

有理点の複雑さ (ヴェイユ理論を超えて)

— 陳華一氏との共同研究 —

中部大学
森脇 淳

この講演は、陳華一氏との共同研究

Arithmetic intersection theory over adelic curves

の一部です。上の論文は、

“Mémoires de la Société mathématique de France”

に掲載予定です。

1. 序

「複雑な整数は何だろうか？」という問に対する常識的な答えは、桁の大きな整数であると思う。桁の大きな2つの整数の積の計算はうんざりするほどだ。

有理数の場合はどうだろうか？一見、複雑そうな有理数でも既約分数にすれば簡単になることがある。例えば、

$$\frac{2345678}{4691356} = \frac{1}{2}$$

である。既約分数に直す操作はユークリッドの互除法で計算できるので、計算機には大変な仕事にはならない。したがって、有理数の場合は既約分数に直して、分母・分子の桁が大きなものが複雑であるといえる。この既約分数に直すという操作は、射影平面の点と考えるとわかりやすい。つまり、

$$(2345678 : 4691356) = (1 : 2)$$

である。

一般的に、 a と b が互いに素な整数のとき、

$$x = (a/b : 1) = (a : b)$$

になり、 $h(x) = \log \max\{|a|, |b|\}$ と定めて、 h を a/b の高さ、または、 $(a : b)$ の高さと言ふ。

それでは、有理数を係数にもつ多項式の場合はどうであろうか？この場合、複雑な多項式は次数の大きなものと言えるであろう。これは、一つの観点である。この観点で、理論を深めたのが、幾何学的な高さ函数の理論であり、いわゆる古典的な代数幾何と親和性がある。

しながら、1変数の多項式でも、

$$32179712399X + 94974010874$$

は簡単な多項式とよべるかという疑問が生じる。このような観点（次数と係数）で構築する高さ函数の理論をこの講演では紹介したいと思う。応用として、一般化されたフェルマー予想が確率1で正しいことを考えていきたい。

2. 体の絶対値

まずは、体の絶対値について復習しよう。

定義 2.1. K は体とする. 次の性質をもつ $|\cdot|$ を K の絶対値という.

- (i) $|x| \in \mathbb{R}_{\geq 0}$ ($\forall x \in K$) であり, $|x| = 0 \iff x = 0$ である.
- (ii) $|xy| = |x||y|$ ($\forall x, y \in K$)
- (iii) $|x + y| \leq |x| + |y|$ ($\forall x, y \in K$) (三角不等式)

M_K で K の絶対値全体の集合を表すことにする.

$\mathbb{Q}$ の普通の絶対値はその例である. それ以外にも $\mathbb{Q}$ には絶対値がある. $x \in \mathbb{Q}^\times$ に対して, 素数 $p_1, \dots, p_n$ と $e_1, \dots, e_n \in \mathbb{Z} \setminus \{0\}$ が存在して, $x = \pm p_1^{e_1} \cdots p_n^{e_n}$ (素因数分解) と分解できる. 一つ素数 p を固定すると

$$x = \pm p^e \cdot (\text{他の素数の積})$$

となるので, この e を $\text{ord}_p(x)$ とかく. このとき,

$$|x|_p = p^{-\text{ord}_p(x)}$$

と定めると $\mathbb{Q}$ の絶対値を与える. これを $\mathbb{Q}$ の p 進絶対値という. 普通の絶対値は $|\cdot|_\infty$ とかく. 多くの p 冪の因子をもっているとき $|x|_p$ は小さくなる.

さらに, $x = \pm p_1^{e_1} \cdots p_n^{e_n} \in \mathbb{Q}^\times$ とすると,

$$\log |x|_\infty + \sum_{p \text{ は素数}} \log |x|_p = \log p_1^{e_1} \cdots p_n^{e_n} + \sum_{i=1}^n \log p_i^{-e_i} = 0$$

つまり, $\Omega_{\mathbb{Q}} = \{\infty\} \cup \{p \mid p \text{ は素数}\}$ とおくと,

$$\sum_{\omega \in \Omega_{\mathbb{Q}}} \log |x|_\omega = 0$$

である. したがって, $\Omega_{\mathbb{Q}}$ に $\nu(\{\omega\}) = 1$ となる離散的な測度 ν を与えると,

$$\int_{\Omega_{\mathbb{Q}}} \log |x|_\omega \nu(d\omega) = 0$$

が成立する. 以上のことは, 体のアデリック構造の概念につながる.

3. 体のアデリック構造

アデリック構造は, この講演の中心的概念である.

定義 3.1. 体 K のアデリック構造 $S = (K, (\Omega, \mathcal{A}, \nu), \phi)$ とは以下を充たすものである.

- (1) $(\Omega, \mathcal{A}, \nu)$ は測度空間である. つまり, $\mathcal{A}$ は Ω の σ -代数であり, ν は可測空間 $(\Omega, \mathcal{A})$ 上の測度である.
 - (2) 最後の ϕ は, Ω から M_K への写像である. ここで, M_K は K の絶対値の集合である. $\omega \in \Omega$ に対して, 絶対値 $\phi(\omega)$ を $|\cdot|_\omega$ とかくことにする.
 - (3) $a \in K^\times$ に対して, Ω 上の函数 $(\omega \in \Omega) \mapsto \log |a|_\omega \in \mathbb{R}$ は ν -可積分である.
- データ S を アデリック曲線 とよぶ. さらに, 任意の $a \in K^\times$ に対して,

$$(3.1) \quad \int_{\Omega} \log |a|_\omega \nu(d\omega) = 0$$

を充たすとき, S は固有であるという. 式 (3.1) を積公式とよぶ. また, $|\cdot|_\omega$ に関する K の完備化を K_ω と表すことにする.

例 3.2. 任意の体 K は K 自明な絶対値 $|\cdot|_{K,0}$ により, アデリック構造を持つ. つまり, $|x|_{K,0} = 1$ ($x \in K^\times$), $|0|_{K,0} = 0$ で与えられる.

