数理解析研究所講究録
986巻 1997年 83-91

拡張されたMahlerのmeasureによる代数的数のゼロ判定

NTT CS研 関川 浩 (Hiroshi Sekigawa)

1. はじめに

本稿では，いくつかの代数的数から加減乗算（除算は除外する）により得られた代数的数のゼロ判定について，数値計算を主にした新しい手法を提案する．提案手法は，数値計算にp進的なものも含んでいる点において，[10, 11, 12]を発展させたものになっている．

代数的数を扱う際，可能ならば，固定した代数体の中で話を進めるのが望ましい．しかし，実数体や複素数体上の多項式の根として，近似値とともに代数的数が与えられ，それらから四則演算で得られた数を扱う場合も，応用上しばしばある．このとき，扱う代数的数をすべて含む代数体の原始元を求める，あるいは，逐次拡大の形にする，といった代数的な計算は，負荷がかかる処理である．しかも，扱う代数的数すべてを含む代数体の拡大次数は大きいが，ゼロ判定をする代数的数の次数がそれほど大きくないときには現実的な方法ではない．なお，代数的数の扱い方に関しては，[3, 8, 4]を参照されたい．

本稿で提案する手法では，数値的な計算を援用することにより，代数的な計算の負荷を軽くしている．具体的には，拡張されたMahlerのmeasureを定義し，数値計算とあわせて用いることにより，正確にゼロ判定ができるようにしている．

以下，2.でMahlerのmeasureを復習し，3.で拡張されたMahlerのmeasureとそれを用いたゼロ判定法を説明する．最後に4.で今後の課題を述べる．なお，本稿では以下の記号を用いる．

$\mathbf{Z}$: 有理整数環,$\mathbf{Q}$: 有理数体,$\mathbf{R}$: 実数体,$\mathbf{C}$: 複素数体,$\mathbf{Z}_p$: p進整数環,$\mathbf{Q}_p$: p進体.

2. Mahlerのmeasure

この節では，Mahlerのmeasure [9]と，それを用いたゼロ判定法[10, 11, 12]を復習する．

定義 1 (Mahlerのmeasure) 多項式$F(x)=\sum_{i=0}^{d}a_ix^i=a_d\prod_{i=1}^{d}(x-\alpha_i)\in\mathbf{C}[x]$ $(a_d\neq 0)$の*Mahler*の*measure* $M(F)$を，以下のように定義する．

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

代数的数αの*Mahler*の*measure* $M(\alpha)$を，$M(\alpha)=M(F)$と定義する．ただし，$F\in\mathbf{Z}[x]$はαの$\mathbf{Q}$上の原始的な最小多項式である．

多項式 $F(x)=\sum_{i=0}^{d}a_ix^i$ に対し，Landau の不等式 $M(F)\le\left(\sum_{i=0}^{d}|a_i|^2\right)^{1/2}$ が成り立つ [7]．そのほか，Mahler の measure の計算に関しては，[2] を参照されたい．

代数的数に対する Mahler の measure は以下のような性質をもつ．

命題 1

1. 任意の代数的数αに対して，$1\le M(\alpha)$.
2. 代数的数αが，$\alpha\neq 0$ かつ $M(\alpha)\le A$，を満たすならば，$1/A\le|\alpha|\le A$.
3. α,βがそれぞれ高々d次，e次の代数的数のとき，以下の不等式が成り立つ．

$$M(\alpha\beta)\le M(\alpha)^eM(\beta)^d$$
$$M(\alpha\pm\beta)\le 2^{de}M(\alpha)^eM(\beta)^d$$

