講義ノート　　Version 1.0, 1995/3/27, 1:09am

Ｄｉｏｐｈａｎｔｕｓ幾何入門

— Ｍｏｒｄｅｌｌ-Ｆａｌｔｉｎｇｓの定理に向けて —

森脇　淳

京都大学大学院理学研究科数学教室
E-mail: moriwaki@kusm.kyoto-u.ac.jp

このノートの著作権は森脇　淳が有し，無断で転用，転載することを禁じます．
©1996 森脇　淳

目次

序 4

第 1 章　高さの理論 7
1.1. 代数体の付値 7
1.2. 格子の体積と積公式 8
1.3. ベクトルと射影空間の点の高さ 11
1.4. 直線束に付随した高さ関数 15
1.5. Ｎｏｒｔｈｃｏｔｔの有限性定理 19
1.6. アーベル多様体上の高さ 20
1.7. 曲線とヤコビ多様体 25
1.8. Ｍｏｒｄｅｌｌ-Ｗｅｉｌの定理 28

第 2 章　Ｍｏｒｄｅｌｌ-Ｆａｌｔｉｎｇｓの定理に向けての準備 33
2.1. Ｓｉｅｇｅｌの補題 33
2.2. 多変数多項式のＷｒｏｎｓｋｉａｎ 35
2.3. 多項式の長さに関する不等式 38
2.4. Ｒｏｔｈの補題 42
2.5. ノルムの高さ 46
2.6. 導関数の長さの評価 55

第 3 章　Ｍｏｒｄｅｌｌ-Ｆａｌｔｉｎｇｓの定理の証明 61
3.1. Ｍｏｒｄｅｌｌ-Ｆａｌｔｉｎｇｓの定理の証明のスケッチ 61
3.2. 定理 3.1.3 , 定理 3.1.4 , 定理 3.1.5 の証明に必要な技術的設定 65
3.3. 高さの小さい切断 (定理 3.1.3 の証明) 68
3.4. Ｉｎｄｅｘの上限 (定理 3.1.4 の証明) 74
3.5. Ｉｎｄｅｘの下限 (定理 3.1.5 の証明) 76
3.6. 代数体上の漸近的Ｆｅｒｍａｔ予想 83

参考文献 89

記号表・索引 90

序

本講義の目的は，Mordell-Faltings の定理

「代数体上定義された種数が 2 以上の曲線の有理点は有限個である．」

の完全な証明を与えることにある．この定理は，今世紀中には証明は無理かもしれないと言われていたが，1983 年に Faltings [4] によって証明され，その業績により彼がフィールズ賞をとったことは周知のことと思う．当時の証明は，相当高度な数論幾何の手法によっていたが，Vojta [14] によってなされた古典的な Diophantus 近似の手法の高次元化によりかなり初等的になった．この後，すぐにこの手法は Faltings [5] によりさらに一般化された．しかし，彼らの方法には，一つだけ初等的でない箇所が含まれていた．それは，いわゆるアラケロフ幾何の部分で，例えば，Vojta は 3 次元の数論多様体上の当時確立されたばかりの数論的リーマン・ロッホを用いていた．その部分をさらに初等化したのが Bombieri [2] で，つまるところ数論的リーマン・ロッホは Dirichlet の部屋割り論法に置き換わった．Bombieri の証明をもとに，Diophantus 幾何の基本事項をおさえながら，Mordell-Faltings の定理に迫ろうというのが講義の主旨である．

古典的な Diophantus 近似について復習しておこう．というのは，ここであらわれる証明のプロトタイプをいかにして高次元化するかというのが講義の主テーマであるからである．問題は，固定された実数 μ に対して，ある実の有理数でない代数的数 α が与えられた時，整数 x, y についての不等式

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{\mu}}$$

が有限個のみの解を持つかどうかということである．$\mu = 2$ の時，成り立たないことは Dirichlet によって示され，$\mu > [\mathbb{Q}(\alpha) : \mathbb{Q}]$ の時は Liouville によって肯定的に解かれた．その後，Thue，Siegel，Dyson 等により μ の改良がなされ，最終的に Roth により $\mu > 2$ で成り立つことが示され，Roth はこの業績でフィールズ賞をとった．彼の証明は複雑だが初等的で，重要な鍵となるのが Roth の補題と呼ばれるものである．この補題は，実際，Mordell-Faltings の定理の証明のために本講義でも用いる．証明のプロトタイプをみるために，ここで Liouville の結果を証明してみよう．大きく 3 つの段階に分かれる．

(A) 何かいい多項式を見つけること．
(B) 見つけた多項式から決まるある種の量の上限を見つけること．
(C) 先の量の下限を見つけること．

以上の後，上限と下限を比較して結論を導くのである．実際にやってみよう．$d = [\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$ とする．

(A) $P(T)$ を α の最小多項式で，係数が整数で，互いに素であり，最高次の係数が正であるものとする．

(B) $x, y \in \mathbb{Z}$ で $|x/y - \alpha| \leq 1$ を満たすものとし，$|P(x/y)|$ を評価する．

$$P(T) = \sum_{i=1}^{d} \frac{P^{(i)}(\alpha)}{i!}(T-\alpha)^i$$

を $P(T)$ の α でのテーラー展開とし，$M(\alpha) = d \max_{i\geq 1}\{|P^{(i)}(\alpha)/i!|\}$ とおくと，

$$|P(x/y)| = \left|\sum_{i=1}^{d} \frac{P^{(i)}(\alpha)}{i!}(x/y-\alpha)^i\right| \leq M(\alpha)|x/y-\alpha|$$

を得る．

(C) $P(x/y) \neq 0$ ゆえ，$|P(x/y)| \geq 1/y^d$ となる．

以上を組み合わせて，$|x/y - \alpha| \leq 1$ なら，

$$\left|\frac{x}{y} - \alpha\right| \geq \frac{1/M(\alpha)}{y^d}$$

を得る．y が十分大きい時，

$$\frac{1/M(\alpha)}{y^d} \geq \frac{1}{y^\mu}$$

となるので，後は容易に Liouville の結果が導き出せる．

高次元化のためには，(A)，(B)，(C) の多項式を直線束の大域切断に読み換え，比較する量として index を用いればいいだけである．(A) は定理 3.1.3，(B) は定理 3.1.4，(C) は定理 3.1.5 に対応している．もう少し詳しくは，第 3 章 の 3.1 節を見るとよい．この節は，比較的予備知識なしでも読めるようにしてある．さらに勉強を進める人のためにそれぞれの (A)，(B)，(C) についてもう少し書いておく．以下述べることについては総合的な解説の [**3**] または [**15**] が参考になると思う．(A) はアラケロフ幾何と関係している箇所で，もっとも一般的なものは Faltings によるものがある．彼は Dirichlet の部屋割り論法より精密な Minkowski の定理を用いて一般化した結果を導いている．(B) は比較的代数幾何学的な部分である．いろいろな人達 (例えば，Dyson, Roth, Esnault-Viehweg, Faltings, Vojta, Nakamaye, etc) によって研究されており，一般的なものは，Faltings による積定理である．(C) は，計算は複雑になるが技術的にはあまり難しくない部分である．

最後にこの講義ノートの読み方のヒントを与えておく．Diophantus 幾何についてはある程度知識があって Mordell-Faltings の定理の証明だけ読みたいという人は，第 3 章 から読み始め，必要に応じて 第 2 章 を読めばいいと思う．Diophantus 幾何の知識が少ない人は，とりあえず 第 1 章 を読み，つづいて 第 3 章 を読みつつ，必要に応じて 第 2 章 を読めばいいと思う．

第 1 章

高さの理論

1.1. 代数体の付値

本節では，代数体の付値について簡単に復習する．詳しいことは，例えば [6] を参照すること．

F を体とする．写像 $|\ |: F \to \mathbb{R}$ が，次の条件を満たすとき付値という．

(1) $|x| \geq 0$ $(\forall x \in F)$ で，等号条件 "$|x| = 0 \iff x = 0$" が成立する．

(2) $|xy| = |x||y|$ $(\forall x, y \in F)$．

(3) $|x + y| \leq |x| + |y|$ $(\forall x, y \in F)$．

条件 (3) の代わりに，付値 $|\ |$ が

(4) $|x + y| \leq \min\{|x|, |y|\}$ $(\forall x, y \in F)$

を満たすとき，非アルキメデス的であるといい，そうでないとき，アルキメデス的であるという．任意の体は，

$$|x| = \begin{cases} 1, & \text{もし } x \neq 0 \\ 0, & \text{もし } x = 0 \end{cases}$$

で定まる付値を持つ．これを自明な付値という．$|\ |_1$，$|\ |_2$ を二つの付値とする．ある正の数 c が存在して，$|\ |_1 = |\ |_2^c$ となる時，$|\ |_1$ と $|\ |_2$ は同値な付値という．

1.1.1. K を代数体，O_K を K の代数的整数全体する．さらに，P を O_K のゼロでない素イデアルとする．O_K の P での局所化は離散的付値環であるので，ある $t_P \in (O_K)_P$ が存在して，$P(O_K)_P = t_P(O_K)_P$ となる．したがって，任意のゼロでない $x \in K$ に対して，ある整数 a と $u \in (O_K)^\times$ が存在して $x = t_P^a \cdot u$ となる．整数 a を $\mathrm{ord}_P(x)$ で表す．そこで，

$$|x|_P = \#\left(O_K/P\right)^{-\mathrm{ord}_P(x)}$$

とおくと，これは非アルキメデス的付値となる．この付値を P での正規化された付値と呼ぶ．

1.1.2. K を代数体，$K(\mathbb{C})$ を K の $\mathbb{C}$-valued points 全体とする．つまり，

$$K(\mathbb{C}) = \{\sigma \mid \sigma : K \hookrightarrow \mathbb{C}\}$$

とする．ここで，$\#(K(\mathbb{C})) = [K:\mathbb{Q}]$ であることは容易にわかる．各 $\sigma \in K(\mathbb{C})$ に対して，$|x|_\sigma$ を $\sigma(x)$ の複素数としての絶対値 (つまり $|x|_\sigma = |\sigma(x)|$) とすると，これは K のアルキメデス的付値となる．

定理 1.1.3. K を代数体とする．この時，K の自明でない付値は1.1.1 と1.1.2であげた例のいずれかと同値である．

今後，代数体 K に対して，

$$M_K = (\mathrm{Spec}(O_K) \setminus \{(0)\}) \amalg K(\mathbb{C})$$

とおき，$v \in M_K$ に対して，

$$|\ |_v = \begin{cases} |\ |_P & \text{もし } v = P \in \mathrm{Spec}(O_K) \setminus \{(0)\} \\ |\ |_\sigma & \text{もし } v = \sigma \in K(\mathbb{C}) \end{cases}$$

と定めることにする．また言葉の乱用であるが M_K の元を単に付値と呼ぶこともある．

注意 1.1.4. $\sigma \in K(\mathbb{C})$ に対して，$\bar{\sigma}(x) = \overline{\sigma(x)}$ と定めると $\bar{\sigma} \in K(\mathbb{C})$ となる．この時，$|\ |_\sigma = |\ |_{\bar{\sigma}}$ となるが，記法の便利さもあって一応区別することにする．

1.2. 格子の体積と積公式

本節では，いわゆる積公式を証明する．これは，コンパクトなリーマン面の有理型関数の主因子の次数がゼロになるということの数論的な類似であり，後で射影空間の点の高さを定義する時に必要となる公式である．

M を階数が r の自由アーベルとし，$\langle\ ,\ \rangle$ を M の (正確には，$M \otimes_{\mathbb{Z}} \mathbb{R}$) の内積とする．$M$ の自由基底 $\{e_1, \ldots, e_r\}$ に対して，

$$\sqrt{\det(\langle e_i, e_j \rangle)}$$

を考えよう．これは，自由基底の取り方に依らない．実際，$\{e'_1, \ldots, e'_r\}$ が別の自由基底とし，$e'_i = \sum_{j=1}^r a_{ij} e_j$ とおき，$A = (a_{ij})$ と定めると，$A \in \mathrm{GL}(r, \mathbb{Z})$ で，

$$(\langle e'_i, e'_j \rangle) = A(\langle e_i, e_j \rangle) A^t$$

である．したがって，

$$\det(\langle e_i, e_j \rangle) = \det(\langle e'_i, e'_j \rangle)$$

である．この数を，$\mathrm{vol}(M, \langle , \rangle)$ と書き，M の $\langle\ ,\ \rangle$ についての体積と呼ぶ．ここで，この節での鍵となる次の補題を考えよう．

補題 1.2.1. $x_1, \dots, x_r$ を M の元で，$\{x_1, \dots, x_r\}$ が $M \otimes_{\mathbb{Z}} \mathbb{Q}$ の基底をなすとする．この時，

$$\sqrt{\det(\langle x_i, x_j \rangle)} = \# \left(\frac{M}{\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_r} \right) \mathrm{vol}(M, \langle , \rangle)$$

である．

証明: $\{e_1, \dots, e_r\}$ を M の自由基底とし，$x_i = \sum_{j=1}^{r} b_{ij} e_j$，$B = (b_{ij})$ とおく．この時，

$$(\langle x_i, x_j \rangle) = B(\langle e_i, e_j \rangle) B^t$$

を得る．したがって，

$$\# \left(\frac{M}{\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_r} \right) = |\det B|$$

を示せば十分である．単因子論より，ある $P, Q \in \mathrm{GL}(r, \mathbb{Z})$ と $c_1, \dots, c_r \in \mathbb{Z}$ が存在して，

$$PBQ = \begin{pmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_r \end{pmatrix}$$

が成り立つ．f_P，f_B，f_Q を P，B，Q で $\{e_1, \dots, e_r\}$ に関して定義される M の準同型とする．この時，

$$\frac{M}{\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_r} = \mathrm{Coker}(M \xrightarrow{f_B} M)$$

である．f_P と f_Q は，同型であるので，

$$\begin{aligned} \# \left(\frac{M}{\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_r} \right) &= \# \left(\mathrm{Coker}(M \xrightarrow{f_B} M) \right) \\ &= \# \left(\mathrm{Coker}(M \xrightarrow{f_Q} M \xrightarrow{f_B} M \xrightarrow{f_P} M) \right) \\ &= |c_1 \cdots c_r| = |\det B| \end{aligned}$$

を得る．よって，補題が示せた． □

K を $[K : \mathbb{Q}] = n$ となる代数体，O_K を K の整数環とする．$\{\omega_1, \dots, \omega_n\}$ を O_K のアーベル群としての自由基底とする．K の $\mathbb{Q}$ 上の判別式は，

$$D_{K/\mathbb{Q}} = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i \cdot \omega_j))$$

で定義され，O_K の自然な内積 $\langle \ , \ \rangle_K$ は，

$$\langle x, y \rangle_K = \sum_{\sigma \in K(\mathbb{C})} \sigma(x) \cdot \bar{\sigma}(y)$$

で定義される．これが内積を与えることを調べるのは読者にまかせる．さて，ここで次を見よう．

補題 1.2.2. $\mathrm{vol}(O_K, \langle , \rangle_K) = \sqrt{|D_{K/\mathbb{Q}}|}$.

証明:　$\{\omega_1, \ldots , \omega_n\}$ を O_K のアーベル群としての自由基底とし，$K(\mathbb{C}) = \{\sigma_1, \cdots , \sigma_n\}$ とおく．この時，$\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i \cdot \omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i) \cdot \sigma_k(\omega_j)$ で，$\langle \omega_i, \omega_j \rangle_K = \sum_{k=1}^{n} \sigma_k(\omega_i) \cdot \bar{\sigma}_k(\omega_j)$ である．よって，もし $\Delta = (\sigma_i(\omega_j))$ とおくと，

$$(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i \cdot \omega_j)) = \Delta^t \cdot \Delta \quad \text{and} \quad (\langle \omega_i, \omega_j \rangle_K) = \Delta^t \cdot \overline{\Delta}$$

である．ゆえに，補題が示せた．　□

定理 1.2.3 (積公式)**.** 任意の $x \in K \setminus \{0\}$ に対して，$\prod_{v \in M_K} |x|_v = 1$ が成立する．

証明:　明らかに，$x \in O_K$ と仮定してよい．$\{\omega_1, \ldots , \omega_n\}$ を O_K のアーベル群としての自由基底とする．この時，$\{x\omega_1, \ldots , x\omega_n\}$ は，$O_K \otimes_{\mathbb{Z}} \mathbb{Q}$ の基底である．したがって，補題 1.2.1 により，

$$\sqrt{\det(\langle x\omega_i, x\omega_j \rangle_K)} = \mathrm{vol}(O_K, \langle , \rangle) \# \left(\frac{O_K}{\mathbb{Z}x\omega_1 + \cdots + \mathbb{Z}x\omega_n} \right)$$

を得る．ここで，$\mathbb{Z}x\omega_1 + \cdots + \mathbb{Z}x\omega_n = xO_K$ であり，補題 1.2.2 により $\mathrm{vol}(O_K, \langle , \rangle) = \sqrt{|D_{K/\mathbb{Q}}|}$ であるので，

$$\sqrt{\det(\langle x\omega_i, x\omega_j \rangle_K)} = \sqrt{|D_{K/\mathbb{Q}}|} \# \left(O_K / xO_K \right)$$

が導かれる．従って，次の二つの式を示せば十分である．

$$\# \left(O_K / xO_K \right) \cdot \prod_{\substack{P \in \mathrm{Spec}(O_K) \\ P \neq (0)}} |x|_P = 1. \tag{1.2.3.1}$$

$$\det(\langle x\omega_i, x\omega_j \rangle_K) = |D_{K/\mathbb{Q}}| \cdot \prod_{\sigma \in K(\mathbb{C})} |x|_\sigma^2. \tag{1.2.3.2}$$

まず，(1.2.3.2) を示めそう．$K(\mathbb{C}) = \{\sigma_1, \cdots , \sigma_n\}$ とおく．この時，

$$\langle x\omega_i, x\omega_j \rangle_K = \sum_{k=1}^{n} \sigma_k(x\omega_i) \cdot \bar{\sigma}_k(x\omega_j) = \sum_{k=1}^{n} |x|_{\sigma_k}^2 \sigma_k(\omega_i) \cdot \bar{\sigma}_k(\omega_j)$$

である．ゆえに，もし $\Delta = (\sigma_i(\omega_j))$ とおくなら，

$$(\langle x\omega_i, x\omega_j \rangle_K) = \Delta^t \begin{pmatrix} |x|_{\sigma_1}^2 & & 0 \\ & \ddots & \\ 0 & & |x|_{\sigma_n}^2 \end{pmatrix} \overline{\Delta}$$

である．よって (1.2.3.2) が示せた．

(1.2.3.1) は次の補題の帰結である．というのは，$xO_K = P_1^{e_1} \cdots P_r^{e_r}$ を xO_K の素イデアル分解とすると，

$$\mathrm{ord}_P(x) = \begin{cases} e_i & \text{もし } P = P_i \\ 0 & \text{もし } P \notin \{P_1, \ldots, P_r\} \end{cases}$$

であるからである． □

補題 1.2.4. K を代数体，O_K を K の整数環，I を O_K のイデアルとする．$I = P_1^{e_1} \cdots P_r^{e_r}$ を I の素イデアル分解とすると，

$$\#(O_K/I) = \prod_{i=1}^{r} \#(O_K/P_i)^{e_i}$$

である．

証明: t_i を $P_i(O_K)_{P_i}$ の生成元とする．中国剰余定理より，

$$O_K/I \simeq \bigoplus_{i=1}^{r} O_K/P_i^{e_i} = \bigoplus_{i=1}^{r} (O_K/P_i^{e_i})_{P_i} = \bigoplus_{i=1}^{r} (O_K)_{P_i}/t_i^{e_i}(O_K)_{P_i}$$

を得る．したがって，$(O_K)_{P_i}/t_i(O_K)_{P_i} \simeq O_K/P_i$ であり，準同型

$$(O_K)_{P_i}/t_i(O_K)_{P_i} \xrightarrow{\times t_i^k} t_i^k(O_K)_{P_i}/t_i^{k+1}(O_K)_{P_i}$$

は同型であるので，

$$\begin{aligned} \#(O_K/I) &= \prod_{i=1}^{r} \#((O_K)_{P_i}/t_i^{e_i}(O_K)_{P_i}) \\ &= \prod_{i=1}^{r} \#((O_K)_{P_i}/t_i(O_K)_{P_i})^{e_i} \\ &= \prod_{i=1}^{r} \#(O_K/P_i)^{e_i} \end{aligned}$$

である． □

1.3. ベクトルと射影空間の点の高さ

本節では，ベクトルと射影空間の点の高さを定義し，その簡単な性質を調べる．

K を代数体し，$x = (x_1, \ldots, x_n) \in K^n$ とする．もし $x \neq 0$ なら，x の 高さ (正確には x の対数的高さ) を

$$h_K(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \left(\max_{1 \leq i \leq n} \{|x_i|_v\} \right)$$

で定義する．さらに，もう一つ類似物を定義しておく．すなわち，

$$h_K^+(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log^+ \left(\max_{1 \le i \le n} \{ |x_i|_v \} \right)$$

ここで，$\log^+$ は，

$$\log^+(a) = \begin{cases} 0 & \text{もし } a < 1 \\ \log(a) & \text{もし } a \ge 0 \end{cases}$$

で定義される関数である．$\log^+$ の性質として，$a, b \ge 0$ の時，$\log^+(ab) \le \log^+(a) + \log^+(b)$ があることを注意しておく．さらに，h^+ の注意であるが，h^+ はゼロであるベクトルにも定義されており，$h^+((0, \dots, 0)) = 0$ である．もう一つ，h と h^+ には，

$$h_K^+((x_1, \dots, x_n)) = h_K((1, x_1, \dots, x_n))$$

という関係があり，これは幾何学的にはアファイン空間の点の高さを射影空間の点の高さとしてみるという意味がある．話を進める上での高さの基本的性質として次がある．

命題 1.3.1. (1) K' を K の有限次拡大体とする．x をゼロでない K^n のベクトルとする．この時，x の K^n のベクトルとしての高さと K'^n のベクトルとしての高さは一致する．つまり，$h_K(x) = h_{K'}(x)$ である．したがって，今後，体の参照をはずして x の高さを $h(x)$ と表すことにする．つまり，$h : \overline{\mathbb{Q}}^n \to \mathbb{R}$ が決まったわけである．

(2) h はスカラー倍について不変である．つまり，ゼロでない $\overline{\mathbb{Q}}$ の元 a とゼロでないベクトル $x \in \overline{\mathbb{Q}}^n$ について，$h(ax) = h(x)$ である．

証明: まず次の補題を示す．

補題 1.3.2. K' を K の有限次拡大体とする．O_K，$O_{K'}$ をそれぞれの整数環とする．P を O_K の素イデアルとし，$PO_{K'} = P_1'^{e_1} \cdots P_r'^{e_r}$ を $PO_{K'}$ の素イデアル分解とする．この時，$f_i = [O_{K'}/P_i' : O_K/P]$ とおくと，$[K' : K] = e_1 f_1 + \cdots + e_r f_r$ である．

証明: $(O_{K'})_P$ は $(O_K)_P$- 加群として階数が $[K' : K]$ の自由加群であるので，

$$\begin{aligned} \dim_{O_K/P} O_{K'}/PO_{K'} &= \dim_{O_K/P} (O_{K'})_P/P(O_{K'})_P \\ &= \dim_{O_K/P} ((O_K)_P/P(O_K)_P) \otimes_{(O_K)_P} (O_{K'})_P = [K' : K] \end{aligned}$$

である．したがって $a = \#(O_K/P)$ とすると，$[K' : K] = \log_a \#(O_{K'}/PO_{K'})$ である．ゆえに，補題 1.2.4 を用いて，

$$[K' : K] = \log_a \#(O_{K'}/PO_{K'}) = \sum_{i=1}^{r} e_i \log_a \#(O_{K'}/P_i') = \sum_{i=1}^{r} e_i f_i$$

を得る． □

命題 1.3.1 の証明に戻ろう．$x \in K$ とする．P を O_K の素イデアルとし，$PO_{K'} = P_1'^{e_1} \cdots P_r'^{e_r}$ を $PO_{K'}$ の素イデアル分解とする．$a = \mathrm{ord}_P(x)$ とおくと，$\mathrm{ord}_{P_i'}(x) = ae_i$ である．ゆえに，$f_i = [O_{K'}/P_i' : O_K/P]$ とすると，

$$\begin{aligned} |x|_{P_1'} \cdots |x|_{P_r'} &= \#(O_{K'}/P_1')^{-\mathrm{ord}_{P_1'}(x)} \cdots \#(O_{K'}/P_r')^{-\mathrm{ord}_{P_r'}(x)} \\ &= \#(O_K/P)^{-f_1 \mathrm{ord}_{P_1'}(x) - \cdots - f_r \mathrm{ord}_{P_r'}(x)} \\ &= \#(O_K/P)^{-(e_1 f_1 + \cdots + e_r f_r)a} \end{aligned}$$

となり，補題 1.3.2 より，

$$|x|_{P_1'} \cdots |x|_{P_r'} = |x|_P^{[K':K]} \tag{1.3.2.1}$$

を得る．一方，$\sigma \in K(\mathbb{C})$ に対して，

$$K'(\mathbb{C})_\sigma = \{\sigma' \in K'(\mathbb{C}) \mid \sigma'|_K = \sigma\}$$

とおく．このとき，$\#(K'(\mathbb{C})_\sigma) = [K' : K]$ であるので，

$$\prod_{\sigma' \in K'(\mathbb{C})_\sigma} |x|_{\sigma'} = |x|_\sigma^{[K':K]} \tag{1.3.2.2}$$

を得る．(1) は，(1.3.2.1) と (1.3.2.2) の帰結である．

次に (2) について考えよう．$a \in K$，$x \in K^n$ としてよい．高さの定義により，

$$h(ax) = \frac{1}{[K : \mathbb{Q}]} \sum_v \log(|a|_v) + h(x)$$

である．一方，積公式 (定理 1.2.3) より，

$$\sum_v \log(|a|_v) = 0$$

である．よって (2) を得る． □

この命題により，$x \in \mathbb{P}^{n-1}(\overline{\mathbb{Q}})$ に対して，その代表元のとり方に依らず $h(x)$ が定まることを言っている．$h(x)$ を射影空間の点 x の高さという．

ここで，後で必要となる幾つかの高さの性質を示しておこう．

命題 1.3.3. (1) 二つの $\overline{\mathbb{Q}}$ 上のベクトル $x = (x_i)$ と $y = (y_j)$ に対して，$x \otimes y$ を成分を $x_i y_j$ とするベクトルとする．すなわち，$x \otimes y = (x_i y_j)$ である．この時，$h(x \otimes y) = h(x) + h(y)$ となる．特に，$h(x^{\otimes m}) = mh(x)$ である．

(2) ϕ を $\overline{\mathbb{Q}}^n$ の $\overline{\mathbb{Q}}$ 上の自己同型とする．このとき，ϕ のみによる定数 C が存在して，

$$|h(x) - h(\phi(x))| \leq C$$

が任意の $x \in \overline{\mathbb{Q}}^n$ で成立する．

証明:　(1) $x_i, y_j \in K$ として示してもよい．$v \in M_K$ に対して，明らかに，

$$\max_{i,j}\{|x_i y_j|_v\} = \max_i\{|x_i|_v\} \max_j\{|y_j|_v\}$$

であるので，(1) が成り立つ．

(2) ϕ の行列表現を (a_{ij})，ϕ^{-1} の行列表現を (b_{ij}) とする．$C_1 = h((a_{ij}))$，$C_2 = h((b_{ij}))$ とおき，

$$h(\phi(x)) \leq h(x) + C_1 + \log(n), \qquad h(\phi^{-1}(x)) \leq h(x) + C_2 + \log(n)$$

がすべての $x \in \overline{\mathbb{Q}}^n$ で成立することをみる．このために，$a_{ij}, b_{ij} \in K$，$x \in K^n$ としてもよい．$x = (x_1, \ldots, x_n)$ とおくと，$\phi(x)$ の i- 成分は，$\sum_k a_{ik}x_k$ である．ここで，

$$\left|\sum_k a_{ik}x_k\right|_v \leq \begin{cases} \max_{i,j}\{|a_{ij}|_v\} \max_i\{|x_i|_v\}, & v \text{ が非アルキメデス的な時} \\ n \max_{i,j}\{|a_{ij}|_v\} \max_i\{|x_i|_v\}, & v \text{ がアルキメデス的な時} \end{cases}$$

である．したがって，$h(\phi(x)) \leq h(x) + C_1 + \log(n)$ を得る．$h(\phi^{-1}(x)) \leq h(x) + C_2 + \log(n)$ も同様である．

$h(\phi^{-1}(x)) \leq h(x) + C_2 + \log(n)$ において，x の代わりに $\phi(x)$ を用いると

$$h(x) \leq h(\phi(x)) + C_2 + \log(n)$$

となる．ゆえに $C = \max\{C_1, C_2\} + \log(n)$ とおくと，

$$|h(x) - h(\phi(x))| \leq C$$

となる．　□

命題 1.3.3 の (2) は重要な意味をもっている．高さの定義からもわかるように，座標の取り方に依っている．別の言い方をすれば，座標変換で不変ではない．これは，高さの定義があまりいいものではないことを示唆しており，実際，英語では naive height と呼ばれる．もっと，良い高さの定義を考えることは数論幾何の重要なテーマの一つである．あとの節ではアーベル多様体上では Neron-Tate の高さと呼ばれる自然な高さを定義する．いずれにせよ naive height は座標変換で不変ではないが，座標変換した場合，差は高々有界関数であることを命題 1.3.3 の (2) は示している．

最後に多項式の高さについて述べておく．P を $\overline{\mathbb{Q}}$ 上の n- 変数多項式，つまり

$$P \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$$

とする．$P = \sum a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$ とおく時，

$$h(P) = h((a_{i_1 \cdots i_n}))$$

で P の高さを定義する．つまり，$P \in K[X_1, \ldots, X_n]$ なら

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \max\{|a_{i_1 \cdots i_n}|_v\}$$

である．同様に，

$$h^+(P) = h^+((a_{i_1 \cdots i_n}))$$

と定める．Q をもう一つの多項式とし，P の X_i についての次数を d_i，Q の X_i についての次数を d_i' とすると，系 $2.3.3$ の (1) により，

$$h(PQ) \leq h(P) + h(Q) + \sum_{i=1}^{n} \log\left(1 + \min\{d_i, d_i'\}\right) \tag{1.3.4}$$

が成り立つことに注意しておく．

1.4. 直線束に付随した高さ関数

本節では，前節の高さ関数をさらに一般化して，直線束に付随した高さ関数を定義する．前節でも注意したように $\mathrm{naive\ height}$ が座標変換で不変でないことが，直線束に付随した高さ関数が有界関数を modulo にして一意的に定まるというあいまいさに影を落としている．まず次の補題から考えよう．

補題 1.4.1. X を $\mathbb{P}^n$ に埋め込まれた $\overline{\mathbb{Q}}$ 上の射影多様体とする．X と交わらない $\mathbb{P}^n$ の線形部分空間 L を中心とした射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^m$ が導く射 $X \to \mathbb{P}^m$ を ϕ とする．このとき，X と L のみによるある定数 C が存在して，

$$|h(x) - h(\phi(x))| \leq C$$

がすべての $x \in X(\overline{\mathbb{Q}})$ で成立する．

証明: 線形部分空間を中心とした射影は点を中心とした射影の合成であるので，L が一点の場合を証明すれば十分である．命題 $1.3.3$ の (2) より，適当に $\mathbb{P}^n$ な座標を変換してもよいことがわかる．よって，L は $P = (0 : \cdots : 0 : 1)$ という座標をもつ点としてよい．この時，射影は $(X_0 : \cdots : X_{n-1} : X_n) \mapsto (X_0 : \cdots : X_{n-1})$ で定義される．負でない整数の列 $I = (e_0, \ldots, e_n)$ に対して，$X^I = X_0^{e_0} \cdots X_n^{e_n}$，$|I| = e_0 + \cdots + e_n$ と書くことにする．$P \notin X$ であるので X の定義方程式の中に $F(0, \ldots, 0, 1) \neq 0$ となる同次多項式が存在する．F の次数を d とすると，F は

$$F = X_n^d - \sum_{\substack{|I|=d, \\ I \neq (0,\ldots,d)}} a_I X^I$$

と書ける．ここで，$C = h^+((a_I)) + \log\left(\binom{n+d}{n} - 1\right)$ とおき，

$$h\left((x^I)_{|I|=d}\right) \leq h\left((x^I)_{\substack{|I|=d,\\ I\neq(0,\dots,d)}}\right) + C$$

