

多項式の零点不在領域と
その数式処理への応用に関する研究

山本 修身

①

多項式の零点不在領域と
その数式処理への応用に関する研究

山本修身

論文概要

本論文は、実数または複素数を係数にもつ多項式 $f(x)$ について、ある複素数 α を $f(x)$ へ代入したときの値から決定される $f(x)$ の零点の存在しない領域の解析とその応用について論じたものである。本論文では、ノルムとして 2-ノルム, 1-ノルムおよび ∞ -ノルムを考える。それぞれのノルムについて、 $\alpha = 0$ のときのこの領域を解析することにより、大まかな零点の存在範囲を求める。また、この概念をいくつかの零点を組にしたものに拡張することにより、2-ノルムについては良く知られた Landau の不等式の別証を与え、1-ノルムについても二つの零点に関して Landau の不等式に良く似た形の不等式を導く。また、さらに、このような領域を 2-ノルムについて実際にいくつかの実数 α について計算することにより、与えられた整係数多項式が実数を零点として持たないことを証明するアルゴリズムを構成する。そして、このアルゴリズムを不等式系などを証明するために応用する。

目次

論文概要	i
目次	ii
1 序論	1
1.1 本研究の概要	1
1.2 本研究の背景	8
2 零点不在領域の定義とその基本的性質	10
2.1 1点のまわりの零点不在領域	10
2.2 複数の零点の零点不在領域の定義	18
3 2-ノルムに関する結果	22
3.1 2-ノルムにおける穴の記述	22
3.2 0のまわりの穴に関する結果	25
3.3 任意の数のまわりの穴の解析	29
4 1-ノルムに関する結果	33
4.1 0のまわりの穴に関する結果	33
4.2 実係数多項式についての任意の実数のまわりの穴の解析	40
4.3 複素係数多項式についての任意の複素数のまわりの穴の解析	43
5 ∞ -ノルムに関する0のまわりの穴についての結果	49
6 2-ノルムの抑えられた整係数多項式の零点の分布について	54
6.1 穴と整係数多項式の零点の分布との関係について	54
6.2 零点の集合 $Z(M, \infty)$ による有理数の近似について	57

7 複数の零点の穴についての結果	63
7.1 Landau の不等式とその別証	63
7.2 1-ノルムについての結果	66
8 2-ノルムによる零点の存在範囲の応用	72
8.1 ポテンシャル関数 $\phi(\beta)$ の性質	72
8.2 整係数多項式が実零点を持たないことを証明するアルゴリズム	76
8.3 不等式の証明への応用例	89
9 代数的数の複雑さとその応用	94
9.1 初等幾何学の定理証明について	94
9.2 初等幾何学の定理の計算過程	95
9.3 数の複雑さの定義と有理数の四則演算による複雑さの解析	99
9.4 代数体上の演算	103
10 結論	110
謝辞	115
参考文献	116

第 1 章

序論

本章では、本論文で取り扱った問題および得られた結果についてまず説明し、その後、このような研究の背景について説明する。

1.1 本研究の概要

本論文の主要テーマは、ノルムの押えられた多項式とその零点が存在しない領域の研究である。多項式の零点の存在しない領域を簡単に目で見えるにはノルムの押えられた多項式のすべての零点を図を書いてみればよい。Fig. 1.1にその例を示す。 $f(x) = \sum_{i=0}^n a_i x^i$ の2-ノルムを $\|f\|_2 = (\sum_{i=0}^n |a_i|^2)^{1/2}$ と定義し、

$$Z^{\text{ext}}(M, n) = \left\{ \beta \in \mathbb{C} \mid f(\beta) \in \mathbb{Z}[x], \|f\|_2 \leq M, \deg f \leq n, f(\beta) = 0 \right\} \quad (1.1)$$

と定義する。Fig. 1.1は $Z^{\text{ext}}(5, 5)$ に属す点を黒丸で表したものである。この図を見ると有理数やいくつかの複素数のまわりに零点の存在しない領域があるのが分かる。有理数のまわりのこのような領域はのちに定義する零点不在領域に対応している。すぐ後に定義するこのような零点の存在しない領域を本論文では「穴」とよぶ。本論文の前半部分はこの穴の解析であり、後半部分は穴の応用である。

本論文では3つの多項式ノルムを考える。これらの多項式ノルムは一般に複素数係数の多項式に対して定義される。 $f(x) = \sum_{i=0}^n a_i x^i$, $a_i \in \mathbb{C}$ とおく。このとき、

$$\|f\|_2 = \left(\sum_{i=0}^n |a_i|^2 \right)^{1/2} \quad (1.2)$$

を $f(x)$ の2-ノルムという。このノルムは2次形式の手法を使って解析できるので、もっとも扱いやすいノルムである。つぎに、1-ノルムは

$$\|f\|_1 = \sum_{i=0}^n |a_i| \quad (1.3)$$

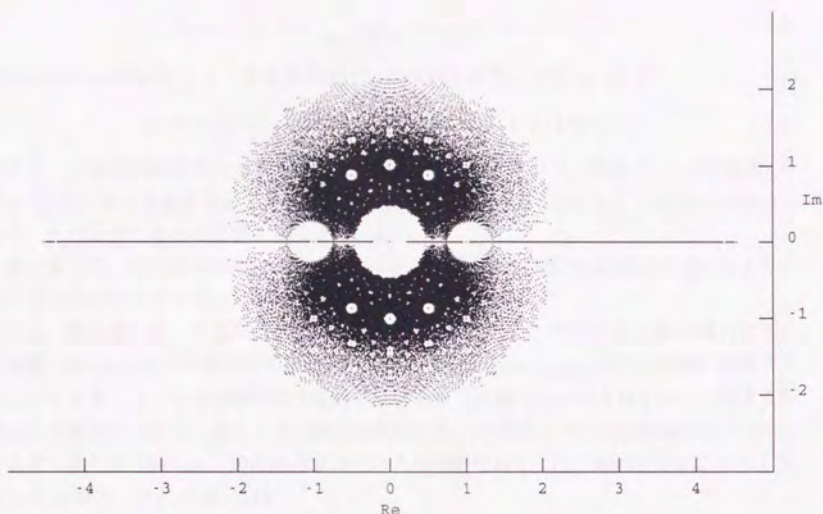


Fig. 1.1. 2-ノルムの押えられた整係数多項式の零点の分布

と定義する。このノルムは、多項式の零点の積の絶対値の最大値

$$M(f) = \left| \max_{i_1, \dots, i_k} \alpha_{i_1} \cdots \alpha_{i_k} \right| \quad (1.4)$$

とおくと

$$\|f\|_1 \leq 2^n M(f) \quad (1.5)$$

が成り立つという性質がある。このような意味でこのノルムは重要である。

3つ目のノルムとして ∞ -ノルムを

$$\|f\|_\infty = \max_{i=0, \dots, n} |a_i| \quad (1.6)$$

と定義する。

以下ではこれら三つのノルムに共通する性質を論じるとき、すなわち、どのノルムであるかを特に限定しないときには $\|f\|_1$, $\|f\|_2$, $\|f\|_\infty$ のかわりに、単に $\|f\|$ と書く。

本論文で考える零点の存在しない領域とはつぎのようなものである。 α を任意の複素数とする。このとき、

$$H_{\alpha,f} = \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(\alpha)| < |f(\alpha)| / \|f\| \right\}, \quad (1.7)$$

で定義される領域 $H_{\alpha,f}$ を「多項式 $f(x)$ の α のまわりの穴」と呼ぶ。ただし、

$$P(\beta) = \{h(x) \in K[x] \mid \deg h \leq n, h(\beta) = 0, \|h\| \leq 1\} \quad (1.8)$$

であり、 K は実数体 \mathbb{R} または複素数体 \mathbb{C} である。穴の定義から、領域 $H_{\alpha,f}$ は複素数 α を含み $f(x)$ の零点を含まない。ただし、 α が $f(x)$ の零点である場合はこの領域は空集合となる。その場合にはこの領域は意味を持たない。

第2章では、その基本的性質について述べた。特に穴の対称性や α の偏角を変えたときの穴の形の不変性などについて述べた。

また、第3章では、ノルムが2-ノルムであるときの $K = \mathbb{C}$ および $K = \mathbb{R}$ の場合について考察した。2-ノルムの場合の穴は2次形式であるので $\max_{h(x) \in P(\beta)} |h(\alpha)|$ を陽に計算することができる。よって穴の解析は比較的容易である。本節では0のまわりの穴に関する解析をまず最初に行ない、そののち一般の穴について、多項式ノルムが定数項に比べて十分に大きい場合を解析した。特に0のまわりの穴は重要であり、 $H_{0,f}$ を解析することにより、 $K = \mathbb{C}$ の場合、 $f(x)$ の零点 β は

$$|\beta| > \frac{|f(0)|}{\|f\|_2} \quad (1.9)$$

となることがわかる。また、 $K = \mathbb{R}$ の場合、 $\beta \in \mathbb{R}$ の場合

$$|\beta| > \frac{|f(0)|}{\|f\|_2} \quad (1.10)$$

であるが、(この結果は $K = \mathbb{C}$ の場合の結果から直接導かれる) $\beta \in \mathbb{C} \setminus \mathbb{R}$ の場合は

$$|\beta| > \sqrt{\frac{|f(0)|}{\|f\|_2}} \quad (1.11)$$

となる。これらの不等式は0のまわりの穴の解析の結果として得られるが、また、Landauの不等式から導くこともできる。これらの結果によって Fig. 1.1 で示した零点の分布の概形について説明することができる。また、第2節の後半では、 $\|f\|/|f(\alpha)|$ が十分に大きいときの穴の漸近的性質について考察した。とくに、 $K = \mathbb{R}$ の場合の一般の実数のまわりの穴と $K = \mathbb{C}$ の場合の一般の複素数のまわりの穴について論じた。 $K = \mathbb{R}$ の場合、次数を固定すれば、穴は $\|f\|/|f(\alpha)|$ に関して漸的に領域

$$\left\{ \beta \in \mathbb{R} \mid |\beta - \alpha| < C_2(n, \alpha) \frac{|f(\alpha)|}{\|f\|_2} \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta - \alpha| < C_3(n, \alpha) \sqrt{\frac{|f(\alpha)|}{\|f\|_2}} \right\} \quad (1.12)$$

へ近づく. また, $K = \mathbb{C}$ の場合は漸近的に領域

$$\left\{ \beta \in \mathbb{C} \mid |\beta - \alpha| < C_1(n, \alpha) \frac{|f(\alpha)|}{\|f\|_2} \right\} \quad (1.13)$$

へ近づく. ただし, $C_1(n, \alpha)$, $C_2(n, \alpha)$, $C_3(n, \alpha)$ は n と α に依存する定数である.

また, α を固定して次数 n を大きくした場合, 穴はどんどん小さくなる. したがって, 次数の制限されないような多項式の解析に穴を用いることはできない. また, このことは ∞ -ノルムについても同様に成り立つ.

また, 第4章では1-ノルムについて考察した. まず, 0のまわりの穴について考察し, その後 $\|f\|_1/|f(\alpha)|$ が十分に大きい場合の解析を行なった. 0のまわりの穴を解析することにより, $K = \mathbb{C}$ の場合に $\|f\|_1/|f(0)| \geq 2$ のとき $f(x)$ の零点 β は

$$|\beta| \geq \left(\frac{\|f\|_1}{|f(0)|} - 1 \right)^{-1} \quad (1.14)$$

である. また, $K = \mathbb{R}$ のとき, $\|f\|_1/|f(0)| \geq 2$, $\beta \in \mathbb{R}$ ならば,

$$|\beta| \geq \left(\frac{\|f\|_1}{|f(0)|} - 1 \right)^{-1} \quad (1.15)$$

であり, さらに, $\|f\|_1/|f(0)| \geq 2$ かつ $\beta \in \mathbb{C} \setminus \mathbb{R}$ ならば,

$$|\beta| \geq \left(\frac{\|f\|_1}{|f(0)|} - 1 \right)^{-1/2} \quad (1.16)$$

である. また, $\|f\|_1/|f(\alpha)|$ が十分大きくなるときの $H_{\alpha, f}$ については $K = \mathbb{C}$ の場合, α と次数 n との間に,

$$|\alpha| \geq \frac{\sqrt{2}+1}{2} n \quad (1.17)$$

または,

$$|\alpha| \leq \frac{2}{(\sqrt{2}+1)n} \quad (1.18)$$

が成り立つとき, $H_{\alpha, f}$ はつぎの領域に近づく.

$$\left\{ \beta \in \mathbb{C} \mid |\beta - \alpha| \leq C_3(n, \alpha) \frac{|f(\alpha)|}{\|f\|_1} \right\}. \quad (1.19)$$

ただし, $C_3(n, \alpha)$ は n と α に依存する定数である. また, $K = \mathbb{R}$ の場合には2-ノルムの場合と同様の結果を得た. 1-ノルムに関する結果は既存の結果から導かれるものではなく, 穴を用いることによりはじめて導かれるものである.

第5章においては ∞ -ノルムによる穴について考察した. ∞ -ノルムについては古くから Cauchy の不等式 [Cau91] と Mignotte による不等式 [Mig92] がすでに知られている. これ

らの不等式は0のまわりの穴の解析によって第2章、第3章と同様にして導くことができる。∞-ノルムの場合、多項式 $f(x)$ の零点 β は

$$|\beta| > \left(\frac{\|f\|_\infty}{|f(0)|} + 1 \right)^{-1} \quad (1.20)$$

であり、また、 β が実数でない場合

$$|\beta| > \left(\sqrt{\frac{\|f\|_\infty}{|f(0)|}} + 1 \right)^{-1} \quad (1.21)$$

となる。2-ノルムや1-ノルムの場合と異なり、全体に平方根がつかないのは興味深い。

第6章においては、整数を係数とする多項式の零点の分布を、2-ノルムについて考察した。ここではつぎのような零点の集合を定義する。 M は実数とし、扱う多項式の次数の最大値を n とする。

$$Z(M, n) = \{ \beta \in \mathbb{C} \mid f(\beta) = 0, f(x) \in P(M, n) \}. \quad (1.22)$$

ただし、

$$P(M, n) = \{ f(x) \in \mathbb{Z}[x] \mid \|f\|_2 \leq M, \deg f \leq n, f(x) \text{ は } \mathbb{Z} \text{ 上で既約な多項式である} \} \quad (1.23)$$

とする。 $Z(M, n)$ は有限集合である。この集合の存在範囲の計算には第3章で得られた限界を直接適用することができる。これは扱う多項式を既約なものに限っているからである。この条件を付けずにつぎのように定義する。

$$Z^{\text{ext}}(M, n) = \{ \beta \in \mathbb{C} \mid f(\beta) = 0, f(x) \in P^{\text{ext}}(M, n) \}. \quad (1.24)$$

ただし、

$$P^{\text{ext}}(M, n) = \{ f(x) \in \mathbb{Z}[x] \mid \|f\|_2 \leq M, \deg f \leq n \}. \quad (1.25)$$

この場合には、複素数 α のまわりの穴について $f(\alpha) = 0$ である可能性があり、そのとき、穴は空集合になってしまうので第3章の結果は使えない。しかし、 α が有理数である場合には、 $\alpha \neq 1$ ならば $\alpha = p/q$, (p, q) = 1 とおくことができ、任意の実係数多項式 $g(x)$ について、 $h(x) = g(x)(px - q)$ とおけば、

$$\|g\|_2 \leq \|h\|_2 \quad (1.26)$$

がなりたつ。この性質から、第3章の結果は $\alpha \neq 1$ である有理数のまわりの穴については適用することができる。また、第6章ではさらに多項式の次数を制限しない場合の零点集合

$$Z(M, \infty) = \bigcup_{n=0}^{\infty} Z(M, n) \quad (1.27)$$

についても考察した。この零点集合は無限集合であるが、第3章の結果より、その存在領域はやはり有界領域

$$\{\beta \in \mathbb{R} \mid |\beta| < M\} \cup \{\beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta| < \sqrt{M}\} \quad (1.28)$$

に存在する。この集合については実軸上の有理数についてつぎのような性質が成り立つ：

任意の有理数 α が $Z(M, \infty)$ に含まれないとき $Z(M, \infty) \setminus \{\alpha\}$ のなかの列で α へ収束する列は存在しない。

この性質により、たとえば

$$\forall \alpha \in Z(5, \infty), |\alpha| < 5 \quad (1.29)$$

であるが、いくら次数をふやしても 5 へ収束する列を構成することができないことがわかる。この性質の証明からわかるように、このようなことが起こるのは M に比べて次数が大きい場合である。また、 M が次数に比べて十分に大きい場合は、明らかに α へ収束する点列が存在する。よって穴によって $Z(M, n)$ を解析する場合、次数 n が無制限に大きいとあまりよい見積もりにならない可能性があることがわかる。

第7章においては、穴を複数の零点に関するものへ拡張して、その手法を 2-ノルムおよび 1-ノルムについて適用した。2-ノルムについては 0 のまわりの穴を解析することにより Landau の不等式 [Lan05] を新しい方法で導くことができる。すなわち、複素係数多項式 $f(x)$ について絶対値が 1 よりも大きな零点 $\alpha_1, \alpha_2, \dots, \alpha_l$ について

$$|\alpha_1 \alpha_2 \cdots \alpha_l| \leq \frac{\|f\|_2}{|lc f|} \quad (1.30)$$

が成り立つ。ただし、 $lc f$ は多項式 $f(x)$ の最高次の係数を表すものとする。また、同様の手法を用いて 1-ノルムについて 0 のまわりの穴を解析した。この問題は、複素数を係数とする非線形計画問題に帰着できる。また、この問題は必ずいくつかの変数が 0 となるようなところで最大値をとるという性質があるので、その性質を用いて解析することができる。任意の数の変数に関する性質は求められていないが、多項式 $f(x)$ の任意の二つの零点 α_1, α_2 について、 $M = \|f\|_1 / |f(0)| \geq 1$ のときは

$$|\alpha_1 \alpha_2| \geq (M - 1)^{-1} \quad (1.31)$$

が成り立つという結果が得られた。この性質を用いれば、複素係数多項式 $f(x)$ の絶対値が 1 よりも大きい零点を α_1, α_2 として、 $\|f\|_1 / |lc f| \geq 1$ であるのならば、

$$|\alpha_1 \alpha_2| \leq \frac{\|f\|_1}{|lc f|} - 1 \quad (1.32)$$

となる。もっと多くの変数について、このような性質が成り立つかどうかは不明である。いくつかの数値実験からはこのような性質は成り立つように思われる。

第8章においては2-ノルムについて、実係数多項式の任意の零点のまわりの穴を計算することを考える。第3章で求めたように2-ノルムについては一般の数のまわりの多項式の零点の穴は比較的単純な式として表すことができる。特に、実係数多項式 $f(x)$ の実数 α のまわりの穴 $H_{\alpha, f}$ は

$$H_{\alpha, f} \cap \mathbb{R} = \left\{ \beta \in \mathbb{R} \mid \frac{\sqrt{|\beta^{[n]}|^2 |\alpha^{[n]}|^2 - |(\alpha^{[n]}, \beta^{[n]})|^2}}{|\beta^{[n]}|} < \frac{|f(\alpha)|}{\|f\|} \right\} \quad (1.33)$$

と単純に表すことができる。ただし、 $\alpha^{[n]} = (1, \alpha, \dots, \alpha^n) \in \mathbb{R}^{n+1}$ であるとする。また、この穴はつぎのような性質をもつ：

$$\frac{|f(\alpha)|}{\|f\|_2} < |\alpha^{[n-1]}| \Rightarrow H_{\alpha, f} \cap \mathbb{R} \text{ は有界であり,} \quad (1.34)$$

$$\frac{|f(\alpha)|}{\|f\|_2} \geq |\alpha^{[n-1]}| \Rightarrow \mathbb{R} \setminus (H_{\alpha, f} \cap \mathbb{R}) \text{ は有界である.} \quad (1.35)$$

この性質より、与えられた多項式が1以上の実零点を持たないことを証明するためのアルゴリズムとして、つぎのようなアルゴリズムを考えるとこれは停止する。 $\alpha = 1$ から出発して

$$\alpha \leftarrow \text{Right}(H_{\alpha, f})$$

を繰り返す。ただし、 $\text{Right}(T)$ は α のまわりの $f(x)$ の零点の穴 T の大きい方の端点であるとする。 $f(x)$ が実零点をもたない場合、いつか

$$\frac{|f(\alpha)|}{\|f\|} > |\alpha^{[n-1]}|$$

となりこの繰り返しがいっまでも続くことはない。 $f(x)$ の係数を次数に関して逆にしたような多項式を $f^{\text{rev}}(x)$ とかくことにする。このアルゴリズムを $f(x)$, $f(-x)$, $f^{\text{rev}}(x)$, $f^{\text{rev}}(-x)$ について実行すれば、 $f(x)$ が実零点を持たないことを証明することができる。与えられた多項式が実零点を持たないということを証明することができれば、これを用いて任意のいくつかの実変数をもつ方程式系が解を持たないことを証明でき、これを用いてたとえば幾何的な図形の性質を証明することができる。第8章の最後の部分ではこのアルゴリズムを用いて実際にいくつかの不等式系を証明する。

第9章では有理数の複雑さを定義し、さらにこれを用いて、ある代数方程式の零点によって拡大された体上の数にたいしてその複雑さを定義した。これらの数の複雑さが四則演算に関してどのように大きくなるかを見積もった。これを用いて初等幾何学の定理を数値的

に証明するための必要精度を見積もった。できることなら、証明したい初等幾何学の定理に対応する方程式系の係数のノルムのようなものを定義し、その方程式系の解の零点の穴のようなものを見積もることが望ましい。しかし、このような方程式系に対してこのようなものをうまく見積もることは、現在のところうまく出来ていない。第9章ではこのような理由から、有理数や一つの代数的数によって拡大された体上の数について複雑さを定義し、その複雑さが四則演算によってどのように大きくなるかを調べた。ただし、この複雑さは拡大体を表現する基底の取り方に依存する。

このように、本論文では第2章で定義した穴をそれ以降の章で解析した。穴の有効性はまだはっきりとしないが、少なくとも現在知られている零点の限界のいくつかに統一的な新しい証明をあたえることができることが分かった。また、2-ノルムに関しては穴を陽に計算することが比較的簡単にできるので、それを用いて与えられた整係数多項式がある区間に実零点を持たないということを計算することができる。この事実を利用した応用の可能性を本論文の後半では論じたわけである。

1.2 本研究の背景

本研究の背景には大きく分けて二つの流れがある。その一つは、数式処理における整係数多項式の因数分解アルゴリズムの研究である。また、もう一つの背景は多項式系の解として定義される数が0であるか否かを判定する問題である。

まず、整係数多項式の因数分解のアルゴリズムとしては、Zassenhaus [Zas75], Wang [W82], Lenstra, Lenstra and Lovász [LLL82] などの研究をはじめとして多くの研究が知られている。このように因数分解のアルゴリズムにはいろいろなものが提案されているが、特に一変数多項式の因数分解アルゴリズムで必ず必要となるのが、与えられた多項式を因数分解したときの因子多項式の係数の大きさの上界である。この上界としては Landau の不等式 [Lan05] [Mig82] から導かれるものを用いるのが普通である。本論文の方法は、この上界の別証を与えている。与えられた整係数多項式 $f(x) \in \mathbb{Z}[x]$ を因数分解する場合、 $f(x) = g(x)h(x)$ と分解できたと仮定したときの $g(x)$ の係数の上界を知る必要がある。因数分解アルゴリズムを探索問題であると考えれば、この上界は探索空間を与えていることになる。現在一般に用いられている公式は

$$\|g\|_{\infty} \leq \left(\binom{n}{\lfloor n/2 \rfloor} \right) \|f\|_2 \quad (1.36)$$

や

$$\|g\|_1 \leq \left(\binom{2n}{n} \right)^{1/2} \|f\|_2 \quad (1.37)$$

がある。これらの不等式はつぎの Landau の不等式によって容易にもとめることができる。Mignotte [Mig82] に述べられているように、Landau の不等式はこの形式の公式では best possible である。しかし、例えば、本論文の第6章で証明されているように、整数の対 (p, q) が $p \neq q$ で互いに素のときは、 $h(x) = g(x)(px - q)$ とおけば、

$$\|g\|_2 \leq \|h\|_2 \quad (1.38)$$

がなりたつ。よって、因数分解すべき多項式にいろいろな制限が加われればそれによって探索空間を小さくできる可能性がある。

また、多変数多項式の因子のノルムともと多項式のノルムの関係については Beauzamy, Bombieri, Enflo and Montgomery [BBEM90] の研究がある。この研究では本論文で扱う p -ノルムに関する結果を得ているが、示されているのは限界の存在であって、実際にこの限界を計算する方法は示されていない。

第二の背景としては、多項式系の解として定義される代数的数が0であるか否かを判定するための必要精度を計算するなどの問題がある。このようなことに関連した問題は、数式処理ばかりでなく、計算幾何学などの分野でも重要である。たとえば、Voronoi Diagramなどを計算する場合、線分どうしの交差判定に要する計算精度の研究として吉田 [吉田 88] がある。また、初等幾何学の定理などは、いくつかの自由変数を含むある方程式系の解（これは一般に自由変数の関数となる）が、自由変数に依存することなく恒等的に0であるということを証明することにより証明することができる。これについては Schwartz [Sch80] により、いくつかのランダムな数をこの自由変数に代入したときの解が0であれば、ある確率でこの解は恒等的に0であるということが示されている。また、Hong [Hon86] は、自由変数にこの方程式系の規模よりも大きな数を代入してそれが0であれば、最終的に0であると判定したい数が恒等的に0であることが言えることを示した。本論文の第9章では、Schwartzの方法に基づいて、ある多項式系が自由変数を含まないとき（自由変数にすでに数が代入されていると考える場合）にその解を数値的に計算して真に0であるかどうかを調べるためにどのくらいの精度で計算すればよいか、という問題について考察している。数式処理の古典的な方法論としては、 p -進体などの付値体を用いてその上の近似を行なうことが多い。多項式の因数分解のアルゴリズムもこのような方法を用いたものが一般的である。これに対して、Lenstra [Len83] では、実数体上の数を用いて因数分解するアルゴリズムを構成している。本論文で扱っている方法も p -進体ではなく実数体上の近似値を判定する問題を考察している。

第 2 章

零点不在領域の定義とその基本的性質

本章では、本研究で中心的な役割を果たす零点の存在しない領域を定義する。この領域の部分領域を求めることが本研究の前半である。本章は二つの部分に分かれる。はじめの部分で多項式の 1 つの零点に関する不在領域を定義し、後の部分ではその概念を拡張し、特定の多項式の幾つかの零点を組にしたものの不在領域を定義する。

2.1 1 点のまわりの零点不在領域

まず、多項式の零点の不在領域を定義しよう。本論文で取り扱うのは複素数体 \mathbb{C} 上または実数体 \mathbb{R} 上の多項式である。多項式の係数体を一般的に K と書く。はじめに、多項式のノルムについて定義する。

定義 1 体 K 上の多項式 $f(x)$ のノルム $F(f)$ とは、 K 上の多項式の集合 $K[x]$ から非負実数への写像 F で、つぎの性質をみたすものである。

1. $\forall f \in K[x], F(f) \geq 0,$
2. $\forall \lambda \in K, f \in K[x], F(\lambda f) = |\lambda|F(f),$
3. $\forall f, g \in K[x], F(f+g) \leq F(f) + F(g),$
4. $\forall f \in K[x], F(f) = 0 \Leftrightarrow f = 0.$

このような多項式ノルム $F(f)$ のことを $\|f\|$ と記す。

まず、多項式ノルムを用いて、つぎのような複素平面の領域を定義する。

定義 2 f を多項式環 $K[x]$ の要素とし、その次数を n とする。また、ある任意の複素数を α とおく。このとき任意の複素数 $\beta \in \mathbb{C}$ に対して、多項式の集合 $P(\beta)$ をつぎのように定める：

$$P(\beta) = \left\{ h(x) \in K[x] \mid \deg h \leq n, h(\beta) = 0, \|h\| \leq 1 \right\}. \quad (2.1)$$

また、複素平面上的領域 $H_{\alpha, f}$ をつぎのように定める：

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(\alpha)| < |f(\alpha)| / \|f\| \right\}. \quad (2.2)$$

つぎの定理に示すように、この領域 $H_{\alpha, f}$ は、多項式 $f(x)$ の零点を含まない。

補助定理 1 領域 $H_{\alpha, f}$ は $f(x)$ の零点を含まない。

証明 ある複素数 β について $\beta \in H_{\alpha, f}$ であるとする。このとき、 $H_{\alpha, f}$ の定義より任意の $h(x) \in P(\beta)$ に対して $|h(\alpha)| < |f(\alpha)| / \|f\|$ である。ここで、多項式 $g(x) = f(x) / \|f\|$ は $|g(\alpha)| = |f(\alpha)| / \|f\|$ を満たし、したがって、 $g(x) \notin P(\beta)$ である。一方、 $\deg(g) \leq \deg(f)$ 、 $\|g\| = 1$ がなりたつので、 $P(\beta)$ の定義と $g(x) \notin P(\beta)$ より $g(\beta) \neq 0$ でなければならない。したがって、 $f(\beta) \neq 0$ である。□

$K = \mathbb{R}$ であるとする、多項式をその係数を要素とする $n+1$ 次元ベクトルとみると、 $P(\beta)$ は K^{n+1} 中の凸な集合であると考えることができる。すなわち、 $h_1, h_2 \in P(\beta)$ となると、 $P(\beta)$ の定義より $h_1(\beta) = 0, \|h_1\|_1 \leq 1$ かつ $h_2(\beta) = 0, \|h_2\|_2 \leq 1$ である。よって、これより $h_3(x) = \gamma h_1(x) + (1-\gamma)h_2(x)$ 、 $(0 \leq \gamma \leq 1)$ とおけば、 $h_3(\beta) = 0$ であり、さらに、ノルムの定義より $\|h_3\| \leq 1$ である。以上より、 $h_3(x) \in P(\beta)$ であることがわかる。よって、集合 $P(\beta)$ は凸集合である。また、 $K = \mathbb{C}$ であるときは多項式の係数の実成分と虚成分をそれぞれ別の成分と考えれば、同様にして $P(\beta)$ は凸集合となる。また、 $|h(\alpha)|$ は多項式の係数を変数とする凸関数である。すなわち、 $|\gamma h_1(\alpha) + (1-\gamma)h_2(\alpha)| < \gamma|h_1(\alpha)| + (1-\gamma)|h_2(\alpha)|$ 、 $(0 \leq \gamma \leq 1)$ が成り立つ。以上より、 $H_{\alpha, f}$ の定義式の中の $\max_{h(x) \in P(\beta)} |h(\alpha)|$ を計算することは、minimize $-|h(\alpha)|$, subject to $h(x) \in P(\beta)$ という形の非線形計画問題を解くことである。この非線形計画問題の解はつねに存在し、それは $P(\beta)$ の境界で解をとる。

複素数 α が $f(x)$ の零点となっていないと仮定すれば、 $\alpha \in H_{\alpha, f}$ であり、したがって領域 $H_{\alpha, f}$ は α を含んで $f(x)$ の零点を含まない領域である。よって領域 $H_{\alpha, f}$ を多項式 $f(x)$ の零点の α のまわりの穴と呼ぶ。また、 α が $f(x)$ の零点となるとき $H_{\alpha, f}$ は空集合となる。また、穴の解析は β の関数 $\max_{h(x) \in P(\beta)} |h(\alpha)|$ の性質の解析であると言える。

つぎに本論文で用いるノルムについて定義する。

定義 3 任意の正の実数 p に対して, $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$ の p -ノルムとは

$$\|f\|_p = \left(\sum_{i=0}^n |a_i|^p \right)^{1/p} \quad (2.3)$$

であり, $f(x)$ の ∞ -ノルムとは

$$\|f\|_\infty = \max_{i=0, \dots, n} |a_i| \quad (2.4)$$

のことである.

穴について, つぎのような性質がある.

補助定理 2 $K = \mathbb{R}$ のとき, $H_{\alpha, f}$ は実軸に関して対称である. また, $K = \mathbb{C}$, $\alpha \in \mathbb{R}$ の場合も $H_{\alpha, f}$ は実軸に関して対称である.

証明 定義より

$$\begin{aligned} P(\bar{\beta}) &= \left\{ h(x) \in \mathbb{R}[x] \mid \deg h \leq n, h(\bar{\beta}) = 0, \|h\| \leq 1 \right\} \\ &= \left\{ h(x) \in \mathbb{R}[x] \mid \deg h \leq n, h(\beta) = 0, \|h\| \leq 1 \right\} \end{aligned}$$

であることから, $H_{\alpha, f} = \overline{H_{\alpha, f}}$ である. ただし, $\overline{H_{\alpha, f}}$ は $H_{\alpha, f}$ の要素の複素共役の全体である. また, $K = \mathbb{C}$, $\alpha \in \mathbb{R}$ の場合,

$$\begin{aligned} P(\bar{\beta}) &= \left\{ h(x) \in \mathbb{C}[x] \mid \deg h \leq n, h(\bar{\beta}) = 0, \|h\| \leq 1 \right\} \\ &= \left\{ \bar{h}(x) \in \mathbb{C}[x] \mid \deg h \leq n, \bar{h}(\beta) = 0, \|h\| \leq 1 \right\} = \overline{P(\beta)} \end{aligned}$$

である. ただし, $\bar{h}(x)$ は $h(x)$ の係数をすべてその複素共役と置き換えたものである. この性質を用いて,

$$\begin{aligned} \overline{H_{\alpha, f}} &= \left\{ \bar{\beta} \in \mathbb{C} \mid \max_{h(x) \in P(\bar{\beta})} |h(\alpha)| \leq \frac{|f(\alpha)|}{\|f\|} \right\} \\ &= \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in P(\bar{\beta})} |h(\alpha)| \leq \frac{|f(\alpha)|}{\|f\|} \right\} \\ &= \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in \overline{P(\beta)}} |h(\alpha)| \leq \frac{|f(\alpha)|}{\|f\|} \right\} \\ &= \left\{ \beta \in \mathbb{C} \mid \max_{\bar{h}(x) \in P(\beta)} |\bar{h}(\alpha)| \leq \frac{|f(\alpha)|}{\|f\|} \right\} = H_{\alpha, f} \end{aligned}$$

となる. □

さらに, $K = \mathbb{C}$ の場合, 穴についてつぎの性質が成り立つ.

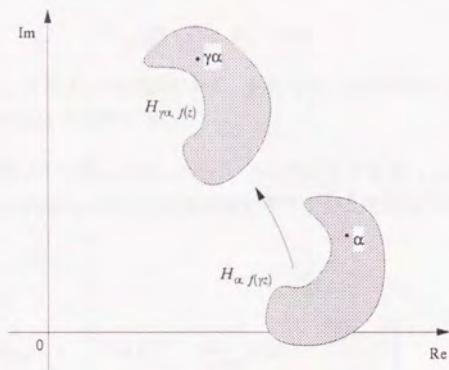


Fig. 2.1. 穴を回転させる

補助定理 3 $K = \mathbb{C}$ でノルムが p -ノルムか ∞ -ノルムであるとき、絶対値 1 の任意の複素数 γ に対して $H_{\gamma\alpha, f(z)} = \gamma H_{\alpha, f(\gamma z)}$ が成り立つ。

証明 定義より

$$\begin{aligned} H_{\gamma\alpha, f(z)} &= \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(\gamma\alpha)| < |f(\gamma\alpha)| / \|f\| \right\} \\ &= \left\{ \gamma\beta \in \mathbb{C} \mid \max_{h(x) \in P(\gamma\beta)} |h(\gamma\alpha)| < |f(\gamma\alpha)| / \|f\| \right\}. \end{aligned}$$

また,

$$P(\gamma\beta) = \left\{ h(x) \in \mathbb{C}[x] \mid \deg h \leq n, h(\gamma\beta) = 0, \|h\| \leq 1 \right\}.$$

以上の結果に対して, $h(\gamma x) \rightarrow h(x)$ という置換えをおこなう. この場合, $h(x)$ は $h(x/\gamma)$ へ置き換えられる. ここで $\tilde{h}(x) = h(x/\gamma)$ とおけば,

$$H_{\gamma\alpha, f(z)} = \left\{ \gamma\beta \in \mathbb{C} \mid \max_{\tilde{h}(x) \in P(\beta)} |\tilde{h}(\alpha)| < |f(\gamma\alpha)| / \|f\| \right\} = \gamma H_{\alpha, f(\gamma z)}.$$

と書くことができる. これは求める結果である. \square

この性質より, $K = \mathbb{C}$ の場合に H_α を計算するには, α が実数の場合について解析しそれを回転させればよいことが分かる (Fig. 2.1 を参照).

また, 単位円に関する鏡像の関係としてつぎのような性質がある. まず, はじめに多項式の係数を上下逆にした多項式を定義する.

定義 4 体 K 上の多項式 $f(x)$ の逆多項式とは, $f(0) \neq 0$ のとき, 多項式

$$f^{\text{rev}}(x) = x^n f(1/x) \quad (2.5)$$

のことである. ただし, n は $f(x)$ の次数である. また, $f(0) = 0$ の場合 $f(x) = x^r g(x)$, $g(0) \neq 0$ として $f^{\text{rev}}(x) = g^{\text{rev}}(x)$ と定義する.

