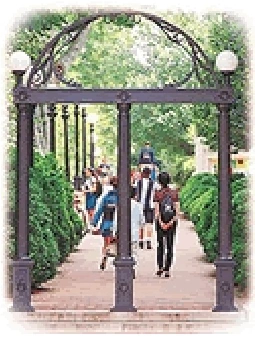
On algebraic integers in a given set of points

Charles Pooh
University of Georgia



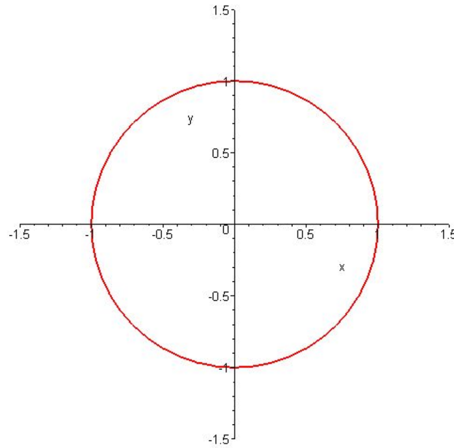
SERMON 2004 - Charleston, SC

Algebraic integers in the unit circle

If z is a nonzero algebraic integer with all its conjugates inside or on the unit circle, then z is a root of unity.

Proof. Assume z and all its conjugates are inside the unit circle. Let β be the product of conjugates of z. Since β is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we get $\beta \in \mathbb{Z}$. But $|\beta| < 1$; it follows that $\beta = 0$ and so z is zero. $\square$

Note $\beta = \prod P(w)$ over w conjugates of z and $P(w) = w$.



Can we generalize this result ?

For a monic polynomial $P(z) \in \mathbb{Z}[z]$ and $c < 1$, the leminscate domain $E = \{z \in \mathbb{C} : |P(z)| \le c\}$ has finitely many conjugate sets of algebraic integers; and the set $F = \{z \in \mathbb{C} : |P(z)| = 1\}$ has infinitely many such sets.

Define the capacity of a compact set E to be

$$\gamma(E) := \lim_{n \to \infty} \left[M_n(E) \right]^{\frac{1}{n}}$$

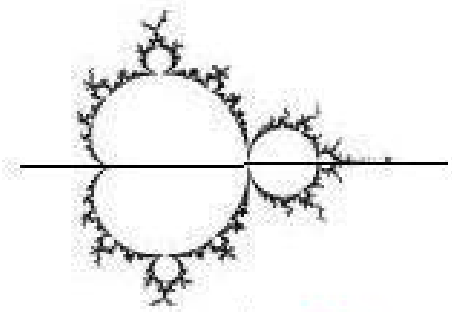
where

$$M_n(E) = \min_{\substack{P(z) \in \mathbb{Z}[z] \\ P(z) \text{ monic} \\ \deg P = n}} \max_{z \in E} |P(z)| \, .$$

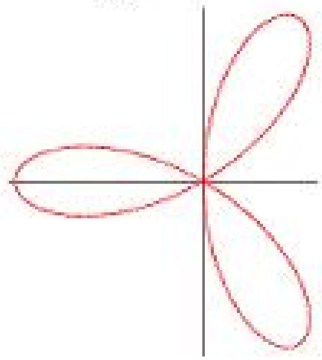
Fekete and Fekete-Szegö theorems

Let E be a compact subset of $\mathbb{C}$ stable under complex conjugation and having capacity $\gamma(E)$.

- **Fekete Theorem** (1923): if $\gamma(E) < 1$ then there is a neighborhood of E which contains only a finite number of complete conjugate sets of algebraic integers.



- **Fekete-Szegö Theorem** (1955): if $\gamma(E) \geq 1$, every neighborhood of E contains infinitely many complete conjugate sets of algebraic integers.



Logarithmic capacity

We have

$$\gamma(E) = \lim_{n\to\infty}\left[M_n(E)\right]^{\frac{1}{n}}, \quad M_n(E) = \min_{\substack{P(z)\in\mathbb{Z}[z] \\ P(z)\text{ monic} \\ \deg P = n}} \max_{z\in E} |P(z)|$$

$$= \lim_{n\to\infty} \delta_n(E), \qquad \delta_n^{\frac{n(n-1)}{2}} = \max_{\{z_1,\ldots,z_n\}\in E} \prod_{1\le j<k\le n} |z_j - z_k|$$

$$= e^{-V(E)},\ V(E) = \inf_{\substack{\text{measure } \nu \\ \nu(E)=1}} \int_E \int_E \log\frac{1}{|z-w|}\mathrm{d}\nu(z)\mathrm{d}\nu(w)$$

Note $\gamma(E) = \gamma(\Gamma)$ with Γ the outer boundary of E.

