1　対数一次形式の理論と応用: Hermite から Baker，Matveev まで

平田典子 (Noriko Hirata-Kohno)　日本大学理工学部数学科

1.1　超越数はなぜ面白いか

Definition 1.1 (代数的数，超越数) 有理数全体のなす体 $\mathbb{Q}$ 上，代数的となる数を代数的数と呼ぶ．すなわち，全てが 0 ではない有理数を係数とする 1 変数多項式の零点となる数が代数的数である．代数的数は複素数になることが知られている．代数的数でない複素数を超越数と呼ぶ．

代数的数全体は体をなすことが分かっている．代数的数全体の集合を，以下 $\overline{\mathbb{Q}}$ と表す．
有理数体 $\mathbb{Q}$ は可算集合であり，実数全体 $\mathbb{R}$ は非可算だから，無理数は必ず非可算無限個存在する．同様に代数的数全体 $\overline{\mathbb{Q}}$ も可算集合であり，複素数全体 $\mathbb{C}$ は非可算だから，その補集合である超越数も必ず非可算無限個存在して，その濃度は代数的数全体より大きい．つまり超越数は代数的数に比すると「ありふれた存在」のはずである．しかし，具体的な無理数や超越数の構成という問題や，また与えられた実数や複素数が無理数かどうか，もしくは超越数であるかどうかの判定は，一般に非自明である．それはひとえに代数的数が「構成的」な定義を持つ数であることに対し，超越数は「$\cdots$ で無い数を超越数と定める」という否定文による定義だからである．$\sqrt{2}$ の無理数性の証明が,「有理数であると仮定して矛盾を導く」という背理法の手段によるしかないことと同じと言える．
現在も超越数であるか，あるいは無理数であるかどうかの証明が与えられていない数が沢山ある．古くより知られる Euler の定数 $\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)$ は超越性，無理数性ともに未だ分からない．超越数の例として，最初に作られた数であると言われているものに 1844 年の J. Liouville の例がある．これは後述のようにディオファントス近似の応用によって構成された．また，Ch. Hermite が自然対数の底 e の超越性を 1873 年に証明し，1882 年には F. Lindemann が円周率 π の超越性を証明した．この円周率 π の超越性と，代数的数全体は体をなすという事実を合わせると，$\sqrt{\pi}$ の超越性が得られる（もしも $\sqrt{\pi}$ が代数的数ならばその 2 乗も代数的数となってしまい，円周率 π の超越性に矛盾する）．この時点ではじめて単位円と等しい面積の正方形の作図可能性を問うギリシャの等積問題は否定的に解決された．
整数論においては，与えられた情報を用いて有限回の操作で有限時間内に計算可能なアルゴリズムを持つ数を effective な数と呼ぶ．effective ということばは数学の他の分野で多少異なる意味で用いられていることもあるようだが，ここではこの意味と定める．
超越数の代数的数によるディオファントス近似理論は，A. Baker の対数一次形式の理論のおかげで effective な結果をもたらす場合が多く，不定方程式の代数的数の解を求める問題などに適用される．
なぜ超越数が面白いかということを説明しよう．それは，原始的な好奇心の所以でもあるが,

それ以外に，超越数の研究は代数的数をより詳しく調べるためにも応用できるという理由もあるからである．標語的に言ってしまえば「興味のある集合を調べることと，その補集合を調べることは同じ」であるからとも言えるが，実はもっと強いことが分かる．簡単にここに述べてみる．

「ある集合 $G \subset \mathbb{C}$ の中の代数的数 $G \cap \overline{\mathbb{Q}}$ を全て具体的に求める」問題を考える．たとえば，与えられた不定方程式の解 $G \subset \mathbb{C}$ のうち代数的数であるもの $G \cap \overline{\mathbb{Q}}$ もしくは，類似として，与えられた代数体や有理整数環などに属する数 $G \cap \mathbb{Z}$ などを求めることを考える．フェルマーの大定理もこのような問題の一種である．近代的な言い方では代数多様体の有理点を求める問題になる．

その場合,「effective な情報」を得られるような次のプログラムを考えよう．

超越数でも代数的でも実数値を取る，ある関数 F を考える．

(1) もし与えられた数が超越数であるならば，その数での関数 F の値が B 以上である，という命題を証明する．

ここで関数 F の値が B 未満である数については，全て「effective に」求めることが出来るような環境が整っているとする．

(2) 次に (1) の対偶を取る．つまり関数 F の値が B 未満である数は，代数的数であることが得られる．

(3) 関数 F の値が B 未満であるような数は，G の元になる代数的数を真部分集合として含むように B を設定できるとする．関数 F の値が B 未満である数が「effective に」全て求められたあと，その数を G の定義にあてはめ，G の元であるものだけを抽出する操作も「effective に」行えれば G の元になる代数的数が全て求まる．

これがいわば，Baker の対数一次形式の理論を用いて楕円曲線の整数点などを求める基本的な方法である．見かけは違うが，フィボナッチ数列のうち完全な累乗数になるものは 1, 8, 144 しか存在しない事実の証明 (Y. Bugeaud - M. Mignotte - S. Siksek の定理, この時点でアナウンス) などにも応用された考え方である．

上記のような議論のうち現実に動くプログラムは，ある種類の数が超越数になるための十分条件を求める問題から派生して来る場合が多い．すなわち，超越数の研究が代数的数を調べるために役立ったと言える．それも，単に「興味のある集合を調べることと，その補集合を調べることは同じ」だけのレベルにはとどまらない，より強力な情報が入ったことになる．研究開始したときには Hermite や Lindemann はここまでは分かっていなかったかもしれない．

科学にはかくなる面があるのだろう，ごく単純に curiosity driven でひたすら勉強していたら，気づいたときにゴールに着いていて，そこがとてつもなく豊富な世界であったことになる．スタート地点とゴール地点がこれだけ異なる様相を呈するのも珍しい．そして後から見ると実にしかるべき路なのだ．

だから，超越数は，面白い．

超越数の研究全般についての一般的な教科書，報告集としては例えば [6], [45], [50], [65], [73], [76], [78], [86], [91] などがある．筆者のおすすめは [65], [91] などである．

1.2 超越数の例について

ディオファントス近似とは，整数論的に意味のある形の近似と言ってしまっても良いが，後述の「高さ」という関数を距離関数の代わりに用いた「近似」の概念であると総称するのが正しい．さて Liouville の定理として次のディオファントス近似が知られている．これは代数的数は有理数であまり良く近似できないことを示す定理であるが，この対偶を用いれば非常に速いスピードで有理数によって近似される数を構成して超越数を作ることができる．
Liouville の定理は，ディオファントス近似や超越数に関する定理のなかでは珍しく，背理法ではない直接証明を持つ．下記の d は 1 以上で良い．

Theorem 1.1 (Liouville の定理) d を 1 以上の整数, α を $\mathbb{Q}$ 上 d 次の代数的数とする．α のみに依存する定数 $c(\alpha) > 0$ が存在して次を満たす．α と等しくない任意の有理数 $\dfrac{p}{q} \neq \alpha$（ただし $q > 0$）に対し

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d} \tag{1}$$

が常に成立する．

Proof $d = 1$ のときについては明らかであるが証明を述べておこう．α が有理数のとき，$\alpha = \dfrac{a}{b}$, a, b は最大公約数 1 の整数，$b > 0$ とおくと，仮定 $\dfrac{p}{q} \neq \dfrac{a}{b}$ より $\left|\alpha - \dfrac{p}{q}\right| = \dfrac{|aq - bp|}{bq} \geq \dfrac{1}{bq}$ となり $c(\alpha) = \dfrac{1}{b}$ と取れば定理が成立する．
$d \geq 2$ について証明する．α の $\mathbb{Z}$ 係数の最小多項式 $f(X)(= f_\alpha(X)$; α を解とする $\mathbb{Z}$ 係数 1 変数多項式のうち $\mathbb{Z}$ 上既約で係数達の最大公約数が 1 であり，かつ最高次の係数が正のものとして定めれば一意である）をとる．$f(X)$ を α で Taylor 展開すると $f(\alpha) = 0$ より

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\sum_{k=1}^{d}\left(\frac{p}{q} - \alpha\right)^k \frac{f^{(k)}(\alpha)}{k!}\right| \leq \left|\frac{p}{q} - \alpha\right| \sum_{k=1}^{d}\left|\frac{p}{q} - \alpha\right|^{k-1}\left|\frac{f^{(k)}(\alpha)}{k!}\right|$$

となる．まず $|\dfrac{p}{q} - \alpha| \leq 1$ の場合は

$$\leq \left|\frac{p}{q} - \alpha\right| \sum_{k=1}^{d}\left|\frac{f^{(k)}(\alpha)}{k!}\right| = \frac{1}{c(\alpha)} \cdot \left|\alpha - \frac{p}{q}\right|$$

が得られる．$d \geq 2$ より $f(\dfrac{p}{q}) \neq 0$ となることから $|f(\dfrac{p}{q})| \geq \dfrac{p}{q^d}$ である．したがって先の $|f(\dfrac{p}{q})|$ の上からの評価とあわせると定理が従う． $|\dfrac{p}{q} - \alpha| > 1$ の場合，定理成立は自明. $c(\alpha) > 0$ は上の取り方より具体的に決定される数である． □

さて，これから次の結果がわかる．

Corollary 1.2 α を $\mathbb{Q}$ 上 d (≥ 2) 次の代数的数とする. 任意の $\varepsilon > 0$ に対して不等式

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{d+\varepsilon}} \tag{2}$$

を満たす有理数 $\frac{p}{q}$（$q>0$）は有限個である．

Proof p,q は最大公約数 1 の整数としてよい．(1) から

$$\frac{c(\alpha)}{q^d} \leq \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{d+\varepsilon}}$$

となるので，$q^{\varepsilon} < \frac{1}{c(\alpha)}$ が得られて有限個の正整数 q が定まる．$\alpha - \frac{1}{q^{d+\varepsilon}} < \frac{p}{q} < \alpha + \frac{1}{q^{d+\varepsilon}}$ から整数 p も決まる．p,q の決まり方は具体的 (effective であることは勿論，全部簡単に求められてしまう）である． □

Theorem1.1 の証明では，整数のような「粗に存在している」集合の元に対して，異なる元の距離が 1 以上つまり「ゼロでない整数の絶対値は 1 以上」という事実に帰着して考えるところが本質的な点である．

ディオファントス問題で我々の興味を持つ対象は，有理点と総称されるような，$\mathbb{Q}$, $\mathbb{Z}$, $\overline{\mathbb{Q}}$，有限次代数体などの元であるが，これらはすべて粗なる集合である．この考え方で見ることが必然である．単に有理数を実数の中で捉えたら，有理数の稠密性という性質があって困る訳だが，有理数を分母と分子の整数の組である数と捉えることが重要なのである．異なる有理数というものを，異なる整数の話に帰着させれば良いのである．そうすれば異なる元の距離が 1 以上という断固たる事実から，非自明なる下からの評価が従い，興味のある有理点の考究が可能となる．

同様に，d 次の代数的数 α も，「$\mathbb{Z}$ 係数の α の最小多項式 f_α の係数」を並べた $d+1$ 次元整数格子の点と考えられる．整数格子の点は距離が一定以上離れているのだから，異なる代数的数同士が互いに近いことは不可能であると言うのが Liouville の定理である．すなわち，代数的数同士は良く近似できないということを表していて，実に自然な定理なのである．なお，Liouville の定理よりも後述の Roth の定理が（一部の範疇の数を除いて）より良い近似を与えている．

さて，Theorem1.1 を用いて Liouville は次のような超越数を構成した. 一般にこのような数を Liouville 数と称する．

Theorem 1.3 $\alpha = \sum_{n=1}^{\infty} 2^{-n!}$ は超越数である.

Proof

$q(k) = 2^{k!}$, $p(k) = 2^{k!}\sum_{n=1}^{k} 2^{-n!}$ とおく. ただし k は 1 以上の整数とする．このとき

$\left|\alpha - \frac{p(k)}{q(k)}\right| = \sum_{n=k+1}^{\infty} 2^{-n!} < 2\cdot 2^{-(k+1)!} = 2(q(k))^{-k-1}$ である．ここで k を十分大きくとれば

$$\left|\alpha - \frac{p(k)}{q(k)}\right| < \frac{1}{(q(k))^{2+\varepsilon}}$$

が無限個の有理数 $\frac{p(k)}{q(k)}$ に対して成り立つことになるが，α が代数的数ならば Liouville の定理に反するので, α は超越数でなければならないことになる． □

$\frac{1}{(q(k))^{2+\varepsilon}}$ は k が大きくなると，ものすごいスピードで小さくなる分数であるから，$\sum_{n=1}^{\infty} 2^{-n!}$ は，非常に良く有理数で近似できる超越数であることがわかる．Liouville 数の集合は非可算であるが，Lebesque 測度は 0 であることが [42] などにより知られている．

Liouville 数は超越数であるが，超越数の例は Liouville 数に限らない．例えば，0.1234567891011121314... という無限小数は超越数であるが Liouville 数ではない．K. Mahler の証明した事実として，一般に $n \in \mathbb{N}$ に対し $f(n) \in \mathbb{N}$，$f(n) \to \infty$ $(n \to \infty)$ となる整数係数 1 変数多項式 f を取り，小数点以下これらを順番に並べた無限小数 $0.f(1)f(2)f(3)...$ は Liouville 数ではない超越数となることが知られている [49]．e や π も Liouville 数ではないことが連分数の議論から得られる．

1.3 Hermite の定理など

Theorem 1.4 (Hermite- Lindemann の定理) α が 0 でない代数的数なら，$\exp(\alpha)$ は常に超越数となる．

上記の定理で $\alpha = i\pi$ とおけば，$\exp(i\pi) = -1$ は超越数ではないので，Lindemann の定理で示されていた π の超越性が従う．$\alpha = 1$ のときが Hermite の定理である．

さて 1900 年のヒルベルトの第 7 問題において，$2^{\sqrt{2}}$ や e^{π} は超越数になるのではないかと問われていた．A. O. Gel'fond と Th. Schneider は独立に次の結果を得て，これを肯定的に解決した．

Theorem 1.5 (Gel'fond-Schneider の定理) $\alpha \neq 0, 1, \beta \notin \mathbb{Q}$ である代数的数 α, β に対し，α^{β} は超越数となる．

これより，$2^{\sqrt{2}}$ や $e^{\pi} = (-1)^{i}$ は超越数であることが従う．つまり，

$$\mathcal{L} = \{\ell \in \mathbb{C} | \exp(\ell) \in \overline{\mathbb{Q}}\}$$

は $\mathbb{Q}$ 上の線形空間だが，$\overline{\mathbb{Q}}$ 上の線形空間にはならないことがわかる．

Hermite- Lindemann の定理は，1 と $\ell \in \mathcal{L}$ が $\mathbb{Q}$ 上一次独立なら，$\overline{\mathbb{Q}}$ 上でも一次独立という命題と同値である．また Gel'fond-Schneider の定理は $\ell_1, \ell_2 \in \mathcal{L}$ が $\mathbb{Q}$ 上一次独立なら，$\overline{\mathbb{Q}}$ 上でも一次独立という命題と同値である．

これを一般的に拡張したのが次の A. Baker の定理である．

Theorem 1.6 (A. Baker) $\ell_1, \cdots, \ell_n \in \mathcal{L}$ が $\mathbb{Q}$ 上一次独立ならば，1 を加えた $n+1$ 個の数である $1, \ell_1, \cdots, \ell_n$ は $\overline{\mathbb{Q}}$ 上で一次独立となる．

したがって，上記の定理の仮定を満たす $\ell_1, \cdots, \ell_n \in \mathcal{L}$ に対して代数的数係数 $\beta_1, \cdots, \beta_n \in \overline{\mathbb{Q}}$ による任意の一次結合 $\beta_1\ell_1 + \cdots + \beta_n\ell_n$，即ち対数一次形式 linear form in logarithms は 0 か超越数であり，0 になる場合は $\beta_1 = \cdots = \beta_n = 0$ である場合に限ることがわかる [6], [88].