例 3.3. K は代数体とし,

$$\Omega := \{|\cdot| \in M_K \setminus \{|\cdot|_{K,0}\} \mid |\cdot| \text{ は } \mathbb{Q} \text{ 上で標準的}\},$$

とおく. つまり,

$$|\cdot|_{\mathbb{Q}} = \begin{cases} |\cdot|_{\infty}, & \text{もし } |\cdot| \text{ はアルキメデスの,} \\ |\cdot|_p, & \text{もし } |\cdot| \text{ が非アルキメデスの} \\ \{x \in \mathbb{Z} \mid |x| < 1\} = p\mathbb{Z} \end{cases}$$

$(\Omega, \mathcal{A})$ は離散的な可測空間で, $\nu(\{\omega\}) = [K_{\omega} : \mathbb{Q}_{\omega}] / [K : \mathbb{Q}]$.

例 3.4. X は体 k 上の e -次元の正規射影代数多様体で, K は X の函数体とする. Ω は X 上の素因子全体の集合で, $(\Omega, \mathcal{A})$ は離散的な可測空間とする. X 上のネフな直線束 $H_1, \dots, H_{e-1}$ を固定する.

$$\nu(\{\omega\}) = (H_1 \cdots H_{e-1} \cdot \Gamma_{\omega})$$

とおく. ここで, Γ_{ω} は ω に対応する素因子である.

ここまでのすべての例は固有である. 以後, S は固有であると仮定する.

$$(x_0, \dots, x_n) \in K^{n+1} \setminus \{(0, \dots, 0)\}$$

に対して, $h_S(x_0, \dots, x_n)$ を

$$h_S(x_0, \dots, x_n) := \int_{\Omega} \log \max\{|x_0|_{\omega}, \dots, |x_n|_{\omega}\} \nu(d\omega).$$

と定める. 積公式 (3.1) により, 写像

$$h_S : K^{n+1} \setminus \{(0, \dots, 0)\} \rightarrow \mathbb{R}$$

は $\mathbb{P}^n(K) \rightarrow \mathbb{R}$ に降下する. 言葉の乱用で, これを $h_S(x_0 : \dots : x_n)$ とかくことにし, S に関する $(x_0 : \dots : x_n)$ の高さとよぶ.

さらに, S がノースcott性をもつとは, 任意の $C \in \mathbb{R}$ に対して, 集合

$$\{a \in K \mid h_S(a : 1) \leq C\}$$

が有限であるときにいう.

命題 3.5. もし S がノースcott性をもつとき, 集合

$$\{(x_0 : \dots : x_n) \in \mathbb{P}^n(K) \mid h_S(x_0 : \dots : x_n) \leq C\}.$$

は, 任意の $C \in \mathbb{R}$ について, 有限である. 特に, 集合

$$\{h_S(x_0 : \dots : x_n) \mid (x_0 : \dots : x_n) \in \mathbb{P}^n(K)\}$$

は離散的である.

証明. $x_i \neq 0$ のとき,

$$\int_{\Omega} \log \max\{|x_j/x_i|_{\omega}, 1\} \nu(d\omega) = h_S(x_i : x_j) \leq h_S(x_0 : \dots : x_n)$$

が, すべての $j = 0, \dots, n$ で成り立つ. また,

$$\begin{aligned} & \{(x_0 : \dots : x_n) \in \mathbb{P}^n(K) \mid h_S(x_0 : \dots : x_n) \leq C\} \\ &= \bigcup_{i=0}^n \{(x_0 : \dots : x_n) \in \mathbb{P}^n(K) \mid x_i \neq 0, h_S(x_0 : \dots : x_n) \leq C\} \end{aligned}$$

である. したがって, 命題が従う. $\square$

$S = (K, (\Omega_K, \mathcal{A}_K, \nu_K), \phi_K)$ はアデリック曲線とする. L/K は分離的な代数拡大とする. $\omega \in \Omega_K$ に対して, K 上の $|\cdot|_\omega$ を拡張した L の絶対値全体を $M_{L,\omega}$ で表す. Ω_L を以下のように $M_{L,\omega}$ の非交和 (disjoint union) として定める.

$$\Omega_L := \coprod_{\omega \in \Omega_K} M_{L,\omega}.$$

このとき, $M_{L,\omega}$ の元を ω に送ることによる射影

$$\pi_{L/K} : \Omega_L \rightarrow \Omega_K$$

が定まる. また, $\phi_L : \Omega_L \rightarrow M_L$ は包含写像 $M_{L,\omega} \rightarrow M_L$ により定まる写像とする. x が Ω_L の元とき, 対応する L の絶対値を $|\cdot|_x$ と表すことにする.

次の図式は可換である.

$$\begin{array}{ccc} \Omega_L & \xrightarrow{\pi_{L/K}} & \Omega_K \\ \phi_L \downarrow & & \downarrow \phi_K \\ M_L & \xrightarrow{\text{rest}_{L/K}} & M_K \end{array}$$

ここで, $\text{rest}_{L/K}$ は L の絶対値を K の絶対値への制限である. さらに, Ω_L は集合のカテゴリーにおける M_K 上の M_L と Ω_K ファイバー積

$$\Omega_K \times_{M_K} M_L := \{(\omega, x) \in \Omega_K \times M_L \mid \phi_K(\omega) = \text{rest}_{L/K}(x)\}$$

と同一視できる.

以後, L/K は有限次と仮定する. Ω_L には $\pi_{L/K}$ と任意の $a \in L$ に対して実関数 $(x \in \Omega_L) \mapsto |a|_x$ が可測となる最小の σ -代数 $\mathcal{A}_L$ を与える. ここで, Ω_K 上では σ -代数 $\mathcal{A}_K$ を, $\mathbb{R}$ ではボレル σ -代数を考えている.

$\omega \in \Omega_K$ に対して, $M_{L,\omega}$ 上に離散的な可測空間を与え, 測度 $\mathbb{P}_{L,\omega}$ を

$$\mathbb{P}_{L,\omega}(\{x\}) = \frac{[L_x : K_\omega]}{[L : K]},$$

と定める. このとき, $\mathbb{P}_{L,\omega}$ は $M_{L,\omega}$ 上の確率測度である. というのは,

$$[L : K] = \sum_{x \in M_{L,\omega}} [L_x : K_\omega]$$

となるからである.