証明: 3 の加算の場合のみ証明する．α,βの $\mathbf{Q}$ 上の整数係数の原始的な最小多項式の主係数を，それぞれ，a,b とし，α,βの $\mathbf{Q}$ 上の共役を，それぞれ，$\alpha_1,\ldots,\alpha_d$と$\beta_1,\ldots,\beta_e$とする．

$$a^eb^d\prod_{i=1}^{d}\prod_{j=1}^{e}\{x-(\alpha_i+\beta_j)\}$$

は，$\alpha+\beta$を根としてもつ整数係数の多項式だから，

$$M(\alpha+\beta)\le a^eb^d\prod_{i=1}^{d}\prod_{j=1}^{e}\max\{1,|\alpha_i+\beta_j|\}\le a^eb^d\prod_{i=1}^{d}\prod_{j=1}^{e}2\max\{1,|\alpha_i|\}\max\{1,|\beta_j|\}$$
$$\le 2^{de}a^eb^d\prod_{i=1}^{d}\max\{1,|\alpha_i|\}^e\cdot\prod_{j=1}^{e}\max\{1,|\beta_j|\}^d=2^{de}M(\alpha)^eM(\beta)^d.\quad\blacksquare$$

次に，Mahler の measure を用いて代数的情報つき区間を定義する．

定義 2 (代数的情報つき区間)

1. αを高々d次の実代数的数とする．I を閉区間でαを含むもの（αの他の共役を含んでいてもよい），$M(\alpha)\le A$ としたとき，三つ組 (I,d,A) をαに対する代数的情報つき区間と定義する．I を数値的情報，d と A の対 (d,A) を代数的情報と呼ぶ．
   数値的情報を表す区間に浮動小数を用いた場合，代数的情報つき区間の精度がμとは，浮動小数の仮数部分をμ桁にとることと定義する．
2. 代数的情報つき区間 (I,d,A) と (J,e,B) の間の演算を以下のように定義する．

$$(I,d,A)\pm(J,e,B)=(I\pm J,de,2^{de}A^eB^d)$$
$$(I,d,A)\times(J,e,B)=(I\times J,de,A^eB^d)$$

ただし，$I\pm J$，$I\times J$ は区間演算 *[1]* による．

このように定義することにより，Mahler の measure の上からの評価がうまく伝播し，ゼロ判定や符号判定に使える．厳密にいえば，以下の定理のようになる．

定理 1 実代数的数$\alpha_1,\ldots,\alpha_k$から加減乗算により得られた実代数的数をαとする．また，$\alpha_1,\ldots,\alpha_k$をある精度で代数的情報つき区間に変換し，αを得たのと同じ計算過程で定義 *2* の計算により得られた代数的情報つき区間を$([a,b],d,N)$とする．このとき，以下が成り立つ．

1. $a\leq 0\leq b$かつ$\max\{-a,b\}<1/N$ならば，$\alpha=0$である．
2. 逆に，$\alpha=0$ならば，$a\leq 0\leq b$は精度によらず成り立ち，さらに，ある有限精度から先でつねに，$\max\{-a,b\}<1/N$が成り立つ．

より詳しい議論や，実際の計算方法は，[10, 11, 12] を参照のこと．

3. 拡張されたMahlerのmeasureとゼロ判定

3.1. 拡張されたMahlerのmeasure

この節では，拡張されたMahlerのmeasureを定義し，その性質について述べる．なお，以下に出てくる$\mathbf{Z}_p,\mathbf{Q}_p$やその拡大体についての詳しいことは [13, 5, 14, 6] などを参照されたい．

定義 3 (拡張されたMahlerのmeasure) $V=\{p\mid p\text{は素数}\}\cup\{\infty\}$とする．

1. 多項式$F=\sum_{i=0}^{d}a_ix^i\in\mathbf{Z}[x]$ $(a_d\neq 0)$の拡張された*Mahler*の*measure* $\widetilde{M}(F)$を，

$$\widetilde{M}(F)=\prod_{v\in V}\widetilde{M}_v(F)$$

と定義する．ただし，各$\widetilde{M}_v(F)$は以下のように定義される．
vが∞のとき．$F(x)=a_d\prod_{i=1}^{d}(x-\alpha_i)$（$\alpha_i\in\mathbf{C}$）と因数分解し，次の通り定義する．

$$\widetilde{M}_\infty(F)=\prod_{i=1}^{d}\max\{1,|\alpha_i|\}$$

vが素数pのとき．K_pをFの$\mathbf{Q}_p$上の分解体とし，$F(x)=a_d\prod_{i=1}^{d}(x-\alpha_{p,i})$ $(\alpha_{p,i}\in K_p)$と因数分解し，次の通り定義する．