がすべての $x \in X(\overline{\mathbb{Q}})$ で成立することを示そう．このために，ある代数体 K をとって，$a_I \in K$，$x \in X(K)$ として調べてもよい．$x_n^d = \sum_{I\neq(0,\dots,d)} a_I x^I$ であるので，

$$|x_n^d|_v \leq \begin{cases} \max_{I\neq(0,\dots,d)}\{|a_I|_v\} \max_{I\neq(0,\dots,d)}\{|x^I|_v\}, & v \text{ が非アルキメデス的な時} \\ \left(\binom{n+d}{n} - 1\right) \max_{I\neq(0,\dots,d)}\{|a_I|_v\} \max_{I\neq(0,\dots,d)}\{|x^I|_v\}, & v \text{ がアルキメデス的な時} \end{cases}$$

が成り立つ．したがって，容易に

$$h\left((x^I)_{|I|=d}\right) \leq h\left((x^I)_{\substack{|I|=d,\\ I\neq(0,\dots,d)}}\right) + C$$

がわかり，不等式が示せた．

一方，

$$h\left((x^I)_{|I|=d}\right) = h(x^{\otimes d})$$

であり，$x' = (x_0 : \cdots : x_{n-1})$ とおくと

$$h\left((x^I)_{\substack{|I|=d,\\ I\neq(0,\dots,d)}}\right) = h(x^{\otimes d-1} \otimes x')$$

である．ゆえに，命題 1.3.3 の (1) より，$dh(x) \leq (d-1)h(x) + h(x') + C$ 即ち，$h(x) \leq h(x') + C$ を得る．$h(x') \leq h(x)$ は自明であるので補題が示せた． □

X を $\overline{\mathbb{Q}}$ 上の射影多様体とし，$\phi : X \to \mathbb{P}^m$ を $\overline{\mathbb{Q}}$ 上の射とする．$x \in X(\overline{\mathbb{Q}})$ に対して，$h_\phi(x) = h(\phi(x))$ と定義し，x の ϕ に関する高さと呼ぶ．この時，次が成立する．

命題 1.4.2. 二つの $\overline{\mathbb{Q}}$ 上の射 $\phi_1 : X \to \mathbb{P}^{m_1}$ と $\phi_2 : X \to \mathbb{P}^{m_2}$ を考える．もし $\phi_1^*(\mathcal{O}_{\mathbb{P}^{m_1}}(1)) \simeq \phi_2^*(\mathcal{O}_{\mathbb{P}^{m_2}}(1))$ なら，ある定数 C が存在して

$$|h_{\phi_1}(x) - h_{\phi_2}(x)| \leq C$$

がすべての $x \in X(\overline{\mathbb{Q}})$ で成立する．

証明: $L = \phi_1^*(\mathcal{O}_{\mathbb{P}^{m_1}}(1))$ とおく．明らかに ϕ_1 は 完備な線形系 $|L|$ で定義されているとしてよい．$\mathbb{P}^{m_2}$ の座標系を $(Y_0 : \cdots : Y_{m_2})$ とし，$s_i = \phi_2^*(Y_i)$ とおく．s_i は $H^0(X, L)$ の元である．必要なら $\mathbb{P}^{m_2}$ を部分線形空間で置き換えて，$\{s_0, \dots, s_{m_2}\}$ は一次独立であると仮定してよい．$\{s_i\}$ を延長して $\{s_0, \dots, s_{m_1}\}$ が $H^0(X, L)$ の基底となるようにする．$\mathbb{P}^{m_1}$ に同次座標 $(X_0 : \cdots : X_{m_1})$ を $\phi_1^*(X_i) = s_i$ となるようにとると，ϕ_2 は ϕ_1 と $(X_0 : \cdots : X_{m_1}) \mapsto (X_0 : \cdots : X_{m_2})$ で定義される射影の合成である．よって，$\phi_1(X)$ について補題 1.4.1を使って命題を得る． □

X を $\overline{\mathbb{Q}}$ 上の射影多様体とする．$X(\overline{\mathbb{Q}})$ 上の関数全体を $F(X)$ で表し，有界関数全体を $B(X)$ で表すことにする．

定理 1.4.3. 各直線束 L に対して，次を満たすような $h_L \in F(X)$ が $\bmod B(X)$ で一意的に定まる．

(1) $h_{L_1 \otimes L_2} = h_{L_1} + h_{L_2} + O(1)$ が任意の直線束 L_1, L_2 で成立する．
(2) $f : X \to Y$ が射影多様体の間の射とすると，$h_{f^*(L)} = f^*(h_L) + O(1)$ である．
(3) $\phi : X \to \mathbb{P}^n$ が射のとき，$h_{\phi^*(\mathcal{O}_{\mathbb{P}^n}(1))} = h_\phi + O(1)$ である．

h_L を直線束 L に付随した高さ関数と呼ぶ．

証明: (a) L が大域切断で生成されているときを考える．完備線形系 $|L|$ が導く

$$\phi_{|L|} : X \to \mathbb{P}(H^0(X, L))$$

を考える．このとき，$h_L = h_{\phi_{|L|}}$ とおく．これは，命題 1.4.2 より条件 (3) を満たす．

(b) L_1, L_2, L が大域切断で生成されているときに条件 (1)，(2) を調べよう．$H^0(X, L_1)$ の基底を $\{s_i\}$，$H^0(X, L_2)$ の基底を $\{t_j\}$ とする．この時，$\{s_i \otimes t_j\}$ は，射 $\phi : X \to \mathbb{P}^N$ で $\phi^*(\mathcal{O}_{\mathbb{P}^N}(1)) = L_1 \otimes L_2$ となるものを定める．さらに，$h_\phi = h_{L_1} + h_{L_2} + O(1)$ である．一方，命題 1.4.2 より $h_\phi = h_{L_1 \otimes L_2} + O(1)$ である．よって (1) がわかった．

$\phi' : Y \to \mathbb{P}^m$ を $|L|$ が定める射とする．この時，$f^*(\phi'^*(\mathcal{O}_{\mathbb{P}^m}(1))) = f^*(L)$ であるので $h_{f^*(L)} = f^*(h_L) + O(1)$ を命題 1.4.2 より得る．

(c) L が一般の場合を考えよう．この時，代数幾何学のよく知られた事実として，大域切断で生成される直線束 L_1，L_2 が存在して，$L = L_1 \otimes L_2^{-1}$ と書けるということがある．ここで，$h_L = h_{L_1} - h_{L_2}$ と定義したいのだが，これが L_1，L_2 の取り方に依らないことを示しておかなければならない．そこで，M_1，M_2 を大域切断で生成される直線束で，$L = M_1 \otimes M_2^{-1}$ となるものとする．この時，$L_1 \otimes M_2 = M_1 \otimes L_2$ であるので，(b) で調べたように $h_{L_1} + h_{M_2} = h_{M_1} + h_{L_2} + O(1)$ がわかる．これは，$\bmod B(X)$ で $h_L = h_{L_1} - h_{L_2}$ が well-defined であることを示している．

(d) 一般の直線束に対して，条件 (1)，(2) を調べよう．大域切断で生成される直線束 A，A'，B，B' を用意して，$L_1 = A \otimes A'^{-1}$，$L_2 = B \otimes B'^{-1}$ と表す．この時，$\bmod B(X)$ で

$$\begin{aligned} h_{L_1 \otimes L_2} &= h_{(A\otimes B)\otimes (A'\otimes B')^{-1}} \\ &= h_{A\otimes B} - h_{A'\otimes B'} \\ &= (h_A + h_B) - (h_{A'} + h_{B'}) \\ &= (h_A - h_{A'}) + (h_B - h_{B'}) \\ &= h_{L_1} + h_{L_2} \end{aligned}$$

となる．また大域切断で生成される直線束 C, C' を用意して，$L = C \otimes C'^{-1}$ と表す．この時，$\bmod B(X)$ で

$$\begin{aligned} h_{f^*(L)} &= h_{f^*(C)\otimes f^*(C')^{-1}} \\ &= h_{f^*(C)} - h_{f^*(C')} \\ &= f^*(h_C) - f^*(h_{C'}) \\ &= f^*(h_L) \end{aligned}$$

となる．

(e) 最後に一意性であるがこれは (a)，(c) の構成を見れば明らかである．　□

命題 1.4.4 (高さの positivity)**.** X を $\overline{\mathbb{Q}}$ 上の射影多様体とし，L を X 上の直線束とする．B を

$$\mathrm{Coker}(H^0(X, L) \otimes \mathcal{O}_X \to L)$$

の台とする．この時，ある定数 C が存在して，$h_L(x) \geq C$ がすべての $x \in (X \setminus B)(\overline{\mathbb{Q}})$ で成立する．

証明:　s を $H^0(X, L)$ のゼロでない元とする．まず，次のことを示そう．

主張 1.4.4.1. ある定数 C' が存在して，$x \in X(\overline{\mathbb{Q}})$ で $s(x) \neq 0$ なら，$h_L(x) \geq C'$ となる．

証明:　まず，大域切断で生成される直線束 L_1，L_2 がとってきて，$L = L_1 \otimes L_2^{-1}$ と書く．$\{s_1, \ldots, s_n\}$ を $H^0(X, L_2)$ の基底とする．この時，$\{ss_i\}$ は一次独立な $H^0(X, L_1)$ の元である．元 $t_{n+1}, \ldots, t_N$ を加えて，$\{ss_1, \ldots, ss_n, t_{n+1}, \ldots, t_N\}$ が $H^0(X, L_1)$ の基底となる

ようにとる．この時，もし $s(x) \neq 0$ なら，

$$\begin{aligned} h_L(x) &= h((s(x)s_1(x), \dots, s(x)s_n(x), t_{n+1}(x), \dots, t_N(x))) - h((s_1(x), \dots, s_n(x))) \\ &\geq h((s(x)s_1(x), \dots, s(x)s_n(x))) - h((s_1(x), \dots, s_n(x))) \\ &= h((s_1(x), \dots, s_n(x))) - h((s_1(x), \dots, s_n(x))) = 0 \end{aligned}$$

となり，主張が証明できた． □

命題 1.4.4 の証明にもどろう．$\{s_1, \dots, s_n\}$ を $H^0(X, L)$ の基底とする．前の主張より，ある定数 C_i が存在して，$x \in X(\overline{\mathbb{Q}})$ で $s_i(x) \neq 0$ なら，$h_L(x) \geq C_i$ となる．

$$C = \min\{C_1, \dots, C_n\}$$

とおく．$B = \{x \in X \mid s_1(x) = \cdots = s_n(x) = 0\}$ であるので，$x \notin B$ なら $h_L(x) \geq C$ が成り立つ． □

1.5. Ｎｏｒｔｈｃｏｔｔの有限性定理

本節では，有理点の有限性を示すための重要な判定法となる Northcott の定理を証明する．

補題 1.5.1. 任意の数 $d \geq 1$，$M \geq 0$ に対して，集合

$$\left\{x \in \overline{\mathbb{Q}} \mid h^+(x) \leq M, \quad [\mathbb{Q}(x) : \mathbb{Q}] \leq d\right\}$$

は有限集合である．

証明: まず，$d = 1$ の時を考える．これは，$x \in \mathbb{Q}$ を意味する．そこで，$x = p/q$，$(p, q) = 1$ と表す．この時，$h^+(x) = h((p, q)) = \max\{|p|, |q|\}$ である．よって，$|p|, |q| \leq M$ であるので結論を得る．

一般の場合を考えよう．$x_1, \cdots, x_n$ を x のすべての共役元とし，$P = (T - x_1) \cdots (T - x_n)$ とおく．このとき，$n \leq d$，$P \in \mathbb{Q}[T]$ で，(1.3.4) より

$$\begin{aligned} h(P) &\leq h(T - x_1) + \cdots + h(T - x_n) + n\log(2) \\ &= h^+(x_1) + \cdots + h^+(x_n) + n\log(2) \\ &\leq n(\log(2) + M) \leq d(\log(2) + M) \end{aligned}$$

である．ここで，$P = T^n + a_1 T^{n-1} + \cdots + a_n$ とおくと，すべての i について $h^+(a_i) \leq h(P)$ である．よって，a_i は有限個の可能性しかなく，P の次数がおさえられているので，P は有限個の可能性のみである．よって，その根 x も有限個のみである． □

この補題により次が示せる．

定理 1.5.2 (Northcott の定理)**.** X を $\overline{\mathbb{Q}}$ 上定義された射影多様体，L を X 上の豊富な直線束とする．任意の数 $d \geq 1$，$M \geq 0$ に対して，集合

$$\left\{x \in X(\overline{\mathbb{Q}}) \mid h_L(x) \leq M, \quad [\mathbb{Q}(x) : \mathbb{Q}] \leq d\right\}$$

は有限集合である．

証明: m を十分大きくとって，L を L^m と置き換えることにより，L を十分豊富としてよい．この時，X は $|L|$ によって射影空間に埋め込まれるので，X は射影空間 $\mathbb{P}^n$ としてよい．つまり，

$$\left\{x = (x_0, \ldots, x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid h(x) \leq M, \quad [\mathbb{Q}(x) : \mathbb{Q}] \leq d\right\}$$

が有限集合であればよい．そこで，

$$U_i = \left\{x = (x_0, \ldots, x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid h(x) \leq M, \quad [\mathbb{Q}(x) : \mathbb{Q}] \leq d, \quad x_i \neq 0\right\}$$

とおくと，前の集合が有限集合であるためには U_i がすべての i について有限集合であればよい．簡単のため，U_0 が有限集合であることを示す．他の場合も同様である．$y_i = x_i/x_0$ とおく．この時，

$$h(x) = h((1 : y_1 : \cdots : y_n)) \geq h^+(y_i), \qquad \mathbb{Q}(y_i) \subseteq \mathbb{Q}(x)$$

がすべての i で成り立つ．よって，補題 1.5.1により，y_i は有限個のみである．つまり，x も有限個のみである． □

1.6. アーベル多様体上の高さ

本節では，前節までの高さの定義にあったあいまいさがアーベル多様体上ではとれることを示そう．

まず始めに次の補題を示しておこう．

補題 1.6.1. A をアーベル群，$h : A \to \mathbb{R}$ を写像で，

$$h(x+y+z) - h(x+y) - h(y+z) - h(z+x) + h(x) + h(y) + h(z) = O(1)$$

が任意の $x, y, z \in A$ で成立しているとする．この時，ある対称な双線形写像 $b : A \times A \to \mathbb{R}$ と線形写像 $l : A \to \mathbb{R}$ が一意的に存在して，

$$h(x) = \frac{1}{2}b(x,x) + l(x) + O(1)$$

が任意の $x \in A$ で成立する．

証明: $\beta(x,y) = h(x+y) - h(x) - h(y)$ とおく．β は対称であり，条件よりある定数 C が存在して，

$$|\beta(x+y,z) - \beta(x,z) - \beta(y,z)| \leq C$$

がすべての $x,y,z \in A$ で成り立つ．よって，容易に

$$|\beta(2^{n+1}x, 2^{n+1}y) - 4\beta(2^n x, 2^n y)| \leq 3C$$

となることがわかる．つまり

$$|4^{-(n+1)}\beta(2^{n+1}x, 2^{n+1}y) - 4^{-n}\beta(2^n x, 2^n y)| \leq 3C4^{-(n+1)}$$

である．したがって数列 $\{4^{-n}\beta(2^n x, 2^n y)\}$ はコーシー列となり，$\lim_{n\to\infty} 4^{-n}\beta(2^n x, 2^n y)$ が存在する．そこで，

$$b(x,y) = \lim_{n\to\infty} 4^{-n}\beta(2^n x, 2^n y)$$

とおく．b の対称性は β の対称性より明らかである．前の評価より

$$|4^{-N}\beta(2^N x, 2^N y) - \beta(x,y)| \leq 3C\sum_{n=0}^{N-1} 4^{-(n+1)} \leq C$$

であるので，$|b-\beta| \leq C$ である．また

$$|4^{-n}\beta(2^n(x+y), 2^n z) - 4^{-n}\beta(2^n x, 2^n z) - 4^{-n}\beta(2^n y, 2^n z)| \leq 4^{-n}C$$

でなるので，b は双線形写像である．

次に $\lambda(x) = h(x) - \frac{1}{2}b(x,x)$ とおく．この時，$\lambda(x+y) - \lambda(x) - \lambda(y) = \beta(x,y) - b(x,y)$ であるので，

$$|\lambda(x+y) - \lambda(x) - \lambda(y)| \leq C$$

となる．よって

$$|2^{-(n+1)}\lambda(2^{n+1}x) - 2^{-n}\lambda(2^n x)| \leq 2^{-(n+1)}C$$

となり，$l(x) = \lim_{n\to\infty} 2^{-n}\lambda(2^n x)$ とおくと，これは収束し，$|l-\lambda| \leq C$ であることが確かめられる．さらに前と同様にして l が線形であることも容易に確かめられる．よって，b と l によって

$$h(x) = \frac{1}{2}b(x,x) + l(x) + O(1)$$

となる．

最後に一意性について考える．別の対称な双線形写像 b' と線形写像 l' で $h = \frac{1}{2}b' + l' + O(1)$ であったとする．この時，$\beta = b' + O(1)$ ゆえ，$b = b' + O(1)$ となる．つまりある定数 C' が存在して，$|b - b'| \leq C'$ である．特に，

$$2^n|b(x,y) - b'(x,y)| = |b(2^n x, y) - b'(2^n x, y)| \leq C'$$

ゆえ，n を ∞ に飛ばして，$b = b'$ を得る．したがって，$l = l' + O(1)$ となり，同様にして $l = l'$ も確かめられる． □

定理 1.6.2. A を $\overline{\mathbb{Q}}$ 上定義されたアーベル多様体とする．この時，任意の直線束 L に対して，対称な双線形写像 $b_L : A(\overline{\mathbb{Q}}) \times A(\overline{\mathbb{Q}}) \to \mathbb{R}$ と線形写像 $l_L : A(\overline{\mathbb{Q}}) \to \mathbb{R}$ が一意的に存在して，

$$h_L(x) = \frac{1}{2}b_L(x,x) + l_L(x) + O(1)$$

が任意の $x \in A(\overline{\mathbb{Q}})$ で成立する．以後，

$$\hat{h}_L(x) = \frac{1}{2}b_L(x,x) + l_L(x)$$

と表し，L の標準的な高さ，あるいは，Neron-Tate の高さと呼ぶ．さらに，L の標準的な高さは以下の性質を満たす．

(1) $\hat{h}_{L_1 \otimes L_2} = \hat{h}_{L_1} + \hat{h}_{L_2}$ が任意の直線束 L_1, L_2 で成立する．
(2) $f : A \to B$ がアーベル多様体の間の準同型射とすると，$\hat{h}_{f^*(L)} = f^*(\hat{h}_L)$ である．
(3) $[-1] : A \to A$ を $[-1](x) = -x$ で定義される準同型射とする．もし L が偶，つまり，$[-1]^*(L) = L$ なら，$l_L = 0$ である．さらに L が奇，つまり，$[-1]^*(L) = L^{-1}$ なら，$B_L = 0$ である．

証明: 定理の前半を示すために，次の補題を用いる．(詳しくは，[**10**, p.58, Corollary 2] を参照)

補題 1.6.3 (立方定理)**.** X を射影多様体，A をアーベル多様体とし，X から A への 3 つの射 f, g, h があるとする．この時，任意の A 上の直線束 L に対して，

$$(f+g+h)^*(L) \otimes (f+g)^*(L^{-1}) \otimes (g+h)^*(L^{-1}) \otimes (h+f)^*(L^{-1}) \\ \otimes f^*(L) \otimes g^*(L) \otimes h^*(L) = \mathcal{O}_X$$

が成立する．

よって，$p_i : A \times A \times A \to A$ を i- 成分への射影とすると，補題 1.6.3 により

$$(p_1+p_2+p_3)^*(L) \otimes (p_1+p_2)^*(L^{-1}) \otimes (p_2+p_3)^*(L^{-1}) \otimes (p_3+p_1)^*(L^{-1}) \\ \otimes p_1^*(L) \otimes p_2^*(L) \otimes p_3^*(L) = \mathcal{O}_A$$

が成立し，これから

$$h_L(x+y+z) - h_L(x+y) - h_L(y+z) - h_L(z+x) + h_L(x) + h_L(y) + h_L(z) = O(1)$$

を得る．よって，補題 1.6.1 を使って定理の前半が示せる．

(1) と (2) は定理 1.4.3 より明らかである．

(3) $[-1]^*L = L$ なら，(2) より $\hat{h}_L(-x) = \hat{h}_L(x)$ である．よって，$l(-x) = l(x)$ が分かるので，$l(x) = 0$ である．$[-1]^*L = L^{-1}$ なら，(2) より $\hat{h}_L(-x) = -\hat{h}_L(x)$ である．よって，$b(-x,-x) = -b(x,x)$ が分かるので，$b(x,x) = 0$ である．ここで，$2b(x,y) = b(x+y, x+y) - b(x,x) - b(y,y)$ であるので $b = 0$ を得る． □

A を $\overline{\mathbb{Q}}$ 上定義されたアーベル多様体とし，L を A 上の偶の豊富な直線束とする．今後，$b_L(x,y)$ を $\langle x,y\rangle_L$ で表し，これを Neron-Tate height pairing と言う．定理 1.6.2 より，$\hat{h}(x) = \frac{1}{2}\langle x,x\rangle_L$ である．

定理 1.6.4. 上の状況のもとで，$\langle\ ,\ \rangle_L : A(\overline{\mathbb{Q}}) \times A(\overline{\mathbb{Q}}) \to \mathbb{R}$ は，$\bmod\ A(\overline{\mathbb{Q}})_{tor}$ で正定値である．さらに，$p_i : A \times A \to A$ を i- 成分への射影とし，$P = (p_1+p_2)^*(L) \otimes p_1^*(L^{-1}) \otimes p_2^*(L^{-1})$ とおくと，$A(\overline{\mathbb{Q}}) \times A(\overline{\mathbb{Q}})$ 上で $\hat{h}_P(x,y) = \langle x,y\rangle_L$ となる．

証明: L は豊富であるので十分大きな n について L^n は射影空間への埋めこみを定める．ゆえに，命題 1.4.4 より，ある定数 C が存在して $\hat{h}_{L^n}(x) \geq C$ である．つまり，$\hat{h}_L(x) \geq C/n$ である．したがって，

$$m^2\hat{h}_L(x) = \hat{h}_L(mx) \geq C/n$$

であるので，m を無限大に飛ばして $\hat{h}_L(x) \geq 0$ を得る．正定値をいうためには $\hat{h}_L(x) = 0$ なら $x \in A(\overline{\mathbb{Q}})_{tor}$ であればよい．ある代数体 K をとって $x \in A(K)$ とし，x の生成する巡回群 G を考える．これは $A(K)$ の部分群であり，$y = nx \in G$ に対して $\hat{h}_L(y) = n^2\hat{h}_L(x) = 0$ である．よって，Northcott の定理 (定理 1.5.2) により G は有限群となる．したがって $x \in A(K)_{tor}$ となる．これで定理の前半が示せた．

$\phi(x) = (x,x)$ で定義される $\phi : A \to A \times A$ を考える．今，$[n] : A \to A$ を n 倍射像とすると，

$$\phi^*(P) = [2]^*(L) \otimes L^{-2}$$

となる．$f=[1], g=[1], h=[-1]$ で補題 1.6.3 を用いて，

$$[2]^*(L) = L^3 \otimes [-1]^*(L)$$

を得る．ここで，L は偶ゆえ，$[2]^*(L) = L^4$ である．したがって，$\phi^*(P) = L^2$ である．これは，

$$\hat{h}_P(x,x) = 2\hat{h}_L(x) = \langle x,x\rangle_L$$

を示している．ここで，$\iota : A\times A \to A\times A$ を $\iota(x,y)=(y,x)$ と定めると，$\iota^*(P)=P$ である．よって，

$$\hat{h}_P(x,y) = \hat{h}_P(y,x)$$

が成り立つ．さらに，

$$\hat{h}_P(x+y,z) = \hat{h}_P(x,z) + \hat{h}_P(y,z)$$

を示そう．ここで，射 $a,b,c : A\times A\times A \to A\times A$ を $a(x,y,z)=(x+y,z)$，$b(x,y,z)=(x,z)$，$c(x,y,z)=(y,z)$ と定める．さらに，$q_i : A\times A\times A \to A$ を i- 成分への射影とする．この時，

$$\begin{array}{ccc}
(p_1+p_2)\cdot a = q_1+q_2+q_3 & (p_1+p_2)\cdot b = q_1+q_3 & (p_1+p_2)\cdot c = q_2+q_3 \\
p_1\cdot a = q_1+q_2 & p_1\cdot b = q_1 & p_1\cdot c = q_2 \\
p_2\cdot a = q_3 & p_2\cdot b = q_3 & p_2\cdot c = q_3
\end{array}$$

であるので，

$$\begin{aligned}
a^*(P) - b^*(P) - c^*(P) &= (q_1+q_2+q_3)^*(L) \\
&\quad - (q_1+q_2)^*(L) - (q_2+q_3)^*(L) - (q_3+q_1)^*(L) - q_1^*(L) - q_2^*(L) - q_3^*(L)
\end{aligned}$$

であることが確かめられる．したがって，補題 1.6.3 より，

$$a^*(P) - b^*(P) - c^*(P) \sim 0$$

である．これより

$$\hat{h}_P(x+y,z) = \hat{h}_P(x,z) + \hat{h}_P(y,z)$$

を得る．以上より，

$$\hat{h}_P(x+y,x+y) = \langle x+y,x+y\rangle_L$$

を展開して，$\hat{h}_P(x,y) = \langle x,y\rangle_L$ が得られる． □

後で示すが，K が代数体のとき $A(K)$ は有限生成アーベル群になる．したがって，

$$\langle\ ,\ \rangle_L : A(K) \times A(K) \to \mathbb{R}$$

は 有限次ベクトル空間 $A(K) \otimes \mathbb{R}$ 上の内積を定める．

1.7. 曲線とヤコビ多様体

本節では，前節の結果を曲線とそのヤコビ多様体の場合についてみてみよう．C を体 F 上定義された非特異射影曲線とする．各整数 n に対して，$\mathrm{Pic}^n(C)$ を次数が n の C 上の直線束の族を表すとする．特に，$J = \mathrm{Pic}^0(C)$ とおき，C のヤコビ多様体という．各 $a \in \mathrm{Pic}^1(C)$ に対して，$\phi_a : C \to J$ を $\phi_a(x) = a - x$ で定義される埋め込みとする．今，定義体 F を少し大きくとって，$(2g-2)\theta \sim \omega_C$ となる因子 θ を固定する．θ による埋め込み ϕ_θ を特に ϕ と書くことにする．$(P_1, \cdots, P_{g-1}) \mapsto P_1 + \cdots + P_{g-1}$ で与えられる写像 $C^{g-1} \to \mathrm{Pic}^{g-1}(C)$ の像を Θ_{g-1} で表し，これをテータ因子と呼ぶ．さらに，$c \mapsto c + (g-1)\theta$ で与えられる同型 $\mathrm{Pic}^0(C) \to \mathrm{Pic}^{g-1}(C)$ による Θ_{g-1} の引き戻しを Θ で表すことにする．この時，次が成立する．

命題 1.7.1. (1) $\mathcal{O}_J(\Theta)$ は偶である．

(2) 任意の $a \in \mathrm{Pic}^1(C)$ に対して，$\phi_a^*(\Theta) \sim (g-1)\theta + a$ である．特に，$\phi^*(\Theta) \sim g\theta$ である．

(3) $p_i : J \times J \to J$ を i-成分への射影とし, $P = (p_1 + p_2)^*(\Theta) - p_1^*(\Theta) - p_2^*(\Theta)$ とおくと，

$$(\phi \times \phi)^*(P) \sim q_1^*(\theta) + q_2^*(\theta) - \Delta$$

である．ここで，$q_i : C \times C \to C$ は i-成分への射影で，Δ は $C \times C$ の対角成分である．

証明: (1) $x \in \Theta \Longrightarrow -x \in \Theta$ を示せば十分である．$x \in \Theta$ は，定義により $x + (g-1)\theta \in \Theta_{g-1}$ ということである．よって，ある点 $P_1, \ldots, P_{g-1}$ が存在して

$$x + (g-1)\theta \sim P_1 + \cdots + P_{g-1}$$

となる．ここで $\dim H^0(C, \omega_C) = g$ であるので，$H^0(C, \omega_C(-P_1 - \cdots - P_{g-1})) \neq 0$ である．つまり，ある点 $Q_1, \ldots, Q_{g-1}$ が存在して

$$(2g-2)\theta \sim \omega_C \sim P_1 + \cdots + P_{g-1} + Q_1 + \cdots + Q_{g-1}$$

となる．よって

$$-x + (g-1)\theta \sim Q_1 + \cdots + Q_{g-1}$$

となるので，$-x \in \Theta$ である．

(2) まず a が一般の点の場合を考えよう．a を一般にとれば，

$$\dim H^0(C, \mathcal{O}_C(a+(g-1)\theta)) = 1$$

で，$|a+(g-1)\theta)|$ の元は相異なる点の和である．つまり，相異なる $P_1, \ldots, P_g$ が順序を除いて一意的に存在して

$$P_1 + \cdots + P_g \sim a + (g-1)\theta$$

となる．さて $P_1, \ldots, P_g$ の順序を除いての一意性を用いると，

$$\begin{aligned}
\phi_a(x) \in \Theta &\iff a - x + (g-1)\theta \in \Theta_{g-1} \\
&\iff a - x + (g-1)\theta \sim Q_1 + \cdots + Q_{g-1} \quad \text{for some } Q_i \in C \\
&\iff a + (g-1)\theta \sim x + Q_1 + \cdots + Q_{g-1} \\
&\iff P_1 + \cdots + P_g \sim x + Q_1 + \cdots + Q_{g-1} \\
&\iff x \in \{P_1, \ldots, P_g\}
\end{aligned}$$

となる．よって，$\phi^{-1}(\Theta) = \{P_1, \ldots, P_g\}$，つまり，

$$\phi_a^*(\Theta) \sim P_1 + \cdots + P_g \sim a + (g-1)\theta$$

である．次にすべての $a \in \mathrm{Pic}^1(C)$ の場合に拡張しよう．Q_g を $C \times \mathrm{Pic}^g(C)$ 上の Poincaré 束とする．つまり，任意の $c \in \mathrm{Pic}^g(C)$ に対して，$Q_g|_{C\times\{c\}} = c$ となる直線束である．さらに $(x, a) \mapsto (x, (g-1)\theta + a)$ で定義される $\alpha : C \times \mathrm{Pic}^1(C) \to C \times \mathrm{Pic}^g(C)$ による Q_g の引き戻し $\alpha^*(Q_g)$ を Q とする．このとき，任意の $a \in \mathrm{Pic}^1(C)$ に対して，$Q|_{C\times\{a\}} = (g-1)\theta + a$ となる．$\Phi : C \times \mathrm{Pic}^1(C) \to J$ を $\Phi(x, a) = a - x$ で定める射とし，$M = \mathcal{O}_{C\times\mathrm{Pic}^1(C)}(\Phi^*(\Theta)) \otimes Q^{-1}$ とおく．さて，第一成分への射影 $p : C \times \mathrm{Pic}^1(C) \to \mathrm{Pic}^1(C)$ を考えよう．ここで，

$$M|_{p^{-1}(a)} = \phi_a^*(\Theta) - (g-1)\theta - a$$

がすべての $a \in \mathrm{Pic}^1(C)$ に対して成立することが大切である．まず，p は平坦射であるので，すべての $a \in \mathrm{Pic}^1(C)$ に対して $\deg(M|_{p^{-1}(a)}) = 0$ である．一方，a が一般の場合，前の結果より，$\dim H^0(C, M|_{p^{-1}(a)}) > 0$ である．よって，コホモロジーの次元の上半連続性より，$\dim H^0(C, M|_{p^{-1}(a)}) > 0$ がすべての $a \in \mathrm{Pic}^1(C)$ に対して成立する．ゆえに $M|_{p^{-1}(a)} \simeq \mathcal{O}_C$ がすべての $a \in \mathrm{Pic}^1(C)$ に対してわかる．

