代数体の拡大で rank が増える楕円曲線について

東京都立大学大学院理学研究科　松野　一夫

1　序

本稿では次の問題 (の非常に特別な場合) を考察する.

問題 I. $K \subset K' \subsetneq L$ を代数体の有限次拡大とする. そのとき K 上の楕円曲線 A で

$$\mathrm{rank}_{\mathbb{Z}} A(L) > \mathrm{rank}_{\mathbb{Z}} A(K') \tag{1}$$

となるものは存在するか?

ここで $A(K')$, $A(L)$ は A の K', L 上の有理点全体のなす群 (Mordell–Weil 群) であり, それらが有限生成アーベル群になることはよく知られている. しかしそのアーベル群の構造, 特に rank に関してはわかっていないことが多く, 例えば具体的に与えられた楕円曲線 A に対してその rank を求めるアルゴリズムも知られていない.

問題 I は (特に $K = K'$ のとき) 与えられた代数体の拡大に対し, その拡大で rank が増える楕円曲線は存在するか, という素朴な疑問なのであるが, 一般にいつでも成り立つべきなのかどうかも良くわからない. しかし, 少なくとも拡大次数 $[L : K]$ が大きくない場合にはそのような曲線がいつでも存在すると想像される. 例えば L/K が 2 次拡大のときにはそのような楕円曲線を rank が正であるような曲線の twist として簡単に構成できる.

例. $[L : K] = 2$ のとき, $L = K(\sqrt{d})$ とすれば $y^2 = x^3 + 3d^2x$ で定義される K 上の楕円曲線 A は $\mathrm{rank}_{\mathbb{Z}} A(L) > \mathrm{rank}_{\mathbb{Z}} A(K)$ を満たす. ($A' : y^2 = x^3 + 3x$ とすると $\mathrm{rank}_{\mathbb{Z}} A'(\mathbb{Q}) = 1$ であることを使う.)

更に次の結果が知られている.

定理 (Rohrlich [R]). L/K を代数体の有限次拡大で $[L : K] \leq 9$ なるものとする. そのとき K 上の楕円曲線 A で, $K \subset K' \subsetneq L$ なる任意の中間体 K' に対して不等式 (1) を満たすものが存在する.

本稿では $[L : K] = 5$ の場合に (1) を満たす楕円曲線の無限族の簡単な構成法を紹介する.

2　主結果

次の記号のもとで主結果を述べる．K を任意の有限次代数体とし，

$$f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e \in K[x]$$

を既約 5 次多項式とする．$f(x)$ の根の 1 つ α を固定し，$L = K(\alpha)$ と置く．更に M を $f(x)$ の K 上の最小分解体とする．

定義 1. $t \in K$ に対し E_t を次の方程式で定義される K 上の射影曲線とする:

$$y^2 + txy + aey = x^3 - dx^2 + cex - e^2(t + b). \tag{2}$$

この Weierstrass 方程式の判別式

$$\Delta_{E_t} = e^2(t^7 + bt^6 + (ac - 12d)t^5 + (a^2d - 36ae - 12bd + c^2)t^4 + \cdots)$$

が 0 になる $t \in K$ は有限個であり ($f(x)$ の既約性より $e \neq 0$), その集合を $I_0 \subset K$ と書くことにすると E_t は任意の $t \in K \setminus I_0$ に対して楕円曲線になる．更に E_t の j 不変量は t に関して定数ではないので $\{E_t\}_{t\in K}$ には無限個の ($\overline{K}$ 上) 同型でない楕円曲線が含まれている．この楕円曲線の無限族の Mordell–Weil 群の rank に関する次の結果が本稿の主結果である．

定理 A. I_0 を含む有限部分集合 $I \subset K$ が存在し，I に含まれない任意の $t \in K$ に対して E_t は

$$\mathrm{rank}_{\mathbb{Z}} E_t(L) > \mathrm{rank}_{\mathbb{Z}} E_t(K), \quad \mathrm{rank}_{\mathbb{Z}} E_t(M) \geq \mathrm{rank}_{\mathbb{Z}} E_t(K) + 4 \tag{3}$$

を満たす．

注．除外集合 I を完全に決定することは理論的には可能であるが，現実には容易でない．しかし E_t が具体的に与えられれば (3) を満たす t は大抵すぐに見つかる．

すなわちこの定理は任意の 5 次拡大 L/K に対して問題 I の不等式 (1) を満たす楕円曲線の無限族を与えていることになる．以下この定理の証明の概略を述べる．まず $\mathrm{rank}_{\mathbb{Z}} E_t(L) > \mathrm{rank}_{\mathbb{Z}} E_t(K)$ となるためには $E_t(L) \setminus E_t(K)$ が位数無限の点を含む必要があるが，実は E_t は L 上に次の点を持つように構成したのであった．