補助定理 4 $K = \mathbb{C}$ でノルムが p -ノルムか ∞ -ノルムであるとき $H_{\alpha, f} = \text{Reciprocal}(H_{1/\alpha, f^{\text{rev}}})$ が成り立つ. ただし, $\text{Reciprocal}(X)$ は複素数を要素とする集合 X の逆数を要素とする集合である.

証明 定義より

$$\begin{aligned} H_{\alpha, f} &= \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(\alpha)| < \frac{|f(\alpha)|}{\|f\|} \right\} \\ &= \left\{ 1/\beta \mid \beta \in \mathbb{C}, \max_{h(x) \in P(1/\beta)} |h(\alpha)| < \frac{|f(\alpha)|}{\|f\|} \right\} \end{aligned}$$

である. また,

$$\begin{aligned} P(1/\beta) &= \left\{ h(x) \in \mathbb{C}[x] \mid \deg h \leq n, h(1/\beta) = 0, \|h\| \leq 1 \right\} \\ &= \left\{ h^{\text{rev}}(x) \mid \deg h \leq n, h(\beta) = 0, \|h\| \leq 1 \right\} \end{aligned}$$

である. よって

$$\begin{aligned} H_{\alpha, f} &= \left\{ 1/\beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(1/\alpha)| \alpha^n < \frac{|f(\alpha)|}{\|f\|} \right\} \\ &= \left\{ 1/\beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(1/\alpha)| < \frac{|f(\alpha)/\alpha^n|}{\|f\|} \right\} \\ &= \left\{ 1/\beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(1/\alpha)| < \frac{|f^{\text{rev}}(1/\alpha)|}{\|f^{\text{rev}}\|} \right\} \end{aligned}$$

となる. 以上より本補助定理を得る. □

Fig. 2.2 にこの補助定理の図形の関係を示す.

また, $|f(\alpha)|/\|f\|$ が十分に小さいとき p -ノルムについてつぎのことがわかる.

補助定理 5 用いるノルムを p -ノルム, または ∞ -ノルムとする. また, $K = \mathbb{C}$ とする. α をある複素数とする. $\{\beta_i\}$ を複素数の列とする. もし,

$$\lim_{i \rightarrow \infty} \max_{h(x) \in P(\beta_i)} |h(\alpha)| = 0 \quad (2.6)$$

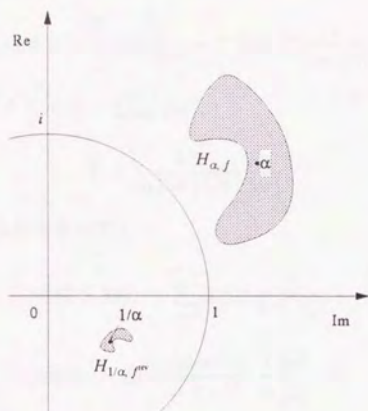


Fig. 2.2. 穴を単位円に関して反転させる

ならば,

$$\lim_{i \rightarrow \infty} \beta_i = \alpha \quad (2.7)$$

である.

証明 仮定より,

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 \forall h(x) \in P(\beta_i) [|h(\alpha)| < \varepsilon].$$

よって, $P(\beta)$ の定義より

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 \forall h(x) \in K[x] [\deg h \leq n, \|h\| \leq 1, h(\beta_i) = 0 \Rightarrow |h(\alpha)| < \varepsilon].$$

$h(\beta_i) = 0$ となる任意の $h(x)$ は複素数体上のある多項式 $g(x)$ を用いて $h(x) = (x - \beta_i)g(x)$ と書くことができる. よってこれよりつぎの命題が成り立つ:

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 \forall g(x) \in K[x] [\deg g \leq n-1, \|h\| \leq 1 \Rightarrow |h(\alpha)| < \varepsilon].$$

また, さらにノルムの定義より

$$\begin{aligned} \|h\| &\leq \|g\| + |\beta_i| \|g\| \\ &= (1 + |\beta_i|) \|g\|. \end{aligned}$$

これよりつぎの命題を得る.

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 \forall g(x) \in K[x] \left[\deg g \leq n-1, \|g\| \leq \frac{1}{1+|\beta_i|} \Rightarrow |g(\alpha)| |\alpha - \beta_i| < \varepsilon \right]$$

$\alpha \neq 0$ と仮定する. このとき $g(x) = \sum_{j=0}^{n-1} b_j x^j$,

$$b_j = \frac{1}{n(1+|\beta_i|)} \cdot \frac{\overline{\alpha^j}}{|\alpha^j|}$$

とおけば $g(x)$ はつぎの条件をみたす:

$$\|g\| \leq \|g\|_1 = \sum_{j=0}^{n-1} |g_j| = \frac{1}{1+|\beta_i|},$$

$$|g(\alpha)| |\alpha - \beta_i| = \frac{|\alpha - \beta_i|}{1+|\beta_i|} \cdot \frac{1}{n} \sum_{j=0}^{n-1} |\alpha^j|.$$

よって以上より

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 \left[c \frac{|\alpha - \beta_i|}{1+|\beta_i|} < \varepsilon \right] \quad (2.8)$$

になりたつ. ただし, c は $1/n \sum_{j=0}^{n-1} |\alpha^j|$ のことでありこれは α と n にのみ依存する. もし $\{\beta_i\}$ が有界でなければ任意の正の数 ε に対して $\varepsilon/c < |\alpha - \beta_i|/(1+|\beta_i|)$ となる i が無限個存在する. これは式 (2.8) に矛盾する. したがってある定数 $d(>0)$ が存在して $|\beta_i| \leq d$ となる. よって

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 \left[|\alpha - \beta_i| < \frac{1+d}{c} \varepsilon \right]$$

であり, したがって, $\lim_{i \rightarrow \infty} \beta_i = \alpha$ である. また, $\alpha = 0$ に関する証明は $b_j = (1+|\beta_i|)^{-n}$ とおくと同様である. \square

また, 同様にして $K = \mathbb{R}$ の場合つぎの性質になりたつ.

補助定理 6 用いるノルムを p -ノルムまたは ∞ -ノルムとする. α をある実数とし, $P(\beta)$ を補助定理 1 で定義した多項式の集合とする. また, $\{\beta_i\}$ を複素数の列とする. このとき

$$\lim_{i \rightarrow \infty} \max_{h(x) \in P(\beta_i)} |h(\alpha)| = 0 \quad (2.9)$$

ならば

$$\lim_{i \rightarrow \infty} \beta_i = \alpha \quad (2.10)$$

である.

証明 ある i について $\beta_i \in \mathbb{R}$ であるとする。補助定理 5 の証明と同様にして

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 [|\alpha - \beta_i| < c_1 \varepsilon]$$

となる。ただし、 c_1 はある定数である。また、 $\beta_i \in \mathbb{C} \setminus \mathbb{R}$ であるとする、 $h(x) = g(x)(x - \overline{\beta_i})(x - \beta_i)$ とおけば

$$\forall \varepsilon > 0 \exists i_0 \forall i \geq i_0 [|\alpha - \beta_i| < c_2 \varepsilon^{1/2}]$$

となる。ただし、 c_2 はある定数である。以上より本補助定理を得る。 \square

系 1 用いるノルムを p -ノルムまたは ∞ -ノルムとする。 $K = \mathbb{C}$ かつ $\alpha \in \mathbb{C}$ であるか、または、 $K = \mathbb{R}$ かつ $\alpha \in \mathbb{R}$ であるとする。このとき任意の正の数 ε に対して δ が存在して

$$\forall \beta \in \mathbb{C} \left[\max_{h(x) \in P(\beta)} |h(\alpha)| < \delta \Rightarrow |\alpha - \beta| < \varepsilon \right]. \quad (2.11)$$

証明 この系の否定は

$$\exists \varepsilon > 0 \forall \delta > 0 \exists \beta \in \mathbb{C} \left[\max_{h(x) \in P(\beta)} |h(\alpha)| < \delta \wedge |\alpha - \beta| \geq \varepsilon \right]$$

である。しかしこれは補助定理 5 および 6 と矛盾する。 \square

この系より十分に $|f(\alpha)|/\|f\|$ が小さい時 $H_{\alpha,f}$ は α の近傍になるということがわかる。このような場合の $H_{\alpha,f}$ の解析は第 3 章および第 4 章において行なう。

第 3 章、第 4 章、第 5 章においてそれぞれ 2-ノルム、1-ノルム、 ∞ -ノルムについて $H_{0,f}$ を解析するが、それぞれの結果に似たような結果は Beauzamy, Bombieri, Enflo および Montgomery [BBEM90] の結果を用いることによって導くことができる。Beauzamy らの結果はつぎのようなものである。

定理 1 ([BBEM90]) P, Q を斉次の多変数多項式で次数がそれぞれ m, n であるとする。また、 p を $1 \leq p$ となる実数、または、 $p = \infty$ とする。このときある定数 $C_1(m, n) > 0$ が存在して

$$C_1(m, n) \|P\|_p \cdot \|Q\|_p \leq \|PQ\|_p \leq 2^{(m+n)(1-1/p)} \|P\|_p \|Q\|_p \quad (2.12)$$

となる。ただし、多変数多項式の p -ノルムはそれぞれの項の係数の絶対値の p 乗の和の $1/p$ 乗として定義する。

この定理を用いてノルムによる零点の評価をすることができる。

系 2 複素数 α を複素数体上の多項式 $f(x)$ の零点とする. また, $f(x)$ の次数を n とおき $c_1 = 1/C_1(1, n-1)$ とおく. ここで C_1 は定理 1 に現れる定数である. このとき

$$|\alpha| \geq ((c_1 \|f\|_2 / |f(0)|)^2 - 1)^{-1/2}, \quad (2.13)$$

$$|\alpha| \geq (c_1 \|f\|_1 / |f(0)| - 1)^{-1}, \quad (2.14)$$

$$|\alpha| \geq (c_1 \|f\|_\infty / |f(0)|)^{-1} \quad (2.15)$$

である. また, $f(x) \in \mathbb{R}[x]$ でかつ α が実数でない場合は

$$|\alpha| \geq ((c_2 \|f\|_2 / |f(0)|)^2 - 1)^{-1/4}, \quad (2.16)$$

$$|\alpha| \geq (c_2 \|f\|_1 / |f(0)| - 1)^{-1/2}, \quad (2.17)$$

$$|\alpha| \geq (c_2 \|f\|_\infty / |f(0)|)^{-1/2} \quad (2.18)$$

である. ただし, $c_2 = C_1(2, n-2)$ であるとする.

証明 $g(x, y), h(x, y)$ を斉次の 2 変数多項式であり, $g(x, 1) = x - \alpha$, $h(x, 1) = f(x) / (|c f|(x - \alpha))$ をみたすものとする. 定理 1 で $P = g(x, y)$, $Q = h(x, y)$ として,

$$C_1(m, n) \|g\|_p \|h\|_p \leq \|gh\|_p$$

であり, これより $C_1(m, n) \|g\|_p \|h\|_p \leq \|gh\|_p$ がなりたつ. ここで $g(x), h(x)$ は一変数多項式である. はじめの定義より $g(x) = x - \alpha$, $h(x) = f(x) / (|c f|(x - \alpha))$ と書くことができる. ここで, $g_1(x) = g(x, 1)$, $h_1(x) = h(x, 1)$ とおけば, $C_1(1, n-1) \|(x - \alpha)\|_p \leq C_1(1, n-1) \|g_1\|_p \|h_1\|_p \leq \|g_1 h_1\|_p = \|f\|_p / |c f|$. この結果より係数の順番を逆にした多項式は元の多項式の零点の逆数を零点とするという性質を用いてはじめの 3 つ不等式が得られる. また, 後半の 3 つの不等式は $g(x) = (x - \alpha)(x - \bar{\alpha})$, $h(x) = f(x) / (|c f|(x - \alpha)(x - \bar{\alpha}))$ とすることによって得られる. \square

Beauzamy らの結果を用いてこのような限界を出すことができるが, いくつかの問題点がある. まずここで用いられている定数 c_1, c_2 は多項式 $f(x)$ の次数に依存することである. これに対して, 第 3 章, 第 4 章, 第 5 章において示す限界は定数が次数に依存しない. また, これらの定数は存在することはわかるが, その値がいくつであるかを計算する方法は知られていない. 存在のみが示されている.

2.2 複数の零点の零点不在領域の定義

前節ではある一つの零点のまわりの穴について考えた. 零点の存在範囲を考えるためにはそれで十分であるが, いくつかの零点どうしの関係について考えるために, 前節の

定義を複数の零点についてのものに拡張する. ある一つの多項式のいくつかの零点を組 $(\delta_1, \delta_2, \dots, \delta_l) \in \mathbb{C}^l$ の存在しない範囲を \mathbb{C}^l のなかで求めることを考える.

定義 5 $f(x)$ を次数 n の複素数体上の多項式とし, α をある複素数とする. $\delta = (\delta_1, \delta_2, \dots, \delta_l)$ を多項式 $f(x)$ の l 個の零点の組とする. ただし, この組の中には同じ零点はその多重度以上には出現しないとする. 複素数体上の多項式の集合 $P(\beta_1, \dots, \beta_l)$ をつぎのように定義する:

$$P(\beta_1, \dots, \beta_l) = \left\{ h(x) \in \mathbb{C}[x] \mid \deg h \leq n, h(x) \text{ は } \prod_{i=1}^l (x - \beta_i) \text{ で割り切れる, } \|h\| \leq 1 \right\}. \quad (2.19)$$

また, これを用いて

$$H_{\alpha, f} = \left\{ (\beta_1, \dots, \beta_l) \in \mathbb{C}^l \mid \phi(\beta_1, \beta_2, \dots, \beta_l) < |f(\alpha)| / \|f\| \right\} \quad (2.20)$$

と定義する. ただし, $\phi(\beta_1, \beta_2, \dots, \beta_l) = \max\{|h(\alpha)| \mid h(x) \in P(\beta_1, \beta_2, \dots, \beta_l)\}$ とする.

補助定理 7 $H_{\alpha, f}$ は δ を含まない.

証明 l 個の複素数の組 $(\beta_1, \beta_2, \dots, \beta_l)$ が $H_{\alpha, f}$ に含まれていると仮定する. このとき $P(\beta_1, \dots, \beta_l)$ のなかの任意の多項式 $h(x)$ について $|h(\alpha)| < |f(\alpha)| / \|f\|$ が成立する. また, 多項式 $g(x) = f(x) / \|f\|$ は $|g(\alpha)| = |f(\alpha)| / \|f\|$ であるので $g(x) \notin P(\beta_1, \dots, \beta_l)$ である. 一方, $\deg g = \deg f$ であり, $\|g\| = 1$ である. よって, これより $\prod_{i=1}^l (x - \beta_i) \nmid g(x)$. ただし, 記号 $A \nmid B$ は A が B の因子とならないことを表す. すなわち, これは $\prod_{i=1}^l (x - \beta_i) \nmid f(x)$ ということである. したがって β_1, \dots, β_l は多項式 $f(x)$ の l 個の零点とはなり得ない. \square

第7章で示すことであれが, この補助定理を用いることにより Mignotte [Mig74] の結果を別の方法で証明することができる. 本論文ではこのような \mathbb{C}^l のなかの領域を多項式 $f(x)$ の l 個の零点の複素数 α のまわりの穴と呼ぶ.

0 のまわりの複数の零点の穴についてはつぎの性質が成り立つ.

補助定理 8 任意のノルムについて $\phi(\beta_1, \dots, \beta_l)$ は連続関数である.

証明 任意のノルムについて $\phi(\beta_1, \dots, \beta_l)$ はつぎのように表現することができる.

$$\phi(\beta_1, \dots, \beta_l) = \max_{b_0, \dots, b_l} \left\{ |h(\alpha)| \mid h(x) \text{ は } \prod_{i=1}^l (x - \beta_i) \text{ で割り切れる, } \|h\| \leq 1 \right\}.$$

ここで $a(x) = \prod_{i=1}^l (x - \beta_i) = \sum_{j=0}^l a_j x^j$ とおき, $h(x) = \sum_{j=0}^n b_j x^j$ とおく. このとき, 条件 $a(x) \mid h(x)$ の必要十分条件は部分終結式 [Bro78]

$$F_{n-1}(h, a) = \mathcal{P} \begin{pmatrix} b_n & b_{n-1} & \cdots & \cdots & \cdots & \cdots & b_0 \\ a_l & a_{l-1} & \cdots & a_0 & & & 0 \\ & a_l & a_{l-1} & \cdots & a_0 & & \\ & & \ddots & & & \cdots & \\ 0 & & & a_l & a_{l-1} & \cdots & a_0 \end{pmatrix}$$

が 0 に等しいことである。ここで \mathcal{P} は与えられた行列の随伴多項式を生成する演算子であるとする。この部分終結式は b_0, \dots, b_n の線形結合としてかける。また、 b_0, \dots, b_n の係数は a_0, \dots, a_l の多項式である。 β_1, \dots, β_l が滑らかに変化するとき $a(x)|h(x)$ と同値なこの方程式系は連続に変化する。また、一方この方程式系は

$$\begin{aligned} h(\beta_1) &= 0, \\ h'(\beta_1) &= 0, \\ &\dots \dots \dots \\ h^{(d_1)}(\beta_1) &= 0, \\ &\dots \dots \dots \\ h(\beta_{k_r}) &= 0, \\ h'(\beta_{k_r}) &= 0, \\ &\dots \dots \dots \\ h^{(d_r)}(\beta_1) &= 0 \end{aligned}$$

と同値である。ただし、

$$\begin{aligned} 1 &= n_1 < n_2 < \dots < n_r < n_{r+1} = l+1, \\ \{\beta_1, \dots, \beta_l\} &= \{\beta_{n_1}, \dots, \beta_{n_r}\}, \quad \beta_{n_i} \neq \beta_{n_j}, \quad (i \neq j), \\ \beta_{n_i} &= \beta_{n_{i+1}} = \dots = \beta_{n_{i+1}-1} \quad (i = 1, \dots, r) \end{aligned}$$

であり、 $a(x)|h(x)$ は $h(x)$ が $a(x)$ で割り切れることを表す。この方程式系はあきらかにランク l である。よって任意の複素数 β_1, \dots, β_l にたいして条件 $a(x)|h(x)$ はランク l の線形方程式系と同値である。ここで点-集合写像 Q をつぎのように定義する:

$$Q(\beta_1, \dots, \beta_l) = \left\{ (b_0, \dots, b_n) \mid \sum_{j=0}^n b_j x^j \text{ は } \prod_{i=1}^l (x - \beta_i) \text{ で割り切れる, } \|h\| \leq 1 \right\}.$$

このとき Q は明らかに連続である。また、関数 $|b_0|$ もまた連続である。よって、非線形計画法の感度解析の理論より $\phi(\beta_1, \beta_2, \dots, \beta_l)$ は連続である。□

この結果より $\phi(\beta_1, \beta_2, \dots, \beta_l)$ を解析する場合は β_1, \dots, β_l は互いに等しくない数であると仮定して解析を行なえばよい。このように仮定しても連続性が保証されているので、たとえば $\phi(\beta_1, \beta_1, \dots, \beta_l)$ の値は $\lim_{\beta_2 \rightarrow \beta_1} \phi(\beta_1, \beta_2, \dots, \beta_l)$ に等しくなる。

また、 β_1, \dots, β_l が互いに等しくないと仮定すると、 $\alpha = 0$ のとき、

$$\phi(\beta_1, \dots, \beta_l) = \max_{b_0, \dots, b_l} \left\{ |b_0| \mid h(\beta_1) = 0, \dots, h(\beta_l) = 0, \|h\| \leq 1 \right\} \quad (2.21)$$

と書くことができる。このように書くことにより0のまわりの多零点の穴の解析は線形システムとノルムによって束縛された集合の中の最大値を求めることになり、解析が比較的楽になる。第7章において多零点の穴について詳しい解析を行なう。

第3章

ノルムに関する結果

本章では、第2章で定義したノルムを用いて、多零点の穴の解析を行う。まず、ノルムの性質をいくつか挙げておく。ノルムは、関数空間上の距離を測る尺度であり、関数の大きさを測る尺度である。ノルムの性質は、関数空間の構造を決定する重要な要素である。本章では、ノルムの性質をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。

ノルムの性質に関する結果

本章では、ノルムの性質に関する結果をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。本章では、ノルムの性質をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。

本章では、ノルムの性質に関する結果をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。本章では、ノルムの性質をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。

本章では、ノルムの性質に関する結果をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。本章では、ノルムの性質をいくつか挙げておく。ノルムの性質は、関数空間の構造を決定する重要な要素である。

第 3 章

2-ノルムに関する結果

本章では、第2章で定義した穴を用いて2-ノルムに関する多項式の零点の位置について調べた結果を述べる。2-ノルムは良く知られたノルムの中でもっとも性質のよいものである。とくに、このノルムに対しては二次形式の手法が使えるので、穴 $H_{\alpha, f}$ を陽に書き表すことができる。本章では、0の回りの穴についてまず解析し、2-ノルムによって制限された多項式の零点がどのような範囲に分布するかを解析する。また、そのうち、一般の複素数 α についてそのまわりの穴について考察する。本章ではノルム $\|\cdot\|$ は $\|\cdot\|_2$ を意味するものとする。

3.1 2-ノルムにおける穴の記述

2-ノルムを扱うときには、多項式をその係数をならべたベクトルと同一視すると都合がよい。この場合、多項式の2-ノルムはそのベクトルのユークリッドノルムになる。または多項式 $f(x)$ の係数をならべてできるベクトルを f と書き、 $a^{[n]} = (1, \alpha, \alpha^2, \dots, \alpha^n)$ とおけば、 $f(\alpha)$ は内積 $(f, \overline{a^{[n]}})$ と等しい。ただし、 $\overline{a^{[n]}}$ は $a^{[n]}$ の複素共役である。

まず、つぎの補助定理を証明する。この性質を用いることによって2-ノルムについての議論を効率的に行なうことができる。

補助定理 9 $a, b, s_i, (i=1, \dots, l)$ を K^{n+1} の要素とする。すなわち、これらは K 上の $n+1$ 次元ベクトルとする。また、 S を $S = (s_1, \dots, s_l)$ とおき、 $A = \overline{S}^T S$ は正則であるとする。 (a, b) を a と b の K^{n+1} 上の内積とする。すなわち $(a, b) = \overline{a}^T b$ とする。このとき

$$\begin{aligned} \max_b \left\{ |(a, b)| \mid (s_i, b) = 0, (i=1, \dots, l), (b, b) \leq 1 \right\} &= \left[(a, a) - \overline{a}^T S A^{-1} \overline{S}^T a \right]^{1/2} \quad (3.1) \\ &= \left[\frac{G(a, s_1, \dots, s_l)}{G(s_1, \dots, s_l)} \right]^{1/2} \quad (3.2) \end{aligned}$$

である。ただし、 $G(a, s_1, \dots, s_l)$ はベクトル a, s_1, \dots, s_l のグラムの行列式 [CH31]

$$\begin{vmatrix} (a, a) & (a, s_1) & \dots & (a, s_l) \\ (s_1, a) & (s_1, s_1) & \dots & (s_1, s_l) \\ \vdots & \vdots & \ddots & \vdots \\ (s_l, a) & (s_l, s_1) & \dots & (s_l, s_l) \end{vmatrix}$$

を表している。

証明 ここでは $K = \mathbb{C}$ について証明する。 $K = \mathbb{R}$ についても全く同様である。 \mathbb{C}^{n+1} の部分集合としてつぎのような集合 X を定義する。

$$X = \left\{ b \in \mathbb{C}^{n+1} \mid (s_i, b) = 0, (i = 1, \dots, l), (b, b) \leq 1 \right\}.$$

ここで

$$c_0 = a - SA^{-1}\overline{S^T}a$$

とおくと、

$$\begin{aligned} (s_i, c_0) &= (s_i, a) - \overline{s_i^T} SA^{-1}\overline{S^T}a \\ &= (s_i, a) - ((s_i, s_1), \dots, (s_i, s_l)) A^{-1}\overline{S^T}a \\ &= (s_i, a) - (0, \dots, 0, 1, 0, \dots, 0) \overline{S^T}a \\ &= (s_i, a) - (s_i, a) = 0 \end{aligned}$$

である。よって、 $b_0 = c_0 / \sqrt{(c_0, c_0)}$ とおけば、 $b_0 \in X$ である。また、一方任意の $d \in X$ に対して、 c_0 の定義より

$$|(a, d)| = |(c_0, d)|$$

よって、Schwartz の不等式より、 $|(a, d)| \leq |c_0| |d| \leq |c_0|$ である。また、 $(b_0, a) = (b_0, c_0) = \sqrt{(c_0, c_0)} = |c_0|$ である。したがって、 $|(a, b)|$ の最大値は $|c_0|$ である。ここで

$$\begin{aligned} (c_0, c_0) &= (a, a) - \overline{a^T} SA^{-1}\overline{S^T}a - \overline{a^T} \overline{S} A^{-1, T} \overline{S^T} a + \overline{a^T} \overline{S} A^{-1, T} \overline{S^T} SA^{-1}\overline{S^T} a \\ &= (a, a) - \overline{a^T} SA^{-1}\overline{S^T}a \end{aligned}$$

である。さらに、 $A^{-1} = \text{adj } A / \det A$ という性質を用いれば、

$$(c_0, c_0) = \frac{G(a, s_1, \dots, s_l)}{G(s_1, \dots, s_l)}$$

である。以上より本補助定理は証明された。 □

まず, $K = \mathbb{C}$, $\alpha, \beta \in \mathbb{C}$ の場合を考える. このとき, $P(\beta)$ と $H_{\alpha, f}$ はつぎのように表せる. ただし, ここで多項式とベクトルは同一視している.

$$P(\beta) = \left\{ h \in \mathbb{C}^{n+1} \mid (h, \overline{\beta^{[n]}}) = 0, (h, h) \leq 1 \right\}, \quad (3.3)$$

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \max_{h \in P(\beta)} |(h, \overline{\alpha^{[n]}})| < |f(\alpha)| / \|f\| \right\}. \quad (3.4)$$

補助定理 9 より

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \left[\frac{G(\overline{\beta^{[n]}}), \alpha^{[n]}}{G(\overline{\beta^{[n]}})} \right]^{1/2} < \frac{|f(\alpha)|}{\|f\|} \right\}$$

である. すなわち,

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \frac{\sqrt{|\beta^{[n]}|^2 |\alpha^{[n]}|^2 - |(\alpha^{[n]}, \overline{\beta^{[n]}})|^2}}{|\beta^{[n]}|} < \frac{|f(\alpha)|}{\|f\|} \right\}$$

である. また, $K = \mathbb{R}$ かつ $\alpha, \beta \in \mathbb{R}$ の場合にはやはり同様にして

$$H_{\alpha, f} \cap \mathbb{R} = \left\{ \beta \in \mathbb{C} \mid \frac{\sqrt{|\beta^{[n]}|^2 |\alpha^{[n]}|^2 - |(\alpha^{[n]}, \overline{\beta^{[n]}})|^2}}{|\beta^{[n]}|} < \frac{|f(\alpha)|}{\|f\|} \right\}$$

である.

つぎに $K = \mathbb{R}$, $\alpha \in \mathbb{R}$, $\beta \in \mathbb{C} \setminus \mathbb{R}$ である場合について考える. この場合,

$$P(\beta) = \left\{ h \in \mathbb{R}^{n+1} \mid (h, \operatorname{Im} \beta^{[n]}) = 0, (h, \operatorname{Re} \beta^{[n]}) = 0, (h, h) \leq 1 \right\},$$

$$H_{\alpha, f} \setminus \mathbb{R} = \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \max_{h \in P(\beta)} |(h, \overline{\alpha^{[n]}})| < \frac{|f(\alpha)|}{\|f\|} \right\}$$

と書くことができる. この場合も補助定理 9 より,

$$H_{\alpha, f} \setminus \mathbb{R} = \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \left[\frac{G(\alpha^{[n]}, \operatorname{Im} \beta^{[n]}, \operatorname{Re} \beta^{[n]})}{G(\operatorname{Im} \beta^{[n]}, \operatorname{Re} \beta^{[n]})} \right]^{1/2} < \frac{|f(\alpha)|}{\|f\|} \right\}$$

となる. 以上の結果をまとめるとつぎの補助定理となる.

補助定理 10 $K = \mathbb{C}$, $\alpha \in \mathbb{C}$ のとき

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \frac{\sqrt{|\beta^{[n]}|^2 |\alpha^{[n]}|^2 - |(\alpha^{[n]}, \overline{\beta^{[n]}})|^2}}{|\beta^{[n]}|} < \frac{|f(\alpha)|}{\|f\|} \right\} \quad (3.5)$$

である. また $K = \mathbb{R}$ であり, かつ $\alpha \in \mathbb{R}$ の場合は

$$H_{0,f} = \left\{ \beta \in \mathbb{R} \mid \frac{\sqrt{|\beta^{[n]}|^2 |\alpha^{[n]}|^2 - (\alpha^{[n]}, \beta^{[n]})^2}}{|\beta^{[n]}|} < \frac{|f(\alpha)|}{\|f\|} \right\} \\ \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \left[\frac{G(\alpha^{[n]}, \operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})}{G(\operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})} \right]^{1/2} < \frac{|f(\alpha)|}{\|f\|} \right\} \quad (3.6)$$

である.

この性質を用いて本章の以降の部分では 2-ノルムの場合の穴の形について解析する.

3.2 0 のまわりの穴に関する結果

前節で導いた性質を用いて 0 のまわりの穴を解析し, 多項式の零点の存在範囲を導く. この結果は Mignotte による結果 [Mig74] から導かれるものと一致する. ここでは Mignotte の結果を経由せずに直接導く.

まず, $K = \mathbb{R}$ の場合について考える. この場合補助定理 10 より

$$H_{0,f} = \left\{ \beta \in \mathbb{R} \mid \frac{\sqrt{|\beta^{[n]}|^2 - 1}}{|\beta^{[n]}|} < \frac{|f(0)|}{\|f\|} \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \left[\frac{G(\alpha^{[n]}, \operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})}{G(\operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})} \right]^{1/2} < \frac{|f(0)|}{\|f\|} \right\}$$

である. このとき $\beta \neq 0$ かつ $\beta \in \mathbb{R}$ のときは

$$\frac{\sqrt{|\beta^{[n]}|^2 - 1}}{|\beta^{[n]}|} = |\beta| \sqrt{\frac{\sum_{i=0}^{n-1} |\beta|^{2i}}{\sum_{i=0}^n |\beta|^{2i}}} < |\beta|$$

となり, これより

$$H_{0,f} \cap \mathbb{R} \supset \widetilde{H_0^{\mathbb{R}}} \equiv \left\{ \beta \in \mathbb{R} \mid |\beta| \leq \frac{|f(0)|}{\|f\|} \right\}$$

が得られる. $\widetilde{H_0^{\mathbb{R}}}$ と $H_{0,f} \cap \mathbb{R}$ のずれは, このグラフと $y = |x|$ のずれに等しい. $y = \frac{\sqrt{|\beta^{[n]}|^2 - 1}}{|\beta^{[n]}|}$ のグラフを Fig. 3.1 に示す. この場合, このずれは原点に近いところでは, ほとんど目で見えない程度であり, $\beta = 1$ および $\beta = -1$ 付近でずれ始めている. このような意味で, ある程度原点に近いところでは $\widetilde{H_0^{\mathbb{R}}}$ は $H_{0,f} \cap \mathbb{R}$ の部分集合であるばかりでなく, 良い近似になっていると言える. また一方, $\beta \in \mathbb{C} \setminus \mathbb{R}$ の場合は $\phi^2(\beta) = \left[\frac{G(0^{[n]}, \operatorname{Im} \beta^{[n]}, \operatorname{Re} \beta^{[n]})}{G(\operatorname{Im} \beta^{[n]}, \operatorname{Re} \beta^{[n]})} \right]$ について考えればよい. ここで

$$\begin{pmatrix} 0^{[n]} \\ \operatorname{Re} \beta^{[n]} \\ \operatorname{Im} \beta^{[n]} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \operatorname{Re} \beta & \operatorname{Re} \beta^2 & \cdots & \operatorname{Re} \beta^n \\ 0 & \operatorname{Im} \beta & \operatorname{Im} \beta^2 & \cdots & \operatorname{Im} \beta^n \end{pmatrix}$$

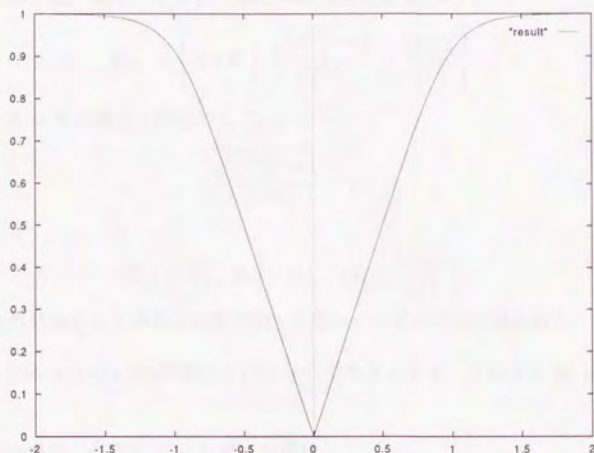


Fig. 3.1. $\beta \in \mathbb{R}$, $n=5$ のときの $y = \frac{\sqrt{|\beta^{[n]}|^2 - 1}}{|\beta^{[n]}|}$ のグラフ

である。行列 $\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & i \\ 0 & 1 & -i \end{pmatrix}$ を左側からかけることにより、

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & i \\ 0 & 1 & -i \end{pmatrix} \begin{pmatrix} 0^{[n]} \\ \operatorname{Re} \beta^{[n]} \\ \operatorname{Im} \beta^{[n]} \end{pmatrix} = \begin{pmatrix} 0^{[n]} \\ \beta(0, 1, \beta, \dots, \beta^{n-1}) \\ \bar{\beta}(0, 1, \bar{\beta}, \dots, \bar{\beta}^{n-1}) \end{pmatrix}$$

と書くことができる。したがって、 $d = (0, 1, \beta, \dots, \beta^{n-1})$ とおけば、

$$\phi^2(\beta) = |\beta|^4 \frac{G(0^{[n]}, d, \bar{d})}{G(d, \bar{d})}.$$

ここで、 $0^{[n]}$ は d, \bar{d} と直交していることから $G(0^{[n]}, d, \bar{d}) = G(d, \bar{d})$ である。 d は要素の位置を無視すれば β^n が 0 に置き換わっただけである。したがって、 $G(\beta^{[n]}, \bar{\beta}^{[n]}) > G(d, \bar{d})$ である。以上より、

$$\phi(\beta) < |\beta|^4$$

であり、すなわち、

$$H_{0,f} \setminus \mathbb{R} \supset H_{0,f}^{\widetilde{\mathbb{C}}} \mathbb{R} \equiv \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta|^2 \leq \frac{|f(0)|}{\|f\|} \right\}.$$

であることがわかる。また、 $K = \mathbb{C}$ の場合には補助定理 10 より、

$$H_{0,f} = \left\{ \beta \in \mathbb{C} \mid \frac{\sqrt{|\beta^{[n]}|^2 - 1}}{|\beta^{[n]}|} < \frac{|f(0)|}{\|f\|} \right\}$$

であるので、 $K = \mathbb{R}$ の場合と同様にして、

$$\frac{\sqrt{|\beta^{[n]}|^2 - 1}}{|\beta^{[n]}|} < |\beta|$$

である。よって、

$$H_{0,f} \supset \widetilde{H}_{0,f} \equiv \left\{ \beta \in \mathbb{C} \mid |\beta| \leq \frac{|f(0)|}{\|f\|} \right\}$$

である。以上の結果をまとめれば補助定理 1 を用いてつぎの定理が得られる。

定理 2 $f(x)$ を体 K 上の n 次多項式で $f(0) \neq 0$ であるとする。このとき $M = \|f\|/|f(0)|$ とおけば、

1. $K = \mathbb{R}$ の場合、多項式 $f(x)$ の零点は領域

$$\widetilde{H}_{0,f} = \left\{ \beta \in \mathbb{R} \mid |\beta| \leq 1/M \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta| \leq 1/\sqrt{M} \right\} \quad (3.7)$$

に含まれない。

2. また、 $K = \mathbb{C}$ の場合、 $f(x)$ の零点は領域

$$\widetilde{H}_{0,f} = \left\{ \beta \in \mathbb{C} \mid |\beta| \leq 1/M \right\} \quad (3.8)$$

に含まれない。

この補助定理より多項式 $f(x)$ の零点の存在範囲をつぎのように定めることができる。

系 3 $f(x)$ を体 K 上の n 次多項式であるとする。 $M = \|f\|/\|c_f\|$ とおく。このとき、

1. $K = \mathbb{R}$ であるのならば領域

$$\widetilde{H}_{\infty,f} = \left\{ \beta \in \mathbb{R} \mid |\beta| \geq M \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta| \geq \sqrt{M} \right\} \quad (3.9)$$

に $f(x)$ の零点は存在しない。

2. また、 $K = \mathbb{C}$ の場合領域

$$\widetilde{H}_{\infty,f} = \left\{ \beta \in \mathbb{C} \mid |\beta| \geq M \right\} \quad (3.10)$$

に $f(x)$ の根は存在しない。

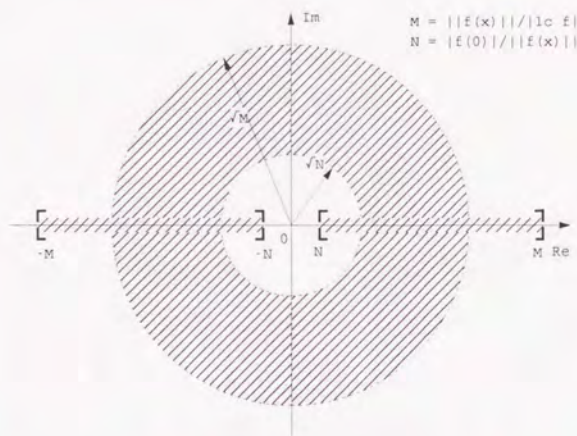


Fig. 3.2. $K = \mathbb{R}$ の場合の $f(x)$ の零点の2-ノルムによる存在範囲

証明 多項式 $f(x)$ が $f(x) = \sum_{i=0}^n a_i x^i$ と表されているとする. $g(x) = \sum_{i=0}^n a_i x^{n-i}$ とおく. このとき多項式 $g(x)$ の0でない根の逆数は $f(x)$ の根となっている. また明らかに $\|f\| = \|g\|$ である. これより定理2を用いればこの系を得る. \square

定理2および系3で述べている零点不在領域以外の領域 (零点の存在する領域) を $K = \mathbb{R}$ の場合と $K = \mathbb{C}$ の場合についてそれぞれ Fig. 3.2および Fig. 3.3に斜線で示す. 両方の図においてドーナツ形の領域の境界は存在範囲に含まれない. また, Fig. 3.2の実軸上の区間の境界も存在範囲に含まれない. 両方の図において M と N は

$$M = \|f\| / |c f|$$

$$N = |f(0)| / \|f\|$$

である.