定理 3.6. Ω_L 上の可測な実数値関数 f に対して,

$$(\omega \in \Omega_K) \mapsto \int_{M_{L,\omega}} f d\mathbb{P}_{L,\omega}$$

は $\mathcal{A}_K$ -可測である.

定義 3.7. $\nu_L : \mathcal{A}_L \rightarrow \mathbb{R}_+ \cup \{+\infty\}$ を

$$\forall B \in \mathcal{A}_L, \quad \nu_L(B) := \int_{\Omega_K} \left(\int_{M_{L,\omega}} \mathbf{1}_B d\mathbb{P}_{L,\omega} \right) d\nu_K.$$

と定める. 定理 3.6 より, この写像はうまく定義されており, $(\Omega_L, \mathcal{A}_L)$ 上の測度を定める. $S_L = (L, (\Omega_L, \mathcal{A}_L, \nu_L), \phi_L)$ とおき, S_L は $S \otimes_K L$ と記されることがある.

命題 3.8. S が固有であるとき, S_L も固有である. さらに, S がノースcott性をもつならば, S_L もノースcott性をもつ.

一般的な場合, つまり, L は K 上代数的で分離的である場合は, 省略するが, カラテオドリの定理 (または, ホップの拡張定理) を用いることにより, 構築される.

4. 可算濃度の体のアデリック構造

まずは, $\mathbb{Q}$ 上可算超越次数の純超越拡大のアデリック構造を考える.

I は高々可算濃度の集合とする. 0 は I の元でないと仮定する. 次の補題から始めよう. 証明は難しくないので省略する.

補題 4.1. $\mathcal{A}_{[0,1]^I}$ と $\nu_{[0,1]^I}$ は $[0,1]^I$ 上の直積位相から定まるボレル σ -代数と標準的なボレル測度とする.

- (1) $(e^{2\pi\sqrt{-1}t_i})_{i \in I}$ が代数的に独立である $(t_i)_{i \in I} \in [0,1]^I$ からなる集合を Ω_∞ と表す. このとき, Ω_∞ は $[0,1]^I$ ボレル部分集合で, $\nu_{[0,1]^I}(\Omega_\infty) = 1$ となる. 特に, Ω_∞ は $[0,1]^I$ のなかで稠密である.
- (2) ゼロでない $\mathbb{C}[(X_i)_{i \in I}]$ の元である多項式に対して, $[0,1]^I$ 上の函数

$$\log |f((e^{2\pi\sqrt{-1}t_i})_{i \in I})|$$

は可積分である.

$f \in \mathbb{C}[(X_i)_{i \in I}]$ に対して, $\mathcal{M}(f)$ を以下のように定める.

$$\mathcal{M}(f) := \begin{cases} 0 & \text{もし } f = 0 \text{ なら,} \\ \exp \left(\int_{[0,1]^I} \log |f((e^{2\pi\sqrt{-1}t_i})_{i \in I})| d\nu_{[0,1]^I} \right) & \text{そうでない場合.} \end{cases}$$

$\mathcal{M}(f)$ は f の係数の大きさを計っている数である. このとき, 以下が成り立つ.

命題 4.2. (1) $f \in \mathbb{Z}[(X_i)_{i \in I}] \setminus \{0\}$ ならば, $\mathcal{M}(f) \geq 1$.

(2) I は有限のとき, 任意の d と C に対して,

$$\left\{ f \in \mathbb{Z}[(X_i)_{i \in I}] \mid \mathcal{M}(f) \leq C \text{ かつ } \deg(f) \leq d \right\}$$

は有限である.

• $\mathbb{Q}^\times$ による積を法としての $\mathbb{Q}[Z_0, (Z_i)_{i \in I}]$ の既約多項式全体を Ω_h で表す. $i \in I$ に対して, $X_i := Z_i/Z_0$ とおく. $\omega \in \Omega_h$ に対して, P_ω で対応する既約多項式を表すことにする. P_ω は $\mathbb{Z}[Z_0, (Z_i)_{i \in I}]$ の元で, 原始的であると仮定してよい. P_ω は ± 1 の積を除いて, 一意的に定まる.

$$p_\omega := P_\omega(1, (X_i)_{i \in I}) \in \mathbb{Z}[(X_i)_{i \in I}]$$

とおく.

ω_0 で, 既約多項式 Z_0 を表すことにする. すなわち, $P_{\omega_0} = Z_0$ である. $\mathbb{Q}((X_i)_{i \in I})$ 上で $\text{ord}_{\omega_0}(\cdot)$ は $-\deg(\cdot)$ に他ならない. つまり,

$$\text{ord}_{\omega_0}(f) = \text{ord}_{Z_0}(f((Z_i/Z_0)_{i \in I})) = -\deg(f).$$

さらに, $\omega \in \Omega_h \setminus \{\omega_0\}$ に対して, $\deg(P_\omega) = \deg(p_\omega)$ である.

$\lambda \in \mathbb{R}_{\geq 0}$ を固定する. $\omega \in \Omega_h$ に対して, $\mathbb{Q}(X_1, \dots, X_n)$ 上の非アルキメデスの絶対値 $|\cdot|_\omega$ を

$$|f|_\omega := (\exp(\lambda \deg(P_\omega)) \mathcal{M}(P_\omega(1, X_1, \dots, X_n)))^{-\text{ord}_\omega(f)}$$

と定義する. ここで, $f \in \mathbb{Q}((X_i)_{i \in I})$ である. $|f|_{\omega_0} = \exp(\lambda)^{\deg(f)}$ である.

