

# Liouville の定理の拡張

灘高校 3 年 西本 将樹

## 1 概要

定義 1 ある整係数多項式の根となる複素数を、代数的数という。また、代数的数  $\alpha$  に対して、 $\alpha$  を根にもつ整係数多項式  $a_0 + a_1x + \cdots + a_nx^n$  であって、次数  $n$  が最小であるもののうち、 $a_n > 0, (a_0, a_1, \dots, a_n) = 1$  を満たすものを、 $\alpha$  の最小多項式という。また、代数的数  $\alpha$  の最小多項式の次数が  $n$  であるとき、 $\deg\alpha = n$  とかき、 $\alpha$  は  $n$  次代数的数であるという。

代数的数に関して次の定理が知られている。

定理 2 (Liouville の定理)  $n(\geq 2)$  次実代数的数  $\alpha$  に対して、正定数  $c = c(\alpha)$  が存在し、不等式

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{q^n}$$

が全ての有理数  $\frac{p}{q}(q > 0)$  に対して成り立つ。

つまり、代数的数の有理数による近似にはある種の限界があるという事である。この定理によって、初めて超越数の存在が示された。

系 3  $\sum_{k=0}^{\infty} 2^{-k!}$  は超越数である。

証明

$$\alpha = \sum_{k=0}^{\infty} 2^{-k!}, \frac{p_m}{q_m} = \sum_{k=0}^m 2^{-k!}, q_m = 2^{m!} \text{ とおくと、} 0 < \alpha - \frac{p_m}{q_m} < \frac{2}{q_m^{m+1}} \text{ が成り立つ。}$$

一方、 $\alpha$  を  $n$  次代数的数と仮定すると、正定数  $c$  が存在して

$$\left| \alpha - \frac{p_m}{q_m} \right| > \frac{c}{q_m^n}$$

従って、 $\frac{c}{q_m^n} < \frac{2}{q_m^{m+1}}$  であるが、この不等式は  $m$  が十分大きいとき成立しない。証明終

さて、Liouville の不等式を拡張することを目的とする。ここでは、上定理の「有理数  $\frac{p}{q}$ 」を一般の代数的数に替えたときにどのような評価が得られるかを考察しよう。

## 2 評価しよう

$\alpha, \beta (\alpha \neq \beta)$  を代数的数とし、 $\alpha$  の最小多項式を、 $f(x) = a_0 + a_1x + \cdots + a_nx^n$   
 $\beta$  の最小多項式を、 $g(x) = b_0 + b_1x + \cdots + b_mx^m$  とする。

$|\beta - \alpha| \leq 1$  のときについて考える。

$F(z) = \left| \frac{f(z)}{z - \alpha} \right|$  とする。 $F$  は連続であるから、領域  $|z - \alpha| \leq 1$  において最大値をもつ。それを  $C_1$ <sup>\*1</sup> とす  
るとき、 $|f(\beta)| = F(\beta) |\beta - \alpha| \leq C_1 |\beta - \alpha|$

$$\therefore |\beta - \alpha| \geq \frac{1}{C_1} |f(\beta)|$$

さて、 $f(x), g(x)$  は既約多項式なので、<sup>\*2</sup>  $f(x) \neq g(x)$  であれば  $f(x), g(x)$  は互いに素であるから、

$$f(x)p(x) + g(x)q(x) = 1$$

となる  $m - 1$  次以下の多項式  $p(x)$  と、 $n - 1$  次以下の多項式  $q(x)$  が存在する。

$$p(x) = p_0 + p_1x + \cdots + p_{m-1}x^{m-1}, q(x) = q_0 + q_1x + \cdots + q_{n-1}x^{n-1}$$

とすれば、 $p_0, p_1, \dots, p_{m-1}, q_1, q_2, \dots, q_{n-1}$  は次のような連立 1 次方程式の解である。

$$\left( \begin{array}{ccccccccc} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & & \vdots \\ a_2 & a_1 & \ddots & 0 & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & a_0 & \vdots & \vdots & & \ddots & 0 \\ \vdots & \vdots & & & \vdots & b_m & \vdots & & b_0 \\ a_n & \vdots & & & 0 & b_m & & & \vdots \\ 0 & a_n & & \vdots & \vdots & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 & \cdots & \cdots & 0 & b_m \end{array} \right) \left( \begin{array}{c} p_0 \\ p_1 \\ \vdots \\ p_{m-1} \\ q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{array} \right) = \left( \begin{array}{c} 1 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{array} \right)$$