定理2の結果は Landau の不等式 [Mig74] から導くことができる. Landau (Mignotte) の不等式とはつぎのようなものである.

定理3 ([Mig74]) 複素数体上の多項式 $f(x)$ のすべての零点 $\alpha_1, \dots, \alpha_n$ がつぎのように絶対値の順番に並んでいるとする:

$$|\alpha_1| \leq |\alpha_2| \leq \dots \leq |\alpha_r| < 1 \leq |\alpha_{r+1}| \leq \dots \leq |\alpha_n|. \quad (3.11)$$

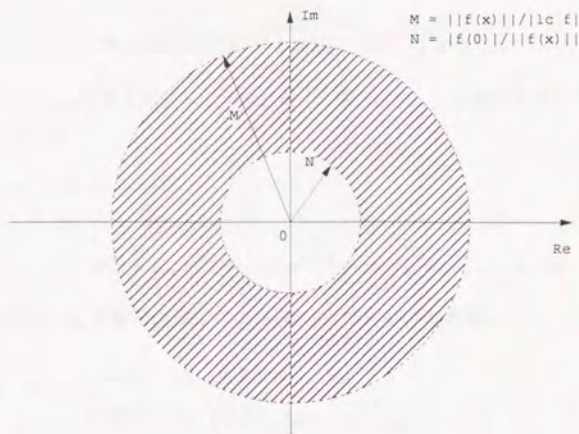


Fig. 3.3. $K = \mathbb{C}$ の場合の $f(x)$ の零点の 2-ノルムによる存在範囲

このとき

$$|\alpha_{r+1} \cdots \alpha_n| < \frac{\|f\|_2}{\|lc f\|} \quad (3.12)$$

である。

実数を係数とする多項式の実数でない零点 α は必ずその複素共役である複素数 $\bar{\alpha}$ を零点として持つ。よって定理 3 よりこのような場合には $|\alpha| \geq 1$ の場合には

$$|\alpha \bar{\alpha}| = |\alpha|^2 < \frac{\|f\|_2}{\|lc f\|}$$

であることがわかる。これは系 3 の結果である。

3.3 任意の数のまわりの穴の解析

実係数多項式について任意の実数のまわりの穴を解析することは大変困難である。本節では $|f(\alpha)|/\|f\|$ が十分に小さいという状況で穴が漸近的にどのような形になるかを解析する。

まず, $K = \mathbb{C}$ の場合について考える. この場合穴は補助定理 10 より

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \frac{G(\alpha^{[n]}, \beta^{[n]})}{G(\beta^{[n]})} < \frac{|f(\alpha)|^2}{\|f\|^2} \right\}$$

である. ここで, $\varepsilon \in \mathbb{C}$ として $\beta = \alpha + \varepsilon$ とおく. 系 1 より, ε は絶対値の小さな複素数と
考えてよい. よって

$$\begin{aligned} \beta^{[n]} &= (\alpha + \varepsilon)^{[n]} \\ &= (1, \alpha + \varepsilon, (\alpha + \varepsilon)^2, \dots, (\alpha + \varepsilon)^n) \\ &= \alpha^{[n]} + D_\alpha \alpha^{[n]} \varepsilon + \frac{1}{2} D_\alpha^2 \alpha^{[n]} \varepsilon^2 + (o(\varepsilon^2), o(\varepsilon^2), \dots, o(\varepsilon^2)) \end{aligned}$$

とかける. ただし, D_α は微分演算子で $\partial/\partial\alpha$ のことである. したがって,

$$\begin{aligned} D_\alpha \alpha^{[n]} &= (0, 1, 2\alpha, \dots, n\alpha^{n-1}), \\ \frac{1}{2} D_\alpha^2 \alpha^{[n]} &= \left(0, 0, 1, 3\alpha, \dots, \frac{n(n-1)}{2} \alpha^{n-2} \right) \end{aligned}$$

である. ここで,

$$\begin{pmatrix} \alpha^{[n]} \\ \beta^{[n]} \end{pmatrix} = \begin{pmatrix} \alpha^{[n]} \\ \alpha^{[n]} + D_\alpha \alpha^{[n]} \varepsilon \end{pmatrix}$$

—であることから,

$$G(\alpha^{[n]}, \beta^{[n]}) = |\varepsilon|^2 G(\alpha, \alpha^{[n]})$$

である. したがって, $|f(\alpha)|/\|f\|$ が十分に小さいとき α のまわりの $f(x)$ の零点の穴は漸近
的に集合

$$\mathcal{H}_{\alpha, f} = \left\{ \alpha + \varepsilon \in \mathbb{C} \mid \varepsilon \in \mathbb{C}, \left[|D_\alpha \alpha^{[n]}|^2 - |(D_\alpha \alpha^{[n]}, \alpha^{[n]})|^2 / |\alpha^{[n]}|^2 \right]^{1/2} |\varepsilon| < \frac{|f(\alpha)|}{\|f\|} \right\}$$

に近づく.

つぎに $K = \mathbb{R}$ の場合について考える. この場合, 補助定理 10 より実軸上の穴の領域は
 $K = \mathbb{C}$ の場合と同様にして漸近的に

$$\mathcal{H}_{\alpha, f}^{\mathbb{R}} = \left\{ \alpha + \varepsilon \mid \varepsilon \in \mathbb{R}, \left[|D_\alpha \alpha^{[n]}|^2 - |(D_\alpha \alpha^{[n]}, \alpha^{[n]})|^2 / |\alpha^{[n]}|^2 \right]^{1/2} |\varepsilon| < \frac{|f(\alpha)|}{\|f\|} \right\}$$

となる. また, 実軸でない部分に関しては補助定理 10 より

$$H_{\alpha, f} \setminus \mathbb{R} = \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \frac{G(\alpha^{[n]}, \operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})}{G(\operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})} < \frac{|f(\alpha)|^2}{\|f\|^2} \right\}$$

とかくことができる。ここで $H_{\alpha, f} \cap \mathbb{R}$ と同様に計算すると、計算が大変複雑になるので、直接計算せず、グラムの行列式を操作する。まず、

$$X = \begin{pmatrix} 1 & 0 & 0 \\ -(\operatorname{Re}\beta - \alpha) & \operatorname{Re}\beta - \alpha & \operatorname{Im}\beta \\ \operatorname{Im}\beta & -\operatorname{Im}\beta & \operatorname{Re}\beta - \alpha \end{pmatrix}$$

とおけば、

$$X \begin{pmatrix} \alpha^{[n]} \\ \operatorname{Re}\beta^{[n]} \\ \operatorname{Im}\beta^{[n]} \end{pmatrix}$$

はつぎのようになる。

まず、第一列は

$$(1, \alpha, \alpha^2, \dots, \alpha^n)$$

となる。また、第二列の第 i 要素は

$$\begin{aligned} & \operatorname{Re}(\beta^i - \alpha^i) \operatorname{Re}(\beta - \alpha) + \operatorname{Im}(\beta^i - \alpha^i) \operatorname{Im}(\beta - \alpha) \\ &= \operatorname{Re} \left(\sum_{j=0}^{i-1} \beta^j \alpha^{i-1-j} \right) (\operatorname{Re}(\beta - \alpha))^2 + \operatorname{Re} \left(\sum_{j=0}^{i-1} \beta^j \alpha^{i-1-j} \right) (\operatorname{Im}(\beta - \alpha))^2 \\ &= \operatorname{Re} \left(\sum_{j=0}^{i-1} \beta^j \alpha^{i-1-j} \right) |\beta - \alpha|^2 \end{aligned}$$

であり、第三列の第 i 要素は

$$\begin{aligned} & -\operatorname{Re}(\beta^i - \alpha^i) \operatorname{Im}(\beta - \alpha) + \operatorname{Im}(\beta^i - \alpha^i) \operatorname{Re}(\beta - \alpha) \\ &= \operatorname{Im} \left(\sum_{j=0}^{i-1} \beta^j \alpha^{i-1-j} \right) (\operatorname{Im}(\beta - \alpha))^2 + \operatorname{Im} \left(\sum_{j=0}^{i-1} \beta^j \alpha^{i-1-j} \right) (\operatorname{Re}(\beta - \alpha))^2 \\ &= \operatorname{Im} \left(\sum_{j=0}^{i-1} \beta^j \alpha^{i-1-j} \right) |\beta - \alpha|^2 \end{aligned}$$

である。よって、

$$X \begin{pmatrix} \alpha^{[n]} \\ \operatorname{Re}\beta^{[n]} \\ \operatorname{Im}\beta^{[n]} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & |\beta - \alpha|^2 & 0 \\ 0 & 0 & |\beta - \alpha|^2 \end{pmatrix} B_2$$

とかける。ただし、

$$B_2 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^n \\ 0 & 1 & \operatorname{Re}(\beta + \alpha) & \dots & \operatorname{Re}(\sum_{i=0}^{n-1} \beta^i \alpha^{n-1-i}) \\ 0 & 0 & \operatorname{Im}(\beta + \alpha) & \dots & \operatorname{Im}(\sum_{i=0}^{n-1} \beta^i \alpha^{n-1-i}) \end{pmatrix}$$

とする。よって、

$$G(\alpha^{[n]}, \operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]}) = |\beta - \alpha|^4 (\operatorname{Im} \beta)^2 G(\alpha^{[n]}, D_\alpha \alpha^{[n]}, D_\alpha^2 \alpha^{[n]})$$

であり、また、 $G(\operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})$ については $\begin{pmatrix} \operatorname{Re} \beta^{[n]} \\ \operatorname{Im} \beta^{[n]} \end{pmatrix}$ が $\begin{pmatrix} 1 & 0 \\ 0 & \operatorname{Im} \beta \end{pmatrix} \begin{pmatrix} \alpha^{[n]} \\ D_\alpha \alpha^{[n]} \end{pmatrix}$ に近づくことから、 $(\operatorname{Im} \beta)^2 G(\alpha^{[n]}, D_\alpha \alpha^{[n]})$ に近づくことになる。以上より、

$$\frac{G(\alpha^{[n]}, \operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})}{G(\operatorname{Re} \beta^{[n]}, \operatorname{Im} \beta^{[n]})}$$

は

$$|\beta - \alpha|^4 \frac{G(\alpha^{[n]}, D_\alpha \alpha^{[n]}, D_\alpha^2 \alpha^{[n]})}{G(\alpha^{[n]}, D_\alpha \alpha^{[n]})}$$

に近づく。以上より、 $|f(\alpha)|/\|f\|$ が十分に小さいとき

$$H_{\alpha, f} \setminus \mathbb{R} \approx \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta - \alpha| < C_3(n, \alpha) \cdot \left(\frac{|f(\alpha)|}{\|f\|} \right)^{1/2} \right\}$$

である。ここで $C_3(n, \alpha)$ は n と α に依存する定数である。本節の内容をまとめるとつぎのようになる。

定理 4 $f(x)$ を体 K 上の多項式とする。 $|f(\alpha)|/\|f\|$ が十分に小さいときある複素数 α のまわりの穴は、 $K = \mathbb{C}$ ならば

$$H_{\alpha, f} \approx \left\{ \beta \in \mathbb{C} \mid |\beta - \alpha| < C_1(n, \alpha) \frac{|f(\alpha)|}{\|f\|} \right\} \quad (3.13)$$

へちかづく。ただし、 $C_1(n, \alpha)$ はある次数 n と α に依存する定数である。また、 $K = \mathbb{R}$ の場合、

$$H_{\alpha, f} \approx \left\{ \beta \in \mathbb{R} \mid |\beta - \alpha| < C_2(n, \alpha) \frac{|f(\alpha)|}{\|f\|} \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta - \alpha| < C_3(n, \alpha) \sqrt{\frac{|f(\alpha)|}{\|f\|}} \right\} \quad (3.14)$$

となる。ただし、 $C_2(n, \alpha)$ 、 $C_3(n, \alpha)$ は n および α に依存する定数である。

また、 $G(\alpha^{[n]}, D_\alpha \alpha^{[n]})/G(\alpha^{[n]})$ 、 $G(\alpha^{[n]}, D_\alpha \alpha^{[n]}, D_\alpha^2 \alpha^{[n]})/G(\alpha^{[n]}, D_\alpha \alpha^{[n]})$ は n に関してそれぞれ $O(\alpha^{2n-2})$ 、 $O(\alpha^{2n-4})$ となる。よって α を固定したとき n が大きくなるにつれて穴は小さくなる。よって、次数を制限しないような多項式では $\alpha \neq 0$ のとき穴は潰れてなくなってしまう。 $\|f\|_\infty \leq \|f\|_2$ 同様な議論は ∞ -ノルムについても言える。

第 4 章

1-ノルムに関する結果

本章では、第 2 章で示した穴を 1-ノルムについて計算し、その性質について分析する。第 3 章で 2-ノルムに関する結果を示したが、1-ノルムについては第 2 章で用いた二次形式の方法を使うことはできないので、全く別の方法で分析しなければならない。しかし、零点の存在範囲については 2-ノルムと同じような結果が得られる。本章では $\|\cdot\|$ は $\|\cdot\|_1$ を表すものとする。

4.1 0 のまわりの穴に関する結果

本節では 1-ノルムについて 0 のまわりの穴を解析する。まず、 $K = \mathbb{R}$ の場合について考える。ここでも多項式の係数をならべたベクトルとその多項式を同一視する。

$$P^{\text{vec}}(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{R}^{n+1} \mid \sum_{i=0}^n b_i \beta^i = 0, \sum_{i=0}^n |b_i| \leq 1 \right\}$$

とおけば、 $H_{0,f}$ は

$$H_{0,f} = \left\{ \beta \in \mathbb{C} \mid \phi(\beta) < \frac{|f(0)|}{\|f\|} \right\}$$

と書ける。ただし、

$$\phi(\beta) = \max \left\{ |b_0| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

とする。まず、 $H_{0,f} \cap \mathbb{R}$ について考える。ある実数 β について、集合 $P^{\text{vec}}(\beta)$ は \mathbb{R}^{n+1} 次元空間の中の n 次元の多面体となっている。また、 $\phi(\beta)$ の定義の中の $|b_0|$ は b_0, \dots, b_n の一次結合の絶対値と考えることができる。よって、 $\phi(\beta)$ の値は $P^{\text{vec}}(\beta)$ の頂点で実現される。ここで $P^{\text{vec}}(\beta)$ を定義している方程式系について考えると、これが表現している多面体の頂点は $n+1$ 個の方程式の解となっていて、その方程式は $\sum_{i=0}^n b_i \beta^i = 0$ と n 個の $\sum_{i=0}^n \pm b_i = 1$ という形をした方程式によって表現される。すなわち、適当な数 $s_{i,j} \in \{+1, -1\}$, $(i =$

$1, \dots, n, j = 0, \dots, n$ を用いて

$$\sum_{i=0}^n b_i \beta^i = 0,$$

$$\sum_{i=0}^n s_{i,j} b_j = 1, \quad (i = 1, \dots, n)$$

と表現することができる。ただし $\sum_{i=0}^n |b_i| \leq 1$ であることから

$$s_{i,j} b_j \geq 0 \quad (i, j = 1, \dots, n)$$

とする。この方程式系が解をもつということから n 個のベクトル

$$(s_{1,0}, \dots, s_{1,n}, 1),$$

$$(s_{2,0}, \dots, s_{2,n}, 1),$$

$$\vdots$$

$$(s_{n,0}, \dots, s_{n,n}, 1)$$

は線形独立である。よって、すくなくとも $n-1$ 個の j について $s_{1,j} \neq s_{i,j}$ となる j が $\{2, \dots, n\}$ のなかに存在する。条件 $s_{i,j} b_j \geq 0$ より、このような j について $b_j \neq 0$ である。すなわち b_0, \dots, b_n の中で 0 でないのは高々 2 つである。ここでは $|b_0|$ の最大値を考えているので $b_0 \neq 0$ と仮定してよい。以上の考察より $\phi(\beta)$ は

$$\phi(\beta) = \max \left\{ |b_0| \mid 1 \leq k \leq n, b_0, b_k \in \mathbb{R}, b_0 + \beta^k b_k = 0, |b_0| + |b_k| = 1 \right\}$$

$$= \max \left\{ \frac{|\beta|^k}{1 + |\beta|^k} \mid 1 \leq k \leq n \right\}$$

と書くことができる。よって、 $\phi(\beta)$ は $0 \leq |\beta| \leq 1$ と $1 \geq |\beta|$ の場合にそれぞれ $|\beta|/(1+|\beta|)$, $|\beta|^n/(1+|\beta|^n)$ となる。このグラフを $n=5$ の場合について Fig. 4.1 に示す。この結果より $H_{0,f} \cap \mathbb{R}$ は

$$H_{0,f} \cap \mathbb{R} = \begin{cases} \emptyset & \text{if } |f(0)|/\|f\| = 0, \\ \left\{ \beta \in \mathbb{R} \mid |\beta| < (\|f\|/|f(0)| - 1)^{-1} \right\} & \text{if } |f(0)|/\|f\| \leq 1/2, \\ \left\{ \beta \in \mathbb{R} \mid |\beta| < (\|f\|/|f(0)| - 1)^{-1/n} \right\} & \text{if } 1/2 < |f(0)|/\|f\| < 1, \\ \mathbb{R} & \text{if } |f(0)|/\|f\| = 1 \end{cases}$$

となる。

つぎに $\beta \in \mathbb{C} \setminus \mathbb{R}$ の場合について考える。この場合、定義より、 $\phi(\beta)$ は

$$\phi(\beta) = \max \left\{ |b_0| \mid (b_0, b_1, \dots, b_n) \in \mathbb{R}^{n+1}, \sum_{i=0}^n b_i \operatorname{Re} \beta^i = 0, \sum_{i=0}^n b_i \operatorname{Im} \beta^i = 0, \sum_{i=0}^n |b_i| \leq 1 \right\}$$

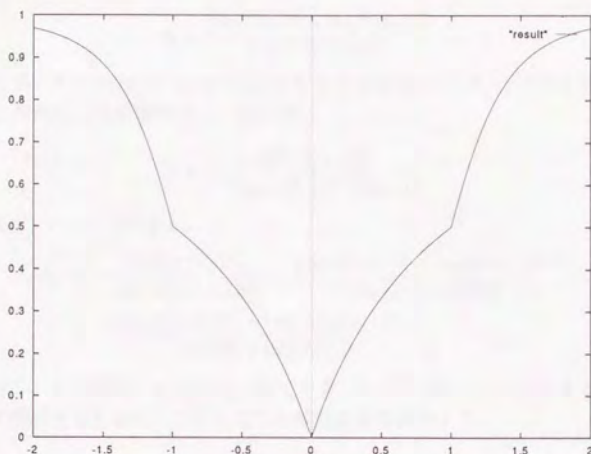


Fig. 4.1. $K = \mathbb{R}$, $\beta \in \mathbb{R}$, $n = 5$ の場合の $\phi(\beta)$ の形

である。前の場合と同様にして、この場合、高々3つの変数の値が0でない。よって、これらを b_0, b_j, b_k , ($0 < j < k \leq n$) とおく。このとき、 $\phi(\beta) = \max_{0 < j < k \leq n} \phi_{j,k}(\beta)$ とかける。ただし

$$\phi_{j,k}(\beta) = \max \left\{ |b_0| \mid b_0, b_j, b_k \in \mathbb{R}, |b_0| + |b_j| + |b_k| = 1, \right. \\ \left. b_0 + b_j \operatorname{Re} \beta^j + b_k \operatorname{Re} \beta^k = 0, b_j \operatorname{Im} \beta^j + b_k \operatorname{Im} \beta^k = 0 \right\}$$

である。まず、 $\operatorname{Im} \beta^j = \operatorname{Im} \beta^k = 0$ ($0 < j \leq n$) の場合について考える。このとき、 β が複素数であることから、 $j \geq 2$ であり、

$$\phi_{j,k} = \max \left\{ \frac{|\beta^j|}{1 + |\beta^j|}, \frac{|\beta^k|}{1 + |\beta^k|} \right\}$$

となる。これより、この場合は、

$$\begin{cases} \phi_{j,k}(\beta) < 1 & \text{if } r > 1 \\ \phi_{j,k}(\beta) \leq \frac{r^2}{1+r^2} & \text{if } 0 < r \leq 1 \end{cases}$$

となる。ただし、 $r = |\beta|$ である。

つぎに、 $\operatorname{Im} \beta^j \neq 0$ または $\operatorname{Im} \beta^k \neq 0$ の場合について考える。この場合、 $\phi_{j,k}$ の定義のなかの3つの方程式より

$$b_0 = \Lambda / (\Lambda + 1)$$

と書ける。ただし,

$$\Lambda = \frac{|\operatorname{Re} \beta^j \operatorname{Im} \beta^k - \operatorname{Re} \beta^k \operatorname{Im} \beta^j|}{|\operatorname{Im} \beta^j| + |\operatorname{Im} \beta^k|}$$

とする。ここで, $\beta = r(\cos \theta + i \sin \theta)$, ($r > 0$, $0 < \theta \leq \pi/2$) とおく。 $0 < \theta \leq \pi/2$ とすることは $H_{0,j}$ の対称性より問題ない。このとき,

$$\Lambda = \frac{|\sin(k-j)\theta|}{r^{-k}|\sin j\theta| + r^{-j}|\sin k\theta|}$$

と書ける。まず, $r=1$ とすると,

$$\begin{aligned} \Lambda &= \frac{|\sin(k-j)\theta|}{|\sin j\theta| + |\sin k\theta|} = \frac{|\sin k\theta \cos j\theta - \cos k\theta \sin j\theta|}{|\sin j\theta| + |\sin k\theta|} \\ &\leq \frac{|\sin k\theta| |\cos j\theta| + |\cos k\theta| |\sin j\theta|}{|\sin j\theta| + |\sin k\theta|} \leq 1 \end{aligned}$$

である。よって, この場合, $\phi_{j,k}(\beta) \leq 1/2$ である。つぎに $0 < r < 1$ であるとする。この場合について解析するために, つぎの二つの補助定理を証明する。

補助定理 11 $n \geq 2$ かつ $0 < \theta \leq \pi/2$ であるとき,

$$\left| \frac{\sin n\theta}{\sin \theta} \right| < n \quad (4.1)$$

である。

証明 帰納法で証明する。 $n=2$ の場合,

$$\left| \frac{\sin 2\theta}{\sin \theta} \right| = 2|\cos \theta| < 2$$

であるので明らかに成り立つ。また, $n=k$ のとき成り立つと仮定すると,

$$\left| \frac{\sin(k+1)\theta}{\sin \theta} \right| = \left| \frac{\sin k\theta \cos \theta}{\sin \theta} + \cos k\theta \right| = \left| \frac{\sin k\theta}{\sin \theta} \right| |\cos \theta| + |\cos k\theta| < k+1$$

となる。よって, 本補助定理を得る。 \square

補助定理 12 r と θ を $0 < \theta < \pi/2$, $0 < r < 1$ を満たす実数であるとする。また, k, j を

$$k > j > 0 \text{ かつ } [\sin j\theta \neq 0 \text{ または } \sin k\theta \neq 0] \quad (4.2)$$

を満たす整数とする。このとき,

$$\frac{|\sin(k-j)\theta|}{r^{-k}|\sin j\theta| + r^{-j}|\sin k\theta|} \leq r^2 \quad (4.3)$$

である。

証明 まず, $j \geq 2$ であると仮定する. このとき, 仮定より $k > 2$ である. よって,

$$\begin{aligned} |\sin(k-j)\theta| &= |\sin j\theta \cos k\theta - \cos j\theta \sin k\theta| \\ &\leq |\sin j\theta| |\cos k\theta| + |\sin j\theta| |\sin k\theta| \\ &\leq |\sin j\theta| + |\sin k\theta| \\ &\leq r^{2-k} |\sin j\theta| + r^{2-j} |\sin k\theta| \\ &= r^2 (r^{-k} |\sin j\theta| + r^{-j} |\sin k\theta|) \end{aligned}$$

となり, この場合補助定理は正しい. つぎに, $j = 1$ の場合について考える. この場合は $k \geq 2$ である. まず, つぎのような r に関する一変数関数 $f(r)$ を考える:

$$f(r) = \frac{\Lambda}{r^2} = \frac{|\sin(k-1)\theta|}{r^{2-k} |\sin \theta| + r |\sin k\theta|}.$$

$k = 2$ の場合,

$$g(r) = \left(1 + \left| \frac{\sin 2\theta}{\sin \theta} \right| r \right)^{-1} \leq 1$$

となり, 補助定理が正しいことが分かる. よって, 残されたケースは $j = 1, k > 2$ の場合のみである. まず, $g(r)$ の導関数は

$$g'(r) = \frac{-|\sin(k-1)\theta|((2-k)r^{1-k}|\sin \theta| + |\sin k\theta|)}{(r^{2-k}|\sin \theta| + r|\sin k\theta|)^2}$$

である. この導関数の意味のある零点は

$$r^* = {}^{k-1}\sqrt{\frac{k-2}{\left| \frac{\sin k\theta}{\sin \theta} \right|}}$$

である. この零点における g の値は

$$f(r^*) = \left[\frac{\frac{1}{(k-1)^{k-1}} \left| \frac{\sin(k-1)\theta}{\sin \theta} \right|^{k-1}}{\frac{1}{(k-2)^{k-2}} \left| \frac{\sin k\theta}{\sin \theta} \right|^{k-2}} \right]^{1/k-1}$$

である. $r^* \geq 1$ の場合は $k-2 > |\sin k\theta|/|\sin \theta|$ であり, $f'(r) > 0$ である. よって,

$$f(r) < f(1) = \frac{|\sin(k-1)\theta|}{|\sin \theta| + |\sin k\theta|}$$

である. よって,

$$\begin{aligned} |\sin(k-1)\theta| &= |\sin k\theta \cos \theta - \cos k\theta \sin \theta| \\ &\leq |\sin k\theta| + |\sin \theta| \end{aligned}$$

であることから, $f(r) < 1$ である. また, $0 < r^* < 1$ のときは

$$\frac{1}{k-2} \left| \frac{\sin k\theta}{\sin \theta} \right| > 1$$

であるので補助定理 11 より

$$f(r^*) < \frac{1}{k-1} \left| \frac{\sin(k-1)\theta}{\sin \theta} \right| \leq 1$$

である. 以上より, 本補助定理は証明された. □

補助定理 12 より $0 < r < 1$ のとき

$$\phi_{j,k} \leq \frac{r^2}{r^2 + 1} \quad (4.4)$$

であることがわかる. 以上の結果をまとめれば,

$$\begin{cases} \phi(\beta) < 1 & \text{if } r > 1 \\ \phi(\beta) \leq r^2/(1+r^2) & \text{if } 0 < r \leq 1 \end{cases} \quad (4.5)$$

となる. これよりつぎの定理を得る.

定理 5 $f(x)$ を実係数多項式で次数が n であるとする. また $M = \|f\|/|f(0)|$ とおく. このとき, 零点の存在しない範囲はつぎのようになる.

1. $M \geq 2$ の場合, 領域

$$\left\{ \beta \in \mathbb{R} \mid |\beta| < \frac{1}{M-1} \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \left| \beta \right| < \frac{1}{\sqrt{M-1}} \right\} \quad (4.6)$$

に $f(x)$ の零点は存在しない.

2. $1 < M < 2$ の場合, 領域

$$\left\{ \beta \in \mathbb{C} \mid |\beta| \leq 1 \right\} \quad (4.7)$$

に $f(x)$ の零点は存在しない.

3. $M = 1$ のとき $f(x)$ は零点を持たない存在しない. すなわち, $f(x)$ は定数である.

また, つぎに $K = \mathbb{C}$ の場合について考える. この場合, $P^{\text{vec}}(\beta)$ はつぎのように定義される:

$$P^{\text{vec}}(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{C}^{n+1} \mid \sum_{i=0}^n b_i \beta^i = 0, \sum_{i=0}^n |b_i| \leq 1 \right\}.$$

このとき、0のまわりの穴は

$$H_{0,f} = \left\{ \beta \in \mathbb{C} \mid \phi(\beta) < \frac{|f(0)|}{\|f\|} \right\}$$

である。ただし、

$$\phi(\beta) = \max \left\{ |b_0| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

である。ここで $|\beta| > 1$ であると仮定すると、任意の $(b_0, \dots, b_n) \in P^{\text{vec}}(\beta)$ について、

$$\begin{aligned} |b_0| &= |b_1\beta + b_2\beta^2 + \dots + b_n\beta^n| \\ &\leq |\beta|^n(|b_1| + \dots + |b_n|) = |\beta|^n(1 - |b_0|) \end{aligned}$$

が成り立つ。よって、 $|b_0| \leq |\beta|^n/(1 + |\beta|^n)$ である。さらに、 $(b_0, \dots, b_n) = (\beta^n/(1 + \beta^n), 0, \dots, 0, -1/(1 + |\beta|^n))$ とおけば、 $(b_0, \dots, b_n) \in P^{\text{vec}}(\beta)$ であり、 $|b_0| = |\beta|^n/(1 + |\beta|^n)$ である。よって $\phi(\beta) = |\beta|^n/(1 + |\beta|^n)$ である。また、 $|\beta| \leq 1$ であると仮定すると、

$$\begin{aligned} |b_0| &= |b_1\beta + b_2\beta^2 + \dots + b_n\beta^n| \\ &\leq |\beta|(|b_1| + \dots + |b_n|) \leq |\beta|(1 - |b_0|) \end{aligned}$$

である。また、 $(b_0, \dots, b_n) = (\beta/(1 + |\beta|), -1/(1 + |\beta|), 0, \dots, 0)$ とおけば $|b_0| = |\beta|/(1 + |\beta|)$ である。よって、 $\phi(\beta) = |\beta|/(1 + |\beta|)$ である。以上の結果より、

$$H_0 = \begin{cases} \left\{ \beta \in \mathbb{C} \mid |\beta| < \left(\frac{\|f\|}{|f(0)|} - 1 \right)^{-1} \right\} & \text{if } \frac{\|f\|}{|f(0)|} > 2 \\ \left\{ \beta \in \mathbb{C} \mid |\beta| < \left(\frac{\|f\|}{|f(0)|} - 1 \right)^{-1/n} \right\} & \text{if } 1 < \frac{\|f\|}{|f(0)|} < 2 \\ \mathbb{C} & \text{if } \frac{\|f\|}{|f(0)|} = 0 \end{cases} \quad (4.8)$$

である。この場合についてまとめると、つぎのようになる。

定理 6 $f(x)$ を複素数体上の n 次多項式であるとする。このとき、 $M = \|f\|/|f(0)|$ とおくと、 $f(x)$ の零点を含まない領域はつぎのようになる。

1. $M > 2$ の場合、

$$\left\{ \beta \in \mathbb{C} \mid |\beta| < \frac{1}{M-1} \right\} \quad (4.9)$$

は $f(x)$ の零点を含まない。

2. $1 < M \leq 2$ の場合、

$$\left\{ \beta \in \mathbb{C} \mid |\beta| < \frac{1}{\sqrt[M-1]{M-1}} \right\} \quad (4.10)$$

は $f(x)$ の零点を含まない。

3. $M = 1$ の場合、 $f(x)$ は零点をもたない。すなわち、 $f(x)$ は 0 でない定数である。

1-ノルムの場合、 $K = \mathbb{R}$ で $1 < M < 2$ の場合にはあまりよい見積りとなっていない。これは $\phi_{j,k}(\beta)$ の見積りがありよくできていないからである。

4.2 実係数多項式についての任意の実数のまわりの穴の解析

本節では $K = \mathbb{R}$ のとき任意の実数 α のまわりの穴を $|f(\alpha)|/\|f\|$ が十分に小さいという仮定のもとで解析する。この場合、系 1 より α のまわりの穴は α の近傍に存在する。ここで、 α は 0 でないと仮定する。

まず、定義より、

$$P^{\text{vec}}(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{R}^{n+1} \mid \sum_{i=0}^n b_i \beta^i = 0, \sum_{i=0}^n |b_i| \leq 1 \right\}$$

とかける。これを用いて穴の実軸の部分は

$$H_{\alpha, f} \cap \mathbb{R} = \left\{ \beta \in \mathbb{R} \mid \phi_{\alpha}(\beta) < \frac{|f(\alpha)|}{\|f\|} \right\}$$

とかける。ただし、

$$\phi_{\alpha}(\beta) = \max \left\{ \left| \sum_{i=0}^n b_i \alpha^i \right| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

とする。ここで $\phi_{\alpha}(\beta)$ を解析する。前節と同様にして、 $\phi_{\alpha}(\beta) \in \mathbb{R}^{n+1}$ の値は多面体 $P^{\text{vec}}(\beta)$ の頂点で達成される。前節と同様にして b_0, \dots, b_n のうち高々 2 つの要素が 0 でない。この要素の添字を j, k ($k > j$) とおく。このときこれらは方程式系

$$\begin{cases} |b_j| + |b_k| = 1, \\ \beta^j b_j + \beta^k b_k = 0 \end{cases}$$

を満たす。この方程式の解は

$$\begin{cases} b_k = \pm 1/(1 + |\beta|^{k-j}) \\ b_j = \mp \beta^{k-j}/(1 + |\beta|^{k-j}) \end{cases}$$

である。ここで複号は同順であるものとする。このとき、

$$\left| \sum_{i=0}^n b_i \alpha^i \right| = \frac{|\alpha^k - \beta^{k-j} \alpha^j|}{1 + |\beta|^{k-j}}$$

である。ただし、 $\beta = \alpha + \varepsilon$ とおく。ここで、系 1 より ε は十分小さな実数であると仮定して良い。このとき、

$$\left| \sum_{i=0}^n b_i \alpha^i \right| = \frac{|\alpha|^{k-1}}{1 + |\alpha|^{k-j}} (k-j) |\varepsilon| + o(\varepsilon)$$

とかける。よって、 $\phi_{\alpha}(\beta)$ はつぎのようにかける：

$$\left[\max_{1 \leq j < k \leq n} \frac{|\alpha|^{k-1}}{1 + |\alpha|^{k-j}} (k-j) \right] |\varepsilon| + o(\varepsilon).$$

よって, $H_{\alpha,f} \cap \mathbb{R}$ は $|f(\alpha)|/\|f\|$ が十分に小さいとき漸近的に

$$H_{\alpha,f} \cap \mathbb{R} \approx \left\{ \beta \in \mathbb{R} \mid |\beta - \alpha| < \left(\max_{0 \leq j < k \leq n} \frac{|\alpha|^k}{1 + |\alpha|^k} (k - j) \right)^{-1} \frac{|f(\alpha)|}{\|f\|} \right\}$$

とかける.

