フヒヒwwwセミナー

@alg_d (http://twitter.com/alg_d)

2011 年 10 月 01 日

定義. $\alpha \in \mathbb{C}$ とする．ある多項式 $f(x) \in \mathbb{Q}[x]$ に対し $f(\alpha) = 0$ となるとき，α を代数的数という．

α を代数的数とする．$f(\alpha) = 0$ となる多項式 $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ $(a_m \neq 0)$ が取れる．そのような f はたくさん有るが，そのうち次数 m が最小になるように選ぶ．更に，$f(\alpha) = 0 \Longleftrightarrow \dfrac{1}{a_m} f(\alpha) = 0$ だから $a_m = 1$ としてよい．こうして得られる多項式 $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ は α から一意に定まる．そこでこの f を α の最小多項式という．

定義. α を代数的数とする．最小多項式の係数が全て整数になるとき，α を代数的整数という．

> ※ 簡単のために，「代数的整数」のことを「整数」と呼ぶことが多い．その為，普通の意味での「整数」を「有理整数」と呼んで区別する．

例 1. $1, \sqrt{2}, \sqrt{-1}, \dfrac{-1+\sqrt{-3}}{2}$ は代数的整数.
それぞれの最小多項式は $x-1,\ x^2-1,\ x^2+1,\ x^2+x+1$ である．

例 2. $\dfrac{1}{2}, \dfrac{1}{\sqrt{2}}$ は代数的数であるが代数的整数ではない.
何故なら，最小多項式が $x - \dfrac{1}{2},\ x^2 - \dfrac{1}{2}$ となり，係数が有理整数でないから.

定義. $\{x_n\}_{n=1}^{\infty} \subset [0,1)$ を実数列とする．区間 $I = [a,b) \subset [0,1)$ に対し $A(N,I) := \#\{1 \leq i \leq N \mid x_n \in I\}$ と置く．

$\{x_n\}_{n=1}^{\infty}$ が $[0,1)$ 上一様分布する
$\Longleftrightarrow$ 任意の I に対し $\lim\limits_{N \leftarrow \infty} \dfrac{A(N,I)}{N} = b - a$

定義. 実数 x に対し $\{x\} := x - [x]$ を x の小数部分と言う．一般の実数列 $\{x_n\}_{n=1}^{\infty} \subset \mathbb{R}$ に対し

$\{x_n\}_{n=1}^{\infty}$ が　mod 1 で一様分布する

$\Longleftrightarrow$ 数列 $\big\{\{x_n\}\big\}_{n=1}^{\infty} \subset [0,1)$ が $[0,1)$ 上一様分布する

定理 1. 殆ど全ての実数 $x > 1$ に対し，$\{x^n\}_{n=1}^{\infty}$ は　mod 1 で一様分布する．

しかし，そのような x はほとんど知られていない．

※ $\big\{\big(\frac{3}{2}\big)^n\big\}_{n=1}^{\infty}$ や $\{e^n\}_{n=1}^{\infty}$ が　mod 1 で一様分布するか，というような問題でさえ未解決問題のようだ．(2004 年時点) また，一様分布するような x の構成法は [1] に載っているとのこと．

逆に，　mod 1 で一様分布しないような x は数多く知られている．例えば $2, 3, 4, \cdots$ は自明な例である．他にも，代数的整数の例が多く知られている．

定義. 代数的整数 γ の最小多項式を $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ とする．f の m 個の根 $\gamma^{(1)},\ \gamma^{(2)},\ \cdots,\ \gamma^{(m)}$ を γ の共役元と言う．番号を付け替えることにより，$\gamma = \gamma^{(1)}$ としてよい．

例 3. $\gamma := \dfrac{1+\sqrt{5}}{2}$ とする．γ の最小多項式は $f(x) = x^2 - x - 1$ だから γ は代数的整数．また γ の共役元は γ と $\gamma' := \dfrac{1-\sqrt{5}}{2}$ である．

$$\gamma^n + \gamma'^n = (\gamma + \gamma')^n + \cdots = (\text{有理整数})$$

である．$|\gamma'| < 1$ だから $\gamma'^n \to 0\ (n \to \infty)$．故に　mod 1 で考えると $\gamma^n \to 0\ (n \to \infty)$ となり，$\{\gamma^n\}_{n=1}^{\infty}$ は　mod 1 で一様分布しないことが分かる．

定義. 実数 $\gamma > 1$ を代数的整数とする．γ の共役元を $\gamma^{(1)}(= \gamma),\ \gamma^{(2)},\ \cdots,\ \gamma^{(m)}$ とする．

