楕円曲線上の標準的高さについて

土屋和由（ 中央大学 ）

本稿は 2002 年 8 月 27 日から 8 月 29 日の間に行われた第 3 回「暗号理論とそれを支える代数曲線理論」ワークショップにおける小暮氏の講演 [3] の補足である．

楕円曲線暗号の安全性は楕円離散対数問題（ECDLP）の困難さに根拠をおいており，ECDLP への攻撃法の研究は大変重要である．近年，Silverman [5] によって xedni 計算法と呼ばれる攻撃法が提案された．それは素体上の楕円曲線に関する攻撃法であり，点自体を持ち上げてその持ち上げた点を通る曲線の上で考えるというものであった．xedni 計算法のアルゴリズムについては本報告集の谷戸氏の論説 [6] に詳しく記載されている．しかしながら，すぐにその攻撃法は有効に働かないという結果が発表された（Jacobson-Koblitz-Silverman-Stein-Teske [2]）．そうではあるが，そのアイデアは生きており現在においても xedni 計算法の改良，一般化の研究は続けられている．特に本報告集の小暮氏の論説 [3] において，素体の有限拡大上の Koblitz 曲線に対しての xedni 計算法の適用が報告されている．

本稿は xedni 計算法の中で「点の独立性」を判定するために用いられている標準的高さ（canonical height）に関する理論のまとめである．まず初めに射影空間上に高さを定義し，それを用いて楕円曲線上に（その上の有理関数に依存する）高さを定義する．そのある意味での極限をとったものが標準的高さである．標準的高さを用いて xedni 計算法で用いられる elliptic regulator の定義を与えることを目標とする．

楕円曲線上の高さは数論において重要な役割を持つ Mordell-Weil の定理の証明に用いられている．この定理は代数体上定義された楕円曲線の有理点のなす群が有限生成 Abel 群となる，というものである．$\mathbb{Q}$ 上の楕円曲線に対してこの定理は Mordell によって証明され，Weil によって代数体上の種数 1 以上の曲線の Jocobi 多様体に一般化された．

第 1 節では射影曲線上の高さに関する解説を行う．第 2 節において楕円曲線上の高さに関する解説を行い，Mordell-Weil の定理の証明を与える．第 3 節で標準的高さに関する解説を行う．

本稿をまとめるのにあたり，主に Silverman [4, CHAPTER VIII] を参考にした．

1. 射影空間上の高さ

この節では射影空間上の高さを定義する．楕円曲線上の高さは射影空間上の高さを用いて定義されており，たくさんの重要な性質がここから導かれる．特に Mordell-Weil の定理の証明で本質的な役割を果たす，ある種の有限性に関する定理を目標として話を進める．

有理数体 $\mathbb{Q}$ 上では斉次座標の絶対値の最大値として高さが定義される．しかしこれは $\mathbb{Q}$ の有理整数環 $\mathbb{Z}$ が PID （単項イデアル整域）であることを用いた定義であり，一般の代

数体上ではこのように定義できない．そこで付値論を用いて高さを定義する．

1.1 K を $\mathbb{Q}$ 上 n 次の代数体とする．K の素点（付値の同値類）の集合 $M_K = M_K^\infty \cup M_K^0$ を以下のように定義する．$K = \mathbb{Q}(\theta)$ となる θ をとり，θ のみたす $\mathbb{Q}$ 上の最小多項式を $f(T)$ とする．今 $f(T)$ の $\mathbb{C}$ 上での分解を $f(T) = (T-\theta_1)\cdots(T-\theta_n)$ とする．ここで $\theta_1, \ldots, \theta_{r_1}$ は実根，$\theta_{r_1+1}, \ldots, \theta_{r_1+2r_2} (r_1 + 2r_2 = n)$ は虚根で $\overline{\theta_{r_1+j}} = \theta_{r_1+r_2+j} (1 \leq j \leq r_2)$ であるとする．今 $\theta \mapsto \theta_i$ により定まる中への同型を $\sigma_i : K \to \mathbb{C}$ とする．$x \in K$ に対して $x^{(1)} = \sigma_1(x), x^{(2)} = \sigma_2(x), \ldots, x^{(n)} = \sigma_n(x)$ で表す．このとき，任意の i に対して

$$|x|_{\infty,i} = |x^{(i)}|$$

と定義する．ただし $|*|$ は普通の絶対値とする．このとき $|x|_{\infty,r_1+j} = |x|_{\infty,r_1+r_2+j} (1 \leq j \leq r_2)$ が成立する．ここで

$$M_K^\infty = \{|*|_{\infty,1}, \ldots, |*|_{\infty,r_1}, |*|_{\infty,r_1+1}, \ldots, |*|_{\infty,r_1+r_2}\}$$

と定義する．$\mathcal{O}_K$ を代数体 K の整数環とする．$\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアルとする．p を $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ をみたす素数とする．このとき

$$p\mathcal{O}_K = \mathfrak{p}^e \mathfrak{p}_2{}^{e_2} \cdots \mathfrak{p}_g{}^{e_g} \quad (\ \mathfrak{p}_2, \ldots, \mathfrak{p}_g \text{ は } \mathcal{O}_K \text{ の素イデアル }\ )$$

と表せる．今 $x \in K$ に対して

$$x\mathcal{O}_K = \mathfrak{p}^r \mathfrak{a}^{-1} \mathfrak{b}$$

と書けたとする．ただし，$\mathfrak{a}, \mathfrak{b}$ は $\mathcal{O}_K$ の整イデアルで，それぞれ $\mathfrak{a} + \mathfrak{p} = 1, \mathfrak{b} + \mathfrak{p} = 1$ をみたすものとする．ここで

$$|x|_\mathfrak{p} = p^{-\frac{r}{e}}$$

と定義し，M_K^0 を

$$M_K^0 = \{|*|_\mathfrak{p} \ \mid \ \mathfrak{p} \text{ は } \mathcal{O}_K \text{ の素イデアル}\}$$

と定義する．M_K^∞ の元はアルキメデス的素点であり，M_K^0 の元は非アルキメデス的素点である．

例 1.2. $K = \mathbb{Q}$ のとき

$$M_K^\infty = \{|*| : \text{普通の絶対値}\},$$
$$M_K^0 = \{|*|_p : p \text{ 進絶対値} \ \mid \ p \text{ は素数}\}$$

である．

$v \in M_K$ に対して $n_v = [K_v : \mathbb{Q}_{v_0}]$ とおく．ただし v_0 を v の $\mathbb{Q}$ への制限（このとき $v|v_0$ と記す），K_v を K の v に関する完備化，$\mathbb{Q}_{v_0}$ を $\mathbb{Q}$ の v_0 に関する完備化とする．

射影空間の点に関する高さを定義する．$P = [x_0, \ldots, x_N] \in \mathbb{P}^N(K)$ とする．このとき代数体 K に関する点 P の高さ $H_K(P)$ を

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}$$

で定義する．

高さの定義の well-defined 性，基本的性質を示さなければならないが，そのために付値論からの命題を用いる．証明等の詳細については例えば 彌永 [1] を参照されたい．

命題 1.3.（拡大公式） $L \supset K \supset \mathbb{Q}$ を代数体の拡大とする．また $v \in M_K$ とする．このとき