Hermite- Lindemann の定理の簡単な系をもうひとつ述べておく．これは代数的数の複素共役も代数的数であることに注意すれば得られる．

Corollary 1.7 $\alpha \in \mathbb{C}, \alpha \neq 0$ のとき αおよび $\sin\alpha$ の少なくとも一方は超越数である．同様に αおよび $\cos\alpha$ の少なくとも一方は超越数である．

1.4 高さと Malher measure

対数一次形式の定理は effctive に定量化される．これが A. Baker がフィールズ賞を授けられた最大の理由であろう．指数和などの評価方法では出来なかったことを可能にしたことになる．そのためには，最初に述べたような良い性質の関数をいくつか定義する必要がある．まず高さと呼ばれる重要な概念を定める．

Definition 1.2 (射影座標の絶対的対数的高さ) $X \in \mathbb{P}^N(\overline{\mathbb{Q}})$ を考える．$X = (x_0, \ldots, x_N) \in \mathbb{P}^N(K)$ となる有限次代数体 K に対して X の絶対的（対数的）高さを次で定める．

$$h(X) := \frac{1}{[K:\mathbb{Q}]} \sum_v n_v \log(\max\{|x_0|_v, \ldots, |x_N|_v\}) \ .$$

ただし和は有限次代数体 K の互いに同値でない全ての非自明な付値の集合を走り，$n_v = [K_v : \mathbb{Q}_v]$ は各付値 v における局所次数とする．
この定義は射影座標の取り方や有限次代数体 K の取り方によらずに定まることが知られている．前者は K を有限次代数体とするときの，付値の Product formula「$a \in K, a \neq 0$ に対し $\prod_v |a|_v^{n_v} = 1$」から従う．後者は付値の Extension formula 「K の任意の有限次拡大体 L に対して v の上にある L の付値を w とかくと $[L:K]n_v = \sum_{w|v} n_w$ であること」から得られる．

Definition 1.3 (代数的数の絶対的 (対数的) 高さ) $\alpha \in \overline{\mathbb{Q}}$ のとき $(1, \alpha) \in \mathbb{P}^1(\overline{\mathbb{Q}})$ を考え，$h(\alpha) := h((1, \alpha))$ と定めて $\alpha \in \overline{\mathbb{Q}}$ の絶対的対数的高さという．$K = \mathbb{Q}(\alpha)$ に対して $(1, \alpha) \in \mathbb{P}^1(K)$ と考えて良い．またこの指数関数値である絶対的高さを $H(\alpha) := \exp(h(\alpha))$ と表す．

すなわち x を正実数とするとき $\log^+ x := \log(\max\{1, x\})$ とおくと

$$h(\alpha) = \sum_v \frac{[K_v : \mathbb{Q}_v]}{[K:\mathbb{Q}]} \log^+ |\alpha|_v$$

である．

Proposition 1.8 K を有限次代数体，$\alpha, \alpha_1, \cdots, \alpha_n \in K$ とするとき，次が成り立つ．
(i) $h(\alpha) = h(\alpha^{-1})$
(ii) $h(\alpha_1\alpha_2) \leq h(\alpha_1) + h(\alpha_2)$
(iii) $h(\alpha_1 + \cdots + \alpha_n) \leq \log n + h(\alpha_1) + \cdots + h(\alpha_n)$.

Proof (i) は定義から従う．(ii) は 正の実数 x, y に対して $\log^+ xy \leq \log^+ x + \log^+ y$ であることから得られる．(iii) について示す．まず v が有限付値ならば $\log^+ |\alpha_1 + \cdots + \alpha_n|_v \leq \max_{1\leq i\leq n} \log^+ |\alpha_i|_v$ である．v が無限付値ならば $\log^+ |\alpha_1+\cdots+\alpha_n|_v \leq \log^+ n+\max_{1\leq i\leq n} \log^+ |\alpha_i|_v$ である．これらから従う． □

代数的数 α に対し $h(\alpha)$ は，α の最小多項式の係数の絶対値の最大値で定義されるごく「原始的な」高さと次のような関係がある [87]（もうすこし精密化された関係式もいくつかある）．その簡単な説明のためにこの「原始的な」（もしくは「ナイーブな」）高さ，そして Mahler measure を導入する（以下の H_{cl} という記号は一般的なものではなく，このテキストにおける記号であることをお断りしておく）．

Definition 1.4 (多項式の「原始的な」高さ) $a_0, \cdots, a_d \in \mathbb{C}, a_0 \neq 0$ に対し d 次の複素係数多項式
$f(X) = a_0X^d + \cdots + a_d \in \mathbb{C}[X]$ を考える．このとき $H_{cl}(f) := \max\limits_{0\leq i\leq d} |a_i|$ と表し，$f(X)$ の「原始的な」高さという．

Definition 1.5 (代数的数の「原始的な」高さ) d 次の代数的数 $\alpha \in \overline{\mathbb{Q}}$ に対し，$\mathbb{Z}$ 係数の α の最小多項式 f_α を取る．$H_{cl}(\alpha) = H_{cl}(f_\alpha)$ すなわち最小多項式の係数の絶対値の最大値を $\alpha \in \overline{\mathbb{Q}}$ の「原始的な」高さという．
$H_{cl}(\alpha)$ は正整数である．

次が本質的である．

Proposition 1.9 $D \geq 1, B \geq 1$ を与えられた実数とする．このとき $H_{cl}(\alpha) \leq B$ かつ α の次数 d が $d \leq D$ を満たすような全ての代数的数 $\alpha \in \overline{\mathbb{Q}}$ は有限個であり，その最小多項式は全て *effective* に列記できる．

Proof 絶対値が B 以下の整数は全て決められることから，自明である． □

つまり「原始的な」高さと次数が bounded なる代数的数は effective に求まる．ただし「方程式を解く」操作についてはここでは考えず，最小多項式を決めれば代数的数が effective に決まると理解することにしておく．

Definition 1.6 (Mahler measure) $a_0, \cdots, a_d \in \mathbb{C}, a_0 \neq 0$ に対し，d 次の複素係数多項式 $f(X) = a_0X^d + \cdots + a_d \in \mathbb{C}[X]$ を考える．このとき

$$M(f) = \begin{cases} \exp\left(\dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \log\left|f(e^{i\theta})\right| d\theta\right) & \text{if } f(X) \not\equiv 0 \\ 0 & \text{if } f(X) \equiv 0 \end{cases} \tag{3}$$

と定める．

$$M(f) = \begin{cases} \exp\left(\displaystyle\int_0^{1} \log\left|f(e^{2\pi i\theta})\right| d\theta\right) & \text{if } f(X) \not\equiv 0 \\ 0 & \text{if } f(X) \equiv 0 \end{cases}$$

と定義している本もあるが，全く同じである．

このとき，次が成り立つ．

Proposition 1.10 (i) M(fg) = M(f) M(g).
(ii) $a_0, \cdots, a_d \in \mathbb{Z}, a_0 \neq 0$ に対し，d 次の整数係数多項式
$f(X) = a_0X^d + \cdots + a_d = a_0(X - \alpha_1)\dots(X - \alpha_d) \in \mathbb{Z}[X]$ を考える．
このとき Mahler measure は

$$M(f) = |a_0| \prod_{i=1}^{d} \max(1, |\alpha_i|)$$

に等しい．
(iii) d 次の代数的数 $\alpha \in \overline{\mathbb{Q}}$ に対して $M(\alpha) = h(\alpha)^d$ が成り立つ．言い換えれば

$$h(\alpha) = d \log M(\alpha).$$

Proof (i) は定義から従う．(ii) であるが，Jensen の公式，たとえば L. V. アールフォルス著の複素解析（現代数学社，笠原乾吉訳）の本の 223 ページから 224 ページを参照する．まず (i) より $M(f) = M(a_0)\prod_{i=1}^{d} M(X - \alpha_1)\dots M(X - \alpha_d) = |a_0|M(X - \alpha_1)\dots M(X - \alpha_d)$ となる．そこで 1 次式 $X - \alpha$ に対する $M(X - \alpha)$ の計算を行う．$|\cdot|$ が無限付値の場合で α が単位円 $|z| = 1$ の内部にある場合，つまり $|\alpha| < 1$ ならば多項式 $X - \alpha$ に対して $\dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \log\left|e^{i\theta} - \alpha\right| d\theta = \log|\alpha| + \log\left|\frac{1}{\alpha}\right| = 0$ であり，またそうでない場合，つまり $|\alpha| \geq 1$ ならば $\dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \log\left|e^{i\theta} - \alpha\right| d\theta = \log|\alpha|$ になることから $|\cdot|$ が無限付値の場合は $\dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \log\left|e^{i\theta} - \alpha\right| d\theta = \log^+|\alpha|$ が分かる．以上より (ii) が従う．(iii) については，まず (ii) から

$$\log M(\alpha) = \log|a_0| + \sum_{i=1}^{d} \log^+|\alpha_i|$$

となる．ここで代数体の無限付値の意味から

$$\frac{1}{d}\sum_{i=1}^{d} \log^+|\alpha_i| = \sum_{v|\infty} \log^+|\alpha|_v$$

であることと，有限付値の場合は

$$\frac{1}{d}\log|a_0| = \sum_{v\nmid\infty}\log^+|\alpha|_v$$

になっていることを合わせれば (iii) が証明された． □

Proposition 1.11 多項式の原始的な高さ $H_{cl}(P) = \max\limits_{1\le i\le d}|\alpha_i|$ に対して

$$M(\alpha) \le (d+1)^{1/2}H_{cl}(\alpha)$$

および

$$H_{cl}(\alpha) \le 2^d M(\alpha)$$

が得られる．

Proof Malher measure の定義より α の最小多項式 $f(X) = a_0X^d + \cdots + a_d$ に対して

$$M(\alpha) \le \left(\frac{1}{2\pi}\int_0^{2\pi}\left|f(e^{i\theta})\right|^2 d\theta\right)^{1/2}$$

が成り立つ．ゆえに

$$M(\alpha) \le \left(\sum_{i=0}^{d}|a_i|^2\right)^{1/2} \le (d+1)^{1/2}H_{cl}(\alpha)$$

である．$H_{cl}(\alpha) \le 2^d M(\alpha)$ については，解と係数の関係および基本対称式の対称性によって

$$|a_0| + \cdots + |a_d| \le |a_0|\prod_{i=1}^{d}(1+|\alpha_i|) \le 2^d M(\alpha)$$

となり従う． □

以上より $H_{cl}(\alpha)$ と $M(\alpha)$ は次数 d が固定されている場合には本質的に同じ働きをする．すなわち，次数及び $M(\alpha)$ がある正定数以下の $\alpha \in \overline{\mathbb{Q}}$ は有限個でかつ理論的に全て effective に求まる．まとめると下記である．これこそ，高さが代数的数を測る理想的なものさしであることを意味する．

Corollary 1.12 $D \ge 1, B \ge 1$ を与えられた実数とする．このとき $h(\alpha) \le B$ かつ α の次数 d が $d \le D$ を満たすような全ての代数的数 $\alpha \in \overline{\mathbb{Q}}$ は有限個であり，その最小多項式は全て *effective* に列記できる．

Proof Proposition1.9 と Proposition1.10 と Proposition1.11 を組み合わせれば良い． □

1.5 A. Baker による対数一次形式の理論

定理の詳細は [6], [88] にあるが，その根幹を述べると Baker の対数一次形式の定理とは次の形で与えられる．

Theorem 1.13 (A. Baker) $\mathbb{Q}$ 上 d 次の代数体 K に属する代数的数の対数 $\ell_1, \cdots, \ell_n \in \mathcal{L}$ が $\mathbb{Q}$ 上一次独立と仮定する．このとき，$n, d, |\ell_i|, h(\exp(\ell_i))(1 \leq i \leq n)$ の関数として具体的に表される *effective* な正定数 C で，次をみたすものが存在する．
$B \geq e$ を満たす実数 B をとる．このとき $h(\beta_i) \leq \log B(0 \leq i \leq n)$ をみたす，すべてが 0 ではない任意の $\beta_0, \beta_1, \cdots, \beta_n \in K$ に対し，$|\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n| > B^{-C}$ となる．

Baker の定性的な定理 Theorem 1.6 から $\beta_0, \beta_1, \cdots, \beta_n$ の全てが 0 ではないことと $\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n \neq 0$ は同値であるから $|\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n| > 0$ であることは分かるが，その情報を $\beta_0, \beta_1, \cdots, \beta_n$ の各々ではなく B によって捉えたことが本質である．$\beta_0, \beta_1, \cdots, \beta_n$ の各々で下からの評価を記述しても意味が無い，$|\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n| > \dfrac{1}{2}|\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n|$ は当たり前である．楕円曲線の整数点の有限性へこの評価を応用する場面では B での表示が重要である．整数点への応用については [80] を参照すれば良い．
この具体的に表される正定数 C を全部書き下し，かつ大きな改良を数の幾何学を用いて行ったのが E. Matveev である [53][54][55]. しかしその実際の評価式は面倒な条件のもとに記されていてなかなか使いにくい．本質的には n の依存部分が，従来の n^n オーダーではなく n の絶対定数乗オーダーに落とせたことが大切で，そのアイデアは数の幾何学における格子の考究に負う．ここではその後の簡略化である Yu. Nesterenko の定理 [52] を紹介しておこう．
$\beta_0, \beta_1, \cdots, \beta_n$ の属する基礎体は，ディオファントス問題に最も応用される有理数体とする．

Theorem 1.14 (Yu. Nesterenko) $\alpha_1, \ldots, \alpha_n$ は正の有理数とする．
その実数対数の値である $\log\alpha_1, \ldots, \log\alpha_n$ は $\mathbb{Q}$ 上一次独立であると仮定する．$B > 0$ を取る．このとき $\max_{1\leq i\leq n}|b_i| \leq B$ をみたす，すべてが 0 ではない任意の $b_1, \ldots, b_n \in \mathbb{Z}$ に対して次の不等式が成り立つ．

$$|b_1\log\alpha_1 + \cdots + b_n\log\alpha_n| \geq \exp\left(-2.9(2e)^{2n+6}(n+2)^{9/2}h(\alpha_1)\cdots h(\alpha_n)\log(eB)\right).$$

Proof Yu. Nesterenko の [52] における Theorem 2.1 である． □
上記の一連の定理における指数関数を任意次元の可換代数群の指数写像に拡張して考える一般の対数一次形式の超越性は G. Wüstholz による ([90])．これより Schneider の予想していた超越性，たとえば代数体上定義された単純 Abel 多様体の 0 でない周期，(指数写像の核に属する元の各座標の意味）は，すべて 0 か超越数となる．次元が 1 の場合つまり楕円曲線の場合は，Schneider が示していたので，その高次元版の解決となる．Schneider の結果 [73] は次のように述べられる．

Theorem 1.15 *Weierstrass* の楕円関数 $\wp(z)$ がみたす微分方程式 $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ において $g_2, g_3 \in \overline{\mathbb{Q}}$ ならば，$\wp(u) \in \overline{\mathbb{Q}} \cup \{\infty\}$ となる $u \in \mathbb{C}$ は 0 か超越数である．

特別な場合として，$\wp$ の周期は 0 か超越数となる．これらの定量化については S. David, 平田らの仕事がある [19], [37]．Masser-Wüstholz による Abel 多様体の同種写像の次数の評価にもこの手法が用いられているが証明で難しい部分であったのは零点の評価である [51].