つぎに $H_{\alpha,f} \setminus \mathbb{R}$ について考える. まず, 定義より,

$$H_{\alpha,f} \setminus \mathbb{R} = \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \phi_{\alpha}(\beta) < \frac{|f(\alpha)|}{\|f\|} \right\}$$

である. ただし,

$$\phi_{\alpha}(\beta) = \max \left\{ \left| \sum_{i=0}^n b_i \alpha^i \right| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

とする. ここで, β は実数でない複素数である. 前節と同様にしてこの場合, $\phi(\beta)$ の値は $P^{\text{vec}}(\beta)$ の頂点で達成される. また, その頂点は $n+1$ 個の座標の要素 b_0, \dots, b_n のなかで高々3つのものが0でない, この0でない要素を b_i, b_j, b_k , ($0 \leq i < j < k \leq n$) とおけば, つぎの方程式系になりたつ:

$$\begin{cases} |b_i| + |b_j| + |b_k| = 1, \\ \text{Re} \beta^i b_i + \text{Re} \beta^j b_j + \text{Re} \beta^k b_k = 0, \\ \text{Im} \beta^i b_i + \text{Im} \beta^j b_j + \text{Im} \beta^k b_k = 0. \end{cases}$$

ここで β は α に十分近いことからこの方程式系は縮退せず, 高々有限個の解をもつ. $(l_1, l_2) \in \{i, j, k\} \times \{i, j, k\}$ について

$$E(\beta, l_1, l_2) = \text{Re} \beta^{l_1} \text{Im} \beta^{l_2} - \text{Im} \beta^{l_1} \text{Re} \beta^{l_2}$$

とおけば, この方程式系の解はつぎようになる.

$$\begin{aligned} |b_i| &= \frac{|E(\beta, j, k)|}{|E(\beta, j, k)| + |E(\beta, i, k)| + |E(\beta, j, i)|}, \\ \begin{pmatrix} b_j \\ b_k \end{pmatrix} &= \frac{-b_i}{E(\beta, j, k)} \begin{pmatrix} E(\beta, i, k) \\ E(\beta, j, i) \end{pmatrix}. \end{aligned}$$

よって, この解をもちいることにより,

$$\begin{aligned} \left| \sum_{i=0}^n b_i \alpha^i \right| &= |\alpha^i b_i + \alpha^j b_j + \alpha^k b_k| \\ &= \frac{|\alpha^i E(\beta, j, k) + \alpha^j E(\beta, k, i) + \alpha^k E(\beta, i, j)|}{|E(\beta, k, i)| + |E(\beta, i, j)| + |E(\beta, j, k)|} \end{aligned}$$

を得る。ここで $\beta = \alpha + \varepsilon$ とおけば、系 1 を用いて ε は絶対値が十分に小さな実数でない複素数であると仮定して良い。このとき、

$$\begin{aligned}\beta^l &= \alpha^l \left(1 + \frac{\varepsilon}{\alpha}\right)^l \\ &= \alpha \left[1 + \frac{\varepsilon}{\alpha} + \frac{l(l-1)}{2} \left(\frac{\varepsilon}{\alpha}\right)^2 + \frac{l(l-1)(l-2)}{6} \left(\frac{\varepsilon}{\alpha}\right)^3\right] + o(\varepsilon^3)\end{aligned}$$

である。ここで $(\operatorname{Re}\varepsilon)^s, (\operatorname{Im}\varepsilon)^s$ をそれぞれ $\operatorname{Re}^s\varepsilon, \operatorname{Im}^s\varepsilon$ と記せば、

$$\begin{aligned}\operatorname{Re}\beta^{l_1}\beta^{l_2} &= \alpha^{l_1+l_2} \left(1 + \frac{l_1}{\alpha}\operatorname{Re}\varepsilon + \frac{l_1(l_1-1)}{2\alpha^2}\operatorname{Re}\varepsilon^2 + o(\varepsilon^2)\right) \times \\ &\quad \left(\frac{l_2}{\alpha}\operatorname{Im}\varepsilon + \frac{l_2(l_2-1)}{2\alpha^2}\operatorname{Im}\varepsilon^2 + \frac{l_2(l_2-1)(l_2-2)}{6\alpha^3}\operatorname{Im}\varepsilon^3 + o(\varepsilon^3)\right) \\ &= \alpha^{l_1+l_2}\operatorname{Im}\varepsilon \left(1 + \frac{l_1}{\alpha}\operatorname{Re}\varepsilon + \frac{l_1(l_1-1)}{2\alpha^2}\operatorname{Re}\varepsilon^2 + o(\varepsilon^2)\right) \times \\ &\quad \left(\frac{l_2}{\alpha} + \frac{l_2(l_2-1)}{\alpha^2}\operatorname{Re}\varepsilon + \frac{l_2(l_2-1)(l_2-2)}{6\alpha^3}(3\operatorname{Re}^2\varepsilon - \operatorname{Im}^2\varepsilon) + o(\varepsilon^3)\right) \\ &= \alpha^{l_1+l_2}\operatorname{Im}\varepsilon \cdot l_2 \left(1 + \frac{l_1}{\alpha}\operatorname{Re}\varepsilon + \frac{l_1(l_1-1)}{2\alpha^2}\operatorname{Re}\varepsilon^2 + o(\varepsilon^2)\right) \times \\ &\quad \left(\frac{1}{\alpha} + \frac{(l_2-1)}{\alpha^2}\operatorname{Re}\varepsilon + \frac{(l_2-1)(l_2-2)}{6\alpha^3}(3\operatorname{Re}^2\varepsilon - \operatorname{Im}^2\varepsilon) + o(\varepsilon^3)\right) \\ &= \alpha^{l_1+l_2-1}\operatorname{Im}\varepsilon l_2 \left(1 + \frac{l_1+l_2-1}{\alpha}\operatorname{Re}\varepsilon + \frac{1}{6\alpha^2}[3(l_1+l_2-1)(l_1+l_2-2)\operatorname{Re}^2\varepsilon + \right. \\ &\quad \left.(-l_2^2+3l_2-2-3l_1^2+3l_1)\operatorname{Im}^2\varepsilon] + o(\varepsilon^2)\right)\end{aligned}$$

である。よって、これより

$$\begin{aligned}E(\beta, l_1, l_2) &= \operatorname{Re}\beta^{l_1}\operatorname{Im}\beta^{l_2} - \operatorname{Im}\beta^{l_1}\operatorname{Re}\beta^{l_2} \\ &= \alpha^{l_1+l_2-1}\operatorname{Im}\varepsilon(l_2-l_1) \left[1 + \frac{l_1+l_2-1}{\alpha}\operatorname{Re}\varepsilon + \frac{1}{6\alpha^2}(2(l_1+l_2-1) \cdot \right. \\ &\quad \left. (l_1+l_2-2))\operatorname{Re}^2\varepsilon - ((l_1-l_2)^2 - 3(l_1+l_2)+2) \cdot \operatorname{Im}^2\varepsilon + o(\varepsilon^2)\right].\end{aligned}$$

以上より、

$$\begin{aligned}\left|\sum_{i=0}^n b_i \alpha^i\right| &= \frac{|\alpha|^{i+j+k-3}|jk^2+ki^2+ij^2-kj^2-ik^2-ji^2|}{2[|\alpha|^{i+k-1}|k-i|+|\alpha|^{i+j-1}|i-j|+|\alpha|^{j+k-1}|j-k|]} \times \\ &\quad (\operatorname{Re}^2\varepsilon + \operatorname{Im}\varepsilon + o(\varepsilon^2))\end{aligned}$$

となる。この結果より、

$$H_{\alpha,f} \setminus \mathbb{R} \approx \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\alpha - \beta| < \left(\max_{0 \leq i < j < k \leq n} \Gamma_{i,j,k}(\alpha) \frac{\|f\|}{|f(\alpha)|} \right)^{-1/2} \right\}$$

となる。ただし、

$$\Gamma_{i,j,k}(\alpha) = \frac{|\alpha|^{i+j+k-3} |jk^2 + ki^2 + ij^2 - kj^2 - ik^2 - ji^2|}{2[|\alpha|^{i+k-1} |k-i| + |\alpha|^{i+j-1} |i-j| + |\alpha|^{j+k-1} |j-k|]}$$

とする。以上より $|f(\alpha)|/\|f\|$ が十分に小さいとき、 $H_{\alpha,f}$ の実数でない部分は漸近的に円盤である。本節の結果をまとめて次の定理を得る。

定理 7 $f(x)$ を実数体上の n 次多項式であるとする。また、 $M = \|f\|/|f(\alpha)|$ とおく。 M が十分に大きいとき実数 α のまわりの穴は漸近的につぎの領域に等しい：

$$H_{\alpha,f} \approx \left\{ \beta \in \mathbb{R} \mid |\alpha - \beta| < c_1(n, \alpha)/M \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\alpha - \beta| < c_2(n, \alpha)/\sqrt{M} \right\}. \quad (4.11)$$

ただし、 $c_1(n, \alpha)$ と $c_2(n, \alpha)$ は n と α のみに依存する定数であるとする。

α を固定して次数を大きくした場合、 $\alpha \neq 0$ ならば $\max_{0 \leq i < j < k \leq n} \Gamma_{i,j,k}$ は $O(n^2 |\alpha|^{2n-5})$ となるので穴はどんどん小さくなる。したがって、次数の制限されていない多項式の零点の穴は空集合となってしまう。

4.3 複素係数多項式についての任意の複素数のまわりの穴の解析

前節では、 $K = \mathbb{R}$ の場合の任意の実数のまわりの穴の漸近的性質を調べたが、本節では、 $K = \mathbb{C}$ のときの任意の複素数のまわりの穴の漸近的性質について調べる。この場合 b_0, \dots, b_n が実数とはならないので前節のように多面体の頂点で最大値をとるとは限らなくなる。

まず、補助定理 3 より $\alpha \in \mathbb{R}$ と仮定してよい。すなわち適当な絶対値 1 の複素数をかけることにより α を実数とすることができる。ここでまず、仮定としてこの α はつぎのような条件を満たしていると仮定する：

条件 1 任意の絶対値 1 の複素数 μ_1, μ_2 と任意の整数 i_1, i_2, i_3 で $0 \leq i_1 < i_2 < i_3 \leq n$ を満たすものに対して三つの複素ベクトル

$$\begin{aligned} & (1, \mu_1, \mu_2), \\ & (\alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}), \\ & (i_1 \alpha^{i_1}, i_2 \alpha^{i_2}, i_3 \alpha^{i_3}) \end{aligned}$$

は線形独立である.

本節の後半でこのような条件を満たすための十分条件を与える. この仮定のもとで, この場合の穴の漸近的な性質を調べる. 定義より

$$P(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{C}^n \mid \sum_{i=0}^n b_i \beta^i = 0, \sum_{i=0}^n |b_i| \leq 1 \right\}$$

である. これを用いて α のまわりの穴は

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \phi_\alpha(\beta) < \frac{|f(\alpha)|}{\|f\|} \right\}$$

である. ただし,

$$\phi_\alpha(\beta) = \max \left\{ \left| \sum_{i=0}^n b_i \alpha^i \right| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

とする. 系 1 より $H_{\alpha, f}$ は α の近傍であると考えて良い. ここで $\beta \in \mathbb{C}$ を $|\beta - \alpha|$ が十分に小さな数でかつ $\beta \neq \alpha$ であるとする.

補助定理 13 実数 α が条件 1 をみたすとき, $(d_0, d_1, \dots, d_n) \in P^{\text{vec}}(\beta)$ にたいして $|\sum_{i=0}^n d_i \alpha^i| = \phi_\alpha(\beta)$ かつ $\sum_{i=0}^n |d_i| = 1$ ならば d_0, \dots, d_n のうち高々 2 個の要素が 0 でない.

証明 3 つの要素が 0 でないと仮定して矛盾を導く. この 3 つの要素を $d_{i_1}, d_{i_2}, d_{i_3}$ とおく. ただし, $(0 \leq i_1 < i_2 < i_3 \leq n)$ であるとする. ここで $\delta_1, \delta_2, \delta_3$ を絶対値の小さな複素数として, ベクトル (d'_0, \dots, d'_n) をつぎのように定義する:

$$\begin{aligned} d'_{i_1} &= d_{i_1} + \delta_1, \\ d'_{i_2} &= d_{i_2} + \delta_2, \\ d'_{i_3} &= d_{i_3} + \delta_3, \\ d'_i &= d_i \quad (i \neq i_1, i_2, i_3). \end{aligned}$$

このとき, $\delta_1, \delta_2, \delta_3$ が次の条件を満足するとする.

$$\sum_{j=1}^3 \operatorname{Re} \delta_j \operatorname{Im} \beta^{i_j} + \operatorname{Im} \delta_j \operatorname{Re} \beta^{i_j} = 0, \quad (4.12)$$

$$\sum_{j=1}^3 \operatorname{Re} \delta_j \operatorname{Re} \beta^{i_j} - \operatorname{Im} \delta_j \operatorname{Im} \beta^{i_j} = 0, \quad (4.13)$$

$$\sum_{j=1}^3 \frac{\operatorname{Re} d_{i_j} \operatorname{Re} \delta_j + \operatorname{Im} d_{i_j} \operatorname{Im} \delta_j}{|d_{i_k}|} = 0. \quad (4.14)$$

この条件と条件

$$\sum_{j=1}^3 \operatorname{Im} \delta_j \alpha^{i_j} = 0, \quad (4.15)$$

$$\sum_{j=1}^3 \operatorname{Re} \delta_j \alpha^{i_j} \neq 0 \quad (4.16)$$

を満足する $\delta_1, \delta_2, \delta_3$ は存在する。なぜならば、このような δ_i が存在しないと仮定すると、つぎの式を満足する実数 $\gamma, \delta, \mu, \eta$ が存在する：

$$\gamma a + \delta b + \mu c + \eta d = r. \quad (4.17)$$

ただし、

$$\begin{aligned} a &= (\operatorname{Im} \beta^{i_1}, \operatorname{Re} \beta^{i_1}, \operatorname{Im} \beta^{i_2}, \operatorname{Re} \beta^{i_2}, \operatorname{Im} \beta^{i_3}, \operatorname{Re} \beta^{i_3}), \\ b &= (\operatorname{Re} \beta^{i_1}, -\operatorname{Im} \beta^{i_1}, \operatorname{Re} \beta^{i_2}, -\operatorname{Im} \beta^{i_2}, \operatorname{Re} \beta^{i_3}, -\operatorname{Im} \beta^{i_3}), \\ c &= \left(\frac{\operatorname{Re} d_{i_1}}{|d_{i_1}|}, \frac{\operatorname{Im} d_{i_1}}{|d_{i_1}|}, \frac{\operatorname{Re} d_{i_2}}{|d_{i_2}|}, \frac{\operatorname{Im} d_{i_2}}{|d_{i_2}|}, \frac{\operatorname{Re} d_{i_3}}{|d_{i_3}|}, \frac{\operatorname{Im} d_{i_3}}{|d_{i_3}|} \right), \\ d &= (0, \alpha^{i_1}, 0, \alpha^{i_2}, 0, \alpha^{i_3}), \\ r &= (\alpha^{i_1}, 0, \alpha^{i_2}, 0, \alpha^{i_3}, 0) \end{aligned}$$

とする。ここで式 (4.17) は $\gamma + i\delta$ と $i\mu$ をそれぞれ ω, ξ とかけば、

$$\begin{aligned} & \left(\operatorname{Im} \left(\omega \beta^{i_1} + \xi \frac{\overline{d_{i_1}}}{|d_{i_1}|} \right), \operatorname{Re} \left(\omega \beta^{i_1} + \xi \frac{\overline{d_{i_1}}}{|d_{i_1}|} + \eta \alpha^{i_1} \right), \operatorname{Im} \left(\omega \beta^{i_2} + \xi \frac{\overline{d_{i_2}}}{|d_{i_2}|} \right), \right. \\ & \left. \operatorname{Re} \left(\omega \beta^{i_2} + \xi \frac{\overline{d_{i_2}}}{|d_{i_2}|} + \eta \alpha^{i_2} \right), \operatorname{Im} \left(\omega \beta^{i_3} + \xi \frac{\overline{d_{i_3}}}{|d_{i_3}|} \right), \operatorname{Re} \left(\omega \beta^{i_3} + \xi \frac{\overline{d_{i_3}}}{|d_{i_3}|} + \eta \alpha^{i_3} \right) \right) \\ &= (\alpha^{i_1}, 0, \alpha^{i_2}, 0, \alpha^{i_3}, 0) \end{aligned}$$

となる。すなわち、

$$\begin{aligned} \omega \beta^{i_1} + \xi \frac{\overline{d_{i_1}}}{|d_{i_1}|} &= (i + \eta) \alpha^{i_1}, \\ \omega \beta^{i_2} + \xi \frac{\overline{d_{i_2}}}{|d_{i_2}|} &= (i + \eta) \alpha^{i_2}, \\ \omega \beta^{i_3} + \xi \frac{\overline{d_{i_3}}}{|d_{i_3}|} &= (i + \eta) \alpha^{i_3} \end{aligned}$$

が成り立つ。しかし、仮定より、三つのベクトル

$$\begin{aligned} (\beta^{i_1}, \beta^{i_2}, \beta^{i_3}) &\approx (\alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}) + \frac{\varepsilon}{\alpha} (i_1 \alpha^{i_1}, i_2 \alpha^{i_2}, i_3 \alpha^{i_3}), \\ &(\alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}), \\ &\left(\frac{\overline{d_{i_1}}}{|d_{i_1}|}, \frac{\overline{d_{i_2}}}{|d_{i_2}|}, \frac{\overline{d_{i_3}}}{|d_{i_3}|} \right) \end{aligned}$$

は一次独立である。 $\sum_{i=0}^n d_i \alpha^i$ が純虚数でなければ、従って、このような複素数 $\delta_1, \delta_2, \delta_3$ を選択することができる。

$$\left| \sum_{i=0}^n d_i \alpha^i + \sum_{j=1}^3 \operatorname{Re} \delta_j \alpha^{i_j} + i \sum_{j=1}^3 \operatorname{Im} \delta_j \alpha^{i_j} \right|$$

を $|\sum_{i=0}^n d_i \alpha^i|$ よりも大きくすることができる。また $\sum_{i=0}^n d_i \alpha^i$ が純虚数の場合、うまく $\delta_1, \delta_2, \delta_3$ を選択して $\sum_{i=0}^n \operatorname{Re} \delta_j \alpha^{i_j} = 0$ か $\sum_{i=0}^n \operatorname{Im} \delta_j \alpha^{i_j} \neq 0$ とすることができる。この結果は (d_0, \dots, d_n) で $\phi_\alpha(\beta)$ が最大値をとるという仮定に反している。すなわち、最大値を改善することができる。これは矛盾である。以上より d_0, \dots, d_n のうち高々二つの要素が 0 でない。
□

この定理より、最大値を与えるベクトル (d_0, \dots, d_n) の要素のうち 0 でないものが、 d_j と d_k であると仮定する。このとき、つぎの方程式が成り立っている。

$$\begin{cases} |d_j| + |d_k| = 1, \\ \beta^j d_j + \beta^k d_k = 0. \end{cases}$$

これを解いて、

$$\begin{cases} d_k = 1/(1 + |\beta|^{k-j}) \cdot e^{i\theta}, \\ d_j = -\beta^{k-j}/(1 + |\beta|^{k-j}) \cdot e^{i\theta} \end{cases}$$

となる。ただし、 θ は $0 \leq \theta < 2\pi$ となる実数である。これより、

$$\phi_{\alpha, j, k}(\beta) = |d_j \alpha^j + d_k \alpha^k| = \frac{|\alpha^k - \beta^{k-j} \alpha^j|}{1 + |\beta|^{k-j}} = \frac{|\alpha|^{k-1}}{1 + |\alpha|^{k-j}} (k-j)|\varepsilon| + o(|\varepsilon|)$$

を得る。よって、

$$\phi_\alpha(\beta) = \left[\max_{0 \leq j < k \leq n} \frac{|\alpha|^{k-1}}{1 + |\alpha|^{k-j}} (k-j) \right] |\varepsilon| + o(|\varepsilon|)$$

である。以上より十分に $|f(\alpha)|/\|f\|$ が小さいとき $H_{\alpha, f}$ は漸近的につぎのような集合となる：

$$H_{\alpha, f} \approx \left\{ \beta \in \mathbb{C} \mid |\beta - \alpha| < \left(\max_{0 \leq j < k \leq n} \frac{|\alpha|^{k-1}}{1 + |\alpha|^{k-j}} (k-j) \right)^{-1} \frac{|f(\alpha)|}{\|f\|} \right\}.$$

以上より、つぎの補助定理を得る。

補助定理 14 $f(x)$ が複素数体上の n 次多項式で $M = \|f\|/|f(0)|$ とおく。 M が十分に多きいと仮定する。また α をある複素数で条件 1 を満足するとする。このとき $f(x)$ の零点の α のまわりの穴は漸近的につぎのようになる。

$$H_{\alpha, f} \approx \left\{ \beta \in \mathbb{C} \mid |\beta - \alpha| < c_3(n, \alpha)/M \right\}.$$

ただし、 $c_3(n, \alpha)$ は n と α に依存する定数である。

本節の最後に、条件1が成り立つための十分条件を求める。

補助定理 15 n を多項式の次数とする。 α がつぎの条件を満たすとき、条件1が成り立つ：

$$|\alpha| \geq \frac{\sqrt{2}+1}{2}n \quad (4.18)$$

または、

$$|\alpha| \leq \frac{2}{(\sqrt{2}+1)n}. \quad (4.19)$$

証明 三つのベクトル $(1, \mu_1, \mu_2)$, $(\alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3})$, $(i_1\alpha_1^i, i_2\alpha_2^i, i_3\alpha_3^i)$ が一次独立であるための必要十分条件はこの三つのベクトルから作られる行列の行列式

$$D = (i_3 - i_2)\alpha^{i_2+i_3} + \mu_1(i_2 - i_3)\alpha^{i_1+i_3} + \mu_2(i_2 - i_1)\alpha^{i_2+i_1}$$

が0でないことである。ここで $|\alpha| > (\sqrt{2}+1)n/2$ であると仮定すると、

$$\begin{aligned} & \left| \frac{i_1 - i_3}{i_3 - i_2} \mu_1 \alpha^{i_1-i_2} + \frac{i_2 - i_1}{i_3 - i_2} \mu_2 \alpha^{i_1-i_3} \right| \\ & \leq \frac{i_3 - i_1}{i_3 - i_2} |\alpha|^{i_1-i_2} + \frac{i_2 - i_1}{i_3 - i_2} |\alpha|^{i_1-i_3} \\ & \leq n |\alpha|^{i_1-i_2} + (n-1) |\alpha|^{i_1-i_3} \\ & \leq \frac{n}{|\alpha|} + \frac{n-1}{|\alpha|^2} \\ & < \frac{2}{\sqrt{2}+1} + \left(\frac{2}{\sqrt{2}+1} \right)^2 \frac{n-1}{n^2} \\ & \leq \frac{2}{\sqrt{2}+1} + \left(\frac{2}{\sqrt{2}+1} \right)^2 \frac{1}{4} = 1 \end{aligned}$$

となる。この不等式より

$$\left| (i_1 - i_3) \mu_1 \alpha^{i_1+i_3} + (i_2 - i_1) \mu_2 \alpha^{i_1+i_2} \right| < \left| (i_3 - i_2) \alpha^{i_2+i_3} \right|$$

となり、これより $D \neq 0$ である。また一方、 $|\alpha| < 2/((\sqrt{2}+1)n)$ と仮定すれば、同様に

$$\begin{aligned} & \left| \frac{1}{\mu_2} \frac{i_3 - i_2}{i_2 - i_1} \alpha^{i_3-i_1} + \frac{\mu_1}{\mu_2} \frac{i_1 - i_2}{i_2 - i_1} \alpha^{i_3-i_2} \right| \\ & \leq \frac{i_3 - i_2}{i_2 - i_1} |\alpha|^{i_3-i_1} + \frac{i_3 - i_1}{i_2 - i_1} |\alpha|^{i_3-i_2} \\ & \leq \frac{i_3 - i_2}{i_2 - i_1} |\alpha|^2 + \frac{i_3 - i_1}{i_2 - i_1} |\alpha| \\ & \leq (n-1) |\alpha|^2 + n |\alpha| \\ & < (n-1) \left(\frac{2}{(\sqrt{2}+1)n} \right)^2 + n \frac{2}{(\sqrt{2}+1)n} \leq 1 \end{aligned}$$

となり、やはり $D \neq 0$ である。以上より本補助定理は証明された。

□

この補助定理と補助定理 14 よりつぎの定理を得る。

定理 8 $f(x)$ を複素数体上の n 次多項式であるとする。また $M = \|f\|_1/|f(0)|$ とおく。 M が十分に大きいと仮定する。このとき、 $|\alpha| \geq (\sqrt{2}+1)n/2$ または $|\alpha| \leq 2/((\sqrt{2}+1)n)$ であると仮定すると、 $f(x)$ の α のまわりの穴は漸近的につぎのようになる。

$$H_{\alpha, f} \approx \left\{ \beta \in \mathbb{C} \mid |\beta - \alpha| < c_3(n, \alpha)/M \right\}. \quad (4.20)$$

ただし、 $c_3(n, \alpha)$ は n と α に依存する定数である。

第 5 章

∞ -ノルムに関する 0 のまわりの穴についての結果

本章では、 ∞ -ノルムによる 0 のまわりの穴について論じる。 ∞ -ノルムの場合の解析は非常に難しい。前の二つの章と同様にして 0 のまわりの穴の部分領域で円であるものを求めるが、それはあまりよい限界とはなっていない。本章では $\|\cdot\|$ は $\|\cdot\|_\infty$ を表すものとする。

まず、 $K = \mathbb{C}$ の場合について考える。この場合、0 のまわりの穴は

$$H_{0,f} = \left\{ \beta \in \mathbb{C} \mid \phi(\beta) < \frac{|f(0)|}{\|f\|} \right\}$$

とかける。ただし、

$$\phi(\beta) = \max \left\{ |b_0| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

であり、

$$P^{\text{vec}}(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{C}^{n+1} \mid \max_{i=0, \dots, n} |b_i| \leq 1, \sum_{i=0}^n b_i \beta^i = 0 \right\}$$

である。ここで $\phi(\beta)$ を解析する。まず $|\beta| < 1$ の場合は、 $\phi(\beta) = |b_0|$ となる $(b_0, \dots, b_n) \in P^{\text{vec}}(\beta)$ に対して

$$\phi(\beta) = \left| \sum_{i=1}^n b_i \beta^i \right| \leq \sum_{i=1}^n |b_i| |\beta|^i \leq \sum_{i=1}^n 1 = n = \frac{1 - |\beta|^{n+1}}{1 - |\beta|} \cdot |\beta| < \frac{|\beta|}{1 - |\beta|}.$$

この結果と $|f(0)|/\|f\|$ が 1 を越えないということからつぎのことがわかる：

$$H_{0,f} \supset \left\{ \beta \in \mathbb{C} \mid \frac{|\beta|}{1 - |\beta|} \leq \frac{|f(0)|}{\|f\|} \right\} = \left\{ \beta \in \mathbb{C} \mid |\beta| \leq \left(\frac{\|f\|}{|f(0)|} + 1 \right)^{-1} \right\}.$$

また、つぎに $K = \mathbb{R}$ の場合について考える。前と同様にして、

$$H_{0,f} = \left\{ \beta \in \mathbb{C} \mid \phi(\beta) < \frac{|f(0)|}{\|f\|} \right\}$$

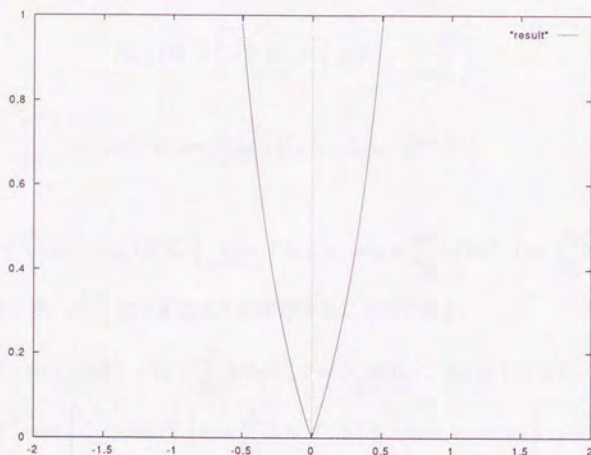


Fig. 5.1. $n = 5$, $K = \mathbb{R}$, $\beta \in \mathbb{R}$ のときの $\phi(\beta)$ の形

とかける。ただし,

$$\phi(\beta) = \max \left\{ |b_0| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

かつ,

$$P^{\text{vec}}(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{R}^{n+1} \mid \max_{i=0, \dots, n} |b_i| \leq 1, \sum_{i=0}^n b_i \beta^i = 0 \right\}$$

である。この場合の $\phi(\beta)$ のグラフを Fig. 5.1 に示す。 $H_{0,f} \cap \mathbb{R}$ については

$$H_{0,f} \cap \mathbb{R} = \left\{ \beta \in \mathbb{R} \mid \phi(\beta) < \frac{|f(0)|}{\|f\|} \right\}$$

とかける。ここで $|\beta| < 1$ のとき, $\phi(\beta) = |b_0|$ なる $(b_0, \dots, b_n) \in P^{\text{vec}}(\beta)$ に対して,

$$\phi(\beta) = \left| \sum_{i=1}^n b_i \beta^i \right| \leq \sum_{i=1}^n |\beta|^i = \frac{1 - |\beta|^{n+1}}{1 - |\beta|} |\beta| < \frac{|\beta|}{1 - |\beta|}$$

が成り立つ。よって,

$$H_{0,f} \cap \mathbb{R} \subset \left\{ \beta \in \mathbb{R} \mid |\beta| < 1, \frac{|\beta|}{1 - |\beta|} < \frac{|f(0)|}{\|f\|} \right\} = \left\{ \beta \in \mathbb{R} \mid |\beta| \leq \left(\frac{\|f\|}{|f(0)|} + 1 \right)^{-1} \right\}$$

である。この結果は Cauchy の不等式そのものである。

また、つぎに、 $H_{0,f} \setminus \mathbb{R}$ を解析する。定義より、

$$H_{0,f} \setminus \mathbb{R} = \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \phi(\beta) < \frac{|f(0)|}{\|f\|} \right\}$$

とかける。ただし、

$$\phi(\beta) = \max \left\{ |b_0| \mid (b_0, \dots, b_n) \in P^{\text{vec}}(\beta) \right\}$$

かつ、

$$P^{\text{vec}}(\beta) = \left\{ (b_0, \dots, b_n) \in \mathbb{R}^n \mid \max_{i=0, \dots, n} |b_i| \leq 1, -b_0 = \sum_{i=1}^n b_i \operatorname{Re} \beta^i, 0 = \sum_{i=0}^n b_i \operatorname{Im} \beta^i \right\}$$

とする。このとき、 $\phi(\beta)$ はつぎのように変形することができる。

$$\begin{aligned} \phi(\beta) &= \max \left\{ |b_0| \mid -b_0 = \sum_{i=1}^n b_i \operatorname{Re} \beta^i, 0 = \sum_{i=1}^n b_i \operatorname{Im} \beta^i, |b_i| \leq 1 \ (i = 0, \dots, n) \right\} \\ &\leq \max \left\{ \left| \sum_{i=1}^n b_i \operatorname{Re} \beta^i \right| \mid 0 = \sum_{i=1}^n b_i \operatorname{Im} \beta^i, |b_i| \leq 1 \ (i = 1, \dots, n) \right\} \\ &= \max \left\{ \left| \sum_{i=1}^n b_i r^i \cos i\theta \right| \mid \sum_{i=1}^n b_i r^i \sin i\theta = 0, |b_i| \leq 1, (i = 1, \dots, n) \right\} \\ &= \max \left\{ \left| \sum_{i=1}^n B_i \cos i\theta \right| \mid \sum_{i=1}^n B_i \sin i\theta = 0, |B_i| \leq r^i, (i = 1, \dots, n) \right\}. \end{aligned}$$

ただし、 $\beta = r e^{i\theta}$, ($0 < \theta \leq \pi/2$) かつ、 $B_i = b_i r^i$ とおいた。さらに、 $\sum_{i=1}^n B_i \cos i\theta$ はつぎのように変形できる。

$$\begin{aligned} \left| \sum_{i=1}^n B_i \cos i\theta \right| &= \left| B_1 \cos \theta + \sum_{i=2}^n B_i \cos i\theta \right| \\ &= \left| \left(-\sum_{i=2}^n \frac{\sin i\theta}{\sin \theta} B_i \right) \cos \theta + \sum_{i=2}^n B_i \cos i\theta \right| \\ &= \left| \sum_{i=2}^n B_i \left(\cos i\theta - \frac{\sin i\theta}{\sin \theta} \cos \theta \right) \right| \\ &= \left| \sum_{i=2}^n B_i \frac{\cos i\theta \sin \theta - \sin i\theta \cos \theta}{\sin \theta} \right| \\ &= \left| \sum_{i=2}^n B_i \frac{\sin(1-i)\theta}{\sin \theta} \right|. \end{aligned}$$

$\phi(\beta)$ は補助定理 11 を用いてつぎのように変形することができる。

$$\phi(\beta) = \max \left\{ \left| \sum_{i=2}^n \frac{\sin(i-1)\theta}{\sin \theta} B_i \right| \mid \sum_{i=1}^m B_i \sin i\theta = 0, |B_i| \leq r^i, (i = 1, \dots, n) \right\}$$

$$\begin{aligned}
&\leq \max \left\{ \left| \sum_{i=2}^n \frac{\sin(i-1)\theta}{\sin \theta} B_i \right| \mid |B_i| \leq r^i, (i=1, \dots, n) \right\} \\
&\leq \sum_{i=2}^n \left| \frac{\sin(i-1)\theta}{\sin \theta} \right| r^i \\
&< r^2 + 2r^3 + \dots + (n-1)r^n \\
&= r^2(1 + 2r + \dots + (n-1)r^{n-2}) \\
&= r^2 \frac{(1 - nr^{n-1})(1-r) + (r - r^n)}{(1-r)^2} \\
&= \left(\frac{r}{1-r} \right)^2 (1 - nr^{n-1} + nr^n - r^n) \\
&= \left(\frac{r}{1-r} \right)^2 (1 - r^{n-1}(n - (n-1)r)) \\
&< \left(\frac{r}{1-r} \right)^2.
\end{aligned}$$

すなわち, $|\beta| < 1$ のとき

$$\phi(\beta) < \left(\frac{|\beta|}{1-|\beta|} \right)^2$$

が成り立つ. これより

$$\begin{aligned}
H_{0,f} \setminus \mathbb{R} &\supset \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta| < 1, \left(\frac{|\beta|}{1-|\beta|} \right)^2 \leq \frac{|f(0)|}{\|f\|} \right\} \\
&= \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta| \leq \left[\left(\frac{\|f\|}{|f(0)|} \right)^{1/2} + 1 \right]^{-1} \right\}
\end{aligned}$$

を得る. 以上の結果をまとめると, つぎのようになる.

定理 9 $f(x)$ を実数体上の n 次多項式とする. このとき領域

$$\left\{ \beta \in \mathbb{R} \mid |\beta| \leq 1/(M+1) \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid |\beta| \leq 1/(\sqrt{M}+1) \right\} \quad (5.1)$$

に $f(x)$ の零点は存在しない. ただし, $M = \|f\|_\infty/|f(0)|$ であるとする. また, $f(x)$ が複素数体上の多項式であるとき, 領域

$$\left\{ \beta \in \mathbb{C} \mid |\beta| \leq 1/(M+1) \right\} \quad (5.2)$$

に $f(x)$ の零点は存在しない.

この定理は Mignotte の結果 [Mig92] と Cauchy [Cau91] の不等式を組み合わせたものにほぼ同等である. Mignotte の結果はつぎのとおりである.

定理 10 ([Mig92]) $f(x)$ を実数体上の n 次多項式であるとする. このとき実数でない $f(x)$ の零点 β の絶対値について, つぎの不等式が成り立つ:

$$|\beta| < \left(\frac{\|f\|_{\infty}}{|\text{lc } f|} \right)^{1/2} + 1. \quad (5.3)$$

また Cauchy の不等式はつぎのとおりである.

定理 11 ([Cau91]) $f(x)$ を複素数体上の多項式であるとする. このとき, 任意の $f(x)$ の零点 β の絶対値についてつぎの不等式がなりたつ.

$$|\beta| < \frac{\|f\|_{\infty}}{|\text{lc } f|} + 1. \quad (5.4)$$

この二つの定理を用いれば, 逆多項式を用いて容易に定理 9 を導くことができる.

∞ -ノルムについては 0 のまわりの穴は解析できるが, その他の一般的な数のまわりの穴について解析するのは大変難しい. $K = \mathbb{R}$ の場合には $n+1$ 個の束縛を持った線形計画問題となる. また, $K = \mathbb{C}$ の場合には非線形計画問題となる.