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K] n_v$$

が成立する．

命題 1.4.（norm 公式） K を付値 v を持つ体とし，L を K の有限次分離拡大とする．$w_1, \ldots, w_g$ を v の L への延長のすべてとする．このとき $x \in L$ に対して

$$\mathrm{N}_{L/K}(x) = \prod_{i=1}^{g} \mathrm{N}_{L_{w_i}/K_v}(\varphi_i(x))$$

が成立する．ただし $\mathrm{N}_{L/K}, \mathrm{N}_{L_{w_i}/K_v}$ はそれぞれ norm を表す．また $\varphi_i : L \to L_{w_i}$ は以下のように定義される．$L = K(\theta)$ とし，$f(T)$ を θ の K 上の最小多項式とする．$f(T) = f_1(T) \cdots f_g(T)$ を K_v での既約分解とする．任意の i に対して，$f_i(T)$ の根を $\theta_i^{(1)}, \ldots, \theta_i^{(n_i)}$ ($n_i = \deg f_i$) とする．$\varphi_i : L \to L_{w_i}$ を $\theta \mapsto \theta_i^{(1)}$ により定まる中への K 同型と定義する．

命題 1.5.（積公式） $x \in K^\times$ とする．このとき

$$\prod_{v \in M_K} |x|_v^{n_v} = 1$$

が成立する．

注意 1.6. $x \in K, v \in M_K$ とする．ここで $||x||_v = |x|_v^{n_v}$ と定義する．$||x||_v$ を v に属する正規付値とよぶ．特に $\mathfrak{p}$ を $\mathcal{O}_K$ の素イデアルとするとき

$$||x||_{\mathfrak{p}} = |x|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-r}$$

が成立する．ただし $\mathrm{N}_{K/\mathbb{Q}}$ は norm を表す．

命題 1.5 を用いて，高さの定義の well-defined 性を示す．

命題 1.7. K を代数体，$P \in \mathbb{P}^N(K)$ とする．このとき $H_K(P)$ は P の斉次座標の取り方に依らずに定まる．

（証明）$P = [x_0, \ldots, x_N] = [\lambda x_0, \ldots, \lambda x_N]$ とする．このとき

$$\begin{aligned} H_K([\lambda x_0, \ldots, \lambda x_N]) &= \prod_{v \in M_K} \max_{0 \le i \le N} \{|\lambda x_i|_v\}^{n_v} = \prod_{v \in M_K} |\lambda|_v^{n_v} \max_{0 \le i \le N} \{|x_i|_v\}^{n_v} \\ &= \prod_{v \in M_K} |\lambda|_v^{n_v} \prod_{v \in M_K} \max_{0 \le i \le N} \{|x_i|_v\}^{n_v} \end{aligned}$$

が成立する．**命題 1.5** より $\prod_{v \in M_K} |\lambda|_v^{n_v} = 1$ であるから

$$H_K([\lambda x_0, \ldots, \lambda x_N]) = \prod_{v \in M_K} \max_{0 \le i \le N} \{|x_i|_v\}^{n_v} = H_K([x_0, \ldots, x_N])$$

を得る．

以下，高さに関する基本的性質をみる．

命題 1.8. K を代数体，$P \in \mathbb{P}^N(K)$ とする．このとき
(1) $H_K(P) \ge 1$ が成立する．
(2) L/K を有限次拡大とする．このとき $H_L(P) = H_K(P)^{[L:K]}$ が成立する．

（証明）斉次座標において，射影空間の定義から少なくとも一つの座標を 1 にできるので (1) は明らか．以下 (2) を示す．今 $x_0, \ldots, x_N \in K$ であるから

$$H_L(P) = \prod_{w \in M_L} \max_{0 \le i \le N} \{|x_i|_w\}^{n_w} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max_{0 \le i \le N} \{|x_i|_v\}^{n_w}$$

が成立する．ここで，**命題 1.3** を用いることにより

$$H_L(P) = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max_{0 \le i \le N} \{|x_i|_v\}^{n_w} = \prod_{v \in M_K} \max_{0 \le i \le N} \{|x_i|_v\}^{[L:K]n_v} = H_K(P)^{[L:K]}$$

を得る．

1.9 さてここで $K = \mathbb{Q}$ の場合を考える．$P \in \mathbb{P}^N(\mathbb{Q})$ とする．このとき斉次座標を用いて $P = [x_0, \ldots, x_N]$ と表すことが出来る．ただし $x_0, \ldots, x_N \in \mathbb{Z}$ でかつ $\gcd(x_0, \ldots, x_N) = 1$

をみたす．このとき, 任意の $v \in M_K^0$ に対して $|x_i|_v \leq 1 \ \ (\forall i)$ であり，またある j が存在して $|x_j|_v = 1$ をみたす．よって

$$\prod_{p\ :\ \text{素数}} \max\{|x_0|_p, \ldots, |x_N|_p\} = 1$$

が成立する．したがって

$$H_{\mathbb{Q}}(P) = \prod_{v \in M_{\mathbb{Q}}} \max_{0 \leq i \leq N} \{|x_i|_v\} = \max\{|x_0|, \ldots, |x_N|\}$$

が成立する．このとき，任意の定数 C に対して

$$\#\{P \in \mathbb{P}^N(\mathbb{Q}) \mid H_{\mathbb{Q}}(P) \leq C\} < (2C+1)^{N+1}$$

が成立し，特に上の集合が有限集合であることが分かる．一般の代数体上に関してはその整数環が PID であるとは限らないので同じ議論を用いることは出来ない.

例 1.10. $K = \mathbb{Q}(\sqrt{-5}), P = [1, \frac{1+\sqrt{-5}}{2}, \frac{1-\sqrt{-5}}{2}] \in \mathbb{P}^2(K)$ とする．$H_K(P)$ を求める．

まず M_K^∞ 部分に関して考察を与える．任意の $a + b\sqrt{-5} \in K$ に対して

$$|a+b\sqrt{-5}|_{\infty,1} = |a+b\sqrt{-5}|, \quad |a+b\sqrt{-5}|_{\infty,2} = |a-b\sqrt{-5}|$$

とする．このとき

$$M_K^\infty = \{\ |*|_{\infty,1}\ \}$$

である．一方

$$n_{|*|_{\infty,1}} = [\mathbb{Q}(\sqrt{-5})_{|*|_{\infty,1}} : \mathbb{Q}_{|*|}] = [\mathbb{C} : \mathbb{R}] = 2$$

が成立する．したがって

$$\prod_{v \in M_K^\infty} \max\left\{|1|_v, \left|\frac{1+\sqrt{-5}}{2}\right|_v, \left|\frac{1-\sqrt{-5}}{2}\right|_v\right\}^{n_v} = \max\left\{1, \sqrt{\frac{3}{2}}, \sqrt{\frac{3}{2}}\right\}^2 = \frac{3}{2}$$

を得る．次に M_K^0 部分を考察する．今 K の整数環 $\mathcal{O}_K$ は $\mathbb{Z}[\sqrt{-5}]$ であり

$$\mathfrak{p}_1 = (2, 1+\sqrt{-5}),\ \mathfrak{p}_2 = (3, 1+\sqrt{-5}),\ \mathfrak{p}_3 = (3, 1-\sqrt{-5})$$

は $\mathcal{O}_K$ の素イデアルである．今

$$(2) = {\mathfrak{p}_1}^2,\ (1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2,\ (1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$$

が成立するので，分数イデアルをもちいて

$$\left(\frac{1+\sqrt{-5}}{2}\right) = {\mathfrak{p}_1}^{-1}\mathfrak{p}_2,\ \left(\frac{1-\sqrt{-5}}{2}\right) = {\mathfrak{p}_1}^{-1}\mathfrak{p}_3$$

と表せる．一方，各素イデアルの norm は

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1) = 2, \quad \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3) = 3$$

である．したがって

$$\begin{aligned}\prod_{v\in M_K^0} \max\left\{|1|_v, \left|\frac{1+\sqrt{-5}}{2}\right|_v, \left|\frac{1-\sqrt{-5}}{2}\right|_v\right\}^{n_v} \\ = \max\{1,2,2\}\max\left\{1,\frac{1}{3},1\right\}\max\left\{1,1,\frac{1}{3}\right\} = 2\end{aligned}$$