(3) $L = \mathcal{O}_{C\times C}(q_1^*(\theta) + q_2^*(\theta) - \Delta - (\phi \times \phi)^*(P))$ とおく．まず，任意の $x_1, x_2 \in C$ について

$$L|_{\{x_1\}\times C} \simeq \mathcal{O}_C, \qquad L|_{C\times\{x_2\}} \simeq \mathcal{O}_C$$

を調べる．$f : C \to J \times J$ を $f(x) = (\phi(x_1), \phi(x))$ で定義すると，

$$(\phi \times \phi)^*(P)|_{\{x_1\}\times C} = f^*(P)$$

である．ここで，$\phi(x_1) + \phi(x) = (\theta - x_1 + \theta) - x$ であることに注意して，(2) の結果を用いると

$$\begin{aligned} f^*(P) &= \phi^*_{\theta - x_1 + \theta}(\Theta) - 0 - \phi^*(\Theta) \\ &= \theta - x_1 + \theta + (g-1)\theta - g\theta \\ &= \theta - x_1 \end{aligned}$$

である．一方，

$$q_1^*(\theta) + q_2^*(\theta) - \Delta|_{\{x_1\}\times C} = \theta - x_1$$

である．よって，$L|_{\{x_1\}\times C} \simeq \mathcal{O}_C$ となる．同様にして，$L|_{C\times\{x_2\}} \simeq \mathcal{O}_C$ もわかる．

$L|_{\{x_1\}\times C} \simeq \mathcal{O}_C$ であるので，$q_{1*}(L)$ は直線束で，$q_1^*(q_{1*}(L)) \to L$ は全射である．よって，$M = q_{1*}(L)$ とおくと $L = q_1^*(M)$ である．ところが $L|_{C\times\{x_2\}} \simeq \mathcal{O}_C$ であるので $M \simeq \mathcal{O}_C$ となる．ゆえに，$L \simeq \mathcal{O}_{C\times C}$ となり (3) が証明できた． □

さて，この結果を高さに応用しよう．C，θ はそれぞれが $\overline{\mathbb{Q}}$ 上定義されていることを除いて前と同じとする．この時，次が成立する．

系 1.7.2. (1) $C \times C$ 上で，$\Delta' = \Delta - q_1^*(\theta) - q_2^*(\theta)$ とおくと，すべての $x, y \in C(\overline{\mathbb{Q}})$ について

$$\langle \phi(x), \phi(y) \rangle_\Theta = h_{-\Delta'}(x, y) + O(1)$$

が成り立つ．

(2) すべての $x \in C(\overline{\mathbb{Q}})$ について

$$\langle \phi(x), \phi(x) \rangle_\Theta = 2g h_\theta(x) + O(1)$$

が成り立つ．

証明: (1) まず定理 $1.6.4$ より

$$\langle \phi(x), \phi(y) \rangle_\Theta = \hat{h}_P(\phi(x), \phi(y))$$

が成り立つ．ここで，$P = (p_1 + p_2)^*(\Theta) - p_1^*(\Theta) - p_2^*(\Theta)$ である．一方，命題 $1.7.1$ を用いると

$$\hat{h}_P(\phi(x), \phi(y)) = h_{(\phi\times\phi)^*(P)}(x, y) + O(1) = h_{-\Delta'}(x, y) + O(1)$$

となるので (1) が示せた．

(2) 命題 1.7.1 より

$$\langle \phi(x), \phi(x) \rangle_\Theta = 2\hat{h}_\Theta(\phi(x)) = 2h_{\phi^*(\Theta)}(x) + O(1) = 2h_{g\theta}(x) + O(1) = 2gh_\theta(x) + O(1)$$

となる． □

1.8. Ｍｏｒｄｅｌｌ-Ｗｅｉｌの定理

本節は，前半の山場である．ここでは，いわゆる Mordell-Weil の定理を証明する．これは数論幾何において基本定理であり，いろいろな研究の出発点である．楕円曲線に限っても，非常に深い定理である．まず始めに次の補題を証明しよう．

補題 1.8.1. K を代数体，O_K を K の整数環，$D_{K/\mathbb{Q}}$ を K の $\mathbb{Q}$ 上の判別式とする．いま，S を $\mathrm{Spec}(\mathbb{Z})$ の有限集合で，O_K は，$\mathbb{Z}$ 上 S の外で不分岐で，$n = [K : \mathbb{Q}]$ であるとする． この時，

$$|D_{K/\mathbb{Q}}| \leq \prod_{p \in S} p^{n-1+n\log_p(n)}$$

が成立する．

証明:　$\mathcal{D}_K$ を K の共役差積 (Difference) とする．つまり，$\mathcal{D}_K^{-1}$ は，

$$\{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(xO_K) \subset \mathbb{Z}\}$$

で定義される．あるいは，$\alpha \in K$ に対して，多項式 $f_\alpha(X) = \mathrm{Norm}_{K/\mathbb{Q}}(X - \alpha)$ と定義すると，$\mathcal{D}_K$ は $\{f'_\alpha(\alpha)\}_{\alpha \in O_K}$ で生成されるイデアルである．この時，$\#(O_K/\mathcal{D}_K) = |D_{K/\mathbb{Q}}|$ となる．$p \in S$ で，$pO_K = P_1^{e_1} \cdots P_l^{e_l}$ とおく．このとき，$\mathcal{D}_K$ はイデアルで，

$$\mathrm{ord}_{P_i}(\mathcal{D}_K) \leq e_i - 1 + \mathrm{ord}_{P_i}(e_i)$$

が成立する．これは，例えば，次のようにして示される．(詳しくは，[8] の III，§2，Proposition 8 の証明を参照のこと．)

A を $\mathbb{Z}$ の p で完備化，B を O_K の P_i での完備化する．A の B 内での不分岐拡大を考えて，B は A 上 totally ramified であるとしてよい．この時，次を満たす A 上の多項式

$$f(X) = a_e X^e + a_{e-1} X^{e-1} + \cdots + a_1 X + a_0$$

が存在する．(1) T は B の parameter で，$f(T) = 0$，(2) $a_e = 1$，$\mathrm{ord}_A(a_0) = 1$，$\mathrm{ord}_A(a_i) \geq 1$ $(i \geq 1)$．局所的に $\mathcal{D}_K$ は，

$$f'(T) = eT^{e-1} + (e-1)a_{e-1}T^{e-2} + \cdots + a_1$$

で生成される．ここで，

$$\mathrm{ord}_B((e-i)a_{e-i}T^{e-i-1}) = e\,\mathrm{ord}_A((e-i)a_{e-i}) + (e-i-1) \equiv e-i-1 \pmod{e}$$

であるので，$f'(T)$ の各項は異なる order を持つ．よって，

$$\mathrm{ord}_B(f'(T)) = \min\{\mathrm{ord}_B((e-i)a_{e-i}T^{e-i-1})\} \leq \mathrm{ord}_B(eT^{e-1}) = e - 1 + \mathrm{ord}_B(e)$$

となる．

$f_i = [O_K/P_i : \mathbb{Z}/p\mathbb{Z}]$ とおく．この時，$\mathrm{ord}_{P_i}(e_i) = e_i \,\mathrm{ord}_p(e_i)$ であるので，

$$\begin{aligned}\log_p\left(\#\left((O_K)_p/(\mathcal{D}_K)_p\right)\right) &= \sum_i \mathrm{ord}_{P_i}(\mathcal{D}_K) f_i \\ &\leq \sum_i (e_i - 1 + e_i \,\mathrm{ord}_p(e_i)) f_i.\end{aligned}$$

ここで，$p^{\mathrm{ord}_p(e_i)} \leq e_i \leq n$ であるので，$\mathrm{ord}_p(e_i) \leq \log_p(n)$ である．よって，$\sum_i e_i f_i = n$ を用いて，

$$\begin{aligned}\log_p\left(\#\left((O_K)_p/(\mathcal{D}_K)_p\right)\right) &\leq \sum_i (e_i - 1 + e_i \log_p(n)) f_i \\ &\leq n - 1 + n \log_p(n)\end{aligned}$$

したがって，$\#(O_K/\mathcal{D}_K) = \prod_{p\in S} \#\left((O_K)_p/(\mathcal{D}_K)_p\right)$ であるので，補題が証明できた． □

定理 1.8.2. *K を代数体，S を $\mathrm{Spec}(O_K)$ の有限集合，n を自然数とする．この時，S の外では不分岐となる高々 n- 次の K の拡大は有限個のみ存在する．*

証明: まず最初に，$K = \mathbb{Q}$ の場合に帰着できることは明らかである．L を S の外では不分岐となる高々 n- 次の拡大とする．Hermite-Minkowski の定理により，$|D_{L/\mathbb{Q}}|$ が有界であればよい．(Hermite-Minkowski の定理については，[**13**, 5.2] を参照のこと) $|D_{L/\mathbb{Q}}|$ の有界性は，補題 1.8.1の主張そのものである． □

定理 1.8.3 (Chevalley-Weil の定理)**.** *K を代数体，$\pi : Y \to X$ を K 上定義された射影多様体の間のエタール写像とする．このとき，ある $f \in O_K \setminus \{0\}$ が存在して，以下の性質を満たす．任意の $P \in X(K)$ に対して，ある拡大体 K' と $Q \in Y(K')$ が存在して，$\pi(Q) = P$，$[K' : K] \leq \deg(\pi)$ であり，$O_{K'}$ は O_K 上 f を割らない素イデアル上エタールとなる．*

証明: Y，X，π は，有限個の多項式で定義されているので，その係数の共通分母として $f \in O_K \setminus \{0\}$ がとれる．この時，ある $O_K[1/f]$ 上の射影スキーム $\widetilde{Y}$，$\widetilde{X}$ と $O_K[1/f]$ 上の射 $\widetilde{\pi} : \widetilde{Y} \to \widetilde{X}$ が存在して，それらは K 上 Y，X，$\pi : Y \to X$ と一致する．さらに f を取り替えて，$\widetilde{\pi} : \widetilde{Y} \to \widetilde{X}$ はエタールとしてよい．さて，$P \in X(K)$，つまり，$\mathrm{Spec}(K) \to X$ をとる．$\widetilde{X}$ は $O_K[1/f]$ 上射影的であるので，これは，$\mathrm{Spec}(O_K[1/f]) \to \widetilde{X}$ に拡張する．$Z = \mathrm{Spec}(O_K[1/f]) \times_{\widetilde{X}} \widetilde{Y}$ とおく．

$$\begin{array}{ccc} Z & \longrightarrow & \widetilde{Y} \\ \downarrow & & \downarrow{\scriptstyle \widetilde{\pi}} \\ \mathrm{Spec}(O_K[1/f]) & \longrightarrow & \widetilde{X} \end{array}$$

$Z \to \mathrm{Spec}(O_K[1/f])$ はエタールな有限射であるので，Z は正則なアファインスキームである．Z' を Z の連結成分とし，K' を Z' の商体とする．このとき，Z' は，$\mathrm{Spec}(O_K[1/f])$ 上エタールで，$[K' : K] \leq \deg(\pi)$ である．さらに，$Z' \hookrightarrow Z \to \widetilde{Y}$ は，$Q \in Y(K')$ を定め，$\pi(Q) = P$ となる． □

定理 1.8.4 (弱 Mordell-Weil の定理)**.** *K を代数体，A を K 上のアーベル多様体とする．$n \geq 2$ を自然数とし，A の n-torsion points はすべて K 上で定義されているとする．この時，$A(K)/nA(K)$ は有限群である．*

証明: $[n](x) = nx$ で定義される射像 $[n] : A \to A$ を考える．これは，エタール射像である．定理 1.8.3 により，ある $\mathrm{Spec}(O_K)$ の有限集合 S が存在して以下の性質を満たす．任意の $P \in A(K)$ に対して，ある拡大体 K' と $Q \in A(K')$ が存在して，$[n](Q) = P$，$[K' : K] \leq \deg([n])$ であり，$O_{K'}$ は S の外で O_K 上エタールとなる．このような K' は，定理 1.8.2により，有限個しか存在しない．よって L をすべての K' を含む K 上のガロア拡大とする．L/K のガロア群を G で表す．A_n で A の n-torsion points 全体を表すことにする．仮定より，$A_n \subset A(K)$ である．

さて，準同型 $h : A(K) \to \mathrm{Hom}(G, A_n)$ を構成することを考えよう．$P \in A(K)$ に対して，$nQ = P$ となる $Q \in A(L)$ をとる．$g \in G$ をとってきて，$g(Q) - Q$ を考える．まず最初に，$g(Q) - Q \in A_n$ を見よう．

$$n(g(Q) - Q) = g(nQ) - nQ = g(P) - P = P - P = 0$$

であるので，$g(Q) - Q \in A_n$ である．さらに，$g(Q) - Q$ は Q の取り方に依らないことを示そう．Q' を $nQ' = P$ となる別の $Q' \in A(L)$ とする．この時，$n(Q' - Q) = P - P = 0$ であるので，$Q' - Q \in A_n \subset A(K)$ である．したがって，

$$(g(Q') - Q') - (g(Q) - Q) = g(Q' - Q) - (Q' - Q) = (Q' - Q) - (Q' - Q) = 0.$$

よって，$g(Q) - Q$ は Q の取り方に依らないことが示せた．

以上のことにより，$h(P)(g) = g(Q) - Q$ と定めると

$$A(K) \to \mathrm{Map}(G, A_n)$$

が定義される．実際，$h(P) : G \to A_n$ は準同型である．というのは，

$$\begin{aligned} h(P)(gg') &= (gg')(Q) - Q = (g(Q) - Q) + g(g'(Q) - Q) \\ &= (g(Q) - Q) + (g'(Q) - Q) = h(P)(g) + h(P)(g') \end{aligned}$$

であるからである．よって，$h : A(K) \to \mathrm{Hom}(G, A_n)$ が定まった．さらに h は準同型である．というのは，$P_1, P_2 \in A(K)$ に対して，$nQ_1 = P_1$，$nQ_2 = P_2$ となる $Q_1, Q_2 \in A(L)$ をとり，$h(P_1 + P_2) = h(P_1) + h(P_2)$ をみよう．$n(Q_1 + Q_2) = P_1 + P_2$ であるので，

$$\begin{aligned} h(P_1 + P_2)(g) &= g(Q_1 + Q_2) - (Q_1 + Q_2) \\ &= (g(Q_1) - Q_1) + (g(Q_2) - Q_2) \\ &= h(P_1)(g) + h(P_2)(g) \end{aligned}$$

である．これは，$h(P_1 + P_2) = h(P_1) + h(P_2)$ を示している．

さて h の核を考えよう．

$$\begin{aligned} h(P) = 0 &\iff g(Q) - Q = 0 \ (\forall g \in G) \\ &\iff Q \in (A(L) \text{ の } G\text{- 不変部分群}) = A(K) \\ &\iff P \in nA(K) \end{aligned}$$

ゆえに，$\mathrm{Ker}(h) = nA(K)$ である．つまり，$A(K)/nA(K)$ は，$\mathrm{Hom}(G, A_n)$ の部分群に同型である．一方，$\mathrm{Hom}(G, A_n)$ は有限群である．よって，定理が証明できた． □

定理 1.8.5 (Mordell-Weil の定理)**.** *K を代数体，A を K 上のアーベル多様体とする．この時，$A(K)$ は有限生成アーベル群である．*

証明: 必要ならば，K を拡大して，A のすべての 2-torsion points は，$A(K)$ に含まれるとしてよい．A 上の $[-1]^*(L) = L$ となる豊富な直線束 L を固定し，$\langle\ ,\ \rangle_L : A(K) \times A(K) \to \mathbb{R}$ を L で決まる 1.6 節で構成された Néron-Tate height pairing とする．ここで，$|x| = \sqrt{\langle x, x \rangle_L}$ とおく．定理 1.8.4 により，$A(K)/2A(K)$ は有限群である．そこで，$\{x_i\}_{1 \le i \le a}$ を $A(K)/2A(K)$ の代表元とする．$C = \max_{1 \le i \le a}\{|x_i|\}$ とおき，B_n で $\{x \in A(K) \mid |x| \le nC\}$ で生成される $A(K)$ の部分群とする．この時，$A(K) = \bigcup_n B_n$ で，

$$B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n \subseteq \cdots$$

である．さてここで，$n \ge 3$ のとき，$B_{n-1} = B_n$ を示そう．$|x| \le nC$ とする．この時，$y \in A(K)$ と x_i が存在して，$x = 2y + x_i$ と書ける．よって，

$$|y| = \frac{|x - x_i|}{2} \le \frac{|x| + |x_i|}{2} \le \frac{n+1}{2} C$$

であるので，$n \ge 3$ に注意すると $|y| \le (n-1)C$ となる．ゆえに，$x \in B_{n-1}$ となり，これは，$B_n \subseteq B_{n-1}$ を示している．したがって，$A(K) = B_2$ で，$\{x \in A(K) \mid |x| \le 2C\}$ は，Northcott の定理により有限であるので，定理が証明できた． □

第 2 章

Ｍｏｒｄｅｌｌ−Ｆａｌｔｉｎｇｓの定理に向けての準備

2.1. Ｓｉｅｇｅｌの補題

本節では，直線束のうまい大域切断を見つけるために必要な Siegel の補題を証明する．これは，アラケロフ幾何にかわる部分である．まず始めに有理整数の場合から考えよう．

補題 2.1.1 (有理整数版 Siegel の補題)**.** $A = (a_{ij})$ を有理整数からなる階数が r の $m \times n$-行列とする．この時，もし $n > r$ なら，有理整数からなるベクトル $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$ で，$x \neq 0$，$Ax = 0$，

$$\max_i\{|x_i|\} \leq \left(n \max_{i,j}\{|a_{ij}|\}\right)^{\frac{r}{n-r}},$$

を満たすものが存在する．

証明: まず最初に，$m = r$ と仮定して話を進める．$Q = \max_{ij}\{|a_{ij}|\}$ とおく．H を $H \leq (n \max_{ij}\{|a_{ij}|\})^{\frac{m}{n-m}} < H + 1$ を満たす自然数とする．$0 \leq x_j \leq H\ (\forall j)$ となる $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$ に対して，$y = (y_1, \dots, y_m) = Ax$ とおく．今，n_i を $\{a_{i1}, \dots, a_{in}\}$ の中の負の数の数とすると

$$-n_i QH \leq y_i = \sum_{j=1}^{n} a_{ij}x_j \leq (n - n_i)QH$$

となる．ここで，

$$(H+1)^n = \#\left\{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid 0 \leq x_j \leq H\ (\forall j)\right\},$$
$$(nQH+1)^m = \#\left\{(y_1, \dots, y_m) \in \mathbb{Z}^m \mid -n_i QH \leq y_i \leq (n - n_i)QH\ (\forall i)\right\}$$

である．一方，

$$\begin{aligned}(H+1)^n &= (H+1)^m (H+1)^{n-m} \\ &> (H+1)^m \left((nQ)^{\frac{m}{n-m}}\right)^{n-m} \\ &= (H+1)^m (nQ)^m \\ &\geq (nQH+1)^m\end{aligned}$$

となる．したがって，Dirichlet の部屋割り論法より，ある

$$x_1, x_2 \in \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid 0 \leq x_j \leq H \ (\forall j)\}$$

が存在して，$x_1 \neq x_2$ かつ $Ax_1 = Ax_2$ が成立する．よって，$x = x_1 - x_2$ とおけば，求めるものである．

さて，一般の場合を考えよう．A の行を並び替えて，A の最初の r 行が一次独立であると仮定してよい．A' を A の最初の r 行からなる行列とする．A の $r+1$ 行以下の行は A' の行の一次結合で書けるので $Ax = 0$ であることと $A'x = 0$ であることは同値である．よって，A' について前の結果を使って結論を得る． □

K を代数体とし，$d = [K : \mathbb{Q}]$ とおく．$K(\mathbb{C})$ を K の $\mathbb{C}$-value points，つまり K の $\mathbb{C}$ への埋め込み全体とする．$x \in K$ に対して，

$$\|x\|_K = \max_{\sigma \in K(\mathbb{C})} \{|\sigma(x)|\}$$

とおく．このとき，$\| \ \|_K$ は，d- 次元 $\mathbb{R}$- ベクトル空間 $K \otimes_{\mathbb{Q}} \mathbb{R}$ のノルムに拡張する．

命題 2.1.2 (代数的整数版 Siegel の補題)**.** K を代数体，O_K を K の代数的整数全体とする．$A = (a_{ij})$ を O_K の元からなる階数が r の $m \times n$- 行列とする．この時，もし $n > r$ なら，O_K の元からなるベクトル $x = (x_1, \dots, x_n) \in O_K^n$ で，$x \neq 0$，$Ax = 0$，

$$\max_i\{\|x_i\|_K\} \leq C_1 \left(C_2 n \max_{i,j}\{\|a_{ij}\|_K\} \right)^{\frac{r}{n-r}},$$

を満たすものが存在する．ここで，C_1, C_2 は定数で，K 及び O_K の $\mathbb{Z}$ 上の自由基底の取り方のみによる．

証明: $\{\omega_1, \dots, \omega_d\}$ を O_K の $\mathbb{Z}$ 上の自由基底とする．$K \otimes_{\mathbb{Q}} \mathbb{R}$ の元 x を，$x = b_1\omega_1 + \cdots + b_d\omega_d \ (b_i \in \mathbb{R})$ と表すとき，

$$\|x\|_0 = \max_i\{|b_i|\}$$

でノルム $\| \ \|_0$ を定める．$\| \ \|_K$ と $\| \ \|_0$ は，有限次元のベクトル空間 $K \otimes_{\mathbb{Q}} \mathbb{R}$ のノルムであるので，ある正の数 M_1, M_2 が存在して，

$$M_1\|x\|_K \leq \|x\|_0 \leq M_2\|x\|_K$$

がすべての $x \in K \otimes_{\mathbb{Q}} \mathbb{R}$ で成立する．ここで，K の元からなるベクトル $v = (v_i)$ 及び 行列 $A = (a_{ij})$ に対して，

$$\|v\|_K = \max_i\{\|v_i\|_K\}, \qquad \|A\|_K = \max_{i,j}\{\|a_{ij}\|_K\}$$

とおく．同様にして，$\|x\|_0$ 及び $\|A\|_0$ も定義する．この時，

$$M_1\|v\|_K \le \|v\|_0 \le M_2\|v\|_K, \qquad M_1\|A\|_K \le \|A\|_0 \le M_2\|A\|_K$$

が成立する．さて，ここで

$$\omega_i \cdot \omega_j = \sum_l \alpha_{ijl}\omega_l \quad (\alpha_{ijl} \in \mathbb{Z})$$

とおく．$\{e_j\}$ を O_K^n，$\{e_i\}$ を O_K^m の標準基底とする．このとき，$\{\omega_t e_j\}$，$\{\omega_l e_i\}$ が，それぞれ O_K^n 及び O_K^m の $\mathbb{Z}$- 上の自由基底を与える．A によって定まる $O_K^n \to O_K^m$ の上の自由基底に関する行列表現を $\widetilde{A}$ であらわす．$\widetilde{A}$ の成分の絶対値の最大値を Q で表すと，補題 2.1.1により，$x \in O_K^n$ が存在して，$x \neq 0$，$Ax = 0$，

$$\|x\|_0 \le (ndQ)^{\frac{dr}{dn-dr}} = (ndQ)^{\frac{r}{n-r}}$$

が成立する．さて，ここで，$a_{ij} = \sum_{s=1}^d a_{ijs}\omega_s$ とおく．この時，$\|A\|_0 = \max_{i,j,s}|a_{ijs}|$ である．$A(\omega_t e_j)$ の i- 成分は，

$$a_{ij}\omega_t = (\sum_{s=1}^d a_{ijs}\omega_s)\omega_t = \sum_{s=1}^d a_{ijs}\sum_{l=1}^d \alpha_{stl}\omega_l = \sum_{l=1}^d\sum_{s=1}^d (a_{ijs}\alpha_{stl})\omega_l$$

であるので $\widetilde{A}$ の成分は $\sum_{s=1}^d (a_{ijs}\alpha_{stl})$ で表せる．よって，$Q \le d\|A\|_0\alpha$ となる．ここで $\alpha = \max_{s,t,l}|\alpha_{stl}|$ である．したがって，

$$\|x\|_0 \le (ndQ)^{\frac{r}{n-r}} \le (nd^2\alpha\|A\|_0)^{\frac{r}{n-r}}$$

となる．一方，$M_1\|x\|_K \le \|x\|_0$，$\|A\|_0 \le M_2\|A\|_K$ であるので，$C_1 = 1/M_1$，$C_2 = d^2\alpha M_2$ とおけばよい． □

2.2. 多変数多項式のＷｒｏｎｓｋｉａｎ

本節では，Roth の補題の証明の鍵となる多変数多項式の Wronskian について考える．

K を標数 0 の体とし，$K(X_1, \dots, X_m)$ を K 上の m- 変数の有理関数体とする．変数 X_i に関する $K(X_1, \dots, X_m)$ の元への偏微分 $\dfrac{\partial}{\partial X_i}$ を考えると，$f \in K(X_1, \dots, X_m)$ について，

$$f \in K \qquad \Longleftrightarrow \qquad \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_m} = 0$$

である．$\mathbb{Z}_+$ で非負の整数全体を表すことする．e_i で i- 番目が 1 で他の成分が 0 のベクトルを表すことにする．$I = (i_1, \cdots, i_m) \in \mathbb{Z}_+^m$ に対して，$|I| = i_1 + \cdots + i_m$，$I! = (i_1)! \cdots (i_m)!$とおく．さらに，微分作用素 ∂^I を

$$\partial^I = \left(\frac{\partial}{\partial X_1}\right)^{i_1} \cdots \left(\frac{\partial}{\partial X_m}\right)^{i_m}$$

で定め，正規化されたものを $\partial_I = \partial^I/I!$ とおく．特に，$\partial^{(0,\dots,0)} = \partial_{(0,\dots,0)} = 1$ とする．

補題 2.2.1. $\phi_0,\dots,\phi_r \in K(X_1,\dots,X_m)$ で，K 上一次独立とする．この時，ある $I_0,\dots,I_r \in \mathbb{Z}_+^m$ が存在して，$|I_i| \leq i\ (\forall i)$ であり，

$$\begin{vmatrix} \partial_{I_0}(\phi_0) & \cdots & \partial_{I_0}(\phi_r) \\ \vdots & \ddots & \vdots \\ \partial_{I_r}(\phi_0) & \cdots & \partial_{I_r}(\phi_r) \end{vmatrix} \neq 0$$

が成立する．

証明:

$$\begin{vmatrix} \partial_{I_0}(\phi_0) & \cdots & \partial_{I_0}(\phi_r) \\ \vdots & \ddots & \vdots \\ \partial_{I_r}(\phi_0) & \cdots & \partial_{I_r}(\phi_r) \end{vmatrix} = \frac{1}{I_0!\cdots I_r!} \begin{vmatrix} \partial^{I_0}(\phi_0) & \cdots & \partial^{I_0}(\phi_r) \\ \vdots & \ddots & \vdots \\ \partial^{I_r}(\phi_0) & \cdots & \partial^{I_r}(\phi_r) \end{vmatrix}$$

であるので，∂^I について補題を証明すればよい．r に関する帰納法で証明する．$r = 0$ の時，$\partial^{(0,\dots,0)} = 1$ であるので自明である．そこで $r \geq 1$ とし，任意の $|I_i| \leq i$ となる $I_i \in \mathbb{Z}_+^m$ に対して，

$$\begin{vmatrix} \partial^{I_0}(\phi_0) & \cdots & \partial^{I_0}(\phi_r) \\ \vdots & \ddots & \vdots \\ \partial^{I_r}(\phi_0) & \cdots & \partial^{I_r}(\phi_r) \end{vmatrix} = 0$$

と仮定する．まず帰納法の仮定により，ある $I'_0,\dots,I'_{r-1} \in \mathbb{Z}_+^m$ が存在して，$|I'_i| \leq i\ (\forall i)$ であり，

$$\begin{vmatrix} \partial^{I'_0}(\phi_0) & \cdots & \partial^{I'_0}(\phi_{r-1}) \\ \vdots & \ddots & \vdots \\ \partial^{I'_{r-1}}(\phi_0) & \cdots & \partial^{I'_{r-1}}(\phi_{r-1}) \end{vmatrix} \neq 0$$

が成立する．ここで，任意の $|I| \leq r$ となる $I \in \mathbb{Z}_+^m$ について，

$$\begin{vmatrix} \partial^{I'_0}(\phi_0) & \cdots & \partial^{I'_0}(\phi_{r-1}) & \partial^{I'_0}(\phi_r) \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \partial^{I'_{r-1}}(\phi_0) & \cdots & \partial^{I'_{r-1}}(\phi_{r-1}) & \partial^{I'_{r-1}}(\phi_r) \\ \partial^{I}(\phi_0) & \cdots & \partial^{I}(\phi_{r-1}) & \partial^{I}(\phi_r) \end{vmatrix} = 0$$

であるので，最後の行についての展開を考えると，ある $a_0,\cdots,a_r \in K(X_1,\dots,X_m)$ が存在して，

$$a_0\partial^I(\phi_0) + \cdots + a_r\partial^I(\phi_r) = 0 \tag{2.2.1.1}$$

が，任意の $|I| \leq r$ となる $I \in \mathbb{Z}_+^m$ について成立する．さらに，$a_r \neq 0$ であるので，$a_r = 1$ としてよい．特に，

$$a_0\partial^{I'_j}(\phi_0) + \cdots + a_r\partial^{I'_j}(\phi_r) = 0$$

が，任意の $0 \leq j \leq r-1$ で成立する．上式に，∂^{e_i} を作用させると，

$$\partial^{e_i}(a_0)\partial^{I'_j}(\phi_0) + \cdots + \partial^{e_i}(a_r)\partial^{I'_j}(\phi_r) + a_0\partial^{e_i}\partial^{I'_j}(\phi_0) + \cdots + a_r\partial^{e_i}\partial^{I'_j}(\phi_r) = 0$$

となり，$\partial^{e_i}\partial^{I'_j} = \partial^{e_i+I'_j}$ で，$|e_i + I'_j| \leq r$ であるので，$(2.2.1.1)$ より，

$$a_0\partial^{e_i}\partial^{I'_j}(\phi_0) + \cdots + a_r\partial^{e_i}\partial^{I'_j}(\phi_r) = 0$$

であることがわかる．よって，$a_r = 1$ ゆえ $\partial^{e_i}(a_r) = 0$ であるから

$$\partial^{e_i}(a_0)\partial^{I'_j}(\phi_0) + \cdots + \partial^{e_i}(a_{r-1})\partial^{I'_j}(\phi_{r-1}) = 0$$

となる．これは，

$$\begin{pmatrix} \partial^{I'_0}(\phi_0) & \cdots & \partial^{I'_0}(\phi_{r-1}) \\ \vdots & \ddots & \vdots \\ \partial^{I'_{r-1}}(\phi_0) & \cdots & \partial^{I'_{r-1}}(\phi_{r-1}) \end{pmatrix} \begin{pmatrix} \partial^{e_0}(a_0) & \cdots & \partial^{e_m}(a_0) \\ \vdots & \ddots & \vdots \\ \partial^{e_0}(a_{r-1}) & \cdots & \partial^{e_m}(a_{r-1}) \end{pmatrix} = 0$$

を示しており，$\partial^{e_i}(a_j) = 0$ が，任意の $1 \leq i \leq m$，$0 \leq j \leq r-1$ を導く．ゆえに，$a_0, \cdots, a_{r-1}$ は定数である．したがって，$(2.2.1.1)$ において，$I = 0$ とすれば

$$a_0\phi_1 + \cdots + a_r\phi_r = 0$$

となり，$\phi_0, \ldots, \phi_r$ の一次独立性に矛盾する． □

命題 2.2.2. $m \geq 2$ となる整数で，$G \in K[X_1, \cdots, X_m]$ であり，X_i についての次数が高々 r_i-次とする．この時，$0 \leq l \leq r_m$ となる整数 l と，$|I_i| \leq i$ となる $I_0, \cdots, I_l \in \mathbb{Z}_+^{m-1}$ が存在して，

$$F = \det\left(((\partial_{I_i+je_m})(G))_{\substack{0\leq i\leq l \\ 0\leq j\leq l}}\right)$$

とおくと，ゼロでない多項式 $U(X_1, \ldots, X_{m-1}) \in K[X_1, \ldots, X_{m-1}]$ と $V(X_m) \in K[X_m]$ が存在して，U の X_i についての次数は高々 $(l+1)r_i$ で，V の X_m についての次数は高々 $(l+1)r_m$ であり，$F = UV$ となる．ここで，$\mathbb{Z}_+^{m-1}$ の元は，自然な対応 $(x_1, \ldots, x_{m-1}) \mapsto (x_1, \ldots, x_{m-1}, 0)$ によって $\mathbb{Z}_+^m$ の元と見なし，$e_m = (0, \ldots, 0, 1) \in \mathbb{Z}_+^m$ である．

証明: G の以下の表現で，

$$G = \phi_0(X_1, \ldots, X_{m-1})\psi_0(X_m) + \cdots + \phi_l(X_1, \ldots, X_{m-1})\psi_l(X_m)$$

l が最小となるものを考える．この時，明らかに，$l \leq r_m$ で，$\{\phi_0, \ldots, \phi_l\}$ と $\{\psi_0, \ldots, \psi_l\}$ は，一次独立である．よって，補題 $2.2.1$ により，$|I_i| \leq i$ となる $I_0, \ldots, I_l \in \mathbb{Z}_+^{m-1}$ が存在

して，$U = \det\left(((\partial_{I_i})(\phi_j))_{\substack{0\le i\le l\\ 0\le j\le l}}\right)$，$V = \det\left(((\partial_{ie_m})(\psi_j))_{\substack{0\le i\le l\\ 0\le j\le l}}\right)$ とおくと，$U \neq 0$ かつ $V \neq 0$ である．さらに，

$$(\partial_{I_i+je_m})(G) = \sum_{s=0}^{l}(\partial_{I_i})(\phi_s)(\partial_{je_m})(\psi_s)$$

であるので，$F = UV$ を得る． □

2.3. 多項式の長さに関する不等式

本節では，後で必要となるいくつかの不等式を証明しよう．$I = (i_1, \dots, i_m) \in \mathbb{Z}_+^m$ に対して，$\mathbb{C}[X_1, \dots, X_m]$ の単項式 $X_1^{i_1} \cdots X_m^{i_m}$ を X^I で表すことにする．$f \in \sum_{I\in\mathbb{Z}_+^m} a_I X^I \in \mathbb{C}[X_1, \dots, X_m]$ に対して，

$$|f| = \max_{I\in\mathbb{Z}_+^m}\{|a_I|\}$$

とおく．さらに，

$$M(f) = \exp\left(\int_0^1 \cdots \int_0^1 \log(|f(\exp(2\pi\sqrt{-1}t_1), \dots, \exp(2\pi\sqrt{-1}t_m))|)dt_1 \cdots dt_m\right)$$

$$L_2(f) = \left(\sum_{I\in\mathbb{Z}_+^m} |a_I|^2\right)^{1/2}$$

とおく．以後，f の X_i についての次数を $\deg_i(f)$ で表すことにする．

命題 2.3.1. (1) $|f| \le L_2(f) \le (\deg_1(f)+1)^{1/2} \cdots (\deg_m(f)+1)^{1/2}|f|$.