2 部分空間定理と単数方程式: Siegel から Schmidt，Faltings まで

2.1 ディオファントス方程式の概念

m を 1 以上の整数とし，$f(X_1, \cdots, X_m) \in \mathbb{Z}[X_1, \cdots, X_m]$，$f(X_1, \cdots, X_m) = 0$ の形の方程式に対して $X_1, \cdots, X_m \in \mathbb{Z}$ の範囲で解を求めるとき，その方程式をディオファントス (Diophantus) 方程式もしくは不定方程式と称する．$\mathbb{Z}$ のみならず，$\mathbb{Q}$，代数的整数，代数的数あるいは有限生成群，有限生成整域などの集合に，係数や解の範囲を限った方程式，及びその有限個の連立方程式や一般化，現代的な解釈を総称してディオファントス問題とも言う．ディオファントス (Diophantus) は 3 世紀頃のギリシャのアレクサンドリアの数学者であろうと言われていて，このような方程式の整数解や有理数解を研究したようであるが，その生涯については余り良く分かっていない．算術 (Arithmetika) という書物を著し，そこで様々な不定方程式を調べている．ピタゴラス方程式と呼ばれる方程式 $X^2 + Y^2 = Z^2$ に対し $XYZ \neq 0$ を満たす整数解 X, Y, Z を求める問題も考察されている（互いに素な X, Y, Z の一般解は $X = a^2 - b^2, Y = 2ab, Z = a^2 + b^2 (a, b \in \mathbb{Z})$ であり，無限個存在する）．n を 3 以上の任意の整数とし，n を固定する．ピタゴラス方程式の一般化に相当する $X^n + Y^n = Z^n$ が，自明解つまり $XYZ = 0$ となる場合以外には整数解 $X, Y, Z \in \mathbb{Z}$ を持たないという命題は，P. de Fermat によって考察されたが Fermat の大定理と呼ばれ，1995 年に A. Wiles によって証明されたことは周知の事実であろう。

このようなディオファントス問題に役立つ近似である，有理数による無理数の近似，代数的数による代数的数の近似，また代数的数による超越数の近似などの近似不等式をディオファントス近似と呼ぶ．近似する数と近似される数の距離を，単なる距離関数ではない「高さ」関数で表記することがその本質である．「高さ」はすなわち有理数や代数的数に対して特別に反応する「ふるい」であり，なおかつ付値から作られていて距離のような性質をもつ「ものさし」なので，三角不等式に近いものが成立することは前述の通りである．

ディオファントス近似は数論幾何学の主要な道具の一つになっており，例えば G. Faltings や P. Vojta により高次元 Mordell 予想の解決に使われたことも知られている（Faltings の議論はその後 E. Bombieri により簡略化された）[30], [31], [32], [83], [84], [85].

ディオファントス近似の教科書や最近の報告集としては [21], [65], [71], [72], [91] などがあげられよう.

2.2 Dirichlet の定理

まず Dirichlet の定理 (1842) を述べよう．まず，引き出し論法 (Box principle) という考え方であるが，これは「11 本の鉛筆を 10 個の引き出しに入れると，どんな入れ方をしても必ず少なくとも 1 個の引き出しに 2 個以上の鉛筆が存在する」ということである．鳩の巣論法とも呼ばれる．引き出し論法によって以下の Lemma 2.1 が証明され，Lemma 2.1 を用いて Theorem 2.1 が得られる．

Theorem 2.1 (Dirichlet)　α を実無理数とする．このとき，$|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ を満たす $\frac{p}{q} \in \mathbb{Q}$ は無限個存在する．

右辺 $\frac{1}{q^2}$ のかわりに単なる正の数を用いて α との距離を近くするならば，有理数の稠密性から，任意の $\varepsilon > 0$ に対し $|\alpha - \frac{p}{q}| < \varepsilon$ を満たすような $\frac{p}{q} \in \mathbb{Q}$ が無限個存在するのは自明である．ここではそのような議論をするのではない．右辺が近似分数の高さであることが重要である．実際，有理数に対し高さ関数は $h(\frac{p}{q}) = \log \max(|p|, |q|)$ であることが高さの定義から分かるが，不等式の右辺を上記のように $\frac{1}{\max(|p|,|q|)}$ のかわりに $\frac{1}{|q|}$ で置き換えても，不等式の結論が変わらないことを確かめることが出来るので，上記の主張の右辺は $\frac{1}{\max(|p|,|q|)^2}$ であると考えて良い．このように，単なる $\varepsilon > 0$ ではない近似関数を用いているところが，ディオファントス近似の骨子である．ここでたとえば $|\alpha - \frac{p}{q}| < \frac{1}{q^3}$ と右辺を変えた瞬間，α が代数的な無理数ならば，この不等式を満たす $\frac{p}{q} \in \mathbb{Q}$ は有限個に限るという Roth の定理 [71] 定理 2A（後述）の主張があることに注意すると，有限性と無限性を分ける臨界は 2 という指数になる．
Theorem 2.1 の証明のために，次の Lemma 2.1 をにおいて変数 Q を導入し，$Q \to \infty$ にすることで互いに素な $p, q \in \mathbb{Z}$ の組み合わせが無限個存在することを示す．

Lemma 2.1 (Dirichlet)　α を実数とする．$Q \in \mathbb{R}, Q > 1$ とする．このとき $1 \leq q < Q$，$|\alpha q - p| \leq \frac{1}{Q}$ を満たす $p, q \in \mathbb{Z}$ が存在する．

では，Theorem 2.1 を証明する．
Proof
$Q_0 \in \mathbb{R}, Q_0 > 1$ とする．Lemma2.1 より $1 \leq q < Q_0$，
$|\alpha q - p| \leq \frac{1}{Q_0}$ を満たす $p, q \in \mathbb{Z}$ が存在する．ここで $\gcd(p, q) = d \geq 1$ ならば，$q = dq', p = dp'$ とおくと $|\alpha q' - p'| \leq d|\alpha q' - p'| = |\alpha d q' - d p'| \leq \frac{1}{Q_0}$ であるから，$\gcd(p, q) = 1$ つまり $\frac{p}{q}$ は既約分数として良い．このような互いに素な $p, q \in \mathbb{Z}$ を 1 組とって固定し，$p_0 = p, q_0 = q$ とおく．
$|\alpha q_0 - p_0| \leq \frac{1}{Q_0}$ であるが，定理 1.1 の仮定において α は無理数だったので $\alpha q_0 - p_0 \neq 0$ であ

る (もし $\alpha q_0 - p_0 = 0$ ならば $\alpha = \dfrac{p_0}{q_0}$ となり有理数になってしまう)．つまり $0 < |\alpha q_0 - p_0|$ であるから，$\dfrac{1}{Q_1} < |\alpha q_0 - p_0|$ となるような $Q_1 \in \mathbb{R}, Q_1 > 1$ が存在する．
この Q_1 に対して再び定理 1.2 を適用する．これを繰り返すと次のように p, q, Q の列が出来る．番号をつけると
$0 < \cdots < \dfrac{1}{Q_2} < |\alpha q_1 - p_1| < \dfrac{1}{Q_1} < |\alpha q_0 - p_0| < \dfrac{1}{Q_0}$.
ここで $Q \to \infty$ とすると互いに素な整数の無限個の組 (p, q) が存在することが上記より得られる．$1 \leq q < Q$ と合わせて考えると，これら無限個の組 (p, q) の全てが $|\alpha - \dfrac{p}{q}| \leq \dfrac{1}{qQ} \leq \dfrac{1}{q^2}$ を満たすことになるから Theorem 2.1 が従う． □
C を正数，α を実無理数とするとき，同様の Diophantus 近似不等式 $|\alpha - \dfrac{p}{q}| < \dfrac{C}{q^2}$ を考えると，$C \geq \dfrac{1}{\sqrt{5}}$ ならば任意の実無理数 α に対し，やはり無限個の有理数解 $\dfrac{p}{q}$ $(p, q \in \mathbb{Z})$ を持つ．
この C の臨界に注目すると $C < \dfrac{1}{\sqrt{5}}$ ならば有限個の有理数解しか存在しないような実無理数 α が作れることが知られている（A. Hurwitz, 1891）．また Theorem 2.1 の代数体版も成立する，すなわち実代数体 K を固定すると K に依存する $C > 0$ が存在し，任意の実数 $\alpha \notin K$ に対し不等式 $|\alpha - \xi| < C \max(1,\ |\alpha|^2) H_K(\xi)^{-2}$ が無限個の $\xi \in K$ に対して成り立つ．
ここで $H_K(\xi)$ は K に依存する代数的数 ξ の高さであり，絶対的対数的高さ h に対し $H(\xi) = \exp(h(\xi))$ とおくとき，$H_K(\xi) = H(\xi)^{[\mathbb{Q}(\xi):\mathbb{Q}]}$ と理解すれば良い．さらに代数体を固定せず，次数のみ固定すると次のようになる．d を自然数とし，α は $d+1$ 次以上の実代数的数であるか，あるいは実超越数とする．d と α に依存する $C > 0$ が存在し，$|\alpha - \xi| < CH(\xi)^{-d(d+1)}$ が無限個の d 次の代数的数 ξ に対して成立するという命題は，$d = 2$ まで証明され（H. Davenport-W. M. Schmidt），$d \geq 3$ では未解決，であるがこれに関して E. Wirsing は $|\alpha - \xi| < CH(\xi)^{-\frac{d(d+3)}{2}}$ を満たす $\deg \xi \leq d$ の実代数的数 ξ が無限個存在することを証明され (1961)，D. Roy の考察が行われている．以上は全て無限個の解をもつ近似不等式である．

2.3 Roth の定理

Liouville の定理は Liouville 以来，A. Thue, C. L. Siegel, H. Davenport, F. J. Dyson らによって改良され，K. F. Roth が右辺を最良の評価まで到達させた (1955)．今日 Roth の定理と言われるものである．すなわち下記の主張である．

Theorem 2.2 (Roth の定理) *α を $d \geq 2$ 次の実代数的数とする. このとき, 任意の $\varepsilon > 0$ に対して, 不等式 $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{q^{2+\varepsilon}}$ を満たす有理数 $\dfrac{p}{q}$ は有限個しか存在しない.*

注意しておくが，$d = 1$ のときと α が実数でない複素数のときは自明である．後者については複素平面で有理数と α が離れていることから分かる．上記の主張はさきの（指数的）高さによって $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{H(\dfrac{p}{q})^{2+\varepsilon}}$ としても有限性は変わらない．Dirichlet の定理から，Roth の定

理は論理的に最良の指数 $2+\varepsilon$ を持つことがわかる．これと同値な述べ方として，下記もある．
「任意の正数 C，任意の $\epsilon > 0$ に対し，$|\alpha - \frac{p}{q}| < CH(\frac{p}{q})^{-2-\epsilon}$ を満たす有理数 $\frac{p}{q}$ は有限個である．」
Roth の定理は Liouville のそれとは本質的に異なり，不等式を満たす有理数 $\frac{p}{q}$ は有限個であっても，それらを有限時間の有限回の操作で具体的に求めうるアルゴリズムはまだ得られていない，つまり Roth の定理は effective ではない．effective な Roth の定理を得ることは人類の夢である．証明方法への寄与に鑑みて，Thue-Siegel-Roth の定理とも呼ばれている．また実際には証明の中で一般化された generalized Wronskian を定義した Dyson の貢献も大きい．

Roth の定理から 2 変数 Thue 方程式の整数解は有限個である事実が従う．[71] 118 ページにその証明が掲載されている．また最近では逐次最小の言葉で Roth の定理を一般化できることも知られている [65].
Liouville の近似不等式と同様に，Roth の定理を次のように述べても良い．

任意の $\epsilon > 0$ に対し α と ϵ に依存する正定数 $A > 0$ が存在して $|\alpha - \frac{p}{q}| > AH(\frac{p}{q})^{-2-\epsilon}$ という不等式が α と異なる全ての有理数 $\frac{p}{q}$ に対し成立する．

しかしこの $A > 0$ は Liouville と異なり，effective ではない正定数である．
Roth の定理は論理的に最良といっても，まだまだ分からない事は非常に多い．ちなみに下記は未解決問題（Serge Lang による）である．

Conjecture 1 α が 3 次以上の代数的数ならば，不等式

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2(\log q)^\kappa}$$

を満たす有理数 $\frac{p}{q}$ は, $\kappa > 1$ ならば （または少なくとも α によって定まる定数 $\kappa_0(\alpha)$ が存在して，$\kappa > \kappa_0(\alpha)$ ならば）有限個しか存在しない．

上記の Conjecture1 は”almost all” 代数的数 α に対しては成立している．これは A. Kintchine の定理から直ちに得られる．

2.4 部分空間定理

Roth の定理の多変数版は，W. M. Schmidt の部分空間定理 subspace theorem である．
その代数多様体上の一般化 [31] では，一次式以外の積の場合にも拡張されているが，本質的な部分はもとの 30 年前の部分空間定理本体から従うことも注意されている．部分空間定理の変数を代数体で考える一般化，通常の絶対値の代わりに代数体の付値をとるもの，定量化および [31] の定量化については [23] および [26] などがある．最近になってオートマトン論や，あ

るいは曲面における整数点の分布への応用が発見されている．近似の指数は最良評価になっている．

部分空間定理とは下記の定理である．この左辺はわかりにくいものであるが，実はいわば内積であり，n 次元での有理点同士の距離と考えられ得る事に注意したい．

Theorem 2.3 (Schmidt's Subspace Theorem)　n を 2 以上の整数とする．
$L_1(\mathbf{x})$, ..., $L_n(\mathbf{x}) \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ を線形独立な線形形式とする. すなわち，これら線形形式の係数を並べて得られる正方行列の行列式は 0 にならないとする．任意の $\delta > 0$ に対し，有理数係数で定まる有限個の真部分空間 $T_1, \ldots, T_w \subset \mathbb{Q}^n$ が存在して次が成立する．

$$|L_1(\mathbf{x}) \ldots L_n(\mathbf{x})| < |\mathbf{x}|^{-\delta} \tag{4}$$

を満たす整数点 $\mathbf{x} \in \mathbb{Z}^n$ $(\mathbf{x} \neq 0)$ はこれらの部分空間の和集合 $T_1 \cup \cdots \cup T_w$ に属する．ただし $|\mathbf{x}| = \left(x_1^2 + \cdots + x_n^2\right)^{\frac{1}{2}}$ とする．

右辺は $\mathbf{x} \in \mathbb{Z}^n$ であることから高さの関数になっているとみなして良い．

Roth の定理はこの部分空間定理の $n = 2$ の場合に相当する．また $L_1(\mathbf{x}), \cdots, L_n(\mathbf{x})$ 全てが有理数係数の場合は自明となる．

部分空間定理は Diophantus 近似で最も深い定理の一つとされているが，Roth の定理と同様に，残念ながら effective ではない．即ち $\mathbb{Q}^n$ の有限個の真部分空間 $T_1, \ldots, T_w$ の定義式は不明である．ここを effective にすることは非常に難しいと考えられている．しかし有限個の真部分空間の個数の上からの評価は，与えられた情報により具体的に記述され，定量的部分空間定理と称される．部分空間定理は Norm 形式方程式と呼ばれる不定方程式の整数解の有限性を与える．また部分空間定理の別証明は [31] により与えられている．部分空間定理の変数 $\mathbf{x}$ を代数体で考える一般化，通常の絶対値の代わりに代数体の付値をとるもの，その定量化および [31] の定量化については [23] および [26] がある．
更に未知数 $\mathbf{x}$ を $\overline{\mathbb{Q}}$ で解くものを絶対部分空間定理と称するが [28] これは数の幾何学の応用によっている [27].