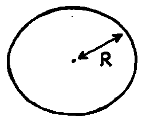
Equilibrium distribution and Green's function

If $\gamma(E) > 0$ then

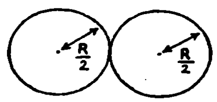
- there exists a unique probability measure μ of E such that
$$V(E) = \int_E \int_E \log \frac{1}{|z-w|} \mathrm{d}\mu(z) \mathrm{d}\mu(w);$$
- there is a harmonic function $g(z)$ defined on the unbounded component of $\mathbb{C} \backslash E$ by
$$g(z) = V(E) + \int_E \log |z-w| \ \mathrm{d}\mu(w).$$

Some planar sets and their capacities

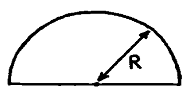
Disc, radius R — R



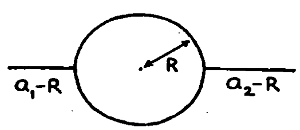
Two Tangent Discs, each of radius R/2 — $(\pi/4)\,R$



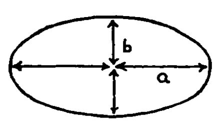
Half Disc, radius R — $\frac{4}{3\sqrt{3}}\,R$



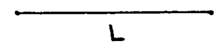
Disc D(0,R) with opposite arms of lengths a_1-R, a_2-R. — $\frac{(a_1+a_2)(R^2+a_1a_2)}{4a_1a_2}$



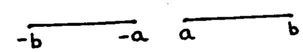
Ellipse $\frac{x^2}{a^2}+\frac{y^2}{b^2}\le 1$ - $(a+b)/2$



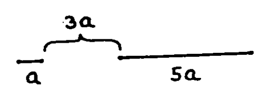
Straight Line Segment, length L — $L/4$



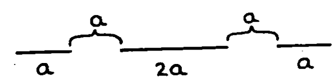
Two segments, $[-b,-a]\cup[a,b]$ — $\frac{\sqrt{b^2-a^2}}{2}$



Two segments, 1:3:5 as shown — $3^{1/3}\,a$

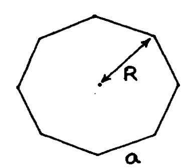


Three segments, 1:1:2:1:1 as shown — $3^{1/6}\,a$



Regular n-gon, inscribed in circle of radius R — $\frac{\Gamma(1+1/n)}{\Gamma(1-1/n)\Gamma(1+2/n)}\,R$

(or, with side length a) — $\frac{\Gamma(1/n)^2}{4\pi\,\Gamma(2/n)}\,a$



Problem: Effective version of Fekete and Fekete-Szegö theorems

Given a compact set E stable under complex conjugation:

1. if $\gamma(E) < 1$, find an upper bound for the number of conjugate sets of algebraic integers in (some neighborhood of) E;
2. if $\gamma(E) \geq 1$ and U is a given neighborhood of E, find a monic polynomial $P(z)$ in $\mathbb{Z}[z]$ of degree d (d explicit) such that $\{z \in \mathbb{C} : |P(z)| = c\} \subset U$ for some positive integer c.

Effective Fekete theorem (P.)

Let E be a connected compact subset of $\mathbb{C}$ stable under complex conjugation and having logarithmic capacity $\alpha < 1$. Then for all positive $\epsilon < (1-\alpha)^2$, all algebraic integers with conjugates in the ϵ-neighborhood $E(\epsilon)$ of E are the roots of a monic polynomial $P(z) = \sum a_r z^r \in \mathbb{Z}[z]$ of degree at most $d = 4^{m^2}$ with

$$m = \left\lceil \frac{4}{1-\sqrt{\beta}} \left(1 + \frac{4\alpha}{\epsilon}\right)^2 \log\left(\frac{16}{\beta\,(1-\beta)}\right) \log^{-1}\left(\frac{1}{\beta}\right) \right\rceil$$

$$\beta = \alpha + \frac{\epsilon}{2} + \frac{1}{2}\sqrt{\epsilon\,(4\alpha + \epsilon)}, \qquad |a_r| \le \binom{r}{d} \left(4\beta + \sup_{z \in E} |z|\right)^r.$$

Effective Fekete-Szegö theorem (P.)

Now assume $\alpha \geq 1$. Then for any real number $\epsilon > 0$, there is a monic polynomial $P(z) \in \mathbb{Z}[z]$ of degree at most d such that the ϵ-neighborhood $E(\epsilon)$ of E contains the polynomial lemniscate $\{z \in \mathbb{C} : |P(z)| = c\}$. Here d and c are (explicit) positive integers depending only on α, ϵ.

