得ることができるというものがある. 例えば以下のことが上の定理から直ちに従う.

系 7 ([O]). *K を代数体, L を K の代数拡大, A を K 上のアーベル多様体とする. 次を仮定する :*
(i) ある p 上の L の素点 w が存在して, w の K への制限 v において, A は K 上 ordinary good reduction を持つ.
(ii) L の w における剰余体は, k の potentially prime-to-p 拡大.
このとき, $A(L)[p^\infty]$ は有限.

系 8 ([O]). *K を代数体, L を K の代数拡大, A を K 上のアーベル多様体とする. 次を仮定する :*
(i) ある p 上の L の素点 w が存在して, w の K への制限 v において, A は K 上 ordinary good reduction を持つ.
(ii) L の w における剰余体は有限体.
このとき, $A(L)_{\mathrm{tors}}$ は有限. 特に $A(L)[p^\infty]$ も有限.

再び局所体上の話に戻す. 上の定理 6 が応用可能な体 L の例として, $K(\mu_{p^\infty})$ や, K に supersingular reduction または multiplicative reduction をもつ K 上の楕円曲線 E の p 冪等分点全てを添加した体 $K(E[p^\infty])$ 等があげられる.

とくに, 定理 6 は定理 3 の, ordinary good reduction をもつアーベル多様体に関する一般化といえる.

2.2 A が楕円曲線で $L = K(E[p^\infty])$ の場合

ここでは, 節のはじめに取り上げた問題を, A が楕円曲線, L が K の p-進 Lie 拡大体 $K_{E,p} := K(E[p^\infty])$ (E : K 上の楕円曲線) である場合に考える.

$E_1 := A, E_2 := E$ とおけば, 今から考えていきたいのは, $E_1(K_{E_2,p})_{\mathrm{tors}}$ や $E_1(K_{E_2,p})[p^\infty]$ は有限になるのか否か, ということになる. (補足 : ℓ が p と異なる素数であるとき, $E_1(K_{E_2,p})[\ell^\infty]$ は必ず有限になるということは容易に分かる. 実際, $E_1(K_{E_2,p})[\ell^\infty] = E_1(K_{E_2,p} \cap K_{E_1,\ell})[\ell^\infty]$ であり, $K_{E_2,p} \cap K_{E_1,\ell}$ は K の有限次拡大であることから, 定理 2(2) により従う.) E_1, E_2 が K 上 ordinary good reduction を持つとき, $\tilde{E}_i(\bar{k})[p] \simeq \mathbb{Z}/p\mathbb{Z}$ $(i = 1, 2)$ への k の絶対 Galois 群 $G_k := \mathrm{Gal}(\bar{k}/k)$ の自然な作用が定める指標を $\tilde{\chi}_i : G_k \to GL(\tilde{E}_i(\bar{k})[p]) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ で表す.

E_1, E_2 が K 上 ordinary good reduction を持っているとき, 次が成り立つ.

命題 9 ([O])**.** E_1, E_2 が K 上 *ordinary good reduction* を持っていると仮定する.
(1) $\mathrm{Im}(\tilde{\chi}_1) \subset \mathrm{Im}(\tilde{\chi}_2)$ が成り立つとき, $E_1(K_{E_2,p})[p^\infty]$ は有限.
(2) K が 1 の p 乗根を全て含み, また, E_2 が虚数乗法を持つとき, $E_1(K_{E_2,p})[p^\infty]$ が有限になるための必要十分条件は $\mathrm{Im}(\tilde{\chi}_1) \subset \mathrm{Im}(\tilde{\chi}_2)$ が成り立つことである.

とくにこのとき, $p = 2$ であれば必ず $E_1(K_{E_2,p})[p^\infty]$ は無限になるということが (2) から分かる. また, E_1 が K 上 ordinary good reduction を持ち, E_2 が supersingular good reduction または multiplicative reduction を持つ場合は $E_1(K_{E_2,p})[p^\infty]$ が有限になることは 2.1 節の最後に述べたということに注意する.

E_1 が K 上 multiplicative reduction を持つときは, K の高々 2 次拡大体上で, E_1 は Tate curve と呼ばれる分かりやすい楕円曲線と同型になる. したがって, (Weil-pairing の存在により) $K(\mu_{p^\infty}) \subset K(E_{E_2,p})$ であることに注意すれば, この場合は $E_1(K_{E_2,p})[p^\infty]$ の有限性に関して, 次のようなこと等が簡単に確認できる.

命題 10 ([O])**.** (1) E_1 が K 上 *split multiplicative reduction* を持つと仮定する. このとき、$E_1(K_{E_2,p})[p^\infty]$ は無限. とくに $E_1(K_{E_2,p})_{\mathrm{tors}}$ も無限.
(2) E_1 は K 上 *non-split multiplicative reduction* を持ち, p は奇素数, $E_1(K_{E_2,p})[p] \subset E_2(K)$ と仮定する. このとき, $E_1(K_{E_2,p})[p^\infty]$ は有限.

最後に, E_1 が supersingular reduction を持つ場合はどうなのだろうか. この場合も, $E_1(K_{E_2,p})[p^\infty]$ が有限になるのか無限になるのかということが, 楕円曲線に付随して得られるある Lie 群 (または Lie 代数) の評価をすることによって, ほとんどの場合判定できる (cf. [Se], Chapter 4, Appendix). 例えば E_1 が supersingular reduction を持ち, E_2 が ordinary good reduction を持つ場合は $E_1(K_{E_2,p})[p^\infty]$ が有限になることが分かり, その他のほとんどの場合も判定できる.

参考文献

[Im] Hideo Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions*, Proc. Japan Acad. **51** (1975), 12-56.

[O] Yoshiyasu Ozeki, *Torsion points of abelian varieties with values in infinite extensions over a p-adic field*, 九州大学修士論文 (2008)

[Se] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, second ed., Avanced Book Classics.

[Si] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathmatics **106**, Springer-Verlag, (1986)