定量的部分空間定理は，単数方程式の解の個数の上からの評価を与えるという著しい応用があり，それを経て様々な不定方程式の解の個数の上からの評価をもたらす．単数方程式の解の個数については [27], [72] に述べられているが下記に少しまとめよう．

2.5　単数方程式

K を $[K : \mathbb{Q}] = d < \infty$ となる有限次代数体とする．S を K の付値の有限集合で， 無限付値を全て含むとする．$s = \#S < \infty$ とおく．

Definition 2.1 (S 整数，S 単数) S 整数とは，次の集合の元である．
$\mathfrak{O}_S := \{x \in K : v(x) \geq 0 \, for \, \forall v \notin S\}$. また S 単数とは
$U_S := \{x \in K : v(x) = 0 \, for \, \forall v \notin S\}$ の元である．

単数方程式というものを定義する．

Definition 2.2 (単数方程式) $\alpha_1, \alpha_2 \in K - \{0\}$ に対して未知数 x, y を単数もしくは S 単数 U_S で考えた $\alpha_1 x + \alpha_2 y = 1$ を単数方程式と呼ぶ．

Theorem 2.4 (Siegel, Mahler, Lang) 単数方程式 $\alpha_1 x + \alpha_2 y = 1 \quad in \quad x, y \in U_S$ の解は有限個に限る．

上記の定理は Roth の定理から得られる．この高次元版としては部分空間定理から得られる単数方程式の解の有限性がある．これらを，単数に限らず有限生成群の元に一般化された主張が得られるのでそれについて述べよう．代数体とは無関係の有限生成乗法群の命題に拡張したことになる [29].

Definition 2.3 (General unit equation) K を *characteristic* 0 の体とする．Γ を $(K^*)^n$ の *finite rank* $r < \infty$ の部分群とする．すなわち有限個の生成元 $u_1, u_2, \cdots, u_r \in \Gamma$ が存在して次を満たす．全ての $x \in \Gamma \subset (K^*)^n$ に対して $x^z = u_1^{z_1} \cdots u_r^{z_r}$ を満たす整数 $z, z_1, \cdots, z_r$ がとれる．
さて $\alpha_1, \cdots, \alpha_n \in K - \{0\}$ とする．このとき *General Unit equation* とは未知数を Γ で探す単数方程式，つまり $\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \, in \, x := (x_1, \cdots, \mathbf{x}_n) \in \Gamma$ と定める．単数という概念は無くなっているが有限生成の群の元と言うところにその名前の根拠がある．ただし空でない任意の *index* の部分集合 $I \subset \{1 \cdots n\}$ に対して $\sum_{i \in I} \alpha_i x_i \neq 0$ であるとする．このような解 $x := (x_1, \cdots, \mathbf{x}_n) \in \Gamma$ を *"non-degenerate"* と称する．従って *"degenerate" solutions* とは消えてしまう部分和 $\sum_{i \in I} \alpha_i x_i = 0$ を持つもののことである．

Theorem 2.5 (Evertse-Schlickeweri-Schmidt, 2002) *General Unit equation* $\alpha_1 x_1 + \cdots + \alpha_n x_n = 1$ を考える．未知数の範囲は $x = (x_1, \cdots, x_n) \in \Gamma$ であるとする．このとき，この解の個数は高々 $c(n)^{r+1}$ ただし $c(n) = \exp\left((6n)^{3n}\right)$ である．

この別証明は G. Rémond によって与えられている．2 変数の場合の Beukers-Schlickewei の定理が 1996 年に証明されており，その $n = 2$ の場合は，これより良い評価になっていて $2^{8(r+2)}$ で与えられている．ここで r は Γ の階数であるので，通常の単数群の場合はその階数の $r = r_1 + r_2 - 1$ にあたる．

なお，一般にこのような解の有限性が従うが，他方で有限個ではあるが「いくらでも」多くの

解を持つ単数方程式も構成できることに注意しておこう．これらは下記の定理であるが Erdős, Stewart, Tijdeman や Konyagin, Soudararajan に負う．

$N(\alpha_1, \cdots, \alpha_n)$ を $\alpha_1 x_1 + \cdots + \alpha_n x_n = 1$ の non-degenerate 解の個数とおく．

Theorem 2.6 (Erdős-Stewart-Tijdeman) $K = \mathbb{Q}$ とする．
このとき絶対定数 $c > 0$ と，付値の有限集合 S で任意の *cardinality* s を持つものが存在して次が成り立つ．

$$N(1,1) \geq \exp\left(c(s/\log s)^{1/2}\right)$$

さらにこの改良は下記で与えられる．

Theorem 2.7 (Konyagin-Soudararajan) 絶対定数 $\gamma < 2 - \sqrt{2}$ と，付値の有限集合 S で任意の *cardinality* s を持つものが存在して次が成り立つ．

$$N(1,1) \geq \exp\left(s^{\gamma}\right).$$

この結果は H. P. Schlikewei らにより回帰数列などに対して応用されている [27].

Roth の定理では 2 数の距離を片方の高さと比較しているが，これを両方の高さと比較する命題が次の Schmidt の予想で，部分的な結果はあるが [24] 未解決である．

Conjecture 2　K を代数体とし，任意の $\epsilon > 0$ をとる．K と ϵ による正定数 C が存在して任意の $\alpha, \beta \in K$，$\alpha \neq \beta$ に対し $|\alpha - \beta| > C \max\{H(\alpha),\ H(\beta)\}^{-2-\epsilon}$ となるであろう．

これは symmmetric ディオファントス近似と呼ばれ，難しい問題とされている．解決されれば単数方程式などに著しい応用が期待される．

2.6　数の幾何学について

数の幾何学とは，数をユークリッド空間の格子点と対応させ，幾何学を用いて数論に役立つ性質を考究する学問の総称で，歴史的には H. Minkowski が称したといわれる．ついでにディオファントス近似という言葉も Minkowski の言葉といわれている．Dirichlet の単数定理の証明や，与えられた判別式をもつ代数体が有限個であるという Hermite-Minkowski の定理の証明も数の幾何学に負う．教科書は [13], [36], [56], [71], [72], [79] などがある．最近では絶対的部分空間定理にその手法が応用されている [27]．絶対的とは，体によらずに主張を述べられる場合に用いる言葉である．その代表的な定理である Minkowski の第 1 および第 2 定理を紹介する．Minkowski の第 2 定理は逐次最小による整数格子の点に対する近似である．

Definition 2.4 空でない $\mathcal{C} \subset \mathbb{R}^n$ に対し次の条件を満たす集合 $\mathcal{C}$ を凸体という．原点を内点にもつ有界閉集合であり，原点で点対称，そして $\mathcal{C}$ の任意の 2 点 P, Q に対し，線分 PQ が $\mathcal{C}$ に含まれる (凸集合) であるもの．

$\mathcal{C}$ は通常の意味の体積を持つ．それを $V(\mathcal{C})$ とおく．
簡単のため，$x = (x_1, \cdots, x_n) \in \mathbb{R}^n$ の $1 \leq i \leq n$ に対する全ての座標 x_i が $x_i \in \mathbb{Z}$ を満たす x を整数点という．また，$\mathbb{Z}^n$ のことを $\mathbb{R}^n$ の整数格子とよぶことにしよう．

Theorem 2.8 (Minkowski の第 1 定理, 1896) $\mathcal{C} \subset \mathbb{R}^n$ を凸体とする．
このとき，$V(\mathcal{C}) \geq 2^n$ ならば $\mathcal{C}$ は原点とは異なる整数点を少なくとも一つ含む．

Definition 2.5 $\mathcal{C} \subset \mathbb{R}^n$ を凸体とする．$1 \leq j \leq n$ を満たす各 j に対し，$\lambda\mathcal{C}$ が j 個の一次独立な整数点を含むような $\lambda \geq 0$ の下限を λ_j とおく．この $\lambda_1, \lambda_2, \cdots, \lambda_n$ を $\mathcal{C}$ の逐次最小とよぶ．

例えば $\mathcal{C} \subset \mathbb{R}^2$ を原点中心の長方形で，2 辺が x 軸と y 軸にそれぞれ平行，横の辺の長さ 1，縦の辺の長さ 4 とする．このとき $\lambda_1 = \dfrac{1}{2}$ (ただし $g_1 = (0,1)$ もしくは $g_1 = (0,-1)$)，$\lambda_2 = 2$ (ただし $g_2 = (1,0)$ もしくは $g_2 = (-1,0)$) である．
逐次最小の定義より $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n < \infty$ であることが従う．

Theorem 2.9 (Minkowski の第 2 定理, 1907) $\mathcal{C}$ を $\mathbb{R}^n$ の凸体とする．
$\lambda_1, \cdots, \lambda_n$ を $\mathcal{C}$ の逐次最小とする．このとき次が成り立つ．
$$\frac{2^n}{n! \cdot V(\mathcal{C})} \leq \lambda_1 \cdots \lambda_n \leq \frac{2^n}{V(\mathcal{C})}.$$

Minkowski の第 2 定理からは，Minkowski の一次形式定理や単数方程式の解の個数に関する性質など，ディオファントス問題に関する様々な応用が従うことが知られている．
たとえば Schmidt は部分空間定理の定量化に第 2 定理を本質的に用いた [72].

2.7 Norm 形式方程式

Schmidt が部分空間定理を証明した当時の最も大事な応用は，Schmidt 自身による Norm 形式方程式という不定方程式の整数解の有限性であった．まずそれについて述べておこう．

Definition 2.6 K を有理数体 $\mathbb{Q}$ 以外の代数体，$\sigma_1, \cdots, \sigma_n$ を K から $\mathbb{C}$ への体の埋め込みの全体とする．

いわゆる共役を $\alpha^{(i)} = \sigma_i(\alpha)\,(\forall \alpha \in K)$ と記する．K の元を係数とする方程式を次のように考える．$\mathbb{Q}$ 上一次独立な係数とする m 元 1 次形式 $L(\mathbf{x}) = \alpha_1 x_1 + \cdots + \alpha_m x_m\,(\alpha_j \in K)$ をとる．$L(\mathbf{x})$ の共役となる一次形式の積 $N_{K/Q}(L(\mathbf{x})) = \prod_{i=1}^{n} \left(\alpha_1^{(i)} x_1 + \ldots + \alpha_m^{(i)} x_m\right)$ を考える．この形を *Norm* 形式と呼ぶ．

Norm 形式とは $\mathbb{Q}$ 係数の n 次形式であり，もしも $m = n$ ならば $\mathbb{Q}$ 上既約であることが知られている．また逆に $\mathbb{Q}$ 上既約で，$\overline{\mathbb{Q}}$ 係数の一次式の積に書けるような m 変数の n 次形式は Norm 形式の定数倍になることが [12] の本に示されている．

いま，整数 $b \in \mathbb{Z}, b \neq 0,$ をとり，$\mathbf{x} = (x_1, \cdots, x_m) \in \mathbb{Z}^m$ を未知数とみなした $\mathbb{Q}$ 係数方程式 $N_{K/Q}(L(\mathbf{x})) = b$ を考える．これを Norm 形式方程式という．これは $m = 2$ なら Thue 方程式で，とくに $n > 2$ で既約なら解は有限個となる．また $n = 2$ ならば Pell 方程式になり，この場合は整数解は無限個になる．

$\mathcal{M} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m \subset K$ とおく．このとき Norm 形式方程式は，$N_{K/Q}(\mathbf{x}) = b \quad (\mathbf{x} \in \mathcal{M})$ で与えられる．さて，K の部分体 L で無限個の単数を持つものおよび $\mu \in K, \mu \neq 0$ が存在して，μL が $\mathbb{Q}\mathcal{M} = \mathbb{Q}\alpha_1 + \cdots + \mathbb{Q}\alpha_m$ に含まれるとき $\mathcal{M}$ は退化するといい，そうでないとき非退化という．$m = n$ なら $\mathbb{Q}\mathcal{M} = K$ となるから，K が虚二次体でなければ退化の場合に相当する．$\mathcal{M}$ が退化するなら，K の部分体 L の単数を使って，$N_{K/Q}(\mathbf{x}) = b$ が無限個の解 $\mathbf{x} \in \mathcal{M}$ を持つ $b \in \mathbb{Q}, b \neq 0$ を取ることができる．$\mathcal{M}$ が非退化な Norm 形式方程式のとき，Schmidt は部分空間定理を用いて，任意の $b \in \mathbb{Q}, b \neq 0$ に対し Norm 形式方程式 $N_{K/Q}(\mathbf{x}) = b$ の解 $\mathbf{x} \in \mathcal{M}$ が有限個に限ることを示した．ここで任意の $b \in \mathbb{Q}, b \neq 0$ に対し Norm 形式方程式の解 $\mathbf{x} \in \mathcal{M}$ が有限個であることと，$\mathcal{M}$ が非退化であることは同値である．

Norm 形式方程式の解の個数の上からの評価は存在するが一般の Norm 形式方程式の解を求めるアルゴリズムを求める問題は，部分空間定理が effective でないことから未解決である．解の個数の漸近公式 Norm 形式方程式の右辺を不等式に直すと，急に難しくなる．それを Norm 形式不等式といい， J. Thunder や Evertse の研究がある．

2.8 部分空間定理の数論幾何学への応用

さて，G. Faltings の高次元 Mordell 予想の証明にも，部分空間定理の証明方法が用いられた [91]．このような数論的幾何学への応用が最近研究されている．一般型のアファインまたは射影曲面 V は，予想ではあまり沢山の有理点を持たないと考えられているが，近年，部分空間定理の直接の応用から P. Corvaja -U. Zannier， P. Autissier， A. Levin によって代数曲線や代数曲面の整数点の分布状態が下記のように調べられた [14][15][16]．下記の Theorem **??**は C. L. Siegel の結果なので，その別証明を与えたことになる．これらは部分空間定理（の関数体バージョン）によって示された．これは Siegel の証明の持つ Jacobi 多様体の経由を回避している．そして P. Autissier，A. Levin らにより，さらなる拡張が試みられた．