With these results, we can determine explicitly a monic polynomial in $\mathbb{Z}[z]$ containing information about algebraic integers in E and the number of their conjugacy classes.

Idea of the proof

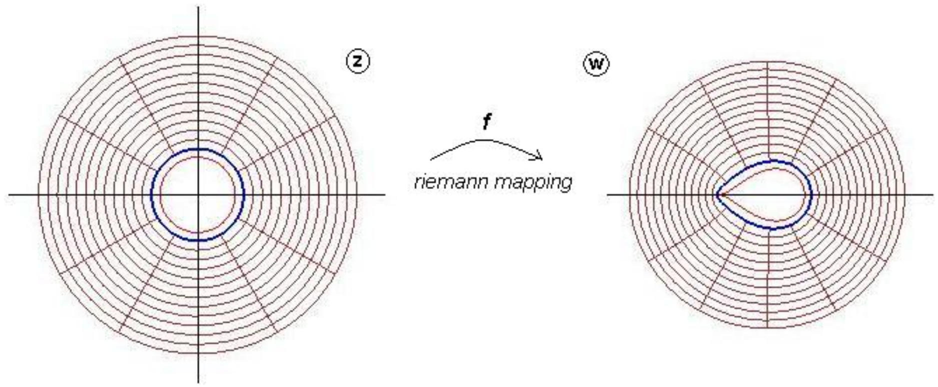
Construct monic polynomials $P(z) \in \mathbb{Z}[z]$ **whose normalized logarithm** $\dfrac{1}{deg\ P}\log|P(z)|$ **closely approximates** $g(z) - V(E)$.

This is done in two steps:

1. first approximate $g(z) - V(E)$ by $\dfrac{1}{deg\ Q}\log|Q(z)|$ where $Q(z) \in \mathbb{R}[z]$;
2. and next, transform $Q(z) \in \mathbb{R}[z]$ into a monic polynomial $P(z) \in \mathbb{Z}[z]$ which still well-approximates $g(z) - V(E)$.

Conformal mapping and Level sets

- $f(z) = \alpha z + \alpha_0 + \dfrac{\alpha_1}{z} + \ldots$
- $g(w) = \log \left| f^{-1}(w) \right|$
- $\mathrm{d}\mu = \frac{1}{2\pi} \left| \mathrm{d}\theta \right|$



The level set E_ρ is the interior of the level curve $\{f(z) : |z| = e^\rho\}$.

Every neighborhood of E contained an ϵ-neighborhood whose outer boundary is squeezed between some level sets E_ρ and E_τ.

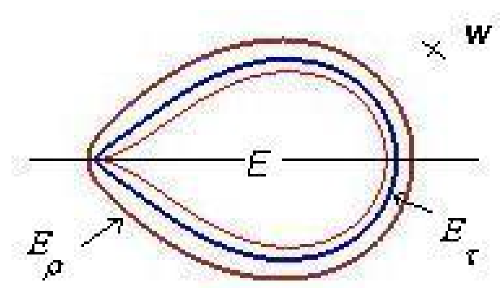
Approximation theorem

Let $0 < \tau < \rho$. Then for $\epsilon > 0$, for $n \in \mathbb{Z}$ and

$$n \geq \frac{2e^{\tau}}{(1-e^{-\epsilon})(\cosh(\rho)-\cosh(\tau))\,(1-e^{-2\tau})} + 1,$$

the real monic polynomial $T(w) = \prod_{k=1}^{2n} \left(w - f(e^{\tau + i\phi_k})\right)$ with $\phi_k = (2k-1)\dfrac{\pi}{2n}$ satisfies

$$\left| g(w) - V(E) - \frac{1}{2n} \log |T(w)| \right| < \epsilon$$



for all $w \notin E_\rho$.

Application

Let E be a connected compact subset of $\mathbb{C}$ stable under complex conjugation and having logarithmic capacity $\alpha \geq 1$. Then for any real number $\epsilon > 0$, there is a positive integer N such that for each $n > N$ there is an algebraic integer ϑ (and all conjugates) in $E(\epsilon)$ with $[\mathbb{Q}(\vartheta) : \mathbb{Q}] \geq n$. Moreover the height of ϑ is bounded by a constant depending only on α, ϵ and $\sup_{w \in E} |w|$.

(possible) Future work

- Generalize to arbitrary compact sets.
- Compute logarithmic capacity of a compact set having a piecewise smooth boundary.
- Effective Fekete and Fekete-Szego theorems on algebraic curves.

`pooh@math.uga.edu`
`http://www.math.uga.edu/~pooh`