この  $m + n$  次正方行列を  $A, A$  の第  $i$  列を  $\left( \begin{array}{c} 1 \\ 0 \\ \vdots \\ 0 \end{array} \right)$  で置き換えた行列を  $A_i$  とすると、Cramer の公式より、

$$p_i = \frac{\det A_i}{\det A}$$

ここで、次の定理を用いる。

<sup>\*1</sup> 今後  $C_1, C_2, \dots$  は全て  $\alpha$  のみに依存する、つまり、 $\beta$  とか  $b_i$  とかに関係無く決まる定数を表します。

<sup>\*2</sup>  $f(x) = f_1(x)f_2(x)$  と分解出来たとすると  $f_1(\alpha) = 0$  または  $f_2(\alpha) = 0$  で  $f$  が最小多項式である事に矛盾するから。

定理 4 (Hadamard の不等式) <sup>\*3</sup>  $A = (a_{ij})$  を任意の  $n$  次正方行列とするとき、不等式

$$|A|^2 \leq \prod_{i=1}^n \left( \sum_{j=1}^n a_{ij}^2 \right)$$

が成り立つ。

さて、Hadamard の不等式より、

$$|p_i|^2 \leq |\det A_i|^2 \leq (a_0^2 + a_1^2 + \cdots + a_n^2)^{m-1} (b_0^2 + \cdots + b_m^2)^n$$

$$|p_i| \leq C_2^m (b_0^2 + \cdots + b_m^2)^{\frac{n}{2}} \quad (C_2 = (a_0^2 + \cdots + a_n^2)^{\frac{1}{2}})$$

$$f(\beta)p(\beta) + g(\beta)q(\beta) = 1 \text{ で } g(\beta) = 0 \text{ であるから、} |f(\beta)| = \frac{1}{|p(\beta)|}$$

$$|p(\beta)| = \left| \sum_{i=0}^{m-1} p_i \beta^i \right| \leq C_2^m (b_0^2 + \cdots + b_m^2)^{\frac{n}{2}} \sum_{i=0}^{m-1} |\beta|^i$$

$|\beta| = |\alpha + (\beta - \alpha)| \leq |\alpha| + |\beta - \alpha| \leq |\alpha| + 1$  であるから、

$$\sum_{i=0}^{m-1} |\beta|^i \leq (1 + |\beta|)^m \leq (2 + |\alpha|)^m$$

$$\therefore |p(\beta)| < C_3^m (b_0^2 + \cdots + b_m^2)^{\frac{n}{2}} \quad (C_3 = C_2(2 + |\alpha|))$$

$$|\beta - \alpha| \geq \frac{1}{C_1} \frac{1}{|p(\beta)|} > \frac{1}{C_1} \frac{1}{C_3^m} \frac{1}{(b_0^2 + \cdots + b_m^2)^{\frac{n}{2}}} \geq \frac{C_4^m}{(b_0^2 + \cdots + b_m^2)^{\frac{n}{2}}}$$

ただし  $C_4 = \min\{\frac{1}{C_1 C_3}, \frac{1}{C_3}\}$  とする。

さて、これは  $|\beta - \alpha| \geq 1$  でしかも  $f(x) \neq g(x)$  の場合であった。

残りの場合は簡単に処理できる (余り本質的では無い)。

まず、 $f(x) = 0$  の解を、 $\alpha_1 (= \alpha), \alpha_2, \dots, \alpha_m$  として、 $C_6 = \min_{2 \leq i \leq m} \{|\alpha_i - \alpha|\}$ ,  $C_7 = \min\{1, C_6\}$  とする。そうすれば、除かれていた場合において、

$$|\beta - \alpha| \geq C_7 \geq \frac{C_7^m}{(b_0^2 + \cdots + b_m^2)^{\frac{n}{2}}}$$