Siegel の古典的な定理とは次のように述べられる．有理数係数の既約な 2 変数多項式の零点つまり $P(x,y)=0$ を満たす点 (x,y) で x も y も整数となる「整数点」は，次の (i) または (ii) の条件下では高々有限個しか存在し得ない：
(i) 曲線 $P(x,y)=0$ の種数が 1 以上である．
(ii) 曲線 $P(x,y)=0$ は少なくとも 3 個の異なる点を無限遠点で持つ．

ここで，(ii) の仮定のもとでの命題を Corvaja-Zannier が部分空間定理を用いて証明した．つまり，次の定理の「別証明」を与えた．

Theorem 2.10 (Corvaja-Zannier) $\tilde{C}$ を有限次代数体 K 上で定義された絶対既約な射影曲線とし，C をその空でない *affine* 部分集合で *affine* 空間 $\mathbb{A}^n$ に埋め込めるとする． S を K の付値の有限集合で，無限付値全てと有限個の有限付値からなるものとする．S 整数の集合 $\mathfrak{O}_S := \{x \in K : v(x) \geq 0 \, for \, \forall v \notin S\}$ を考える．もし $\sharp\left(\tilde{C}-C\right) \geq 3$ であるならば $\sharp(C \cap \mathbb{A}^n(\mathfrak{O}_S)) < \infty$ である．

Theorem2.10 の証明は [15] にあるが，その概略 [14] はそれほど難しくない．

一般に，general type の affine または射影曲面 V は「あまり沢山の有理点を持たない」と信じられている．Faltings の示した高次元 Mordell は V がアーベル多様体の部分多様体の場合である．P. Vojta はそれを V が semi-abelian 多様体の部分多様体の場合に拡張したが，それでも曲面についてのディオファントス問題に関しては，余り多くの結果は知られていない．しかし，Theorem2.10 の手法は高次元に拡張され，曲面の場合についても，同じように部分空間定理の直接の応用から P. Corvaja -U. Zannier[16]， P. Autissier， A. Levin らによって次が示された．

Theorem 2.11 (Corvaja-Zannier, Autissier, Levin) $\tilde{X}$ を有限次代数体 K 上で定義された非特異射影曲面とし，X をその空でない *affine* 部分集合で *affine* 空間 $\mathbb{A}^n$ に埋め込めるとする． $C_1, \cdots, C_r$ を $\tilde{X}-X$ の *effective* で豊富な *divisors* で *properly intersecting* であるとする，即ち，$C_1, \cdots, C_r$ のうちの，どの 2 個も共通の *component* を持たず，かつ，どの 3 個も共通の点を持たないと仮定する．更に，$r \geq 4$ を仮定する．このとき，K の無限付値全てと有限個の有限付値からなるような付値のどんな集合 S に対しても，$X \cap \mathbb{A}^n(\mathfrak{O}_S)$ は *Zariski-dense* にならない．

2.9 オートマトン論への部分空間定理の応用

ある古典的な無理数の問題が，部分空間定理の応用によって解決された．B. Adamczewski-Y. Bugeaud の「オートマトン的な無理数は超越数である」[1] という命題を含む定理である．

Definition 2.7 (complexity function) A を有限集合とする．
A をアルファベットとよび，A の元を文字という．U を A の元からなる無限数列の集合とする，すなわち $U = \{u_1, u_2, \dots, u_n, \dots, : u_i \in A\}$．任意の自然数 $n \in \mathbb{N}$ に対して $\rho(n)(= \rho_U(n))$ を $\rho(n) := \sharp\{u_k u_{k+1} \cdots u_{k+n-1} : k = 1, 2, 3, \dots\}$ とおく．$\rho(n)$ は U の続き番号の n 個の元からなる異なる「単語」n-words の個数となる．明らかに $1 \leq \rho(n) \leq (\sharp(A))^n$ である．$\rho(n)$ は勿論 $\mathbb{N}$ 上の関数である．この $\rho(n)$ を数列 U の complexity function　もしくは，U の complexity と呼ぶ．

いま，α を開区間 $(0,\, 1)$ に属する実数とする．任意の整数 $b \geq 2$ に対して，α を b 進展開する．

$$\alpha = u_1 b^{-1} + u_2 b^{-2} + u_3 b^{-3} + \cdots$$

ここで $u_1, u_2, u_3, \dots, \in \{0, 1, 2, \cdots, b-1\}$．$\alpha$ が有理数ならばその b 進展開は，ある小数位より先は周期的（有限で止まる小数展開を含むとみなす）であるので，complexity function は有界である．

Adamczewski-Bugeaud[1] は，α が代数的数で，かつ無理数ならば，その b 進展開は「非線形」である事を示した．即ち，次である．

Theorem 2.12 (Adamczewski-Bugeaud) α を開区間 $(0,\, 1)$ に属する代数的数で，かつ無理数であるとする．整数 $b \geq 2$ に対して定まる b 進展開 $\alpha = u_1 b^{-1} + u_2 b^{-2} + u_3 b^{-3} + \cdots$ の *digits* から成る $U = \{u_1, u_2, \dots, u_n, \dots, \}$ の *complexity function* $\rho(n)(= \rho_U(n))$ は次を満たす．

$$\lim_{n \to \infty} \frac{\rho(n)}{n} = \infty.$$

long repetition の定義をする．

Definition 2.8 (long repetition) 無限数列 $(u_1, u_2, \dots, u_n, \dots,)$ が *long repetition* を持つとは，次のことと定める．
ある正の数 ε と，無限個の自然数 N が存在して「単語」$u_1 u_2 \cdots u_N$ が重ならないような，同じ文字からなる「部分単語」2 箇所をもち，その長さ（部分単語の文字数）が $\varepsilon \cdot N$ を越えるようになっているときに言う．

これより次を得る．

Theorem 2.13 (Adamczewski-Bugeaud-Luca) α を開区間 $(0,\, 1)$ に属する実数であるとする．ある整数 $b \geq 2$ に対して定まる α の b 進展開 $\alpha = u_1 b^{-1} + u_2 b^{-2} + u_3 b^{-3} + \cdots$ の *digits* から成る $(u_1, u_2, \dots, u_n, \dots,)$ が，*long repetition* を持つと仮定する．このとき，α は有理数か，または超越数のいずれかに限る．

一つの無限列 $(u_1, u_2, \ldots, u_n, \ldots,)$ の complexity function $\rho(n)$ に対して $\liminf_{n\to\infty} \frac{\rho(n)}{n} < \infty$ ならば，(u_n) は必ず long repetition を持つと言う事は知られている [1] ので，Theorem2.12 が Theorem2.13 からが従う．
この Theorem2.13 の証明に部分空間定理が用いられる！

2.10 Kronecker の定理

ここに高さ 1 の代数的数は 1 のベキ根に限るという Kronecker の定理を紹介しておこう．

Theorem 2.14 (Kronecker) 0 でない代数的数 α をとる．このとき, 次の 2 つは同値である
(1) $M(\alpha) = 1$
(2) α は 1 の冪根である．

Proof $K = \mathbb{Q}(\alpha)$ とする．まず (2)⇒(1) を示そう．$\alpha^m = 1$ とする．K の任意の付値 v に対し, $|\alpha|_v^m = |\alpha^m|_v = |1|_v = 1$ である．一方, $|\alpha|_v$ は 0 以上の実数であるので, $|\alpha|_v = 1$．したがって $M(\alpha) = 1$ が得られる．
つぎに (1)⇒(2) を証明する． $M(\alpha) = 1$ とすると α は代数的整数になる. そして α の共役元に対して $|\alpha^{(j)}| \leq 1$ つまり無限付値での値は 1 以下である．最小多項式の係数 a_i は $\alpha^{(j)}$ たちの基本対称式で与えられる．したがって次数 d のみに依存する正定数 $C(d)$ が存在して, 任意の無限付値 v に対して $|a_i|_v \leq C(d)$ となる．

最小多項式の係数が整数であることより, α の最小多項式となりうる多項式は有限個しか存在しない．それらを, $f_1, \cdots, f_t$ とおくと, $f_1 \times \cdots \times f_t = 0$ は解を有限個しかもたない．

仮定より, $M(\alpha) = 1$ であるので, 任意の $m \in \mathbb{N}$ に対して, $M(\alpha^m) = 1$.
したがって, α^m も $f_1 \times \cdots \times f_t = 0$ の解である．
ゆえに, 異なる 2 個の自然数 $m \neq m'$ が存在して $\alpha^m = \alpha^{m'}$ となる．
これより α は 1 の冪根でなければならない． □

2.11 三角関数と有理数の話題

ついでに，三角関数と有理数の話題にちょっと脱線する．超越数はもちろん無理数であるし，また $\cos(r) \in \mathbb{Q}$ となる $r \in \mathbb{C}$ も，当然無限個ある. しかしながら，$\cos(r \times \pi) = s$ であり $r \in \mathbb{Q}$ かつ $s \in \mathbb{Q}$ ならば，$s = 0, \pm\frac{1}{2}, \pm 1$ に限ることが初等的に証明できる．

すなわち $\pi \times$ 有理数 に対し余弦の値が有理数になるのは上記の場合しかないことが簡単に示せ

る. 円分体の次数を調べれば [33] [34] [35] この事実は証明できるのであるが, H. W. Richmond, H. S. M. Coxeter によるチェビシェフ多項式に基づいた易しい証明が [18] にある. ちょっと面白いのでついでにここに書いておく.

Proposition 2.15 $\cos(r \times \pi) = s$ であり $r \in \mathbb{Q}$ かつ $s \in \mathbb{Q}$ ならば $s = 0, \pm\frac{1}{2}, \pm 1$ に限る.

Proof $r = \dfrac{p}{q}, p, q \in \mathbb{Z}, q > 0, \gcd(p, q) = 1$ とする. $u_n = \cos 2^n \left(\dfrac{p}{q}\pi\right)$ とおくと $\{u_n | n \in \mathbb{Z}, n \geq 0\}$ は次に示すように有限集合である. なぜなら $\zeta_{2q} = \zeta_{2q,n} = \cos \dfrac{2^{n+1}p}{2q}\pi + i \sin \dfrac{2^{n+1}p}{2q}\pi$ とおくと, $\zeta_{2q}^{2q} = 1$ であり, かつ $u_n = Re(\zeta_{2q})$ である. つまり u_n は高々$2q$ 通りしか値をとらないので $\{u_n\}$ は有限集合となるわけである. さてここで $u_0 = \cos \dfrac{p}{q}\pi \in \mathbb{Q}$ ならば全ての n に対して $u_n \in \mathbb{Q}$ となる理由であるが, これは $\dfrac{p}{q}\pi = \alpha$ とおくと $\cos 2\alpha = 2\cos^2 \alpha - 1$ つまり $u_{n+1} = 2u_n^2 - 1$ という漸化式を満たすことから明らかである. したがって任意の n に対して $u_n \in \mathbb{Q}$ で, しかも高々$2q$ 通りの値しかとらないから, このような u_n の中で最大分母をもつものを改めて u_n とおき, $u_n = \dfrac{a}{b}$ (b はすべての u_n の分母の中で最大数) と書くことができる. $-1 \leq \cos \leq 1$ より $\dfrac{a}{b} \leq 1$, $b > 0$ なので $a \leq b$, $u_{n+1} = \dfrac{2a^2 - b^2}{b^2}$ となる.
(I) $a = 0$ のときは $u_n = 0$ である.
(II) 次に $a \neq 0$ ならば以下のように場合分けする.
(i) b が奇数のとき, $\gcd(a, b) = 1$ より, $\gcd(2a^2, b^2) = 1$ となる. $u_{n+1} = \dfrac{2a^2 - b^2}{b^2}$ において b は u_n の最大分母であることより $b^2 \leq b \Leftrightarrow b(b-1) \leq 0 \Leftrightarrow b \leq 1 \Leftrightarrow b = 1$ となる.
(ii) b が偶数のとき, $\gcd(a, b) = 1$ より, $\gcd(2a^2, b^2) = 2$ となる. これも同様に $u_{n+1} = \dfrac{a^2 - \dfrac{b^2}{2}}{\dfrac{b^2}{2}}$ において b は u_n の最大分母としたことより $\dfrac{b^2}{2} \leq b \Leftrightarrow b^2 \leq 2b \Leftrightarrow b(b-2) \leq 0 \Leftrightarrow b - 2 \leq 0 \Leftrightarrow b \leq 2 \Leftrightarrow b = 2$ (b は偶数だった) というわけである. これから $b = 1$ または 2 となるので, 全ての n に対し $2u_n \in \mathbb{Z}$, 特に $2u_0 \in \mathbb{Z}$ となる. すなわち $2\cos \dfrac{p}{q}\pi \in \mathbb{Z}$. $-1 \leq \cos \leq 1$ より $u_0 = 0, \pm\frac{1}{2}, \pm 1$ に限る. □

3 最近の新結果の紹介

3.1 Nesterenko による 3 数の代数的独立性について

まず, 特に顕著なのは少し古いが, 次の話題であろう.
楕円モジュラー関数を $j(\tau)$ とし, $0 < |z| < 1$ なるとき,

$$J(z) := j(\frac{\log z}{2\pi i})$$

とおく ([62] の第 2 章)．$0 < |\alpha| < 1$ となる代数的数 α での $J(z)$ の値の超越性は Malher-Manin 予想であったが，K. Barré-Sirieix, Diaz, F. Gramain, G. Philibert により 1996 年に証明された．Nesterenko がそれを一般化し，3 つの Eisenstein 級数と指数関数の値によって生成される体の超越次数の下からの評価を得た．

Ramanujan 関数というものをまず定めよう．

Definition 3.1 (Ramanujan functions) いま $q \in \mathbb{C}$ とし，$0 < |q| < 1$ を仮定する．
Ramanujan 関数とは

$$P(q) = 1 - 24\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}, Q(q) = 1 + 240\sum_{n=1}^{\infty} \frac{n^3q^n}{1-q^n}, R(q) = 1 - 504\sum_{n=1}^{\infty} \frac{n^5q^n}{1-q^n}.$$

をさす．

いわゆる Eisenstein series は

$$E_{2k}(z) = 1 + (-1)^k \frac{4k}{B_k} \sum_{n=1}^{\infty} \frac{n^{2k-1}z^n}{1-z^n},$$

で与えられているが，それを用いると

$$P(z) = E_2(z), Q(z) = E_4(z), R(z) = E_6(z)$$

と表示することができる．

Theorem 3.1 (Yu. V. Nesterenko, 1996) 任意の $q \in \mathbb{C}$，$0 < |q| < 1$ をとる．このとき 4 個の値 $q, P(q), Q(q), R(q)$ のうち，少なくとも 3 個は代数的独立である．

K. Mahler は関数 $P(q), Q(q), R(q)$ は $\mathbb{C}(q)$ 上（関数として）独立であることを証明した．Nesterenko の寄与はこれらの関数がつぎの微分方程式を，微分作用素 $D = q \cdot \dfrac{d}{dq}$ に関して満たしていることを証明した点にある．
その微分方程式は

$$12\frac{DP}{P} = P - \frac{Q}{P}, \quad 3\frac{DQ}{Q} = P - \frac{R}{Q}, \quad 2\frac{DR}{R} = P - \frac{Q^2}{R}$$

である．

この系として次が成り立つ [62].