$$\widetilde{M}_p(F)=\prod_{i=1}^{d}\max\{1,|\alpha_{p,i}|_p\}$$

ここで，$|\cdot|_p$は，$|p|_p=1/p$と正規化したK_pのp進絶対値である．($|0|_p=0$．$a\in\mathbf{Q},a\neq 0$のとき，$|a|_p=p^{-e}$．ただし，$a=p^eb/c$ $(e,b,c\in\mathbf{Z},(b,p)=(c,p)=1)$．)
2. 代数的数αの拡張された*Mahler*の*measure* $\widetilde{M}(\alpha)$を，$\widetilde{M}(\alpha)=\widetilde{M}(F)$と定義する．ただし，$F\in\mathbf{Z}[x]$は$\alpha$の$\mathbf{Q}$上の最小多項式である．また，各$v\in V$に対して，$\widetilde{M}_v(\alpha)=\widetilde{M}_v(F)$と定義する．

注意 1 $p\nmid a_d$ならば，$|\alpha_{p,i}|_p\leq 1$，$\widetilde{M}_p(F)=1$より，定義 *3* の無限積は実質，有限積である．

次の命題は，拡張されたMahlerのmeasureの別の定義といってもよい．

命題 2 pを素数とし，F, K_pを定義3の通りとする．$F=\prod_{i=1}^{g} F_i$，ただし，各$F_i=\sum_{j=0}^{d_i} a_{i,j}x^j \in \mathbf{Z}_p[x]$は$\mathbf{Z}_p$上既約，と因数分解する．このとき，以下が成り立つ．

$$\widetilde{M}_p(F)=\prod_{i=1}^{g}\max\left\{1,\left|\frac{a_{i,0}}{a_{i,d_i}}\right|_p\right\}$$

証明: $\alpha_{p,i}$と$\alpha_{p,j}$がFの同じ既約因子F_kの根ならば，そのp進絶対値は等しい．よって，$\alpha_{p,j}$がF_kの根全体を動くときの積について，以下が成り立ち，命題の主張が証明できる．

$$\prod\max\{1,|\alpha_{p,j}|_p\}=\max\left\{1,\left|\prod\alpha_{p,j}\right|_p\right\}=\max\left\{1,\left|\frac{a_{k,0}}{a_{k,d_k}}\right|_p\right\}\quad\blacksquare$$

拡張されたMahlerのmeasureと従来のMahlerのmeasureの間には，以下の大小関係がある．

命題 3 $F\in\mathbf{Z}[x]$，また，αは代数的数とする．このとき，次が成り立つ．

1. $1\le\widetilde{M}(F)\le M(F)$，$1\le\widetilde{M}(\alpha)\le M(\alpha)$.
2. αが代数的整数のとき，$\widetilde{M}(\alpha)=M(\alpha)$.

証明:

1. 多項式Fについてのみ証明すればよい．まず，$1\le\widetilde{M}(F)$は，定義より明らかである．以下，右側の不等号を証明する．Fを命題2の通りに因数分解する．$a_{i,0}, a_{i,d_i}\in\mathbf{Z}_p$より，$|a_{i,0}/a_{i,d_i}|_p\le|1/a_{i,d_i}|_p$である．また，$|1/a_{i,d_i}|_p\ge 1$だから，命題2より，

$$\widetilde{M}_p(F)\le\prod_{i=1}^{g}\left|\frac{1}{a_{i,d_i}}\right|_p=\left|\frac{1}{a_d}\right|_p$$

が成り立つ．すべての素数pに渡る積$\prod_p|1/a_d|_p=|a_d|$より，以下が成り立つ．

$$\begin{aligned}\widetilde{M}(F)&=\prod_p\widetilde{M}_p(F)\cdot\widetilde{M}_\infty(F)\\&\le\prod_p\left|\frac{1}{a_d}\right|_p\prod_{i=1}^{d}\max\{1,|\alpha_i|\}=|a_d|\prod_{i=1}^{d}\max\{1,|\alpha_i|\}=M(F).\end{aligned}$$