が成立する．以上をあわせて

$$H_K(P) = \frac{3}{2}\times 2 = 3$$

を得る．

命題 1.8 から，代数体の取り方に依らない高さの定義を与えることが出来る．$P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ とする．P の（絶対）高さ $H(P)$ を以下で定義する．$P \in \mathbb{P}^N(K)$ となる代数体 K を一つ選ぶ．このとき

$$H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$$

と定義する．

有理数体 $\mathbb{Q}$ 上成立した有限性を一般に考えるために命題を用意する．まず，射影空間の射と高さの関係を調べる．

命題 1.11. $F : \mathbb{P}^N \to \mathbb{P}^M$ を次数 d の射とする．このとき（ F に依存する）定数 C_1, C_2 が存在して，任意の $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ に対して

$$C_1 H(P)^d \le H(F(P)) \le C_2 H(P)^d$$

が成立する．

（証明）まず記号を準備する．$F = [f_0, \dots, f_M]$ とする．ただし $f_0, \dots, f_M$ は d 次斉次式である．$P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}})$ とする．ここで代数体 K を $\mathbb{Q}$ に $x_0, \dots x_N$ および各 f_i の係数を添加した体とする．任意の $v \in M_K$ に対して

$$\begin{aligned}&|P|_v = \max\{|x_0|_v, \dots, |x_N|_v\},\\ &|F(P)|_v = \max\{|f_0(P)|_v, \dots, |f_M(P)|_v\},\\ &|F|_v = \max\{|a|_v \mid a \text{ は多項式 } f_0, \dots, f_M \text{ の係数 }\}\end{aligned}$$

とおく．このとき

$$H_K(P) = \prod_{v\in M_K} |P|_v^{n_v}, \quad H_K(F(P)) = \prod_{v\in M_K} |F(P)|_v^{n_v}$$

であるので，$H_K(F)$ を上と同様に

$$H_K(F) = \prod_{v \in M_K} |F|_v^{n_v} \ (= H_K([a_0, a_1, \dots]))$$

と定義する．今，ε を

$$\varepsilon(v) = \begin{cases} 1 & v \in M_K^\infty \\ 0 & v \in M_K^0 \end{cases}$$

で定義する．このとき任意の $v \in M_K$ に対して

$$|t_1 + \cdots + t_n|_v \leq n^{\varepsilon(v)} \max\{|t_1|_v, \dots, |t_n|_v\} \tag{1}$$

が成立する．

以上の準備の下で，証明に戻る．$v \in M_K$ とする．各 f_i は d 次斉次式であったから (1) より

$$|f_i(P)|_v \leq {C_1}^{\varepsilon(v)} |F|_v |P|_v^d$$

が成立する．ただし C_1 は f_i の項の個数であり，$C_1 < \binom{N+d}{N}$ が成立する．したがって

$$|F(P)|_v \leq {C_1}^{\varepsilon(v)} |F|_v |P|_v^d$$

が成立する．よって

$$\prod_{v \in M_K} |F(P)|_v^{n_v} \leq \prod_{v \in M_K} {C_1}^{\varepsilon(v) n_v} |F|_v^{n_v} |P|_v^{n_v d}$$

が成立し，さらに

$$H_K(F(P)) \leq {C_1}^{\sum_{v \in M_K} \varepsilon(v) n_v} H_K(F) H_K(P)^d$$

を得る．

ところが一方

$$\sum_{v \in M_K} \varepsilon(v) n_v = \sum_{v \in M_K^\infty} n_v = [K : \mathbb{Q}]$$

が成立するので

$$H(F(P)) \leq C_1 H(F) H(P)^d$$

を得る．

次に lower bound をみる．仮定から F は射であったから

$$\{Q \in \mathbb{A}^{N+1}(\overline{\mathbb{Q}}) \mid f_0(Q) = \cdots = f_M(Q) = 0\} = \{(0, \dots, 0)\}$$

が成立する．よって Hilbert の零点定理より

$$(X_0, \ldots, X_N) = I(V(f_0, \ldots, f_{,M})) = \sqrt{(f_0, \ldots, f_M)}$$

を得る．したがって，整数 $e \geq 1$ が存在して，任意の i に対して

$$X_i{}^e = \sum_{j=0}^{M} g_{ij} f_j$$

をみたす多項式 $g_{ij} \in \overline{\mathbb{Q}}[X_0, \ldots, X_N]$ が存在する．ここで，代数体 K を $g_{ij} \in K[X_0, \ldots, X_N]$ をみたすように取り直す．さらに，多項式 g_{ij} は $e-d$ 次斉次多項式であると仮定してよい．ここで

$$\begin{aligned} |G|_v &= \max\{|b|_v \mid b \text{ は多項式 } g_{ij} \text{ の係数 }\}, \\ H_K(G) &= \prod_{v \in M_K} |G|_v{}^{n_v} \end{aligned}$$

とおく．今

$$|x_i|_v{}^e = \left| \sum_{j=0}^{M} g_{ij}(P) f_j(P) \right| \leq C_2{}^{\varepsilon(v)} \max_{0 \leq j \leq M} \{|g_{ij}(P) f_j(P)|_v\}$$

が成立する．よって

$$|P|_v{}^e \leq C_2{}^{\varepsilon(v)} \max_{\substack{0 \leq i \leq N \\ 0 \leq j \leq M}} \{|g_{ij}(P)|_v\} |F(P)|_v$$

を得る．一方 $\deg g_{ij} = e - d$ より

$$|g_{ij}(P)|_v \leq C_3{}^{\varepsilon(v)} |G|_v |P|_v{}^{e-d}$$

が成立するので

$$|P|_v{}^d \leq C_4{}^{\varepsilon(v)} |G|_v |F(P)|_v$$

を得，さらに

$$H(P)^d \leq C H(F(P))$$

を得る．

系 1.12. $A \in PGL_N(\overline{\mathbb{Q}})$ とする．このとき（A に依存する）定数 C_1, C_2 が存在して，任意の $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ に対して

$$C_1 H(P) \leq H(AP) \leq C_2 H(P)$$

が成立する．

次に，多項式の係数と根の間の高さの関係をみる．まず，記号の準備から始める．任意の $x \in \overline{\mathbb{Q}}$ に対して $H(x) = H([x,1])$ とおく．同様に $x \in K$ に対して $H_K(x) = H_K([x,1])$ とおく．

命題 1.13. 多項式 $f(T) \in \overline{\mathbb{Q}}[X]$ を

$$f(T) = a_0T^d + a_1T^{d-1} + \cdots + a_d = a_0(T-\alpha_1)\cdots(T-\alpha_d) \quad (a_0 \neq 0)$$

とおく．このとき

$$2^{-d}\prod_{j=1}^{d} H(\alpha_j) \leq H([a_0,\ldots,a_d]) \leq 2^{d-1}\prod_{j=1}^{d} H(\alpha_j)$$

が成立する．

（証明）$f(T)$ を $f(T)/a_0$ に置き換えることにより，$a_0 = 1$ と仮定してよい．$K = \mathbb{Q}(\alpha_1,\ldots,\alpha_d)$ とおく．**命題 1.11** と同様の議論から，

$$2^{-d\varepsilon(v)}\prod_{j=1}^{d}\max\{|\alpha_j|_v, 1\} \leq \max_{0\leq i\leq d}\{|a_i|_v\} \leq 2^{(d-1)\varepsilon(v)}\prod_{j=1}^{d}\max\{|\alpha_j|_v, 1\} \tag{2}$$