Ω_v で, $\mathbb{Z}$ の素数全体を表すことにする. $p \in \Omega_v$ に対して, $|\cdot|_p$ は $\mathbb{Z}$ の $|p|_p = 1/p$ を充たす p -進絶対値を表すことにする. $f = \sum_{T \in \mathbb{Z}_{\geq 0}^I} a_T X^T \in \mathbb{Q}[(X_i)_{i \in I}]$ に対して,

$$|f|_p = \max_{T \in \mathbb{Z}_{\geq 0}^I} \{ |a_T|_p \}$$

とおくと, ガウスの補題より, $|fg|_p = |f|_p |g|_p$ が成り立つ. したがって, $\mathbb{Q}((X_i)_{i \in I})$ 上の絶対値に拡張する.

$\Omega_{\text{fin}} := \Omega_h \coprod \Omega_v$ とおく. 測度空間 $(\Omega_{\text{fin}}, \mathcal{A}_{\text{fin}}, \nu_{\text{fin}})$ は離散的な測度空間とし, $\nu_{\text{fin}}(\{\omega\}) = 1$ がすべての $\omega \in \Omega_{\text{fin}}$ が成り立つものとする.

- 以前と同様に, Ω_∞ は,

$$(e^{2\pi\sqrt{-1}t_i})_{i \in I}$$

が $\mathbb{Q}$ 上代数的に独立となる $(t_i)_{i \in I} \in [0, 1]^I$ からなる部分集合とする. 補題 4.1 より, Ω_∞ は $[0, 1]^I$ の稠密なボレル集合で, $\nu_{[0, 1]^I}(\Omega_\infty) = 1$ を充たす. $t = (t_i)_{i \in I} \in \Omega_\infty$ に対して, $|f|_t$ を

$$|f|_t := \left| f((e^{2\pi\sqrt{-1}t_i})_{i \in I}) \right|_{\mathbb{C}}$$

を定める. ここで, $|\cdot|_{\mathbb{C}}$ は $\mathbb{C}$ の普通の絶対値である. 測度空間 $(\Omega_\infty, \mathcal{A}_\infty, \nu_\infty)$ は, ボレル σ -代数 $\mathcal{A}_{[0, 1]^I}$ とボレル測度 $\nu_{[0, 1]^I}$ の Ω_∞ への制限とする.

定義 4.3. $\mathbb{Q}((X_i)_{i \in I})$ のアデリック構造は

$$(\Omega_{\text{fin}}, \mathcal{A}_{\text{fin}}, \nu_{\text{fin}}) \coprod (\Omega_\infty, \mathcal{A}_\infty, \nu_\infty)$$

と定め, $\Sigma_{I, \lambda}$ と表す.

定理 4.4. (1) $\Sigma_{I, \lambda}$ は固有的である. つまり,

$$\sum_{\omega \in \Omega_{\text{fin}}} \log |f|_\omega + \int_{\Omega_\infty} \log |f|_t dt = 0$$

が, すべての $f \in \mathbb{Q}((X_i)_{i \in I})^\times$ で成り立つ.

(2) I が有限で, $\lambda > 0$ のとき, $\Sigma_{I, \lambda}$ はノースcott性をもつ.

定理 4.4 の証明. (1) $\mathbb{Z}[(X_i)_{i \in I}]$ は UFD であるので, $a \in \mathbb{Q}$ が存在して,

$$f = a \cdot \prod_{\omega \in \Omega_h \setminus \{\omega_0\}} p_\omega^{\text{ord}_\omega(f)}$$

と表せる。したがって、

$$\begin{aligned}
\sum_{\omega \in \Omega_{\text{fin}}} \log |f|_{\omega} &= \sum_{\omega \in \Omega_h \setminus \{\omega_0\}} -\text{ord}_{\omega}(f)(\lambda \deg(p_{\omega}) + \log \mathcal{M}(p_{\omega})) \\
&\quad + \lambda \deg(f) + \sum_{p \in \Omega_v} -\text{ord}_p(a) \log p \\
&= \sum_{\omega \in \Omega_h \setminus \{\omega_0\}} -\text{ord}_{\omega}(f) \log \mathcal{M}(p_{\omega}) + \sum_{p \in \Omega_v} -\text{ord}_p(a) \log p \\
&= - \int_{[0,1]^n} \log |f((e^{2\pi\sqrt{-1}t_i})_{i \in I})| d\nu_{[0,1]^I}
\end{aligned}$$

となる。

一方、補題 4.1 により、 $[0,1]^I \setminus \Omega_{\infty}$ は測度がゼロのボレル部分集合であるので、

$$\begin{aligned}
\int_{\Omega_{\infty}} \log |f|_t d\nu_{\infty} &= \int_{\Omega_{\infty}} \log |f((e^{2\pi\sqrt{-1}t_i})_{i \in I})| d\nu_{\infty} \\
&= \int_{[0,1]^I} \log |f((e^{2\pi\sqrt{-1}t_i})_{i \in I})| d\nu_{[0,1]^I},
\end{aligned}$$

となり、固有である。

(2) $I = \{1, \dots, n\}$ とおく。集合 $\{f \in \mathbb{Q}(X_1, \dots, X_n) \mid h_{\Sigma_{I,\lambda}}(1 : f) \leq C\}$ が任意の C について有限であることを示せばよい。 $f_1, f_2 \in \mathbb{Z}[X_1, \dots, X_n]$ は、 $f = f_2/f_1$ となり、 f_1 と f_2 は $\mathbb{Z}[X_1, \dots, X_n]$ で共通成分を持たないものをとる。このとき、(1) により、

$$\begin{aligned}
h_{\Sigma_{I,\lambda}}(1 : f) &= h_{\Sigma_{I,\lambda}}(f_1 : f_2) = \lambda \max\{\deg(f_1), \deg(f_2)\} \\
&\quad + \int_{[0,1]^n} \log \max\{|f_1(e^{2\pi it_1}, \dots, e^{2\pi it_n})|, \\
&\quad |f_2(e^{2\pi it_1}, \dots, e^{2\pi it_n})|\} dt_1 \cdots dt_n
\end{aligned}$$

であるので、もし $h_{\Sigma_{I,\lambda}}(1 : f) \leq C$ ならば

$$\max\{\log \mathcal{M}(f_1), \log \mathcal{M}(f_2)\} + \lambda \max\{\deg(f_1), \deg(f_2)\} \leq C$$