第 6 章

2-ノルムの抑えられた整係数多項式の零点の分布について

いままで第2章で定義した多項式の零点の存在しない領域、穴の形などを考察した。本章ではノルムの限定された整係数多項式の零点の分布を考える。ここでノルムとして用いるのは今まで扱ったなかでもっとも解析が容易である 2-ノルムである。

6.1 穴と整係数多項式の零点の分布との関係について

本節では今まで考察してきた穴と整係数多項式の零点の関係について考察する。まず対象となる零点の集合を定義する。

定義 6 $Z(M, n)$ は複素数の集合でつぎのように定義されるものである：

$$Z(M, n) = \left\{ \alpha \in \mathbb{C} \mid f(\alpha) = 0, f(x) \in P(M, n) \right\}. \quad (6.1)$$

ただし、 $P(M, n)$ は多項式の集合で

$$P(M, n) = \left\{ f(x) \in \mathbb{Z}[x] \mid \|f\| \leq M, \deg f \leq n, \right. \\ \left. f(x) \text{ は } \mathbb{Z} \text{ 上で既約な多項式である} \right\} \quad (6.2)$$

とする。また、 $Z(M, \infty)$ は

$$\bigcup_{n=0}^{\infty} Z(M, n) \quad (6.3)$$

を表すものとする。

また、穴については第2章で定義したものをを用いるが、一つの多項式についてではなく、いくつかのまとまった多項式について考えなければならないのでつぎのような記法を用いる。

定義 7 $H_\alpha(N)$ は複素数平面上の領域でつぎのように定義されるものである。ただし N はある非負実数であるとする。

$$H_\alpha(N) = \left\{ \beta \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(\alpha)| < N \right\}. \quad (6.4)$$

ただし,

$$P(\beta) = \left\{ h(x) \in K[x] \mid \deg h \leq n, h(\beta) = 0, \|h\| = 1 \right\} \quad (6.5)$$

とする。

穴とこの零点の集合にはつぎのような関係がある。

補助定理 16 任意の有理数 α について

$$Z(M, n) \cap H_\alpha \left(\frac{1}{M \text{Den}(\alpha)^n} \right) = \begin{cases} \{\alpha\} & \alpha \in Z(M, n) \\ \emptyset & \alpha \notin Z(M, n) \end{cases} \quad (6.6)$$

である。ただし, $\text{Den}(\alpha)$ は α の分母を表す。

証明 補助定理 1 より $P(M, n)$ のそれぞれの多項式 $f(x)$ に対して $H_{\alpha, f}$ を計算し, その共通集合をとれば, それは $Z(M, n)$ と共通部分を持たない。定義よりこの共通集合は

$$H_\alpha \left(\min_{f(x) \in P(M, n)} \frac{|f(\alpha)|}{\|f\|} \right)$$

とかける。ここで定義より $\|f\| \leq M$ であり, $\alpha = p/q$, $f(x) = \sum_{i=0}^n a_i x^i$ とおけば,

$$f(\alpha) = \sum_{i=0}^n a_i \left(\frac{p}{q} \right)^i = \frac{\sum_{i=0}^n a_i p^i q^{n-i}}{q^n}$$

とかける。 $f(x)$ は $qx - p$ である場合以外は \mathbb{Z} 上で既約で p/q を零点として持たないので, これより $|f(\alpha)| \geq 1/q^n$ である。以上より本補助定理を得る。□

多項式の集合 $P(M, n)$ の定義において $f(x)$ が既約であるということは補助定理 16 を成り立たせるためには必要ではない。実際「 $f(x)$ は一次式を因子としてもたない」程度で十分である。しかし, Lenstra [Len83] では既約な整係数を用いて議論を行なっている。ここでは既約であるという定義を採用した。また, 既約であるという条件も一次式を因子として持たないという条件も与えない場合, $(px - q)g(x)$ という形の多項式が $P(M, n)$ のなかに入るので一般には補助定理 16 は成り立たない。しかし, その場合も $h(x) = (px - q)g(x)$ とおけば,

$$\|h\| \geq \|g\|$$

が成り立てば, 補助定理 16 は成り立つ。つぎに, この関係がほとんどの p, q に対して成り立つことを示す。まず, 準備としてつぎの補助定理を示す。

補助定理 17 正の整数 p, q が互いに素であり, $p \neq q$ であるとき, 任意の実数係数の多項式 $g(x)$ に対して $h(x) = g(x)(px - q)$ とおけば,

$$\|g\|_2 \leq \|h\|_2 \quad (6.7)$$

が成り立つ.

証明 $g(x) = \sum_{i=0}^n g_i x^i$ とおく. このとき, 多項式をその係数を並べた縦ベクトルとすると $g(x)(px - q)$ はつぎのように表現できる:

$$\begin{pmatrix} -q & & & 0 \\ p & -q & & \\ & p & -q & \\ & & \ddots & \ddots \\ 0 & & & p & -q \\ & & & p & \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{n-1} \\ g_n \end{pmatrix}.$$

よって, $\|g(x)(px - q)\|_2$ はつぎのようにかける.

$$\|g(x)(px - q)\|_2 = (g_0, \dots, g_n) \begin{pmatrix} p^2 + q^2 & -pq & & 0 \\ -pq & p^2 + q^2 & -pq & \\ \ddots & \ddots & \ddots & \\ 0 & -pq & p^2 + q^2 & -pq \\ & -pq & p^2 + q^2 & \end{pmatrix} \begin{pmatrix} g_0 \\ \vdots \\ g_n \end{pmatrix}.$$

ここでこの式の $(n+1) \times (n+1)$ 行列の固有値について考える. この行列は三重対角行列であるのでその $n+1$ 個の固有値は

$$\lambda_i = p^2 + q^2 - 2pq \cos\left(\frac{i+1}{n+2}\pi\right), \quad (i = 0, \dots, n)$$

である. ここで $p \neq q$ であるので

$$\lambda_i = (p - q)^2 + 2pq \left(1 - \cos\left(\frac{i+1}{n+2}\pi\right)\right) > 1$$

である. □

ここで $Z(M, n)$ の定義を拡張する.

定義 8 多項式の集合 $P^{\text{ext}}(M, n)$ をつぎのように定義する:

$$P^{\text{ext}}(M, n) = \left\{ f(x) \in \mathbb{Z}[x] \mid \|f\| \leq M, \deg f \leq n \right\}. \quad (6.8)$$

このとき零点の集合 $Z^{\text{ext}}(M, n)$ をこれを用いてつぎのように定義する.

$$Z^{\text{ext}}(M, n) = \left\{ \alpha \in \mathbb{C} \mid f(\alpha) = 0, f(x) \in P^{\text{ext}}(M, n) \right\}. \quad (6.9)$$

このとき明らかに $Z^{\text{ext}}(M, n) \supset Z(M, n)$ である.

零点の集合 $P^{\text{ext}}(M, n)$ についてつぎのような性質が成り立つ.

補助定理 18 任意の有理数 $\alpha \neq 1$ について

$$Z^{\text{ext}}(M, n) \cap H_\alpha \left(\frac{1}{M \text{Den}(\alpha)^n} \right) = \begin{cases} \{\alpha\} & \alpha \in Z^{\text{ext}}(M, n) \\ \emptyset & \alpha \notin Z^{\text{ext}}(M, n) \end{cases} \quad (6.10)$$

である.

証明 $\alpha = p/q$ とおく. $P(M, n)$ のそれぞれの多項式 $f(x)$ についてもし $f(x)$ が $qx - p$ で割り切れなければ $f(\alpha) \neq 0$ であり, この場合, 補助定理 16 の証明と全く同様にして導くことができる. $f(x)$ が $qx - p$ で割り切れる場合,

$$f(x) = (qx - p)^k g(x)$$

とかくことができる. ただし, $g(x)$ は $qx - p$ を因子としてもたないとする. $f_i(x) = (qx - p)^i g(x)$ とおけば, ここで仮定より $\alpha \neq 1$ であるので補助定理 17 より,

$$\|f\| = \|f_k\| \geq \|f_{k-1}\| \geq \cdots \geq \|f_0\| = \|g\|$$

である. よって, $1/(\|g\| \text{Den}(\alpha)) \geq 1/(M \text{Den}(\alpha))$ である. よって,

$$H_\alpha \left(\frac{1}{\|g\| \text{Den}(\alpha)} \right) \supseteq H_\alpha \left(\frac{1}{M \text{Den}(\alpha)} \right)$$

であり, $g(x)$ の零点は $H_\alpha(1/(M \text{Den}(\alpha)))$ と共通部分を持たない. $f(x)$ の零点は $g(x)$ の零点と α であるので, 以上より本補助定理を得る. \square

この補助定理より, 1 でない有理数のまわりの穴には $Z(M, n)$ にも $Z^{\text{ext}}(M, n)$ に対しても適用できることがわかる.

6.2 零点の集合 $Z(M, \infty)$ による有理数の近似について

本節では, $Z(M, \infty)$ について考察する. 第 3 章の定理 2 および系 3 より, $Z(M, n)$ が次数によらずある領域に存在することがわかる. よって, $Z(M, \infty)$ もまた, 同じ領域に存在することが分かる.

系 4 $Z(M, \infty)$ はつぎの領域に存在する:

$$Z(M, \infty) \subset \left\{ \beta \in \mathbb{R} \mid \frac{1}{M} < |\beta| < M \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid \frac{1}{\sqrt{M}} < |\beta| < \sqrt{M} \right\} \cup \{0\}. \quad (6.11)$$

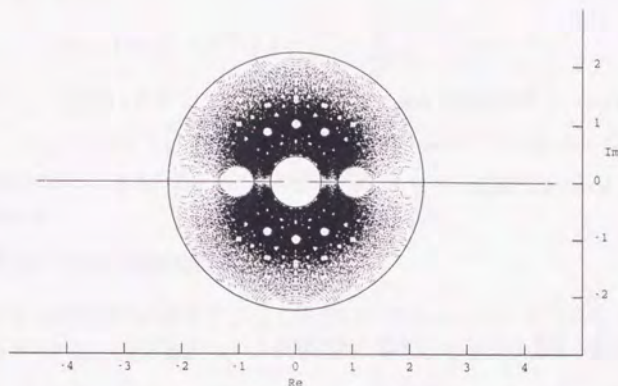


Fig. 6.1. $Z(5,5)$ の分布と系 4 による分布の限界

証明 任意の次数 n に対して集合 $Z(M, n)$ の定義より, その要素の多項式は, 整係数多項式であるから $|f(0)|$ は 0 であるか, または 1 以上である. $f(0) = 0$ である場合, $f(x) = g(x)x^k, g(0) \neq 0$ とかける. この場合 $|g(0)| \geq 1$ であり, かつ $\|g\| = \|f\|$ である. この事実と定理 2 および系 3 より, 系は証明される. \square

Fig. 6.1 に $Z(5,5)$ の分布と系 4 による限界を示す. この系は 0 のまわりの穴を考えているので補助定理 18 と全く同様の性質が $Z^{\text{ext}}(M, n)$ に対しても成り立つ. 証明は全く同様である.

つぎに $Z(M, \infty)$ の点を用いて収束列を構成できる点について考える. そのためにまずつぎの補助定理を示す.

補助定理 19 p を素数とする. また $g(x)$ を整数を係数とする多項式であるとする. このとき, つぎの多項式は整数環上で既約である.

1. $x^{2^m} + 1$ ($m = 0, 1, \dots$),
2. $f(x) = x^n + pg(x)x + p$ ($\deg g < n - 1$),
3. $f(x)(x^m - p) \pm p$ ($m > n$).

証明 Eisenstein の定理 [vdW37] を用いる. まず $r(x) = x^{2^m} + 1$ とおき $r(x+1)$ が既約であることを示す. ここで

$$r(x+1) = (x+1)^{2^m} + 1 = x^{2^m} + \sum_{i=1}^{2^m-1} \binom{2^m}{i} x^i + 2$$

である. $j = 1, \dots, 2^m - 1$ に対して, $2^m - j$ と j の 2 で割れる回数が等しいということより $i = 1, \dots, 2^m - 1$ に対して $\binom{2^m}{i}$ は 2 で割り切れる. よって, Eisenstein の定理より $r(x+1)$ は既約である. また, あとの二つの多項式については, 直接 Eisenstein の定理から既約性がわかる. \square

この性質を用いてつぎの補助定理を示す.

補助定理 20 α を複素数体上の多項式 $f(x)$ の零点であって $|\alpha| > 1$ であるとする. このとき $f(x)(x^m - p) \pm p = 0$ ($m \geq \deg f$) という多項式列の零点で α へ収束するものが存在する.

証明 まず, $|f(x)|$ と $|p/(x^m - p)|$ を α の近傍 $D_\varepsilon = \{\beta \in \mathbb{C} \mid |\alpha - \beta| < \varepsilon\}$ の上で比較する. m が十分に大きいとき ∂D_ε 上で

$$|f(x)| > \left| \frac{p}{(x^m - p)} \right|$$

である. よって, Rouché の定理より, 二つの方程式 $f(x) = 0$ と $f(x) - p/(x^m - p) = 0$ は D のなかで同数の零点をもつ. あきらかに $f(x) = 0$ は一つ以上の根を D の中にもつ. よって $f(x) - p/(x^m - p) = 0$ も D のなかに一つ以上の根をもつ. ここで ε はいくらでも小さく選択できる. よって α へ収束する点列をこの方程式の根で構成することができる. \square

つぎの二つの定理で $Z(M, \infty)$ のなかの点を使ってある数を近似することができることを示す.

定理 12 $M > \sqrt{2}$ かつ $|\alpha| = 1$ であるとする. このとき $Z(M, \infty) \setminus \{\alpha\}$ の点で α へ収束するものが存在する.

証明 補助定理 19 の 1 より, $x^{2^m} - 1$ は $Z(M, \infty)$ に含まれる. この多項式の零点は m を大きくしてゆくと, 単位円上にちゅう密に分布する. よって α へいくらでも近づくことができる. \square

定理 13 p を素数とする. また $M > p$.

$$\alpha \in Z\left(\frac{M-p}{1+p}, \infty\right) \quad (6.12)$$

であるとする。また、 $|\alpha| > 1$ かつ α の最小多項式が $x^m + pg(x)x \pm p$, ($g(x) \in \mathbb{Z}[x]$, $\deg g < n-1$) という形をしているとする。このとき $Z(M, \infty) \setminus \{\alpha\}$ のなかに α へ収束する列が存在する。

証明 $h(x) = f(x)(x^m - p) \pm p$ とおけば、ノルムの定義より $\|h\| \leq (1+p)\|f\| + p$ である。よって $f(x)$ が α を零点としてもつとすると、 $\|h\| \leq (1+p)\|f\| + p$ は補助定理 19 より既約であるので $P(M, \infty)$ に含まれる。また、補助定理 20 よりこの多項式の零点は m を大きくすると α へ収束するようにとれる。よって本命題が得られる。 \square

例 1 定理 13 において、 $p=2$, $n=3$, $g(x)=0$ とすると、 $Z(2+3\sqrt{5}, \infty) \setminus \{2+3\sqrt{5}\}$ は $2+3\sqrt{5}$ へ収束する列を含む。

定理 14 $\alpha \in \mathbb{Q} \setminus (Z(M, \infty) \setminus \{0\})$ であるとする。このとき $Z(M, \infty) \setminus \{\alpha\}$ のなかの列で α へ収束するものは存在しない。

証明 $\alpha = q/p \notin Z(M, \infty)$, ($p, q \in \mathbb{Z}$, $(p, q) = 1$) であると仮定する。また $0 < |\alpha| < 1$ であるとする。このとき、 α は一次式 $px - q$ の零点となっている。また、 $f(x) = \sum_{i=0}^n f_i x^i \in P(M, n)$ とする。任意の有理数体上の多項式 $g(x) = \sum_{i=0}^{n-1} g_i x^i$ ($g_i \in \mathbb{Q}$) に対して有理数 C と D をつぎのように定義する。

$$g(x)(px - q) + Cf(x) = D, \quad g(x) \in \mathbb{Q}[x], C, D \in \mathbb{Q}. \quad (6.13)$$

このときこれを行列表示でかけば

$$(C, g_0, g_1, \dots, g_{n-1}) \begin{pmatrix} f_0 & f_1 & \cdots & \cdots & f_n \\ -q & p & & & 0 \\ & -q & p & & \\ & & \ddots & \ddots & \\ 0 & & & -q & p \end{pmatrix} = (D, 0, \dots, 0)$$

とかける。この式の $(n+1) \times (n+1)$ 行列の行列式は $p^n f(q/p)$ である。ここで、 $D = p^n f(q/p)$ とおくと $C = p^n$ となり、クラメル公式より

$$\begin{aligned} |g_i| &= \begin{vmatrix} f_1 & \cdots & f_i & f_{i+1} & \cdots & f_n \\ p & 0 & & & & 0 \\ -q & p & 0 & & & \\ & \ddots & \ddots & \ddots & & \\ & & -q & p & 0 & \\ & & & 0 & -q & p \\ & & & & \ddots & \ddots & \ddots \\ 0 & & & & & 0 & -q & p \end{vmatrix} \\ &= \left| f_n (q/p)^i + \cdots + f_{i+1} \right| p^i, \quad (i = 0, \dots, n-1) \end{aligned}$$

よって、これより、 $|\alpha| < 1$ であるから、 $|g_i| \leq p^{n-1}(|f_n| + \cdots + |f_1|)$ である。ここで $Z(M, \infty)$ のなかに $\{\alpha_i\}$ が存在して α へ収束すると仮定する。この仮定の下で矛盾を導く。ここで $\{f^{(j)}(x)\}$ を $P(M, \infty)$ の中の多項式列でそれぞれの $f^{(j)}(x)$ は $\{\alpha_j\}$ を零点として持つとする。多項式の集合 $P(M, \infty)$ の定義より $f^{(j)}(x)$ の 0 でない項の個数は高々 $N = [M^2]$ 個である。よって、 $f^{(j)}(x)$ はつぎのように表現することができる。

$$f^{(j)}(x) = f_{r(0,j)}^{(j)} + f_{r(1,j)}^{(j)} x^{r(1,j)} + \cdots + f_{r(N_j,j)}^{(j)} x^{r(N_j,j)}.$$

ただし、 N_j は $f^{(j)}(x)$ の 0 でない項の個数であり、 $r(i, j)$ はそれぞれの項の次数であるとする。すなわち、

$$\begin{aligned} f_{r(k,j)}^{(j)} &\neq 0 \quad (k = 0, \dots, N_j, j = 0, \dots), \\ 0 = r(0, j) &< r(1, j) < \cdots < r(N_j, j) = \deg f^{(j)}(x) \quad (j = 0, 1, \dots), \\ r(k, j) &= \infty \quad (k > N_j) \end{aligned}$$

である。ここで $r_k = \liminf_{j \rightarrow \infty} r(k, j)$ とおく。このとき定義より、 $r_i \leq r_j$, $(i < j)$ である。 K を r_i が有界となる最大のインデックスとする。すなわち、 r_0, r_1, \dots, r_K は有界であり、 r_{K+1}, \dots は無限大であるとする。ここで $B = r_K$ とする。式 (6.13) のおいて、 $f(x) = f^{(j)}$ とおき、このときの $g(x)$ と n をそれぞれ $g^{(j)}$, n_j とおく。前に述べたことから、

$$\begin{aligned} |D^{(j)}| &= p^{n_j} \left| f_1^{(j)} \left(\frac{q}{p} \right) + f_2^{(j)} \left(\frac{q}{p} \right) \right|, \\ f_1^{(j)}(x) &= \sum_{k=0}^K f_{r(k,j)}^{(j)} x^{r(k,j)}, \\ f_2^{(j)}(x) &= \sum_{k>K} f_{r(k,j)}^{(j)} x^{r(k,j)} \end{aligned}$$

とかける。仮定 $\alpha \notin Z(M, \infty)$ および補助定理 17 より、つぎのようなある正の数 L が存在する：

$$L = \min \left\{ \left| l_0 + l_1 \alpha + \cdots + l_B \alpha^B \right| \mid \left| l_0^2 + \cdots + l_B^2 \right| \leq M^2, l_i \in \mathbb{Z}, (i = 0, \dots, B) \right\} > 0.$$

よって、これより

$$\limsup_{j \rightarrow \infty} \left| f_1^{(j)} \left(\frac{q}{p} \right) \right| \geq L$$

となる。また、一方

$$\lim_{j \rightarrow \infty} f_2^{(j)} \left(\frac{q}{p} \right) = 0$$

である。よって、

$$\limsup_{j \rightarrow \infty} \left| f_1^{(j)} \left(\frac{q}{p} \right) \right| \geq L$$

である。ここで $g^{(j)}(x) = \sum_{i=0}^{n_j-1} g_i^{(j)} x^i$ とおく。このとき、

$$|g^{(j)}(\alpha_j)| = \left| \sum_{i=0}^{n_j-1} g_i^{(j)} \alpha_j^i \right| \leq p^{n_j-1} G \sum_{i=0}^{n_j-1} |\alpha_j|^i = p^{n_j-1} G \frac{1 - |\alpha_j|^{n_j}}{1 - |\alpha_j|}$$

である。ただし、 G は

$$G = \max \left\{ |l_0| + |l_1| + \cdots + |l_i| \in \mathbb{Z} \mid \sum_{i=0}^{\infty} |l_i|^2 \leq M^2 \right\}$$

であるとする。この定数 G が存在することは明らかである。定義より

$$|\alpha_j - \alpha| = \frac{|D^{(j)}|}{|pg^{(j)}(\alpha_j)|}$$

である。 $n_j \geq 1$ であるから、これより

$$\begin{aligned} \limsup_{j \rightarrow \infty} |\alpha_j - \alpha| &\geq \limsup_{j \rightarrow \infty} \frac{p_j^n L}{p \cdot p^{n_j-1} G (1 - |\alpha_j|^{n_j}) / (1 - |\alpha_j|)} \\ &\geq \limsup_{j \rightarrow \infty} \frac{L}{G} \frac{1 - |\alpha_j|}{1 - |\alpha_j|^{n_j}} \\ &\geq \frac{L}{G} > 0 \end{aligned}$$

である。これははじめの仮定である $\lim_{j \rightarrow \infty} \alpha_j = \alpha$ と矛盾する。以上より $Z(M, \infty) \setminus \{\alpha\}$ の点列で α へ収束するものは $|\alpha| > 1$ の場合は存在しない。また $|\alpha| < 1$ の場合は $Z(M, \infty)$ が単位円に関して対称であることから同様に証明できる。また、 $|\alpha| = 1$ の場合は、 α が有理数であることから $\alpha = \pm 1$ である。このとき、 $\alpha \in Z(M, \infty)$ となってしまうので、本定理の仮定を満たさない。以上より、本定理は証明された。 \square

この定理より、たとえば、つぎのようなことがわかる。

例 2 零点の集合 $Z(5, \infty)$ について考える。この集合は系 4 より有理数 5 を要素として含まない。よって定理 14 より $Z(5, \infty)$ を用いて 5 を近似することはできない。第 3 章の定理 4 より、 $Z(5, n)$ の 5 のまわりの穴は n が大きくなるにつれて指数的に小さくなってゆく。よってこの場合穴は現実の零点の分布を説明できなくなっている。また、定理 14 の証明よりわかるように、このような現象が起こるのは次数 n が M^2 に比べて極端に大きくなる場合である。

また、内部の点も例えば $3/5$ は $Z(5, \infty)$ に入らない。よって、 $3/5$ へ収束する点列をつくこともできない。

また、 $\max(Z(5, \infty) \cap \mathbb{R})$ は存在するかどうかは不明である。定理 14 よりもし、 $\max Z(5, \infty)$ が存在しないとすると $\sup Z(5, \infty)$ は無理数でなければならない。

第 7 章

複数の零点の穴についての結果

本章では、2.2 節で定義した複数の零点の穴を用いて、2-ノルムおよび 1-ノルムについて 0 のまわりの零点の存在範囲について考える。2-ノルムに関する結果は Landau の不等式として知られているものに一致する。

7.1 Landau の不等式とその別証

本節では 2-ノルムについて 0 のまわりの穴を考える。補助定理 9 を用いて l 個の零点に関する 0 のまわりの穴を解析する。定理 3 として示した Landau の不等式とほぼ等価な不等式をつぎに証明する。その後、定理 3 の別証を示す。

補助定理 21 $f(x)$ を複素数体上の多項式で $f(0) \neq 0$ であるものとする。また、 $\delta_1, \delta_2, \dots, \delta_l$ を l 個の $f(x)$ の零点とする。このとき $(\delta_1, \dots, \delta_l)$ はつぎの集合に含まれない：

$$\left\{ (\beta_1, \dots, \beta_l) \in \mathbb{C}^l \mid |\beta_1 \cdots \beta_l| < \frac{|f(0)|}{\|f\|} \right\}. \quad (7.1)$$

証明 補助定理 7 より、 $f(x)$ の 0 のまわりの l 個の零点の穴はつぎのようになり、そこには $f(x)$ の l 個の零点の組は存在しない。

$$H_{0,f} = \left\{ (\beta_1, \dots, \beta_l) \in \mathbb{C}^l \mid \phi(\beta_1, \dots, \beta_l) < \frac{|f(0)|}{\|f\|} \right\}.$$

ただし、 $\phi(\beta_1, \dots, \beta_l) = \max \left\{ |h(0)| \mid h(x) \in P(\beta_1, \dots, \beta_l) \right\}$ であり、

$$P(\beta_1, \dots, \beta_l) = \left\{ h(x) \in \mathbb{C}[x] \mid \deg h \leq n, \prod_{i=1}^l (x - \beta_i) | h(x), \|h\|_2 \leq 1 \right\}$$

であるとする。ここで $h(x) = \sum_{j=0}^n b_j x^j$ とおけば、 $\phi(\beta_1, \dots, \beta_l)$ はつぎのように表現することができる：

$$\phi(\beta_1, \dots, \beta_l) = \max_{b_0, \dots, b_l} \left\{ |b_0| \mid \prod_{i=1}^l (x - \beta_i) \mid \sum_{j=0}^n b_j x^j, \sum_{j=0}^n |b_j|^2 \leq 1 \right\}.$$

補助定理 8 より関数 $\phi(\beta_1, \dots, \beta_l)$ は β_1, \dots, β_l に関して連続である。従って β_1, \dots, β_l は互いに等しくないとは仮定してよい（等しい β_i, β_j が存在するときは $\beta_i \rightarrow \beta_j$ として極限を考えればよい）。このとき $\phi(\beta_1, \dots, \beta_l)$ はつぎのように書くことができる。

$$\phi(\beta_1, \dots, \beta_l) = \max_{b_0, \dots, b_l} \left\{ |b_0| \mid \sum_{j=0}^n b_j \beta_i^j = 0, (i = 1, \dots, l), \sum_{j=0}^n |b_j|^2 \leq 1 \right\}.$$

補助定理 9 を用いれば、

$$\phi(\beta_1, \dots, \beta_l) = \sqrt{\frac{G(0^{[n]}, \beta_1^{[n]}, \dots, \beta_l^{[n]})}{G(\beta_1^{[n]}, \dots, \beta_l^{[n]})}}$$

と書くことができる。ここで $G(0^{[n]}, \beta_1^{[n]}, \dots, \beta_l^{[n]})$ に左から行列

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -1 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

を掛けることにより、

$$A \begin{pmatrix} 0^{[n]} \\ \beta_1^{[n]} \\ \vdots \\ \beta_l^{[n]} \end{pmatrix} = \begin{pmatrix} 0^{[n]} \\ \beta_1 \cdot d_1 \\ \vdots \\ \beta_l \cdot d_l \end{pmatrix}$$

となる。ただし $d_i = (0, 1, \beta_i, \dots, \beta_i^{[n-1]})$ とする。ここで $\det A = 1$ であることからこのような変形はグラムの行列式を変化させない。したがって、

$$\phi(\beta_1, \dots, \beta_l) = |\beta_1 \cdots \beta_l|^2 \frac{G(0^{[n]}, d_1, \dots, d_l)}{G(\beta_1^{[n]}, \dots, \beta_l^{[n]})}.$$

さらに、 $0^{[n]}$ は d_1, \dots, d_l と直交しているので

$$G(0^{[n]}, d_1, \dots, d_l) = G(d_1, \dots, d_l)$$

となる。要素の順番を無視すれば、 d_i は $\beta_i^{[n]}$ の β^n を0に置き換えたものであるから

$$G(0^{[n]}, d_1, \dots, d_l) < G(\beta_1^{[n]}, \dots, \beta_l^{[n]})$$

である。以上より $\beta_i \neq 0$ ($i = 1, \dots, l$) ならば

$$\phi(\beta_1, \dots, \beta_l) < |\beta_1 \cdots \beta_l|.$$

以上の議論は β_1, \dots, β_l が互いに等しくないという仮定のもとで行なったが、補助定理8より $\phi(\beta_1, \dots, \beta_l)$ は連続関数であるので一般の β_1, \dots, β_l に対しては

$$|\phi(\beta_1, \dots, \beta_l)| \leq |\beta_1 \cdots \beta_l|$$

となる。 □

ここで l の選び方は自由である。よって、 $|\beta_1 \cdots \beta_l|$ が最大となるようにとることにする。このようにすることによってつぎの系を得る。

系5 n 次の複素係数多項式 $f(x)$ の零点を β_1, \dots, β_n とおく。 $f(0) \neq 0$ であるとする。このときこの零点は

$$|\beta_1| \leq \cdots \leq |\beta_r| < 1 \leq |\beta_{r+1}| \leq \cdots \leq |\beta_n| \quad (7.2)$$

なっているとす。このとき、

$$|\beta_1 \cdots \beta_r| \geq \frac{|f(0)|}{\|f\|} \quad (7.3)$$

である。

証明 $l = r$ として、補助定理21を適用する。 □

これを用いて Landau の不等式の別証が得られる。

定理3の別証 $f(0) = (-1)^n (\text{lc } f) \beta_1 \beta_2 \cdots \beta_n$ であるから、これを系5に適用すれば

$$\frac{\|f\|_2}{|\text{lc } f|} \geq |\beta_{r+1} \cdots \beta_n|$$

が得られる。 □

ここで得られた限界がどの程度よいものであるかは、 $G(0^{[n]}, \beta_1^{[n]}, \dots, \beta_l^{[n]}) / G(\beta_1^{[n]}, \dots, \beta_l^{[n]})$ がいかに1に近いかで決定される。

7.2 1-ノルムについての結果

本節では前節と同じような方法で1-ノルムについてどのような性質が成り立つかということ解析する。前節と同様にして0のまわりの穴は

$$H_{0,f} = \left\{ (\beta_1, \dots, \beta_l) \in \mathbb{C}^l \mid \phi(\beta_1, \dots, \beta_l) < \frac{|f(0)|}{\|f\|_1} \right\}$$

となる。ただし,

$$\phi(\beta_1, \dots, \beta_l) = \max_{b_0, \dots, b_l} \left\{ |b_0| \mid \prod_{i=1}^l (x - \beta_i) \sum_{j=0}^n b_j x^j, \sum_{j=0}^n |b_j| \leq 1 \right\}$$

である。ここで補助定理8より, $\phi(\beta_1, \dots, \beta_l)$ は連続関数である。まず, $\phi(\beta_1, \dots, \beta_l)$ の性質を解析するためにつぎの補助定理を証明する。

補助定理 22 つぎの非線形計画問題を考える。

$$\begin{aligned} b_0, \dots, b_n &\in \mathbb{C}, \\ \sum_{j=0}^n b_j \beta_i^j &= 0, \quad (i = 1, \dots, l), \\ \sum_{j=0}^n |b_j| &\leq 1, \\ \max |b_0|. \end{aligned} \tag{7.4}$$

この非線形計画問題の解を与えるベクトル (b_0, \dots, b_n) で n 個の要素のうち少なくとも $n-l$ 個の要素は0であるものが存在する。

証明 $b_j = c_j + id_j$ とおく。この問題は b_0 を実数と仮定しても一般性を失わないので与えられた問題はつぎの問題と同値である。

$$\begin{aligned} b, c_1, d_1, \dots, c_n, d_n &\in \mathbb{R}, \\ b + \sum_{j=1}^n (c_j \operatorname{Re} \beta_i^j - d_j \operatorname{Im} \beta_i^j) &= 0, \\ \sum_{j=1}^n (d_j \operatorname{Re} \beta_i^j + c_j \operatorname{Im} \beta_i^j) &= 0, \quad (i = 1, \dots, l), \\ b + \sum_{j=1}^n \sqrt{c_j^2 + d_j^2} &\leq 1, \\ \max b. \end{aligned}$$

この問題を問題 N とおき, ベクトル $(b, c_1, d_1, \dots, c_n, d_n)$ が問題 N の解を与えると仮定する。さらに, もとの非線形計画問題において b_0 を含む $l+2$ 個以上の変数が0でないと仮定し矛盾を導く。0でない変数に b_0 が含まれない場合, $b_0 = 0$ である。よって, $b_0 = b_1 = \dots = b_n = 0$

が一つの解であり、これは本補助定理を満たしている。ここでは、0でない変数がちょうど b_0 を含めて $l+2$ 個である場合について考える。それ以上の変数が0でない場合も同様にして証明することができる。この場合、この $l+2$ 個の変数は、問題 N では、 $b, c_{i_1}, d_{i_1}, \dots, c_{i_{l+1}}, d_{i_{l+1}}$ であるとする。また、 $b > 0$ と仮定してよい。これらの変数に対してつぎの式が成り立つ：

$$\begin{aligned} b + \sum_{k=1}^{l+1} \sqrt{c_{i_k}^2 + d_{i_k}^2} &= 1, \\ b + \sum_{k=1}^{l+1} (c_{i_k} \operatorname{Re} \beta_i^{i_k} - d_{i_k} \operatorname{Im} \beta_i^{i_k}) &= 0, \\ \sum_{k=1}^{l+1} (d_{i_k} \operatorname{Re} \beta_i^{i_k} + c_{i_k} \operatorname{Im} \beta_i^{i_k}) &= 0. \end{aligned}$$

ここでこのベクトルに微小変化を加えて最大値がどのように変化するかを調べる。 b', c'_i, d'_i をつぎのように定義する。

$$\begin{aligned} b' &= b + \delta b, \\ c'_i &= c_i + \delta c_i, \\ d'_i &= d_i + \delta d_i \quad (i = i_1, \dots, i_{l+1}). \end{aligned}$$

このとき問題 N の条件を満たすためには b', c'_i, d'_i はつぎの条件を満たさなければならない。

$$\begin{aligned} \delta b + \sum_{k=1}^{l+1} \frac{c_{i_k} \delta c_{i_k} + d_{i_k} \delta d_{i_k}}{\sqrt{c_{i_k}^2 + d_{i_k}^2}} &= 0, \\ \delta b + \sum_{k=1}^{l+1} (\operatorname{Re} \beta_j^{i_k} \delta c_{i_k} - \operatorname{Im} \beta_j^{i_k} \delta d_{i_k}) &= 0, \quad (j = 1, \dots, l), \\ 0 + \sum_{k=1}^{l+1} (\operatorname{Re} \beta_j^{i_k} \delta d_{i_k} + \operatorname{Im} \beta_j^{i_k} \delta c_{i_k}) &= 0, \quad (j = 1, \dots, l). \end{aligned}$$

ここで $\delta b \neq 0$ となる解がこの方程式系にあれば、これを用いて b を微小に大きくすることができる。これは仮定に反する。よってこの方程式系のすべての解について $\delta b = 0$ である。よって、これよりつぎの $2l+1$ 個のベクトルは線形従属であることが分かる。

$$\begin{aligned} &\left(\frac{c_{i_1}}{\sqrt{c_{i_1}^2 + d_{i_1}^2}}, \frac{d_{i_1}}{\sqrt{c_{i_1}^2 + d_{i_1}^2}}, \dots, \frac{c_{i_{l+1}}}{\sqrt{c_{i_{l+1}}^2 + d_{i_{l+1}}^2}}, \frac{d_{i_{l+1}}}{\sqrt{c_{i_{l+1}}^2 + d_{i_{l+1}}^2}} \right), \\ &(\operatorname{Re} \beta_j^{i_1}, -\operatorname{Im} \beta_j^{i_1}, \dots, \operatorname{Re} \beta_j^{i_{l+1}}, -\operatorname{Im} \beta_j^{i_{l+1}}), \quad (j = 1, \dots, l), \\ &(\operatorname{Im} \beta_j^{i_1}, \operatorname{Re} \beta_j^{i_1}, \dots, \operatorname{Im} \beta_j^{i_{l+1}}, \operatorname{Re} \beta_j^{i_{l+1}}), \quad (j = 1, \dots, l). \end{aligned}$$

よって、この条件は

$$\sum_{k=1}^{l+1} \delta b_{ik} \beta_j^{ik} = 0, \quad (j = 1, \dots, l)$$

と書くことができる。ただし、 $\delta b_i = \delta c_i + i \delta d_i (i = i_1, \dots, i_{l+1})$ とかける。この条件は c_{ik} , d_{ik} に依存しない。よって、この解を用いて最大値を変化させないである c_{ik} と d_{ik} を小さくすることができる。この操作を繰り返してゆけば $c_{ik} = 0$, $d_{ik} = 0$ とすることができる。□

関数 ϕ については次の補助定理が成り立つ。

補助定理 23 任意の整数 i, j , ($i \neq j$) に対して $\beta_i \neq \beta_j$ であるとする。また、 i_1, \dots, i_l を l 個の整数で $0 < i_1 < \dots < i_l \leq n$ であるとする。また、 $l \times l$ 行列 B を $B = (B_{j,k}) = (\beta_j^{i_k})$ とおく。さらに $\bar{B}_{j,k}$ を B の (j, k) 余因子とする。また、 $l \times l$ 行列 F を $F = (\beta_j^{i_k-1})$ とおく。このとき、

$$\phi(\beta_1, \dots, \beta_l) = \frac{1}{1 + 1/\Lambda} \quad (7.5)$$

である。ただし、

$$\Lambda = |\beta_1 \cdots \beta_l| \cdot \max_{0 < i_1 < \dots < i_l \leq n} \frac{|\det F|}{\left| \sum_{j=1}^l \sum_{k=1}^l \bar{B}_{j,k} \right|} \quad (7.6)$$

とする。

証明 $\phi(\beta_1, \dots, \beta_l)$ の計算はつぎの非線形計画の問題を解くことと同値である。

$$\begin{aligned} \sum_{j=0}^n b_j \beta_i^j &= 0, \quad (i = 1, \dots, l), \\ \sum_{j=0}^n |b_j| &\leq 1, \\ \max |b_0|. \end{aligned}$$

補助定理 22 より、この問題の解は $n+1$ 個の変数 b_0, \dots, b_n のうち少なくとも $n-l$ 個の変数については 0 である。よって、この解においてはつぎの条件が成り立っている。

$$\begin{aligned} b_0 + \sum_{k=1}^l b_{i_k} \beta_j^{i_k} &= 0, \quad (j = 1, \dots, l), \\ |b_0| + \sum_{k=1}^l |b_{i_k}| &= 1. \end{aligned}$$

ただし、 $0 < i_1 < \dots < i_l \leq n$ であるとする。ここでクラメールの公式より、

$$\begin{pmatrix} b_{i_1} \\ \vdots \\ b_{i_l} \end{pmatrix} = -B^{-1} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} b_0 = \frac{\text{adj } B}{\det B} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} b_0.$$

