Minimal polynomials of algebraic numbers with rational parameters

Joint with Karl Dilcher and Rob Noble (Dalhousie University)

Chris Smyth (U. Edinburgh)

Three special classes of polynomials

We study three classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ of polynomials with rational coefficients, and irreducible.

Three special classes of polynomials

We study three classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ of polynomials with rational coefficients, and irreducible.

- $\mathcal{C}_1$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational real part;

Three special classes of polynomials

We study three classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ of polynomials with rational coefficients, and irreducible.

- $\mathcal{C}_1$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational real part;
- $\mathcal{C}_2$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational imaginary part;

Three special classes of polynomials

We study three classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ of polynomials with rational coefficients, and irreducible.

- $\mathcal{C}_1$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational real part;
- $\mathcal{C}_2$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational imaginary part;
- $\mathcal{C}_3$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational modulus.

Three special classes of polynomials

For simplicity of exposition, will only discuss polynomials where the rational parameter is nonzero:

- $\mathcal{C}_1$ is the class of such polynomials that are minimal polynomials of an algebraic number having nonzero rational real part;
- $\mathcal{C}_2$ is the class of such polynomials that are minimal polynomials of an algebraic number having positive rational imaginary part;
- $\mathcal{C}_3$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational modulus.

Three special classes of polynomials

For simplicity of exposition, will only discuss polynomials where the rational parameter is nonzero:

- $\mathcal{C}_1$ is the class of such polynomials that are minimal polynomials of an algebraic number having nonzero rational real part;
- $\mathcal{C}_2$ is the class of such polynomials that are minimal polynomials of an algebraic number having positive rational imaginary part;
- $\mathcal{C}_3$ is the class of such polynomials that are minimal polynomials of an algebraic number having rational modulus.

What form must such polynomials take?

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

- Polynomials in $\mathcal{C}_1$ are of the form $Q\left((z-r)^2\right)$, where $r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a negative real root $-\beta$.

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

- Polynomials in $\mathcal{C}_1$ are of the form $Q\left((z-r)^2\right)$, where $r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a negative real root $-\beta$. Then such a polynomial has $r + i\sqrt{\beta}$ as a root.

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

- Polynomials in $\mathcal{C}_1$ are of the form $Q\left((z-r)^2\right)$, where $r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a negative real root $-\beta$. Then such a polynomial has $r + i\sqrt{\beta}$ as a root.

- Polynomials in $\mathcal{C}_2$ are of the form $Q(z+ir)Q(z-ir)$, where $0 < r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a real root β.

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

- Polynomials in $\mathcal{C}_1$ are of the form $Q\left((z-r)^2\right)$, where $r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a negative real root $-\beta$. Then such a polynomial has $r + i\sqrt{\beta}$ as a root.

- Polynomials in $\mathcal{C}_2$ are of the form $Q(z+ir)Q(z-ir)$, where $0 < r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a real root β. Then such a polynomial has $\beta + ir$ as a root.

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

- Polynomials in $\mathcal{C}_1$ are of the form $Q\left((z-r)^2\right)$, where $r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a negative real root $-\beta$. Then such a polynomial has $r + i\sqrt{\beta}$ as a root.

- Polynomials in $\mathcal{C}_2$ are of the form $Q(z+ir)Q(z-ir)$, where $0 < r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a real root β. Then such a polynomial has $\beta + ir$ as a root.

- Polynomials in $\mathcal{C}_3$ are of the form $Q(z/R + R/z)$, where $0 < R \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a real root β in $(-2, 2)$.

Forms for polynomials in $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$

We can give a general form for polynomials of these classes:

- Polynomials in $\mathcal{C}_1$ are of the form $Q\left((z-r)^2\right)$, where $r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a negative real root $-\beta$.
  Then such a polynomial has $r + i\sqrt{\beta}$ as a root.

- Polynomials in $\mathcal{C}_2$ are of the form $Q(z+ir)Q(z-ir)$, where $0 < r \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a real root β.
  Then such a polynomial has $\beta + ir$ as a root.

- Polynomials in $\mathcal{C}_3$ are of the form $Q(z/R + R/z)$, where $0 < R \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a real root β in $(-2, 2)$.
  Then such a polynomial has α of modulus R as a root, where α is a root of $\alpha/R + R/\alpha = \beta$.

Observations

- For polynomials $P(z) \in \mathcal{C}_1$, P determines r.

Observations

- For polynomials $P(z) \in \mathcal{C}_1$, P determines r.
- For polynomials $P(z) \in \mathcal{C}_2$, P determines $r > 0$.

Observations

- For polynomials $P(z) \in \mathcal{C}_1$, P determines r.
- For polynomials $P(z) \in \mathcal{C}_2$, P determines $r > 0$.
- For polynomials $P(z) \in \mathcal{C}_3$, P determines R.

Observations

- For polynomials $P(z) \in \mathcal{C}_1$, P determines r.
- For polynomials $P(z) \in \mathcal{C}_2$, P determines $r > 0$.
- For polynomials $P(z) \in \mathcal{C}_3$, P determines R.
- For polynomials $P(z) \in \mathcal{C}_1$, $P'(r) = 0$.

Intersecting the three classes

Are there any polynomials in more than one, or indeed all three, of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$?

Intersecting the three classes

Are there any polynomials in more than one, or indeed all three, of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$?

Certainly: for example the minimal polynomial of $3 + 4i$.

To avoid such trivialities, we confine our attention to polynomials of degree at least 3.

Intersecting the three classes

Are there any polynomials in more than one, or indeed all three, of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$?

Certainly: for example the minimal polynomial of $3 + 4i$.

To avoid such trivialities, we confine our attention to polynomials of degree at least 3.