である。

命題 4.2 の (1) により、 $\max\{\log \mathcal{M}(f_1), \log \mathcal{M}(f_2)\} \geq 0$ である。したがって、

$$\max\{\deg(f_1), \deg(f_2)\} \leq C/\lambda, \text{ かつ } \max\{\log \mathcal{M}(f_1), \log \mathcal{M}(f_2)\} \leq C$$

である。よって、(2) は命題 4.2 の (2) から従う。 $\square$

定理 4.5. K は標数 0 で可算濃度をもつ体とする。このとき、以下の性質をもつ K のアデリック構造 $S = (\Omega, \mathcal{A}, \nu)$ が存在する。

(1) S は固有である。

(2) K_0 は K の部分体で、 $\mathbb{Q}$ 上有限生成であるとする、集合

$$\left\{ a \in K \mid \int_S \log \max\{|a|_{\omega}, 1\} d\nu \leq C \text{ かつ } [K_0(a) : K_0] \leq \delta \right\}$$

は、任意 C と δ について、有限である。

定理 4.5 の証明. 高々可算濃度をもつ集合 I と $(X_i)_{i \in I} \in K^I$ が存在して, $(X_i)_{i \in I}$ は $\mathbb{Q}$ 上代数的独立であり, K は $\mathbb{Q}((X_i)_{i \in I})$ 上代数的になるように取れる.

$\lambda > 0$ を固定する. $\Sigma_{I,\lambda}$ は, 定義 4.3 に記述されているアデリック構造とする. K は $\mathbb{Q}((X_i)_{i \in I})$ 代数的であるので, S は $\Sigma_{I,\lambda}$ から K への自然な拡張とする.

(1): 構成法から, (1) は自明である.

(2): I の有限部分集合 I' により, $K_0 = \mathbb{Q}((X_i)_{i \in I'})$ と与えられた場合, 定理 4.4 の (2) により, $\Sigma_{I',\lambda}$ はノースcott性をもつので, その主張は自明である.

$K_0 = \mathbb{Q}(\theta_1, \dots, \theta_\ell)$ とおく. K は $\mathbb{Q}((X_i)_{i \in I})$ 上代数的であるので, I の有限の部分集合 I' が存在して, $\theta_1, \dots, \theta_\ell$ は $\mathbb{Q}((X_i)_{i \in I'})$ 上代数的である. したがって, $K_0((X_i)_{i \in I'})$ は $\mathbb{Q}((X_i)_{i \in I'})$ 上有限次元である.

$a \in K$ に対して,

$$\begin{aligned} [\mathbb{Q}((X_i)_{i \in I'})(a) : \mathbb{Q}((X_i)_{i \in I'})] &\leq [K_0((X_i)_{i \in I'})(a) : \mathbb{Q}((X_i)_{i \in I'})] \\ &= [K_0((X_i)_{i \in I'})(a) : K_0((X_i)_{i \in I'})][K_0((X_i)_{i \in I'}) : \mathbb{Q}((X_i)_{i \in I'})] \\ &\leq [K_0(a) : K_0][K_0((X_i)_{i \in I'}) : \mathbb{Q}((X_i)_{i \in I'})], \end{aligned}$$

であることに注意すると, (2) にある集合は

$$\left\{ a \in K \left| \begin{array}{l} \int_S \log \max\{|a|_\omega, 1\} \leq C \text{ かつ} \\ [\mathbb{Q}((X_i)_{i \in I'})(a) : \mathbb{Q}((X_i)_{i \in I'})] \leq \delta [K_0((X_i)_{i \in I'}) : \mathbb{Q}((X_i)_{i \in I'})] \end{array} \right. \right\},$$

の部分集合であるので, 題意を得る. $\square$

5. 一般化されたフェルマー予想

K は $\mathbb{Q}$ 上有限生成な体とする. このような体を算術的函数体とよぶ.

オリジナルなフェルマー予想と同様に, 算術的函数体 K に対して, N が十分に大きければ, $x^N + y^N = 1$ ($x, y \in K$) は $xy = 0$ を導くかという問は考えられるが, これは, よい予想とは言えない. 実際, $e^{\pi i/3}, e^{-\pi i/3} \in K$ と仮定し, $x = e^{\pi i/3}$ と $y = e^{-\pi i/3}$ と置くと, $x + y = 1$, $x^6 = y^6 = 1$, $x^5 = y$, $y^5 = x$ となる. したがって, $N \equiv 1, 5 \pmod{6}$ となる N について, $x^N + y^N = 1$ かつ $xy \neq 0$ である. もう少し筋のよい予想を考えてみたい.

$\mu(K)$ で K に含まれる 1 の冪根の集合を表すことにする. つまり,

$$\mu(K) = \{x \in K \mid x^n = 1 \text{ となる } n \in \mathbb{Z}_{\geq 1} \text{ が存在する}\}.$$

である. $f \in K[X, Y, Z]$ をゼロでない同次多項式とする. 正の整数 N に対して, $f_N(X, Y, Z) = f(X^N, Y^N, Z^N)$ と定める. さらに,

$$F_N = \text{Proj}(K[X, Y, Z]/f_N(X, Y, Z)).$$

と定める. f が強い意味で非特異的であるとは, F_N がすべての N で非特異であるときと定める.

例 5.1. (1) $f = \alpha X + \beta Y + \gamma Z$ ($\alpha, \beta, \gamma \in K^\times$) は強い意味で非特異的.

(2) f は対称行列 $\begin{pmatrix} a & d & e \\ d & b & s \\ e & s & c \end{pmatrix}$ から定まる 2 次の同次式とする.

$$\det \begin{pmatrix} a & d & e \\ d & b & s \\ e & s & c \end{pmatrix} \neq 0 \text{ かつ } \det \begin{pmatrix} b & s \\ s & c \end{pmatrix} \neq 0 \text{ かつ } \det \begin{pmatrix} a & e \\ e & c \end{pmatrix} \neq 0 \text{ かつ } \det \begin{pmatrix} a & d \\ d & b \end{pmatrix} \neq 0$$

のとき, f は強い意味で非特異的.