$\Gamma(z)$ を通常のガンマ関数とする．つまり $\Gamma(z) = \int_0^{\infty} e^{-t}t^z \cdot \frac{dt}{t} = e^{-\gamma z}z^{-1}\prod_{n=1}^{\infty}\left(1+\frac{z}{n}\right)^{-1} e^{z/n}$.
ここで γ は Euler 定数 $\gamma = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$ のことを指す．

さきの関数の特殊値について考える．$\tau = i, \quad q = e^{-2\pi}$，$\omega_1 = \frac{\Gamma(1/4)^2}{\sqrt{8\pi}}$ とおく．このとき

$$P(q) = \frac{3}{\pi}, \quad Q(q) = 3\left(\frac{\omega_1}{\pi}\right)^4, \quad R(q) = 0$$

である．また

$$\tau = \rho, \quad q = -e^{-\pi\sqrt{3}}, \quad \omega_1 = \frac{\Gamma(1/3)^3}{2^{4/3}\pi} = 2.428\,650\,648\ldots,$$

とすると

$$P(q) = \frac{2\sqrt{3}}{\pi}, \quad Q(q) = 0, \quad R(q) = \frac{27}{2}\left(\frac{\omega_1}{\pi}\right)^6$$

が成立する．

Theorem 3.2 (Yu. Nesterenko) $\Gamma(z)$ を上記のガンマ関数とする．
(i) π, e^{π} と $\Gamma(\frac{1}{4})$ の 3 数は $\mathbb{Q}$ 上代数的に独立である．
(i)i$\pi, e^{\pi\sqrt{3}}, \Gamma(\frac{1}{3})$ は $\mathbb{Q}$ 上代数的に独立である．

Corollary 3.3 (Yu. Nesterenko) 特に，次が得られる．
π と e^{π} は代数的に独立である．

3.2 単数方程式と指数方程式

K は標数 0 の体，Γ を $(K^*)^n$ の，$\mathrm{rank}\, r < \infty$ の乗法部分群とする．$n \geq 2$ に対して $f_1, \cdots, f_R \in K[x_1, \cdots, x_n] - \{0\}$ とする．未知数 $x = (x_1, \cdots, x_n) \in \Gamma$ に対して，連立方程式

$$f_i(x_1, \cdots, x_n) = 0 \quad (i = 1, \cdots, R)$$

を考える．

Definition 3.2 変数 λ に対し，$x = (x_1, \cdots, x_n)$ が次の条件を満たすときに *degenerate* 解と称する．$gcd(c_1, \cdots, c_n) = 1$ なる整数の組 $c_1, \cdots, c_n \in \mathbb{Z}$ が存在して，λ に関して恒等的に

$$f_i(\lambda^{c_1}x_1, \cdots, \lambda^{c_n}x_n) = 0 \quad (i = 1, \cdots, R)$$

すなわち，λ に関して $f_i(\lambda^{c_1}x_1, \cdots, \lambda^{c_n}x_n)$ を展開したときに，λ の累乗で左辺を整理するときに現れる係数 ($x_1, \cdots, x_n$ の多項式となる）が恒等的に消える，ということを意味するとする．*degenerate* 解ではない解を *non-degenerate* 解と言う．

[46] の議論より，つぎの一般化が従う [25].

Theorem 3.4 (Evertse) 連立方程式

$$f_i(\lambda^{c_1}x_1,\cdots,\lambda^{c_n}x_n)=0 \quad (i=1,\cdots,R)$$

の *non-degenerate* 解 x は有限個である．

Proof $X=\{(x_1,\cdots,x_n)\in(K^*)^n : f_i(x_1,\cdots,x_n)=0 \quad (i=1,\cdots,R)\}$ とおく．S. Lang により予想されていた問題における M. Laurent[46] の torus の場合の解決，その発展である Evertse らの議論 [25][91] により，解 $x\in\Gamma$ は次の形の，有限個の coset の和集合 $x_1H_1\cup\cdots\cup x_tH_t$ に含まれる．ここで $xH=\{x\times y : y\in H\}$，$x\in\Gamma$ であり，また H は $(K^*)^n$ の既約な代数部分群（乗法群）で $xH\subset X$ となるものとする．X は有限集合というわけではない，あくまで我々の設定は $(x_1,\cdots,x_n)\in\Gamma$ の場合に限るのであり，$X\cap\Gamma$ を考えていることになる．Lang の有限性予想の $\mathbb{G}_m^n$ の場合である．

有限個の coset の個数の評価のうち，[91] にあるものは，$A=\dfrac{(n+d)!}{n!d!}$ とおくと

$$t\le c(n,d)^{r+1},\quad c(n,d)\le\exp\left((6dA)^{5dA}\right)$$

である．

さて $x\in\Gamma$，$xH\subset X$，$\dim H>0$ の場合，H_0 を次元 1 の H の既約な代数部分群としたとき，$gcd(c_1,\cdots,c_n)=1$ なる整数の組 $c_1,\cdots,c_n\in\mathbb{Z}$ が存在して，$H_0=\{(\lambda^{c_1},\cdots,\lambda^{c_n}) : \lambda\in K^*\}$ と書ける．従って $xH_0=\{(x_1\lambda^{c_1},\cdots,x_n\lambda^{c_n}) : \lambda\in K^*\}\subset xH\subset X$ となってしまい，λ に関して恒等的に 0 になる，つまり $f_i(\lambda^{c_1}x_1,\cdots,\lambda^{c_n}x_n)=0 \quad (i=1,\cdots,R)$ の場合に至り，degenerate 解となる．また逆に x が degenerate 解のときは，ある次元 1 の H_0 が存在して $xH_0\subset X$ となる．

従って，$x\in\Gamma$，$xH\subset X$，$\dim H>0$ の場合とは，degenerate 解の場合に一致する．つまり non-degenerate 解は $\dim H=0$ の場合，すなわち $H=(1,\cdots,1)$ の場合に限られる．これより xH の coset の個数の有限性が，そのまま x の個数の有限性を従える．以上で指数方程式の場合の解の個数の有限性が証明される． □

3.3 Euler 型の指数型ディオファントス方程式について

n,d,k,y を整数とする． $\gcd(n,d)=1$ とする．$n\ge1,d\ge1,y\ge1,k\ge2$（k を固定する訳ではない）の範囲で次の方程式を考える．$y^2=n(n+d)\cdots(n+(k-1)d)$.
未知数は n,d,k および y とする． n,y を未知数とするのは通常の代数曲線の整数点の考察にあるが，d,k も未知数としている処に困難さがある．$k=2$ or 3 のときは解は無限個あることが知られている．それ以外については次の予想がある．

Conjecture 3 $gcd(n,d)=1$ とする．方程式 $y^2=n(n+d)\cdots(n+(k-1)d)$ は $n,d,k,y\in\mathbb{Z}$, $n\ge1,d\ge1,y\ge1,k\ge4$ の範囲において整数解をもたない．

L. Euler により，$k = 4$ のとき予想 1 は既に証明されている．これに関し [38] において次の結果を示した．

Theorem 3.5 *$gcd(n, d) = 1$ とする．方程式 $y^2 = n(n + d) \cdots (n + (k - 1)d)$ は $n, d, k, y \in \mathbb{Z}$, $n \geq 1, d \geq 1, y \geq 1,\ 4 \leq k \leq 109$ の範囲で解をもたない．*

$k = 5$ の場合の定理は R. Obláth によって得られている．M. Bennett, N. Bruin, K. Győry, L. Hajdu によって，$6 \leq k \leq 11$ の場合もこの定理が証明されている．$d = 1$ に対しては P. Erdős と O. Rigge によって（独立に）任意の k に対して示されていた．これより，我々はここでは $d > 1$ を仮定する．この方程式では指数も未知数となる．指数が固定されているような通常の代数曲線の整数点の決定の手法は，弱すぎてあまり役に立たない．しかし各 k, d を固定し種数が 1 より大きい代数曲線になる場合，G. Faltings の定理から解が有限個に限ることは従う．

以下 $\nu > 1$ に対して $P(\nu)$ を ν の最大素因数とする．また $P(1) = 1$ と定める．b を squarefree 正整数で $P(b) < k$ なるものとする． ここで上記をさらに一般化した次の方程式を考える．$by^2 = n(n + d) \cdots (n + (k - 1)d)$. ここで $n + id = a_i x_i^2 \quad (0 \leq i < k)$ ただし a_i squarefree かつ $P(a_i) \leq \max\{P(b), k - 1\}$ とし， x_i も正整数とする．
方程式 $by^2 = n(n+d) \cdots (n+(k-1)d)$ の解は k-tuple $(a_0, a_1, \cdots, a_{k-1})$ に一意に対応する．方程式 $by^2 = n(n+d) \cdots (n+(k-1)d)$ を $by^2 = N(N-d) \cdots (N-(k-1)d), \quad N = n+(k-1)d.$ と書き直したとき，方程式 $by^2 = N(N - d) \cdots (N - (k - 1)d), \quad N = n + (k - 1)d$ は方程式 $by^2 = n(n + d) \cdots (n + (k - 1)d)$ の mirror image と呼ばれる．対応する k-tuple $(a_{k-1}, a_{k-2}, \cdots, a_0)$ についても $(a_0, a_1, \cdots, a_{k-1})$ の mirror image という．従って方程式 $y^2 = n(n+d) \cdots (n+(k-1)d)$ の mirror image は $y^2 = N(N-d) \cdots (N-(k-1)d), \quad N = n + (k - 1)d$ である．

Erdős と J. L. Selfridge は $by^2 = n(n + d) \cdots (n + (k - 1)d)$ の $d = 1$ の場合は， この方程式の右辺が k 以上の素数で割れるという仮定のもとで，解をもたないことを示した．この仮定がはずせないことも知られている．したがってここではこの方程式を常に $d > 1$ の場合に限って考える．先に述べたようにこの方程式の $k = 2, 3$ および $b = 1$ の場合は解が無限個存在する．$k = 4$ かつ $b = 6$ の場合も解が無限個あることを R. Tijdeman が示した．この無限個の解の存在は，$by^2 = n(n + d) \cdots (n + (k - 1)d)$ の方程式から得られる楕円曲線の有理点が無限個，つまり rank が正の場合への帰着をおこなうことにより得られる．
一方では， $by^2 = n(n + d) \cdots (n + (k - 1)d)$ で $k = 4$ かつ $b \neq 6$ の場合に解は無いことが知られている．したがって $k \geq 5$ を仮定して良い．

Conjecture 4 *b を squarefree 正整数で $P(b) < k$ を満たすものとし，固定する． $gcd(n, d) = 1$ とする．方程式 $by^2 = n(n + d) \cdots (n + (k - 1)d)$ は $n, d, k, y \in \mathbb{Z}$, $n \geq 1, d > 1, y \geq 1, k \geq 5$ の範囲において整数解をもたない．*

A. Granville は abc-予想を仮定するならば，整数解を持ち得る場合の方程式 $by^2 = n(n+d)\cdots(n+(k-1)d)$ の k は絶対定数で上からおさえられることを示した．さらに以下の結果が得られる [38].

Theorem 3.6 方程式 $by^2 = n(n+d)\cdots(n+(k-1)d)$ は $d > 1, P(b) < k, 5 \leq k \leq 100$ かつ $k \neq 8, k \neq 9, k \neq 14, k \neq 24$ のときに整数解を持たない．

Bennett, Bruin, Győry, Hajdu は Chabauty の方法を用いて $k = 6$ の場合に Theorem3.6 を証明している．また $k = 8$ の場合は S. Tengely の結果がある．

3.4 楕円曲線における対数一次形式の最良評価

K を有限次代数体，$\mathcal{E}_1, \ldots, \mathcal{E}_k$ を K 上定義された k 個の楕円曲線とする．次の標準形で定められているとして良い．

$$y^2 = 4x^3 - g_{2,i}x - g_{3,i} \ : \quad g_{2,i}, g_{3,i} \in K, \quad 1 \leq i \leq k.$$

Weierstraßのペエ関数およびシグマ関数を $\wp_i$,$1 \leq i \leq k$ (resp. σ_i,$1 \leq i \leq k$) とおく．周期格子を $\Lambda_i = \omega_{1,i}\mathbb{Z} + \omega_{2,i}\mathbb{Z},\ 1 \leq i \leq k$ と書くことにする．各々の $1 \leq i \leq k$ に対して $u_i \in \mathbb{C}$ を $\gamma_i \ := (\sigma_i^3(u_i), \sigma_i^3(u_i)\wp_i(u_i), \sigma_i^3(u_i)\wp_i'(u_i)) \in \mathcal{E}_i(\overline{\mathbb{Q}})$ を満たす点とする．
この $u_1, \ldots, u_k$ は楕円対数と呼ばれる．
さて $\mathcal{L}(z) = \beta_0 z_0 + \cdots + \beta_k z_k$ を恒等的にゼロではない対数一次形式 $\mathbb{C}^{k+1}$ で，K 内に係数を持つものとする．$u = (1, u_1, \ldots, u_k)$ とおく．P. Philippon と M. Waldschmidt は 1988 年に楕円対数の一次形式の評価を，楕円関数が虚数乗法を持たない場合に $|\mathcal{L}(u)|$ の下からの評価をはじめて証明をした．我々は今回，この最良評価に到達した．これは 1964 年に S. Lang によって予想されていたものである．

$\tau_i = \dfrac{\omega_{2,i}}{\omega_{1,i}}, 1 \leq i \leq k$ とおく．τ_i が上半平面 H に属すると仮定しても良い．
$h = \max\{1, h(1, g_{2,i}, g_{3,i})\ ;\ 1 \leq i \leq k\}$ とおく．これは楕円曲線の高さである．また $\hat{h}(\gamma_i)$ を γ_i における Néron–Tate の高さ ，つまり $\hat{h}(\gamma_i) = \lim_{n\to\infty} \frac{h(n\gamma_i)}{n^2}$ とする．さらに $G = G_a \times \mathcal{E}_1 \times \cdots \times \mathcal{E}_k$ とおくとこれは連結な代数群である．その tangent space$T_G(\mathbb{C})$ は $\mathbb{C}^{k+1}$ と同一視して良い．$T_{\mathfrak{G}'}(\mathbb{C})$ を G の部分代数群 G' の tangent space とする．このとき，次が得られた [19].