よって、これより

$$\left(\left| \sum_{j=1}^l \left| \sum_{i=1}^l \tilde{B}_{i,j} \right| \right| / |\det B| + 1 \right) |b_0| = 1$$

である。 $|b_0| = (1 + 1/\Lambda)^{-1}$ とおけば、

$$\Lambda = \frac{|\det B|}{\left| \sum_{j=1}^l \left| \sum_{k=1}^l \tilde{B}_{j,k} \right| \right|} = \frac{|\beta_1 \cdots \beta_l| |\det F|}{\left| \sum_{j=1}^l \left| \sum_{k=1}^l \tilde{B}_{j,k} \right| \right|}$$

となり、本補助定理は証明された。 \square

この補助定理を用いて $l=2$ の場合について考えてみる。

補助定理 24 β_1, β_2 を条件 $0 < |\beta_2| \leq |\beta_1| < 1$ とおく。また、 $0 < i_1 < i_2 \leq n$ とおく。このとき、

$$\Delta(\beta_1, \beta_2) = \left| \det \begin{pmatrix} \beta_1^{i_1-1} & \beta_1^{i_2-1} \\ \beta_2^{i_1-1} & \beta_2^{i_2-1} \end{pmatrix} \right| / \left(\left| \det \begin{pmatrix} 1 & \beta_1^{i_2} \\ 1 & \beta_2^{i_2} \end{pmatrix} \right| + \left| \det \begin{pmatrix} \beta_1^{i_1} & 1 \\ \beta_2^{i_1} & 1 \end{pmatrix} \right| \right) \leq 1 \quad (7.7)$$

が成り立つ。

証明 $\alpha_2 = \beta_2/\beta_1, r = |\beta_1|$ とおく。ここで条件より、 $0 < |\alpha_2| \leq 1$ である。このとき、つぎのように書ける。

$$\Delta(\beta_1, \beta_2) = \left| \det \begin{pmatrix} 1 & 1 \\ \alpha_2^{i_1-1} & \alpha_2^{i_2-1} \end{pmatrix} \right| / \left(\left| \det \begin{pmatrix} 1 & 1 \\ 1 & \alpha_2^{i_2} \end{pmatrix} \right| / r^{i_1-2} + \left| \det \begin{pmatrix} 1 & 1 \\ \alpha_2^{i_1} & 1 \end{pmatrix} \right| / r^{i_2-2} \right)$$

となる。ここで i_1 の値によって場合分けをおこなう。

場合 1 $i_1 \geq 2$ の場合。このとき

$$\max \Delta(\beta_1, \beta_2) = \Delta(\beta_1, \beta_2)|_{r=1}$$

である。よって、

$$\max \Delta(\beta_1, \beta_2) = \frac{|\alpha_2^{i_1-1} - \alpha_2^{i_2-1}|}{|\alpha_2^{i_1} - 1| + |\alpha_2^{i_2} - 1|}$$

である。

$$\begin{aligned} |\alpha_2^{i_1-1} - \alpha_2^{i_2-1}| &= |\alpha_2^{i_1-1} - \alpha_2^{i_1+i_2-1} + \alpha_2^{i_1+i_2-1} - \alpha_2^{i_2-1}| \\ &\leq |\alpha_2^{i_1-1}| |1 - \alpha_2^{i_2}| + |\alpha_2^{i_2-1}| |1 - \alpha_2^{i_1}| \\ &\leq |1 - \alpha_2^{i_2}| + |1 - \alpha_2^{i_1}| \end{aligned}$$

という不等式より $\Delta(\beta_1, \beta_2) \leq 1$ を得る。

場合 2 つぎに $i_1 = 1$ の場合について考える. このとき $i_2 \geq 2$ である.

$$g(r) = \Delta(\beta_1, \beta_2) = \frac{A}{rA_1 + A_2/r^{i_2-2}}$$

とおく. ただし,

$$A = \left| \det \begin{pmatrix} 1 & 1 \\ 1 & \alpha_2^{i_2-1} \end{pmatrix} \right|, \quad A_1 = \left| \det \begin{pmatrix} 1 & 1 \\ 1 & \alpha_2^{i_2} \end{pmatrix} \right|, \quad A_2 = \left| \det \begin{pmatrix} 1 & 1 \\ \alpha_2 & 1 \end{pmatrix} \right|$$

とする. このとき $g(r)$ の導関数は

$$g'(r) = -A \frac{A_1 - A_2(i_2 - 2)/r^{i_2-1}}{(rA_1 + A_2/r^{i_2-2})^2}$$

である. $i_2 = 2$ のとき, $g(r) = A/(rA_1 + A_2) \leq A/A_2 = 1$ となる. また, $i_2 \geq 3$ の場合,

$$r^* = \left(\frac{A_2(i_2 - 1)}{A_1} \right)^{1/(i_2-1)}$$

とおく. $r^* \geq 1$ ならば, $0 < r \leq 1$ において $g'(r) > 0$ である. よって, $\max_{0 < r \leq 1} g(r) = g(1) = A/(A_1 + A_2)$ となるので場合 1 と同様にして証明することができる. また, $r^* < 1$ のとき, すなわち, $A_2(i_2 - 2)/A_1 < 1$ のときは,

$$\begin{aligned} \max_{0 < r \leq 1} g(r) = g(r^*) &= \left[\left(\frac{A}{A_2(i_2 - 1)} \right)^{i_2-1} / \left(\frac{A_1}{A_2(i_2 - 2)} \right)^{i_2} \right]^{1/(i_2-1)} \\ &< \frac{A_1}{A_2(i_2 - 1)} = \frac{|\alpha_2^{i_2-1} - 1|}{|\alpha_2 - 1|(i_2 - 1)} \\ &= \frac{|\alpha_2^{i_2-2} + \alpha_2^{i_2-3} + \cdots + 1|}{i_2 - 1} \leq 1 \end{aligned}$$

となる. これより本補助定理は証明された. \square

この補助定理を用いて $l = 2$ の場合の Landau の不等式に似た性質を導くことができる.

定理 15 δ_1, δ_2 を複素数体上の多項式 $f(x)$ の任意の 2 つの零点とする. このとき, $\phi(\beta_1, \beta_2) \leq (1 + 1/|\beta_1\beta_2|)^{-1}$ であるので, $M = \|f\|_1/|f(0)| \geq 2$ ならば,

$$|\delta_1\delta_2| \geq (M - 1)^{-1} \quad (7.8)$$

である.

証明 補助定理 23 および補助定理 24 より, $|\beta_1|, |\beta_2| \leq 1$ の場合, $\phi(\beta_1, \beta_2) \leq |\beta_1 \beta_2|$ であり, $\phi(\beta_1, \beta_2)$ の定義より,

$$\phi(\beta_1, \beta_2) \leq \begin{cases} (1 + 1/|\beta_1 \beta_2|)^{-1} & \text{if } |\beta_1|, |\beta_2| \leq 1, \\ 1 & \text{otherwise} \end{cases}$$

となる. $M \geq 2$ という仮定より, $|f(0)|/\|f\|_2 \leq 1/2$ である. したがって, $H_{0,f}$ はつぎのような領域を含む.

$$\begin{aligned} \tilde{H} &= \left\{ (\beta_1, \beta_2) \mid |\beta_1|, |\beta_2| \leq 1, (1 + 1/|\beta_1 \beta_2|)^{-1} < 1/M \right\} \\ &= \left\{ (\beta_1, \beta_2) \mid |\beta_1|, |\beta_2| \leq 1, |\beta_1 \beta_2| < 1/(M-1) \right\}. \end{aligned}$$

(δ_1, δ_2) は $H_{0,f}$ に含まれないという性質から, $|\delta_1|, |\delta_2| \leq 1$ の場合には $|\delta_1 \delta_2| \geq 1/(M-1)$ である. また, 定理 5 より, $|\delta_1| > 1$ の場合には $|\delta_2| \geq 1/(M-1)$ であるのでやはり $|\delta_1 \delta_2| \geq 1/(M-1)$ がなりたつ. 以上より本定理が証明された. \square

この定理の系として, 2-ノルムについての Landau の不等式に対応する性質が, 1-ノルムについて成り立つ.

系 6 $f(x)$ を複素数体上の n 次多項式とする. また, その零点を β_1, \dots, β_n として, $0 < |\beta_1| \leq |\beta_2| \leq \dots \leq |\beta_p| < 1 \leq |\beta_{p+1}| \leq \dots \leq |\beta_n|$ であるとする. このとき $\|f\|_1/\|c f\| \geq 2$ ならば

$$|\beta_{n-1} \beta_n| \leq \frac{\|f\|}{\|c f\|} - 1 \quad (7.9)$$

である.

証明 定理 15 より明らか. \square

$l=2$ については, このようにして Landau の不等式と同様の形をした式を導くことができた. $l \geq 3$ の場合にはこのような式が成り立つかどうか不明である. この場合, 補助定理 23 における Λ は大変複雑なものとなり補助定理 24 で行なったような方法を使うことはできない.

第 8 章

2-ノルムによる零点の存在範囲の応用

本章では、第3章で論じた2-ノルムを用いて、与えられた実係数多項式が実零点を持たないことを証明するアルゴリズムについて考える。2-ノルムにおいては穴は方程式で陽に記述することができるので、実際にその範囲を求めることはそれほど難しい。また、はじめの節で述べるように穴 $H_{\alpha, f}$ はある条件のもとではその補集合 $\mathbb{R} \setminus H_{\alpha, f}$ が有界であるようなものとなる。この性質を用いてアルゴリズムを設計する。2-ノルムにおける零点の穴を解析するためにまず、穴の定義にでてくる関数 $\phi(\beta)$ の性質について考察する。その後実際にこの性質を応用することを考える。本節ではノルムの記号 $\|\cdot\|$ は2-ノルム $\|\cdot\|_2$ を表すものとする。

8.1 ポテンシャル関数 $\phi(\beta)$ の性質

本章で実際に応用するのは実係数多項式の実数のまわりの穴である。しかし、ここでは多項式の係数体が複素数体の場合の複素平面上の穴の性質についても同時に考察する。両者は大変良く似た性質をもつからである。

本章で考察する集合は2-ノルムによる穴である。これはつぎのようなものである。 $K = \mathbb{C}$ の場合は

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{C} \mid \phi_{\alpha}(\beta) < \frac{|f(\alpha)|}{\|f\|} \right\}$$

ただし、

$$\phi_{\alpha}(\beta) = \frac{\sqrt{|\beta^{[n]}|^2 |\alpha^{[n]}|^2 - |(\alpha^{[n]}, \beta^{[n]})|^2}}{|\beta^{[n]}|}$$

とする。また、 $K = \mathbb{R}$ のとき解析するのは、

$$H_{\alpha, f} \cap \mathbb{R} = \left\{ \beta \in \mathbb{R} \mid \phi_{\alpha}(\beta) < \frac{|f(\alpha)|}{\|f\|} \right\}$$

である。 $\phi_\alpha(\beta)$ は変わらない。本節ではこの関数 $\phi_\alpha(\beta)$ の性質を $\alpha \in \mathbb{C}$, $\beta \in \mathbb{C}$ の場合と $\alpha \in \mathbb{R}$, $\beta \in \mathbb{R}$ の場合について解析する。まず、つぎの性質が成り立つ。

補助定理 25 ある固定された α に対して

$$L = \phi_\alpha^2(\beta) = |\alpha^{[n]}|^2 - \frac{|(\alpha^{[n]}, \beta^{[n]})|^2}{|\beta^{[n]}|^2} \in [0, |\alpha^{[n]}|^2] \quad (8.1)$$

であり、この区間の任意の値に対して L がその値を実現するような $\beta \in \mathbb{C}$ が存在する。また、さらに

$$R = \frac{|f(\alpha)|^2}{\|f\|^2} \in [0, |\alpha^{[n]}|^2] \quad (8.2)$$

である。この区間の任意の値に対して R がその値をとるような多項式 $f(x)$ が存在する。 $\alpha \in \mathbb{R}$ の場合この多項式は実数体上でとることができる。

証明 Schwartz の不等式から

$$|\alpha^{[n]}|^2 |\beta^{[n]}|^2 - |(\alpha^{[n]}, \beta^{[n]})|^2 \geq 0$$

であるので $0 \leq L \leq |\alpha^{[n]}|^2$ である。また、 $\beta = \alpha$ とすれば $L = 0$ となり、 $\beta = \xi_{n+1}$ (ξ_{n+1} は 1 の $(n+1)$ 乗根で 1 でないものとする) とすれば、 $L = |\alpha^{[n]}|^2$ となる。 L は連続的に変化するのので $[0, |\alpha^{[n]}|^2]$ の間の任意の値をとる。

また、 R については $f(x) = \sum_{i=0}^n a_i x^i$ において $\mathbf{a} = (a_0, \dots, a_n)$ とすれば

$$R = \frac{|(\mathbf{a}, \alpha^{[n]})|^2}{|\mathbf{a}|^2}$$

とかける。これと Schwartz の不等式より $R \leq |\alpha^{[n]}|^2$ である。また、実際、

$$a_i = \alpha^i, \quad (i = 0, \dots, n)$$

とおけば、 $R = |\alpha^{[n]}|^2$ となる。また $f(x)$ を α を零点とする多項式とおけば $R = 0$ となる。 R は f について連続的に変化するののでこの間の任意の値をとる f が存在する。また、 $K = \mathbb{R}$ 、 $\alpha \in \mathbb{R}$ の場合には $a_i = \alpha^i \in \mathbb{R}$ となるので $f(x)$ を実多項式としてとることができる。□

また、これよりつぎの性質が成り立つことが分かる。

補助定理 26 領域 $H_{\alpha, f}$ は $|f(\alpha)| = 0$ のとき空集合であり、また $|f(\alpha)|/\|f\| = |\alpha^{[n]}|$ のとき複素平面から有限個の点を取り除いたものである。また $H_{\alpha, f}$ は $|f(\alpha)|/\|f\|$ が減少するともとの集合の真の部分集合となる。すなわち、

$$\frac{|f_1(\alpha)|}{\|f_1\|} > \frac{|f_2(\alpha)|}{\|f_2\|} \Rightarrow H_{\alpha, f_1} \supset H_{\alpha, f_2} \quad (8.3)$$

である。

証明 補助定理 25 およびその証明より明らか. とくに, $|f(\alpha)|/\|f\| = |\alpha|^{[n]}$ の場合には, 補助定理 25 の証明より, $\beta = \xi_{n+1}/\alpha$ において最大値をとることから,

$$H_{\alpha, f} = \mathbb{C} \setminus \left\{ \xi_{n+1}^i \mid i = 1, \dots, n \right\}$$

となる. ただし ξ_{n+1} は 1 の $n+1$ 乗根である. □

ここで $H_{\alpha, f}$ が有界であるかどうかについてつぎのような性質が成り立つ.

補助定理 27 任意の複素係数多項式 $f(x)$ と複素数 α に対して

$$\frac{|f(\alpha)|}{\|f\|} < |\alpha|^{[n-1]} \Rightarrow H_{\alpha, f} \text{ は有界}, \quad (8.4)$$

$$\frac{|f(\alpha)|}{\|f\|} > |\alpha|^{[n-1]} \Rightarrow \mathbb{C} \setminus H_{\alpha, f} \text{ は有界} \quad (8.5)$$

である.

証明 まず, $|(\alpha^{[n]}, \beta^{[n]})|^2/|\beta^{[n]}|^2$ の値について考える.

$$\begin{aligned} \frac{|(\alpha^{[n]}, \beta^{[n]})|^2}{|\beta^{[n]}|^2} &= \frac{|\sum_{i=0}^n (\alpha\beta)^i|^2}{\sum_{i=0}^n |\beta|^{2i}} \\ &= \frac{|\beta|^2 - 1}{|\beta|^{2(n+1)} - 1} \left| \frac{(\alpha\beta)^{n+1} - 1}{\alpha\beta - 1} \right|^2 \\ &= \frac{1 - 1/|\beta|^2}{1 - 1/|\beta|^{2(n+1)}} \left| \frac{\alpha^{n+1} - 1/\beta^{n+1}}{\alpha - 1/\beta} \right|^2 \end{aligned}$$

となるので β の絶対値が十分に大きければ $|(\alpha^{[n]}, \beta^{[n]})|^2/|\beta^{[n]}|^2$ は $|\alpha|^{2n}$ へ近づく. $|f(\alpha)|/\|f\| < |\alpha|^{[n-1]}$ の場合は補助定理 25 より β の絶対値が十分に大きくなると $\beta \notin H_{\alpha, f}$ である. 従って $H_{\alpha, f}$ は有界である. また一方 $|f(\alpha)|/\|f\| > |\alpha|^{[n-1]}$ の場合は逆に絶対値の十分大きな β について $\beta \in H_{\alpha, f}$ となるので $\mathbb{C} \setminus H_{\alpha, f}$ は有界となる. □

Fig. 8.1 に多項式の次数 $n=5$, $\alpha=1+2i$ の場合の $\phi_\alpha(\beta)$ の等高線図を示す. この図において右上の円が集まっている部分が α である. $|f(\alpha)|/\|f\|$ が大きくなるにつれて α のまわりから広がり続け, $|f(\alpha)|/\|f\| = |\alpha|^{[n-1]}$ のところで穴が反転し, 穴でない部分が有界となるのが分かる. 同じ図を鳥かん図で示したものを Fig. 8.2 に示す. Fig. 8.1 において原点付近の部分は ξ_{n+1}^i が集まったものでそこで $\phi_\alpha(\beta)$ が最大値をとるということが分かる.

また, α が実数である場合, 集合 $H_\alpha \cap \mathbb{R}$ に対しても同様の性質がある.

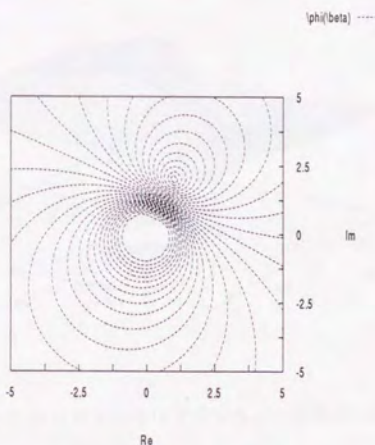


Fig. 8.1. $n = 5$, $\alpha = 1 + 2i$ のときの $\phi_\alpha(\beta)$ の等高線図

補助定理 28 任意の実係数多項式 $f(x)$ と任意の実数 α に対して

$$\frac{|f(\alpha)|}{\|f\|} < |\alpha|^{n-1} \Rightarrow H_\alpha \cap \mathbb{R} \text{ は有界であり,} \quad (8.6)$$

$$\frac{|f(\alpha)|}{\|f\|} > |\alpha|^{n-1} \Rightarrow \mathbb{R} \setminus (H_\alpha \cap \mathbb{R}) \text{ は有界である.} \quad (8.7)$$

証明 補助定理 27 の証明と全く同様である. \square

$n = 5$, $\alpha = 5$ のときの $K = \mathbb{R}$, $\alpha \in \mathbb{R}$ としたときの $\phi_\alpha(\beta)$ の形を Fig. 8.3 に示す. これは補助定理 3 より Fig. 8.1 と Fig. 8.2 の断面図となっている. このとき

$$|\alpha^{[5]}| = 3189.43$$

であり,

$$|\alpha^{[4]}| = 637.89$$

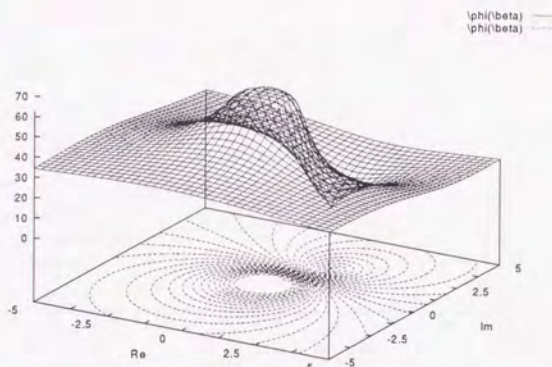


Fig. 8.2. $n=5$, $\alpha=1+2i$ のときの $\phi_\alpha(\beta)$ の鳥かん図

であるので、この関数の漸近線は縦軸の 637.89 を横切る水平線である。この場合 $n=5$ であるので実際に $-1/5$ においてこの関数は最大値をとり、その最大値は $|\alpha^{[5]}| = 3189.43$ である。

8.2 整係数多項式が実零点を持たないことを証明するアルゴリズム

本節では前節の結果を用いて与えられた整係数多項式が実根を持たないことを示すためのアルゴリズムについて述べる。次数が奇数の多項式は、必ず実根をもつので次数が奇数の場合は意味がないがここで述べる方法論はたとえば正の実数を持たないことの判定などに応用できるので、一応次数は奇数に限ることは、ここでは行なわない。また、数値計算は誤差なく行なえるものと仮定する。

まず準備としてつぎの良く知られた補助定理を記す。

補助定理 29 (Hadamard の不等式 [Sch86]) 実数体上の正方行列 B が $B = (r_1, r_2, \dots, r_n)$ ($r_i \in \mathbb{R}^n$) と表されるとき

$$|\det B| \leq |r_1| |r_2| \cdots |r_n| \quad (8.8)$$

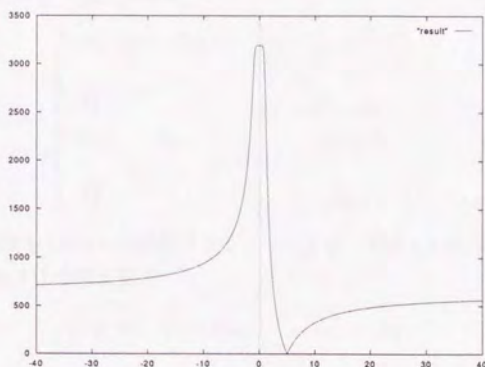


Fig. 8.3. $n = 5, \alpha = 5$ の場合の $\phi_\alpha(\beta)$ のグラフ

が成り立つ.

この性質を用いてつぎの補助定理を示す.

補助定理 30 整係数多項式 $f(x)$ が実根を持たないとき,

$$\forall \alpha \in \mathbb{R}, |f(\alpha)| > \left(\frac{1}{\sqrt[n]{\pi(n-1)}} 2^{n-1} n^{n+1/(48(n-1))} \|f\|^{2n-1} \right)^{-1} \quad (8.9)$$

である.

証明 多項式 $f(x)$ が x 軸に一番近づくときの x を α とおく. このとき $f'(\alpha) = 0$ を満たす. よってこのときの値を β とおくとつぎのような連立方程式が成り立つ:

$$\begin{cases} f'(\alpha) = 0, \\ f(\alpha) - \beta = 0. \end{cases}$$

これより, β は方程式 $F(\beta) = \text{Res}_x(f'(x), f(x) - \beta) = 0$ を満たさなければならない. ここで $\text{Res}_x(f(x), g(x))$ は $f(x)$ と $g(x)$ の変数 x に関する終結式を表す. $f(x) = \sum_{i=0}^n a_i x^i$ とお

いてこの終結式を行列式で表示すれば,

$$F(\beta) = \det \begin{pmatrix} na_n & (n-1)a_{n-1} & \cdots & a_1 & 0 \\ & \ddots & \ddots & \ddots & \ddots \\ 0 & & na_n & (n-1)a_{n-1} & \cdots & a_1 \\ a_n & a_{n-1} & \cdots & a_0 - \beta & 0 \\ & \ddots & \ddots & \ddots & \ddots \\ 0 & & a_n & a_{n-1} & \cdots & a_0 - \beta \end{pmatrix}$$

となる. この行列式を β について展開することを考える. そのためにつぎのような行列式 $F_{i_1, i_2, \dots, i_{n-1}}$ ($i_j \in \{0, 1\}$) を考える.

$$F_{i_1, i_2, \dots, i_{n-1}} = \det \begin{pmatrix} na_n & (n-1)a_{n-1} & \cdots & a_1 & 0 \\ & \ddots & \ddots & \ddots & \ddots \\ 0 & & na_n & (n-1)a_{n-1} & \cdots & a_1 \\ b_n & b_{n-1} & \cdots & b_0 & 0 \\ & \ddots & \ddots & \ddots & \ddots \\ 0 & & b_n & b_{n-1} & \cdots & b_0 \end{pmatrix}.$$

ただし,

$$n + i_j \text{ 行目の } (b_n, b_{n-1}, \dots, b_0) = \begin{cases} (a_n, a_{n-1}, \dots, a_0) & (i_j = 0), \\ (0, 0, \dots, 0, -1) & (i_j = 1). \end{cases}$$

である. このようにおくと, $F(\beta)$ の β^k の係数は

$$\sum_{i_1 + \dots + i_{n-1} = k, i_j \in \{0, 1\}} F_{i_1, i_2, \dots, i_{n-1}}$$

である. 補助定理 29 (Hadamard の不等式) より

$$|F_{i_1, i_2, \dots, i_{n-1}}| \leq n^n \|f\|^{2n-1}$$

である. したがって, $F(\beta)$ の β^k の係数の絶対値は上から

$$\binom{n-1}{k} n^n \|f\|^{2n-1}$$

で押えることができる. このことから, $F(x)$ の 2-ノルムは

$$\|F\| \leq \left[\sum_{k=0}^{n-1} \binom{n-1}{k} \right]^{1/2} n^n \|f\|^{2n-1}$$

となる. ここで $m = n - 1$ とおいて, Stirling の公式を用いれば,

$$\begin{aligned} \sum_{k=0}^{n-1} \binom{n-1}{k}^2 &= \binom{2(n-1)}{n-1} = \frac{(2m)!}{(m!)^2} \\ &\leq \frac{\sqrt{4\pi m} \left(\frac{2m}{e}\right)^{2m+1/(24m)}}{\left(\sqrt{2\pi m} \left(\frac{m}{e}\right)^m\right)^2} \\ &= \sqrt{\frac{1}{\pi m}} 2^{2m} \left(\frac{2m}{e}\right)^{1/(24m)} \end{aligned}$$

となるので, これより

$$\|F\| \leq \sqrt{\frac{1}{\pi m}} 2^m \left(\frac{2m}{e}\right)^{1/(48m)} n^n \|f\|^{2n-1}$$

を得る. □

注意: この補助定理の証明では Stirling の公式としてつぎの式を用いた.

$$\sqrt{2\pi n} \left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2\pi n} \left(\frac{n}{e}\right)^{n+1/(12n)}. \quad (8.10)$$

また, $f(x)$ がある実零点をもち, α がその実零点に十分近いときつぎの性質が成り立つ.

補助定理 31 α が実多項式 $f(x)$ の零点に十分に近いとき $H_{\alpha, f} \cap \mathbb{R}$ は漸近的に開区間 $(\alpha - \varepsilon, \alpha + \varepsilon)$ に近づく. ただし,

$$\varepsilon = \frac{|f(\alpha)|}{\|f\|} \cdot \left(|D_\alpha \alpha^{[n]}|^2 - |(D_\alpha \alpha^{[n]}, \alpha^{[n]})|^2 / |\alpha^{[n]}|^2 \right)^{-1/2}$$

とする.

証明 $\beta = \alpha + \varepsilon$ とおく. 定理 4 の $C_2(n, \alpha)$ を用いて

$$\varepsilon = C_2(n, \alpha) \frac{|f(\alpha)|}{\|f\|}$$

と書くことができる. これは本補助定理である. □

系 7 整係数多項式 $f(x)$ が実根をもたない場合, 任意の実数 α について

$$H_{\alpha, f} \supset (\alpha - \varepsilon, \alpha + \varepsilon). \quad (8.11)$$

ただし,

$$\varepsilon = \left(\frac{1}{\sqrt[n]{\pi(n-1)}} 2^{n-1} n^{n+1/(48(n-1))} \|f\|^{2n} \right)^{-1} \times \\ (|D_\alpha \alpha^{[n]}|^2 - |(D_\alpha \alpha^{[n]}, \alpha^{[n]})|^2 / |\alpha^{[n]}|^2) \quad (8.12)$$

とする.

証明 補助定理 30 および 補助定理 31 より明らか. \square

この補助定理より, $f(x)$ が零点を持たないときの穴の幅のある下界が分かったことになる. よって, これよりも穴の幅が小さくなった場合この $f(x)$ は実零点を持つことになる. つぎに, 実際に $H_{\alpha, f}$ を効率良く計算するためにつぎの補助定理を示す.

補助定理 32 実数 α, β が $1 < \alpha < \beta$ を満たすとする. このとき $\phi_\alpha(\beta)$ は β とともに単調に増加する.

証明 まず, $e = \beta^2$, $f = \alpha\beta$ とおく. また $\phi(\beta)$ が単調増加であるということは

$$\Omega = \frac{(1 + f + f^2 + \cdots + f^n)^2}{1 + e + e^2 + \cdots + e^n}$$

が単調減少することと同値である. ここで,

$$F(y) = 1 + y + y^2 + \cdots + y^n$$

とおくと,

$$\frac{d\Omega}{d\beta} = \frac{2F'(f)F(f)F'(e)(df/d\beta) - F'(e)F^2(f)(de/d\beta)}{F^2(e)}$$

ここで $df/d\beta = \alpha$ であり, $de/d\beta = 2\beta$ であるので,

$$\frac{d\Omega}{d\beta} = 2 \frac{F(f)}{F^2(e)} [F'(f)F(e)\alpha - F'(e)F(f)\beta]$$

となる. ここで関数

$$y \frac{F'(y)}{F(y)}$$

は $y \geq 1$ ならば y の増加とともに単調に増加する. $\alpha < \beta$ であるので $f < e$ である. よって

$$d \frac{F'(f)}{F(f)} < d \frac{F'(e)}{F(e)}$$

であり, これより $d\Omega/d\beta < 0$ を得る. \square

$\alpha \geq 1$ に対して $\phi_\alpha(\beta)$ を用いて $d \in \mathbb{R}^{\geq 0}$ として

$$R(d) = \max\{\delta \in \mathbb{R} \mid \phi_\alpha(\delta) \leq d\}$$

を定義する。ただし、 $\mathbb{R}^{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$ とする。これを用いてまず、つぎのようなアルゴリズムを考える。

アルゴリズム 1 n 次整係数多項式 $f(x)$ が与えられたとき $f(x)$ が実零点をもつかどうかを判定する。ここで $f(x)$ を計算するアルゴリズムが与えられ、 $\|f\|$ の上界が分かっているものとする。実数軸上の区間 T に対して $\text{Right}(T)$ をその区間の大きい方の端であるとする。

- A1. $N \leftarrow \|f\|$ の上界
- A2. $S \leftarrow \emptyset$
- A3. $\delta \leftarrow f(x)$ が実零点を持たないと仮定したときの $|f(x)|$ の下限
- A4. **while** $S \neq \mathbb{R}$ **do**
- A5. **begin**
- A6. $T \leftarrow \{\beta \in \mathbb{R} \mid |\alpha^{[n]}|^2 - |(\alpha^{[n]}, \beta^{[n]})|^2 / |\beta^{[n]}|^2 < |f(\alpha)|^2 / N^2\}$
 の α を含む最大の部分区間
- A7. **if** $|f(\text{Right}(T))| < \delta$ **then goto** A12
- A8. $S \leftarrow S \cup T$
- A9. $\alpha \leftarrow \text{Right}(T)$
- A10. **end**
- A11. $f(x)$ は実根を持たない。終了。
- A12. $f(x)$ は実根を持つ。終了。

つぎにアルゴリズム 1 が停止することを示す。まず、つぎの補助定理を証明する。

補助定理 33 アルゴリズム 1 で整係数多項式 $f(x)$ が実零点をもつ場合、 α はその零点の一つへ一次収束する。

証明 $f(x)$ のある零点を α_0 とし、 $\alpha = \alpha_0 - \varepsilon$ とおく。 ε は十分に小さいものとする。このとき、

$$|f(\alpha)| = |f(\alpha_0 - \varepsilon)| = |f'(\alpha_0)\varepsilon|$$

である。よって、

$$\frac{|f(\alpha)|}{N} = \frac{|f'(\alpha_0)|}{N} |\varepsilon|$$

となる。補助定理 7 より アルゴリズム 1 における T は $(\alpha_0 - \varepsilon - \delta, \alpha_0 - \varepsilon + \delta)$ である。ただし $\delta = C_1 |\varepsilon|$ かつ

$$C_1 = \frac{|f'(\alpha)|}{N} \left(|D_\alpha \alpha^{[n]}|^2 - |(D_\alpha \alpha^{[n]}, \alpha^{[n]})|^2 / |\alpha^{[n]}|^2 \right)^{1/2}$$

であるとする。これにより、 $|\alpha - \alpha_0|$ は $\varepsilon \leftarrow (1 - C_1)\varepsilon$ となる。すなわち n 回くりかえせば $|\alpha - \alpha_0| = C_2(1 - C_1)^n$ となる。ただし、 C_2 はある定数とする。よって α は α_0 へ一次収束する。□

この補助定理を用いてつぎの定理が示される。

定理 16 アルゴリズム 1 は停止する。

証明 整係数多項式 $f(x)$ が実零点を持たない場合、補助定理 31 より、 α をいくつにとっても穴の幅 $|H_{\alpha,f}|$ はある定数以上である。よって A4 から A10 のループでは α は一回につきある定数以上大きくなる。 α が十分に大きくなれば、 $|f(\alpha)|/\|f\|$ の値は α が大きくなるにつれて増加する。ここで α に関して、 $|\alpha^{[n-1]}| = O(\alpha^{n-1})$ であり、 $|f(\alpha)|/\|f\| = O(\alpha^n)$ であるので、 α が大きくなるといつか $|f(\alpha)|/\|f\|$ は $|\alpha^{[n-1]}|$ を超える。このとき補助定理 28 より $\mathbb{R} \setminus (H_{\alpha,f} \cap \mathbb{R})$ が有界となり、無限に広い領域を含むことになる。よって、この時点で零点の存在しうる区間は有界となる。したがってそのあと α は大きくなってゆくのでいつか $T = \mathbb{R}$ となる。

また、一方 $f(x)$ が実零点を持つ場合、補助定理 33 よりその実零点のうちのひとつへ一次収束する。また、このとき、その零点に十分に近ければ、補助定理 30 より、

$$O(n \log \|f\| + n \log n)$$

ステップ程度で停止する。□

アルゴリズム 1 の A5 において「最大の部分区間」となっているがこれは大抵の場合 $H_{\alpha,f} \cap \mathbb{R}$ 自体が区間となるのでそれそのものとなる。しかし、一般には、 $H_{\alpha,f} \cap \mathbb{R}$ は単一の区間とはならない。そこで補助定理 32 を用いてこのアルゴリズムを改良する。

アルゴリズム 2 n 次整係数多項式 $f(x)$ が与えられたとき $f(x)$ が 1 以上の実零点を持つかどうかを判定する。ここで $f(x)$ を計算するアルゴリズムと $\|f\|$ の上界が与えられているとする。

A1. $N \leftarrow \|f\|$ の上界

A2. $\alpha \leftarrow 1$

A3. $\delta \leftarrow f(x)$ が実零点を持たないと仮定したときの $|f(x)|$ の下限

```

A4.   while True do
A5.     begin
A6.       if  $|f(\alpha)|/N > |\alpha|^{n-1}$  then goto A11
A7.        $T \leftarrow \{\beta \in \mathbb{R} \mid |\alpha|^{[n]}|^2 - |(\alpha^{[n]}, \beta^{[n]})|^2 / |\beta^{[n]}|^2 < |f(\alpha)|^2 / N^2\}$ 
A8.       if  $|f(\text{Right}(T))| < \delta$  then goto A12
A9.        $\alpha \leftarrow \text{Right}(T)$ 
A10.    end
A11.     $f(x)$  は実根を持たない. 終了.
A12.     $f(x)$  は実根を持つ. 終了.

```

アルゴリズム 2 が停止するのは明らかである. また, 補定理 32 より, $H_{\alpha, f}$ の右端はいつも確定し, 2 分法で簡単に求めることができる. アルゴリズム 2 を用いて $f(x)$ が実数全域で零点を持たないことを証明するアルゴリズムを示す.

アルゴリズム 3 n 次整係数多項式 $f(x)$ が与えられたとき $f(x)$ が実零点を持つかどうかを判定する. ここで $f(x)$ を計算するアルゴリズムと $\|f\|$ の上界が与えられているとする.

```

A1.   アルゴリズム 2 を  $f(x)$  について実行する.
A2.   アルゴリズム 2 を  $f(-x)$  について実行する.
A3.   アルゴリズム 2 を  $f^{\text{rev}}(x)$  について実行する.
A4.   アルゴリズム 2 を  $f^{\text{rev}}(-x)$  について実行する.

```

アルゴリズム 3 についての簡単な例をつぎに示す.

例 3 整係数多項式 $f(x) = x^4 - 4x^3 + 8x^2 - 14x + 74 = (x-1)^4 + (x+3)^2 + (x-8)^2$ が実零点を持たないことをつぎのようにして証明できる. このとき $\|f\| = \sqrt{5753}$ であり, これをノルムの上界として用いる. アルゴリズム 3 に従って, つぎの 4 つの多項式に対してアルゴリズム 2 を適用する.

$$\begin{aligned}
f_1(x) &= x^4 - 4x^3 + 8x^2 - 14x + 74 \\
f_2(x) &= f(-x) = x^4 + 4x^3 + 8x^2 + 14x + 74 \\
f_3(x) &= f^{\text{rev}}(x) = 74x^4 - 14x^3 + 8x^2 - 4x + 1 \\
f_4(x) &= f^{\text{rev}}(-x) = 74x^4 + 14x^3 + 8x^2 + 4x + 1
\end{aligned}$$

それぞれについて $\alpha = 1$ から出発して $x \geq 1$ の部分に零点が存在しないことを示す. Fig. 8.4 にそれぞれの場合について α の移り変わる様子を示す. また, $f(x)$ の実際の形を Fig. 8.5 に示す. また, この場合の繰り返しの回数は Table 8.1 の様になる.