(3) $f = \alpha X^3 + \beta Y^3 + \gamma Z^3 - 3\lambda XYZ$ ($\alpha\beta\gamma \neq 0$ かつ $\lambda^3 \neq \alpha\beta\gamma$) は強い意味で非特異的.

以後, f は強い意味で非特異的であると仮定する. F_N が K 上のフェルマー性をもつとは, $f_N(x, y, z) = 0$ かつ $(x, y, z) \in K^3 \setminus \{(0, 0, 0)\}$ であるとき, ある $t \in K^\times$ が存在して, $tx, ty, tz \in \{0\} \cup \mu(K)$ となる時にいう.

算術的函数体上の一般化されたフェルマー予想を考えたい.

予想 5.2 (算術的函数体上の一般化されたフェルマー予想). ある N_0 が存在して, $N \geq N_0$ に対して, F_N はフェルマー性をもつか?

補題 5.3. $(a_0 : \dots : a_n) \in \mathbb{P}^n(K)$ に対して, 以下は同値.

- (1) $h_S(a_0 : \dots : a_n) = 0$.
- (2) $t \in K^\times$ が存在して, $ta_i \in \{0\} \cup \mu(K)$ ($i = 0, \dots, n$) である.

証明. (1) $\implies$ (2): $a_0 = 1$ と仮定しても一般性を失わない.

$$h_S(a_0^N : \dots : a_n^N) = Nh_S(a_0 : \dots : a_n) = 0$$

であることに注意すると, ノースcott性から, 集合

$$\{(a_1^N, \dots, a_n^N) \mid N \in \mathbb{Z}_{\geq 1}\}$$

は有限である. よって, $N < N'$ かつ $(a_1^N, \dots, a_n^N) = (a_1^{N'}, \dots, a_n^{N'})$ となる $N, N' \in \mathbb{Z}_{\geq 1}$ が存在する. これは, $a_i \in \{0\} \cup \mu(K)$ を示す.

(2) $\implies$ (1) は自明. □

補題 5.4. S は $\mathbb{P}^n(K)$ の有限集合とし,

$$\begin{cases} H = \max\{h_S(x) \mid x \in S\}, \\ a = \inf\{h_S(x) \mid x \in \mathbb{P}^n(K) \text{ かつ } h_S(x) > 0\} \end{cases}$$

とおく. このとき, $a > 0$ であり, $am > H$ となる任意の整数 m について, $(x_0^m : \dots : x_n^m) \in S$ ならば $h_S(x_0 : \dots : x_n) = 0$ となる.

証明. 命題 3.5 から $a > 0$ である. $h_S(x_0 : \dots : x_n) > 0$ と仮定する. このとき,

$$H \geq h_S(x_0^m : \dots : x_n^m) = mh_S(x_0 : \dots : x_n) \geq ma,$$

となるので, 矛盾である. □

定理 5.5. 算術的函数体上の一般化されたフェルマー予想は確率 1 で正しい. つまり,

$$\lim_{m \rightarrow \infty} \frac{\#\{N \in \mathbb{Z} \mid 1 \leq N \leq m \text{ かつ } F_N \text{ はフェルマー性をもつ}\}}{m} = 1.$$

証明. p は 5 以上の素数とする. F_p の種数は 2 以上であるので, ファルティングスの定理 (算術的函数体上で定義された代数曲線の種数が 2 以上であればその有理点は有限である) により, $F_p(K)$ は有限である. $(x : y : z) \in F_{pm}$ なら $(x^m : y^m : z^m) \in F_p$ であることに注意すると,

$$m > \frac{\max\{h_S(x) \mid x \in F_p(K)\}}{\inf\{h_S(x) \mid x \in \mathbb{P}^2(K) \text{ and } h_S(x) > 0\}}$$

ならば, 補題 5.4 より, $h_S(x : y : z) = 0$ である. ゆえに, 補題 5.3 により, F_{pm} はフェルマー性をもつ. したがって, 以下の補題 5.7 から, 定理が従う. □

注意 5.6. $K = \mathbb{Q}$ かつ $f = X + Y - Z$ の場合は, M. Filaseta, A. Granville, D. R. Heath-Brown による.

補題 5.7. T は $\mathbb{Z}_{\geq 1}$ の部分集合であり, ある正の整数 p_0 が存在して, p_0 より大きな素数 p に対して, $m_p \in \mathbb{Z}_{\geq 1}$ を見つけることができ, $p\mathbb{Z}_{\geq m_p} \subseteq T$ となると仮定する. このとき,

$$\lim_{m \rightarrow \infty} \frac{T \cap [1, m]}{m} = 1$$

である.

証明. リーマン・ゼータ関数は 1 で極をもつので, 任意の $0 < \epsilon < 1$ に対して, $p_0 < p_1 < \dots < p_r$ で $\prod_{i=1}^r (1 - 1/p_i) \leq \epsilon$ となる素数 $p_1, \dots, p_r$ が存在する. よって, 仮定より, $Q = p_1 \dots p_r$ とおくと,

$$\{n \in \mathbb{Z}_{\geq 1} \mid n \geq n_0 \text{ かつ } \text{GCD}(Q, n) \neq 1\} \subseteq T,$$

となる $n_0 \in \mathbb{Z}_{\geq 1}$ が存在する. つまり,

$$\mathbb{Z}_{\geq 1} \setminus T \subseteq \{n \in \mathbb{Z}_{\geq 1} \mid n < n_0\} \cup \{n \in \mathbb{Z}_{\geq 1} \mid \text{GCD}(Q, n) = 1\},$$

である. ゆえに,

$$\#((\mathbb{Z}_{\geq 1} \setminus T) \cap [1, m]) \leq (n_0 - 1) + \#\{1 \leq n \leq m \mid \text{GCD}(Q, n) = 1\}.$$