Theorem 3.7 (S. David-N. Hirata) k によって書ける *effective* な定数 $C > 0$ が存在して，次を満たす．
$\mathcal{L}(z) = \beta_0 z_0 + \cdots + \beta_k z_k$ を $\mathbb{C}^{k+1}$ 上の恒等的にゼロでない一次形式で K に係数をもつものとする．$\mathcal{W} = \ker(\mathcal{L}), \gamma_i = (1, \wp_i(u_i), \wp_i'(u_i)) \in \mathcal{E}_i(K) \subset \mathbb{P}^2(K)$ $(1 \leq i \leq k)$ とおく．また

$u=(1,u_1,\dots,u_k)$ とする．実数 B, E, $V_1,\dots,V_k$ を以下をみたすものとする．

$$\log B \geq \max\{1, h(\beta_i)\ ;\ 0\leq i\leq k\}$$

$$V_1\geq\cdots\geq V_k$$

$$\log V_i \geq \max\left\{\hat{h}(\gamma_i)\ ,\ \frac{|u_i|^2}{D|\omega_{1,i}|^2 Im\tau_i}\right\},\quad 1\leq i\leq k$$

$$e\leq E\leq \min\left\{\frac{|\omega_{1,i}|\left(Im\tau_i\cdot D\log V_i\right)^{\frac{1}{2}}}{|u_i|}1\leq i\leq k\right\}.$$

さて，G の連結な部分代数群 G' で $T_{G'}(\mathbb{C})\subset\mathcal{W}$ であるものは $u\notin T_{G'}(\mathbb{C})$ を満たすとする．このとき，次が得られる．

$$\log|\mathcal{L}(u)|\geq\ -C\cdot D^{2k+2}\left(\log B+\log(DE)+h+\log\log V_1\right)$$

$$\times\left(\log(DE)+h+\log\log V_1\right)^{k+1}\prod_{i=1}^{k}\left(h+\log V_i\right)\times\left(\log E\right)^{-2k-1}.$$

4　ディオファントス問題における未解決問題

4.1　いろいろな関数の値の超越性や無理数性に関する未解決問題

少し超越数論に戻ろう．

Hermite- Lindemann の定理は，α が代数的数ならば自明な場合を除き $f(\alpha)$ は超越数であるという命題を $f(z)=\exp(z)$ の場合に示したものであるから，Schneider の結果は，$g_2,g_3\in\overline{\mathbb{Q}}$ の仮定下での $f(z)=\wp(z)$ に対する命題であり，類似であると考えて良い．代数的数で必ず代数的な値をとる超越関数もあるが（P. Stäckel の 1895 年の例など，[50] 参照），代数的数では自明な場合を除いて超越的な値を取る関数は，上記のような代数群の指数写像となるものの他にも知られている．

たとえばまず簡単なのは，代数群の指数写像の話に帰着される場合である．たとえば媒介変数が $\alpha,\beta,\gamma\in\mathbb{Q}$ になっている Gauss の超幾何級数 ${}_2F_1(\alpha,\beta,\gamma:z)$ は，F. Beukers-J. Wolfart により，Wüstholz の定理を用いて，無限個の代数的数で代数的な値をとるような ${}_2F_1$ と，有限個の例外を除いて代数的数で超越的な値をとる ${}_2F_1$ に具体的に判別される ([10])．実際に代数的な値を取る場合についてはモノドロミーを詳しく調べている．

他の解析関数ではどうであろうか．

Definition 4.1 (E 関数) $E(z)=\sum_{n=0}^{\infty} a_n \frac{z^n}{n!}$ は，次の条件 *(i),(ii)* をみたすとき E 関数と呼ばれる．
(i) a_n は代数体 K に属し，その $\mathbb{Q}$ 上の共役元の絶対値の最大値を $\overline{|a_n|}$ で表すと，任意の $\epsilon>0$ に対し $\overline{|a_n|}=O(n^{\epsilon n})(n\to\infty)$ となる．
(ii) $q_n=O(n^{\epsilon n})(n\to\infty)$ となる列 $q_n\in\mathbb{N}$ で，$k=0,\ldots,n$ に対し $q_n a_k$ がすべて代数的整数となるものが存在する．

例えば，z の代数的数係数多項式，$\exp(z)$, $\sin z$, $\cos z$，Bessel 関数などは E 関数となる．E 関数の研究は C. L. Siegel が始めた．典型的な結果としてはたとえば次 [76] が得られている．

Theorem 4.1 (A. B. Shidlovskii) E 関数 $E_1(z),\cdots,E_n(z)$ を考える．
これらが，$Q_{ki}(z)\in\mathbb{C}(z)$ を係数とする連立線形微分方程式

$$Y_k'=Q_{k0}(z)+\sum_{i=1}^{n} Q_{ki}(z)Y_i \quad (k=1,\cdots,n)$$

をみたすとする．どの $Q_{ki}(z)$ の極にもならない $0\neq\xi\in\overline{\mathbb{Q}}$ に対し，$E_1(\xi),\cdots,E_n(\xi)$ が $\mathbb{Q}$ 上代数的独立であるための必要十分条件は，$E_1(z),\cdots,E_n(z)$ が $\mathbb{C}(z)$ 上代数的独立であることである．

これは Siegel-Shidlovskii の定理と呼ばれるが，その代数的な別証明もある ([4], [5])．Y. André による最近の研究が進んでいる．

さらに G 関数と呼ばれる関数を定めよう．

Definition 4.2 (G 関数) 次のような解析関数を考える．
$G(z)=\sum_{n=0}^{\infty} a_n z^n$ という関数が $c>1$ に対し次の 2 条件を満たすとする．
(i) a_n は代数体 K に属し，$\overline{|a_n|}=O(c^n)(n\to\infty)$.
((ii) $q_n=O(n^{\epsilon n})(n\to\infty)$ となる列 $q_n\in\mathbb{N}$ で，$k=0,\ldots,n$ に対し $q_n a_k$ がすべて代数的整数となるものが存在する．
このときこれを G 関数と呼ぶ．

定義において，(i),(ii) に加え線形微分方程式の解となることを入れることもある．G 関数の例としては通常の対数関数，その一般化である polylogarithm，Gauss の超幾何級数や一般超幾何関数などがある．G 関数の数論的な性質については微分方程式論とも深く関連している [3], [65].

数論において意味のある良く知られた関数として Riemann のゼータ関数 $\zeta(s)$ がある．s が 2 以上の奇整数のときに $\zeta(s)$ が超越数か否かという問題がある．最も一般的な予想としては次がある．

Conjecture 5 $\pi, \zeta(3), \zeta(5), \zeta(7), \cdots$ のすべてが $\mathbb{Q}$ 上代数的独立であろう.

ちなみに，$\mathbb{Q}$ 上代数的独立と $\overline{\mathbb{Q}}$ 上代数的独立は同じことですので，ご注意.

現在知られている結果としては R. Apéry の示した $\zeta(3)$ が無理数である事実がある．これは F. Beukers によって簡略化された証明がある．またそのあとの発展としてはつぎの T. Rivoal の仕事がある ([7], [61], [68]).

Theorem 4.2 $\epsilon > 0$ に対して十分大きい奇数の整数 a が存在し
次を満たす:
$1, \zeta(3), \zeta(5), \cdots, \zeta(a)$ によって張られた $\mathbb{Q}$ 線形空間の次元は $\dfrac{1-\epsilon}{1+\log 2}\log a$ 以上である.

改良として次の W. Zudilin の定理をあげておこう [92], [93].

Theorem 4.3 4 個の数 $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ のうち少なくとも一つは無理数である.

なお，Hurwitz ゼータ関数についての問題は下記のようなものがある.

Definition 4.3 (Hurwitz zeta function) $z \in \mathbb{C}, z \neq 0, \quad \Re e(s) > 1$ とする.
関数 $\zeta(s,z) = \sum_{n=0}^{\infty} \frac{1}{(n+z)^s}$ を *Hurwitz* ゼータ関数と呼ぶ.

明らかに $\zeta(s,1) = \zeta(s)$ である.

Hurwitz ゼータ関数については Sarvadaman Chowla および J. W. Milnor が次の予想を述べている.

Conjecture 6 (Chowla-Milnor) k および q を整数 > 1 とする.
このとき $\varphi(q)$ 個の数 $\zeta(k, a/q) \quad (1 \leq a \leq q, (a,q) = 1)$ は $\mathbb{Q}$ 上一次独立である.

この Chowla-Milnor 予想における $q = 4$ の場合は $\zeta(2n+1)/\pi^{2n+1}$ の $n \geq 1$ に対する無理数性を従える.
さらに強い形の予想も，提案されている.

Conjecture 7 (Strong Chowla-Milnor) k および q を整数 > 1 とする.
このとき $1 + \varphi(q)$ 個の数 : 1 および $\zeta(k, a/q) \quad (1 \leq a \leq q, (a,q) = 1)$ は $\mathbb{Q}$ 上一次独立である.

これはゼータ関数 $\zeta(k)$ の値の無理数性も従える．

polylogarithms についての予想も与えられている．これらは Sanoli Gun, Ram Murty および Purusottam Rath によるものである．

Definition 4.4 (Polylogarithms) $k \geq 1$ および $|z| < 1$ に対して $\mathrm{Li}_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}$ を考える．この $\mathrm{Li}_k(z)$ は *polylogarithm* もしくは *polylogarithmic* 関数と呼ばれる．

定義から直ちに $\mathrm{Li}_1(z) = \log(1-z)$ および $\mathrm{Li}_k(1) = \zeta(k)$ が $k \geq 2$ に対して成立する．
E. M. Nikishin の結果 ([63]) の発展として，Rivoal はこの polylogarithm $Li_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}$ （但し $k = 1$ ならば $|z| < 1$， $k \geq 2$ ならば $|z| \leq 1$）に対しても $x \in \mathbb{Q}$， $0 < |x| < 1$ ならば $Li_j(x) \notin \mathbb{Q}$ となる $j \in \mathbb{Z}$ は無限個存在する事実を証明した．

polylogarithm についての予想としては下記がある．

Conjecture 8 (Polylogarithms Conjecture) 整数 $k > 1$ をとる．
$\alpha_1, \ldots, \alpha_n$ を代数的数として，$\mathrm{Li}_k(\alpha_1), \ldots, \mathrm{Li}_k(\alpha_n)$ は $\mathbb{Q}$ 上一次独立であると仮定する．このとき $\mathrm{Li}_k(\alpha_1), \ldots, \mathrm{Li}_k(\alpha_n)$ は $\overline{\mathbb{Q}}$ 上でも一次独立である．

もしも Polylogarithms Conjecture が正しければ，Chowla-Milnor conjecture が全ての k と全ての q に対して正しいことも知られている．

なお，E 関数に関する Shidlovskii の結果から，次の古い定理が再び得られる．Lindemann-Weierstrass の定理：代数的数 $\alpha_1, \cdots, \alpha_n$ が $\mathbb{Q}$ 上一次独立なら，$e^{\alpha_1}, \cdots, e^{\alpha_n}$ は $\mathbb{Q}$ 上代数的独立である．これを $\alpha_1, \cdots, \alpha_n$ が代数的数とは限らなくても成立するという主張が Schanuel 予想であり，まだ未解決である．

Conjecture 9 (Schanuel 予想) n 個の複素数 $x_1, \cdots, x_n$ が $\mathbb{Q}$ 上一次独立であるとする．
このとき，体 $\mathbb{Q}(x_1, \cdots, x_n, e^{x_1}, \cdots, e^{x_n})$ の $\mathbb{Q}$ 上の超越次数は n 以上である．

この特別な場合である未解決予想として，次の Gel'fond の予想がある：

Conjecture 10 (Gel'fond の予想)　代数的数 α は $\alpha \neq 0, 1$ であるとする．
$1, \beta_1, \cdots, \beta_n$ は $\mathbb{Q}$ 上一次独立な代数的数だとする．このとき，$\alpha^{\beta_1}, \cdots, \alpha^{\beta_n}$ は $\mathbb{Q}$ 上代数的独立となる．

これに関しての部分的な進展としては $\mathbb{Q}$ 上 d 次 ($d \geq 2$) の代数的数 γ に対して体 $\mathbb{Q}(\alpha^{\gamma}, \cdots, \alpha^{\gamma^{d-1}})$ の $\mathbb{Q}$ 上超越次数が $[\frac{d+1}{2}]$ 以上（$[x]$ は x を超えない整数）であることを示した G. Diaz の結果

がある ([62]).
代数的独立性に関して知られる他の未解決予想としては，Schneider の 8 問題 ([73]) の第 1 問である 4 指数問題 four exponential conjecture がある．

Conjecture 11 (4 指数問題) x_1, x_2 と y_1, y_2 を各々$\mathbb{Q}$ 上一次独立な複素数とする．
このとき *4* 数 $\exp(x_i y_j)(1 \leq i, j \leq 2)$ のうち少なくとも *1* 個は超越数であろう．

この 4 指数問題の系として，例えば上半平面の元 τ に対し $\exp(2\pi i\tau)$ と $\exp(-\dfrac{2\pi i}{\tau})$ は同時には代数的数にならないという予想が含まれる ([62], [88]).

4.2 対数一次形式に関する未解決問題

対数一次形式に関連する未解決問題として，次がある．

Conjecture 12 $\ell_1, \cdots, \ell_n \in \mathcal{L}$ が $\mathbb{Q}$ 上一次独立ならば，$\ell_1, \cdots, \ell_n$ は $\mathbb{Q}$ 上代数的独立であろう．

正標数では W. D. Brownawell と M. Papanikos により解決された．

なお，Baker の一連の理論と関連づけられる数のことを「Baker 周期」と称する．この定義は「代数的数の対数で張られた $\overline{\mathbb{Q}}$ 上の線形空間の元」である．Euler 定数 γ はこの意味で，あるいはもっと広い意味で「周期」にはならないであろうということが，Kontsevich と Zagier によって予想されている．

4.3 *abc* 予想

p 進対数一次形式とは，*abc* 予想との関連によって急に着目されているがもともとは対数一次形式の理論の p 進アナロジーであるから，考えられるのは自然なものである．

さて，*abc* 予想は整数論の最大の未解決問題の一つである．整数論の様々な問題と深く関わっていることが知られている．Mordell 予想や Fermat の大定理もここから従うし，素数の分布に関しても多くの結果が従う．

いま a, b, c を $\gcd(a, b, c) = 1$ をみたす正整数とする．コンダクターと呼ばれる次の数 N を次のように定義する．

$$N = N(a, b, c) = \prod_{p|abc} p.$$

1985 年に D. W. Masser と J. Oesterlé が次の予想を提出した.

Conjecture 13 (有理数体上での abc 予想) 任意の正の数 ϵ について ϵ のみに依存する正定数 $C(\epsilon)$ が存在し、

$$a+b=c \quad , \quad gcd(a,b,c)=1 \tag{5}$$

を満たす任意の正整数 a,b,c に対して

$$c < C(\epsilon)N^{1+\epsilon} \tag{6}$$

が成り立つ.

これについて，いくつか部分的な結果があるが，それらを述べる前に関数体における abc 予想はすでに解決されているのでそれを紹介しよう.

関数体での abc 予想には N. Snyder による簡素化されたものなどの様々な証明がある．初めて証明をしたのは R. C. Mason である．いま，複素数を係数とする多項式 $f(x) \in \mathbb{C}[x]$ を考える．$f(x)$ の相異なる既約因子の数を $N_0(f)$ とする．重複因子のない 1 変数多項式に対しては $N_0(f)$ は $\deg f$ 個に等しいが，2 変数以上では一般に $\deg f$ 個以下になる.

Theorem 4.4 (R. C. Mason) $f,g,h \in \mathbb{C}[x]$ を定数でない 2 つずつ互いに素な多項式で $f+g=h$ を満たすものとする．このとき

$$\max(\deg f, \deg g, \deg h) \leq N_0(fgh) - 1$$

が成り立つ.

Mason の定理を多変数に拡張した場合についても考察されており，H. N. Shapiro と G. H. Sparer は Mason の定理の一般化として m 変数 $(m \geq 1)$，n 個 $(n \geq 3)$ の多項式に対して類似が成り立つことを証明した.