γ が Pisot 数

$\Longleftrightarrow |\gamma^{(2)}| < 1,\ \cdots,\ |\gamma^{(m)}| < 1$

先の例 3 と同様にして，次が分かる．

定理 2. Pisot 数 γ に対し，$\{\gamma^n\}_{n=1}^{\infty}$ は　mod 1 で一様分布しない．

証明. $\gamma^n + (\gamma^{(2)})^n + \cdots + (\gamma^{(m)})^n = (\text{整数})$ より　mod 1 で $\gamma^n \to 0\ (n \to \infty)$ となるから．　□

定義. 実数 $\gamma > 1$ を代数的整数，$\gamma^{(1)}(=\gamma)$，$\gamma^{(2)}$，$\cdots$，$\gamma^{(m)}$ を共役元とする．

γ が Salem 数

$\Longleftrightarrow |\gamma^{(2)}| \leq 1, \cdots, |\gamma^{(m)}| \leq 1$ で，少なくとも一つの $\gamma^{(i)}$ について $|\gamma^{(i)}| = 1$ となる

定理 3. Salem 数 γ に対し，$\{\gamma^n\}_{n=1}^{\infty}$ は　mod 1 で一様分布しない．

※ 一様分布はしないが，$[0,1)$ 上稠密に分布することも証明できる．
証明は *[2]* に載っていたと思うのですが，確認したのが随分前なので自信が無いです．

例 4. $\gamma := \dfrac{1+\sqrt{13}}{4} + \dfrac{1}{2}\sqrt{\dfrac{-1+\sqrt{13}}{2}}$ の最小多項式は $f(x) = x^4 - x^3 - x^2 - x + 1$ である．よって γ は代数的整数．γ の共役元は

$$\begin{cases} \gamma^{(2)} = \dfrac{1+\sqrt{13}}{4} - \dfrac{1}{2}\sqrt{\dfrac{-1+\sqrt{13}}{2}} \\ \gamma^{(3)} = \dfrac{1-\sqrt{13}}{4} + \dfrac{1}{2}\sqrt{\dfrac{1+\sqrt{13}}{2}}i \\ \gamma^{(4)} = \dfrac{1-\sqrt{13}}{4} - \dfrac{1}{2}\sqrt{\dfrac{1+\sqrt{13}}{2}}i \end{cases}$$

絶対値を計算すると

$$\begin{cases} |\gamma^{(1)}| = 1.72208\cdots > 1 \\ |\gamma^{(2)}| = 0.58069\cdots < 1 \\ |\gamma^{(3)}| = |\gamma^{(4)}| = 1 \end{cases}$$

が分かる．即ち γ は Salem 数である．

Salem 数 γ の見つけ方について述べる．その為には，$(0,1)$，$(1,\infty)$，$\{z \in \mathbb{C} \mid |z| = 1\}$ にそれぞれ根を持つような最小多項式 $f(x) \in \mathbb{Z}[x]$ を探せばよい．

まず，$|\delta| = 1$ となるような代数的整数 δ の最小多項式 $f(x)$ は適当な多項式 $g(x)$ を用いて

$$f(x) = x^m g\left(x + \frac{1}{x}\right)$$

と表せることが分かる．

$\ddots$) $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ を δ の最小多項式とする．複素共役 $\overline{\delta} = \delta^{-1}$ も $f(x)$ の根なので

$$f(\delta^{-1}) = \delta^{-n} + a_{n-1}\delta^{-n+1} + \cdots + a_1\delta^{-1} + a_0 = 0$$

ゆえに, δ^n を掛ければ次が成立する.

$$\delta^n + \frac{a_1}{a_0}\delta^{n-1} + \cdots + \frac{a_{n-1}}{a_0}\delta + \frac{1}{a_0} = 0$$

最小多項式は一意的なので

$$a_0 = \frac{1}{a_0},\ a_1 = \frac{a_{n-1}}{a_0},\ \cdots,\ a_{n-1} = \frac{a_1}{a_0}$$

ゆえに $a_0 = \pm 1,\ a_{n-1} = a_0 a_1,\ a_{n-2} = a_0 a_2,\ \cdots$ である.

$a_0 = -1$ と仮定する. $n = 2m$ ならば

$$f(x) = x^n - a_1 x^{n-1} + \cdots - a_{m-1}x^{m+1} + a_{m-1}x^{m-1} + \cdots + a_1 x - 1$$

$n = 2m+1$ ならば

$$f(x) = x^n - a_1 x^{n-1} + \cdots - a_m x^{m+1} + a_m x^m + \cdots + a_1 x - 1$$

よっていずれの場合も $f(1) = 0$ となり, $f(x)$ が最小多項式である事に矛盾. ゆえに $a_0 = 1$ である. この時, $n = 2m+1$ ならば

$$f(x) = x^{2m+1} + a_1 x^{2m} + \cdots + a_m x^{m+1} + a_m x^m + \cdots + a_1 x + 1$$

よって $f(-1) = 0$ となり, $f(x)$ が最小多項式である事に矛盾. ゆえに $n = 2m$, 即ち $f(x)$ は偶数次である.