補題 2. 点 $P = (-\frac{e}{\alpha}, e\alpha)$ は $E_t(L)$ に含まれる．

(証明)．$f(\alpha) = 0$ の両辺に $\frac{e^2}{\alpha^3}$ を掛ければ良い．　□

この点 P が (ほとんど全ての $t \in K$ で) 位数無限であり，実際に L/K で E_t の rank を増やすことを示せば良いのであるが，E_t それぞれを調べるよりも t を変数として関数体上の楕円曲線と見る方が考えやすい．そこで以下，E_t と同じ Weierstrass 方程式

(2) で定義される関数体 $K(t)$ 上の楕円曲線を E と書くことにし ($\Delta_E \in K[t]$ は 0 でない), 補題 2 の点 P も $E(L(t))$ 上の点と見なすことにする.

実は関数体上では次のより強い結果が示せる.

定理 B. 次が成り立つ.

$$E(K(t)) = \{0\}, \quad \mathrm{rank}_{\mathbb{Z}} E(L(t)) > 0, \quad E(M(t)) = E(\overline{K}(t)) \cong \mathbb{Z}^4.$$

注. $\mathrm{rank}_{\mathbb{Z}} E(K(t)) = 0$ であるが, $\mathrm{rank}_{\mathbb{Z}} E_t(K)$ の方は必ずしも 0 とは限らない. また $E_t(K)$ や $E_t(L)$ などは torsion-free であるとも限らないため, 関数体を経由せずに定理 A を証明しようとすると, このあとの議論がより大変になる.

特に rank に関しては

$$\mathrm{rank}_{\mathbb{Z}} E(L(t)) > \mathrm{rank}_{\mathbb{Z}} E(K(t)), \quad \mathrm{rank}_{\mathbb{Z}} E(M(t)) = \mathrm{rank}_{\mathbb{Z}} E(K(t)) + 4$$

が成り立つ. 定理 A はこれらと Silverman の定理 ([Sil, Theorem III.11.4]) から従う. (I としては特殊化写像 $E(L(t)) \to E_t(L)$ が単射にならない t の集合を取れば良い.)

定理 B の証明には楕円曲面の理論を用いる. $\mathcal{E} \to \mathbb{P}^1$ を $E \otimes \overline{K}(t)$ に対応する楕円曲面 ([Shi] 参照) とする. E の定義式 (2) の係数の t の次数が 1 次以下であることより, これは有理楕円曲面 (すなわち $\mathcal{E}$ は射影平面 $\mathbb{P}^2$ と双有理同値) になる ([Shi, 補題 6.13]). 有理楕円曲面に対応する関数体上の楕円曲線の Mordell–Weil 群の構造はその楕円曲面の特異ファイバーだけで完全に決定されることが知られている (アーベル群としてだけでなく格子としての構造; [OS], [Shi, §6] 参照) が, 今の場合, 変数変換して E を別の model に取りかえることで次はわかる.

補題 3. 楕円曲面 $\mathcal{E} \to \mathbb{P}^1$ は $t = \infty$ 上に I_5 型の特異ファイバーを持つ.

その他の特異ファイバーを決めるのは (E を定める $f(x)$ を任意に取っているため) 簡単ではないが, これだけでも [P] や [OS] の表から次が読み取れる.

系. (i) $\mathrm{rank}_{\mathbb{Z}} E(\overline{K}(t)) \leq 4$.

(ii) $\mathrm{rank}_{\mathbb{Z}} E(\overline{K}(t)) > 0$ のとき $E(\overline{K}(t))$ は torsion-free. そうでないとき $E(\overline{K}(t)) \cong \mathbb{Z}/5\mathbb{Z}$.

これより点 $P \in E(L(t)) \subset E(\overline{K}(t))$ が位数無限であることを示すには $5P \neq 0$ を言えば十分であり, これはすぐに確かめることができる. 特に $\mathrm{rank}_{\mathbb{Z}} E(L(t)) > 0$ がわかった. すると今度は $E(\overline{K}(t))$ が torsion-free になることより

$$\mathrm{rank}_{\mathbb{Z}} E(L(t)) > \mathrm{rank}_{\mathbb{Z}} E(K(t)) \tag{4}$$

がわかる. 実際, $P \notin E(K(t))$ より $P^\sigma \neq P$ となる $\sigma \in \mathrm{Gal}(M/K)$ が取れるが, そのとき $P^\sigma - P$ は位数無限だから, 任意の $n \neq 0$ に対し $nP^\sigma \neq nP$ で, 特に $nP \notin E(K(t))$