(2) $M(f) \le L_2(f)$.

(3) $|f| \le 2^{\deg_1(f)+\cdots+\deg_m(f)} M(f)$.

(4) $|fg| \le (1+\min\{\deg_1(f), \deg_1(g)\}) \cdots (1+\min\{\deg_m(f), \deg_m(g)\})|f||g|$.

(5) $|f||g| \le \exp(m(\deg(f)+\deg(g)))|fg|$.

証明: (1) は自明であり，(4) は次のことより簡単に示せる．固定された $a, b, c \in \mathbb{Z}_+$ に対して，

$$\#\{(i,j) \in \mathbb{Z}_+^2 \mid i+j = c, 0 \le i \le a, 0 \le j \le b\} \le 1+\min\{a,b\}$$

である．

(1) + (2) + (3) $\Longrightarrow$ (5) を示そう．f または g が定数なら (5) は，自明である．よって，$\deg(f) \geq 1$ かつ $\deg(g) \geq 1$ としてよい．

$$\begin{aligned}
|f||g| \leq & 2^{m\deg(f)} M(f) 2^{m\deg(g)} M(g) && ((3) \text{ より}) \\
= & 2^{m(\deg(f)+\deg(g))} M(fg) && (M(fg) = M(f)M(g) \text{ ゆえ}) \\
\leq & 2^{m(\deg(f)+\deg(g))} L_2(fg) && ((2) \text{ より}) \\
\leq & \left(2^{(\deg(f)+\deg(g))}(\deg(f)+\deg(g)+1)^{1/2}\right)^m |fg| && ((1) \text{ より}) \\
\leq & \exp(m(\deg(f)+\deg(g)))|fg| && (2^d(d+1)^{1/2} \leq e^d \ (d \geq 2) \text{ ゆえ})
\end{aligned}$$

(2) を示そう．$n \in \mathbb{Z}$ に対して，

$$\int_0^1 \exp(2n\pi\sqrt{-1}t)dt = \begin{cases} 0 & \text{if } n \neq 0 \\ 1 & \text{if } n = 0 \end{cases}$$

に注意すれば，直接計算により，

$$L_2(f) = \left(\int_0^1 \cdots \int_0^1 |f(\exp(2\pi\sqrt{-1}t_1), \ldots, \exp(2\pi\sqrt{-1}t_m))|^2 dt_1 \cdots dt_m\right)^{1/2}$$

であることが確かめられる．よって，

(2.3.1.1)

$$\exp\left(\int_0^1 \cdots \int_0^1 u(t_1, \cdots, t_m)dt_1 \cdots dt_m\right) \leq \int_0^1 \cdots \int_0^1 \exp(u(t_1, \cdots, t_m))dt_1 \cdots dt_m$$

を示せばよい．というのは，(2.3.1.1) に $u = 2\log|f(\exp(2\pi\sqrt{-1}t_1), \ldots, \exp(2\pi\sqrt{-1}t_m))|$ を代入すると $M(f) \leq L_2(f)$ を得る．(2.3.1.1) についてであるが，これは指数関数の凸性を利用して得られる不等式で，例えば次のように示せる．

φ を一変数の C^2- 関数で，$\varphi'' \geq 0$ とする．この時，

$$\varphi\left(\int_0^1 \cdots \int_0^1 u(t_1, \cdots, t_m)dt_1 \cdots dt_m\right) \leq \int_0^1 \cdots \int_0^1 \varphi(u(t_1, \cdots, t_m))dt_1 \cdots dt_m$$

が成立する．というのは，$c = \int_0^1 \cdots \int_0^1 u(t_1, \cdots, t_m)dt_1 \cdots dt_m$ とおくと，二階までのテーラー展開を考えれば，

$$(x-c)\varphi'(c) \leq \varphi(x) - \varphi(c)$$

が成り立つ．よって

$$\int_0^1 \cdots \int_0^1 (u-c)\varphi'(c)dt_1 \cdots dt_m \leq \int_0^1 \cdots \int_0^1 (\varphi(u) - \varphi(c))dt_1 \cdots dt_m$$

である．ここで，

$$\int_0^1 \cdots \int_0^1 (\varphi(u) - \varphi(c))dt_1 \cdots dt_m = \int_0^1 \cdots \int_0^1 \varphi(u(t_1, \cdots, t_m))dt_1 \cdots dt_m - \varphi(c)$$

で

$$\int_0^1 \cdots \int_0^1 (u-c)\varphi'(c)dt_1 \cdots dt_m = 0$$

であるので，不等式を得る．

さて最後に (3) を考えよう．まずはじめに $m = 1$ の場合を取り扱う．$f = a_0 + a_1X + \cdots + a_dX^d$ とおく．(3) を示すためには，$a_d = 1$ と仮定してよい．f を因数分解して $f = (X - c_1)\cdots(X - c_d)$ とおく．ここで，

$$\int_0^1 \log|\exp(2\pi\sqrt{-1}t) - c|dt = \begin{cases} \log|c| & \text{もし } |c| \geq 1 \\ 0 & \text{もし } |c| < 1 \end{cases}$$

であるので (これはいわゆる Jensen の公式の一部で，例えば [**1**, Chapter 5, §3.1] を参照)，

$$M(f) = \prod_{i=1}^{d} \max\{1, |c_i|\}$$

が確かめられる．a_j は，$c_1, \ldots c_d$ の基本対称式で表されるので

$$|a_j| \leq \binom{d}{j} M(f)$$

となる．一方，$\binom{d}{j} \leq 2^d$ である．よって $m = 1$ 場合が示せた．

$m \geq 2$ とし，帰納法で示す．$d_i = \deg_i(f)$ とおく．

$$f = f_0(X_1, \ldots, X_{m-1}) + f_1(X_1, \ldots, X_{m-1})X_m + \cdots + f_{d_m}(X_1, \ldots, X_{m-1})X^{d_m}$$

とおく．まず，$m = 1$ の結果より，固定された任意の $b_1, \ldots, b_{m-1}$ に対して，

$$\log(|f_i(b_1, \ldots, b_{m-1})|) \leq d_m \log(2) + \int_0^1 \log(|f(b_1, \cdots, b_{m-1}, \exp(2\pi\sqrt{-1}t_m))|)dt_m.$$

一方，帰納法の仮定から，

$$\begin{aligned} \log(|f_i|) \leq{}& (d_1 + \cdots + d_{m-1}) \log(2) \\ &+ \int_0^1 \cdots \int_0^1 \log(|f_i(\exp(2\pi\sqrt{-1}t_1), \ldots, \exp(2\pi\sqrt{-1}t_{m-1}))|)dt_1 \cdots dt_{m-1}. \end{aligned}$$

b_i は任意であったので，$\exp(2\pi\sqrt{-1}t_i)$ を代入して，二つの不等式を比較すれば結論を得る．

□

K を代数体，$v \in M_K$ とする．$F = \sum_{I \in \mathbb{Z}_+^m} a_I X^I \in K[X_1, \ldots, X_m]$ に対して，F の v に関する長さ $|F|_v$ を

$$|F|_v = \max_{I \in \mathbb{Z}_+^m} \{|a_I|_v\}$$

で定める．

命題 2.3.2 (Gauss の補題)**.** $F, G \in K[X_1, \ldots, X_m]$ とする．v が非アルキメデス的な時, $|FG|_v = |F|_v|G|_v$ が成立する．

証明: $|\ |_v$ は，K の整数環 O_K の素イデアル P で定まる．ここで，$F=\sum_I a_I X^I$，$G=\sum_I b_I X^I$，$FG=\sum_I c_I X^I$ とおく．$|FG|_v=|F|_v|G|_v$ は，

$$\min_I\{\mathrm{ord}_P(a_I)\}+\min_I\{\mathrm{ord}_P(b_I)\}=\min_I\{\mathrm{ord}_P(c_I)\}$$

と同値である．t を $P(O_K)_P$ の生成元とし，$a=\min_I\{\mathrm{ord}_P(a_I)\}$，$b=\min_I\{\mathrm{ord}_P(b_I)\}$ とおく．さらに，$a'_I=t^{-a}a_I$，$b'_I=t^{-b}b_I$，$c'_I=t^{-a-b}c_I$，$F'=\sum_I a'_I X^I$，$G'=\sum_I b'_I X^I$，$H'=\sum_I c'_I X^I$ とおく．この時，$H'=F'G'$ である．$F',G'\in(O_K)_P[X_1,\dots,X_m]$ であるので，H' もそうである．そこで，$\{c'_I\}_I$ によって生成される $(O_K)_P$ のイデアルを J とする．$J=(O_K)_P$ を示したい．そうでないとすると，$J\subseteq P(O_K)_P$ である．F'，G' の係数を $\bmod P(O_K)_P$ で考えたものを，$\bar{F}'$，$\bar{G}'$ で書くと，$\bar{F}'\bar{G}'=0$ である．$((O_K)_P/P(O_K)_P)[X]$ は，整域であるので $\bar{F}'=0$ または $\bar{G}'=0$ を得る．これは，$\min_I\{\mathrm{ord}_P(a'_I)\}>0$ または $\min_I\{\mathrm{ord}_P(b'_I)\}>0$ を意味しており，矛盾である．よって，$J=(O_K)_P$ が示せた．つまり，$\min_I\{\mathrm{ord}_P(c'_I)\}=0$ である．よって，$\min_I\{\mathrm{ord}_P(c_I)\}=a+b$ となる． □

ここで，命題 2.3.1 の応用を二つ示しておく．$P\in\overline{\mathbb{Q}}[X_1,\dots,X_m]\setminus\{0\}$ とする．$P=\sum_{I\in\mathbb{Z}_+^m}a_I X^I$ と表すとき，P の高さを a_I から作られるベクトルの高さとして定める．つまり $h(P)=h\left((a_I)_{I\in\mathbb{Z}_+^m}\right)$.

系 2.3.3. P と Q を $\overline{\mathbb{Q}}$ 上のゼロでない m-変数多項式とする．このとき，次が成立する．

(1) d_i を X_i についての P の次数，d'_i を X_i についての Q の次数とすると

$$h(PQ)\le h(P)+h(Q)+\sum_{i=1}^m\log\left(1+\min\{d_i,d'_i\}\right)$$

である．

(2) $h(P)+h(Q)\le h(PQ)+m(\deg(P)+\deg(Q))$

証明: ある代数体 K をとって $P,Q\in K[X_1,\dots,X_m]$ としてよい．v が非アルキメデス的付値のとき，命題 2.3.2 より，$|PQ|_v=|P|_v|Q|_v$ である．v がアルキメデス的付値のときは，命題 2.3.1 の (4) と (5) より

$$|PQ|_v\le(1+\min\{d_1,d'_1\})\cdots(1+\min\{d_m,d'_m\})|P|_v|Q|_v$$

と

$$|P|_v|Q|_v\le|PQ|_v e^{m(\deg(P)+\deg(Q))}$$

が成立する．したがって，結論を得る． □

系 2.3.4. K を代数体とし，命題 2.2.2 の状況下で，

$$|F|_v \leq \begin{cases} |G|_v^{l+1} & v \text{ が非アルキメデス的な時} \\ (l+1)!\left((r_1+1)\cdots(r_m+1)\right)^l 2^{(l+1)(r_1+\cdots+r_m)}|G|_v^{l+1} & v \text{ がアルキメデス的な時} \end{cases}$$

が成立する．

証明: $I=(i_1,\ldots,i_m)$，$J=(j_1,\ldots,j_m)$ の時，

$$\partial_I(X^J) = \begin{cases} \binom{j_1}{i_1}\cdots\binom{j_m}{i_m}X^{J-I} & J \geq I \text{ の時} \\ 0 & \text{上以外} \end{cases}$$

ここで，$\binom{a}{b} \leq 2^a$ であるので，

$$|(\partial_{I_i+je_m})(G)|_v \leq \begin{cases} |G|_v & v \text{ が非アルキメデス的な時} \\ 2^{r_1+\cdots+r_m}|G|_v & v \text{ がアルキメデス的な時} \end{cases}$$

となる．ゆえに，命題 2.3.1 の (4) より行列式の展開にあらわれる各項は，v が非アルキメデス的な時 $|G|_v^{l+1}$ で，v がアルキメデス的な時 $\left((r_1+1)\cdots(r_m+1)\right)^l 2^{(l+1)(r_1+\cdots+r_m)}|G|_v^{l+1}$ でおさえられる．よって，系を得る． □

2.4. Ｒｏｔｈの補題

本節では，Roth の補題を証明する．一見しただけでは，意味のよくわからない補題であるが，使うと有用なのが不思議である．

自然数の列 $d=(d_1,\ldots,d_m)$ を固定する．$I=(i_1,\ldots,i_m)\in\mathbb{Z}_+^m$ に対して，

$$|I|_d = \frac{i_1}{d_1}+\cdots+\frac{i_m}{d_m}$$

とおく．$P\in\mathbb{C}[X_1,\ldots,X_m]$ とし，$x=(x_1,\ldots,x_m)\in\mathbb{C}^m$ とする．P の d についての x での index は，

$$\mathrm{ind}_x(P;d) = \min\{|I|_d \mid (\partial_I)(P)(x)\neq 0\}$$

と定義する．

命題 2.4.1. (1) $\mathrm{ind}_x((\partial_I)(P);d) \geq \mathrm{ind}_x(P;d) - |I|_d$.

(2) $\mathrm{ind}_x(P+Q;d) \geq \min\{\mathrm{ind}_x(P;d), \mathrm{ind}_x(Q;d)\}$

(3) $\mathrm{ind}_x(PQ;d) = \mathrm{ind}_x(P;d) + \mathrm{ind}_x(Q;d)$.

証明: (1) と (2) は，定義に従えばただちに得る．(3) を見るために $x=(0,\ldots,0)$ としてよい．この時，もし $P=\sum_I a_I X^I$ とおけば，

$$\mathrm{ind}_x(P;d) = \min\{|I|_d \mid a_I\neq 0\}$$

とある．したがって，(3) は簡単にチェックできる． □

定理 2.4.2 (Roth の補題)**.** P は，ゼロでない $\overline{\mathbb{Q}}$ 上の m-変数の多項式で，X_i についての次数が高々 d_i-次であるとし，$d=(d_1,\dots,d_m)$ とおく．$a=(a_1,\dots,a_m)\in\overline{\mathbb{Q}}^m$ とし，正の数 ϵ が次の二つを満たすとする．

(1) $d_{i+1}\le\epsilon^{2^{m-1}}d_i \quad (i=1,\dots m-1)$． (ただし, $m=1$ の場合，この条件は不要．)

(2) $h(P)+2md_1\le\epsilon^{2^{m-1}}\min_{1\le i\le m}\{d_ih^+(a_i)\}$．

この時，$\mathrm{ind}_a(P;d)\le 2m\epsilon$ が成立する．$m=1$ の時は，さらによい評価 $\mathrm{ind}_a(P;d)\le\epsilon$ が成立する．

証明: もし $P(a)\neq 0$ なら，$\mathrm{ind}_a(P;d)=0$ であるので，$P(a)=0$ と仮定してよい．まず始めに，$m=1$ の場合を考えよう．$P=(X_1-a_1)^{i_1}Q(X)$，$Q(a)\neq 0$ とおく．系 2.3.3 より，$i_1h(X-a_1)+h(Q)\le h(P)+\deg(P)$ であるので，$i_1h^+(a_1)\le h(P)+\deg(P)$ を得る．仮定 $h(P)+2d_1\le\epsilon d_1h^+(a_1)$ を用いて，$h^+(a_1)>0$ で，

$$i_1h^+(a_1)\le\epsilon d_1h^+(a_1)-d_1\le\epsilon d_1h^+(a_1)$$

を得る．よって，$\mathrm{ind}_a(P;d)\le\epsilon$ である．

さて，$m>1$ とする．$\mathrm{ind}_a(P;d)\le m$ であるので，$\epsilon\le 1/2$ としてよい．さらに，m に関する帰納法で証明するので，$d_m\ge 1$ としてよい．命題 2.2.2 により，$0\le l\le d_m$ となる整数 l と，$|I_i|\le i$ となる $I_0,\cdots,I_l\in\mathbb{Z}_+^{m-1}$ が存在して，

$$F=\det\left(((\partial_{I_i+je_m})(P))_{\substack{0\le i\le l\\ 0\le j\le l}}\right)$$

とおくと，ゼロでない多項式 $U(X_1,\dots,X_{m-1})\in\overline{\mathbb{Q}}[X_1,\dots,X_{m-1}]$ と $V(X_m)\in\overline{\mathbb{Q}}[X_m]$ が存在して，U の X_i についての次数は高々 $(l+1)d_i$ で，V の X_m についての次数は高々 $(l+1)d_m$ であり，$F=UV$ となる．

$\mathrm{ind}_a(P;d)$ を評価しよう．命題 2.4.1 の (1) を用いて，$I_i=(e_{1,i},\dots,e_{m-1,i})$ とおくと，

$$\begin{aligned}\mathrm{ind}_a((\partial_{I_i+je_m})(P);d)&\ge\mathrm{ind}_a(P;d)-\left(\frac{e_{1,i}}{d_1}+\cdots+\frac{e_{m-1,i}}{d_{m-1}}+\frac{j}{d_m}\right)\\&\ge\mathrm{ind}_a(P;d)-\frac{e_{1,i}+\cdots+e_{m-1,i}}{d_{m-1}}-\frac{j}{d_m}\\&\ge\mathrm{ind}_a(P;d)-\frac{l}{d_{m-1}}-\frac{j}{d_m}\\&\ge\mathrm{ind}_a(P;d)-\frac{d_m}{d_{m-1}}-\frac{j}{d_m}\end{aligned}$$

となる．ここで，$\mathrm{ind}_a((\partial_{I_i+je_m})(P);d) \geq 0$ であることに注意すれば，

$$\mathrm{ind}_a((\partial_{I_i+je_m})(P);d) \geq \max\left\{\mathrm{ind}_a(P;d) - \frac{j}{d_m}, 0\right\} - \frac{d_m}{d_{m-1}}$$

が成立する．よって，命題 2.4.1 の (2) と (3) を用いて，

$$\mathrm{ind}_a(F;d) \geq \sum_{j=0}^{l}\left(\max\left\{\mathrm{ind}_a(P;d) - \frac{j}{d_m}, 0\right\}\right) - (l+1)\frac{d_m}{d_{m-1}}$$

となる．さて，ここで，

$$\sum_{j=0}^{l}\left(\max\left\{\mathrm{ind}_a(P;d) - \frac{j}{d_m}, 0\right\}\right) \geq (l+1)\min\left\{\frac{\mathrm{ind}_a(P;d)}{2}, \frac{\mathrm{ind}_a(P;d)^2}{4}\right\} \tag{2.4.2.1}$$

を見よう．まず，$\mathrm{ind}_a(P;d) \geq l/d_m$ の場合を考えよう．この時，

$$\begin{aligned}\sum_{j=0}^{l}\left(\max\left\{\mathrm{ind}_a(P;d) - \frac{j}{d_m}, 0\right\}\right) &= (l+1)\,\mathrm{ind}_a(P;d) - \frac{l(l+1)}{2d_m}\\ &\geq (l+1)\,\mathrm{ind}_a(P;d) - \frac{(l+1)\,\mathrm{ind}_a(P;d)}{2}\\ &= (l+1)\frac{\mathrm{ind}_a(P;d)}{2}\end{aligned}$$

となる．そこで，$\mathrm{ind}_a(P;d) < l/d_m$ とし，$s/d_m \leq \mathrm{ind}_a(P;d) < (s+1)/d_m$ となる整数 $0 \leq s \leq l-1$ を固定する．この時，前と同様にして，

$$\sum_{j=0}^{l}\left(\max\left\{\mathrm{ind}_a(P;d) - \frac{j}{d_m}, 0\right\}\right) \geq (s+1)\frac{\mathrm{ind}_a(P;d)}{2}$$

である．さらに，$s+1 > d_m\,\mathrm{ind}_a(P;d)$ であることと $d_m/(d_m+1) \geq 1/2$ (というのは，$d_m \geq 1$ であるので) であることに注意すれば，

$$\begin{aligned}\sum_{j=0}^{l}\left(\max\left\{\mathrm{ind}_a(P;d) - \frac{j}{d_m}, 0\right\}\right) &\geq \frac{d_m}{2}\,\mathrm{ind}_a(P;d)^2\\ &= (d_m+1)\frac{d_m}{2(d_m+1)}\,\mathrm{ind}_a(P;d)^2\\ &\geq (l+1)\frac{d_m}{2(d_m+1)}\,\mathrm{ind}_a(P;d)^2\\ &\geq (l+1)\frac{\mathrm{ind}_a(P;d)^2}{4}\end{aligned}$$

を得る．よって (2.4.2.1) が示せた．

したがって，(2.4.2.1) と $\mathrm{ind}_a(F;d) = \mathrm{ind}_a(U;d) + \mathrm{ind}_a(V;d)$ と $d_m/d_{m-1} \leq \epsilon^{2^{m-1}}$ により，

$$\min\left\{\frac{\mathrm{ind}_a(P;d)}{2}, \frac{\mathrm{ind}_a(P;d)^2}{4}\right\} \leq \frac{1}{l+1}\,\mathrm{ind}_a(U;d) + \frac{1}{l+1}\,\mathrm{ind}_a(V;d) + \epsilon^{2^{m-1}} \tag{2.4.2.2}$$

を得る．そこで，帰納法の仮定を使って，$\mathrm{ind}_a(U;d)$ と $\mathrm{ind}_a(V;d)$ の上限を求め，$\mathrm{ind}_a(P;d)$ の上限を求めようというのがアイデアである．帰納法を進めるために次の不等式を証明する必要がある．

$$h(U)+h(V)\le (l+1)(h(P)+2d_1) \tag{2.4.2.3}$$

系 2.3.4 より，

$$h(F)\le (l+1)h(P)+(l+1)(d_1+\cdots+d_m)\log(2) \\ +l\log((d_1+1)\cdots(d_m+1))+\log((l+1)!)$$

である．ここで，$1+a\le 2^a\ (a\ge 0)$ かつ $\log((l+1)!)\le (l+1)\log(l+1)\le (l+1)l$ であるので，上の不等式は，

$$h(F)\le (l+1)(h(P)+2(d_1+\cdots+d_m)\log(2)+l)$$

を導く．ここで，$a_m=\epsilon^{2^{m-1}}$ とおくと，$d_i\le a_m^{i-1}d_1$ であるから，

$$h(F)\le (l+1)\left(h(P)+\left(2(1+a_m+\cdots+a_m^{m-1})\log(2)+a_m^{m-1}\right)d_1\right)$$

を得る．よって，

$$2(1+a_m+\cdots+a_m^{m-1})\log(2)+a_m^{m-1}\le 2$$

を示せばよい．というのは，U と V は，共通の変数を含まないので，

$$h(F)=h(U)+h(V)$$

が成り立つからである．まず $m=2$ の場合，$a_2\le 1/4$ であるので，

$$2(1+a_2)\log(2)+a_2\le 2(1+1/4)\log(2)+1/4<2$$

である．$m\ge 3$ の場合，$a_m\le 1/16$ であるので，

$$\begin{aligned}2(1+a_m+\cdots+a_m^{m-1})\log(2)+a_m^{m-1}\le&2(1+1/16+\cdots+(1/16)^{m-1})\log(2)+(1/16)^{m-1}\\ \le&\frac{2}{1-1/16}\log(2)+1/16<2\end{aligned}$$

となり，(2.4.2.3) が示せた．

(2.4.2.3) より，

$$h(U)\le (l+1)(h(P)+2d_1)\quad と\quad h(V)\le (l+1)(h(P)+2d_1)$$

を得る．よって，

$$\begin{aligned} h(U)+2(m-1)(l+1)d_1 &\leq (l+1)(h(P)+2md_1) \\ &\leq \epsilon^{2^{m-1}} \min_{1\leq i\leq m}\{(l+1)d_i h^+(a_i)\} \\ &\leq \epsilon^{2^{m-1}} \min_{1\leq i\leq m-1}\{(l+1)d_i h^+(a_i)\} \end{aligned}$$

及び

$$\begin{aligned} h(V)+2(l+1)d_m &\leq h(V)+2(l+1)(m-1)d_1 \\ &\leq (l+1)(h(P)+2md_1) \\ &\leq \epsilon^{2^{m-1}} \min_{1\leq i\leq m}\{(l+1)d_i h^+(a_i)\} \\ &\leq \epsilon^{2^{m-1}} (l+1)d_m h^+(a_m) \end{aligned}$$

が示せる．したがって，U に対して $\epsilon(U)=\epsilon^2$，V に対して $\epsilon(V)=\epsilon^{2^{m-1}}$ を用いて，帰納法の仮定より，

$$\mathrm{ind}_a(U;((l+1)d_1,\ldots,(l+1)d_{m-1}))\leq 2(m-1)\epsilon^2 \quad \text{と} \quad \mathrm{ind}_a(V;(l+1)d_m)\leq \epsilon^{2^{m-1}}$$

が得られる．($m=1$ の場合は，良い評価があることに注意する.) つまり，

$$\mathrm{ind}_a(U;d)\leq 2(l+1)(m-1)\epsilon^2 \quad \text{と} \quad \mathrm{ind}_a(V;d)\leq (l+1)\epsilon^{2^{m-1}}$$

が成り立つ．よって，(2.4.2.2) により，

$$\min\left\{\frac{\mathrm{ind}_a(P;d)}{2}, \frac{\mathrm{ind}_a(P;d)^2}{4}\right\} \leq 2(m-1)\epsilon^2+\epsilon^{2^{m-1}}+\epsilon^{2^{m-1}}\leq 2m\epsilon^2$$

となる．ここで，場合分けをする．

$\mathrm{ind}_a(P;d)\geq 2$ の場合，$\mathrm{ind}_a(P;d)/2\leq \mathrm{ind}_a(P;d)^2/4$ である．したがって，$\mathrm{ind}_a(P;d)/2\leq 2m\epsilon^2$，つまり，

$$\mathrm{ind}_a(P;d)\leq 4m\epsilon^2=(2\epsilon)2m\epsilon<2m\epsilon$$

である．ここで，$\epsilon<1/2$ を用いている．

$\mathrm{ind}_a(P;d)<2$ の場合，$\mathrm{ind}_a(P;d)^2/4\leq 2m\epsilon^2$，つまり，$\mathrm{ind}_a(P;d)\leq 2\sqrt{2m}\epsilon$ である．ここで，$m\geq 2$ であるので，$\sqrt{2m}\leq m$ である．したがって，$\mathrm{ind}_a(P;d)\leq 2m\epsilon$ を得る．

よって，定理の証明が完成した． □

2.5. ノルムの高さ

本節では，ノルムの高さの評価をする．少し複雑であるが，本質的には単純な計算の繰り返しだけである．まず最初にノルムの定義の復習から始めよう．

F を体，F' を F の有限次代数拡大体とし，F' の F 上の基底 $\{\omega_1, \ldots, \omega_n\}$ を固定する．$x \in F'$ に対して，$x\omega_i = \sum a_{ij}\omega_j$ によって，F を成分とする行列 $A = (a_{ij})$ が定まる．A は x をかけることによって得られる F 上の準同型 $F' \to F'$ の行列表現である．この時，$\mathrm{Norm}_{F'/F}(x)$ は $\det(A)$ で定義される．$\mathrm{Norm}_{F'/F}(x)$ には別の定義がある．$\overline{F}$ を F の代数閉包とし，$\{\sigma_1, \ldots, \sigma_n\}$ を F' の F を固定する $\overline{F}$ への埋め込み全体とする．この時，$\mathrm{Norm}_{F'/F}(x)$ は，$\sigma_1(x)\cdots\sigma_n(x)$ に等しい．さらに，F が正規環 A の商体の時，B を A の F' での正規化とすると，任意の $b \in B$ について，$\mathrm{Norm}_{F'/F}(b) \in A$ である．まず始めに次の補題を考えよう．

補題 2.5.1. K を代数体，$K[X,Y,Z]$ を 3- 変数の多項式環とし，N- 次の同次多項式

$$Z^N + a_{N-1}(X,Y)Z^{N-1} + \cdots + a_0(X,Y)$$

による剰余環

$$K[X,Y,Z]/(Z^N + a_{N-1}(X,Y)Z^{N-1} + \cdots + a_0(X,Y))$$

を考える．ここで，$a_i(X,Y)$ は，$K[X,Y]$ の $(N-i)$- 次の同次多項式である．X,Y,Z の剰余環における像を x,y,z とおく．$K[x,y,z]$ は，$\{1, z, \ldots, z^{N-1}\}$ を基底とする $K[x,y]$- 自由加群であり，$K[x,y]$ は x,y を不定元とする多項式環であるので，任意の l に対して，ある $\beta_{l,i}(X,Y) \in K[X,Y]$ が一意的に存在して，

$$z^l = \sum_{0 \le i < N} \beta_{l,i}(x,y)z^i$$

と書ける．この時，以下が成立する．

(1) $\beta_{l,i}(X,Y)$ は，高々 $(l-i)$- 次の同次多項式である．さらに，もし $a_i \in O_K[X,Y]$ なら，$\beta_{l,i}(X,Y) \in O_K[X,Y]$ である．
(2) 各 $v \in M_K$ に対して，a_i のみに依存する定数 C_v が存在して，任意の l,i について，

$$|\beta_{l,i}|_v \le \exp(C_v l)$$

が成立する．しかも，有限個の v をのぞいて，$C_v = 0$ である．

証明: まず

$$\begin{aligned} z^{l+1} &= z\sum_{i=0}^{N-1}\beta_{l,i}z^i \\ &= \beta_{l,N-1}z^N + \sum_{i=1}^{N-1}\beta_{l,i-1}z^i \\ &= -\beta_{l,N-1}\sum_{i=0}^{N-1}a_iz^i + \sum_{i=1}^{N-1}\beta_{l,i-1}z^i \\ &= \sum_{i=1}^{N-1}(-\beta_{l,N-1}a_i + \beta_{l,i-1})z^i - \beta_{l,N-1}a_0 \end{aligned}$$