α を $f(x)$ の根とすると

$$f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \cdots + a_1\alpha + 1 = 0$$

α^n で割れば

$$\left(\frac{1}{\alpha}\right)^n + a_1\left(\frac{1}{\alpha}\right)^{n-1} + \cdots + a_1\frac{1}{\alpha} + 1 = 0$$

ゆえに $\dfrac{1}{\alpha}$ も $f(x)$ の根. 従って $\alpha_1, \dfrac{1}{\alpha_1}, \cdots, \alpha_m, \dfrac{1}{\alpha_m}$ を $f(x)$ の全ての根とすれば

$f(x)$ は次の様に表せる.

$$\begin{aligned} f(x) &= \prod_{j=1}^{m}(x-\alpha_j)\Big(x-\frac{1}{\alpha_j}\Big) \\ &= \prod_{j=1}^{m}\left(x^2-\Big(\alpha_j+\frac{1}{\alpha_j}\Big)x+1\right) \\ &= x^m\prod_{j=1}^{m}\left(x+\frac{1}{x}-\Big(\alpha_j+\frac{1}{\alpha_j}\Big)\right) \end{aligned}$$

故に適当な多項式 $g(x)$ を用いて

$$f(x) = x^m g\left(x+\frac{1}{x}\right)$$

次の補題が成立する.

補題. $x(\neq 0)\in\mathbb{C}$ に対し

(1) x が実数でなく, かつ $|x|=1 \Longleftrightarrow x+\dfrac{1}{x}$ は実数で, $\left|x+\dfrac{1}{x}\right|<2$

(2) x が実数で, かつ $|x|\neq 1 \Longleftrightarrow x+\dfrac{1}{x}$ は実数で, $\left|x+\dfrac{1}{x}\right|>2$

この補題によって次のようなことが分かる.

(i) $g(x)$ が $-2<\alpha<2$ となる根を持つとする. $\beta+\dfrac{1}{\beta}=\alpha$ となる複素数 β を取る.

※ $\beta+\dfrac{1}{\beta}=\alpha \Longleftrightarrow \beta^2-\alpha\beta+1=0$ だから, そのような $\beta\in\mathbb{C}$ は必ず存在する. もちろん $\beta\neq 0$ である.

このとき $\left|\beta+\dfrac{1}{\beta}\right|<2$ だから, 補題により $|\beta|=1$ で, β は実数でない. また

$$f(\beta)=\beta^m g(\beta+\frac{1}{\beta})=\beta^m g(\alpha)=0$$

つまり, $f(x)$ は $|x|=1$ なる非実数根を持つ.

(ii) $g(x)$ が $\alpha<-2,\ 2<\alpha$ となる根を持つとする. $\beta+\dfrac{1}{\beta}=\alpha$ となる複素数 β を取る

((i) と同様). このとき $\left|\beta+\frac{1}{\beta}\right|>2$ だから，補題により β は実数で，$|\beta|\neq 0,1$. また

$$f(\beta)=\beta^m g(\beta+\frac{1}{\beta})=\beta^m g(\alpha)=0$$

つまり，$f(x)$ は $|x|\neq 0,1$ なる実数根を持つ.

(i)(ii) より

(1) $g(x)$ が $-2<x<2$ なる根を持つ $\Longleftrightarrow$ $f(x)$ は $|x|=1$ なる非実数根を持つ.

(2) $g(x)$ が $x<-2,\ 2<x$ なる根を持つ $\Longleftrightarrow$ $f(x)$ は $|x|\neq 0,1$ なる実数根を持つ.

が分かる. 従って, $g(x)$ として区間 $(-2,2),(2,+\infty)$ にそれぞれ根を持つような多項式をとれば, $f(x)$ が Salem 数を根に持つことが期待される.

例えば $g(x)=x^2-x-3$ とおくと, $g(x)$ の根は $x=\frac{1\pm\sqrt{13}}{2}$ であるので, $g(x)$ は区間 $(-2,2),(2,+\infty)$ にそれぞれ根を一つずつ持つ. この時の $f(x)$ の根の一つが, 例 4 の $\gamma=\frac{1+\sqrt{13}}{4}+\frac{1}{2}\sqrt{\frac{-1+\sqrt{13}}{2}}$ である.

参考文献

[1] M. B. Levin, On the complete uniform distribution of the fractional parts of the exp onential function. (Russian) Trudy Sem. Petrovsk. No. 7 (1981), 245?256.

[2] M. J. Bertin, A. Decomp-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.P. Schreiber, Pisot and Salem numbers, BirkhäuserVerlag, Basel-Boston-Berlin, 1992.