We can describe $\mathcal{C}_1 \cap \mathcal{C}_2$:

Polynomials in $\mathcal{C}_1 \cap \mathcal{C}_2$ are of the form $Q\left((z - r' + ir)^2\right) Q\left((z - r' - ir)^2\right)$, where $r, r' \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a positive real root β and a negative real root $-\beta'$.

Intersecting the three classes

Are there any polynomials in more than one, or indeed all three, of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$?

Certainly: for example the minimal polynomial of $3 + 4i$.

To avoid such trivialities, we confine our attention to polynomials of degree at least 3.

We can describe $\mathcal{C}_1 \cap \mathcal{C}_2$:

Polynomials in $\mathcal{C}_1 \cap \mathcal{C}_2$ are of the form $Q\left((z - r' + ir)^2\right) Q\left((z - r' - ir)^2\right)$, where $r, r' \in \mathbb{Q}$, $Q \in \mathbb{Q}[z]$ is irreducible and has a positive real root β and a negative real root $-\beta'$.
Then such a polynomial has $(r' + \sqrt{\beta}) + ir$ and $r' + i(r + \sqrt{\beta'})$ amongst its roots.

Detour: the special rational function $\ell(z)$

For positive rational numbers t, let H_t denote the subgroup of G generated by $t - z$ and $1/z$.

Lemma

The subgroup H_t of G is infinite in all cases except

$$H_1 = \left\{ z, \frac{1}{z}, 1 - z, \frac{1}{1 - z}, \frac{z}{z - 1}, \frac{z - 1}{z} \right\}.$$

Furthermore

$$\frac{1}{2} \sum_{h \in H_1} h^2 = \ell(z)^2 + \frac{21}{4},$$

where

$$\ell(z) = \frac{(z - 2)(z - \frac{1}{2})(z + 1)}{z(z - 1)}. \tag{1}$$

More on $\ell(z)$

$\ell(z)$ is related to the classical j-invariant $j(\lambda)$ of the general elliptic curve in Legendre form

$$Y^2 = X(X-1)(X-\lambda).$$

Indeed,

$$j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} = 256\,\ell(\lambda)^2 + 1728.$$

Polynomials in $\mathcal{C}_1 \cap \mathcal{C}_3$

With the help of $\ell(z)$ we can describe $\mathcal{C}_1 \cap \mathcal{C}_3$:

Theorem

Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ if and only if P is irreducible and $P(z)$ or $P(-z)$ is given by

$$(Rz)^{2n}(z - R)^{2n} Q\left(\ell(z/R)^2\right)$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a negative real root. Furthermore, $r = \pm R/2$.

Polynomials in $\mathcal{C}_2 \cap \mathcal{C}_3$

Theorem

Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ *if and only if P is irreducible and has the form*

$$P(z) = (Rz)^{2n}(z^2 + R^2)^n Q\left(-i\ell(iz/R)\right) Q\left(i\ell(-iz/R)\right)$$

for some positive $R \in \mathbb{Q}$ *and monic irreducible polynomial* $Q(z) \in \mathbb{Q}[z]$ *of degree n that has a nonzero real root. Furthermore,* $r = R/2$.

Another group of Möbius transformations

Lemma

The group H of Möbius transformations generated by $1 - z$ and $\frac{\frac{i}{2}z+\frac{3}{4}}{z+\frac{i}{2}}$, is given by

$$H = \left\{ z, \frac{2iz-3}{-4z+2i}, \frac{(-4+2i)z+1}{-4z+4+2i}, \frac{(-2+4i)z-i}{4iz-2-4i}, \frac{-2z+3i}{4iz-2}, \frac{-2iz-3+2i}{4z-4+2i}, \frac{(4-2i)z-3+2i}{4z+2i}, \frac{(-2+2i)z-1-3i}{(-4+4i)z+2-2i}, \frac{(2+2i)z+1-3i}{(4+4i)z-2-2i}, \frac{-2iz+3+2i}{-4z+4+2i}, \frac{(-4-2i)z+3+2i}{-4z+2i}, 1-z \right\}.$$

Also,

$$\sum_{h \in H} h^2 = \frac{v^3+3v^2+36v+12}{v^2+4},$$

where $v = w - 1/w$ with $w = \frac{1}{2}(2z-1)^2$.

Polynomials in $\mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$

Theorem

Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$ if and only if P is irreducible and $P(z)$ or $P(-z)$ is given by

$$(Rz/2)^{4n}(z-R)^{4n}\left((z^2+R^2)(z^2-2Rz+2R^2)(2z^2-2Rz+R^2)\right)^{2n}$$
$$\times Q\left(s\left(\tfrac{1}{2}(2z/R-1+i)^2\right)\right) Q\left(s\left(\tfrac{1}{2}(2z/R-1-i)^2\right)\right)$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a real root, where

$$s(w) = \frac{v^3+3v^2+36v+12}{v^2+4}, \qquad v = w - 1/w.$$

In this case, P has a root with rational modulus R. Furthermore $r = \pm R/2$.

An example of $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$

Example

Let $Q(z) = z$, and so, using the theorem above,

$$P(z) = 16z^{24} - 192z^{23} + 1200z^{22} - 5104z^{21} + 16644z^{20} - 44472z^{19} + 100856z^{18} - 197028z^{17} + 333669z^{16} - 492808z^{15} + 640944z^{14} - 743916z^{13} + 780398z^{12} - 743916z^{11} + 640944z^{10} - 492808z^{9} + 333669z^{8} - 197028z^{7} + 100856z^{6} - 44472z^{5} + 16644z^{4} - 5104z^{3} + 1200z^{2} - 192z + 16$$

has four roots with real part $\frac{1}{2}$, two roots with imaginary part $\frac{1}{2}$ and four roots of modulus 1. It is irreducible, and $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$.