であるので，

$$\begin{cases} \beta_{l+1,i} = -\beta_{l,N-1}a_i + \beta_{l,i-1} & (1 \le i \le N-1) \\ \beta_{l+1,0} = -\beta_{l,N-1}a_0 \end{cases}$$

がわかる．これから，ただちに (1) が帰納的にわかる．

さて，ここで，$v \in M_K$ に対して，

$$H_v = \max\{1, |a_0|_v, \ldots, |a_{N-1}|_v\}$$

とおく．このとき，有限個の v を除いて，$H_v = 1$ である．さらに，

$$C_v = \begin{cases} \log(H_v) & v \text{ が非アルキメデス的な時} \\ \log((1+N)^2H_v + 1) & v \text{ がアルキメデス的な時} \end{cases}$$

とおく．有限個の v を除いて，$C_v = 0$ である．$|\beta_{l,i}|$ の不等式を l についての帰納法で示す．

$0 \le l \le N$ の場合は自明である．そこで $l > N$ とする．まず，v が非アルキメデス的な時を考える．$i > 0$ の時，

$$\begin{aligned} |\beta_{l+1,i}|_v &\le \max\{|\beta_{l,N-1}a_i|_v, |\beta_{l,i-1}|_v\} \\ &= \max\{|\beta_{l,N-1}|_v|a_i|_v, |\beta_{l,i-1}|_v\} \\ &\le \max\{\exp(C_vl)H_v, \exp(C_vl)\} \\ &= \exp(C_vl)H_v = \exp(C_v(l+1)) \end{aligned}$$

となり示せた．$i = 0$ の場合も同様である．

次に，v がアルキメデス的な時を考える．$i>0$ の時，命題 2.3.1 の (4) を用いて

$$\begin{aligned}|\beta_{l+1,i}|_v &\le |\beta_{l,N-1}a_i|_v + |\beta_{l,i-1}|_v\\ &\le (N+1)^2|\beta_{l,N-1}|_v|a_i|_v + |\beta_{l,i-1}|_v\\ &\le (N+1)^2\exp(C_v l)H_v + \exp(C_v l)\\ &= ((N+1)^2H_v+1)\exp(C_v l) = \exp(C_v)\exp(C_v l) = \exp(C_v(l+1))\end{aligned}$$

となり示せた．$i=0$ の場合も同様であるので，補題が示せた． □

命題 2.5.2. K を代数体，$K[X,Y,Z,X',Y',Z']$ を 6-変数の K 上の多項式環とする．S,T,U についての N-次の K 上の同次多項式

$$P(S,T,U) = U^N + a_{N-1}(S,T)U^{N-1} + \cdots + a_0(S,T)$$

による剰余環

$$K[X,Y,Z,X',Y',Z']/(P(X,Y,Z),P(X',Y',Z'))$$

を考える．ここで，X,Y,Z,X',Y',Z' の像を x,y,z,x',y',z' とおく．$K[x,y,z,x',y',z']$ は，$\{z^iz'^{i'}\}_{\substack{0\le i<N\\ 0\le i'<N}}$ を基底とする $K[x,y,x',y']$-自由加群である．この時，以下が成立する．

(1) $F\in K[X,Y,Z,X',Y',Z']$ を両次数が (d,d') の同次多項式とする．$F_{ii'}(X,Y,X',Y')\in K[X,Y,X',Y']$ が一意的に存在して，

$$F(x,y,z,x',y',z') = \sum_{\substack{0\le i<N\\ 0\le i'<N}} F_{ii'}(x,y,x',y')z^iz'^{i'}$$

とおける．この時，$F_{ii'}$ は，高々両次数が $(d-i,d'-i')$ の同次多項式であり，もし a_i，F の係数が O_K の元なら，F_{ii} の係数も O_K の元である．さらに，各 $v\in M_K$ に対して，次を満たす a_i のみによる定数 C_v が存在する．

$$|F_{ii'}|_v \le |F|_v\exp(C_v(d+d'))$$

であり，有限個の v を除いて $C_v=0$ である．

(2) $\mathrm{Norm}: K[x,y,z,x',y',z']\to K[x,y,x',z']$ を考える．$F\in K[X,Y,Z,X',Y',Z']$ を両次数が (d,d') の同次多項式とする．各 $v\in M_K$ に対して，次を満たす a_i のみによる定数 C'_v が存在する．

$$|\mathrm{Norm}(F(x,y,z,x',y',z'))|_v \le |F|_v^{N^2}\exp(C'_vN^2(d+d'+2N))$$

であり，有限個の v を除いて $C'_v=0$ である．

証明: (1) まず，$F = Z^l Z'^{l'}$ の時を，考える．補題 2.5.1 より任意の l, l' に対して，ある $\beta_{l,i}(X,Y) \in K[X,Y]$ と $\beta'_{l',i'}(X',Y') \in K[X',Y']$ が一意的に存在して，

$$z^l = \sum_{0 \le i < N} \beta_{l,i}(x,y) z^i, \qquad z'^{l'} = \sum_{0 \le i < N} \beta'_{l',i'}(x',y') z'^{i'}$$

と書け，$\beta_{l,i}$ は高々 $(l-i)$- 次の同次多項式で，$\beta'_{l',i'}$ は高々 $(l'-i')$- 次の同次多項式である．さらに，任意の付値 v に対して，次を満たす定数 C_v が存在する．任意の l, i, l', i' について，$|\beta_{l,i}|_v \le \exp(C_v l)$，$|\beta'_{l',i'}|_v \le \exp(C_v l')$ であり，有限個の付値 v をのぞいて，$C_v = 0$ である．一方，

$$z^l z'^{l'} = (\sum_{0 \le i < N} \beta_{l,i}(x,y) z^i)(\sum_{0 \le i < N} \beta'_{l',i'}(x',y') z'^{i'}) = \sum_{\substack{0 \le i < N \\ 0 \le i' < N}} \beta_{l,i}(x,y)\beta'_{l',i'}(x',y') z^i z'^{i'}$$

であるので，

$$z^l z'^{l'} = \sum_{\substack{0 \le i < N \\ 0 \le i' < N}} \beta_{l,l',i,i'}(x,y,x',y') z^i z'^{i'}$$

で定まる $\beta_{l,l',i,i'}(X,Y,X',Y') \in K[X,Y,X',Y']$ を考えると，$\beta_{l,l',i,i'} = \beta_{l,i}\beta'_{l',i'}$ である．よって，$\beta_{l,i}$ と $\beta'_{l',i'}$ が共通の変数を含まないことに注意すれば，$F = Z^l Z'^{l}$ の場合を得る．

次に一般の場合を考えよう．

$$F \quad = \sum_{l,l'} G_{l,l'}(X,Y,X',Y') Z^l Z'^{l'}$$

とおくと，前の結果より，

$$\begin{aligned} F(x,y,z,x',y',z') &= \sum_{l,l'} G_{l,l'}(x,y,x',y') z^l z'^{l'} \\ &= \sum_{l,l'} G_{l,l'}(x,y,x',y') \sum_{\substack{0 \le i < N \\ 0 \le i' < N}} \beta_{l,l',i,i'}(x,y,x',y') z^i z'^{i'} \\ &= \sum_{\substack{0 \le i < N \\ 0 \le i' < N}} \left(\sum_{l,l'} G_{l,l'}(x,y,x',y') \beta_{l,l',i,i'}(x,y,x',y') \right) z^i z'^{i'} \end{aligned}$$

であるので，

$$F_{ii'}(X,Y,X',Y') = \sum_{l,l'} G_{l,l'}(X,Y,X',Y') \beta_{l,l',i,i'}(X,Y,X',Y')$$

である．この時，$G_{l,l'}$ は両次数が高々 $(d-l, d'-l')$ の同次多項式で，$\beta_{l,l',i,i'}$ は両次数が高々 $(l-i, l'-i')$ の同次多項式であるので，$F_{ii'}(X,X')$ は両次数が高々 $(d-i, d'-i')$ の同次多項式である．

次に各付値 v に関しての $F_{ii'}$ の長さの評価をしよう．まず，v が非アルキメデス的な時を考える．この時，

$$\begin{aligned}|F_{ii'}|_v &= \max\{|G_{l,l'}\beta_{l,l',i,i'}|_v\}\\ &= \max\{|G_{l,l'}|_v|\beta_{l,l',i,i'}|_v\}\\ &\leq |F|_v \exp(C_v(d+d'))\end{aligned}$$

となり題意が示せた．

v がアルキメデス的な時，

$$\begin{aligned}|F_{ii'}|_v &= \sum_{l,l'} |G_{l,l'}\beta_{l,l',i,i'}|_v\\ &= \sum_{l,l'} (1+d)^2(1+d')^2|G_{l,l'}|_v|\beta_{l,l',i,i'}|_v\\ &\leq \sum_{l,l'} (1+d)^2(1+d')^2|F|_v \exp(C_v(d+d'))\\ &\leq (1+d)^3(1+d')^3|F|_v \exp(C_v(d+d'))\\ &\leq \exp(3d)\exp(3d')|F|_v \exp(C_v(d+d')) = |F|_v \exp((C_v+3)(d+d'))\end{aligned}$$

となり，v がアルキメデス的な時は，C_v を C_v+3 とすれば，結論を得る．

(2) $0 \leq i < N$，$0 \leq i' < N$ に対して，$F^{ii'} = Z^i Z'^{i'} F$ とおく．さらに，

$$F^{ii'}(x,y,z,x',y',z') = \sum_{\substack{0\leq j<N\\ 0\leq j'<N}} F^{ii'}_{jj'}(x,y,x',y')z^j z'^{j'}$$

とおくと，(1) より，$F^{ii'}_{jj'}$ は，高々両次数が $(d+N, d'+N)$ の同次多項式であり，

$$|F^{ii'}_{jj'}|_v \leq |F|_v \exp(C_v(d+d'+2N))$$

が成立する．ここで，$F(x,y,z,x',y',z')$ をかけることで得られる準同型の基底 $\{z^i z'^{i'}\}_{\substack{0\leq i<N\\ 0\leq i'<N}}$ に関する行列表現を A_F とする．この時，$\mathrm{Norm}(F) = \det(A_F)$ であり，A_F の要素は $F^{ii'}_{jj'}$ からなる．そこでそれらの N^2 個の積のひとつを G で表すと，

$$|G|_v \leq \begin{cases} |F|_v^{N^2} \exp(C_v N^2(d+d'+2N)) & v \text{ が非アルキメデス的な時}\\ |F|_v^{N^2} \exp((C_v+2)N^2(d+d'+2N)) & v \text{ がアルキメデス的な時}\end{cases}$$

を得る．ここで，不等式

$$(1+d+N)^{2N^2}(1+d'+N)^{2N^2} \leq \exp(2N^2(d+N))\exp(2N^2(d'+N))$$

を用いた．ゆえに，

$$|\mathrm{Norm}(F)|_v \leq \begin{cases} |F|_v^{N^2} \exp(C_v N^2(d+d'+2N)) & v \text{ が非アルキメデス的な時}\\ |F|_v^{N^2} \exp((C_v+2)N^2(d+d'+2N))(N!)^2 & v \text{ がアルキメデス的な時}\end{cases}$$

ここで，

$$(N^2)! \leq \exp(N^2 \log(N^2)) \leq \exp(2N^3) \leq \exp(N^2(d+d'+2N))$$

であるので，v がアルキメデス的な時，

$$|\operatorname{Norm}(F)|_v \leq |F|_v^{N^2} \exp((C_v+3)N^2(d+d'+2N))$$

となり，結論が導かれる． □

さて，最後に後で必要となる結果を考えよう．まず，状況を設定する．K を代数体，$\mathbb{P}^n$ を K- 上の n- 次元射影空間，C を $\mathbb{P}^n$ の次数が N の部分多様体で絶対既約な非特異射影曲線であるとする．今，$\mathbb{P}^n$ の座標 $(X_0, X_1, \ldots, X_n)$ を，C と部分線形空間 $\{X_0 = X_1\}$ と交わらず，$(X_0 : \ldots : X_n) \mapsto (X_0 : X_1 : X_2)$ によって定まる射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^2$ による C の像と C は双有理的であるとする．射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^2$ による C の像を C' で表す．このとき，$\deg(C') = N$ である．C と部分線形空間 $\{X_0 = X_1\}$ と交わらないことにより C' は，$(0:0:1)$ を通らない．したがって，C' は，次の形の

$$X_2^N + a_{N-1}(X_0, X_1)X_2^{N-1} + \cdots + a_1(X_0, X_1)X_2 + a_0(X_0, X_1)$$

N- 次同次多項式で定義される．さて，$(X_0 : \ldots : X_n) \mapsto (X_0 : X_1)$ によって定まる射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^1$ が導く射 $C \to \mathbb{P}^1$ を f で表し，$f \times f : C \times C \to \mathbb{P}^1 \times \mathbb{P}^1$ を π で表す．さらに，$p_i : C \times C \to C$，$q_i : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ を i- 番目の成分への射影とする．また，$X_i|_C$，$X_i'|_C$ を x_i，x_i' で表すことにする．この時，両次数が (d, d') の同時多項式 $F \in K[X_0, \cdots, X_n, X_0', \cdots, X_n']$ に対して，$F(x_0, \cdots, x_n, x_0', \cdots, x_n')$ は $H^0(C \times C, \mathcal{O}_{C\times C}(d, d'))$ の元を表す．以上の準備で，次が成立する．

命題 2.5.3. $F \in K[X_0, \cdots, X_n, X_0', \cdots, X_n']$ を両次数が (d, d') の同時多項式とする．この時，$\operatorname{Norm}_\pi(F(x_0, \cdots, x_n, x_0', \cdots, x_n'))$ は，両次数が (N^2d, N^2d') の $K[x_0, x_1, x_0', x_1']$ の同次多項式であり，C と a_i のみによる定数 M_1 と M_2 が存在して

$$h(\operatorname{Norm}_\pi(F(x_0, \ldots, x_n, x_0', \ldots, x_n'))) \leq N^2(h(F) + M_1(d+d') + M_2)$$

が成立する．

証明: $\operatorname{Norm}_\pi(F)$ の両次数を計算するために次の射影公式に注意する．詳しくは，[**11**, Lecture10, Lecture 16] を参照のこと．

> $f : X \to Y$ を非特異射影曲面の間の有限射とする．D を X 上の因子とする．いま，$\{Y_i\}$ を Y のアファイン被覆とする．この時，$X_i = f^{-1}(Y_i)$ もアファインである．d_i を D の X_i での定義方程式とする．$\operatorname{Norm}_f(d_i)$ で定まる Y 上の因子を $f_*(D)$ で書くことにすると，次の射影公式が成立する．E が Y 上の因子の時，
>
> $$(D \cdot f^*(E)) = (f_*(D) \cdot E)$$
>
> である．

$F(x,x')=0$ で定まる因子を D とする．$\pi_*(D)$ の第 1 成分についての次数を計算するには，$(\pi_*(D)\cdot q_2^*(\mathcal{O}_{\mathbb{P}^1}(1)))$ を求めればよい．射影公式によって，

$$(\pi_*(D)\cdot q_2^*(\mathcal{O}_{\mathbb{P}^1}(1)))=(D\cdot\pi^*(q_2^*(\mathcal{O}_{\mathbb{P}^1}(1))))$$

である．一方，$\pi^*(q_2^*(\mathcal{O}_{\mathbb{P}^1}(1)))=p_2^*(\mathcal{O}_C(1))$ で，D は $dp_1^*(\mathcal{O}_C(1))+d'p_2^*(\mathcal{O}_C(1))$ と線形同値である．よって，

$$(\pi_*(D)\cdot q_1^*(\mathcal{O}_{\mathbb{P}^1}(1)))=N^2d$$

である．第 2 成分についての次数を計算も同様であるので，$\mathrm{Norm}_\pi(F(x,x'))$ は，両次数が (N^2d,N^2d') の同次多項式である．

C と C' は双有理であるので，$K[x_1/x_0,\cdots,x_n/x_0]/K[x_1/x_0,x_2/x_0]$ の $K[x_1/x_0]$- 加群としての台は有限個の点である．あるゼロでない多項式 $b(S)\in K[S]$ が存在して，

$$b(x_1/x_0)K[x_1/x_0,\cdots,x_n/x_0]\subseteq K[x_1/x_0,x_2/x_0]$$

となる．特に，$i\geq 3$ に対して，$b(x_1/x_0)(x_i/x_0)\in K[x_1/x_0,x_2/x_0]$ となる．ゆえに，適当に同次化して，あるゼロでない同次多項式 $\beta(X_0,X_1)\in K[X_0,X_1]$ が存在して，$\beta(x_0,x_1)x_i\in K[x_0,x_1,x_2]$ となる．つまり，$i\geq 3$ に対して，同次多項式 $G_i(X_0,X_1,X_2)$ が存在して，

$$\beta(x_0,x_1)x_i=G_i(x_0,x_1,x_2)$$

と表せる．同様に，$\beta(x_0',x_1')x_i'=G_i(x_0',x_1',x_2')$ である．さて，

$$F=\sum F_{i_3,\dots,i_n,i_3',\dots,i_n'}(X_0,X_1,X_2,X_0',X_1',X_2')X_3^{i_3}\cdots X_n^{i_n}{X_3'}^{i_3'}\cdots {X_n'}^{i_n'}$$

とおく．このとき，

$$\beta(X)^d\beta(X')^{d'}F=\sum\beta(X)^{d-(i_3+\cdots+i_n)}\beta(X')^{d'-(i_3'+\cdots+i_n')}F_{i_3,\dots,i_n,i_3',\dots,i_n'}\times$$
$$(\beta(X)X_3)^{i_3}\cdots(\beta(X)X_n)^{i_n}(\beta(X')X_3')^{i_3'}\cdots(\beta(X')_n)^{i_n'}$$

となる．さて，ここで，

$$T=\sum\beta(X)^{d-(i_3+\cdots+i_n)}\beta(X')^{d'-(i_3'+\cdots+i_n')}F_{i_3,\dots,i_n,i_3',\dots,i_n'}\times$$
$$G_3(X)^{i_3}\cdots G_n(X)^{i_n}G_3(X')^{i_3'}\cdots G_n(X')^{i_n'}$$

の各付値 v における $|T|_v$ を評価しよう．

$$A_v=\max\{|\beta|_v,|G_3|_v,\dots,|G_n|\},\qquad s=\max\{\deg(\beta),\deg(G_3),\dots,\deg(G_n)\}$$

とおく．v が非アルキメデス的のとき，

$$|T|_v\leq A_v^{d+d'-(i_3+\cdots+i_n+i_3'+\cdots+i_n')}|F|_vA_v^{i_3}\cdots A_v^{i_n}\cdot A_v^{i_3'}\cdots A_v^{i_n'}=A_v^{d+d'}|F|_v$$

である．v がアルキメデス的のときは，まず

$$|\beta(X)^{d-(i_3+\cdots+i_n)}\beta(X')^{d'-(i'_3+\cdots+i'_n)}F_{i_3,\ldots,i_n,i'_3,\ldots,i'_n}G_3(X)^{i_3}\cdots G_n(X)^{i_n}G_3(X')^{i'_3}\cdots G_n(X')^{i'_n}|_v$$

は，$(1+d)^3(1+d')^3(1+s)^{3(d+d')}A_v^{d+d'}|F|_v$ でおさえられる．ゆえに，

$$|T|_v \le (1+d)^n(1+d')^n(1+s)^{3(d+d')}A_v^{d+d'}|F|_v$$

である．よって，v がアルキメデス的のとき，A_v を $\left(\max\{2^n,(1+s)^3,A_v\}\right)^3$ で置き換えると，

$$|T|_v \le A_v^{d+d'}|F|_v$$

が成立する．

命題 2.5.2 より各付値 v に対して，次を満たす a_i のみによる定数 C'_v が存在して，

$$|\operatorname{Norm}(T(x_0,x_1,x_2,x'_0,x'_1,x'_1))|_v \le |T|_v^{N^2}\exp(C'_vN^2(d+d'+2N))$$

である．よって，

$$|\operatorname{Norm}(T(x_0,x_1,x_2,x'_0,x'_1,x'_1))|_v \le A_v^{N^2(d+d')}|F|_v^{N^2}\exp(C'_vN^2(d+d'+2N))$$

である．これより，

$$M_1=\sum_v(\log(A_v)+C'_v),\qquad M_2=2N\sum_v C'_v$$

とおくと，

$$h(\operatorname{Norm}(T(x_0,x_1,x_2,x'_0,x'_1,x'_1))) \le N^2(h(F)+M_1(d+d')+M_2)$$

が成立する．一方，

$$T(x_0,x_1,x_2,x'_0,x'_1,x'_2)=\beta(x_0,x_1)^d\beta(x'_0,x'_1)^{d'}F(x_0,\ldots,x_n,x'_0,\ldots,x'_n)$$

であるので，

$$\operatorname{Norm}(T(x_0,x_1,x_2,x'_0,x'_1,x'_1))=\beta(x_0,x_1)^{N^2d}\beta(x'_0,x'_1)^{N^2d'}\operatorname{Norm}(F(x_0,\ldots,x_n,x'_0,\ldots,x'_n))$$

である．よって，系 2.3.3 により，

$$\begin{aligned}&h(\operatorname{Norm}(F(x_0,\ldots,x_n,x'_0,\ldots,x'_n)))\\&\qquad\le h(\operatorname{Norm}(T(x_0,x_1,x_2,x'_0,x'_1,x'_1)))+4(N^2(d+d')\deg(\beta)+N^2(d+d'))\end{aligned}$$

となり，M_1 を $M_1+4\deg(\beta)+4$ で置き換えると，

$$h(\operatorname{Norm}(F(x_0,\ldots,x_n,x'_0,\ldots,x'_n))) \le N^2(h(F)+M_1(d+d')+M_2)$$

が成立する．　□

2.6. 導関数の長さの評価

K を代数体，C を K 上定義された絶対既約非特異射影曲線とする．今，$\mathbb{P}^1$ への射影 $\pi : C \to \mathbb{P}^1$ を固定する．ここで，$\mathbb{P}^1$ の有限集合 S を次のように定める．

$$S = \{\infty\} \cup \{a \in \mathbb{P}^1 \mid \pi \text{ は } a \text{ 上分岐している．}\}$$

さらに，$C_0 = C \setminus \pi^{-1}(S)$，$\mathbb{P}^1 \setminus \{\infty\} = \mathrm{Spec}(K[T])$ とおく．$z \in C_0(K)$ に対して，$\pi(z) = a \in K$ の時，$x = T - a$ は，C の z での局所変数を定める．y を C 上の K 上定義された有理型関数とすると，y は $K(T)$ 上代数的であるので，ある多項式 $P(X,Y) \in K[X,Y]$ が存在して，$P(x,y) = 0$ を満たす．さらに，z は K- 有理点であるので，$\mathcal{O}_{C,z}$ の完備化 $\widehat{\mathcal{O}}_{C,z}$ は $K[[x]]$ と同形である (例えば，[**9**, (28.M)] を参照)．したがって，$\mathcal{O}_{C,z}$ の元を x についてテーラー展開した時の係数はすべて K の元である．つまり，すべての $l \geq 0$ について

$$\left(\left(\frac{d}{dx}\right)^l y\right)(0) \in K$$

である．ここで上式での (0) は $x = 0$ を代入することを意味する．

この時，以下が成立する．

補題 2.6.1 (Eisenstein の定理の局所版)**.** v を K の付値で，$|y(0)|_v \leq 1$ であると仮定する．y が z で極を持たず，$(\partial P/\partial Y)(0, y(0)) \neq 0$ なら，$l \geq 0$ に対して，v が非アルキメデス的な時，

$$\left|\frac{1}{l!}\left(\left(\frac{d}{dx}\right)^l y\right)(0)\right|_v \leq \left(\frac{|P|_v}{|(\partial P/\partial Y)(0, y(0))|_v}\right)^{\max\{2l-1,0\}}$$

が，v がアルキメデス的な時，

$$\left|\frac{1}{l!}\left(\left(\frac{d}{dx}\right)^l y\right)(0)\right|_v \leq (2\deg(P))^{7l}\left(\frac{|P|_v}{|(\partial P/\partial Y)(0, y(0))|_v}\right)^{\max\{2l-1,0\}}$$

が成り立つ．ここで，$|P|_v$ は多項式としての長さである．

証明: y の x についての l- 階微分を $y^{(l)}$ で表すことにする．さらに，多項式 $F(X,Y) \in K[X,Y]$ に対して，$F_{X^iY^j}$ で X について i- 階，Y について j- 階の偏微分を表すことにする．まず初めに，次のことを示そう．

$$\text{(2.6.1.1)} \qquad \begin{cases} Q_1 = P_X, \\ Q_{l+1} = (Q_l)_X (P_Y)^2 - (Q_l)_Y P_X P_Y + (2l-1) Q_l (P_{YY} P_X - P_{XY} P_Y) \end{cases}$$

という漸化式によって多項式 Q_l を定めると

$$Q_l(x,y) + (P_Y(x,y))^{2l-1} y^{(l)} = 0$$

となる．

$P(x,y)=0$ を x で微分して，

$$P_X(x,y)+P_Y(x,y)y'=0$$

を得る．これは，$l=1$ の場合である．

$Q_l(x,y)+(P_Y(x,y))^{2l-1}y^{(l)}=0$ を x で微分して，

$$(Q_l)_X(x,y)+(Q_l)_Y(x,y)y'+$$
$$(2l-1)(P_Y(x,y))^{2l-2}(P_{XY}(x,y)+P_{YY}(x,y)y')y^{(l)}+(P_Y(x,y))^{2l-1}y^{(l+1)}=0$$

を得る．上式に $P_Y(x,y)^2$ を掛け，$P_X(x,y)+P_Y(x,y)y'=0$ と $Q_l(x,y)+(P_Y(x,y))^{2l-1}y^{(l)}=0$ に注意して，変形すると，

$$Q_{l+1}(x,y)+(P_Y(x,y))^{2l+1}y^{(l+1)}=0$$

を得る．よって，主張が証明できた．

漸化式 $(2.6.1.1)$ から，$n=\deg(P)$ とすると，Q_l は，高々 $(2l-1)(n-1)$ の多項式であることがわかる．v が非アルキメデス的な場合を考えよう．$l=0$ の場合は，明らかである．$l\geq 1$ と仮定する．まず，命題 $2.3.1$ の (4) を用いて，

$$\begin{aligned}|Q_{l+1}|_v &\leq |(Q_l)_X P_Y^2|_v+|(Q_l)_Y P_X P_Y|_v+(2l-1)|Q_l P_{YY}P_X|_v+(2l-1)|Q_l P_{XY}P_Y|\\ &\leq n^4(|(Q_l)_X|_v|P_Y|_v^2+|(Q_l)_Y|_v|P_X|_v|P_Y|_v\\ &\qquad +(2l-1)|Q_l|_v|P_{YY}|_v|P_X|_v+(2l-1)|Q_l|_v|P_{XY}|_v|P_Y|_v)\\ &\leq n^4\{4(2l-1)n^3\}|P|_v^2|Q_l|_v\leq 8n^7 l|P|_v^2|Q_l|_v\end{aligned}$$

ゆえに，

$$|Q_l|_v\leq (8n^7)^{l-1}(l-1)!|Q_1|_v^{2l-2}\leq n(8n^7)^{l-1}(l-1)!|P|_v^{2l-1}$$

を得る．したがって，$|y(0)|_v\leq 1$ に注意すると

$$\begin{aligned}|Q_l(0,y(0))|_v &\leq ((2l-1)(n-1)+1)|Q_l|_v\\ &\leq (2ln)n(8n^7)^{l-1}(l-1)!|P|_v^{2l-1}\\ &\leq l!(2n)^{7l}|P|_v^{2l-1}\end{aligned}$$

である．ここで，

$$|Q_l(0,y(0))|_v=|P_Y(0,y(0))|_v^{2l-1}|y^{(l)}(0)|_v$$

であるので結論を得る．

v が非アルキメデス的な時，上と同様の方法では，$l!$ の処理が難しいので別の方法をとる．$l \geq 0$ に対して，$\partial_l = \dfrac{1}{l!}\dfrac{d^l}{dx^l}$ とおく．∂_l の記法のよさは，ライプニッツの公式が簡単に書けることである．すなわち，

$$\partial_l(f_1 \cdots f_r) = \sum_{a_1+\cdots+a_r=l} \partial_{a_1}(f_1) \cdots \partial_{a_r}(f_r)$$

が成立する．さらに，$P(X,Y) = \sum_{ij} p_{ij} X^i Y^j$ とおく．l に関する帰納法で証明する．$l = 0$ の時は自明で，$l = 1$ の時，

$$|P_Y(0, y(0))|_v |y'(0)|_v = |P_X(0, y(0))|_v \leq |P|_v$$

ゆえ，成立する．そこで，$l \geq 2$ とする．ライプニッツの公式より，

$$\begin{aligned}
0 &= \partial_l(P(x,y)) \\
&= \sum_{ij} p_{ij} \sum_{e_0+e_1+\cdots+e_j=l} \partial_{e_0}(x^i)\partial_{e_1}(y) \cdots \partial_{e_j}(y) \\
&= \sum_{ij} p_{ij} j x^i y^{j-1} \partial_l(y) + \sum_{ij} p_{ij} \sum_{\substack{e_0+e_1+\cdots+e_j=l \\ 0 \leq e_1 < l, \cdots, 0 \leq e_j < l}} \partial_{e_0}(x^i)\partial_{e_1}(y) \cdots \partial_{e_j}(y) \\
&= P_Y(x,y)\partial_l(y) + \sum_{ij} p_{ij} \sum_{\substack{e_0+e_1+\cdots+e_j=l \\ 0 \leq e_1 < l, \cdots, 0 \leq e_j < l}} \partial_{e_0}(x^i)\partial_{e_1}(y) \cdots \partial_{e_j}(y)
\end{aligned}$$

である．ゆえに

$$|P_Y(0, y(0))\partial_l(y)(0)|_v \leq |P|_v \max_{\substack{e_1+\cdots+e_j=l-i, \\ 0 \leq i \leq l, \\ 0 \leq e_1 < l, \cdots, 0 \leq e_j < l}} \{|\partial_{e_1}(y)(0)|_v \cdots |\partial_{e_j}(y)(0)|_v\}$$

となる．ここで，$e_1 + \cdots + e_j = l - i$，$0 \leq i \leq l$，$0 \leq e_1 < l, \cdots, 0 \leq e_j < l$，の仮定のもとで

$$\max\{2e_1 - 1, 0\} + \cdots + \max\{2e_j - 1, 0\} \leq 2l - 2$$

であるので，$|P_X(0, y(0))|_v \leq |P|_v$ に注意して，帰納法の仮定を用いると，

$$|P_Y(0, y(0))|_v |\partial_l(y)(0)|_v \leq |P|_v \left(\frac{|P|_v}{|P_Y(0, y(0))|_v}\right)^{2l-2}$$

である．よって，v が非アルキメデス的な場合も証明できた． □

この補題をもう少し使いやすい形で書いておこう．前と同じ状況下で，$y_1, \cdots, y_e$ を K 上定義された C 上の有理型関数とし，$P_i(X,Y) \in K[X,Y]$ を y_i の定義多項式，つまり，$P_i(x, y_i) = 0$ となる多項式とする．さらに，$\partial_l = \dfrac{1}{l!}\dfrac{d^l}{dx^l}$ とおくことにする．この時，以下が成立する．

系 2.6.2. v を K の付値で，すべての i について $|y_i(0)|_v \leq 1$ であり，$(\partial P_i/\partial Y)(0, y_i(0)) \neq 0$ であると仮定する．この時，$l \geq 0$ に対して，次が成り立つ．