となる. $\#\{1 \leq n \leq Q \mid \text{GCD}(Q, n) = 1\}$ はオイラー数 $\varphi(Q)$ に等しいので,

$$\begin{aligned} \#\{1 \leq n \leq m \mid \text{GCD}(Q, n) = 1\} &\leq (m/Q + 1)\varphi(Q) \\ &= (m + Q)(1 - 1/p_1) \dots (1 - 1/p_r) \leq (m + Q)\epsilon. \end{aligned}$$

を得る. したがって, $m \geq \max\{(n_0 - 1)/\epsilon, Q/\epsilon\}$ のとき,

$$\begin{aligned} 1 \geq \frac{\#(T \cap [1, m])}{m} &= 1 - \frac{\#((\mathbb{Z}_{\geq 1} \setminus T) \cap [1, m])}{m} \geq 1 - \frac{(n_0 - 1) + (m + Q)\epsilon}{m} \\ &= 1 - \left(\frac{n_0 - 1}{m} + \left(1 + \frac{Q}{m}\right)\epsilon \right) \\ &\geq 1 - (\epsilon + (1 + \epsilon)\epsilon) \geq 1 - 3\epsilon, \end{aligned}$$

である. □

注意 5.8. $f = \alpha X + \beta Y + \gamma Z$ ($\alpha, \beta, \gamma \in \mathbb{Q}^\times$) の場合, abc 予想より, 一般化されたフェルマー予想が成立することが以下のようにしてわかる.

$\alpha, \beta, \gamma \in \mathbb{Z} \setminus \{0\}$ と仮定してもよい. $(x, y, z) \in \mathbb{Q}^3 \setminus \{(0, 0, 0)\}$ が存在して,

$$\alpha x^N + \beta y^N + \gamma z^N = 0 \quad \text{かつ} \quad h(x, y, z) > 0$$

であると仮定する. $x, y, z \in \mathbb{Z}$ かつ $\text{GCD}(x, y, z) = 1$ であると仮定してよい. したがって, $h(x, y, z) = \log \max\{|x|, |y|, |z|\} > 0$ である. つまり, $t := \max\{|x|, |y|, |z|\} \geq 2$ となる. ここで, $A = \alpha x^N$, $B = \beta y^N$, $C = \gamma z^N$ とおく.

$$N \geq \max_{p \text{ は素数}} \left\{ \max\{\text{ord}_p(\alpha), \text{ord}_p(\beta), \text{ord}_p(\gamma)\} \right\} + 1.$$

のとき, 以下が成り立つことを見よう.

- (1) $xyz \neq 0$.
- (2) $G = \text{GCD}(A, B, C)$ とおくと, $G \mid \text{LCM}(\alpha, \beta, \gamma)$ となる.

(1): $x = 0$ と仮定する. このとき, $\beta y^N = -\gamma z^N$ であり, y と z は互いに素であるので, $\beta = \beta' z^N, \gamma = -\gamma' y^N$ ($\beta', \gamma' \in \mathbb{Z}$) とおける. $\max\{|y|, |z|\} \geq 2$ であるので, ある素数 p が存在して, $\text{ord}_p(y) \geq 1$ または $\text{ord}_p(z) \geq 1$ である. 一方,

$$\text{ord}_p(\beta) \geq N \text{ord}_p(z) \quad \text{かつ} \quad \text{ord}_p(\gamma) \geq N \text{ord}_p(y)$$

であるので, $\text{ord}_p(\beta) \geq N$ または $\text{ord}_p(\gamma) \geq N$ が成り立ち, N の取り方に矛盾する. $y = 0$ または $z = 0$ の場合も同様である.

(2): p は素数とする. $\text{GCD}(x, y, z) = 1$ であるので,

$$\begin{aligned} & \min\{\text{ord}_p(A), \text{ord}_p(B), \text{ord}_p(C)\} \\ &= \min\{\text{ord}_p(\alpha) + N \text{ord}_p(x), \text{ord}_p(\beta) + N \text{ord}_p(y), \text{ord}_p(\gamma) + N \text{ord}_p(z)\} \\ &\leq \max\{\text{ord}_p(\alpha), \text{ord}_p(\beta), \text{ord}_p(\gamma)\}, \end{aligned}$$

となる. したがって, 主張を得る.

ここで, 2 種類の abc 予想を考えよう.

(I) 任意の $\epsilon > 0$ に対して, $\kappa(\epsilon) \in \mathbb{R}_{>0}$ が存在して, $a + b + c = 0$ かつ $abc \neq 0$ かつ $\text{GCD}(a, b, c) = 1$ となる $a, b, c \in \mathbb{Z}$ について,

$$\max\{|a|, |b|, |c|\} < \kappa(\epsilon)(\text{rad}(abc))^{1+\epsilon}$$

が成り立つ. ここで, $\text{rad}(D) = \prod_{p \text{ は } p|D \text{ となる素数}} p$ である.

(II) $a + b + c = 0$ かつ $abc \neq 0$ かつ $\text{GCD}(a, b, c) = 1$ となる $a, b, c \in \mathbb{Z}$ について,

$$\max\{|a|, |b|, |c|\} < (\text{rad}(abc))^2$$

が成り立つ.

(I) の場合から考える. $0 < \epsilon < 1$ となる $\epsilon \in \mathbb{R}$ を固定する.

$$\begin{aligned} N \geq \max \left\{ \frac{3(1+\epsilon)}{1-\epsilon}, \frac{\log_2(\kappa(\epsilon)|\alpha\beta\gamma|^{2+\epsilon})}{\epsilon} \right\}, \\ \max_{p \text{ は素数}} \left\{ \max\{\text{ord}_p(\alpha), \text{ord}_p(\beta), \text{ord}_p(\gamma)\} + 1 \right\}. \end{aligned}$$

となる自然数 N に対して, (I) の abc 予想を用いて, F_N が $\mathbb{Q}$ 上フェルマー性をもつことを示そう.