2. 代数的整数の$\mathbf{Q}$上の整係数最小多項式の主係数は1にとれるから主張は成り立つ．$\blacksquare$

次の命題は，拡張されたMahlerのmeasureの第三の定義といってもよい．

命題 4 αを代数的数とし，$K=\mathbf{Q}(\alpha)$とおく．

1. vが∞のとき，Kの共役のうち，実のものがr_1個，虚のものが$2r_2$個とする（$r_1+2r_2=[K:\mathbf{Q}]$）．このとき，$|\cdot|$をKに延長したものを$|\cdot|_1,\ldots,|\cdot|_{r_1+r_2}$とする．このうち，$r_1$個が$\mathbf{R}$の絶対値，$r_2$個が$\mathbf{C}$の絶対値となるが，このとき，以下が成り立つ．

$$\widetilde{M}_\infty(\alpha)=\prod_{i=1}^{r_1+r_2}\max\{1,|\alpha|_i\}$$

ただし，$\mathbf{C}$の絶対値は通常の絶対値の2乗である（*[13]II*章*1*節）．

2. v が素数 p のとき，K に入る絶対値のうち，$|\cdot|_p$ を延長したものを $|\cdot|_{p,1},\ldots,|\cdot|_{p,g}$ とする．なお，ここの g と，命題 2 に出てくる g（F として α の最小多項式をとる）は一致する．また，各 $|\cdot|_{p,i}$ は以下のように正規化しておく．まず，K の $|\cdot|_{p,i}$ による完備化を $K_{p,i}$ と書く．$K_{p,i}/\mathbf{Q}_p$ の分岐指数を $e_{p,i}$，剰余体の拡大次数を $f_{p,i}$ としたとき，$|p|_{p,i}=p^{-e_{p,i}f_{p,i}}$ となるように正規化する．このとき，以下が成り立つ．

$$\widetilde{M}_p(\alpha)=\prod_{i=1}^{g}\max\{1,|\alpha|_{p,i}\}$$

証明: 2 のみ証明する．ここでの正規化に対しては，

$$|\alpha|_{p,i}=|N_{K_{p,i}/\mathbf{Q}_p}(\alpha)|_p=\left|\frac{a_{i,0}}{a_{i,d_i}}\right|_p$$

が成り立つこと（[13] II 章 1,2,3 節）から命題の主張がしたがう． ■

次に，加減乗算により，拡張された Mahler の measure がどのように変化するのかを調べる．

命題 5 α,β を，それぞれ，高々 d 次，e 次の代数的数とする．

1. 任意の $v\in V$ に対して，$\widetilde{M}_v(\alpha\beta)\le\widetilde{M}_v(\alpha)^e\widetilde{M}_v(\beta)^d$ である．
2. v が素数 p のときは，以下が成り立つ．

$$\widetilde{M}_p(\alpha\pm\beta)\le\widetilde{M}_p(\alpha)^e\widetilde{M}_p(\beta)^d$$

v が ∞ のときは，以下が成り立つ．

$$\widetilde{M}_\infty(\alpha\pm\beta)\le 2^{ed}\widetilde{M}_\infty(\alpha)^e\widetilde{M}_\infty(\beta)^d$$

証明: v が素数 p で加減算のときのみ証明する（他の場合は，従来の Mahler の measure のときと同じように証明できる）．

$$|\alpha_i\pm\beta_j|_{p,i}\le\max\{|\alpha_i|_{p,i},|\beta_j|_{p,i}\}$$

に注意すれば，

$$\max\{1,|\alpha_i\pm\beta_j|_{p,i}\}\le\max\{1,|\alpha_i|_{p,i},|\beta_j|_{p,i}\}\le\max\{1,|\alpha_i|_{p,i}\}\max\{1,|\beta_j|_{p,i}\}$$

となり，乗算の場合と同じ評価ができる． ■

3.2. ゼロ判定

前節の準備の下で，ゼロ判定の原理を説明する．α を代数的数とし，命題 4 のように正規化した $K=\mathbf{Q}(\alpha)$ の絶対値全体の集合を W とする．以下，$|\cdot|_w\in W$ のことを単に $w\in W$ と書く．一つでも $|\alpha|_w\neq 0$ となる $w\in W$ があれば，$\alpha\neq 0$ である．