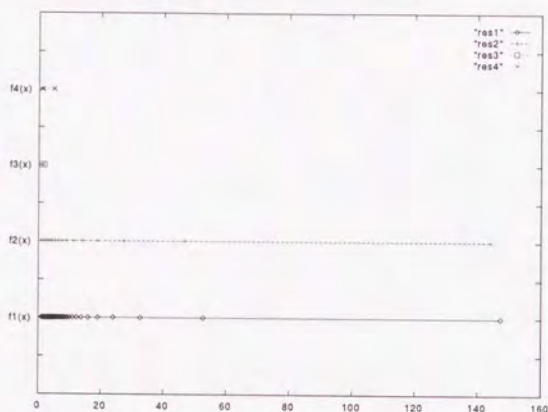


Fig. 8.4. アルゴリズム 3の実行例 1

例 4 つぎに、つぎのような例を考える。

$$f(x) = 2x^6 - 3x^5 + 185x^4 - 380x^3 + 1455x^2 + 156x + 793 = (x-2)^6 + (x+3)^6$$

前の例と同様にして Fig. 8.6 に実行例を示す。また、この多項式のグラフを Fig. 8.7 に示す。この例についてもそれぞれの多項式が評価された回数をつぎに Table 8.2 に示す。

例 5 また、多項式が実零点をもつ場合の一番単純な例として、

$$f(x) = x^2 - 2$$

について計算してみる。この場合、補助定理 33 によって、理想的には $\sqrt{2}$ へ収束することになる。しかし実際には 64 ビット実数程度で計算すると誤差などの集積によってつぎのように $\sqrt{2}$ の付近で収束しかけるが、誤差の集積によって再び大きくなり始める。Fig. 8.8 にその様子を示す。

例 6 つぎのような多項式は実零点をもつ。この多項式に対するアルゴリズム 3 の動きをつぎに示す。

$$f(x) = x^6 - 19x^5 + 100x^4 + 250x^3 - 4375x^2 + 15625x - 18750$$

この多項式は $x=5$ で 5 重の零点を持つ。このとき繰り返しとそれに伴う α の動きを Fig. 8.9 に示す。この場合、実際には誤差によって 5 よりも手前で一定の値になってしまう。

アルゴリズム 3 の計算の複雑さなどは全く知られていない.

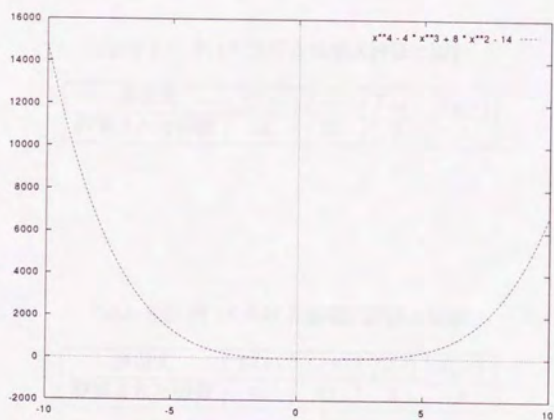


Fig. 8.5. $f(x) = x^4 - 4x^3 + 8x^2 - 14x + 74$ のグラフ

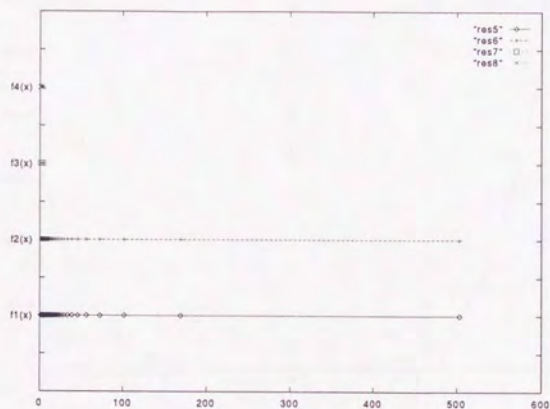


Fig. 8.6. アルゴリズム 3 の実行例 2

Table 8.1. 例 3 における多項式評価の回数

多項式	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
評価された回数	54	17	2	3

Table 8.2. 例 4 における多項式評価の回数

多項式	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
評価された回数	43	43	3	3

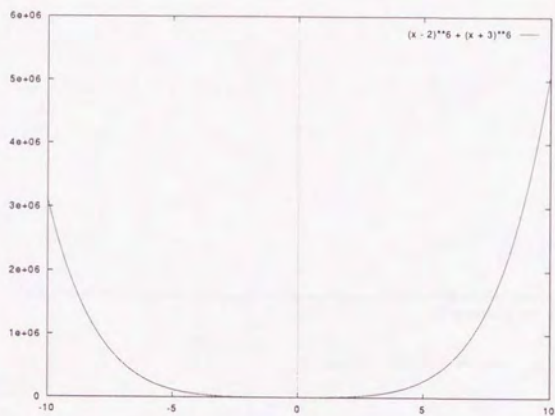


Fig. 8.7. $f(x) = 2x^6 - 3x^5 + 185x^4 - 380x^3 + 1455x^2 + 156x + 793$ のグラフ

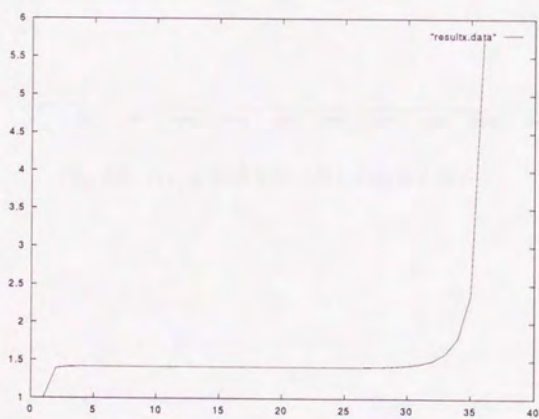


Fig. 8.8. $f(x) = x^2 - 2$ の場合の $\sqrt{2}$ への収束の様子

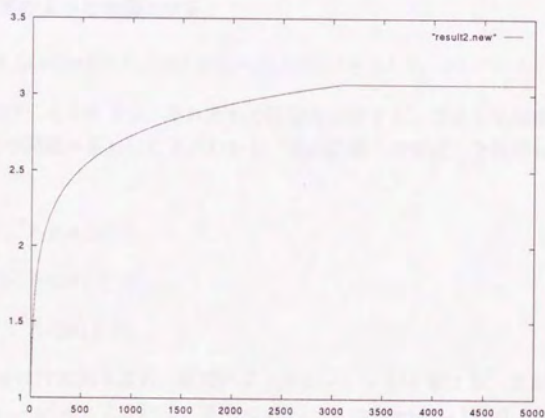


Fig. 8.9. $f(x)$ が零点を持つ場合の収束の様子

8.3 不等式の証明への応用例

本節では, Schwartz [Sch80] で説明されている Tarski の方法をこれに沿って説明し, その方法とここで述べた方法を組合せてある種の不等式が証明できることを示す.

まず, つぎのような三つの形式の命題を証明することを考える:

1. $\forall x \in \mathbb{R}^n, [T \Rightarrow g(x) = 0]$
2. $\forall x \in \mathbb{R}^n, [T \Rightarrow h(x) \leq 0],$
3. $\forall x \in \mathbb{R}^n, [T \Rightarrow e(x) < 0].$

ただし, T はつぎのような命題とする:

$$f_1(x) = 0 \wedge \cdots \wedge f_k(x) = 0 \wedge f_{k+1}(x) \leq 0 \wedge \cdots \wedge f_l(x) \leq 0 \wedge f_{l+1}(x) < 0 \wedge \cdots \wedge f_m(x) < 0.$$

これらの問題を解くためにまず, それぞれの問題を否定する. 否定した問題が正しくないことを示せば元の問題が正しいことがわかる. 元の問題の否定は, それぞれ, つぎのようになる.

1. $\exists x \in \mathbb{R}^n, [T \wedge g(x) \neq 0],$
2. $\exists x \in \mathbb{R}^n, [T \wedge h(x) \geq 0],$
3. $\exists x \in \mathbb{R}^n, [T \wedge e(x) > 0].$

ここで $g(x) \neq 0$ は付加的な変数 y を用いて $g(x)y - 1 = 0$ と書ける. また, 同様にして $h(x) \geq 0$ は $h(x) - y^2 = 0$ とかける. さらに $e(x) > 0$ は $e(x)y^2 - 1 = 0$ と書ける. T の要素となっている式もまた, 同様にして等式で書き直すことが出来る. よって, 否定したそれぞれの命題はつぎのように書き直せる.

$$\exists x \in \mathbb{R}^n, y \in \mathbb{R}^p, r_1(x, y) = 0, \dots, r_l(x, y) = 0.$$

さらに, この命題は

$$\exists x \in \mathbb{R}^n, y \in \mathbb{R}^p, r_1(x, y)^2 + \cdots + r_l(x, y)^2 = 0$$

と書けるのでこれをまとめてあらためて $\exists x \in \mathbb{R}^n, R(x) = 0$ と書くことにする. この命題が成り立たないことを示せばよい. R は多変数多項式である. ここであるベクトル $y_0 \in \mathbb{R}^p$ を適当に決めて, $R(x) = 0$ の解空間のなかの点で y_0 に一番近い点を求めることにする. このような解空間が存在しない場合は, このような点は存在しない. また, 一方このような

解空間が存在すれば一番近い点を一意に決定することができる。\$R\$から、この点を求めるためにはつぎの方程式系の解を求めればよいことがわかる。

$$\begin{aligned} R &= 0, \\ (x_i - y_i)R_{x_i} - (x_1 - y_1)R_{x_1} &= 0 \quad (i = 2, \dots, n). \end{aligned}$$

ただし、\$R_{x_i}\$は\$R\$の変数\$x_i\$に関する偏微分を表すものとする。この方程式系が実零点を解として持てばこのような解空間は存在し、もし存在しなければ解空間は存在しない。このようにして得られた方程式系を

$$F(x, y) = 0$$

と書く。ただし、\$0\$は長さ\$0\$のベクトルであり、\$F\$はベクトル値関数であるとする。

例 7 (Bernoulli の不等式) つぎの不等式を証明することを考える。ただし、\$n\$は\$2\$以上の整数とする。

$$\alpha > 0, (1 + \alpha)^n > 1 + n\alpha \tag{8.13}$$

この不等式は簡略化のため\$\alpha = t^2, t \neq 0\$とおけば

$$(1 + t^2)^n > 1 + nt^2$$

と書くことができる。任意の実数\$t\$についてこの不等式が成り立つことを示せばよい。この不等式の否定は、ある実数\$t\$について

$$(1 + t^2)^n \leq 1 + nt^2$$

であり、これは

$$R \equiv (1 + t^2)^n - (1 + nt^2) + h^2 = 0$$

が実数解\$(t, h)\$を持たないことと同値である。ただし、\$t \neq 0\$とする。このとき、

$$\begin{aligned} \frac{\partial R}{\partial t} &= 2tn(1 + t^2)^{n-1} - 2tn, \\ \frac{\partial R}{\partial h} &= 2h \end{aligned}$$

であることから\$R = 0\$を成り立たせる\$(t, h)\$存在すれば

$$\begin{aligned} R &= 0, \\ \frac{\partial R}{\partial t}h - \frac{\partial R}{\partial h}t &= 0 \end{aligned}$$

を成り立たせる (t, h) が存在する。よって、この解が存在しないことを示せば十分である。
この式は

$$\begin{aligned}(1+t^2)^n - (1+nt^2) + h^2 &= 0, \\ 2t[n(1+t^2)^{n-1} - (n+1)h] &= 0\end{aligned}$$

であり、さらに $t \neq 0$ という条件より、

$$\begin{aligned}(1+t^2)^n - (1+nt^2) + h^2 &= 0, \\ \frac{n}{n+1}(1+t^2)^{n-1} - h &= 0.\end{aligned}$$

この結果より、 h は容易に消去することができて、

$$S(t) \equiv (n+1)^2 [(1+t^2)^n - (1+nt^2)] + n^2(1+t^2)^{2(n-1)} = 0 \quad (8.14)$$

となる。これが $t \neq 0$ という条件のもとで実数解を持たなければ、もともとの不等式が証明できたことになる。ここで、 $S(t)$ の 1-ノルム $\|S\|_1$ はつぎのように上から押えることができる。

$$\|S\|_1 \leq (n+1)^2 [2^n + 1 + n] + n^2 2^{2(n-1)} \equiv D(n).$$

$\|S\|_2 \leq \|S\|_1$ であるから、これより $\|S\|_2 \leq D(n)$ である。すなわち、 $\|S\|_2$ の上界を見積もることができるのでアルゴリズム 3 を用いることができる。

ここで $n=5$ について実際に数値計算を行なう。まず、この場合、 $D(5) = 7768$ である。また、 $\deg S(t) = 16$ である。アルゴリズム 3 では具体的に多項式を書き下す必要はなく、 $S(t)$ が実際に計算できて、 $\|S\|_2$ の上界が分かていれば実行することができる。また、この場合は $S(t) = S(-t)$ であるので $t < 0$ の場合については確かめる必要がなく、アルゴリズム 3 の A1, A3 のみを実行すれば十分である。この実行結果を Fig. 8.10 に示す。A1 と A3 において一番外側のループで実行された繰り返しはそれぞれ 118 回と 269 回であった。

このような証明法は必ずしもうまくゆくとは限らない。つぎにその例を示す。

例 8 二変数についての Schwartz の不等式を考える。すなわち

$$(x_1 x_2 + y_1 y_2)^2 \leq (x_1^2 + y_1^2)(x_2^2 + y_2^2)$$

について考える。これを証明するためには前に述べたようにまず与えられた不等式を否定してから余分な変数を用いて等式へ変形する。結局この不等式の否定は

$$\exists x_1, x_2, y_1, y_2, h \in \mathbb{R}, M = (x_1^2 y_2^2 + x_2^2 y_1^2 - 2x_1 x_2 y_1 y_2) h^2 + 1 = 0$$

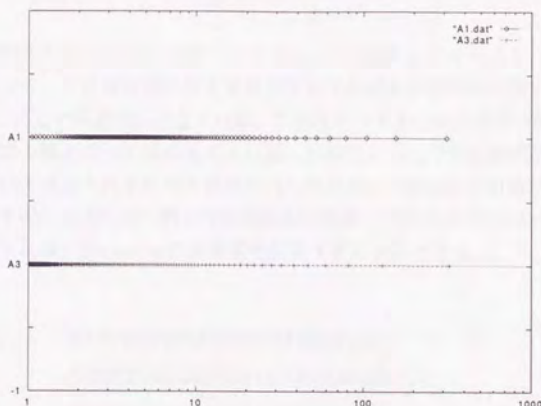


Fig. 8.10. $S(t)$ についてアルゴリズム 3 を実行した結果

である。これより、変数を消去するためにはつぎのような式を作ればよい。

$$\begin{aligned}
 M &= 0, \\
 M_{x_1}(x_2 - 1) - M_{x_2}(x_1 - 1) &= 0, \\
 M_{x_1}(y_1 - 1) - M_{y_2}(x_1 - 1) &= 0, \\
 M_{x_1}(y_2 - 1) - M_{y_2}(x_1 - 1) &= 0, \\
 M_{x_1}(h - 1) - M_h(x_1 - 1) &= 0.
 \end{aligned}$$

ここでは座標 $(1, 1, 1, 1, 1)$ から $M = 0$ となる集合への最近点を求めることにする。この場合は座標 $(1, 1, 1, 1, 1)$ を選択したが、この点は任意に選ぶことができる。この方程式系を数式処理システム Mathematica [Wol88] で計算するとつぎのようになる。

$$\begin{aligned}
 h^2 x_2^2 y_1^2 - 2h^2 x_1 x_2 y_1 y_2 + h^2 x_1^2 y_2^2 + 1 &= 0, \\
 -y_1 + x_1 y_1 - y_2 + x_2 y_2 &= 0, \\
 -x_2 + x_1 x_2 - y_2 + y_1 y_2 &= 0, \\
 (-x_1 + y_2)(-1 + x_1 + y_2) &= 0, \\
 -x_2 y_1 + x_1 y_2 y_1 - h y_2 + h^2 y_2 + x_1 y_2 - x_1^2 y_2 &= 0.
 \end{aligned}$$

ただし、それぞれの式は因数分解をして自明に意味のない因子は取り除いてある。この

Schwartz の不等式を証明するにはこの方程式系が実数の範囲に零点をもたないことを示せばよい。

このような方程式系が与えられればこれは Bezout の定理 [vdW37] より、有限個の解しか持たない。よって、この有限個の解を求めてそのそれぞれが実数解でないことを示せばよい。また、もしここで実数解が存在すれば、これはそのままこの不等式の反例となる。しかし、この方程式の解をすべて求めることは難しいので、ここでは変数消去を行なう。この変数消去は方程式系のそれぞれの方程式に対してお互いの終結式を計算することにより求めることができる。たとえば、例 8 の方程式系の場合、つぎの 52 次多項式が実零点をもたないことを示せれば、Schwartz の不等式を証明することができる。

$$\begin{aligned} f(x) = & 1381172598030064708896849677025 - \\ & 21980211869348085224454494549220 x + \\ & 176218245308174982815338022684358 x^2 + \ll 48 \gg + \\ & 12000000000000000000000000000000 x^{51} + \\ & 10000000000000000000000000000000 x^{52} \end{aligned}$$

ただし、 $\ll 48 \gg$ は 48 個の項の省略を表す。この多項式のノルムを計算すると、 4.32×10^{35} となる。一方、繰り返しの出発点での多項式の値 $f(1)$ は約 2.527×10^{25} となる。これは、 $x=1$ において $f(x)$ はそのノルムに比べて極端に実軸に接近しているということが分かる。このような状況で $\alpha=1$ のとき $|f(\alpha)|/\|f\|$ は約 5.8×10^{-11} となり、 α のまわりの穴は極端に小さくなる。よって、アルゴリズム 3 が停止するためには膨大な繰り返しが必要となってくる。

この例から分かるように本章で示したアルゴリズムは必ずしもうまく働かない。このアルゴリズムでやっていることは多項式の値とノルムの情報からその零点の存在しない領域を計算しているわけで、多項式の構造の情報は他には用いていない。今後、このアルゴリズムを改善するには多項式の構造の情報をある程度とり入れなければならないと思われる。

第 9 章

代数的数の複雑さとその応用

本章では、本論文での中心的話題である穴の理論を等式の証明へ応用する。ここではいくつかの変数をもった方程式系を対象とする。理想的にはこれに対する穴を定義しその穴を解析することであるが、これは今のところ大変困難である。ここでは Hong [Hon86] などのアプローチと同様に最終的に多変数多項式による方程式系を変数消去によって 1 変数多項式へ変換したときの複雑さを見積もっている。しかし、このようにして 1 変数多項式をつくるとその係数は大変大きいものになってしまう。これに対して、本章で示す方法は扱う対象を有理数体および有理数体にある一つの代数的数を加えた体の上の数に限定する。このようにすることにより、Hong の方法のように広い範囲の問題を扱えない代わりに複雑さを小さくすることができる。

本章で扱う代数拡大体はその基底があらかじめ与えられているものと仮定している。

9.1 初等幾何学の定理証明について

本節では [Sch80] の結果に基づいていかにして初等幾何学の定理を証明するかについて説明する。

まず、多変数多項式についてつぎのような性質が成り立つ。

定理 17 ([Sch80]) Q を n 個の変数 x_1, \dots, x_n の多項式であるとする。また Q は恒等的に 0 には等しくないとする。 Q の x_1 に関する次数を d_1 とし Q_2 を Q の $x_1^{d_1}$ の係数多項式とする。つぎに Q_2 の x_2 に関する次数を d_2 とする。このようにして順々に d_1, \dots, d_n を決定する。また一方 I_i ($i = 1, \dots, n$) を実数体上の n 個の有限集合とする。このとき Q は高々

$$|I_1 \times \cdots \times I_n| \left(\frac{d_1}{|I_1|} + \cdots + \frac{d_n}{|I_n|} \right) \quad (9.1)$$

個の零点を $I_1 \times \cdots \times I_n$ にもつ。ただし、 $|\cdot|$ は集合の要素数を表すものとする。

この定理を用いればつぎのことが言える。

系 8 ([Sch80]) 定理 17において $I = I_1 = \dots = I_n$ とし、 d を多項式 Q の全次数とする。また ある十分大きな定数 c について $|I| \geq cd$ が成り立っているとすると、 Q が恒等的に 0 でないとなれば I^n の要素が Q の零点となる確率は $1/c$ 以下である。

よって、十分大きく I をとって何回か Q の値を計算しそれが 0 に等しいということが確かめられれば、 Q が恒等的に 0 に等しいということが確率的に証明できる。すなわち、 n 回計算した結果がすべて 0 に等しい場合、それらが偶然に Q の零点である確率は c^{-n} ということになる。

9.2 初等幾何学の定理の計算過程

まず、はじめに幾何学の定理の証明アルゴリズムを説明するために計算過程を定義する。計算過程は本章で取り扱う幾何学の定理をもっと一般的にした問題のクラスである。

定義 9 入力変数 x_1, x_2, \dots, x_m をもつ計算過程とは n 個の順序のついた整係数多変数多項式の組 f_1, f_2, \dots, f_n で、つぎのような条件を満たすものである： 任意のインデックス i ($1 \leq i \leq n$) について f_i は f_1, \dots, f_{i-1} のなかに出現しないちょうど 1 つの入力変数でない変数を含む。(f_1, \dots, f_{i-1} のなかに出現した入力変数以外の変数をこの個数は 0 でもよい。) このとき f_n の入力変数でない、 f_1, f_2, \dots, f_{n-1} のなかに出現しない変数をこの計算過程の出力変数と呼ぶ。入力変数でも出力変数でも変数を中間変数と呼ぶ。

例 9 つぎのような多項式列は計算過程である。

$$f_1 = x_1^2 - 2 + y = 0,$$

$$f_2 = x_2^2 - 3 = 0,$$

$$f_3 = x_1 - \lambda x_2 = 0.$$

この計算過程では入力変数は y で出力変数は λ である。 x_1, x_2 は中間変数である。

計算過程は定義より必ずループのないグラフとして表現することができる。上の例をグラフとして書けば Fig. 9.1 となる。

定義より入力変数にある値を入れると出力変数の値が確定する。ここではこの論文で考える初等幾何学の定理の証明への応用の方法の概略を述べる。ここで扱う初等幾何学の定理はその定理に対応する計算過程が存在して、その定理が正しいことと、その計算過程の入力変数にどのような値を代入しても出力変数が 0 となることが同値であるとする。初等幾何学のある定理が与えられたとき、それを証明するのにつぎのようなステップを踏む。

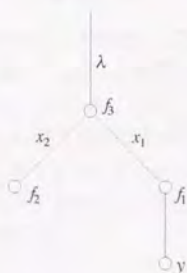


Fig. 9.1. 計算過程を表現するグラフ

1. 与えられた定理に対応する計算過程を A とする
2. 計算過程 A の中間的な変数を終結式 [vdW37] によって消去したときのの人力変数に関する全次数の上界を見積もる。このとき、実際に終結式を計算するのではなく、用いられてる変数と多項式の係数および次数から見積もる。
3. 系 8 を用いるために入力変数へ代入する有理数の組を適当に決定する。
4. その有理数の組を実際に代入して目的の出力変数の値を代入した場合最終的にその値がどの程度の「複雑さ」となるかを計算する。(複雑さについてはつぎの節で述べる.)
5. 求めた複雑さを基に計算すべき精度を見積り、その精度で出力変数を数値計算する。その値がその複雑さからみて十分に 0 に近ければこの入力に対して出力は正確に 0 であるということが証明できる。
6. この操作を十分な回数繰り返す。1 回でも出力が 0 でなければ定理は成り立たないことが証明できる。一方、すべての場合に出力が 0 であれば、高い確率で与えられた定理が正しいことが証明できる。

本論文では方程式を作る部分については詳しく述べず、本節の最後に簡単な例を示すにとどめる。(変数の消去などを含めた定理の計算過程については [山本 89] を参照)。基本的な方法としてはたとえば三角形に関する定理であれば三角形を記述する点 (x_1, x_2) , (x_3, x_4) , (x_5, x_6) を変数として含む多項式を作る。ただし、角の 2 等分など代数拡大を伴うものについては

$$f_1(x, t) = 0,$$

$$f_2(x, t, y) = 0$$

のような形になるのでこれは終結式によって変数 t を消去する、すなわち、 $\text{Res}_t(f_1, f_2) = 0$ という式で表すことができる。ただし、 x は入力変数のベクトルであり、 y は出力変数を表す。この式は x と y の方程式ということになる。ここで、この方程式が恒等的に $y = 0$ という解を持つことは、この方程式の y に関する定数項が恒等的に 0 であることと同値である。よって、この場合も Schwartz の方法を用いることができる。

本論文では Schwartz の方法におけるそれぞれの有理数の入力について、いかに数値的に多項式の恒等性を示すかについて論じる。

例 10 「三角形の三つの角のそれぞれの 2 等分線は一点で交わる」という命題について考える。ここで三角形は Fig. 9.2 で示す (x, y) を変数として決まるものとする。このように三角形を定義するということは、この命題が縮尺に対して不変であることを暗黙に仮定している。このように定義すると、それぞれの角の 2 等分線とその相対する辺との交点をそれぞれ (x_1, y_1) , (x_2, y_2) , (x_3, y_3) とすればこれらは、まず、

$$\begin{aligned} f_1 &= x^2 + y^2 - t^2 = 0 \\ f_2 &= (x-1)^2 + y^2 - s^2 = 0 \end{aligned}$$

とにおいて、

$$\begin{aligned} f_3 &= (1+t)x_1 - (t+x) = 0, \\ f_4 &= (1+t)y_1 - y = 0, \\ f_5 &= (1+s)x_2 - x = 0, \\ f_6 &= (1+s)y_2 - y = 0, \\ f_7 &= (t+s)x_3 - t = 0, \\ f_8 &= y_3 = 0 \end{aligned}$$

と書ける。この 3 点と $(u_1, v_1) = (0, 0)$, $(u_2, v_2) = (1, 0)$, $(u_3, v_3) = (x, y)$ をそれぞれ結んだ 3 線が一点で交わることを示せばよい。これは

$$f_9 = \begin{vmatrix} y_1 - v_1 & x_1 - u_1 & x_1 v_1 - y_1 u_1 \\ y_2 - v_2 & x_2 - u_2 & x_2 v_2 - y_2 u_2 \\ y_3 - v_3 & x_3 - u_3 & x_3 v_3 - y_3 u_3 \end{vmatrix} - \lambda = 0$$

としたとき、 $\lambda = 0$ が成り立つことと同値である。ここで示した方程式系 $f_1 = 0, f_2 = 0, \dots, f_9 = 0$ は入力変数を (x, y) として、出力変数を λ とする計算過程となっている。この計算過程に対応するグラフは Fig. 9.3 となる。

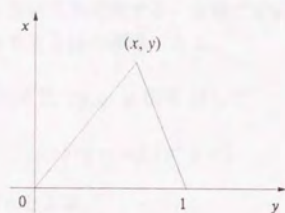


Fig. 9.2. 三角形の表現

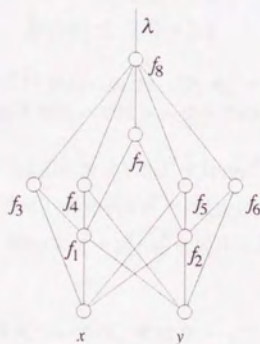


Fig. 9.3. 例 10 の計算過程を表現するグラフ

9.3 数の複雑さの定義と有理数の四則演算による複雑さの解析

本節では、ここで扱う数の複雑さを定義する。本章で定義する数は有理数体のある一つの代数的数によって拡大してできる体の要素である。

定義 10 有理数 $r = p/q$ ($p, q \in \mathbb{Z}$, $(p, q) \neq 0$) に対して

$$\|r\| = \log_2(p^2 + q^2) \quad (9.2)$$

と定義する。これを r の複雑さとよぶ。

この定義では複雑さをベクトルのユークリッドノルムの対数のようなもので定義している。この定義は不自然のように見えるが、つぎに示すように、このようにすることによってシュワルツの不等式が使える、比較的単純な見積りができる。この定義に基づいて有理数の四則演算によってどの程度複雑さが増すかということについて考える。

補助定理 34 有理数 r, s の複雑さについて次の不等式が成り立つ。

$$\|r \pm s\| \leq \|r\| + \|s\| + 1, \quad (9.3)$$

$$\|rs\| \leq \|r\| + \|s\|, \quad (9.4)$$

$$\|r/s\| \leq \|r\| + \|s\|. \quad (9.5)$$

証明 二つの数を r, s がそれぞれ $q_1/p_1, q_2/p_2$, $((p_1, q_1) = 1, (q_2, p_2) = 1)$ と表されているとする。このとき和と差の複雑さについてはシュワルツの不等式を用いて

$$\begin{aligned} \|r \pm s\| &\leq \log_2((q_1 p_2 \pm q_2 p_1)^2 + (p_1 p_2)^2) \\ &\leq \log_2((q_1^2 + p_1^2)(q_2^2 + p_2^2) + (p_1 p_2)^2) \\ &\leq \log_2(2(q_1^2 + p_1^2)(q_2^2 + p_2^2)) = \|r\| + \|s\| + 1 \end{aligned}$$

と成り立つ。また、積の複雑さについては、やはりシュワルツの不等式を用いてつぎのように見積もれる。

$$\|rs\| \leq \log_2((q_1 q_2)^2 + (p_2 p_1)^2) \leq \log_2((q_1^2 + p_1^2)(q_2^2 + p_2^2)) = \|r\| + \|s\|.$$

商についても積と同様である。

□

また、さらに有理数を要素とする行列の複雑さをつぎのように定義する。

定義 11 行列 $M = (a_{i,j})_{i=1,\dots,n, j=1,\dots,m}$ の複雑さを $\|M\|$ と記し,

$$\|M\| = \sum_{i=1}^n \sum_{j=1}^m \|a_{i,j}\| \quad (9.6)$$

と定義する. ただし, $a_{i,j} \in \mathbb{Q}$ とする.

つぎに, 二つの行列の積の複雑さについて考える.

補助定理 35 二つの有理数体上の $n \times m$ 行列および $m \times l$ 行列をそれぞれ M, N とおく. このとき

$$\|MN\| \leq nml + l\|M\| + n\|N\| \quad (9.7)$$

が成り立つ.

証明 $M = (a_{i,j})_{i=1,\dots,n, j=1,\dots,m}$, $N = (b_{i,j})_{i=1,\dots,m, k=1,\dots,l}$ とおく. このとき補助定理 34 を用いて

$$\begin{aligned} \|MN\| &= \left\| \left(\sum_{j=1}^m a_{i,j} b_{j,k} \right)_{i=1,\dots,n, k=1,\dots,l} \right\| = \sum_{i=1}^n \sum_{k=1}^l \left\| \sum_{j=1}^m a_{i,j} b_{j,k} \right\| \\ &\leq \sum_{i=1}^n \sum_{k=1}^l \left(m - 1 + \sum_{j=1}^m (\|a_{i,j}\| + \|b_{j,k}\|) \right) \leq nlm + l\|M\| + n\|N\| \end{aligned}$$

を得る. \square

また, さらに行列式の複雑さはつぎのように見積もることができる.

補助定理 36 M を $n \times n$ 有理行列とする. このとき M の行列式の複雑さについてつぎの不等式が成り立つ.

$$\|\det M\| \leq 2n \log_2 n + \|M\| + C. \quad (9.8)$$

ただし, $n = 2$ の場合 C は 0.2 以下のある定数であり, $n \geq 3$ の場合 C は負の数である.

証明 $M = (q_{i,j}/p_{i,j})_{i,j=1,\dots,n}$ ($q_{i,j}, p_{i,j} \in \mathbb{Z}$, $(p_{i,j}, q_{i,j}) = 1$) とおき, また, $\det M = q/p$ ($q, p \in \mathbb{Z}$, $(p, q) = 1$) とおく. このとき $|p| \leq \prod_{i=1}^n \prod_{j=1}^n |p_{i,j}|$ であり, また, さらに $|q| \leq n! \prod_{i=1}^n \prod_{j=1}^n \tilde{q}_{i,j}$ である. ただし, $\tilde{q}_{i,j} = \max(|q_{i,j}|, |p_{i,j}|)$ である. これより

$$\begin{aligned} \|\det M\| &\leq \log_2(p^2 + q^2) \leq \log_2 \left((n!)^2 \prod_{i=1}^n \prod_{j=1}^n \tilde{q}_{i,j}^2 + \prod_{i=1}^n \prod_{j=1}^n |p_{i,j}|^2 \right) \\ &\leq 2 \log_2 n! + \log_2 \left(\prod_{i=1}^n \prod_{j=1}^n \tilde{q}_{i,j}^2 + \prod_{i=1}^n \prod_{j=1}^n |p_{i,j}|^2 \right) \leq 2 \log_2 n! + \log_2(2 \tilde{q}_{i,j}^2) \\ &\leq 2 \log_2 n! + \log_2 \tilde{q}_{i,j}^2 + 1 \leq 2 \log_2 n! + \log_2 \prod_{i=1}^n \prod_{j=1}^n (|q_{i,j}|^2 + |p_{i,j}|^2) + 1 \\ &\leq 2 \log_2 n! + \|M\| + 1 \leq 2n \log_2 n + \|M\| + C \end{aligned}$$

である。ここでスターリングの公式より、 $C = 2 + \log_2 \pi - (2 \log_2 e)n + \frac{1}{2} \log_2 n$ と表すことができる。これは $n = 2$ のとき約 0.15 であり $n \geq 3$ では $C < 0$ である。これより補助定理は証明された。□

また、さらにこの結果を用いると、線形方程式の解についてつぎの性質が成り立つ。

補助定理 37 M を $n \times n$ 有理行列とし、 b を長さ n のベクトルとする。このとき線形方程式 $Mx = b$ の解 x の一つの要素を x_i とおけば

$$\|x_i\| \leq 4n \log_2 n + 2\|M\| + \|b\| + 2C \quad (9.9)$$

とかけ、ここで C は補助定理 36 と同じ定数である。

証明 クラメル公式より $x_i = \det M_i / \det M$ と書くことができる。ここで M_i は行列 M のある行を b で置き換えたものである。よって $\|M_i\| \leq \|M\| + \|b\|$ と評価することができる。これを用いて補助定理 34、補助定理 36 を用いて補助定理を得る。□

有理数に関する似たような議論は [Sch86] にもみられるが、若干定義が異なる。

つぎに本節の前半で示した公式を用いて実際に良く知られた初等幾何学の定理を証明する手順について示す。まず、実際の問題について考える前にある有理数の複雑さの上界が分かったときどの程度の精度で数値的に計算すれば、その数が本当に 0 といえるかということについて考える。

補助定理 38 ある有理数 r の複雑さの上界が M であるとき r が 0 に等しいかどうかを数値的に判定するには r を精度 $2^{-(M/2+1)}$ で計算すれば十分である。また、 r が 1 に等しいかどうかを判定するには精度 $2^{-(M/2+2)}$ で計算すれば十分である。

証明 $r = p/q$ とおけば r は $qx - p = 0$ という方程式の根となる。系 4 を用いれば $r \neq 0$ ならば $|r| > 1/\sqrt{p^2 + q^2}$ であり、従って複雑さの定義より $|r| > 2^{-M/2}$ となる。またさらに r が 1 かどうかの判定については $s = r - 1$ が $px + (q - p) = 0$ という方程式を満たすことから $p^2 + (q - p)^2 \leq 4 \cdot 2^M$ より、 $s \neq 0$ ならば $|s| > 2^{-(M/2+1)}$ となる。以上より本補助定理を得る。□

以上よりある数が 0 であるかまたは 1 であるかの判定は数値的に行なえることが分かった。ここでつぎのような初等幾何学の定理を証明するプロセスを考える。

定理 18 三角形の 3 つの中線は一点で交わる。

この定理を定式化するためにつぎのような補助定理を示す。

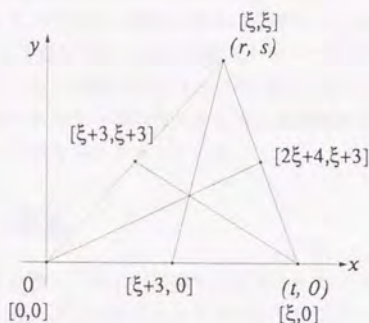


Fig. 9.4. 定理 18 の証明に用いる三角形 ($[\cdot, \cdot]$ は点の複雑さを表している)

補助定理 39 有理数を座標とする 6 つの点 $P_i = (r_i, s_i)$, $(i = 1, \dots, 6)$ が与えられたとき直線 P_1P_2 , P_3P_4 , P_5P_6 が一点で交わる必要十分条件はつぎの行列式が 0 に等しいことである.

$$\begin{vmatrix} s_2 - s_1 & r_2 - r_1 & s_1 r_2 - s_2 r_1 \\ s_4 - s_3 & r_4 - r_3 & s_3 r_4 - s_4 r_3 \\ s_6 - s_5 & r_6 - r_5 & s_5 r_6 - s_6 r_5 \end{vmatrix} = 0. \quad (9.10)$$

証明 略.