となる. よって $P \otimes 1$ は $E(K(t)) \otimes \mathbb{Q}$ に含まれず, (4) を得る. 更に $[L : K]$ が素数であることを使うと (4) は

$$\mathrm{rank}_{\mathbb{Z}} E(M(t)) \geq \mathrm{rank}_{\mathbb{Z}} E(K(t)) + 4$$

を導くことがわかる. これらをまとめて

$$\mathrm{rank}_{\mathbb{Z}} E(K(t)) = 0, \quad \mathrm{rank}_{\mathbb{Z}} E(M(t)) = \mathrm{rank}_{\mathbb{Z}} E(\overline{K}(t)) = 4$$

が得られた. 再び $E(\overline{K}(t))$ が torsion-free であることを使って定理 B の主張を得る.

3 例

最後に, 主結果の応用例として楕円曲線の岩澤理論に関係するものを挙げる.

p を素数とし, $\mathbb{Q}_\infty$ を有理数体 $\mathbb{Q}$ の円分 $\mathbb{Z}_p$ 拡大とする. すなわち $\mathbb{Q}_\infty$ は $\mathbb{Q}$ に 1 の p べき根をすべて添加した体の部分体であり, $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ が p 進整数環 $\mathbb{Z}_p$ の加法群と同型となる唯一のものである. $\mathbb{Q}_\infty/\mathbb{Q}$ には $\mathbb{Q}$ 上 p^n 次の中間体がただ一つ存在するが, それを $F_{p,n}$ と表わす.

楕円曲線の岩澤理論では, 楕円曲線に付随する Mordell–Weil 群や Tate–Shafarevich 群などの $\mathbb{Q}_\infty/\mathbb{Q}$ での振る舞いが問題になる. その中で Mordell–Weil rank に関しては次が知られている.

定理 (加藤, Rubin). A を $\mathbb{Q}$ 上の楕円曲線とするとき $A(\mathbb{Q}_\infty)$ は有限生成アーベル群である. 特に十分大きな n に対し $\mathrm{rank}_{\mathbb{Z}} A(F_{p,n})$ は一定.

注. この結果は有理数体だけでなく一般の代数体の円分 $\mathbb{Z}_p$ 拡大で正しいと予想されている (Mazur).

この定理により, A および p に対して次の量を定義することができる.

定義 4. $n_0(A, p)$ を次の性質を満たす最小の非負整数とする.

$$n > n_0(A, p) \Rightarrow \mathrm{rank}_{\mathbb{Z}} A(F_{p,n}) = \mathrm{rank}_{\mathbb{Z}} A(F_{p,n_0(A,p)}).$$

この量に関して Greenberg は次の問を提出している ([G2, Chapter 1]).

問題 II. 楕円曲線 $A/\mathbb{Q}$ や素数 p を動かすとき $n_0(A, p)$ はどのような値を取り得るか? 特にそれらは有界か否か?

つまり, 楕円曲線の A の $F_{p,n}$ 上の rank は上の定理によって十分大きな n で一定になることはわかるが, では実際にはどれくらいのところから一定になるのかという問である. この問について今のところ多くのことは知られていないが, もし 1 節の問題

I が肯定されれば任意の $m \geq 0$ に対し, $n_0(A,p) \geq m$ となる楕円曲線 $A/\mathbb{Q}$ が存在することになる (つまり $n_0(A,p)$ は A を動かすとき有界でない). また 1 節に挙げた Rohrlich の結果により

$$n_0(A_1,2) \geq 3,\ n_0(A_2,3) \geq 2,\ n_0(A_3,5) \geq 1,\ n_0(A_4,7) \geq 1$$

となる楕円曲線 A_1, A_2, A_3, A_4 が存在することはわかる. これらの曲線を [R] で与えられている構成法を使って具体的に求めるのは容易ではないが, Greenberg は $p = 2, 3$ の場合に次のような例を挙げている ([G1, Chapter 5], [G2, p. 8]).

例. $p = 2$, $A : y^2 + xy = x^3 - 115x + 392$ とすると

$$\mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}) = 0,\ \mathrm{rank}_{\mathbb{Z}} A(F_{2,1}) = 1,\ \mathrm{rank}_{\mathbb{Z}} A(F_{2,n}) = 3 \quad (n \geq 2).$$

特に $n_0(A,2) = 2$.