まず，任意の絶対値 $w\in W$ に対して，以下の不等式が成り立つ．

$$|\alpha|_w\le|\alpha|_w\max\{1,|\alpha|_w\}$$
$$|\alpha|_w\le\max\{1,|\alpha|_w\}$$

また，$\alpha \neq 0$ のとき，次の積公式が成り立つ（[13] II章1節）．

$$\prod_{w \in W} |\alpha|_w = 1$$

よって，$U \subset W$ に対して，

$$1 = \prod_{w \in W} |\alpha|_w \leq \prod_{u \in U} |\alpha|_u \prod_{w \in W} \max\{1, |\alpha|_w\} = |\alpha|_u \cdot \widetilde{M}(\alpha)$$

なので，もし，$\prod_{u \in U} |\alpha|_u \cdot \widetilde{M}(\alpha)$ の上からの評価が1より小さければ$\alpha = 0$である．

ここで，$\mathbf{Q}(\alpha)$が$\mathbf{R}$に埋め込まれるものを考え，Uとして$\mathbf{R}$の絶対値ただ一つからなる集合をとり，$\widetilde{M}$の上からの評価として従来のMahlerのmeasureをとったものが，[10, 11, 12]での提案手法であり，その組織的な実現方法が定義2，定理1である．

とくに，$\mathbf{Q}_p$への埋め込みを一つだけ考え，この埋め込みにより，扱っている代数的数がすべて$\mathbf{Z}_p$に入っているものとすると，定義2，定理1に対応する以下の定義，定理が得られる．（このようなpがつねに存在することは，Čebotarevの定理（[6] p. 410など）よりわかる．）

定義 4 (代数的情報つき p 進近似)

1. αは高々d次の代数的数で，$\mathbf{Z}_p$に埋め込まれた形で与えられているとする．$a, \mu \in \mathbf{Z}$（$\mu > 0$）で$a \equiv \alpha \pmod{p^\mu}$，$\widetilde{M}_p(\alpha) \leq A$としたとき，三つ組$(a, d, A)$を$\alpha$に対する代数的情報つき$p$進近似と定義する．$a$を$p$進的な数値的情報，$d$と$A$の対$(d, A)$を代数的情報，$\mu$を精度と呼ぶ．
2. 精度μの代数的情報つきp進近似(a, d, A)と(b, e, B)の間の演算を次のように定義する．

$$(a, d, A) \pm (b, e, B) = (a \pm b, de, 2^{de} A^e B^d)$$
$$(a, d, A) \times (b, e, B) = (ab, de, A^e B^d)$$

ただし，$a \pm b$，abは$\bmod p^\mu$で計算してよい．

注意 2 $a \equiv \alpha \pmod{p^\mu}$のとき，$\{x \in \mathbf{Z}_p \mid x \equiv \alpha \pmod{p^\mu}\}$は$\{x \in \mathbf{Z}_p \mid |x - a|_p \leq p^{-\mu}\}$に等しく，近似値と誤差の対で表した円区間*[1]*と見なせる．しかも，$\{x \in \mathbf{Z}_p \mid x \equiv a \pmod{p^\mu}\} = a + p^\mu \mathbf{Z}_p$だから，円区間の間の区間演算は，$\mathbf{Z}_p$の中の$\bmod p^\mu$での計算に対応している．

定理 2 (定理1の p 進版) 代数的数$\alpha_1, \ldots, \alpha_k$が$\mathbf{Z}_p$に埋め込まれた形で与えられているとし，これらから加減乗算により得られた代数的数をαとする．また，$\alpha_1, \ldots, \alpha_k$を精度$\mu$で代数的情報つき$p$進近似に変換し，$\alpha$を得たのと同じ計算過程で定義4の計算により得られた代数的情報つきp進近似を(a, d, N)とする．このとき，以下が成り立つ．

1. $a \equiv 0 \pmod{p^\mu}$かつ$p^{-\mu} < 1/N$ならば，$\alpha = 0$である．
2. 逆に，$\alpha = 0$ならば，$a \equiv 0 \pmod{p^\mu}$は精度μによらず成り立ち，さらに，ある有限精度から先でつねに，$p^{-\mu} < 1/N$が成り立つ．

3.3. 例

ここで例を三つ挙げる．最初は通常の絶対値を使った例，あとの二つはp進的な例である．

例 1 $\sqrt{2}\cdot\sqrt{3}-\sqrt{6}\ (=0)$.