を証明すればよいことがわかる．

多項式の次数 $d := \deg f$ に関する帰納法を用いる．$d = 1$ のとき $f(T) = t - \alpha_1$ と表されるので (2) は明らか．

次に（K に解を持つ）すべての $d-1$ 次以下の多項式に関して (2) が成立すると仮定する．任意の i に対して

$$|\alpha_k|_v \geq |\alpha_i|_v$$

をみたす α_k を一つ選ぶ．さらに

$$\begin{aligned} g(T) &= \frac{1}{T-\alpha_k}f(T) = (T-\alpha_1)\cdots(T-\alpha_{k-1})(T-\alpha_{k+1})\cdots(T-\alpha_d) \\ &= b_0T^{d-1} + b_1T^{d-2} + \cdots + b_{d-1} \end{aligned}$$

と定義する．$f(T) = (T-\alpha_k)g(T)$ より，係数を比較して

$$a_i = b_i - \alpha_k b_{i-1} \quad (0 \leq i \leq d)$$

を得る．ただし $b_{-1} = b_d = 0$ と定義する．このとき

$$\begin{aligned} \max_{0\leq i\leq d}\{|a_i|_v\} &= \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \leq 2^{\varepsilon(v)}\max_{0\leq i\leq d}\{|b_i|_v, |\alpha_k b_{i-1}|_v\} \\ &\leq 2^{\varepsilon(v)}\max_{0\leq i\leq d}\{|b_i|_v\}\max\{|\alpha_k|_v, 1\} \leq 2^{(d-1)\varepsilon(v)}\prod_{j=1}^{d}\max\{|\alpha_j|_v, 1\} \end{aligned}$$

を得る．実際，不等式 (1) および帰納法の仮定を用いればよい．

次に lower bound をみる．$|\alpha_k|_v \leq 2^{\varepsilon(v)}$ のとき，k の選び方から

$$\prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} \leq \max\{|\alpha_k|_v, 1\}^d \leq 2^{d\varepsilon(v)}$$

が成立する．$a_0 = 1$ より lower bound を得る．

$|\alpha_k|_v > 2^{\varepsilon(v)}$ と仮定する．このとき

$$\max_{0\leq i\leq d}\{|a_i|_v\} = \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \geq 2^{-\varepsilon(v)} \max_{0\leq i\leq d}\{|b_i|_v\} \max\{|\alpha_k|_v, 1\}$$

が成立する．実際 $b_s = \max_{0\leq i\leq d}\{|b_i|_v\}$ とおくと $v \in M_K^\infty$ のとき

$$\begin{aligned}\max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} &\geq |b_{s+1} - \alpha_k b_s|_v = |\alpha_k b_s - b_{s+1}|_v \geq |\alpha_k b_s|_v - |b_{s+1}|_v \\ &\geq (|\alpha_k|_v - 1)|b_s|_v > 2^{-\varepsilon(v)}|\alpha_k|_v|b_s|_v\end{aligned}$$

を得る．また $v \in M_K^0$ のとき

$$\max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \geq |b_{s+1} - \alpha_k b_s|_v = |\alpha_k|_v|b_s|_v$$

を得る．したがって，帰納法の仮定から

$$2^{-d\varepsilon(v)} \prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} \leq \max_{0\leq i\leq d}\{|a_i|_v\}$$

を得る．

まず高さの Galois 不変性に関する補題を示し，そのあと有限性を証明する．

補題 1.14. $P \in \mathbb{P}^N(\overline{\mathbb{Q}}), \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ する．このとき $H(P^\sigma) = H(P)$ が成立する．

（証明）代数体 K を $P \in \mathbb{P}^N(K)$ をみたすものとする．$K/\mathbb{Q}$ は Galois 拡大であると仮定してよい．今，体の同型 $\sigma : K \to K^\sigma; x \mapsto x^\sigma$ から，写像 $\sigma : M_K \to M_{K^\sigma}; v \mapsto v^\sigma$ が誘導される．すなわち $x \in K, v \in M_K$ に対して $|x^\sigma|_{v^\sigma} = |x|_v$ と定義することにより上の写像を得る．さらに $K_v \xrightarrow{\sim} K_{v^\sigma}^\sigma$ も得る．特に $n_v = n_{v^\sigma}$ を得る．このとき

$$H_{K^\sigma}(P^\sigma) = \prod_{w\in M_{K^\sigma}} \max_{0\leq i\leq N}\{|x_i^\sigma|_w\}^{n_w} = \prod_{v\in M_K} \max_{0\leq i\leq N}\{|x_i^\sigma|_{v^\sigma}\}^{n_{v^\sigma}} = \prod_{v\in M_K} \max_{0\leq i\leq N}\{|x_i|_v\}^{n_v} = H_K(P)$$

が成立する．$[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$ より $H(P^\sigma) = H(P)$ を得る．

定理 1.15. C, d を定数とする．このとき

$$\#\{P \in \mathbb{P}^N(\overline{\mathbb{Q}}) \mid H(P) \leq C,\ [\mathbb{Q}(P) : \mathbb{Q}] \leq d\} < \infty$$

が成立する．特に，任意の代数体 K に対して

$$\#\{P \in \mathbb{P}^N(K) \mid H(P) \leq C\} < \infty$$

が成立する．

（証明）$P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ とする．今 $P = [x_0, \ldots, x_N]$ $(x_j = 1)$ と表されるとする．このとき $\mathbb{Q}(P) = \mathbb{Q}(x_0, \ldots, x_N)$ が成立する．よって

$$H_{\mathbb{Q}(P)}(P) = \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq N} \{|x_i|_v\}^{n_v} \geq \max_{0 \leq i \leq N} \left\{ \prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v, 1\} \right\} = \max_{0 \leq i \leq N} H_{\mathbb{Q}(P)}(x_i)$$

を得る．今 $H(P) \leq C$, $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$ とすると

$$\max_{0 \leq i \leq N} H(x_i) \leq C, \quad \max_{0 \leq i \leq N} [\mathbb{Q}(x_i) : \mathbb{Q}] \leq d$$

が成立する．したがって

$$\#\{x \in \overline{\mathbb{Q}} \ \mid \ H(x) \leq C, \ [\mathbb{Q}(x) : \mathbb{Q}] \leq d\} < \infty$$

を示せばよい．

$$x \in \{x \in \overline{\mathbb{Q}} \ \mid \ H(x) \leq C, \ [\mathbb{Q}(x) : \mathbb{Q}] \leq d\}$$

とする．$e = [\mathbb{Q}(x) : \mathbb{Q}]$ とおくと $e \leq d$ が成立する．ここで $y_1 = x, y_2, \ldots, y_e$ を x の $\overline{\mathbb{Q}}$ 上の共役元とする．x の $\mathbb{Q}$ 上の最小多項式を

$$f_x(T) = (T - y_1) \cdots (T - y_e) = T^e + a_1 T^{e-1} + \cdots + a_e \in \mathbb{Q}[T]$$

とする．このとき，仮定および上の **命題 1.13**，**補題 1.14** より

$$H([1, a_1, \ldots, a_e]) \leq 2^{e-1} \prod_{j=1}^{e} H(y_i) = 2^{e-1} H(x)^e \leq (2C)^d$$

が成立する．$1, a_1, \ldots, a_e \in \mathbb{Q}$ より，定理は $K = \mathbb{Q}$ の場合に帰着されるが，上で考察したとおり $K = \mathbb{Q}$ の場合, 定理は成立する．