4.4 p 進対数一次形式

さて，上記の abc 予想について，進展は実は余り無い．しかし p 進対数一次形式がその「指数版程度に右辺が大きい評価」を与えるものであることを, 以下に述べておこう.
1986 年に C. L. Stewart と R. Tijdeman は abc 予想に関し部分的結果:

$$c < exp(C_1 N) \tag{7}$$

を発表した．ここで $C_1 > 0$ は絶対定数である．この証明には p 進付値における対数一次形式の評価を用いるが，1991 年に Stewart と K. Yu により改良された．これは Yu による p 進対数一次形式の下からの評価の改良に負う.

Theorem 4.5 (C. L. Stewart & K. Yu) 正定数 C_2 が存在して次が成り立つ.
$a+b=c,\ gcd(a,b,c)=1$ である任意の正整数 a,b,c に対し、

$$c < exp(C_2 N^{1/3}(\log N)^3) \tag{8}$$

が成立する.

これには Yu により更に改良された p 進対数一次形式の評価のみならずアルキメデス的付値における E. Matveev の対数一次形式の評価も用いられている. a,b,c の最大の素因数を用いた表示による次の改良も得られる. p_a, p_b, p_c を a,b,c の最大素因数とする. $p_1=1$ とおく.
$\log_i$ によって対数関数の i 回繰り返しつまり $\log_1 t = \log t$, $\log_i t = \log(\log_{i-1} t)(i=2,3\cdots)$ と表わす.

Theorem 4.6 (C. L. Stewart & K. Yu) 正定数 C_3 が存在し次が成り立つ.
$a+b=c,\ \ gcd(a,b,c)=1,\ c\geq 3$ である任意の正整数 a,b,c について $N^*=\max(N,16)$,
$p'=\min\{p_a,p_b,p_c\}$ に対し

$$c < exp(p' C_3 N^{(\log_3 N^*/\log_2 N)}) \tag{9}$$

が成立する.

参考文献

[1] B. Adamczewski & Y. Bugeaud, On the complexity of algebraic numbers II. Continued fractions, Acta Math., 195 (2005), 1-20.

[2] M. Amou, On Sprindžuk's classification of transcendental numbers, J. reine. angew, Math. 470, 27–50, 1996.

[3] Y. André, *G*-functions and Geometry, Aspects of Mathematics, E13, Vieweg, 1989.

[4] Y. André, Séries Gevrey de type arithmétique I: Théorèmes de pureté et de dualité, Ann. of Math., 151, No. 2, 705–740, 2000.

[5] Y. André, Séries Gevrey de type arithmétique II: Transcensance sans transcensance, Ann. of Math., 151, No. 2, 741–756, 2000.

[6] A. Baker, Transcendental Number Theory, Cambridge Univ. Press, 1975.

[7] K. M. Ball & T. Rivoal, Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs, Invent. Math., 146, 1, 193–207, 2001.

[8] V. I. Bernik & M. M. Dodson, Metric diophantine Approximation on Manifolds, Cambridge Univ. Press, 1999.

[9] M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, and J. P. Schreiber, Pisot and Salem numbers, Birkhäuser, Basel, 1992.

[10] F. Beukers & G. Wolfart, Algebraic Values of hypergeometric functions, in New advances in Transcendence Theory (ed. A. Baker), Cambridge Univ. Press, 68–81, 1988.

[11] E. Bombieri, Forty Years of Effective Results in Diophantine Theory, in A Panorama in Number Theory (ed. G. Wüstholz) Cambridge University Press, 194–213, 2002.

[12] Z. I. Borevich & I. R. Shafarevich, Number Theory, Academic Press, 1966. 邦訳　ボレビッチ・シャハレビッチ，佐々木義雄訳，整数論 (上)(下) 数学叢書 14 POD 版，吉岡書店，2000.

[13] J. W. S. Cassels, An introduction to the geometry of numbers, Grundl. Math. Wiss. 99, Springer, 1959, corrected reprint, Springer, 1971.

[14] P. Corvaja & U. Zannier, A subspace Theorem approach to integral points on curves, C. R. Acad. Sci. Paris, Ser. I , 334 (2002), 267-271.

[15] P. Corvaja & U. Zannier, Some new applications of the Subspace Theorem, Compositio Math., 131 (2002), 319-340.

[16] P. Corvaja & U. Zannier, On integral points on surfaces, Ann. of Math., 160 (2004), 705-726.

[17] J. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups, Springer, 1988.

[18] H. S. M. Coxeter, Introduction to Geometry, John Wiley & Sons, New York, 1961.

[19] S. David & N. Hirata-Kohno, Recent progress on linear forms in elliptic logarithms, in A Panorama in Number Theory (ed. G. Wüstholz) Cambridge University Press, 26–37, 2002.

[20] M. Drmota, R. F. Tichy, Sequences, discrepancies and applications. Lecture Notes in Mathematics, 1651. Springer-Verlag, Berlin, 1997.

[21] B. Edixhoven & J.-H. Evertse, Diophantine Approximation and Abelian Varieties, Lecture Notes in Math., 1566, Springer, 1993.

[22] E. Ehrhart, Sur une probleme de geometrie diophantine linéaire, J. reine angew. Math. 227, 1–29, 1967.

[23] J. -H. Evertse, An improvement of the quantitative Subspace theorem, Compositio Math., 101, 225–311, 1996.

[24] J. -H. Evertse, Symmetric improvements of Liouville's inequality. J. reine angew. Math. 527, 69–95, 2000.

[25] J. -H. Evertse, Linear equations with unknowns from a multiplicative group whose solutions lie in a small number of subspaces, Indag. Math. 15, 2004, 347-355.

[26] J. -H. Evertse & R. G. Ferretti, Diophantine inequalities on projective varieties, Intern. Math. Res. Not. 2002:25, 1295–1330, 2002.

[27] J. -H. Evertse & H. P. Schlickewei, The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group, in Number Theory in Progress, I, (eds. K. Győry, H. Iwaniec, J. Urbanowicz), Walter de Gruyter, 121–142, 1999.

[28] J. -H. Evertse & H. P. Schlickewei, A quantitative version of the Absolute Subspace Theorem, J. reine angew. Math. 548, 21–127, 2002.

[29] J. -H. Evertse, H. P. Schlickewei & W.M. Schmidt, Linear equations in variables which lie in a multiplicative group, Ann. Math. 155, 1–30, 2002.

[30] G. Faltings, Diophantine approximation on abelian varieties, Ann. of Math., 133, 549–576, 1991.

[31] G. Faltings & G. Wüstholz, Diophantine approximations on projective spaces, Invent. Math., 116, 109–138, 1994.

[32] G. Faltings, A New Application of Diophantine Approximations, in A Panorama of Number Theory (ed. G. Wüstholz), Cambridge Univ. Press, 231–246, 2002.

[33] F. Gramain, Sur les degrés des nombres algébriques, $\cos(2\pi/n)$ et $\sin(2\pi/n)$, Séminaire d'Arithmétique de Saint-Étienne, 1990-91-92, 24–27.

[34] F. Gramain, Les degrés des nombres algébriques, $\cos(2\pi/n)$ et $\sin(2\pi/n)$ et la transcendance de π,
Gazette des Mathématiciens, No.58, novembre, 1993, 29–37.

[35] F. Gramain, Encore $\cos(2\pi/n)$ et $\sin(2\pi/n)$,
Séminaire d'Arithmétique, Saint-Étienne, 1994-95, No.4, 47–53.

[36] P. M. Gruber, C. G. Lekkerkerker, Geometry of numbers, North-Holland, 1987 (first edition by C. G. Lekkerkerker, 1969).

[37] N. Hirata-Kohno, Formes linéaires de logarithmes de points algébriques sur les groupes algébriques, Invent. Math. 104, 401–433, 1991.

[38] N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman, An extension of a theorem of Euler, Acta Arithmetica, to appear.

[39] E. Hlawka, Zur Geometrie des Zahlen, Math. Zeit., 49, 285–312, 1943.

[40] M. N. Huxley, Area, lattice points, and exponential sums. London Mathematical Society Monographs. New Series, 13. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1996.

[41] 河田敬義, 数論 -古典数論から類体論へ-, 岩波書店, 1992.

[42] A. Y. Khinchin, Continued fractions, Chicago Univ. Press, 1964.

[43] E. Krätzel, Lattice points. Mathematics and its Applications (East European Series), 33. Kluwer Academic Publishers Group, Dordrecht, 1988.

[44] L. Kuipers and H. Niederreiter, Uniform Distribution of Sequences. John Wiley, New York, 1974.

[45] S. Lang (ed.), Number Theory III, Encyclopaedia of Mathematical Sciences Vol. 60, Springer, 1991.

[46] M. Laurent, Équations diophantiennes exponentielles, Invent. Math. 78, 1984, 299-327.

[47] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovasz, Factoring Polynomials with Rational Coefficients, Math. Ann., 261, 1982. North-Holland Math. Library, Vol 37, 第2版 1987

[48] J. H. Loxton, Automata and transcendence, in New advances in Transcendence Theory (ed. A. Baker), Cambridge Univ. Press, 1988, 215–228.

[49] K. Mahler, Arithmetische Eigenschaften einer Klasse von Dezimalbrûchen, Proc. Akad. Wetensch. Amsterdam 40, 1937, 421–428.

[50] K. Mahler, Lectures on Transcendental Numbers, Lecture Notes in Math. 546, Springer, 1976.

[51] D. W. Masser & G. Wüstholz, Isogeny estimates for abelian varieties and finiteness theorem, Ann. Math., II, Ser 137, 459–472, 1993.

[52] D. W. Masser, Yu. V. Nesterenko, H. P. Schlickewei, & M. Waldschmidt, Diophantine approximation :Lectures from the C.I.M.E. Summer School held in Cetraro 2000. Edited by F. Amoroso and U. Zannier, Lecture Notes in Math. 1819, , Springer, 2003.

[53] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. (Russian) Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), no. 6, 125–180; translation in Izv. Math. 64 (2000), no. 6, 1217–1269.

[54] E. M. Matveev, On the successive minima of the extended logarithmic height of algebraic numbers. (Russian) Mat. Sb. 190 (1999), no. 3, 89–108; translation in Sb. Math. 190 (1999), no. 3-4, 407–425.

[55] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. (Russian) Izv. Ross. Akad. Nauk Ser. Mat. 62 (1998), no. 4, 81–136; translation in Izv. Math. 62 (1998), no. 4, 723–772.

[56] H. Minkowski, Geometrie des Zahlen, Teubner, 1896 and 1910, reprint, Chelsea, 1953.

[57] H. Minkowski, Diophantische Approximationen, Teubner, 1907 and 1927.

[58] H. Minkowski, Gesammelte Abhandlungen I, II, Teubner, 1911, reprint, Chelsea, 1967.

[59] T. Mitsui, 解析数論，共立講座現代の数学 12, 共立出版, 1977.

[60] Y. Morita, On transcendency of special values of arithmetic automorphic functions, J. Math. Soc. Japan, 24, No. 2, 268–274, 1972.

[61] Yu. V. Nesterenko, A few remark on $\zeta(3)$, Math. Notes 59, 6, 625–636, 1996.

[62] Yu. V. Nesterenko & P. Philippon, Introduction to Algebraic Independence Theory, Lecture Notes in Math. 1752, Springer, 2001.

[63] E. M. Nikishin, On the irrationality of the numbers of the functions $F(x, s)$, Mat. Sbornik 37, 3, 381–388, 1979.

[64] K. Nishioka, Mahler Functions and Transcendence, Lecture Notes in Math. 1631, Springer, 1996.

[65] A. N. Parshin & I. R. Schfarevich (eds.), N. I. Fel'dman & Yu. V. Nesterenko (authors), Number Theory IV, Encyclopaedia of Mathematical Sciences Vol 44, 1998.

[66] J. Pommersheim, Toric Varieties, Lattices Points, and Dedekind Sums, Math. Ann., 295, 1-24, 1993.

[67] N. Pytheas-Fogg, Substitutions in Dynamics, Arithmetics and Combinatorics, Lectures Notes in Mathematics 1794, Springer-Verlag, 2002.

[68] T. Rivoal, Irrationalité d'au moins un des neuf nombres $\zeta(5), \zeta(7), \cdots, \zeta(21)$, Acta Arith. 103, 2, 157–167, 2002.

[69] D. Roy & J. L. Thunder, An absolute Siegel's lemma, J. Reine Angew Math. 476, 1–26, 1996, Addendum and erratum, ibidem, 508, 47–51, 1999.

[70] W. M. Schmidt, Norm form equations, Ann. of Math., (2) 96, 526–551, 1972.

[71] W. M. Schmidt, Diophantine approximation, Lecture Notes in Math., 785, Springer, 1980.

[72] W. M. Schmidt, Diophantine approximation and Diophantine Equations, Lecture Notes in Math., 1467, Springer, 1991.

[73] T. Schneider, Einführungn in die transzendenten Zahlen, Grundlehren 81, Springer, 1957 (translated in French, Gauthier-Villars, 1959).

[74] F. Schweiger, Ergodic Theory of Fibered Systems and Metric Number Theory, Oxford: Clarendon Press.

[75] M.Senechal, Quasicrystals and Geometry. New York: Cambridge University Press, 1995.

[76] A. B. Shidlovski, Transcendental Numbers, Walter de Gruyter, 1989.

[77] H. Shiga & J. Wolfart, Criteria for complex multiplication and transcendence properties of automorphic functions, J. reine angew. Math. 463, 1–25, 1995.

[78] C. L. Siegel, Transcendental numbers, Princeton Univ. Press, 1949.

[79] C. L. Siegel, Lectures on the Geometry of Numbers, Springer, 1989.

[80] J. H. Silverman, The arithmetic of Elliptic curves, GTM 106, Springer, 1986.

[81] A. Thue, Über Annäherungswerte algebraischer Zahlen, J. Reine Angew. Math. 135, 184–305, 1909.

[82] J. Thunder, Decomposable form inequalities. Ann. of Math. (2) 153, no. 3, 767–804, 2001.

[83] P. Vojta, Siegel's theorem in the compact case, Ann. of Math., 133, 509–548, 1991.

[84] P. Vojta, Integral points on subvarieties of semiabelian varieties I, Invent. Math., 126, 133–181, 1996.

[85] P. Vojta, Integral points on subvarieties of semiabelian varieties II, Amer. J. Math., 121, 283–313, 1999.

[86] M. Waldschmidt, Nombres transcendents, Lecture Notes in Math. 402, Springer, 1974.

[87] M. Waldschmidt, Nombres transcendents et groupes algébriques, Astérisque 69/70, 1979.

[88] M. Waldschmidt, Diophantine Approximation on Linear Algebraic Groups, Grundlehren der Math. Wissenschften 326, Springer, 2000.

[89] A. Walfisz, Weylsche Exponentialsummen in der neueren Zahlentheorie. (German) Mathematische Forschungsberichte, XV. VEB Deutscher Verlag der Wissenschaften, Berlin, 231 pp, 1963.

[90] G. Wüstholz, Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen, Ann. Math. 129, 501–517, 1989.

[91] G. Wüstholz, A Panorama of Number Theory, Cambridge Univ. Press, 2002.

[92] W. Zudilin, One of the numbers $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ is irrational, Russian Math. Surveys 56, 4, 774–776, 2001.

[93] W. Zudilin, Irrationality of values of the Riemann zeta function, Izvestiya Mathematics 66, 3, 489–542, 2002.