通常の絶対値を用い，精度11の10進浮動小数による代数的情報つき区間により計算する．$\sqrt{2},\sqrt{3},\sqrt{6}$はそれぞれ，

$$([1.4142135623, 1.4142135624], 2, 2),$$
$$([1.7320508075, 1.7320508076], 2, 3),$$
$$([2.4494897427, 2.4494897428], 2, 6),$$

に変換される．$\sqrt{2}\cdot\sqrt{3}$に対応する計算結果は，

$$([2.4494897425, 2.4494897429], 4, 36),$$

$\sqrt{2}\cdot\sqrt{3}-\sqrt{6}$に対応する計算結果は，

$$([-0.3\times10^{-9},\ 0.2\times10^{-9}], 8, 429981696),$$

となる．区間$[-0.3\times10^{-9}, 0.2\times10^{-9}]$は0を含むが，

$$0.3\times10^{-9}\cdot429981696 = 0.12899\cdots < 1$$

となり，計算結果は0と判定できる．

二番目の例はごく簡単だが，本稿の手法の特別な場合にあたる．

例 2 pを素数とする．$\alpha\in\mathbf{Z}$，$p|\alpha$，かつ$|\alpha|<p$ならば，$\alpha=0$である．

まず，pがαを割り切ることと，$|\alpha|_p\le 1/p$であることが同値であるのは，定義から明らかである．次に，$\alpha\in\mathbf{Z}$かつ$|\alpha|<p$ならば$\widetilde{M}(\alpha)=M(\alpha)<p$であるから，

$$|\alpha|_p\cdot\widetilde{M}(\alpha)<\frac{1}{p}\cdot p=1$$

より，$\alpha=0$と決定できる．

最後の例は，もう少し複雑な例である．ただし，途中に現れる代数的数の次数の上からの評価を小さく押えるため，代数的情報つきp進近似は用いていない．

例 3 αの$\mathbf{Q}$上の最小多項式をx^2+x-1とし，βの$\mathbf{Q}(\alpha)$上の最小多項式を$x^2-\alpha x+1$とする．このとき，$\gamma=\beta^5-1$が0となることを，$\mathbf{Q}(\beta)$を$\mathbf{Q}_{11}$に埋め込むことにより示せ．

1. β,γは代数的整数なので，$\widetilde{M}(\beta)=M(\beta)$，$\widetilde{M}(\gamma)=M(\gamma)$である．よって，$\mathbf{C}$内で考え，$M(\beta),M(\gamma)$を計算する．$\alpha\in\mathbf{R}$で，$|\alpha|<2$だから，$x^2-\alpha x+1=0$の根は虚で互いに複素共役になり，その絶対値は1である．したがって，$M(\beta)=1$，$M(\beta^5)=1$となる．β^5は$\mathbf{Q}$上高々4次だから，$\widetilde{M}(\gamma)$に関して，以下の評価が成り立つ．

$$\widetilde{M}(\gamma)=M(\gamma)\le 2^4M(\beta^5)M(1)^4=16\cdot1\cdot1=16$$

2. 次に，$\mathbf{Q}_{11}$内で$|\gamma|_{11}$の計算を行う．

(a) まず， mod 11 で考える．

$$x^2+x-1\equiv 0 \pmod{11}$$

は，$x\equiv 3,7 \pmod{11}$という解をもつ．今，$\alpha\equiv 3 \pmod{11}$としよう．

$$x^2-3x+1\equiv 0 \pmod{11}$$

は，$x\equiv 5,9 \pmod{11}$という解をもつ．今，$\beta\equiv 5 \pmod{11}$としよう．

$$\gamma=\beta^5-1\equiv 5^5-1\equiv 0 \pmod{11}$$

だから，$|\gamma|_{11}\leq 1/11$となる．

$$|\gamma|_{11}\cdot\widetilde{M}(\gamma)\leq\frac{1}{11}\cdot 16=\frac{16}{11}\geq 1$$