$A = GA', B = GB', C = GC'$ とおく. このとき, (1) から, $A', B', C' \in \mathbb{Z} \setminus \{0\}$ であり, さらに, $A' + B' + C' = 0$ かつ $\text{GCD}(A', B', C') = 1$ となる. ゆえに, (I) の abc 予想から,

$$\max\{|A'|, |B'|, |C'|\} < \kappa(\epsilon) \text{rad}(A'B'C')^{1+\epsilon}$$

となる.

したがって, (2) より,

$$\begin{aligned} t^N &\leq \max\{|A|, |B|, |C|\} = |G| \max\{|A'|, |B'|, |C'|\} \\ &< \kappa(\epsilon) |G| \text{rad}(A'B'C')^{1+\epsilon} \\ &\leq \kappa(\epsilon) |G| \text{rad}(ABC)^{1+\epsilon} \\ &\leq \kappa(\epsilon) |\alpha\beta\gamma| (|\alpha||\beta||\gamma||x||y||z|)^{1+\epsilon} \leq \kappa(\epsilon) |\alpha\beta\gamma|^{2+\epsilon} t^{3(1+\epsilon)} \end{aligned}$$

となる．ゆえに，

$$t^{N(1-\epsilon)} < \frac{\kappa(\epsilon)|\alpha\beta\gamma|^{2+\epsilon}}{t^{\epsilon N}} t^{3(1+\epsilon)} \leq \frac{\kappa(\epsilon)|\alpha\beta\gamma|^{2+\epsilon}}{2^{\epsilon N}} t^{3(1+\epsilon)} \leq t^{3(1+\epsilon)}$$

である．よって， $(1-\epsilon)N < 3(1+\epsilon)$ となるので， $N < 3(1+\epsilon)/(1-\epsilon)$ を得るが，これは， N の取り方に矛盾する．

(II) の場合を考える．

$$N \geq \max \left\{ \log_2 |\alpha\beta\gamma|^3 + 6, \max_{p \text{ は素数}} \left\{ \max\{\text{ord}_p(\alpha), \text{ord}_p(\beta), \text{ord}_p(\gamma)\} \right\} + 1 \right\}$$

のとき，(I) の場合の計算と同様にして，

$$\begin{aligned} t^N &\leq \max\{|A|, |B|, |C|\} = |G| \max\{|A'|, |B'|, |C'|\} < |G| \text{rad}(A'B'C')^2 \\ &\leq |G| \text{rad}(ABC)^2 \leq |\alpha\beta\gamma|(|\alpha||\beta||\gamma||x||y||z|)^2 \leq |\alpha\beta\gamma|^3 t^6 \end{aligned}$$

となり， $2^{N-6} \leq t^{N-6} < |\alpha\beta\gamma|^3$ を得るので，矛盾する．ゆえに， F_N がフェルマー性をもつことがわかる． $\square$

6. 算術的力学系における一般化されたフェルマー予想

講演終了後，前節におけるフェルマー予想が，算術的力学系に一般化できることを発見した．そのことについて簡単に述べておく．詳細は，「Arithmetic dynamics and generalized Fermat's conjecture, arXiv:2601.08207」を参照．

K は前節と同様，算術的函数体とする． X は K 上定義された幾何学的に既約な射影スキーム， L は X 上の豊富な直線束とする．正の整数 N_0 を固定し， $F = \{f_N\}_{N=N_0}^\infty$ は以下の性質をもつ X から X への K 上の射の列とする：

- (1) ある整数 $d_N \geq 2$ が存在して， $f_N^*(L) \simeq L^{\otimes d_N}$ が成り立つ．
- (2) $\lim_{N \rightarrow \infty} \deg(f_N) = \infty$ である．
- (3) $f_N \circ f_{N'} = f_{N'} \circ f_N$ がすべての $N, N' \geq N_0$ で成り立つ．

すべての $N, N' \geq N_0$ で， $f_N \circ f_{N'} = f_{N'} \circ f_N = f_{NN'}$ が成り立つとき， F は **乗法的** という．さらに，すべての $N, N' \geq N_0$ で， $f_N \circ f_{N'} = f_{N'} \circ f_N = f_{N+N'}$ が成り立つとき，**加法的** という． $f_N \circ f_{N'} = f_{N'} \circ f_N$ という性質から，

$$h_F(x) \geq 0 \text{ and } h_F(f_N(x)) = d_N h_F(x) \quad (\forall x \in X(K))$$

となる高さ函数を構成することができる． Y は同次元的な X の部分スキームで， $Y_N := f_N^{-1}(Y)$ ($N \geq N_0$) と定める．

$$Y_N(K) \subseteq \{x \in X(K) \mid h_F(x) = 0\}$$

が成り立つとき， Y_N は K 上の**フェルマー性**をもつという．前節においては， $X = \mathbb{P}_K^2$ ， $f(X : Y : Z) = (X^N : Y^N : Z^N)$ ， Y が強い意味で非特異的な同次多項式で与えられている場合を考えている．

予想 6.1 (算術的力学系における一般化されたフェルマー予想)．ある $N_1 \geq N_0$ が存在して，すべての $N \geq N_1$ について， $Y_N(K)$ が有限となるとき，ある $N_2 \geq N_0$ が存在して，すべての $N \geq N_2$ について， Y_N はフェルマー性をもつか？

これについて，以下のような根拠がある．

定理 6.2. (1) もし $Y(K)$ が有限なら，ある $N_2 \geq N_0$ が存在して，すべての $N \geq N_2$ について， Y_N はフェルマー性をもつ．

- (2) F が加法的で, $Y_{N_1}(K)$ が有限となる $N_1 \geq N_0$ が存在するなら, ある $N_2 \geq N_0$ が存在して, すべての $N \geq N_2$ について, Y_N はフェルマー性をもつ.
- (3) F が乗法的であり, ある正の整数 p_0 が存在して, $p \geq p_0$ となる素数 p について, $Y_p(K)$ が有限なら,

$$\lim_{m \rightarrow \infty} \frac{\#\{N_0 \leq N \leq m \mid F_N \text{ は } K \text{ 上でフェルマー性をもつ}\}}{m} = 1$$

が成立する.