最後に  $C = \min\{C_4, C_7\}$  とすれば、 $C$  は  $\alpha$  のみによって定まる定数であって、 $\alpha \neq \beta$  なる任意の代数的数  $\beta$  に対して

$$|\beta - \alpha| \geq \frac{C^m}{(b_0^2 + \cdots + b_m^2)^{\frac{n}{2}}}$$

よって次の定理が得られた。

---

<sup>\*3</sup> ハダマードと読むのではなくアダマールと読みます

定理 5  $n(\geq 2)$  次実代数的数  $\alpha$  に対して、正定数  $c = c(\alpha)$  が存在し、 $\alpha \neq \beta$  なる任意の代数的数  $\beta$ , その最小多項式<sup>\*4</sup>  $b_0 + b_1x + \cdots + b_nx^n$  に対して不等式

$$|\alpha - \beta| > \frac{c^m}{(b_0^2 + b_1^2 + \cdots + b_n^2)^{\frac{n}{2}}}$$

が成り立つ。

この定理が今回の主要な結果です。ところでこの話をある所でした時に、「それは Liouville を含んでいるのか（つまり拡張になっているか）」という質問を受けました。実際、なっています。大雑把にですが説明しましょう。

先ほどの証明の最後を見れば分かるように、この定理の本質は  $|\alpha - \beta|$  が十分小さいときになります。つまり、 $\frac{p}{q}$  が十分  $\alpha$  に近い時について考えれば良いわけです。 $\frac{p}{q}$  の最小多項式は  $qx - p = 0$  ですが、 $\frac{p}{q}$  が十分  $\alpha$  に近い時は、 $p$  と  $q$  は大体比例していて、 $p^2 + q^2$  は、ほぼ  $q^2$  に比例、従って定数倍でおさえられます。それに定理 5 を適用すればちゃんと Liouville が出てきますね。

### 3 今後の課題など

実は以前から、代数的数の有理近似という分野には興味があったが、何も有利近似に拘らなくても、例えば 2 次無理数で近似するなどという事も考えてみても面白いのでは無いかと思っていたというのが動機です。今回調べてみて、それなりに綺麗な結果が出て、Liouville 型の不等式を代数的数による近似に拡張するという当初の目的は達成出来た。ただ、Liouville の定理自体、歴史的意味は大きいものの元々すごく弱い定理で、この定理の拡張形も、色々と試行錯誤をしてみたけれど、余りある数の超越数を示すのには向かないようでした。勿論いくつかの応用は出来たけれど、いかにもわざとらしく作った数に対してのみ有効なようです。

Liouville 型の不等式に関して、かなり強い形の次の不等式が知られています。

定理 6 (リドウ (Ridout) の定理)  $\alpha \neq 0$  を代数的数とする。

$P_1, \dots, P_s, Q_1, \dots, Q_t$  を相異なる素数,  $d > 0, 0 \leq \lambda \leq 1, 0 \leq \rho \leq 1$  とする。 $p, q$  を次の形の整数とする。

$$p = p^* P_1^{\sigma_1} \cdots P_s^{\sigma_s}, q = q^* Q_1^{\tau_1} \cdots Q_t^{\tau_t}$$

ただし  $\sigma_1, \dots, \sigma_s, \tau_1, \dots, \tau_t$  は非負整数で、 $p^*, q^*$  は

$$0 < |p^*| \leq dp^\lambda, 0 < |q^*| \leq dq^\rho$$

を満たす。この時  $\kappa > \lambda + \rho$  ならば、不等式

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\kappa}$$

を満たす  $p, q$  は有限個しかない。

$\lambda = \rho = 1$  の場合は、1955 年に証明された次の定理である。

<sup>\*4</sup> 実は証明に使われているのは、 $f(x)$  と  $g(x)$  が互いに素である事だけなので、最小多項式である必要はありません。次の節でこの例も持ち出します。

定理 7 (ロス (Roth) の定理)  $\alpha$  を  $n(\geq 2)$  次代数的数、 $\kappa > 2$  とすると、不等式

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\kappa}$$

を満たす  $p, q$  は有限個しかない。

このような定理に対しても、有理近似に限らなくても似た形の結果が言えないかと思っています。代数体上の”代数的数”を代数体上の”有理数”で近似すると見なせる点では、類似していると思うので。こういった事に関する事も今後調べてみたいなと思っています。

今回の記事に関して意見や質問があれば [nisimotomasaki@funifuni.net](mailto:nisimotomasaki@funifuni.net) までお願いします。