2. 楕円曲線上の高さ

この節では射影空間上の高さを用いて楕円曲線上の高さを定義する．Mordell-Weil の定理を証明するためにある種の有限性が必要であるが，それは射影空間上の有限性からの簡単な帰結である．しかしそれだけでは不十分であり，楕円曲線上の高さが「定数倍を除い

て」二次形式になるという性質を示さなければならない．この事実は次節で扱う標準的高さにも関係が深い．

2.1 K を代数体，E を K 上の楕円曲線とする．このとき定数でない $E_{\overline{K}}$ の有理関数 $f \in \overline{K}(E)$ は射

$$f : E \longrightarrow \mathbb{P}^1$$
$$P \longmapsto \begin{cases} [1,0] & P \text{ が } f \text{ で極を持つ} \\ [f(P),1] & \text{その他} \end{cases}$$

を定める．このとき $f : E \to \mathbb{P}^1$ は全射である．楕円曲線 E 上の高さを f を用いて射影空間 $\mathbb{P}^1$ 上で定義すればよいが，加法的に扱うために対数をとる．

射影空間上の（絶対対数）高さ $h : \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{R}$ を $h(P) = \log H(P)$ で定義する．**命題 1.8** より，任意の $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ に対して $h(P) \geq 0$ が成立する．K を代数体，E を K 上の楕円曲線とする．$f \in \overline{K}(E)$ とし，f は定数でないとする．このとき（f に関する）E 上の高さ $h_f : E(\overline{K}) \to \mathbb{R}$ を $h_f(P) = h(f(P))$ で定義する．**定理 1.15** を用いて，楕円曲線上の高さに関する有限性をみる．

定理 2.2. K を代数体，E を K 上の楕円曲線とする．$f \in \overline{K}(E)$ とし，f は定数でないとする．このとき，任意の定数 C に対して

$$\#\{P \in E(K) \mid h_f(P) \leq C\} < \infty$$

が成立する．

（証明）射 $f : E \to \mathbb{P}^1$ は次数有限である．したがって

$$\#\{Q \in \mathbb{P}^1(K) \mid H(Q) \leq e^C\} < \infty$$

を示せばよい．これは **定理 1.15** より成立する．

上の **定理 2.2** は Mordell-Weil の定理を証明するのに重要であるが，それだけでは不十分である．以下，楕円曲線 E 上の高さと群構造との関係をみる．そのために，まず記号および言葉を導入する．

X を集合とする．f, g を X 上の実数値関数とする．このとき $f = g + O(1)$ であるとは，ある定数 C_1, C_2 が存在して，任意の $P \in X$ に対して $C_1 \leq f(P) - g(P) \leq C_2$ が成立することであると定義する．K を代数体，E を K 上の楕円曲線とする．$f \in K(E)$ とし，f は定数でないとする．f が偶関数であるとは f が -1 倍写像で不変，すなわち $f \circ [-1] = f$ が成立することをいう．このとき，以下の定理が成立する．

定理 2.3. K を代数体，E を K 上の楕円曲線とする．$f \in K(E)$ を定数でない偶関数とする．このとき，任意の $P, Q \in E(\overline{K})$ に対して

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$$

が成立する．

定理を証明するために，まず補題をいくつか準備する．まず，判別式に関するある恒等式を示す．証明は実際に計算を確かめればよい．

補題 2.4. $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ を体 K 上の楕円曲線とする．Δ を判別式 $\Delta = 4A^3 + 27B^2 \neq 0$ とする．さらに多項式 F, G, f, g をそれぞれ

$$\begin{aligned} F(X,Z) &= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4, \\ G(X,Z) &= 4X^3Z + 4AXZ^3 + 4BZ^4, \\ f(X,Z) &= 12X^2Z + 16AZ^3, \\ g(X,Z) &= 3X^3 - 5AXZ^2 - 27BZ^3 \end{aligned}$$

とおく．このとき

$$f(X,Z)F(X,Z) - g(X,Z)G(X,Z) = 4\Delta Z^4$$

が成立する．

補題 2.5. K を体，E を

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

で定義される K 上の楕円曲線とする．$f \in K(E) = K(x, y)$ とする．このとき

$$f \text{ が偶関数} \iff f \in K(x)$$

が成立する．

（証明）$P = (x_0, y_0)$ のとき $-P = (x_0, -y_0 - a_1x_0 - a_3)$ であるから $(\Leftarrow)$ は明らか．$(\Rightarrow)$ を示す．

$$f(x,y) = g(x) + h(x)y \quad (g, h \in K(x))$$

とおく．このとき

$$g(x) + h(x)y = f(x,y) = f(x, -y - a_1x - a_3) = g(x) + h(x)(-y - a_1x - a_3)$$

を得る．よって

$$(2y + a_1x + a_3)h(x) = 0$$

が成立する．

$2 = a_1 = a_3 = 0$ と仮定すると，$\Delta = 0$ となり E が楕円曲線であることに矛盾する．したがって $h(x) = 0$ が成立し，$f(x,y) = g(x) \in K(x)$ を得る．

補題 2.6. K を代数体，E を K 上の楕円曲線とする．$f, g \in K(E)$ を定数でない偶関数とする．このとき

$$(\deg g)h_f = (\deg f)h_g + O(1)$$

が成立する．

（証明）$x, y \in K(E)$ を E の Weierstrass 座標とする．このとき **補題 2.5** から

$$K(E) = K(x, y) \supset K(x) = \{ \text{偶関数} \}$$

であるから，射 $\rho : \mathbb{P}^1 \to \mathbb{P}^1$ が存在して $f = \rho \circ x$ が成立する．したがって **命題 1.11** から

$$h_f = (\deg \rho)h_x + O(1)$$

を得る．
一方 $f = \rho \circ x$ より

$$\deg f = \deg x \deg \rho = 2 \deg \rho$$

が成立するので

$$2h_f = (\deg f)h_x + O(1)$$

を得る．同様にして

$$2h_g = (\deg g)h_x + O(1)$$

が成立するので

$$(\deg g)h_f = (\deg f)h_g + O(1)$$

を得る．

（ **定理 2.3** の証明）楕円曲線 E の Weierstrass 方程式を

$$E : y^2 = x^3 + Ax + B$$

のように選ぶ．**補題 2.6** より，$f = x$ のときを示せばよい．今 $h_x(P) = h_x(-P), h_x(O) = 0$ が成立する．ただし O は無限遠点を表す．したがって $P = O$ または $Q = O$ のとき

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q)$$

が成立する．

以下，$P \neq O$ かつ $Q \neq O$ と仮定する．$x(P) = [x_1, 1], x(Q) = [x_2, 1]$ とおく．さらに

$$\begin{aligned} G : E \times E &\longrightarrow E \times E \\ (P, Q) &\longmapsto (P + Q, P - Q), \end{aligned}$$

$$\begin{aligned} \sigma : E \times E &\longrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^2 \\ (P, Q) &\longmapsto (x(P), x(Q)) \\ ([\alpha_1, \beta_1], [\alpha_2, \beta_2]) &\longmapsto [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2], \end{aligned}$$

$$\begin{aligned} g : \mathbb{P}^2 &\longrightarrow \mathbb{P}^2 \\ [t, u, v] &\longmapsto [u^2 - 4tv, 2u(At + v) + 4Bt^2, (v - At)^2 - 4Btu] \end{aligned}$$

と定義する．このとき，図式

$$\begin{array}{ccc} E \times E & \xrightarrow{G} & E \times E \\ \downarrow & & \downarrow \\ \sigma \quad \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \quad \sigma \\ \downarrow & & \downarrow \\ \mathbb{P}^2 & \xrightarrow{g} & \mathbb{P}^2 \end{array} \tag{3}$$