例. $p = 3$, $A : y^2 + xy = x^3 - 3x + 1$ とすると

$$\mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}) = 0,\ \mathrm{rank}_{\mathbb{Z}} A(F_{3,n}) = 2, \quad (n \geq 1).$$

特に $n_0(A,3) = 1$. ($F_{3,1} = \mathbb{Q}(\beta)$, $\beta^3 - 3\beta + 1 = 0$ であることに注意.)

本稿の主結果 (定理 A) は $p = 5$ の場合に $n_0(E_t,5) \geq 1$ となる楕円曲線の無限族 E_t の具体例を与える. 以下その一例を挙げる. 記号の簡略化のため $F = F_{5,1}$ と書く.

定義 1 の楕円曲線 E_t は $F = \mathbb{Q}(\alpha)$ となる α を決めるごとに定まるが, ここでは

$$\alpha = \mathrm{Tr}_{\mathbb{Q}(\zeta_{25})/F}(\zeta_{25}) = \zeta_{25} + \zeta_{25}^{-1} + \zeta_{25}^{7} + \zeta_{25}^{-7}$$

に対する曲線を考える. ただし ζ_{25} は 1 の原始 25 乗根であり, $\mathrm{Tr}_{\mathbb{Q}(\zeta_{25})/F}$ は $\mathbb{Q}(\zeta_{25})$ から F へのトレースを表わす. この α の $\mathbb{Q}$ 上の最小多項式は $f(x) = x^5 - 10x^3 + 5x^2 + 10x + 1$ であるから E_t は

$$y^2 + txy = x^3 - 10x^2 + 5x - t + 10$$

という方程式で定義される. E_t の判別式

$$\Delta_{E_t} = t^7 - 10t^6 - 120t^5 + 1225t^4 + 4440t^3 - 46832t^2 - 40960t + 484800$$

は $\mathbb{Q}$ 上既約なので, 全ての $t \in \mathbb{Q}$ で E_t は楕円曲線になる. (すなわち $I_0 = \emptyset$.) このとき定理 A より有限個を除くほとんど全ての $t \in \mathbb{Q}$ に対して点 $P = (-\alpha^{-1}, \alpha) \in E_t(F)$ は位数無限で

$$\mathrm{rank}_{\mathbb{Z}} E_t(F) \geq \mathrm{rank}_{\mathbb{Z}} E_t(\mathbb{Q}) + 4$$

となっていることがわかる.

さて, 定理 A の後にも述べたように, 除外しなくてはならない t を完全に決めることは難しい. その理由の一つは E_t の torsion 部分群がどうなるかが一般にはわからな

いところにある (関数体上では定理 B のように torsion まで完全にわかってしまう). しかし楕円曲線が具体的に与えられているような場合には, 適当な素点での reduction に条件を加えるなどして torsion を制限することで, rank が増えるような t を実際に無限個取り出すことができる. 今の場合には例えば 3 と 5 での reduction を見ることで次が示せる.

命題 5. E_t は上のとおりとする. そのとき $t \in \mathbb{Z}$ で $t \equiv 1, 4, 8, 11, 13, 14 \pmod{15}$ ならば実際に

$$\mathrm{rank}_{\mathbb{Z}} E_t(F) \geq \mathrm{rank}_{\mathbb{Z}} E_t(\mathbb{Q}) + 4$$

が成り立つ. 特に $n_0(E_t, 5) \geq 1$.

例. $t = 4$ とする. このとき E_4 は $y^2 = x^3 - 7x$ で定義される楕円曲線と同型である. $E_4(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ なので $\mathrm{rank}_{\mathbb{Z}} E_4(F) \geq 5$ となる.

参考文献

[G1] Greenberg, R.: *Iwasawa theory for elliptic curves*, in "Arithmetic Theory of Elliptic Curves", Lecture Notes in Math., vol. 1716, Springer-Verlag, 1999, pp. 51–144.

[G2] Greenberg, R.: *Introduction to Iwasawa theory for elliptic curves*, preprint, 1999.

[OS] Oguiso, K. and Shioda, T.: *The Mordell-Weil lattice of a rational elliptic surface*, Comm. Math. Univ. Sancti Pauli **40** (1991), 83–99.

[P] Persson, U.: *Configurations of Kodaira fibers on rational elliptic surfaces*, Math. Z. **205** (1990), 1–47.

[R] Rohrlich, D. E.: *Realization of some Galois representations of low degree in Mordell-Weil groups*, Math. Research Letters **4** (1997), 123–130.

[Shi] 塩田 徹治: "Mordell-Weil Lattice の理論とその応用", 東京大学数理科学セミナリーノート 1, 1993.

[Sil] Silverman, J. H.: "Advanced Topics in the Arithmetic of Elliptic Curves", Graduate Texts in Math., vol. 151, Springer-Verlag, 1994.