(1) v が非アルキメデス的な時，

$$\log^+(|\partial_l(y_1 \cdots y_e)(0)|_v) \leq 2l \max_i \left\{ \log^+ \left(\frac{|P_i|_v}{|(\partial P_i/\partial Y)(0, y_i(0))|_v} \right) \right\}$$

である．

(2) v が非アルキメデス的な時，

$$\log^+(|\partial_l(y_1 \cdots y_e)(0)|_v) \leq 2l \max_i \left\{ \log^+ \left(\frac{|P_i|_v}{|(\partial P_i/\partial Y)(0, y_i(0))|_v} \right) \right\} + 7l \max_i \{\log(2 \deg(P_i))\} + \log \binom{l+e-1}{l}$$

である．

証明: $l = 0$ の場合は，$|y_i(0)|_v \leq 1$ より成り立つ．さらに，$e = 1$ の場合は，補題 2.6.1 より成立する．$e > 1$ の場合は，ライプニッツの公式を用いて，

$$\partial_l(y_1 \cdots y_e) = \sum_{l_1 + \cdots + l_e = l} \partial_{l_1}(y_1) \cdots \partial_{l_e}(y_e)$$

である．よって，v が非アルキメデス的な時，

$$|\partial_l(y_1 \cdots y_e)(0)|_v \leq \max_{l_1 + \cdots + l_e = l} \{|\partial_{l_1}(y_1)|_v \cdots |\partial_{l_e}(y_e)|_v\}$$

であるので，$e = 1$ の場合を用いて，

$$\begin{aligned} \log^+(|\partial_l(y_1 \cdots y_e)(0)|_v) &\leq \max_{l_1 + \cdots + l_e = l} \{\log^+(|\partial_{l_1}(y_1)|_v) + \cdots + \log^+(|\partial_{l_e}(y_e)|_v)\} \\ &\leq 2l \max_i \left\{ \log^+ \left(\frac{|P_i|_v}{|(\partial P_i/\partial Y)(0, y_i(0))|_v} \right) \right\} \end{aligned}$$

となる．

v がアルキメデス的な時，

$$|\partial_l(y_1 \cdots y_e)(0)|_v \leq \binom{l+e-1}{l} \max_{l_1 + \cdots + l_e = l} \{|\partial_{l_1}(y_1)|_v \cdots |\partial_{l_e}(y_e)|_v\}$$

である．ここで，$e = 1$ の場合を用いて，

$$\log^+(|\partial_{l_1}(y_1)|_v \cdots |\partial_{l_e}(y_e)|_v) \leq 7l \max_i \{\log(2 \deg(P_i))\} + 2l \max_i \left\{ \log^+ \left(\frac{|P_i|_v}{|(\partial P_i/\partial Y)(0, y_i(0))|_v} \right) \right\}$$

となるので，

$$\log^+(|\partial_l(y_1 \cdots y_e)(0)|_v) \leq 2l \max_i \left\{ \log^+ \left(\frac{|P_i|_v}{|(\partial P_i/\partial Y)(0, y_i(0))|_v} \right) \right\} + 7l \max_i \{\log(2 \deg(P_i))\} + \log \binom{l+e-1}{l}$$

を得る．□

第 3 章

Ｍｏｒｄｅｌｌ−Ｆａｌｔｉｎｇｓの定理の証明

3.1. Ｍｏｒｄｅｌｌ−Ｆａｌｔｉｎｇｓの定理の証明のスケッチ

C を 代数体 K 上定義された種数 g が 2 以上の絶対既約非特異射影曲線とする．この章の目標は，Mordell-Faltings 定理を証明することにある．つまり，次の定理を証明する．

定理 3.1.1 (Mordell-Faltings の定理)**.** C の K-有理点は，有限個しか存在しない．

K を K の適当な有限次拡大でおきかえて，C 上の因子 θ で $(2g-2)\theta \sim \omega_C$ となるものを固定しておく．(このような θ が存在することをみるためには，$\mathrm{Pic}^0(C)(\overline{K})$ が可除群であることに注意すればよい.) J を C のヤコビ多様体とし，以後，$j(z) = \theta - z$ で定まる標準的な埋め込み $j : C \to J$ を固定し，$C(\overline{K})$ の点は $J(\overline{K})$ の点と思う．また，

$$\langle\ ,\ \rangle : J(\overline{K}) \times J(\overline{K}) \to \mathbb{R}$$

を J の theta 因子から定まる Neron-Tate height pairing とする．さらに，$x \in J(\overline{K})$ に対して，$|x| = \sqrt{\langle x, x\rangle}$ とおく．Mordell-Faltings 定理は，次の定理の帰結である．

定理 3.1.2. $g\cos(\alpha) > \sqrt{g}$ となる $0 \le \alpha < \pi/2$ を固定する．この時，次を満たす γ，γ' が存在する．$z, z' \in C(K)$ で $|z| \ge \gamma$，$|z'| \ge |z|\gamma'$ なら，

$$\langle z, z'\rangle < \cos(\alpha)|z||z'|$$

が成立する．

というのは，$g \ge 2$ のとき $g > \sqrt{g}$ であるので，$g\cos(\alpha) > \sqrt{g}$ となる $0 < \alpha < \pi/2$ がとれる．$L = J(K) \otimes_{\mathbb{Z}} \mathbb{R}$ とおくと，Mordell-Weil の定理により，L は有限次元のベクトル空間である．$C(K)$ の点 z, z' に対して，L の中での角度を $\theta(z, z')$ とすると，定理 3.1.2 は，$|z| \ge \gamma$，$|z'| \ge |z|\gamma'$ なら，$\theta(z, z') > \alpha$ であることを言っている．ここで，もし $C(K)$ が無限集合であるなら，いわゆる Dirichlet の部屋割り論法により，L の中に原点を中心とする錐 Σ が存在して次の性質を満たす．Σ には $C(K)$ からくる元を無限個含み，任意の $x, x' \in \Sigma$ に対して，x と x' のなす角度は $\alpha/2$ 以下である．一方，Σ には $C(K)$ からくる元を無限個含むので，Northcott の定理より，$|z| \ge \gamma$，$|z'| \ge |z|\gamma'$ で，z, z' の L における像が Σ に含まれる $z, z' \in C(K)$ がとれる．これは，定理 3.1.2 に矛盾する．

さらに，定理 3.1.2 は次の 3 つの定理の帰結である．これを述べる前に少し言葉を準備する．$C \times C$ を考える．$p_i : C \times C \to C$ を i- 成分への射影とする．$C \times C$ の対角成分を Δ で表し，$\Delta' = \Delta - p_1^*(\theta) - p_2^*(\theta)$ とおく．$gd^2 < d_1 d_2 < g^2 d^2$ を満たす正の整数 d_1, d_2, d に対して，因子

$$V(d_1, d_2, d) = d_1 p_1^*(\theta) + d_2 p_2^*(\theta) + d\Delta'$$

を Vojta 因子と呼ぶ．$V(d_1, d_2, d)$ のゼロでない大域切断 s，つまり

$$s \in H^0(C \times C, \mathcal{O}_{C\times C}(V(d_1, d_2, d))) \setminus \{0\}$$

に対して，s の高さ $h(s)$ が定義できる．いかに定義するかは，§3.2 で論ずることにする．さらに，s の点 $(z, z') \in C \times C$ での (d_1, d_2) についての index を定義する．ζ，ζ' を C の z，z' での局所変数とする．(ζ，ζ' は，解析的であってもかまわない.) s_0 を (z, z') での $\mathcal{O}_{C\times C}(V(d_1, d_2, d))$ の局所底とする．この時，ある局所的な解析関数 $f(\zeta, \zeta')$ が存在して，$s = f s_0$ と書ける．$f(\zeta, \zeta')$ をテーラー展開して，

$$f(\zeta, \zeta') = \sum_{i,j} a_{ij} \zeta^i \zeta'^j$$

とおく．この時，

$$\min \left\{ \frac{i}{d_1} + \frac{j}{d_2} \mid a_{ij} \neq 0 \right\}$$

は，ζ，ζ'，s_0 のとりかたに依らないことが容易にわかる．そこで，これを $\mathrm{ind}_{(z,z')}(s; (d_1, d_2))$ で表し，s の点 $(z, z') \in C \times C$ での (d_1, d_2) についての index と呼ぶ．以上の準備で，次の定理 3.1.3，定理 3.1.4，定理 3.1.5を満たす正の定数 C_1，C_2，C_3，C_4，C_5，C_6 と $C(\overline{K})$ の有限集合 Z が存在する．(以下において，$V(d_1, d_2, d))$ は，Vojta 因子である.)

定理 3.1.3 (高さの小さい切断の存在)**.** 正の数 δ_0 を固定する．$d_1 d_2 - gd^2 \geq \delta_0 d_1 d_2$ であり，d_1, d_2, d が十分大きければ，

$$h(s) \leq \frac{C_1}{\delta_0} \left(1 + \frac{\log(d_1 + d_2 + d)}{d}\right) (d_1 + d_2 + d)$$

となるゼロでない切断 $s \in H^0(C \times C, \mathcal{O}_{C\times C}(V(d_1, d_2, d)))$ が存在する．

定理 3.1.4 (切断の index の上限)**.** $0 < \epsilon < 1$ となる ϵ を固定し，$d_2/d_1 \leq \epsilon$ と仮定する．この時，ゼロでない切断 $s \in H^0(C \times C, \mathcal{O}_{C\times C}(V(d_1, d_2, d)))$ に対して，もし $z, z' \in C(K) \setminus Z$ で，

$$\epsilon^2 \min\{d_1 |z|^2, d_2 |z'|^2\} \geq C_2 h(s) + C_3 (d_1 + d_2 + d)$$

なら，

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \leq C_4\epsilon$$

が成り立つ．

定理 3.1.5 (切断の index の下限)**．ゼロでない切断** $s \in H^0(C\times C, \mathcal{O}_{C\times C}(V(d_1,d_2,d)))$ **に対して，** $z,z' \in C(K)\setminus Z$ **なら，**

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \geq \frac{2gd\langle z,z'\rangle - d_1|z|^2 - d_2|z'|^2 - 2gh(s) - C_5(d_1+d_2+d)}{C_6\max\{d_1(1+|z|^2), d_2(1+|z'|^2)\}}$$

が成立する．

定理 3.1.3，定理 3.1.4，定理 3.1.5から定理 3.1.2 を導くアイデアは，序でもすこし述べたように，高さの小さい切断に対してその index の上限と下限をうまく比較して結論を導くということである．すこし複雑になるがやってみよう．まず，$g\cos(\alpha)-\sqrt{g+\delta}>0$ となる $\delta>0$ と，$\delta_0<\delta$ となる $\delta_0>0$ を固定し，

$$f(t) = \frac{g\cos(\alpha)-\sqrt{g+\delta}}{C_6\sqrt{g+\delta}} - \frac{3}{2}\frac{4gC_1+C_5\delta_0}{C_6\delta_0}\frac{1}{t^2}$$

とおく．さらに，C_0 を $f(C_0)>0$ となる正の数とする．さて，γ' を

$$\begin{cases}\gamma' > 1\\ \gamma' > C_4/f(C_0)\end{cases}$$

を満たすようにとる．さらに，固定した γ' に対して，γ を

$$\begin{cases}\gamma > 1\\ \gamma > C_0\\ \gamma > (1+\delta)\gamma'\sqrt{3\left(\dfrac{2C_1C_2}{\delta_0}+C_3\right)}\\ \gamma > \max_{z\in Z}\{|z|\}\end{cases}$$

を満たすようにとる．以上のように定めた γ，γ' に対して，定理 3.1.2 が成り立つことをみよう．

$z,z' \in C(K)$ を $|z|\geq\gamma$ かつ $|z'|\geq\gamma'|z|$ となるものとする．この時，結論を否定して，

$$\langle z,z'\rangle \geq \cos(\alpha)|z||z'|$$

であると仮定する．$\delta_1>0$ を $\sqrt{g+\delta_1}\frac{|z'|}{|z|}$ が有理数になり，$\delta_0<\delta_1<\delta$ となるようにとる．さらに，$\delta_2>0$ を $\sqrt{g+\delta_2}\frac{|z|}{|z'|}$ が有理数になり，$\delta_0<\delta_2<\delta_1$ であり，$\sqrt{\frac{g+\delta_1}{g+\delta_2}}\leq(1+\delta)^2$ となるようにとる．ここで，

$$a_1 = \sqrt{g+\delta_1}\frac{|z'|}{|z|}, \qquad a_2 = \sqrt{g+\delta_2}\frac{|z|}{|z'|}$$

とおく．a を十分大きな整数で aa_1，aa_2 が整数になるようなものとする．この時，整数 m に対して，$d_1 = aa_1m$，$d_2 = aa_2m$，$d = am$ とおく．

$$\sqrt{g+\delta_1}\sqrt{g+\delta_2} \leq g+\delta < g^2\cos(\alpha) \leq g^2$$

であることより，$gd^2 < d_1d_2 < g^2d^2$ がチェックできるので，d_1, d_2, d の定める因子は Vojta 因子である．また，

$$\sqrt{g+\delta_1}\sqrt{g+\delta_2} - g \geq g+\delta_0 - g = \delta_0$$

であるので，$d_1d_2 - gd^2 \geq \delta_0 d^2$ である．よって，m を十分大きくとれば，

$$\frac{\log(d_1+d_2+d)}{d} < 1$$

であることに注意して，定理 3.1.3 より，

$$h(s) \leq \frac{2C_1}{\delta_0}(d_1+d_2+d)$$

となるゼロでない切断 $s \in H^0(C\times C, \mathcal{O}_{C\times C}(V(d_1,d_2,d)))$ が存在する．まず，定理 3.1.4 を利用して，$\mathrm{ind}_{(z,z')}(s;(d_1,d_2))$ の上限を調べよう．$\epsilon = 1/\gamma'$ とおく．γ の取り方より，$z, z' \notin Z$ である．さらに，

$$d_2/d_1 = \frac{\sqrt{g+\delta_2}}{\sqrt{g+\delta_1}}\frac{|z|^2}{|z'|^2} \leq \frac{|z|^2}{|z'|^2} \leq (1/\gamma')^2$$

となる．よって，

$$(1/\gamma')^2\min\{d_1|z|^2, d_2|z'|^2\} \geq C_2h(s) + C_3(d_1+d_2+d)$$

を調べなければならない．実際，

$$u = (1/\gamma')^2\min\{d_1|z|^2, d_2|z'|^2\} - C_2h(s) - C_3(d_1+d_2+d)$$

とおくと，$d_1 \geq \max\{d_1,d_2,d\}$ に注意すれば，

$$\begin{aligned}
u &\geq (1/\gamma')^2\min\{d\sqrt{g+\delta_1}|z||z'|, d\sqrt{g+\delta_2}|z||z'|\} - \left(\frac{2C_2C_1}{\delta_0}+C_3\right)(d_1+d_2+d)\\
&\geq (1/\gamma')^2 d\sqrt{g+\delta_2}|z||z'| - 3\left(\frac{2C_2C_1}{\delta_0}+C_3\right)d_1\\
&= \frac{d\sqrt{g+\delta_2}|z'|}{|z|\gamma'^2}\left(|z|^2 - 3\left(\frac{2C_2C_1}{\delta_0}+C_3\right)\gamma'^2\frac{\sqrt{g+\delta_1}}{\sqrt{g+\delta_2}}\right)\\
&\geq \frac{d\sqrt{g+\delta_2}|z'|}{|z|\gamma'^2}\left(|z|^2 - 3\left(\frac{2C_2C_1}{\delta_0}+C_3\right)(\gamma'(1+\delta))^2\right)\\
&\geq \frac{d\sqrt{g+\delta_2}|z'|}{|z|\gamma'^2}\left(\gamma^2 - 3\left(\frac{2C_2C_1}{\delta_0}+C_3\right)(\gamma'(1+\delta))^2\right) > 0
\end{aligned}$$

となり，成立する．よって，定理 3.1.4 より，

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \leq \frac{C_4}{\gamma'}$$

である．

次に，$\mathrm{ind}_{(z,z')}(s;(d_1,d_2))$ の下限を求めよう．そこで，定理 3.1.5 にあらわれる

$$\frac{2gd\langle z,z'\rangle - d_1|z|^2 - d_2|z'|^2 - 2gh(s) - C_5(d_1+d_2+d)}{C_6\max\{d_1(1+|z|^2), d_2(1+|z'|^2)\}}$$

を評価しよう．まず，分子から考える．$d_1 > d_2$，$d_1 > d$ に注意して，

$$\begin{aligned}
\text{分子} &\geq 2gd\langle z,z'\rangle - d_1|z|^2 - d_2|z'|^2 - \frac{4gC_1}{\delta_0}(d_1+d_2+d) - C_5(d_1+d_2+d)\\
&\geq 2gd\langle z,z'\rangle - d_1|z|^2 - d_2|z'|^2 - 3\frac{4gC_1+\delta_0C_5}{\delta_0}d_1\\
&\geq 2gd\cos(\alpha)|z||z'| - d\sqrt{g+\delta_1}|z||z'| - d\sqrt{g+\delta_2}|z||z'| - 3\frac{4gC_1+\delta_0C_5}{\delta_0}d\sqrt{g+\delta_1}\frac{|z'|}{|z|}\\
&\geq 2d(g\cos(\alpha) - \sqrt{g+\delta})|z||z'| - 3\frac{4gC_1+\delta_0C_5}{\delta_0}d\sqrt{g+\delta}\frac{|z'|}{|z|}\\
&= 2d\sqrt{g+\delta}C_6|z||z'|f(|z|)
\end{aligned}$$

を得る．さらに，

$$\begin{aligned}
\text{分母} &\leq 2C_6\max\{d_1|z|^2, d_2|z'|^2\}\\
&= 2C_6\max\{d\sqrt{g+\delta_1}|z||z'|, d\sqrt{g+\delta_2}|z||z'|\}\\
&\leq 2d\sqrt{g+\delta}C_6|z||z'|
\end{aligned}$$

である．よって，

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \geq f(|z|) > f(C_0)$$

となる．上限，下限の二つの評価をあわせて，

$$f(C_0) < \mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \leq \frac{C_4}{\gamma'}$$

を得る．つまり，$\gamma' f(C_0) < C_4$ となり，γ' の取り方に矛盾する．

3.2. 定理 3.1.3，定理 3.1.4，定理 3.1.5 の証明に必要な技術的設定

C を 代数体 K 上定義された種数 g が 2 以上の絶対既約非特異射影曲線とする．以後，必要なら順次 K の有限次拡大を考えることにする．

3.2.1. θ を C 上の因子で，$(2g-2)\theta$ が C の標準因子 ω_C と線形同値であるとする．このような因子は，K の適当な有限次拡大を考えることで存在する．$(2g-2)\theta \sim \omega_C$ ゆえ，$\deg(\theta)=1$ であり，C 上の豊富な因子である．ゆえに，N が十分大きな数とするとき，$N\theta$ は十分豊富となる．つまり，$\{\phi_0,\cdots,\phi_n\}$ を $H^0(C,\mathcal{O}_C(N\theta))$ を基底とすると，$\Phi_{N\theta}(x) = (\phi_0(x) : \cdots : \phi_n(x))$ で定まる有理射 $\Phi_{N\theta} : C \to \mathbb{P}^n$ を考えると，これは埋め込みを定める．$\mathbb{P}^n$ の同次座標系 $\{X_0,\ldots,X_n\}$ (あるいは，$H^0(C,\mathcal{O}_C(N\theta))$ の基底 $\{\phi_0,\cdots,\phi_n\}$) を十分一般にとれば，次を仮定してよい．(詳しくは，[**7**, IV-3] を参考のこと．)

仮定 **3.2.1.1.** 任意の $i \neq j$ に対して，C と 線形空間 $\{X_i = X_j = 0\}$ は，共通部分を持たない．さらに，任意の相異なる i,j,k に対して，$(X_0 : \cdots : X_n) \mapsto (X_i : X_j : X_k)$ によって決まる射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^2$ による C の像と C は双有理である．

任意の $i \neq j$ に対して，$(X_0 : \cdots : X_n) \mapsto (X_i : X_j)$ よって定まる射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^1$ から導かれる射 $C \to \mathbb{P}^1$ を $\Phi^{ij}_{N\theta}$ で表し，さらに，相異なる i,j,k について，$(X_0 : \cdots : X_n) \mapsto (X_i : X_j : X_k)$ よって定まる射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^2$ から導かれる射 $C \to \mathbb{P}^2$ を $\Phi^{ijk}_{N\theta}$ で表す．また，$\Phi^{ijk}_{N\theta}(C)$ を C_{ijk} で表す．この時，$(\Phi^{ij}_{N\theta})^*(\mathcal{O}_{\mathbb{P}^1}(1)) = (\Phi^{ijk}_{N\theta})^*(\mathcal{O}_{\mathbb{P}^2}(1)) = \mathcal{O}_C(N\theta)$ である．特に，$\deg(\Phi^{ij}_{N\theta}) = N$ で，C_{ijk} の $\mathbb{P}^2$ の中での次数は N である．C は $\{X_0 = X_1 = 0\}$ と交わらないので，C_{012} は $(0:0:1)$ を通らない．よって，C_{012} は

$$X_2^N + a_{N-1}(X_0,X_1)X_2^{N-1} + \cdots + a_1(X_0,X_1)X_2 + a_0(X_0,X_1)$$

という形の N- 次の同次多項式で定義される．$c \in O_K \setminus \{0\}$ を $ca_i \in O_K[X_0,X_1]$ となる元とする．この時，上の多項式に c^N をかけて，

$$(cX_2)^N + ca_{N-1}(X_0,X_1)(cX_2)^{N-1} + \cdots + c^{N-1}a_1(X_0,X_1)(cX_2) + c^N a_0(X_0,X_1)$$

となる．ゆえに，X_2 の代わりに cX_2 を用いて次を仮定してよい．

仮定 **3.2.1.2.** C_{012} の定義方程式

$$X_2^N + a_{N-1}(X_0,X_1)X_2^{N-1} + \cdots + a_1(X_0,X_1)X_2 + a_0(X_0,X_1) = 0$$

において，すべての i について $a_i \in O_K[X_0,X_1]$ と仮定してよい．

3.2.2. $C \times C$ を考える．$p_i : C \times C \to C$ を i- 成分への射影とする．$C \times C$ の対角成分を Δ で表し，$\Delta' = \Delta - p_1^*(\theta) - p_2^*(\theta)$ とおく．$gd^2 < d_1 d_2 < g^2 d^2$ を満たす正の整数 d_1, d_2, d に対して，因子

$$V(d_1,d_2,d) = d_1 p_1^*(\theta) + d_2 p_2^*(\theta) + d\Delta'$$

を Vojta 因子と呼ぶ．t が十分大きい時，

$$B = tp_1^*(\theta) + tp_2^*(\theta) - \Delta'$$

は，十分豊富な因子になり，それの定める埋め込みを

$$\Phi_{|B|} : C \times C \to \mathbb{P}^m$$

で表す．$\mathbb{P}^m$ の同次座標を $(Y_0 : \cdots : Y_m)$ とし，$y_i = Y_i|_{C\times C}$ とおく．$\{y_0, \ldots, y_m\}$ は，$H^0(C \times C, \mathcal{O}_{C\times C}(B))$ の基底である．ここで，$N|(d_1 + td)$，$N|(d_2 + td)$ とし，

$$\delta_1 = \frac{d_1 + td}{N}, \qquad \delta_2 = \frac{d_2 + td}{N}$$

とおくと，

$$V(d_1, d_2, d) = \delta_1 p_1^*(N\theta) + \delta_2 p_2^*(N\theta) - dB$$

である．自然な準同形

$$H^0(\mathbb{P}^n \times \mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n\times\mathbb{P}^n}(\delta_1, \delta_2)) \to H^0(C \times C, \mathcal{O}_{C\times C}(\delta_1 p_1^*(N\theta) + \delta_2 p_2^*(N\theta)))$$

を考える．$\mathbb{P}^n \times \mathbb{P}^n$ の第 1 成分の同次座標を $(X_0 : \cdots : X_n)$，第 2 成分の同次座標を $(X_0' : \cdots : X_n')$ で表すと，$H^0(\mathbb{P}^n \times \mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n\times\mathbb{P}^n}(\delta_1, \delta_2))$ は，$K[X_0, \ldots, X_n, X_0', \ldots, X_n]$ の両次数が (δ_1, δ_2) の同次式全体である．(ここで，$(X_0 : \cdots : X_n)$，$(X_0' : \cdots : X_n')$ は，十分一般で，前の条件，仮定 3.2.1.1 と仮定 3.2.1.2 を満たしているとする.) これを

$$K[X_0, \ldots, X_n, X_0', \ldots, X_n]_{(\delta_1,\delta_2)}$$

で表すことにする．さらに，$X_i|_C$，$X_i'|_C$ を x_i，x_i' で表すことにする．以後，

$$K[X_0, \ldots, X_n, X_0', \ldots, X_n]$$

を $K[X, X']$ で略記する．

命題 3.2.2.1.

$$U = \left\{(F_0, \ldots, F_m) \in \left(K[X, X']_{(\delta_1,\delta_2)}\right)^{m+1} \mid F_0(x, x')/y_0^d = \cdots = F_m(x, x')/y_m^d\right\}$$

とおくと，自然な準同形

$$R : U \longrightarrow H^0(C \times C, \mathcal{O}_{C\times C}(V(d_1, d_2, d)))$$

が存在し，R は全射である．

証明: $(F_0,\dots,F_m)\in U$ とする．$F_0(x,x')\in H^0(C\times C,\mathcal{O}_{C\times C}(\delta_1 p_1^*(N\theta)+\delta_2 p_2^*(N\theta)))$ であり，$y_0^d\in H^0(C\times C,\mathcal{O}_{C\times C}(dB))$ であるので，$s=F_0(x,x')/y_0^d$ は，$\mathcal{O}_{C\times C}(V(d_1,d_2,d))$ の有理切断であり，

$$F_0(x,x')/y_0^d=\cdots=F_m(x,x')/y_m^d$$

は，s が至る所，極をもたないことを示している．よって，$R((F_0,\dots,F_m))=s$ で R が定義できる．

逆に，$s\in H^0(C\times C,\mathcal{O}_{C\times C}(V(d_1,d_2,d)))$ に対して，sy_i^d を考えると，これは

$$H^0(C\times C,\mathcal{O}_{C\times C}(\delta_1 p_1^*(N\theta)+\delta_2 p_2^*(N\theta)))$$

の元である．ゆえに $F_i(X,X')\in K[X,X']_{(\delta_1,\delta_2)}$ が存在して，$F_i(x,x')=sy_i^d$ となる．

$$s=F_0(x,x')/y_0^d=\cdots=F_m(x,x')/y_m^d$$

であるので，$(F_0,\cdots,F_m)\in U$ となる．つまり，R は全射である． □

$\mathcal{O}_{C\times C}(V(d_1,d_2,d))$ の大域切断 $s\neq 0$ に対して，$R((F_0,\dots,F_m))=s$ となる U の中の多項式の列 $(F_0,\dots,F_m)$ を s を表現する多項式列と呼ぶことにする．$h(F_0,\dots,F_m)$ で F_i のすべての係数からなるベクトルの高さを表すことにする．つまり，$F_i=\sum a_{i,I,I'}X^IX'^{I'}$ とおくと，

$$h(F_0,\dots,F_m)=\frac{1}{[K:\mathbb{Q}]}\sum_v \log\max_{i,I,I'}\{|a_{i,I,I'}|_v\}$$

と定める．さらに，s の高さ $h(s)$ を

$$h(s)=\inf_{\substack{(F_0,\cdots,F_m)\in U,\\ R((F_0,\cdots,F_m))=s}} h(F_0,\dots,F_m)$$

で定義する．

3.2.3. 定理 3.1.4 と定理 3.1.5 にあらわれる除外集合 Z は，定理 3.1.4 にとっての除外集合 Z_1 と定理 3.1.5 にとっての除外集合 Z_2 の和 $Z_1\cup Z_2$ とする．

3.3. 高さの小さい切断 (定理 3.1.3 の証明)

命題 3.2.2.1 より，

$$U=\left\{(F_0,\dots,F_m)\in\left(K[X,X']_{(\delta_1,\delta_2)}\right)^{m+1}\mid F_0(x,x')/y_0^d=\cdots=F_m(x,x')/y_m^d\right\}$$

とおくと，自然な準同形

$$R:U\longrightarrow H^0(C\times C,\mathcal{O}_{C\times C}(V(d_1,d_2,d)))$$

は全射である．つまり，方程式 $F_i(x,x')y_j^d = F_j(x,x')y_i^d$ を解けばよいのであるが，まず最初に y_i を単純化しよう．ϕ を $H^0(C\times C, \mathcal{O}_{C\times C}(\Delta))$ の標準元とする．この時，ϕy_i は，

$$H^0(C\times C, \mathcal{O}_{C\times C}((t+1)(p_1^*(\theta)+p_2^*(\theta))))$$

の元である．ここで，t' を，$t+1+t'$ が N の倍数になり，$t'\geq 2g+2$ となる整数とする．ϕ' を $H^0(C,\mathcal{O}_C(t'\theta))$ のゼロでない元とする．この時，$t+1+t'=Nr$ とおくと，$\phi y_i p_1^*(\phi')p_2^*(\phi')$ は，

$$H^0(C\times C, \mathcal{O}_{C\times C}(r(p_1^*(N\theta)+p_2^*(N\theta)))) = H^0(C\times C, \mathcal{O}_{C\times C}(r,r))$$

の元 である．よって，ある両次数が (r,r) の同次多項式 $G_i(X,X')$ が存在して，$G_i(x,x') = \phi y_i p_1^*(\phi')p_2^*(\phi')$ となる．このとき，

$$F_i(x,x')y_j^d = F_j(x,x')y_i^d \quad\Longleftrightarrow\quad F_i(x,x')G_j(x,x')^d = F_j(x,x')G_i(x,x')^d$$

である．さらに，$(X_0 : \cdots : X_n) \mapsto (X_0 : X_1 : X_2)$ で定まる射影 $\mathbb{P}^n \dashrightarrow \mathbb{P}^2$ による C の像を C' (3.2.1では C_{012} で表されていた.) とすると，C と C' は双有理である．したがって，命題 $2.5.3$ の証明と同様にして, あるゼロでない同次多項式 $\beta(X_0,X_1)$ が存在して，$\beta(x_0,x_1)x_j \in K[x_0,x_1,x_2]$ がすべての $j\geq 3$ で成立する．よって，$\beta(x_0,x_1)^r\beta(x_0',x_1')^r G_i(x,x')$ は，$K[x_0,x_1,x_2,x_0',x_1',x_2']$ の元である．つまり，$G_i \in K[X_0,X_1,X_2,X_0',X_1',X_2']$ と仮定してよい．さらに G_i たちの係数の共通分母を掛けて，$G_i \in O_K[X_0,X_1,X_2,X_0',X_1',X_2']$ としてよい．

以上をまとめると，両次数が (r,r) の同次多項式 $G_i \in O_K[X_0,X_1,X_2,X_0',X_1',X_2']$ が存在して，

$$F_i(x,x')y_j^d = F_j(x,x')y_i^d \ \ (\forall i,j) \quad\Longleftrightarrow\quad F_i(x,x')G_j(x,x')^d = F_j(x,x')G_i(x,x')^d \ \ (\forall i,j)$$

であることがわかった．

さて $\alpha(f_0,\ldots,f_m) = \sum_{i<j}(f_iG_j(x,x')^d - f_jG_i(x,x')^d)$ で定まる準同型

$$\alpha : H^0(C\times C, \mathcal{O}_{C\times C}(\delta_1,\delta_2))^{m+1} \longrightarrow H^0(C\times C, \mathcal{O}_{C\times C}(\delta_1+rd,\delta_2+rd))^{m(m+1)/2}$$

を考える．$H^0(C\times C,\mathcal{O}_{C\times C}(V)) = \mathrm{Ker}(\alpha)$ である．$H^0(C\times C,\mathcal{O}_{C\times C}(\delta_1,\delta_2))$ の基底を具体的に計算することは難しいので, 部分空間 $H^0(C'\times C',\mathcal{O}_{C'\times C'}(\delta_1,\delta_2))$ を考える．$G_i(x,x') \in H^0(C'\times C',\mathcal{O}_{C'\times C'}(r,r))$ であるので，α から

$$\alpha' : H^0(C'\times C', \mathcal{O}_{C'\times C'}(\delta_1,\delta_2))^{m+1} \longrightarrow H^0(C'\times C', \mathcal{O}_{C'\times C'}(\delta_1+rd,\delta_2+rd))^{m(m+1)/2}$$