は可換である．実際，$P = Q$ のとき $x(2P) = [x_3, 1]$ とおくと

$$x_3 = \frac{(x_1^2 - A)^2 - 8Bx_1}{4y_1^2}$$

が成立し，$P \neq Q$ かつ $P \neq -Q$ のとき $x(P + Q) = [x_3, 1], x(P - Q) = [x_4, 1]$ とおくと

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}, \quad x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}$$

が成立することから導かれる．

次に $g : \mathbb{P}^2 \to \mathbb{P}^2$ が射であることを示す．$g([t, u, v]) = 0$ と仮定する．$t = 0$ のとき $u = v = 0$ が成立する．$t \neq 0$ と仮定する．以下，$g([t, u, v]) = 0$ が共通零点を持たないことを示す．$x = u/2t$ とおく．$u^2 - 4tv = 0$ より $x^2 = v/t$ が成立する．また

$$\begin{cases} 2u(At + v) + 4Bt^2 = 0 \\ (v - At)^2 - 4Btu = 0 \end{cases}$$

であるから

$$\begin{cases} \psi(x) := 4x(A + x^2) + 4B = 4x^3 + 4Ax + 4B = 0 \\ \phi(x) := (x^2 - A)^2 - 8Bx = x^4 - 2Ax^2 - 8Bx + A^2 = 0 \end{cases}$$

が成立する．**補題 2.4** より

$$(12x^2+16A)\phi(x)-(3x^2-5Ax-27B)\psi(x)=4\Delta\neq 0$$

を得る．したがって共通零点が存在しないことが示された．

g が射であることが示されたので，上の可換図式に **命題 1.11** を適用する．すると

$$h(\sigma(P+Q,P-Q))=h(\sigma\circ G(P,Q))=h(g\circ\sigma(P,Q))=2h(\sigma(P,Q))+O(1)$$

が成立する．したがって，任意の $R_1,R_2\in E(\overline{K})$ に対して

$$h(\sigma(R_1,R_2))=h_x(R_1)+h_x(R_2)+O(1)$$

を示せばよい．$R_1=R_2=O$ のときは明らか．$R_1\neq O$ かつ $R_2=O$ とする．このとき $x(R_1)=[\alpha_1,1]$ とおくと

$$\begin{aligned}h(\sigma(R_1,R_2))&=h([0,1,\alpha_1])=\log H([[0,1,\alpha_1]),\\ h_x(R_1)+h_x(R_2)&=h_x(R_1)=\log H([\alpha_1,1])\end{aligned}$$

より

$$h(\sigma(R_1,R_2))=h_x(R_1)+h_x(R_2)$$

が成立する．$R_1\neq O$ かつ $R_2\neq O$ とする．$x(R_1)=[\alpha_1,1],x(R_2)=[\alpha_2,1]$ とおくと

$$\begin{aligned}h(\sigma(R_1,R_2))&=h([1,\alpha_1+\alpha_2,\alpha_1\alpha_2]),\\ h_x(R_1)+h_x(R_2)&=h(\alpha_1)+h(\alpha_2)\end{aligned}$$

が成立する．ここで **命題 1.13** を多項式 $(T+\alpha_1)(T+\alpha_2)$ に適用することにより

$$h(\alpha_1)+h(\alpha_2)-\log 4\leq h([1,\alpha_1+\alpha_2,\alpha_1\alpha_2])\leq h(\alpha_1)+h(\alpha_2)+\log 2$$

を得る．したがって

$$h([1,\alpha_1+\alpha_2,\alpha_1\alpha_2])=h(\alpha_1)+h(\alpha_2)+O(1)$$

が成立する．

系 2.7. K を代数体，E を K 上の楕円曲線とする．$f\in K(E)$ を定数でない偶関数とする．

(1) $Q\in E(\overline{K})$ を一つ固定する．このとき任意の $P\in E(\overline{K})$ に対して

$$h_f(P+Q)\leq 2h_f(P)+O(1)$$

が成立する．

(2) $m\in\mathbb{Z}$ とする．任意の $P\in E(\overline{K})$ に対して

$$h_f([m]P)=m^2h_f(P)+O(1)$$

が成立する．

（証明）(1) は **定理 2.3** より明らか．(2) を示す．f は偶関数であるから $m \geq 0$ と仮定してよい．m に関する帰納法を用いる．$m = 0, 1$ のとき明らか．$m-1, m$ に関して定理が成立すると仮定する．このとき **定理 2.3** において $P = [m]P, Q = P$ を適用すると

$$h([m+1]P) = -h_f([m-1]P) + 2h_f([m]P) + 2h_f(P) + O(1)$$

が成立する．帰納法の仮定から

$$\begin{aligned} h([m+1]P) &= -(m-1)^2 h_f(P) + 2m^2 h_f(P) + 2h_f(P) + O(1) \\ &= (m+1)^2 h_f(P) + O(1) \end{aligned}$$

を得る．

2.8 以下 Mordell-Weil の定理の証明を行う．弱 Mordell-Weil の定理と呼ばれる以下の定理から導く．

定理 2.9.（弱 Mordell-Weil の定理） K を代数体，E を K 上の楕円曲線とする．$m \geq 2$ とする．このとき $E(K)/mE(K)$ は有限群である．

定理 2.10.（ Mordell-Weil の定理） K を代数体，E を K 上の楕円曲線とする．このとき $E(K)$ は有限生成 Abel 群である．

（証明）$Q_1, \ldots, Q_r \in E(K)$ を

$$E(K)/mE(K) = \{\overline{Q_1}, \ldots, \overline{Q_r}\}$$

であるように選ぶ（**定理 2.9** より選べる）．$P \in E(K)$ とする．このとき

$$P = [m]P_1 + Q_{i_1} \quad (1 \leq i_1 \leq r)$$

と書ける．この操作を繰り返すことにより

$$\begin{aligned} P_1 &= [m]P_2 + Q_{i_2} \\ &\vdots \\ P_{n-1} &= [m]P_n + Q_{i_n} \end{aligned}$$

を得る．ここで定数でない偶関数 $f \in K(E)$ を一つ選び，高さ h_f を考える．任意の j に対して，**系 2.7** より

$$h_f(P_j) \leq \frac{1}{m^2}[h_f([m]P_j) + C_2] = \frac{1}{m^2}[h_f(P_{j-1} - Q_{i_j}) + C_2] \leq \frac{1}{m^2}[2h_f(P_{j-1}) + C_1' + C_2]$$

を得る．したがって

$$h_f(P_n) \leq \left(\frac{2}{m^2}\right)^n h_f(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2)$$
$$< \left(\frac{2}{m^2}\right)^n h_f(P) + \frac{C_1' + C_2}{m^2 - 1} \leq \frac{1}{2^n} h_f(P) + \frac{C_1' + C_2}{2}$$

が成立する（最後の不等式は $m \geq 2$ を用いる）．今 n を十分大きく取ると

$$h_f(P_n) \leq 1 + \frac{C_1' + C_2}{2}$$

が成立し，また

$$P = [m^n]P_n + \sum_{j=1}^{n} [m^{j-1}]Q_{i_j}$$

であるから P は

$$\{Q_1, \ldots Q_r\} \cup \left\{ Q \in E(K) \mid h_f(Q) \leq 1 + \frac{C_1' + C_2}{2} \right\}$$

の元の線型和である．したがって **定理 2.2** より $E(K)$ の有限生成性がいえた．

3. 楕円曲線上の標準的高さ

前節では代数体上の楕円曲線に対して高さを定義し，それを用いて Mordell-Weil の定理を証明した．そのとき用いた高さは偶関数に依存するものであり，そこで用いた定理も「定数倍を除いて」二次形式になるというものだった．それらを補正するために，高さの極限をとって標準的高さ（canonical height）を定義する．