□

上の結果を Schwartz の結果 [Sch80] と組み合わせるといくつかの例について定理 18 が成り立つことが示せれば、これが一般的に正しい定理であることが確率的に証明できる。この場合、図 9.4 のような形で定式化する。まず判定に用いる多項式 Q の変数は r, s および t である。これらを動かすことによってすべての三角形が表現できる。また一点で三つの直線が交わることは補助定理 39 によって判定できる。この補助定理で与えられている行列式の r_i, s_i に代入されるべき式は明らかに r, s, t の 1 次式である。よって Q の全次数は高々 4 次である。このことから、系 8 を用いれば、たとえば $I = \{i/100000 \mid i = 0, 1, \dots, 99999\}$ とおけば $|I| = 100000$ であり、この中から r, s, t の値を選んで Q 恒等的に 0 でないのに Q の値が 0 になる確率は高々 $1/25000$ である。よってこれを何回か繰り返せば Q が恒等的に 0 であることが確率的に示される。このときそれぞれの値についてそれが正確に正しいことを本節の方法に従って数値的に証明するにはその計算過程について考えれば良い。すなわち入力される数の複雑さは高々 $\xi = \log_2(2 \cdot 100000^2) = 34.219$ である。また $\|0\| = 0$, $\|2\| = \log_2 5 < 3$ であることを考えれば補助定理 34 を用いて Fig. 9.4 に示した複雑さとな

る。よって、これより補助定理 39 によって示された行列式の行列の複雑さは高々 $18\xi + 39$ ということになる。よって、行列式の複雑さは補助定理 36 より $18\xi + 51$ である。これは大体 666.94 である。これより最終的な行列式の精度を $2^{-334.47}$ 程度にすれば本当に正しいかどうか判定できる。これは 10 進数で考えると小数点以下 100 桁程度であり、これは十分に実行可能である。実際に計算する場合はそれぞれの数の複雑さはもっと小さくなるので必要な精度もこれよりも小さくなると考えられる。

9.4 代数体上の演算

前節において有理数の演算についての複雑さの見積りについて論じた。本節では同様の議論をある一つの代数的数によって拡大された体の演算に拡張して論じる。ここで述べる拡大体はその基底があらかじめ与えられているものとする。

まず、はじめに代数体上の代数的数の複雑さをつぎのように定義する。この複雑さは拡大体に普遍なものではなく、拡大するとき用いる代数的数を変更すると変わるものである。

定義 12 ある代数的数を α とし、これを定義する多項式を $f(x) = \sum_{i=0}^n a_i x^i$ ($a_i \in \mathbb{Z}$) とする。すなわち $f(\alpha) = 0$ である (必ずしも最小多項式でなくてもよい)。さらに $\mathbb{Q}(\alpha)$ 上の数 β が

$$\beta = \sum_{i=0}^{n-1} b_i \alpha^i \quad (b_i \in \mathbb{Q}) \quad (9.11)$$

と書けるとする。このとき数 β の複雑さを $\|\beta\|_\alpha$ と記し

$$\|\beta\|_\alpha = \sum_{i=0}^{n-1} \|b_i\| \quad (9.12)$$

と定義する。

本節では代数拡大を行なうものとなる数を α とし、その定義多項式を $f(x) = \sum_{i=0}^n a_i x^i$, ($a_i \in \mathbb{Z}, i = 0, \dots, n$) とおく。まずつぎの性質が成り立つ。

補助定理 40 α^{i+n} をつぎのように表現する：

$$\alpha^{i+n} = \frac{1}{a_n^{i+1}} \sum_{j=0}^{n-1} a_{i,j} \alpha^j \quad (i = 0, 1, \dots), \quad (a_{i,j} \in \mathbb{Z}). \quad (9.13)$$

$B = \sum_{i=0}^n a_i^2$ とおけば、

$$\sum_{j=0}^n a_{i,j}^2 \leq B^{i+1} \quad (i = 0, 1, \dots). \quad (9.14)$$

証明 はじめに α の定義より $\alpha^n = -(1/a_n)(a_{n-1}\alpha^{n-1} + \cdots + a_0)$ である。よって $i=0$ に関してこの補助定理は成り立つ。また、 $\mathbb{Q}(\alpha)$ 上の数を δ とおけば $\delta = d_{n-1}\alpha^{n-1} + \cdots + d_0$ ($d_i \in \mathbb{Q}$) と表現できる。このとき $\gamma = \alpha\delta = d_{n-1}\alpha^n + \cdots + d_0\alpha = d_{n-1}(-(1/a_n)(a_{n-1}\alpha^{n-1} + \cdots + a_0)) + (d_{n-2}\alpha^{n-1} + \cdots + d_0\alpha)$ である。ここで δ と γ を $(\alpha^0, \dots, \alpha^{n-1})$ を基底とするベクトルで表現する。 δ と γ に対応するベクトルをそれぞれ $(d_0, \dots, d_{n-1})^T$ と $(e_0, \dots, e_{n-1})^T$ とおけば、

$$a_n \begin{pmatrix} e_0 \\ \vdots \\ e_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 0 & -a_0 \\ a_n & \ddots & \vdots \\ & \ddots & 0 & \vdots \\ 0 & & a_n & -a_{n-1} \end{pmatrix} \begin{pmatrix} d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} \quad (9.15)$$

が得られる。ここでこの式の右辺の $n \times n$ 行列の固有値 λ を考える。この行列の固有方程式は

$$\Phi(t) = a_n^n \left[\left(\frac{t}{a_n} \right)^n + \left(\frac{a_{n-1}}{a_n} \right) \left(\frac{t}{a_n} \right)^{n-1} + \cdots + \left(\frac{a_1}{a_n} \right) \left(\frac{t}{a_n} \right) + \left(\frac{a_0}{a_n} \right) \right] \quad (9.16)$$

となり、定理2より λ についてつぎのような式が成り立つ。

$$\left| \frac{\lambda}{a_n} \right| \leq \left(1^2 + \left(\frac{a_{n-1}}{a_n} \right)^2 + \cdots + \left(\frac{a_0}{a_n} \right)^2 \right)^{1/2}. \quad (9.17)$$

これより $|\lambda| \leq \sqrt{B}$ である。式9.15より $a_{i,j}$ が整数であることはあきらかであり、 $|\lambda|$ の大きさから $\sum_{i=0}^n a_{i,j}^2 \leq B^{i+1}$ であることが証明された。□

この性質を用いて $\mathbb{Q}(\alpha)$ 上の二つの数の四則演算における複雑さの増大について見積もる。まず、有理数と $\mathbb{Q}(\alpha)$ との演算についてはつぎの性質が成り立つ。

補助定理 41 β を $\mathbb{Q}(\alpha)$ の要素とし、 r を有理数とする。このとき

$$\|\beta \pm r\|_\alpha \leq \|r\| + \|\beta\|_\alpha + 1, \quad (9.18)$$

$$\|\beta r\|_\alpha \leq n\|r\| + \|\beta\|_\alpha, \quad (9.19)$$

$$\|\beta/r\|_\alpha \leq n\|r\| + \|\beta\|_\alpha. \quad (9.20)$$

証明 代数的数の複雑さの定義と補助定理34より明らかである。□

また、二つの代数的数に対してはつぎの性質が成り立つ。

補助定理 42 二つの $\mathbb{Q}(\alpha)$ 上の代数的数を β_1 と β_2 とする。また、 B は補助定理40での定義と同様であるとする。このとき

$$\|\beta_1 + \beta_2\|_\alpha \leq \|\beta_1\|_\alpha + \|\beta_2\|_\alpha + n \quad (9.21)$$

であり,

$$\|\beta_1 \cdot \beta_2\|_\alpha \leq \frac{n(2n+1)(n-1)}{2} + n^2(\|\beta_1\|_\alpha + \|\beta_2\|_\alpha) + \frac{n^2(n-1)(n+1)}{6} \log_2 B \quad (9.22)$$

である.

証明 和に関しては補助定理 34 より明らかである. ここで $\beta_j = \sum_{i=0}^{n-1} r_{j,i} \alpha^i$, ($j=1, 2$) とおけば, 積 $\beta_1 \cdot \beta_2$ については補助定理 40 の $a_{i,j}$ を用いてつぎのように変形できる.

$$\begin{aligned} \beta_1 \cdot \beta_2 &= \left(\sum_{i=0}^{n-1} r_{1,i} \alpha^i \right) \left(\sum_{j=0}^{n-1} r_{2,j} \alpha^j \right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} r_{1,i} r_{2,j} \alpha^{i+j} \\ &= \left(\sum_{k=0}^{n-1} \sum_{j=0}^k + \sum_{k=n}^{2n-2} \sum_{j=k-n+1}^{n-1} \right) r_{1,k-j} r_{2,j} \alpha^k \\ &= \sum_{k=0}^{n-1} \sum_{j=0}^k r_{1,k-j} r_{2,j} \alpha^k + \sum_{k=n}^{2n-2} \sum_{j=k-n+1}^{n-1} \sum_{l=0}^{n-1} \frac{a_{k-n,l}}{a_n^{k-n+1}} r_{1,k-j} r_{2,j} \alpha^l \end{aligned}$$

この結果より $\|\beta_1 \cdot \beta_2\|_\alpha$ は $l=0, \dots, n-1$ についてつぎのように見積もることができる.

$$\begin{aligned} \|\beta_1 \cdot \beta_2\|_\alpha &\leq \sum_{l=0}^{n-1} \left\| \sum_{j=0}^l r_{1,l-j} r_{2,j} + \sum_{k=n}^{2n-2} \sum_{j=k-n+1}^{n-1} \frac{a_{k-n,l}}{a_n^{k-n+1}} r_{1,k-j} r_{2,j} \right\| \\ &\leq \sum_{l=0}^{n-1} \left(1 + \left\| \sum_{j=0}^l r_{1,l-j} r_{2,j} \right\| + \left\| \sum_{k=n}^{2n-2} \sum_{j=k-n+1}^{n-1} \frac{a_{k-n,l}}{a_n^{k-n+1}} r_{1,k-j} r_{2,j} \right\| \right) \\ &\leq \sum_{l=0}^{n-1} \left[l + 1 + \frac{(n-2)(n+1)}{2} + \sum_{j=0}^l (\|r_{1,l-j}\| + \|r_{2,j}\|) \right. \\ &\quad \left. + \sum_{k=n}^{2n-2} \sum_{j=k-n+1}^{n-1} \left(\left\| \frac{a_{k-n,l}}{a_n^{k-n+1}} \right\| + \|r_{1,k-j}\| + \|r_{2,j}\| \right) \right] \\ &\leq \frac{n(n+1)(n-1)}{2} + n^2(\|\beta_1\|_\alpha + \|\beta_2\|_\alpha) + \sum_{l=0}^{n-1} \sum_{k=n}^{2n-2} \sum_{j=k-n+1}^{n-1} \left\| \frac{a_{k-n,l}}{a_n^{k-n+1}} \right\| \end{aligned}$$

ここで B の定義および補助定理 40 より, $\|a_{k-n,l}/a_n^{k-n+1}\| \leq 1 + (k-n+1) \log_2 B$ であるので

$$\|\beta_1 \cdot \beta_2\|_\alpha \leq \frac{n(2n+1)(n-1)}{2} + n^2(\|\beta_1\|_\alpha + \|\beta_2\|_\alpha) + \frac{n^2(n-1)(n+1)}{6} \log_2 B$$

となる. □

また, さらに逆数についてはつぎのように見積もることができる.

補助定理 43 β を $\mathbb{Q}(\alpha)$ 上の代数的数とする. このとき

$$\|1/\beta\|_{\alpha} \leq n \left[(2n \log_2 n + 2n^2(3n-1) + 1 + 2C) + n^3(n-1) \log_2 B + 2n^2 \|\beta\|_{\alpha} \right]. \quad (9.23)$$

証明 $\gamma\beta = 1$ とする. この等式を補助定理 40 の証明と同様にしてベクトル表示をする. γ, β に対応するベクトルをそれぞれ $(s_0, \dots, s_{n-1})^T, (r_0, \dots, r_{n-1})^T$ とおけば

$$XYZ = (1, 0, \dots, 0)$$

とかける. ただし,

$$X = \begin{pmatrix} 1 & & 0 & a_{0,0}/a_n & a_{1,0}/a_n^2 & \cdots & a_{n-2,0}/a_n^{n-1} \\ & \ddots & & \vdots & \vdots & & \vdots \\ 0 & & 1 & a_{0,n-1}/a_n & a_{1,n-1}/a_n^2 & \cdots & a_{n-2,n-1}/a_n^{n-1} \end{pmatrix},$$

$$Y = \begin{pmatrix} r_0 & & 0 \\ \vdots & \ddots & \\ r_{n-1} & \vdots & r_0 \\ & \ddots & \vdots \\ 0 & & r_{n-1} \end{pmatrix},$$

$$Z = (s_0, \dots, s_{n-1})^T$$

とする. このとき行列 X の複雑さは

$$\begin{aligned} \|X\| &\leq n + \sum_{i=0}^{n-2} \sum_{j=0}^{n-1} \log_2(b_{i,j}^2 + b_n^{2i}) \\ &\leq n + \sum_{i=0}^{n-2} \sum_{j=0}^{n-1} \log_2(B^{i+1} + B^i) \leq n^2 + \frac{n^2(n-1)}{2} \log_2 B \end{aligned}$$

であり, また行列 Y の複雑さは $\|Y\| \leq n\|\beta\|_{\alpha}$ である. これより行列 XY の複雑さは

$$\|XY\| \leq n^2(3n-1) + \frac{n^3(n-1)}{2} \log_2 B + n^2 \|\beta\|_{\alpha}$$

である. これより補助定理 37 を用いて本補助定理を得る. □

以上より代数的数の四則演算による複雑さを見積もることができた.

本論文で扱っているのは, 一つの代数的数によって拡大された体の中の要素に対して複雑さを定義し, それが演算によってどのように大きくなるかということである. 現実の幾何の定理では代数拡大が 1 回ではなく何回も行なわれることがあるので, このような場合には本論文の結果を直接用いることはできない. ここでは 1 回だけ代数拡大が起こる場合を例に挙げて, 本論文の結果がどのように応用できるかを説明する.

まず、はじめにある代数体 $\mathbb{Q}(\alpha)$ の要素の α に関する複雑さの上界が分かっているとき、実際に数値計算結果でどの程度の精度で求めればよいかということについて考える。拡大次数が一般の場合は大変複雑であるのでここでは拡大次数が 2 である場合について考える。

補助定理 44 代数的数 α は $a_2\alpha^2 + a_1\alpha + a_0 = 0$ によって定義されたとする。すなわち $\mathbb{Q}(\alpha)$ の拡大次数は 2 であると仮定する。また、 $a_2^2 + a_1^2 + a_0^2 = B$ とする。このとき $\mathbb{Q}(\alpha)$ の要素 η が正確に 0 であるかどうかを判定するためには精度

$$2^{-(65/4+7\|\eta\|_\alpha+2\log_2 B)} \quad (9.24)$$

で η を計算すればよい。

証明 α は 2 次の数なのでその拡大体の要素である η は $\eta = r_1\alpha + r_0$ とかける。ここで r_1 と r_0 は有理数である。このとき複雑さの定義より $\|\eta\|_\alpha = \|r_1\| + \|r_0\|$ となる。

$$\eta^2 = \left(2r_1r_0 - \frac{a_1}{a_2}r_1^2\right)\alpha + \left(r_0^2 - \frac{a_0}{a_2}r_1^2\right)$$

であるから、 η が $g(x) = x^2 + d_1x + d_0 = 0$ の零点となっているとすると、

$$\begin{pmatrix} 1 & r_0 \\ 0 & r_1 \end{pmatrix} \begin{pmatrix} d_0 \\ d_1 \end{pmatrix} = \begin{pmatrix} r_0^2 - \frac{a_0}{a_2}r_1^2 \\ 2r_1r_0 - \frac{a_1}{a_2}r_1^2 \end{pmatrix}$$

となる。この式の右辺の 2×2 行列の複雑さは $1 + \|\eta\|_\alpha$ であり、また、右辺のベクトルの複雑さは

$$\left\|r_0^2 - \frac{a_0}{a_2}r_1^2\right\| + \left\|2r_1r_0 - \frac{a_1}{a_2}r_1^2\right\| \leq 3 + 5\|\eta\|_\alpha + 2\log_2 B$$

である。従って補助定理 37 より

$$\max(\|d_1\|, \|d_0\|) \leq 27/2 + 7\|\eta\|_\alpha + 2\log_2 B$$

と見積もることができる。これより

$$\sqrt{d_0^2 + d_1^2 + 1^2} \leq 2^{(35/4+7/2\|\eta\|_\alpha+\log_2 B)}$$

であり、さらに

$$|d_0| \geq 2^{-(27/4+7/2\|\eta\|_\alpha+\log_2 B)}$$

である。これより定理 2 を用いて $\eta \neq 0$ ならば

$$|\eta| \geq 2^{-(61/4+7\|\eta\|_\alpha+2\log_2 B)}$$

である。これより本補助定理を得る。 □

本節ではつぎのような初等幾何学の定理を証明することを考える。

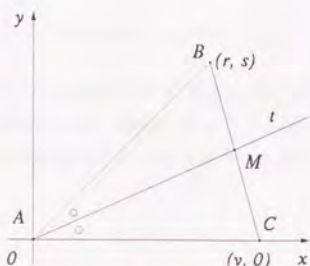


Fig. 9.5. 定理 19 の証明に用いる三角形

定理 19 三角形 ABC の角 A の 2 等分線と相対する辺 BC の交点を M とおくこのとき $\overline{AB} : \overline{AC} = \overline{BM} : \overline{CM}$ である.

この定理は 2 等分線を用いるので 2 次拡大が起こる. この定理を証明するために, 二つのステップを考える. 一つは 2 等分線を引くことの定式化であり, もう一つはそれが定理 19 で示した式を満足するかどうかを判定することである. まずこれを証明するための枠組を Fig. 9.5 に示す. ここでは入力変数として点 B の座標成分 r, s , 二等分線の傾き t を用いる. まず, t については,

$$st^2 + 2rt - s = 0 \quad (9.25)$$

が成り立つ. ここで t は点 C の座標成分 v には依存しない. また, t を用いて, 定理 19 で示した式を満足するかどうかを確かめるために

$$X = (s - rt)^2 - t^2(r^2 + s^2) \quad (9.26)$$

が 0 に等しいかどうかを確かめればよい. よって終結式 $\text{Res}_t(s^2 - 2srt + t^2s^2, X - (s - rt)^2 + t^2(r^2 + s^2))$ が X の式としてどのように表現されるかということが問題になる. この式の X に関する係数はすべて全次数で s, r の 8 次式となる. よって系 8 より $I = \{i \mid i = 0, 1, \dots, 99999\}$ とすれば, X が恒等的には 0 に等しくなっておかつ, s, t, r を I の中から選択して偶然 0 になってしまう確率は高々 $8/100000$ である. よって, これを繰り返せば確率的にこの定理を証明することができる. それぞれの入力の複雑さは高々 $w = 33.3$ である. よってまた式 (9.25) のそれぞれの係数は高々 200000 なので $B \leq 12 \times 10^{10}$ である. これより補助定理 41 および補助定理 42 を用いることにより,

$$\|X\|_\alpha \leq 43 + 64w + 4\log_2 B \leq u = 2322.$$

これより補助定理 44を用いて精度

$$2^{-(65/4+7u+2\log_2 B)} \geq 2^{-16345} \geq 10^{-5000}$$

で計算すれば良い。すなわち、この場合大体 10 進表示で小数点以下 5000 桁程度で計算すれば十分であるということが分かった。実際には入力する数の複雑さはもっと小さくなるのでこの見積もりよりも少ない桁数で十分であると考えられる。

第 10 章

結論

本論文ではまず、1 変数多項式のノルムを定義し、そのノルムを用いて多項式の零点の穴を定義した。この穴はその多項式の零点を含まない複素平面上の領域である。本論文では主につぎのようなノルムを取り扱った。多項式 $f(x)$ を $f(x) = \sum_{i=0}^n a_i x^i$ とおく。

- 2-ノルム。これは多項式の係数をベクトルと考えたときのユークリッドノルムである。すなわち

$$\|f\|_2 = \left(\sum_{i=0}^n a_i^2 \right)^{1/2}$$

のことである。

- 1-ノルム。これは多項式の係数の絶対値の和をノルムと定義するノルムである。すなわち、

$$\|f\|_1 = \sum_{i=0}^n |a_i|$$

で定義される。

- ∞ -ノルム。これは多項式の係数の絶対値の最大値をノルムと定義するようなノルムである。すなわち、

$$\|f\|_\infty = \max_{i=0, \dots, n} |a_i|$$

一方、多項式 $f(x)$ の穴はつぎのように定義される。

$$H_{\alpha, f} = \left\{ \beta \in \mathbb{R} \mid \max_{h(x) \in P(\beta)} |h(\alpha)| < \frac{|f(\alpha)|}{\|f\|} \right\}.$$

ただし、

$$P(\beta) = \left\{ h(x) \in K[x] \mid \deg h \leq n, h(\beta) = 0, \|h\| \leq 1 \right\}$$

Table 10.1. それぞれのノルムに関する 0 のまわりの穴の解析によって得られる零点の存在しない領域を記述する述語

	2-ノルム	1-ノルム	∞ -ノルム
Q_1	$ \beta \leq 1/M$	$ \beta < \begin{cases} 1/(M-1) & M > 2 \\ 1 & M \leq 2 \end{cases}$	$ \beta \leq 1/(M+1)$
Q_2	$ \beta \leq 1/\sqrt{M}$	$ \beta < \begin{cases} 1/\sqrt{M-1} & M > 2 \\ \beta \leq 1 & M \leq 2 \end{cases}$	$1/(\sqrt{M}+1)$
Q_3	$ \beta \leq 1/M$	$ \beta < \begin{cases} 1/(M-1) & M > 2 \\ 1 & M \leq 2 \end{cases}$	$ \beta \leq 1/(M+1)$

である。

第3章, 第4章, 第5章においてそれぞれのノルムに関する多項式の零点の0のまわりの穴について解析した。2-ノルムについては穴は陽な形に書くことができ, 比較的容易に解析することができる。また1-ノルム および ∞ -ノルムについては係数体 K が実数である場合には線形計画問題となり, 複素数の場合には非線形計画問題となる。0のまわりの穴を解析することによりつぎのような結果を得た。多項式 $f(x)$ の零点は $M = \|f\|/f(0)$ とおいたとき $K = \mathbb{R}$ のときは零点を含まない領域としてつぎのようなものが得られた

$$\widetilde{H}_0 = \left\{ \beta \in \mathbb{R} \mid Q_1 \right\} \cup \left\{ \beta \in \mathbb{C} \setminus \mathbb{R} \mid Q_2 \right\}$$

ただし, Q_1, Q_2 は Table 10.1 に示す述語である。また, $K = \mathbb{C}$ の場合はつぎのような領域が $f(x)$ の零点を含まない

$$\widetilde{H}_0 = \left\{ \beta \in \mathbb{C} \mid Q_3 \right\}$$

ただし Q_3 は Table 10.1 に示す述語である。これらの領域は穴の部分集合になっているものであって穴そのものではない。2-ノルムの結果については Landau の不等式を用いることによって同様の結果を得ることが出来, また ∞ -ノルムについては Cauchy の不等式や Mignotte による結果と一致してる。1-ノルムについての結果は穴によってはじめて得られたものである。

また, 第3章および第4章においてそれぞれ2-ノルムと1-ノルムの $M = \|f\|/|f(\alpha)|$ が十分に大きいとき $K = \mathbb{C}$ の場合は任意の α のまわりの穴について, $K = \mathbb{R}$ の場合は任意の実数 α のまわりの穴について, その漸近的な形を解析した。2-ノルムについてはもともと穴は具体的な式で記述することができるので, 比較的容易に漸近的な形を求めることができる。2-ノルムについては $K = \mathbb{C}$ の場合, 穴は α を中心とする円に近づき, その半径は $\Theta(1/M)$ であり, $K = \mathbb{R}$ の場合は穴は α を中心とする実軸上の区間と α を中心とする実軸

を含まない円に漸近的にちかづく。ここで区間の半径（区間の幅の半分の長さ）は $\Theta(1/M)$ であり、円の半径は $\Theta(1/\sqrt{M})$ となる。一方扱うノルムが 1-ノルムの場合は $K = \mathbb{R}$ の場合については線形計画問題となり、やはり 2-ノルムの場合と同様にして α を中心とする実軸上の区間と α を中心とする実軸を含まない円に漸近的にちかづく。また区間と円の半径はそれぞれ $\Theta(1/M)$ と $\Theta(1/\sqrt{M})$ である。しかし、 $K = \mathbb{C}$ の場合には単純にこのような性質を導くことができない。それは、還元される計画問題が線形でなくなるからである。しかし、

$$|\alpha| \geq \frac{\sqrt{2}+1}{2}n$$

または

$$|\alpha| \leq \frac{2}{(\sqrt{2}+1)n}$$

となっている場合にはやはりその半径が $\Theta(1/M)$ の円に近づく。

また、第 6 章においては整数を係数とする多項式について 2-ノルムについて考察した。ノルムによって制限された整係数多項式とその零点の集合をつぎのように定義した。

$$\begin{aligned} Z(M, n) &= \left\{ \alpha \mid f(\alpha) = 0, f(x) \in P(M, n) \right\}, \\ P(M, n) &= \left\{ f(x) \in \mathbb{Z}[x] \mid \|f\|_2 \leq M, \deg f \leq n, \right. \\ &\quad \left. f(x) \text{ は } \mathbb{Z} \text{ 上で既約な多項式である.} \right\} \end{aligned}$$

零点の集合 $Z(M, n)$ の中の零点の存在しない領域については穴によって説明することができる。また、 $P(M, n)$ の定義のなかに「 $f(x)$ は \mathbb{Z} 上で既約な多項式である」という条件があるが、これは α が有理数であるとき、多項式 $f(x)$ がすでに α を零点としてもってなおかつ別の零点を持つということがないようにするためである。

ここで

$$H_\alpha(N) = \left\{ \alpha \in \mathbb{C} \mid \max_{h(x) \in P(\beta)} |h(\alpha)| < N \right\},$$

ただし、

$$P(\beta) = \left\{ h(x) \in K[x] \mid \deg h \leq n, h(\beta) = 0, \|h\| = 1 \right\}$$

とおく。このような定義のもとで α が有理数であれば、

$$Z(M, n) \cap H_\alpha \left(\frac{1}{M \operatorname{Den}(\alpha)^n} \right) = \begin{cases} \{\alpha\} & \alpha \in Z(M, n) \\ \emptyset & \alpha \notin Z(M, n) \end{cases} \quad (10.1)$$

が成り立つ. また, 既約でない多項式とその零点の集合をつぎのように定義する.

$$\begin{aligned} Z^{\text{ext}}(M, n) &= \left\{ \alpha \mid f(\alpha) = 0, f(x) \in P(M, n) \right\}, \\ P^{\text{ext}}(M, n) &= \left\{ f(x) \in \mathbb{Z}[x] \mid \|f\|_2 \leq M, \deg f \leq n, \right. \\ &\quad \left. f(x) \text{ は } \mathbb{Z} \text{ 上で既約な多項式である.} \right\} \end{aligned}$$

このとき 2-ノルムについては α が 1 でない有理数であれば式 (10.1) が成り立つ. また, さらに $Z(M, n)$ については M を固定して次数 n を大きくしてゆくと, 有界な範囲の中に無限個の点が存在するようになる. この極限 (すなわち次数の条件を外したような集合) を $Z(M, \infty)$ と書くと, $\alpha \in \mathbb{Q} \setminus (Z(M, \infty) \setminus \{0\})$ について $Z(M, \infty) \setminus \{\alpha\}$ のなかの列で α へ収束するものは存在しない. この結果よりたとえば $Z(5, \infty)$ は 5 を要素として含まないので, $Z(5, \infty)$ のなかの点列で 5 へ収束するものは存在しないことがわかる. すなわちいくら次数 n を上げても $Z(5, n)$ の点を 5 へ限りなくちかづけることは不可能であることが分かる. これに対して 5 のまわりの穴はこの場合も次数 n が大きくなれば 5 のまわりで小さくなってゆく. 従ってこの場合穴は現実の分布をうまく説明できないことになる.

第 7 章においては, 複数の零点の 0 のまわりの穴を 2-ノルムおよび 1-ノルムについて解析した. 2-ノルムについては 0 のまわりの穴を解析することによって Landau の不等式の別証を得た. また, 1-ノルムについては扱う多項式 $f(x)$ が条件

$$\frac{\|f\|_1}{|f(0)|} \geq 1$$

を満たすとき, 任意の二つの零点 β_1, β_2 について

$$|\beta_1 \beta_2| \geq \left(\frac{\|f\|_1}{|f(0)|} - 1 \right)^{-1}$$

が成り立つことが分かった. これは二つの零点についての穴を解析した結果であるが, 一般の 1 個の零点について同じような性質が成り立つかどうかは不明である.

第 8 章においては, 整係数多項式 $f(x)$ が与えられたとき 2-ノルムについて任意の実数のまわりの穴がある程度大きくなると無限遠点を含むような領域になるという性質を示した. この性質を用いることによって, $f(x)$ が実数を零点として持たない場合, そのことを証明するためのアルゴリズムを作ることができる. このアルゴリズムについて, その計算の複雑さはまだよくわからない. しかし, このアルゴリズムは万能ではなく, 特に $\|f\| \gg |c_f|$ のような状況では大変効率悪いことが分かっている.

第 9 章においては初等幾何学の定理をある自由変数 r_1, \dots, r_l を含む方程式系として書き表したときその方程式系が r_1, \dots, r_l の任意の値に対しての正確に 0 となることを示すのに

どの程度の演算精度を必要とするかということについて論じた。特に扱う方程式系が、四則演算のみで構成できる場合や、一回だけ代数拡大を許すような場合について必要精度の限界を見積もった。これを用いることにより数値的にいくつかの初等幾何学の定理を証明することができる。しかし、一般的な複数の代数拡大が起こる場合に対して計算時間がかかりすぎるためには応用することはできない。

本論文では穴という概念を中心に多項式の零点の限界について論じた。このような概念が有用であるかどうかについてはさらに研究が必要であるが、少なくともいままで知られている零点の限界を一つの統一的方法論から導くことができた。また、このような穴を実際に任意の実数のまわりについてローカルに計算することを繰り返すことにより実軸についてグローバルな零点の存在しない領域を作ることが可能であるということもわかった。しかし、これらの方法はそのままではまだ強力なものとは言えず、さらにいろいろな改良が必要であると考えられる。

謝辞

本論文を執筆するにあたり 東京大学大学院工学系研究科計数工学専攻 杉原厚吉 教授には懇切丁寧な御指導をいただきました。深く感謝申し上げます。

また、東京大学名誉教授（中央大学教授）伊理正夫 先生には本研究の初期の段階からいろいろ御指導いただきました。心から感謝申し上げます。

また、さらに、東京工業大学情報理工学研究科数理計算科学専攻 小林孝次郎 教授には長年にわたり、いろいろな面で御指導いただきました。深く感謝申し上げます。

東京大学大学院工学系研究科物理学専攻 杉原正顕 助教授には、2-ノルムにおける穴の記述がグラムの行列式を用いることによって単純に表現できることを指摘していただきました。また、東京大学大学院工学系研究科計数工学専攻 伏見正則 教授、岡部靖憲 教授、速水謙 助教授 には貴重なコメントを頂きました。心から感謝申し上げます。

参考文献

- [BBEM90] Beauzamy, B., Bombieri, E., Enflo, P., and Montgomery, H. L.: Products of polynomials in many variables. *Journal of Number Theory*, Vol. 36, pp. 219–245, 1990.
- [Bro78] W. S. Brown: The subresultant PRS Algorithm. *ACM Trans. Math. Soft.*, Vol. 4, No. 3, pp. 237–249, 1978.
- [Cau91] A. L. Cauchy: *Exercices de mathématiques, quatrième année, de bure frères, 1829*, Oeuvres Ser II, Vol. IX, Gauthier-Villars, Paris, 1891.
- [CH31] Courant, R. and Hilbert, D.: *Methoden der Mathematischen Physik*. Springer, 1931.
- [Hon86] J. W. Hong: Proving by Example and Gap Theorem. In *27th Annual Symposium on Foundations of Computer Science, Tronto, Ontario*, pp. 107–116. IEEE Computer Society Press, 1986.
- [Lan05] E. Landau: Sur quelques théorèmes de M. Petrovic relatifs aux zéros des fonctions analytiques. *Bull. Soc. Math. France*, Vol. 33, pp. 251–261, 1905.
- [Len83] A. K. Lenstra: Factoring polynomials over algebraic number fields. In *Proc. EUROCAL 83*, volume 144 of *Springer Lecture Notes in Computer Science*, pp. 251–261, Berlin Heidelberg-New York, 1983. Springer-Verlag.
- [LLL82] Lenstra, A. K., Lenstra, H. W., and Lovász, L.: Factoring polynomials with rational coefficients. *Math. Ann.*, Vol. 261, pp. 515–534, 1982.
- [Mar49] M. Marden: The Geometry of the Zeros of Polynomial in Complex Variables. Volume 3 of *Math. Surveys*. AMS, Providence, Rhode Island, 1949.

- [Mig74] M. Mignotte: An inequality about factors of polynomials. *Mathematics of Computation*, Vol. 28, pp. 1153-1157, 1974.
- [Mig82] M. Mignotte: Some useful bounds. In G.E. Collins Buchbueger and R. Loos, editors, *Symbolic And Algebraic Computation*, Computing Supplementum 4, pp. 259-263, Springer-Verlag, Wien-New York, 1982.
- [Mig92] M. Mignotte: On the product of the largest roots of a polynomial. *Journal of Symbolic Computation*, Vol. 13, pp. 605-661, 1992.
- [Mis93] B. Mishra: *Algorithmic Algebra*. Texts and Monographs in Computer Science. Springer-Verlag, 1993.
- [Sch80] J. T. Schwartz: Fast probabilistic algorithms for verification of polynomial identities. *Journal of ACM*, Vol. 27, No. 4, pp. 701-717, 1980.
- [Sch86] A. Schrijver: *Theory of Linear and Integer Programming*. John Wiley & Sons, 1986.
- [vdW37] B. L. van der Waerden: *Moderne Algebra*. Springer, 1937.
- [Wa82] P. S. Wang: Factoring multivariate polynomials over algebraic number fields. *Math. Comp.*, Vol. 30, pp. 324-336, 1976.
- [Wol88] S. Wolfram: *Mathematica, A System for Doing Mathematics by Computer*. Addison-Wesley, 1988.
- [Wu78] Wen-tsü Wu: On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientia Sinica*, Vol. 21, pp. 157-179, 1978.
- [Wu94] Wen-tsü Wu: *Mechanical Theorem Proving in Geometries*. Texts and Monographs in Symbolic Computation, Springer-Verlag, Wien, New York, 1994. Translated from the Chinese by Xiaofan Jin and Dongming Wang.
- [Yam91] O. Yamamoto: The distribution of the zeros generated by length-bounded polynomials. *Appl. Math. Lett.*, Vol. 4, No. 1, pp. 63-66, 1991.
- [Yam94a] O. Yamamoto: On some bounds for zeros of norm-bounded polynomials. *Journal of Symbolic Computation*, Vol. 18, pp. 403-427, 1994.

- [Yam94b] O. Yamamoto: A new proof of Landau's inequality by the analysis of distributions of zeros of polynomials. Research Reports on Information Sciences C-112, Department of Information Sciences Tokyo Institute of Technology, 1994, Submitted to *Journal of Symbolic Computation*.
- [Zas75] H. Zassenhaus: On Hensel factorization II. *Symposia Mathematica*, Vol. 15, pp. 499-513, 1975.
- [佐々81] 佐々木建昭: 数式処理. 情報処理叢書 7. 情報処理学会, オーム社, 1981.
- [山伊 86] 山本 修身, 伊理正夫: 整係数多項式の零点の存在範囲について. 応用数学合同研究集会報告集, pp. 122-134, 1986.
- [山本 87a] 山本修身: 高さを制限した整係数多項式の零点について. 応用数学合同研究集会報告集, pp. 90-99, 1987.
- [山本 87b] 山本修身: 整係数多項式の零点の存在範囲について, 夏の LA シンポジウム 資料, 1987.
- [山本 88] 山本修身: On the distribution of the zero generated by height-bounded polynomials. 応用数学合同研究集会報告集, pp. 205-214, 1988.
- [山本 89] 山本修身: 代数方程式の複雑さと初等幾何学の定理証明. 情報基礎論ワークショップ, pp. 1-4, 1989.
- [山本 90] 山本修身: Mignotte の不等式について. 応用数学合同研究集会報告集, pp. 15-22, 1990.
- [山本 91] 山本修身: 代数的数の複雑さと計算過程. 応用数学合同研究集会報告集, pp. 26-31, 1991.
- [山本 95] 山本修身: 代数的数の複雑さと初等幾何学の定理証明への応用. 応用数理学会論文誌, Vol. 5, No. 3, pp. 199-214, 1995.
- [吉田 88] 吉田清範: 初等的図形の交差判定法 — 計算量および計算精度の立場から —. 東京大学工学部計数工学科 博士論文, 1988.