が導かれる．今後，$\mathrm{Ker}(\alpha')$ の元を求めることを考える．まず $H^0(C'\times C',\mathcal{O}_{C'\times C'}(\delta_1,\delta_2))$ の基底を求める．

主張 **3.3.1.** $V(\delta_1,\delta_2)$ を

$$\sum_{\substack{0\leq c<N\\ 0\leq c'<N}} q_{cc'}(X_0,X_1,X_0',X_1')X_2^c{X_2'}^{c'}$$

の形で表せる両次数が (δ_1,δ_2) の $K[X_0,X_1,X_2,X_0',X_1',X_2']$ の同次多項式全体とする．このとき，$F(X,X')\mapsto F(x,x')$ で定まる

$$V(\delta_1,\delta_2)\to H^0(C'\times C',\mathcal{O}_{C'\times C'}(\delta_1,\delta_2))$$

は同型である．

証明:　仮定 3.2.1.2 により，C' は

$$X_2^N+a_{N-1}(X_0,X_1)X_2^{N-1}+\cdots+a_1(X_0,X_1)X_2+a_0(X_0,X_1)=0$$

で定義されているのでこの主張は明らかである． □

従って，$\delta_1\geq N,\delta_2\geq N$ の時

$$\left\{X_0^aX_1^bX_2^c{X_0'}^{a'}{X_1'}^{b'}{X_2'}^{c'}\right\}_{\substack{0\leq c<N\\ a+b=\delta_1-c\\ 0\leq c'<N\\ a'+b'=\delta_2-c'}}$$

が $V(\delta_1,\delta_2)$ の基底となるので，

$$\begin{aligned}\dim_K H^0(C'\times C',\mathcal{O}_{C'\times C'}(\delta_1,\delta_2)) &= \left(N\delta_1-\frac{N(N-3)}{2}\right)\left(N\delta_2-\frac{N(N-3)}{2}\right)\\ &= \left(N^2\delta_1\delta_2-\frac{N^2(N-3)}{2}(\delta_1+\delta_2)+\left(\frac{N(N-3)}{2}\right)^2\right)\end{aligned}$$

である．よって，d_1,d_2,d が十分大きければ，

$$\dim_K H^0(C'\times C',\mathcal{O}_{C'\times C'}(\delta_1,\delta_2))^{m+1}\leq(m+1)(d_1+dt)(d_2+dt)$$

である．ここで $N^2\delta_1\delta_2=(d_1+dt)(d_2+dt)$ に注意する．

さて，$\dim_K\mathrm{Ker}(\alpha')$ を評価しよう．まず，容易に

$$\begin{aligned}\dim_K\mathrm{Ker}(\alpha')\geq{}&\dim_K\mathrm{Ker}(\alpha)\\ &-\left(\dim_K H^0(C\times C,\mathcal{O}_{C\times C'}(\delta_1,\delta_2))^{m+1}-\dim_K H^0(C'\times C',\mathcal{O}_{C'\times C'}(\delta_1,\delta_2))^{m+1}\right)\end{aligned}$$

がわかる．まず，C 上の Riemann-Roch の定理より，

$$\begin{aligned}\dim_K H^0(C\times C,\mathcal{O}_{C\times C}(\delta_1,\delta_2))^{m+1} &= (m+1)(N\delta_1+1-g)(N\delta_2+1-g)\\ &= (m+1)(N^2\delta_1\delta_2-N(g-1)(\delta_1+\delta_2)+(g-1)^2)\end{aligned}$$

である．さらに，d_1, d_2, d が十分大きい時，$H^2(C\times C, \mathcal{O}_{C\times C}(V)) = 0$ に注意すれば，$C\times C$ 上の Riemann-Roch により，

$$\begin{aligned}\dim_K \mathrm{Ker}(\alpha) &= \dim_K H^0(C\times C, \mathcal{O}_{C\times C}(V)) \\ &\geq \chi(\mathcal{O}_{C\times C}(V)) \\ &= \frac{(V\cdot V - \omega_{C\times C})}{2} + \chi(\mathcal{O}_{C\times C}) \\ &= (d_1d_2 - gd^2) - 2(g-1)(d_1+d_2) + \chi(\mathcal{O}_{C\times C}) \\ &\geq \delta_0 d_1 d_2 - O(d_1+d_2)\end{aligned}$$

となる．よって，$\dim_K \mathrm{Ker}(\alpha') \geq \delta_0 d_1 d_2 - O(d_1+d_2+d)$ である．したがって，$d_1d_2 > gd^2$ に注意すれば，d_1, d_2, d が十分大きい時，

$$\dim_K \mathrm{Ker}(\alpha') \geq \frac{\delta_0 d_1 d_2}{2} \tag{3.3.2}$$

である．

次に，$H^0(C\times C, \mathcal{O}_{C\times C}(\delta_1,\delta_2))$ と $H^0(C'\times C', \mathcal{O}_{C'\times C'}(\delta_1+rd, \delta_2+rd))$ のそれぞれの基底

$$\left\{ x_0^a x_1^b x_2^c {x'_0}^{a'} {x'_1}^{b'} {x'_2}^{c'} \right\}_{\substack{0\leq c<N \\ a+b=\delta_1-c \\ 0\leq c'<N \\ a'+b'=\delta_2-c'}} \qquad \left\{ x_0^a x_1^b x_2^c {x'_0}^{a'} {x'_1}^{b'} {x'_2}^{c'} \right\}_{\substack{0\leq c<N \\ a+b=\delta_1+rd-c \\ 0\leq c'<N \\ a'+b'=\delta_2+rd-c'}}$$

で α' を表現した時の行列の係数を評価しよう．まず

$$F_i(X,X') = \sum_{\substack{0\leq c<N \\ a+b=\delta_1-c \\ 0\leq c'<N \\ a'+b'=\delta_2-c'}} T_{i,abca'b'c'} X_0^a X_1^b X_2^c {X'_0}^{a'} {X'_1}^{b'} {X'_2}^{c'}$$

とおく．$T_{i,abca'b'c'}$ は求める未知数である．この時，

$$F_i(x,x')G_j(x,x')^d = \sum_{\substack{0\leq c<N \\ a+b=\delta_1-c \\ 0\leq c'<N \\ a'+b'=\delta_2-c'}} T_{i,abca'b'c'} x_0^a x_1^b {x'_0}^{a'} {x'_1}^{b'} \left(x_2^c {x'_2}^{c'} G_j(x,x')^d \right)$$

となる．ここで

$$x_2^c {x'_2}^{c'} G_j(x,x')^d = \sum_{\substack{0\leq l<N \\ 0\leq l'<N}} H_{ll'}^{jcc'}(x_0,x_1,x'_0,x'_1) x_2^l {x'_2}^{l'}$$

とおくと，命題 2.5.2 より，$H_{ll'}^{jcc'}(X_0,X_1,X'_0,X'_1)$ は，高々両次数が $(c+dr-l, c'+dr-l')$ の同次多項式であり，仮定 3.2.1.2 より，C' の定義多項式

$$X_2^N + a_{N-1}(X_0,X_1)X_2^{N-1} + \cdots + a_1(X_0,X_1)X_2 + a_0(X_0,X_1) = 0$$

において $a_i \in O_K[X_0, X_1]$ ゆえ，$H_{ll'}^{jcc'}$ の係数はすべて O_K の元である．ここで，$H_{ll'}^{jcc'}$ の係数が行列表現にあらわれる数である．さらに，命題 2.5.2 より，K の各付値 v に対して，a_i のみによる定数 C_v が存在して，

$$|H_{ll'}^{jcc'}|_v \leq |X_2^c X_2'^{c'} G_j(X, X')^d|_v \exp(C_v(c + c' + 2dr)) \leq |G_j(X, X')^d|_v \exp(C_v(2dr + 2N))$$

となる．さらに，ここで v がアルキメデス的な場合のみを考えると

$$\begin{aligned} |G_j(X, X')^d|_v &= |G_j(X, X')^d|_v \\ &\leq (1 + r)^{6d} |G_j(X, X')|_v^d \end{aligned}$$

であるので，d_1, d_2, d に無関係なある定数 A_1 が存在して，すべての j, c, c', l, l' とアルキメデス的付値 v に対して

$$|H_{ll'}^{jcc'}|_v \leq \exp(A_1 d)$$

が成立する．まとめると，α' の行列の任意の要素 e に対して，$e \in O_K$ であり，

$$\|e\|_K \leq \exp(A_1 d)$$

となる．ここで，$\|e\|_K$ は，v をすべての K のアルキメデス的付値を走らせた時の $|e|_v$ の最大値である．

Siegel の補題 (命題 2.1.2) より，K 及び O_K の $\mathbb{Z}$ 上の自由基底の取り方のみによる定数 A_2，A_3 が存在して，未知数 $T_{i,abca'b'c'}$ の自明でない解 $t_{i,abca'b'c'} \in O_K$ を次を満たすようにとれる．

$$\begin{aligned} &\max_{i,a,b,c,a',b',c'} \log \|t_{i,abca'b'c'}\|_K \\ &\qquad \leq \frac{\operatorname{rk} \alpha'}{\dim \operatorname{Ker}(\alpha')} \left(A_1 d + \log \left(\dim_K H^0(C' \times C', \mathcal{O}_{C' \times C'}(\delta_1, \delta_2))^{m+1} \right) + A_2 \right) + A_3 \end{aligned}$$

$\dim_K H^0(C' \times C', \mathcal{O}_{C' \times C'}(\delta_1, \delta_2))^{m+1} \leq (m + 1)(d_1 + dt)(d_2 + dt)$ であるので，A_4 を適当にとると，

$$A_1 d + \log \left(\dim_K H^0(C' \times C', \mathcal{O}_{C' \times C'}(\delta_1, \delta_2))^{m+1} \right) + A_2 \leq A_4 d \left(1 + \frac{\log(d_1 + d_2 + d)}{d} \right)$$

となる．さて，$\dfrac{\operatorname{rk}\alpha'}{\dim \operatorname{Ker}(\alpha')}d$ を評価しよう．$d^2 < g^2 d_1 d_2$ と (3.3.2) に注意して，

$$\begin{aligned}
\frac{\operatorname{rk}\alpha'}{\dim \operatorname{Ker}(\alpha')}d &\leq \frac{\dim_K H^0(C' \times C', \mathcal{O}_{C'\times C'}(\delta_1, \delta_2))^{m+1}}{\dim \operatorname{Ker}(\alpha')}d \\
&\leq \frac{(m+1)(d_1+td)(d_2+td)}{\delta_0 d_1 d_2/2}d \\
&\leq \frac{2(m+1)}{\delta_0}\left\{d + t(d_1+d_2)\frac{d^2}{d_1 d_2} + t^2 d\frac{d^2}{d_1 d_2}\right\} \\
&\leq \frac{2(m+1)}{\delta_0}\left\{d + t(d_1+d_2)g^2 + t^2 d g^2\right\} \\
&\leq \frac{2(m+1)}{\delta_0}(1 + tg^2 + t^2 g^2)(d_1 + d_2 + d)
\end{aligned}$$

を得る．よって，$A_5 = 2(m+1)(1+tg^2+t^2g^2)$ とおくと，

$$\frac{\operatorname{rk}\alpha'}{\dim \operatorname{Ker}(\alpha')}d \leq \frac{A_5}{\delta_0}(d_1+d_2+d)$$

である．ゆえに，

$$\begin{aligned}
\max_{i,a,b,c,a',b',c'} \log \|t_{i,abca'b'c'}\|_K &\leq \frac{\operatorname{rk}\alpha'}{\dim \operatorname{Ker}(\alpha')}dA_4\left(1 + \frac{\log(d_1+d_2+d)}{d}\right) + A_3 \\
&\leq \frac{A_4 A_5}{\delta_0}(d_1+d_2+d)\left(1 + \frac{\log(d_1+d_2+d)}{d}\right) + A_3
\end{aligned}$$

よって，C_1 を A_4A_5 より少し大きくとれば，d_1, d_2, d が十分大きい時，

$$\max_{i,a,b,c,a',b',c'} \log \|t_{i,abca'b'c'}\|_K \leq \frac{C_1}{\delta_0}\left(1 + \frac{\log(d_1+d_2+d)}{d}\right)(d_1+d_2+d)$$

となる．ここで，$t_{i,abca'b'c'} \in O_K$ であるので，任意の非アルキメデス的付値 v に対して，$|t_{i,abca'b'c'}|_v \leq 1$ である．また，任意のアルキメデス的付値 v に対して，

$$|t_{i,abca'b'c'}|_v \leq \max_{i,a,b,c,a',b',c'} \log \|t_{i,abca'b'c'}\|_K$$

である．よって，$t_{i,abca'b'c'}$ で作った多項式列 $(F_0, \ldots, F_m)$ について，

$$h(F_0, \ldots, F_m) \leq \frac{C_1}{\delta_0}\left(1 + \frac{\log(d_1+d_2+d)}{d}\right)(d_1+d_2+d)$$

が成り立つ．したがって，$(F_0, \ldots, F_m)$ が定める切断を s とすると，

$$h(s) \leq h(F_0, \ldots, F_m) \leq \frac{C_1}{\delta_0}\left(1 + \frac{\log(d_1+d_2+d)}{d}\right)(d_1+d_2+d)$$

となり，証明が完成した． □

3.4. Ｉｎｄｅｘの上限 (定理 3.1.4 の証明)

相異なる i,j に対して，$\pi_{ij}=\Phi^{ij}_{N\theta}\times\Phi^{ij}_{N\theta}:C\times C\to\mathbb{P}^1\times\mathbb{P}^1$ を考える．この時，命題 2.5.3 より，$F\in K[X,X']_{(\delta_1,\delta_2)}$ に対して，$\mathrm{Norm}_{\pi_{ij}}(F(x,x'))$ は，$K[X_i,X_j,X'_i,X'_j]$ の両次数が $(N^2\delta_1,N^2\delta_2)$ の同次多項式である．さらに，C，$\Phi_{N\theta}$，i，j のみに依存する定数 M が存在して，

$$h(\mathrm{Norm}_{\pi_{ij}}(F))\le N^2h(F)+M(\delta_1+\delta_2)$$

が成立する．M は一応 i,j に依るが，i,j についての最大値を考えれば，i,j に依らないとしてよい．さらに，$C(\overline{K})$ の有限集合 Z_1 が存在して，$z\notin Z_1$ なら，すべての i,j について，$\Phi^{ij}_{N\theta}:C\to\mathbb{P}^1$ は $\Phi^{ij}_{N\theta}(z)$ 上不分岐となる．さらに，Z_1 に $x_0=0$ となる点を加えて，$z\notin Z_1$ なら $x_0(z)\neq 0$ としてよい．

さて，多項式列 $(F_0,\dots,F_m)$ で表現される切断 s を考える．ここで，$(F_0,\dots,F_m)$ をうまくとって，$h(F_0,\dots,F_m)\le h(s)+1/2$ とする．E を s の零点集合とする．$(\pi_{ij})_*(E)$ は，両次数が (Nd_1,Nd_2) の $\mathbb{P}^1\times\mathbb{P}^1$ の因子であることを示そう．このためには，

$$((\pi_{ij})_*(E)\cdot\mathcal{O}(0,1))=Nd_1,\qquad((\pi_{ij})_*(E)\cdot\mathcal{O}(1,0))=Nd_2$$

を調べればよい．射影公式を用いて，

$$\begin{aligned}((\pi_{ij})_*(E)\cdot\mathcal{O}(0,1))&=(E\cdot(\pi_{ij})^*(\mathcal{O}(0,1)))\\&=((d_1-d)p_1^*(\theta)+(d_2-d)p_2^*(\theta)+d\Delta\cdot Np_2^*(\theta))=Nd_1\end{aligned}$$

となる．同様に，$((\pi_{ij})_*(E)\cdot\mathcal{O}(1,0))=Nd_2$ である．ここで，$\mathrm{Norm}_{\pi_{ij}}(s)$ は両次数が (Nd_1,Nd_2) の同次多項式であるので多項式としての高さ $h(\mathrm{Norm}_{\pi_{ij}}(s))$ を考える．$s=F_0/y_0^d$ ゆえ，$\mathrm{Norm}_{\pi_{ij}}(s)$ は，$\mathrm{Norm}_{\pi_{ij}}(F_0(x,x'))$ の約元である．したがって，$\deg(\mathrm{Norm}_{\pi_{ij}}(F_0(x,x')))=N^2(\delta_1+\delta_2)$ に注意して，系 2.3.3 より，

$$\begin{aligned}h(\mathrm{Norm}_{\pi_{ij}}(s))&\le h(\mathrm{Norm}_{\pi_{ij}}(F_0(x,x')))+4N^2(\delta_1+\delta_2)\\&\le N^2h(F_0)+(M+4N^2)(\delta_1+\delta_2)\\&\le N^2h(F_0,\dots,F_m)+(M+4N^2)(\delta_1+\delta_2)\\&\le N^2h(s)+N^2/2+(M+4N^2)(\delta_1+\delta_2)\end{aligned}$$

となるので，適当な M' をとって，

$$h(\mathrm{Norm}_{\pi_{ij}}(s))+4Nd_1\le N^2h(s)+M'(d_1+d_2+d)$$

となる．

系 1.7.2 の (2) より，ある定数 A が存在して，

$$\frac{N}{2g}|z|^2 \leq h_{N\theta}(z) + A$$

が任意の $z \in C(\overline{K})$ で成立する．

さて，ここで

$$C_2 = 2ng, \qquad C_3 = \frac{2gn}{N^2}M' + \frac{2g}{N}A, \qquad C_4 = 4N$$

とおいて，定理 3.1.4 を示そう．$z, z' \notin Z_1$ とする．この時，$h_{N\theta}(z) \leq \sum_{\nu=1}^{n} h^+((x_\nu/x_0)(z))$ であるので，$h^+((x_i/x_0)(z))$ が $\{h^+((x_\nu/x_0)(z))\}_{1\leq\nu\leq n}$ の最大値を与えているとすると，

$$nh^+((x_i/x_0)(z)) \geq h_{N\theta}(z)$$

である．同様にして，$nh^+((x_j/x_0)(z')) \geq h_{N\theta}(z')$ となる j がとれる．$\mathrm{Norm}_{\pi_{ij}}(s)$ を x_0，x_0' について非同次化した多項式を P とし，$a = (x_i/x_0)(z)$，$b = (x_j/x_0)(z')$ とおく．$r_1 = Nd_1$，$r_2 = Nd_2$ で，P と (a, b) に Roth の補題 (定理 2.4.2) を応用しよう．というのは，(z, z') のまわりで局所的には，s は $\mathrm{Norm}_{\pi_{ij}}(s)$ の約元であるので，

$$\mathrm{ind}_{(z,z')}(s; (d_1, d_2)) \leq \mathrm{ind}_{(z,z')}(\mathrm{Norm}_{\pi_{ij}}(s); (d_1, d_2))$$

である．さらに，$z, z' \notin Z_1$ ゆえ，(z, z') の近傍と (a, b) の近傍は複素解析的に同型である．よって，

$$\mathrm{ind}_{(z,z')}(\mathrm{Norm}_{\pi_{ij}}(s); (d_1, d_2)) = \mathrm{ind}_{(a,b)}(P; (d_1, d_2)) = N\,\mathrm{ind}_{(a,b)}(P; (Nd_1, Nd_2))$$

である．まとめると

$$\mathrm{ind}_{(z,z')}(s; (d_1, d_2)) \leq N\,\mathrm{ind}_{(a,b)}(P; (Nd_1, Nd_2))$$

となる．Roth の補題を適用して結論を得るためには，

$$\epsilon^2 \min\{Nd_1h^+(a), Nd_2h^+(b)\} \geq h(P) + 4Nd_1$$

とチェックしなけらばならない．実際，

$$\begin{aligned}
h(P) + 4Nd_1 &\leq N^2 h(s) + M'(d_1 + d_2 + d) \\
&\leq N^2 \frac{\epsilon^2 \min\{d_1|z|^2, d_2|z'|^2\} - C_3(d_1 + d_2 + d)}{2gn} + M'(d_1 + d_2 + d) \\
&= \frac{N}{n}\left(\epsilon^2 \min\left\{d_1 \frac{N}{2g}|z|^2, d_2 \frac{N}{2g}|z'|^2\right\} - A(d_1 + d_2 + d)\right) \\
&\leq \frac{N}{n}\left(\epsilon^2 \min\{d_1(h_{N\theta}(z) + A), d_1(h_{N\theta}(z) + A)\} - A(d_1 + d_2 + d)\right) \\
&\leq \frac{N}{n}\left(\epsilon^2 \min\{d_1 h_{N\theta}(z), d_1 h_{N\theta}(z)\} + \epsilon^2 A(d_1 + d_2) - A(d_1 + d_2 + d)\right) \\
&\leq \epsilon^2 \frac{N}{n} \min\{d_1 h_{N\theta}(z), d_1 h_{N\theta}(z)\} \\
&\leq \epsilon^2 N \min\{d_1 h^+(a), d_2 h^+(b)\} \\
&= \epsilon^2 \min\{N d_1 h^+(a), N d_2 h^+(b)\}
\end{aligned}$$

となる．よって，Roth の補題から

$$\mathrm{ind}_{(a,b)}(P; (Nd_1, Nd_2)) \leq 4\epsilon$$

となる．これは，結論を導く．

3.5. Ｉｎｄｅｘの下限 (定理 3.1.5 の証明)

まず次の主張から始めよう．

主張 3.5.1. $0 \leq \nu \leq n$，$0 \leq \mu \leq n$，$\nu \neq \mu$ に対して，高々 $2N$- 次の多項式 $P_{\nu,\mu}(U,V) \in K[U,V]$ が存在して，$P_{\nu,\mu}(x_1/x_0, x_\nu/x_\mu) = 0$ であり，$(\partial P_{\nu,\mu}/\partial V)(x_1/x_0, x_\nu/x_\mu)$ は恒等的にゼロでない．さらに，$x_0(z) \neq 0$ となる $z \in C(K)$ に対して，$P'_{\nu,\mu}(U,V) = P_{\nu,\mu}(U + (x_1/x_0)(z), V)$ とおくと，次が成立する．

(1) $h^+(P'_{\nu,\mu}) \leq h^+(P_{\nu,\mu}) + \log(2N+1)(N+1) + 2N\log(2) + 2N h_{N\theta}(z)$ である．

(2) $x_\mu(z) \neq 0$ の時，

$$h^+((\partial P'_{\nu,\mu}/\partial V)(0, (x_\nu/x_\mu)(z))) \leq h^+(P'_{\nu,\mu}) + 2\log(2N) + (2N-1)h_{N\theta}(z)$$

が成立する．

証明: $a \mapsto (x_0(a) : x_1(a))$ によって定義される $C \to \mathbb{P}^1$ を π，$a \mapsto (x_\nu(a) : x_\mu(a))$ によって定義される $C \to \mathbb{P}^1$ を π' で表す．ここで，$\Pi = \pi \times \pi' : C \to \mathbb{P}^1 \times \mathbb{P}^1$ を考える．$\Pi(C)$ は，$\mathbb{P}^1 \times \mathbb{P}^1$ の中で次数は高々 (N,N) である．ゆえに，高々 $2N$- 次の絶対既約な多項式 $P_{\nu,\mu} \in K[S,T]$ が存在して，$P_{\nu,\mu}(x_1/x_0, x_\nu/x_\mu) = 0$ となる．$p_1 : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ を第 1 成

分への射影とすると，K の標数がゼロであるので，$p_1 : \Pi(C) \to \mathbb{P}^1$ は，$\mathbb{P}^1$ の開集合の上で不分岐である．これは，$(\partial P_{\nu,\mu}/\partial V)(x_1/x_0, x_\nu/x_\mu)$ は恒等的にゼロでないことを示している．

次に，(1) の不等式を考える．

$$P_{\nu,\mu} = \sum_{ij} p_{ij} U^i V^j$$

とおく．この時，

$$P'_{\nu,\mu} = \sum_{ij} p_{ij} (U + (x_1/x_0)(z))^i V^j$$

であるので，v が非アルキミデス的な時，

$$\begin{aligned} |P'_{\nu,\mu}|_v &\leq \max_{ij}\{|p_{ij}|_v |(U + (x_1/x_0)(z))^i|_v\} \\ &\leq |P_{\nu,\mu}|_v \max_i\{|U + (x_1/x_0)(z)|_v^i\} \\ &\leq |P_{\nu,\mu}|_v \max\{1, |(x_1/x_0)(z)|_v\}^{2N} \end{aligned}$$

である．さらに，v がアルキミデス的な時，

$$\begin{aligned} |P'_{\nu,\mu}|_v &\leq (N+1)(2N+1) \max_{ij}\{|p_{ij}|_v |(U + (x_1/x_0)(z))^i|_v\} \\ &\leq (N+1)(2N+1)|P_{\nu,\mu}|_v \max_i\{2^i |U + (x_1/x_0)(z)|_v^i\} \\ &\leq (N+1)(2N+1)|P_{\nu,\mu}|_v 2^{2N} \max\{1, |(x_1/x_0)(z)|_v\}^{2N} \end{aligned}$$

である．よって，

$$h^+(P'_{\nu,\mu}) \leq h^+(P_{\nu,\mu}) + \log(N+1)(2N+1) + 2N\log(2) + 2N h^+((x_1/x_0)(z))$$

したがって，$h^+((x_1/x_0)(z)) \leq h_{N\theta}(z)$ に注意すれば不等式を得る．

最後に，(2) の不等式について考えよう．$P'_{\nu,\mu} = \sum_{ij} p'_{ij} U^i V^j$ とおく．この時，

$$(\partial P'_{\nu,\mu}/\partial V)(0, (x_\nu/x_\mu)(z)) = \sum_{j=1}^{2N} j p'_{0j} (x_\nu/x_\mu)(z)^{j-1}$$

である．ゆえに，v が非アルキメデス的な付値の時，

$$\begin{aligned} |(\partial P'_{\nu,\mu}/\partial V)(0, (x_\nu/x_\mu)(z))|_v &\leq \max_{i,j} |p'_{ij}|_v \max_{0 \leq j \leq 2N-1}\{|(x_\nu/x_\mu)(z)^j|_v\} \\ &\leq \max_{i,j} |p'_{ij}|_v \max\{1, |(x_\nu/x_\mu)(z)|_v\}^{2N-1} \end{aligned}$$

である．したがって，

$$\log^+(|(\partial P'_{\nu,\mu}/\partial V)(0, (x_\nu/x_\mu)(z))|_v) \leq \max_{i,j} \log^+(|p'_{ij}|_v) + (2N-1)\log^+(|(x_\nu/x_\mu)(z)|_v)$$

を得る．v がアルキメデス的な付値の時，

$$\begin{aligned}|(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))|_v &\le (2N)^2 \max_{i,j}|p'_{ij}|_v \max_{0\le j\le 2N-1}\{|(x_\nu/x_\mu)(z)^j|_v\}\\ &\le (2N)^2 \max_{i,j}|p'_{ij}|_v \max\{1,|(x_\nu/x_\mu)(z)|_v\}^{2N-1}\end{aligned}$$

である．したがって，

$$\begin{aligned}&\log^+(|(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))|_v)\\ &\qquad\le 2\log(2N)+\max_{i,j}\log^+(|p'_{ij}|_v)+(2N-1)\log^+(|(x_\nu/x_\mu)(z)|_v)\end{aligned}$$

を得る．よって，

$$\begin{aligned}h^+((\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))) &\le 2\log(2N)+h^+(P'_{\nu,\mu})+(2N-1)h^+((x_\nu/x_\mu)(z))\\ &\le 2\log(2N)+h^+(P'_{\nu,\mu})+(2N-1)h_{N\theta}(z)\end{aligned}$$

となり証明できた．　□

$a\mapsto(x_0(a):x_1(a))$ によって定義される射影 $C\to\mathbb{P}^1$ を π で表す．$T=x_1/x_0$ とすると，$\mathbb{P}^1\setminus\{\infty\}=\mathrm{Spec}(K[T])$ である．

$$Z'=\{\infty\}\cup\{p\in\mathbb{P}^1\mid \pi \text{ は } p \text{ 上分岐している．}\}$$

とおく．ここで，定理 3.1.5 にとっての除外集合を

$$\begin{aligned}Z_2=\pi^{-1}(Z')\cup\bigcup_j\{a\in C\mid x_j(a)\neq 0\}\cup\bigcup_i\{a\in C\mid y_i(a)\neq 0\}\cup\\ \bigcup_{\nu\neq\mu}\{a\in C\mid(\partial P_{\nu,\mu}/\partial V)((x_1/x_0)(a),(x_\nu/x_\mu)(a))=0\}\end{aligned}$$

とおく．以後，$z,z'\notin Z_2$ とする．$t=T-x_1(z)/x_0(z)$ とおくと，t は，z のまわりでの局所変数となる．同様にして，z' のまわりでの局所変数 $t'=T-x_1(z')/x_0(z')$ を用意する．以後，

$$\partial_i=\frac{1}{i!}\left(\frac{\partial}{\partial t}\right)^i,\qquad \partial'_{i'}=\frac{1}{i'!}\left(\frac{\partial}{\partial t'}\right)^{i'}$$

とおく．

さて，多項式列 $(F_0(X,X'),\dots,F_m(X,X'))$ で表現される切断

$$s\in H^0(C\times C,\mathcal{O}_{C\times C}(V(d_1,d_2,d)))$$

の $\mathrm{ind}_{(z,z')}(s;(d_1,d_2))$ の下限を評価しよう．

まず，$h_V(z,z')$ を考える．$V=\delta_1N\theta+\delta_2N\theta-dB$ であるので，$a_j=x_j(z)$，$a'_{j'}=x_{j'}(z')$，$b_i=y_i(z,z')$ とおき，各付値 $v\in M_K$ に対して，$|a_{j(v)}|_v=\max_j\{|a_j|_v\}$，$|a'_{j'(v)}|_v=$

$\max_{j'}\{|a'_{j'}|_v\}$ ， $|b_{i(v)}|_v = \max_i\{|b_i|_v\}$ となる $j(v)$ ， $j'(v)$ ， $i(v)$ を選らんでおく．この時，

$$[K:\mathbb{Q}]h_V(z,z') = \delta_1\sum_v \max_j \log(|a_j|_v) + \delta_2\sum_v \max_{j'}\log(|a'_{j'}|_v) - d\sum_v \max_i \log(|b_i|_v)$$
$$= \sum_v \log\left|\frac{{a_{j(v)}}^{\delta_1}{a'_{j'(v)}}^{\delta_2}}{b^d_{i(v)}}\right|_v$$

となる．ここで，有理型関数 g を

$$g = \frac{s}{x_0^{\delta_1}{x'_0}^{\delta_2}y_0^{-d}}\left(= \frac{F_i(x/x_0, x'/x'_0)}{(y_i/y_0)^d}\right)$$

とおく．いま (l,l') を

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) = \frac{l}{d_1} + \frac{l'}{d_2}$$

となるものとする．このとき index の定義から，任意の (α,α') で， $\alpha \le l$ ， $\alpha' \le l'$ ， $(\alpha,\alpha') \neq (l,l')$ となるものについて

$$(\partial_\alpha \partial'_{\alpha'} g)(z,z') = 0$$

である．ここで， $f = (\partial_l\partial'_{l'}g)(z,z')$ とおく．この時，次が成立することを見よう．

主張 **3.5.2.** $f \neq 0$ であり，任意の i,j,j' について，

$$f = (b_i/b_0)^{-d}(a_j/a_0)^{\delta_1}(a'_{j'}/a'_0)^{\delta_2}\partial_l\partial_{l'}F_i(x/x_j, x'/x'_{j'})(z,z')$$

が成立する．

証明: $f \neq 0$ は， index の定義より明らかである．一方 g の定義より

$$g = (y_i/y_0)^{-d}F_i(x/x_0, x'/x'_0) = (y_i/y_0)^{-d}(x_j/x_0)^{\delta_1}(x'_{j'}/x'_0)^{\delta_2}F_i(x/x_j, x'/x'_{j'})$$

である．つまり，

$$F_i(x/x_j, x'/x'_{j'}) = (y_i/y_0)^d(x_j/x_0)^{-\delta_1}(x'_{j'}/x'_0)^{-\delta_2}g$$