標準的高さはある $\mathbb{R}$ 線型空間上の正定値二次形式になっており，それを用いて Néron-Tate pairing と呼ばれる双線型形式および elliptic regulator と呼ばれるものが定義される．その性質が xedni 計算法における点の独立性の判定に用いられる．

3.1 K を代数体，E を K 上の楕円曲線とする．E 上の標準的高さ $\hat{h} : E(\overline{K}) \to \mathbb{R}$ を

$$\hat{h}(P) = \frac{1}{\deg f} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

で定義する．ただし $f \in K(E)$ は定数でないある偶関数である．

上の極限が収束することおよび f の取り方に依らずに定まることを見る．

命題 3.2.（Tate） K を代数体，E を K 上の楕円曲線とする．$f \in K(E)$ を定数でない偶関数とする．$P \in E(\overline{K})$ とする．このとき

$$\frac{1}{\deg f} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

は収束し，さらに f に依らずに定まる．

（証明）$\mathbb{R}$ 上の数列 $\{4^{-N}h_f([2^N]P)\}_N$ が Cauchy 列であることを示せばよい．**系 2.7** から，ある定数 C が存在して，任意の $Q \in E(\overline{K})$ に対して

$$|h_f([2]Q) - 4h_f(Q)| \leq C$$

が成立する．$0 \leq M \leq N \in \mathbb{Z}$ とする．このとき

$$\begin{aligned}
&|4^{-N}h_f([2^N]P) - 4^{-M}h_f([2^M]P)| \\
&\leq \left| \sum_{n=M}^{N-1} \{4^{-(n+1)}h_f([2^{n+1}]P) - 4^{-n}h_f([2^n]P)\} \right| \\
&\leq \sum_{n=M}^{N-1} 4^{-(n+1)}|h_f([2^{n+1}]P) - 4h_f([2^n]P)| \leq \sum_{n=M}^{N-1} 4^{-(n+1)}C \leq \frac{C}{4^{M+1}}
\end{aligned}$$

が成立する．したがって $\{4^{-N}h_f([2^N]P)\}_N$ が Cauchy 列であることが示された．

$g \in K(E)$ を f と異なる定数でない偶関数とする．**補題 2.6** から

$$(\deg g)h_f = (\deg f)h_g + O(1)$$

が成立する．したがって

$$(\deg g)4^{-N}h_f([2^N]P) - (\deg f)4^{-N}h_g([2^N]P) = \frac{O(1)}{4^N}$$

を得る．いま，右辺に $N \to \infty$ を施すと $\frac{O(1)}{4^N} \to 0$ が成立する．したがって，極限が一致することが示された．

標準的高さに関する基本的性質をみる．

定理 3.3.（Néron-Tate） K を代数体，E を K 上の楕円曲線とする．$\hat{h}$ を E 上の標準的高さとする．このとき，以下が成立する．
(1) 任意の $P, Q \in E(\overline{K})$ に対して

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

が成立する．
(2) 任意の $P \in E(\overline{K}), m \in \mathbb{Z}$ に対して

$$\hat{h}([m]P) = m^2\hat{h}(P)$$

が成立する．
(3) $\hat{h}$ は E 上の二次形式である．すなわち $\hat{h}$ は対称二次形式であり

$$\begin{aligned}
< \ , \ > \ : E(\overline{K}) \times E(\overline{K}) &\longrightarrow \mathbb{R} \\
(P, Q) &\longmapsto \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)
\end{aligned}$$

は双線型写像である．
(4) $P \in E(\overline{K})$ とする．このとき $\hat{h}(P) \geq 0$ が成立する．さらに

$$\hat{h}(P) = 0 \Longleftrightarrow P \in E(\overline{K})_{\mathrm{tors}}$$

が成立する．
(5) $f \in K(E)$ を定数でない偶関数とする．このとき

$$(\deg f)\hat{h} = h_f + O(1)$$

が成立する．
さらに $\hat{h}' : E \to \mathbb{R}$ をある定数でない f に対して (5) をみたし，かつ任意の $m \geq 2$ に対して (2) をみたすものとする．このとき $\hat{h} = \hat{h}'$ が成立する．

（証明）まず (5) を示す．今 **命題 3.2** の証明よりある定数 C が存在して，任意の $0 \leq M \leq N \in \mathbb{Z}$ および任意の $P \in E(\overline{K})$ に対して

$$|4^{-N}h_f([2^N]P) - 4^{-M}h_f([2^M]P)| \leq \frac{C}{4^{M+1}}$$

が成立する．ここで $M = 0, N \to \infty$ を施すことにより

$$|(\deg f)\hat{h}(P) - h_f(P)| \leq \frac{C}{4}$$

を得る．したがって

$$(\deg f)\hat{h} = h_f + O(1)$$

が成立する．
(1) を示す．**定理 2.3** より，任意の $P, Q \in E(\overline{K})$ に対して

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$$

が成立する．よって

$$\begin{aligned}\frac{4^{-N}}{\deg f}h_f([2^N](P+Q)) + \frac{4^{-N}}{\deg f}h_f([2^N](P-Q)) \\ = 2\frac{4^{-N}}{\deg f}h_f([2^N](P)) + 2\frac{4^{-N}}{\deg f}h_f([2^N](Q)) + \frac{O(1)}{4^N}\end{aligned}$$

を得る．ここで $N \to \infty$ を施すことにより

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

を得る．

(2) を示す．**系 2.7** より，任意の $P \in E(\overline{K}), m \in \mathbb{Z}$ に対して

$$h_f([m]P) = m^2 h_f(P) + O(1)$$

が成立する．このとき (1) と同様の操作を行うことにより

$$\hat{h}([m]P) = m^2 \hat{h}(P)$$

を得る．

(3) は (1) より線型代数から結果を得る．

(4) を示す．$\hat{h}(P) \geq 0$ は明らか．$P \in E(\overline{K})_{\mathrm{tors}}$ とする．このとき $m \geq 1 \in \mathbb{Z}$ が存在して $[m]P = O$ が成立する．このとき (2) より

$$m^2 \hat{h}(P) = \hat{h}([m]P) = \hat{h}(O) = 0$$

が成立する．したがって $\hat{h}(P) = 0$ を得る．

$P \in E(K')$ とする．ただし K' は K の有限次拡大である．$\hat{h}(P) = 0$ と仮定する．このとき任意の $m \in \mathbb{Z}$ に対して $\hat{h}([m]P) = m^2 \hat{h}(P) = 0$ が成立する．(5) より定数 C が存在して，任意の $m \in \mathbb{Z}$ に対して

$$\begin{aligned} h_f([m]P) &= \mid (\deg f)\hat{h}([m]P) - h_f([m]P) \mid \\ &\leq C \end{aligned}$$

が成立する．したがって

$$\{P, [2]P, [3]P, \dots\} \subset \{Q \in E(K') \mid h_f(Q) \leq C\}$$

が成立するが，**定理 2.2** より

$$\#\{Q \in E(K') \mid h_f([m]P) \leq C\} < \infty$$

であるから

$$\#\{P, [2]P, [3]P, \dots\} < \infty$$

が成立する．したがって $P \in E(\overline{K})_{\mathrm{tors}}$ を得る．

$\hat{h}' : E \to \mathbb{R}$ を

$$\hat{h}' \circ [m] = m^2 \hat{h}', \quad (\deg f)\hat{h}' = h_f + O(1)$$

をみたすと仮定する．$\hat{h}$ が (5) をみたすので $\hat{h}' - \hat{h} = O(1)$ を得る．一方

$$\hat{h}' \circ [m^N] = m^{2N} \hat{h}' \quad (N = 1, 2, \dots)$$

が成立する．したがって

$$\hat{h}' = m^{-2N} \hat{h}' \circ [m^N] = m^{-2N}(\hat{h} \circ [m^N] + O(1)) = \hat{h} + \frac{O(1)}{m^{2N}} \longrightarrow \hat{h} \quad (N \longrightarrow \infty)$$