だから，$\gamma=0$とは判定できない．

(b) 次いで， mod 121（$121=11^2$）で考える．なお，合同式の解の持ち上げに関しては，[14] を参照のこと．

$$x^2+x-1\equiv 0 \pmod{11}$$

の解 3 mod 11 を， mod 121 の解に持ち上げると，36 mod 121 になる．

$$x^2-36x+1\equiv 0 \pmod{11}$$

の解 5 mod 11 を， mod 121 の解に持ち上げると，27 mod 121 になる．

$$\gamma=\beta^5-1\equiv 27^5-1\equiv 0 \pmod{121}$$

だから，$|\gamma|_{11}\leq 1/121$となる．

$$|\gamma|_{11}\cdot\widetilde{M}(\gamma)\leq\frac{1}{121}\cdot 16=\frac{16}{121}<1$$

だから，$\gamma=0$と判定できる．

4. おわりに

拡張された Mahler の measure を導入し，それを用いた，代数的数のゼロ判定法を提案した．この枠組によって，ゼロ判定法に関して，$\mathbf{R}$や$\mathbf{C}$での近似計算（区間演算など）と$\mathbf{Q}_p$やその拡大体での近似計算（ mod p^μでの計算など）を統一的に扱うことができる．

今後の課題として，従来の Mahler の measure を用いた代数的情報つき区間のように，数式処理システム上に本手法を用いたゼロ判定のパッケージを作成し，数式処理の実際のアルゴリズムに適用することが挙げられる．

参 考 文 献

[1] Alefeld, G. and Herzberger, J., *Introduction to Interval Computations*, Academic Press, 1983.

[2] Cerlienco, L., Mignotte, M., and Piras, F., Computing the Measure of a Polynomial, *J. Symbolic Computation* **4**, pp. 21–33, 1987.

[3] Cohen, H., *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[4] Coste, M. and Roy, F., Thom's Lemma, the Coding of Real Algebraic Numbers and the Computation of the Topology of Semi-algebraic Sets, *J. Symbolic Computation* **5**, pp. 121–129, 1988.

[5] 彌永昌吉（編），数論，岩波書店，1969.

[6] 河田敬義，数論（岩波講座基礎数学），岩波書店，1979.

[7] Landau, E., Sur quelques théorèmes de M. Petrovic relatifs aux zéros des fonctions analytiques, *Bull. Soc. Math. France* **33**, pp. 251–261, 1905.

[8] Loos, R., Computing in Algebraic Extensions, *Computer Algebra, Symbolic and Algebraic Computation (Ed. B. Buchberger, G. E. Collins, and R. Loos)*, Springer-Verlag, pp. 173–187, 1983.

[9] Mahler, K., An Application of Jensen's Formulae to Polynomials, *Mathematica* **7**, pp. 98–100, 1960.

[10] 関川 浩，近似計算による代数的数の符号判定について，京都大学数理解析研究所講録究 941「数式処理における理論と応用の研究」，pp. 185–193，1996.

[11] 関川 浩，区間演算と多項式ノルムによる代数的数の符号判定，京都大学数理解析研究所講究録 "Researches on Algorithms for Computer Algebra" (to appear).

[12] Sekigawa, H., Using Interval Arithmetic and Polynomial Norms to Determine Signs of Algebraic Numbers, *Proc. of Asian Symposium on Computer Mathematics (ASCM'96)*, pp. 43–53, 1996.

[13] Serre, J.-P., *Corps Locaux*, Hermann, 1962. （英訳: *Local Fields*, Springer-Verlag, 1979.）

[14] Serre, J.-P., *Cours d'Arithmetique*, Presses Univ. de France, 1970. （英訳: *A Course in Arithmetic (2nd ed.)*, Springer-Verlag, 1978, 和訳: 数論講義，岩波書店，1979.）