である．ライプニッツの公式より，

$$\partial_l\partial_{l'}(F_i(x/x_j, x'/x'_{j'})) = \sum_{\substack{e_1+e_2=l\\ e'_1+e'_2=l'}} \partial_{e_1}\partial_{e'_1}((y_i/y_0)^d(x_j/x_0)^{-\delta_1}(x'_{j'}/x'_0)^{-\delta_2})\partial_{e_2}\partial_{e'_2}(g)$$

となる．よって，

$$\partial_l\partial_{l'}(F_i(x/x_j, x'/x'_{j'}))(z,z') = (b_i/b_0)^d(a_j/a_0)^{-\delta_1}(a'_{j'}/a'_0)^{-\delta_2}(\partial_l\partial'_{l'}g)(z,z')$$

を得るので，主張が証明できた． □

さて，前式

$$[K:\mathbb{Q}]h_V(z,z') = \sum_v \log \left| \frac{{a_{j(v)}}^{\delta_1} {a'_{j'(v)}}^{\delta_2}}{b_{i(v)}^d} \right|_v$$

にもどる．積公式と主張 3.5.2 より上式は，以下のように変形できる．

$$\begin{aligned}
[K:\mathbb{Q}]h_V(z,z') &= \sum_v \log \left| \frac{{a_{j(v)}}^{\delta_1} {a'_{j'(v)}}^{\delta_2}}{f b_{i(v)}^d} \right|_v \\
&= -\sum_v \log \left| \partial_l \partial_{l'} F_{i(v)}(x/x_{j(v)}, x'/x'_{j'(v)})(z,z') \frac{b_0^d}{{a_0^{\delta_1}}{a'_0}^{\delta_2}} \right|_v \\
&= -\sum_v \log \left| \partial_l \partial_{l'} F_{i(v)}(x/x_{j(v)}, x'/x'_{j'(v)})(z,z') \right|_v .
\end{aligned}$$

ここで，

$$F_i(X,X') = \sum_{I,I' \in \mathbb{Z}_+^{n+1}} p_{i,I,I'} X^I {X'}^{I'}$$

とおくと，

$$\partial_l \partial_{l'} F_{i(v)}(x/x_{j(v)}, x'/x'_{j'(v)})(z,z') = \sum_{I,I' \in \mathbb{Z}_+^{n+1}} p_{i(v),I,I'} \partial_l((x/x_{j(v)})^I)(z) \partial_{l'}((x'/x'_{j'(v)})^{I'})(z')$$

である．v が非アルキメデス的である時は，

$$\begin{aligned}
|\partial_l \partial_{l'} F_{i(v)}(x/x_{j(v)}, x'/x'_{j'(v)})(z,z')|_v &\le \max_{I,I'} \left\{ |p_{i(v),I,I'} \partial_l((x/x_{j(v)})^I)(z) \partial_{l'}((x'/x'_{j'(v)})^{I'})(z')|_v \right\} \\
&\le \max_{i,I,I'} \{|p_{i,I,I'}|_v\} \times \\
&\qquad \max_I \left\{ |\partial_l((x/x_{j(v)})^I)(z)|_v \right\} \max_{I'} \left\{ |\partial_{l'}((x'/x'_{j'(v)})^{I'})(z')|_v \right\}
\end{aligned}$$

であり，v がアルキメデス的である時は，

$$\begin{aligned}
|\partial_l \partial_{l'} F_{i(v)}(x/x_{j(v)}, x'/x'_{j'(v)})(z,z')|_v &\le \binom{\delta_1+n}{n} \binom{\delta_2+n}{n} \times \\
&\qquad \max_{I,I'} \left\{ |p_{i(v),I,I'} \partial_l((x/x_{j(v)})^I)(z) \partial_{l'}((x'/x'_{j'(v)})^{I'})(z')|_v \right\} \\
&\le \binom{\delta_1+n}{n} \binom{\delta_2+n}{n} \max_{i,I,I'} \{|p_{i,I,I'}|_v\} \times \\
&\qquad \max_I \left\{ |\partial_l((x/x_{j(v)})^I)(z)|_v \right\} \max_{I'} \left\{ |\partial_{l'}((x'/x'_{j'(v)})^{I'})(z')|_v \right\}
\end{aligned}$$

である．よって，$\binom{\delta_1+n}{n}\binom{\delta_2+n}{n} \leq 2^{\delta_1+n}2^{\delta_2+n}$ に注意すると，

$$\begin{aligned}[K:\mathbb{Q}]h_V(z,z') \geq -[K:\mathbb{Q}]h(F_0,\dots,F_m) - [K:\mathbb{Q}]\log(2)(\delta_1+\delta_2+2n)\\ -\sum_v \max_{\substack{I\in\mathbb{Z}_+^{n+1}\\ |I|=\delta_1}} \left\{\log^+|\partial_l((x/x_{j(v)})^I)(z)|_v\right\}\\ -\sum_v \max_{\substack{I'\in\mathbb{Z}_+^{n+1}\\ |I'|=\delta_2}} \left\{\log^+|\partial_{l'}((x'/x'_{j'(v)})^{I'})(z')|_v\right\}\end{aligned}$$

となる．

主張 **3.5.3.** ある定数 A_1 が存在して，

$$\sum_v \max_{\substack{I\in\mathbb{Z}_+^{n+1}\\ |I|=\delta_1}} \left\{\log^+|\partial_l((x/x_{j(v)})^I)(z)|_v\right\} \leq [K:\mathbb{Q}](\delta_1\log(2)+A_1(1+|z|^2)l)$$

と

$$\sum_v \max_{\substack{I'\in\mathbb{Z}_+^{n+1}\\ |I'|=\delta_2}} \left\{\log^+|\partial_{l'}((x'/x'_{j'(v)})^{I'})(z')|_v\right\} \leq [K:\mathbb{Q}](\delta_2\log(2)+A_1(1+|z'|^2)l')$$

が成立する．

証明: まず，$\log^+(|\partial_l((x/x_{j(v)})^I)(z)|_v)$ の評価を考えよう．

$$P'_{\nu,\mu}(X,Y) = P_{\nu,\mu}(X+(x_0/x_1)(z),Y)$$

とおいて，系 2.6.2 を用いると次を得る．v が非アルキメデス的な時，

$$\log^+(|\partial_l((x/x_{j(v)})^I)(z)|_v) \leq 2l\max_\nu\left\{\log^+\left(\frac{|P'_{\nu,j(v)}|_v}{|(\partial P'_{\nu,j(v)}/\partial V)(0,(x_\nu/x_{j(v)})(z))|_v}\right)\right\}$$

であり，v がアルキメデス的な時，

$$\begin{aligned}\log^+(|\partial_l((x/x_{j(v)})^I)(z)|_v) \leq (l+\delta_1)\log 2 + 7l\log(4N)\\ +2l\max_\nu\left\{\log^+\left(\frac{|P'_{\nu,j(v)}|_v}{|(\partial P'_{\nu,j(v)}/\partial V)(0,(x_\nu/x_{j(v)})(z))|_v}\right)\right\}\end{aligned}$$

となる．

以上より，

$$\begin{aligned}\sum_v \max_{\substack{I\in\mathbb{Z}_+^{n+1}\\ |I|=\delta_1}} \left\{\log^+|\partial_l((x/x_{j(v)})^I)(z)|_v\right\} \leq (\delta_1\log 2 + l(\log 2+7\log(4N)))\,[K:\mathbb{Q}]\\ +2l\sum_v\max_\nu\left\{\log^+\left(\frac{|P'_{\nu,j(v)}|_v}{|(\partial P'_{\nu,j(v)}/\partial V)(0,(x_\nu/x_{j(v)})(z))|_v}\right)\right\}\end{aligned}$$

さらに，

$$H = \sum_v \max_\nu \left\{ \log^+ \left(\frac{|P'_{\nu,j(v)}|_v}{|(\partial P'_{\nu,j(v)}/\partial V)(0,(x_\nu/x_{j(v)})(z))|_v} \right) \right\}$$

を評価しよう．

$$\begin{aligned}
H &\leq \sum_v \max_{\nu,\mu} \left\{ \log^+ \left(\frac{|P'_{\nu,\mu}|_v}{|(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))|_v} \right) \right\} \\
&\leq \sum_v \sum_{\nu,\mu} \log^+ \left(\frac{|P'_{\nu,\mu}|_v}{|(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))|_v} \right) \\
&\leq \sum_{\nu,\mu} \sum_v \log^+ \left(\frac{|P'_{\nu,\mu}|_v}{|(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))|_v} \right) \\
&\leq \sum_{\nu,\mu} \sum_v \left\{ \log^+(|P'_{\nu,\mu}|_v) + \log^+ \left(\frac{1}{|(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))|_v} \right) \right\} \\
&\leq [K:\mathbb{Q}] \sum_{\nu,\mu} \left(h^+(P'_{\nu,\mu}) + h^+ \left(\frac{1}{(\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z))} \right) \right) \\
&\leq [K:\mathbb{Q}] \sum_{\nu,\mu} \left(h^+(P'_{\nu,\mu}) + h^+ \left((\partial P'_{\nu,\mu}/\partial V)(0,(x_\nu/x_\mu)(z)) \right) \right)
\end{aligned}$$

である．したがって，主張 3.5.1 より，N，n と $h^+(P_{\nu,\mu})$ からなる定数 B，B' がとれて，

$$H \leq [K:\mathbb{Q}](B + B' h_{N\theta}(z))$$

となる．したがって，定数 B，B' を適当に取り替えると，

$$\frac{1}{[K:\mathbb{Q}]} \sum_v \max_{\substack{I \in \mathbb{Z}_+^{n+1} \\ |I|=\delta_1}} \left\{ \log^+ |\partial_l((x/x_{j(v)})^I)(z)|_v \right\} \leq \delta_1 \log 2 + (B + B' h_{N\theta}(z)) l$$

となる．さらに，系 1.7.2 の (2) より，$h_{N\theta} = \frac{N}{2g}|\ |^2 + O(1)$ であるので，最初の主張を得る．z' の場合も同様である． □

これまでのことをまとめると，

$$h_V(z,z') \geq -h(F_0,\dots,F_m) - 2\log(2)(\delta_1+\delta_2+n) - A_1((1+|z|^2)l + (1+|z'|^2)l')$$

が示せた．したがって，

$$\begin{aligned}
h_V(z,z') &\geq -h(F_0,\dots,F_m) - 2\log(2)(\delta_1+\delta_2+n) - A_1(d_1(1+|z|^2)\frac{l}{d_1} + d_2(1+|z'|^2)\frac{l'}{d_2}) \\
&\geq -h(F_0,\dots,F_m) - 2\log(2)(\delta_1+\delta_2+n) \\
&\quad - A_1 \max\{d_1(1+|z|^2), d_2(1+|z'|^2)\} \operatorname{ind}_{(z,z')}(s;(d_1,d_2))
\end{aligned}$$

が成立する．一方，系 1.7.2 を用いると

$$h_V(z,z') \leq \frac{d_1}{2g}|z|^2 + \frac{d_2}{2g}|z'|^2 - d\langle z,z'\rangle + A_2(d_1+d_2+d)$$

であるので，必要なら A_2 をさらに大きくとって，

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \geq \frac{d\langle z,z'\rangle - \frac{d_1}{2g}|z|^2 - \frac{d_2}{2g}|z'|^2 - h(F_0,\dots,F_m) - A_2(d_1+d_2+d)}{A_1\max\{d_1(1+|z|^2), d_2(1+|z'|^2)\}}$$

が成立する．ここで，切断 s を定める多項式列 $(F_0,\dots,F_m)$ を走らせて，上式の右辺の上限をとれば，

$$\mathrm{ind}_{(z,z')}(s;(d_1,d_2)) \geq \frac{2gd\langle z,z'\rangle - d_1|z|^2 - d_2|z'|^2 - 2gh(s) - 2gA_2(d_1+d_2+d)}{2gA_1\max\{d_1(1+|z|^2), d_2(1+|z'|^2)\}}$$

が成立する．よって，$C_5 = 2gA_2$，$C_6 = 2gA_1$ とおけば，定理 3.1.5 を得る．

3.6. 代数体上の漸近的Ｆｅｒｍａｔ予想

本節では，Faltings-Mordell 予想の簡単な応用として，代数体上の漸近的 Fermat 予想に関してわかることを考察しよう．

まず，始めに射影空間の点の高さに関する簡単な性質を示しておこう．

補題 3.6.1. K を代数体とし，高さ関数 $h : \mathbb{P}^n(K) \to \mathbb{R}$ を考える．この時，次が成立する．

(1) $x \in \mathbb{P}^n(K)$ に対して，$h(x) \geq 0$ であり，等号条件は，$x = (x_0,\dots,x_n) \in \mathbb{P}^n(K)$ とおくと，ある $\lambda \in K^\times$ とゼロ か 1 のべき根である y_i が存在して

$$(x_0,\dots,x_n) = \lambda(y_0,\dots,y_n)$$

となることである．

(2) $h(\mathbb{P}^n(K))$ は，$\mathbb{R}$ の中で離散的である．

証明: (1) $x = (x_0,\dots,x_n)$ とおき，$x_0 \neq 0$ としても一般性を失わない．ここで，$y_i = x_i/x_0$ とおく．この時，

$$h(x) = h((1,y_1,\dots,y_n)) = h^+((y_1,\dots,y_n)) \geq 0$$

であり，前半が示せた．後半を考える．y_i がゼロか 1 のべき根なら $h(x) = 0$ は自明である．そこで，$h(x) = 0$ と仮定する．この時，各 i について

$$0 \leq h^+(y_i) \leq h^+((y_1,\dots,y_n)) = h(x) = 0$$

となり，$h^+(y_i) = 0$ を得る．ここで，$y_i \neq 0$ とし，G を y_i で生成される $K^\times$ の部分群とする．$h^+(y_i^n) = nh^+(y_i) = 0$ であるので，Northcott の定理より G は有限群である．よって，y_i は 1 のべき根である．つまり，(1) が示せた．

(2) これは，Northcott の定理より明らかである． □

以上の準備で，以下の予想を考えよう．

予想 3.6.2 (代数体上の漸近的 Fermat 予想)**.** 自然数 n に対して，

$$F_n = \mathrm{Proj}\,(\mathbb{Z}[X,Y,Z]/(X^n + Y^n - Z^n)) \subset \mathbb{P}^2_{\mathbb{Z}}$$

とおく．代数体 K に対して，ある数 m が存在して，もし $n \geq m$ なら，$F_n(K)$ は高さがゼロとなる点から成る．つまり，$F_n(K) \subset \{x \in \mathbb{P}^3(K) \mid h(x) = 0\}$ である．

補題 3.6.1 より，$K = \mathbb{Q}$ の場合は，Wiles-Taylor の定理により，$m = 3$ で正しい．ここでは，一般の代数体に対しても，ほとんどの n で正しいことを示そう．($K = \mathbb{Q}$ の場合は，Granville と Heath-Brown による．詳しくは [**12**] を参照.)

命題 3.6.3. 代数体 K を固定し，$T(u)$ で，$1 \leq n \leq u$ であり，$F_n(K)$ が高さゼロの点のみからなるような n の個数とする．この時，

$$\lim_{u\to\infty} \frac{T(u)}{u} = 1$$

である．

証明:　鍵となるのは，次の補題である．($K = \mathbb{Q}$ の場合は，Filaseta による．詳しくは [**12**] を参照.)

補題 3.6.4. $n \geq 4$ とする．この時，ある m_0 が存在し，$m \geq m_0$ なら，$F_{mn}(K)$ は高さゼロの点のみから成る．

証明:　$n \geq 4$ であるので F_n の種数は 2 以上であるので，Mordell-Faltings の定理より，$F_n(K)$ は有限個の点のみから成る．$H = \max_{x\in F_n(K)}\{h(x)\}$ とおく．補題 3.6.1 より $h(\mathbb{P}^2(K))$ は離散的であるので，

$$a = \{h(x) \mid x \in \mathbb{P}^2(K), \quad h(x) > 0\}$$

とおくと，$a > 0$ である．ここで，自然数 m_0 を

$$m_0 \geq \exp(H/a)$$

となるようにとる．$m \geq m_0$ について，$F_{mn}(K)$ は高さゼロの点のみから成るということをみよう．$x = (x_0, x_1, x_2) \in F_{mn}(K)$ で，$h(x) > 0$ とする．この時，$h(x) \geq a$ であり，$y = (x_0^m, x_1^m, x_2^m) \in F_n(K)$ である．よって，

$$H \geq h(y) = mh(x) \geq ma$$

つまり，$\exp(H/a) \geq \exp(m)$ である．したがって，$m \geq \exp(m)$ を得る．これは矛盾である． □

命題 3.6.3 の証明に戻ろう．補題 3.6.4 より，5 以上の素数の倍数である大きな数については，K 上の Fermat 予想が正しくなるので，そうでない数はめずらしことを言えばよい．

もう少し正確にやるために，$N(u)$ で，$1 \leq n \leq u$ であり，$F_n(K)$ が正の高さの点をもつような n の個数とする．ゼータ関数 Euler 積表示と $\zeta(1) = \infty$ であることより，

$$\prod_{p \text{ は素数}} (1 - 1/p) = 0$$

である．よって，任意の $0 < \epsilon < 1$ に対して，5 以上の素数の列 $p_1, \ldots, p_s$ が存在して，

$$(1 - 1/p_1) \cdots (1 - 1/p_s) \leq \epsilon/4$$

となる．補題 3.6.4 より，各 p_i に対して，m_i が存在して，$m \geq m_i$ なら $F_{p_i m}(K)$ は高さゼロの点のみから成る．ここで，$P = p_1 \cdots p_s$，$M = \max\{p_i m_i\}$ とおく．さて，$M < n \leq u$ で，$(n, P) \neq 1$ なら，$F_n(K)$ は高さゼロの点のみから成るので

$$N(u) \leq M + \#\{1 \leq n \leq u | (n, P) = 1\}$$

である．n を P で割った余りを r とすると，$(n, P) = (r, P)$ であるので，

$$\#\{1 \leq n \leq u | (n, P) = 1\} \leq (u/P + 1)\varphi(P) = (u + P)(1 - 1/p_1) \cdots (1 - 1/p_s)$$

となる．ここで，φ は Euler 関数である．つまり，

$$N(u) \leq M + (u + P)(1 - 1/p_1) \cdots (1 - 1/p_s)$$

である．ここで，$u_0 = \max\{2M/\epsilon, 2P/\epsilon\}$ とすると，$u \geq u_0$ について，

$$\frac{N(u)}{u} \leq \frac{M}{u} + \left(1 + \frac{P}{u}\right)(1 - 1/p_1) \cdots (1 - 1/p_s) \leq \frac{\epsilon}{2} + \left(1 + \frac{\epsilon}{2}\right)\frac{\epsilon}{4} \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

である．したがって，$\lim_{u \to \infty} N(u)/u = 0$，つまり，

$$\lim_{u \to \infty} \frac{T(u)}{u} = 1$$

である． □

最後に，代数体上の漸近的 Fermat 予想と高さ不等式の予想との関係を示しておこう．C を代数体 K 上定義された種数が 2 以上の絶対既約非特異射影曲線とする．$P \in C(\overline{K})$ に対して，$K(P)$ を K 上 P の生成する体を表す時，P の正規化された対数的判別式を

$$d(P) = \frac{1}{[K(P) : \mathbb{Q}]} \log |D_{K(P)/\mathbb{Q}}|$$

で定義する．この時，高さ不等式の予想とは，以下のとうりである．

予想 **3.6.5** (高さ不等式の予想)**.** ある定数 A，B が存在して，任意の $P \in C(\overline{K})$ に対して，

$$h_{\omega_C}(P) \leq Ad(P) + B$$

が成立する．

代数体上の漸近的 Fermat 予想と高さ不等式の予想との関係は次の命題で表せる．

命題 **3.6.6.** もし高さ不等式が F_4 に対して正しければ，代数体上の漸近的 Fermat 予想は成立する．

証明: 命題の証明を始める前に，幾つかのの補題を証明する．

補題 **3.6.7.** K を代数体とし，O_K を K の整数環とする．

(1) 有限個の O_K のイデアル $I_1, \ldots, I_h$ が存在して以下を満たす．任意の分数イデアル Q に対して，ある I_j と $a \in K$ が存在して，$Q = aI_j$ となる．

(2) 次を満たす定数 M_1 が存在する．任意の $x \in \mathbb{P}^n$ に対して，ある $a_0, \ldots, a_n \in O_K$ が存在して，$x = (a_0 : \cdots : a_n)$ であり，

$$\frac{1}{[K:\mathbb{Q}]} \sum_{\sigma \in K(\mathbb{C})} \log \max_i \{|a_i|_\sigma\} \leq h(x) + M_1$$

である．

証明: (1) K の $\mathrm{class\ group}$ が有限群であるので (1) は成り立つ．

(2) まず x を表現する座標 $(x_0 : \cdots : x_n)$ をとる．$Q = O_K x_0 + \cdots + O_K x_n$ は，分数イデアルである．よって，(1) よりあるイデアル I_j と $a \in K$ が存在して $aQ = I_j$ と書ける．ここで，$a_i = ax_i$ とおくと，$a_i \in O_K$ であり，$O_K a_0 + \cdots + O_K a_n = I_j$ である．この時，補題 1.2.4 より，

$$h(x) = -\frac{1}{[K:\mathbb{Q}]} \log\left(\#(O_K/I_j)\right) + \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma \in K(\mathbb{C})} \log \max_i \{|a_i|_\sigma\}$$

である．ゆえに，

$$M_1 = \frac{1}{[K:\mathbb{Q}]} \max_{1 \leq j \leq h} \left\{\log\left(\#(O_K/I_j)\right)\right\}$$

とおけば，(2) が成立する． □

補題 **3.6.8.** K を代数体，K' を K の有限次代数拡大，S を $\mathrm{Spec}(O_K) \setminus \{(0)\}$ の有限集合とする．もし，K' が S の外で K 上不分岐なら，

$$|D_{K'/K}| \leq \prod_{P \in S} \#(O_K/P)^{[K':K]-1} [K' : K]^{[K':\mathbb{Q}]}$$

である．ここで，$D_{K'/K}$ は K' の K 上の判別式である．とくに，$[K:\mathbb{Q}]$ と $[K':K]$ にのみによる定数 M_2 が存在して，

$$\log(|D_{K'/K}|) \leq M_2 \sum_{P\in S} \log(\#(O_K/P))$$

である．

証明: これは，補題 1.8.1 の一般化である．$\mathcal{D}_{K'/K}$ を K' の K 上の共役差積とする．この時，$\#(O_{K'}/\mathcal{D}_{K'/K}) = |D_{K'/K}|$ となる．$P \in S$ で，$PO_{K'} = Q_1^{e_1}\cdots Q_l^{e_l}$ とおく．このとき，補題 1.8.1 と同様にして，

$$\mathrm{ord}_{Q_i}(\mathcal{D}_{K'/K}) \leq e_i - 1 + \mathrm{ord}_{Q_i}(e_i)$$

が成立する．したがって，$a = \#(O_K/P)$ とおき，f_i を P と Q_i の間の剰余体の拡大次数とすると，

$$\log_a \#\left((O_{K'})_P/(\mathcal{D}_{K'/K})_P\right) \leq \sum_i f_i(e_i - 1 + \mathrm{ord}_{Q_i}(e_i)) = \sum_i f_i(e_i - 1 + e_i\,\mathrm{ord}_P(e_i))$$

である．一方，積公式より，$a^{\mathrm{ord}_P(e_i)} \leq e_i^{[K:\mathbb{Q}]}$ であるので，

$$\mathrm{ord}_P(e_i) \leq [K:\mathbb{Q}]\log_a(e_i) \leq [K:\mathbb{Q}]\log_a([K':K])$$

である．よって，

$$\log_a \#\left((O_{K'})_P/(\mathcal{D}_{K'/K})_P\right) \leq [K':K] - 1 + [K':\mathbb{Q}]\log_a([K':K])$$

が成り立つ．つまり，

$$\#\left((O_{K'})_P/(\mathcal{D}_{K'/K})_P\right) \leq \#(O_K/P)^{[K':K]-1}[K':K]^{[K':\mathbb{Q}]}$$

であり，補題を得る． □

さて，命題 3.6.6 の証明に戻ろう．$P \in F_n(K)$，$h(P) > 0$ とする．補題 3.6.1 の (2) より，ある正の数 a が存在して，$h(P) \geq a$ である．また，補題 3.6.7 の (2) により，ある定数 M_1 が存在して，$x,y,z \in O_K$ がとれ，$P = (x:y:z)$ であり，

$$\frac{1}{[K:\mathbb{Q}]}\sum_{\sigma\in K(\mathbb{C})} \log\max\{|x|_\sigma, |y|_\sigma, |z|_\sigma\} \leq h(P) + M_1$$

が成り立つ．$Q = (x^{n/4}:y^{n/4}:z^{n/4})$ とおくと，$Q \in F_4(\overline{\mathbb{Q}})$ である．F_4 に対する高さ不等式より，

$$h_{\omega_{F_4}}(Q) \leq Ad(Q) + B$$

である．ここで，$\omega_{F_4} = \mathcal{O}(1)$ ゆえ，$h_{\omega_{F_4}} = h$ としてよい．したがって，$h_{\omega_{F_4}}(Q) = \frac{n}{4}h(P)$ である．さて，ここで $d(Q)$ を評価しよう．まず，はじめに $\log|D_{K(Q)/K}|$ を考える．$K(Q) \subset K' = K(x^{1/4}, y^{1/4}, z^{1/4})$ である．したがって，$|D_{K(Q)/K}| \leq |D_{K'/K}|$ である．一方，$[K' : K] \leq 4^3$ であるので，補題 3.6.8 より，ある定数 M_2 が存在して，

$$\log|D_{K'/K}| \leq M_2 \sum_{P|xyx} \log \#(O_K/P)$$

である．ゆえに，積公式を用いて，

$$\begin{aligned}
\log|D_{K(Q)/K}| &\leq M_2 \sum_{P|xyx} \log \#(O_K/P) \\
&\leq M_2 \sum_{P} \log \#(O_K/P)^{\mathrm{ord}_P(xyz)} \\
&= M_2 \sum_{\sigma \in K(\mathbb{C})} |xyx|_\sigma \\
&\leq 3M_2 \sum_{\sigma \in K(\mathbb{C})} \max\{|x|_\sigma, |y|_\sigma, |z|_\sigma\} \\
&\leq 3M_2[K : \mathbb{Q}](h(P) + M_1)
\end{aligned}$$

である．ところが，

$$d(Q) = \frac{1}{[K' : \mathbb{Q}]} \log|D_{K(Q)/K}| + \frac{1}{[K : \mathbb{Q}]} \log|D_{K/\mathbb{Q}}|$$

であるので，M_1，M_2 を適当に取り替えると，

$$d(Q) \leq M_2 h(P) + M_1$$

が成立する．よって，

$$\frac{n}{4}h(P) \leq AM_2 h(P) + AM_1 + B$$

が成り立ち，$h(P) \geq a$ に注意すると，

$$\left(\frac{n}{4} - AM_2\right) a \leq AM_1 + B$$

となり，n が十分大きいとこれは矛盾する．　□

参考文献

[1] L. V. Ahlfors, Complex Analysis, McGRAW-HILL.

[2] E, Bombieri, The Mordell Conjecture Revisited, Ann. Scu. Sup. Pisa (1991), 615–640.

[3] B. Edixhoven & J.-H. Evertse, Diophantine Approximation and Abelian Varieties, Lecture Notes in Math., 1566.

[4] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Inv. Math. 73 (1983), 349–366, (English Translation) : Finiteness Theorems for Abelian Varieties over Number fields, Chapter II in 'Arithmetic Geometry' edited by G. Cornell & J. H. Silverman.

[5] ———, Diophantine approximation on abelian varieties, Ann. of Math., 133 (1991), 549–576.

[6] 藤崎源二郎, 体とガロア理論，岩波基礎数学講座

[7] R. Hartshorne, Algebraic Geometry, GTM 52, Springer-Verlag (1977).

[8] ———, Algebraic Number Theory

[9] H. Matsumura, Commutaive Algebra, Mathematics Lecture Note Series, The Benjamin/Cummings Publishing Company, INC., 1980.

[10] D. Mumford, Abelian Varieties, Tata Institute of Foundamental Research, 1970.

[11] ———, Lectures on curves on an algebraic surface, Ann. of Math. Studies, 59, (1966).

[12] P. Riebenboim, Recent results about Fermat's last theorem, Expo. Math. 5 (1987), 75–90.

[13] 高木　貞治,　代数的整数論,　岩波書店

[14] P. Vojta, Siegel's theorem in the compact case, Ann. of Math., 133 (1991), 509–548.

[15] ———, Applications of arithmetic algebraic geometry to Diophantine approximations, Lecture Notes in Math., 1553, 164–208.

記号表・索引

B, 67
$B(X)$, 17
C_{ijk}, 66
$\deg_i(f)$, 38
Δ, 25, 62, 66
δ_1, 67
δ_2, 67
Δ', 27, 62, 66
$\mathcal{D}_K$, 28
$D_{K/\mathbb{Q}}$, 9
$d(P)$, 85
e_i, 35
$F(X)$, 17
$\hat{h}_L(x)$, 22
$h_K(x)$, 12
$h_L(x)$, 17
$h(P)$, 15
$h_\phi(x)$, 16
$h_K^+(x)$, 12
$h^+(P)$, 15
$h(s)$, 68
$h(x)$, 12
$I!$, 35
$\mathrm{ind}_x(P;d)$, 42
$\mathrm{ind}_{(z,z')}(s;(d_1,d_2))$, 62
J, 25, 61
j, 61
$K(\mathbb{C})$, 8, 34
$K(P)$, 85
$L_2(f)$, 38
$\langle x,y\rangle$, 61
$\langle x,y\rangle_K$, 9
$\langle x,y\rangle_L$, 23
$\log^+(a)$, 12
$M(f)$, 38
M_K, 8
$[n]$, 23, 30
$\mathrm{Norm}_{F'/F}(x)$, 47
$N\theta$, 66
$\mathrm{ord}_P(x)$, 7
∂_l, 57
∂^I, 35
∂^I, 35
$\phi_a(x)$, 25
$\Phi_{N\theta}$, 66
$\Phi_{N\theta}^{ij}$, 66
$\Phi_{N\theta}^{ijk}$, 66
Θ, 25
θ, 25, 61, 66
Θ_{g-1}, 25
$V(d_1,d_2,d)$, 62
$|f|$, 38
$|F|_v$, 40
$|I|$, 15, 35
$|I|_d$, 42
$|x|_P$, 7
$|x|_\sigma$, 8
$|x|_v$, 8
$|x|$, 61
$\|x\|_K$, 34
$\mathrm{vol}(M,\langle,\rangle)$, 8
X^I, 15, 38
x_i, 67
x_i', 67
$x\otimes y$, 13
y_i, 67
$\mathbb{Z}_+$, 35

$\mathbb{C}$-value points, 7
Chevalley-Weil **の定理**, 29

Eisenstein の定理の局所版, 55

Gauss の補題, 41

Hermite-Minkowski の定理, 29

Index
  大域切断の —, 62
  多項式の —, 42

Jensen の公式, 40

Mordell-Faltings の定理, 61
Mordell-Weil の定理, 31
  弱 Mordell-Weil の定理, 30

Naive height, 14
Neron-Tate height pairing, 23
Northcott の定理, 20

Poincaré 束, 26

Roth の補題, 43

Siegel の補題, 33

Vojta 因子, 67

アーベル多様体上の直線束
  — が奇, 22
  — が偶, 22

共役差積, 28

射影公式, 52

正規化された対数的判別式, 85
積公式, 10

漸近的 Fermat 予想, 84

大域切断を表現する多項式列, 68
高さ
  Neron-Tate の —, 22
  射影空間の点の —, 13
  — の positivity, 18
  多項式の —, 14
  直線束に付随した —, 17
  標準的な —, 22
  ベクトルの —, 11
高さ不等式の予想, 86
多項式の付値に関する長さ, 40
多変数多項式の Wronskian, 35

代数的整数の自然な内積, 9

テータ因子, 25

内積付き自由加群の体積, 8

ノルム, 46

判別式, 9

付値, 7
  アルキメデス的 —, 7
  自明な —, 7
  正規化された —, 7
  同値な —, 7
  非アルキメデス的 —, 7

ヤコビ多様体, 25

ライプニッツの公式, 57

立方定理, 22