を得る．

3.4 Mordell-Weil の定理から $\mathbb{R}\otimes_{\mathbb{Z}}E(K)$ は有限次元 $\mathbb{R}$ 線型空間である．一方 $E(K)/E(K)_{\mathrm{tors}}$ は $\mathbb{R}\otimes_{\mathbb{Z}}E(K)$ 内の lattice とみることができる．さらに **定理 3.3** より $\hat{h}$ は $E(K)/E(K)_{\mathrm{tors}}$ 上の正定値二次形式であることが分かる．今 $\hat{h}$ を $\mathbb{R}\otimes_{\mathbb{Z}}E(K)$ へ延長しても，正定値性が保たれることを見る．そのために鍵となる補題を示す．

補題 3.5.（Minkowski の定理） V を r 次元 $\mathbb{R}$ 線型空間とする．$B\subset V$ を凸でかつ原点に対して対称な集合とする．$\mathrm{vol}(B)>4^r$ のとき，B は原点でない lattice の点を含む．

（証明）$V=\mathbb{R}^r$ として話を進める．B は原点しか lattice の元を持たないと仮定する．ここで $N>0\in\mathbb{Z}$ を「原点を中心とした 1 辺の長さ $2N$ の立方体を考えたとき，それが B を含む」ようにとる．C を原点を中心とした 1 辺の長さ $4N$ の立方体とする．

$\ell_1,\ell_2\in\mathbb{Z}^r$ $(\ell_1\neq\ell_2)$ とする．このとき

$$\left\{\ell_1+\frac{1}{2}b\mid b\in B\right\}\cap\left\{\ell_2+\frac{1}{2}b\mid b\in B\right\}=\emptyset$$

が成立する．実際，共通部分が空でないとすると，$b_1,b_2\in B$ が存在して

$$\ell_1+\frac{1}{2}b_1=\ell_2+\frac{1}{2}b_2$$

が成立する．よって

$$(\ell_1-\ell_2)=\frac{1}{2}(b_2-b_1)$$

を得る．B は対称であるから $-b_1\in B$ が成立し，さらに B が凸であるから

$$\frac{1}{2}(b_2-b_1)\in B$$

が成立する．したがって $0\neq\ell_1-\ell_2\in B$ 得る．これは B は原点しか lattice の元を持たないという仮定に矛盾する．

今 $\ell\in\mathbb{Z}^r$ のすべての座標が N 以下のとき $|\mathrm{coordi}\ell|\leq N$ と記す．$|\mathrm{coordi}\ell|\leq N$ をみたす任意の $\ell\in\mathbb{Z}^r$ に対して

$$\left\{\ell+\frac{1}{2}b\mid b\in B\right\}\subset C$$

が成立する．したがって

$$\begin{aligned}(4N)^r=\mathrm{vol}(B)&\geq\sum_{|\mathrm{coordi}\ell|\leq N}\mathrm{vol}\left(\ell+\frac{1}{2}B\right)\\&\geq(2N)^r\mathrm{vol}\left(\frac{1}{2}B\right)=2^rN^r2^{-r}\mathrm{vol}(B)=N^r\mathrm{vol}(B)\end{aligned}$$

より $4^r \geq \mathrm{vol}(B)$ を得る．これは $\mathrm{vol}(B) > 4^r$ に矛盾する．

補題 3.6. V を有限次元 $\mathbb{R}$ 線型空間とする．$L \subset V$ を lattice とする．$q : V \to \mathbb{R}$ を以下をみたす二次形式とする．
(i) $P \in L$ とする．このとき

$$q(P) = 0 \Longleftrightarrow P = 0$$

が成立する．
(ii) 任意の定数 C に対して

$$\#\{P \in L \mid q(P) \leq C\} < \infty$$

が成立する．
このとき q は V 上正定値である．

（証明）V の基底を適当に取ることにより，任意の $\boldsymbol{x} = {}^t(x_1, \ldots, x_r) \in V$ に対して

$$q(\boldsymbol{x}) = \sum_{i=1}^{s} x_i^2 - \sum_{i=1}^{t} x_{s+i}^2 \quad (s + t \leq r)$$

と表せる．

$$B := B(\varepsilon, \delta) = \left\{ \boldsymbol{x} = (x_1, \ldots, x_r) \in V \mid \sum_{i=1}^{s} x_i^2 \leq \varepsilon,\ \sum_{i=1}^{t} x_{s+i}^2 \leq \delta \right\}$$

とおく．このとき $B \subset V$ は凸でかつ原点に対して対称な集合である．また条件 (i), (ii) より

$$\lambda := \inf\{q(P) \mid P \in L, P \neq O\} > 0$$

が成立する．実際 $\mathbf{0} \neq P \in L$ を一つ固定すると (i) より $q(P) \neq 0$ $(=: C)$ が成立する．このとき (ii) より

$$\#\{P \in L \mid q(P) \leq C\} < \infty$$

より，上の集合は離散的である．よって $\lambda \to 0$ にはならない．
　q は正定値ではないと仮定する，すなわち $s < r$ と仮定する．**補題 3.5** より $\delta > 0$ を十分大きくとれば $B(\frac{1}{2}, \delta)$ は $\mathbf{0}$ でない lattice の元 P を含む．ところがこのとき

$$q(P) = \sum_{i=1}^{s} x_i^2 - \sum_{i=1}^{t} x_{s+i}^2 \leq \frac{1}{2}\lambda$$

が成立し，これは λ の選び方に矛盾する．

以上より，次の命題が成立する．

命題 3.7. 標準的高さ $\hat{h}$ は $\mathbb{R} \otimes_{\mathbb{Z}} E(K)$ 上の正定値二次形式である．

上の性質を用いて lattice の基本領域の面積に相当する概念を導入する．まず，標準的高さの二次形式としての性質から次を得る．

K を代数体，E を K 上の楕円曲線とする．今，双線型形式 $< \ , \ >: E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}$ を $< P, Q >= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ で定義する．これを Néron-Tate pairing と呼ぶ．

$P_1, \ldots, P_r \in E(K)$ を $[P_1], \ldots, [P_r]$ が $E(K)/E(K)_{\mathrm{tors}}$ を生成している点とする．このとき $R_{E/K} := \det(< P_i, P_j >)$ を E の elliptic regulator と呼ぶ．ただし $r = 0$ のとき $R_{E/K} = 1$ と定義する．**命題 3.7** より elliptic regulator $R_{E/K}$ は常に正の値を取る．

参考文献

[1] 彌永昌吉, 数論, 現代数学 10, 岩波書店 1969

[2] M.J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein and E. Teske, Analysis of the xedni calculus attack, Des. Codes Cryptogr., 20, 41-64(2000)

[3] 小暮淳, Koblitz 曲線への Xedni Calculus 適用について, 本報告集所収

[4] J. H. Silverman, The arithmetic of elliptic curves, GTM 106, Springer-Verlag, New York 1986

[5] J. H. Silverman, The xedni calculus and the elliptic curve discrete logarithm problem, Des. Codes Cryptogr., 20, 5-40(2000)

[6] 谷戸光昭, Xedni Calculus について, 本報告集所収

土屋和由
中央大学大学院理工学研究科数学専攻博士後期課程
112-8551
東京都文京区春日 1-13-27
e-mail address : kazu@grad.math.chuo-u.ac.jp