

## Kleiner maken van binaire vormen.

BSc-project. Begeleider: Marco Streng

De polynomen

$$\begin{aligned} f = & 54483077490880466235051062156851601084631825918867552966876953940456343983555005735749581732856 X^6 \\ & + 990809574373316073008326446924226962125258627241752694382432648412841882792930791138037878831796 X^5 Z \\ & + 9550240276628933798303625862171745458160135646268522819972302252550987899377800556235883602877325 X^4 Z^2 \\ & + 57165546969868973442682672879479866154789447227261543488899347884097865128651506960916610916364894 X^3 Z^3 \\ & + 153680336549268442271186636651532969660522204475345576198085469489856342803548826018365229016300991 X^2 Z^4 \\ & + 304320355122616427243045937068763255127862932635024403214419562331707908366448854342540129000480050 X Z^5 \\ & + 176301772040150234721101717513571942129443943129001668823025863330919470022725855330597190598219057 Z^6 \end{aligned}$$

en

$$g = X^6 + 6X^5Z + 11X^4Z^2 + 6X^3Z^3 + 5X^2Z^4 + 4Z^6 \in \mathbf{Q}[X, Z]$$

zijn equivalent, in de zin dat ze uit elkaar te verkrijgen zijn door middel van een  $\mathbf{Z}$ -lineaire verandering van variabelen.

Gegeven een polynoom zoals  $f$ , willen we soms een ‘kleiner’ equivalent polynoom, zoals  $g$  kunnen vinden. Dit heeft toepassingen op hyperelliptische krommen, zo bestaan er complex analytische constructies van speciale hyperelliptische krommen die polynomen als  $f$  opleveren.

Die kleine  $g$  kan je vinden met een algoritme van Stoll en Cremona [2], en dat werkt als volgt.

We kunnen lineaire verandering van variabelen zien als een werking van de groep  $\mathrm{SL}_2(\mathbf{Z}) = \{M \in \mathbf{Z}^{2 \times 2} : \det(M) = 1\}$  op de verzameling  $V_n$  van homogene polynomen over  $\mathbf{Z}$  van graad  $n > 5$ . Dezelfde groep werkt op het *bovenhalvlak*  $\mathcal{H} = \{\tau \in \mathbf{C} : \mathrm{Im}(\tau) > 0\}$  door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Binnen  $\mathcal{H}$  is er het *fundamentele domein*

$$\mathcal{F} = \left\{ \tau \in \mathcal{H} : \begin{array}{l} |\tau| \geq 1, \\ |\mathrm{Re}(\tau)| \leq \frac{1}{2}, \\ \text{als } |\tau| = 1 \text{ of } |\mathrm{Re}(\tau)| = \frac{1}{2}, \text{ dan } \mathrm{Re}(\tau) \geq 0 \end{array} \right\}$$

dat van elke baan precies 1 element bevat. Bovendien bestaat er een snel algoritme dat voor elke  $\tau \in \mathcal{H}$  een element  $A \in \mathrm{SL}_2(\mathbf{Z})$  vindt met  $A \cdot \tau \in \mathcal{F}$ .

Stoll en Cremona geven een afbeelding van  $\mathrm{SL}_2(\mathbf{Z})$ -verzamelingen

$$z : V_n \rightarrow \mathcal{H},$$

en hun algoritme is als volgt. Gegeven  $F \in V_n$ , bereken een  $A \in \mathrm{SL}_2(\mathbf{Z})$  met  $A \cdot z(F) \in \mathcal{F}$ . Voor  $G = A \cdot F$  geldt dan  $z(G) = A \cdot z(F) \in \mathcal{F}$  en dit is één van de ‘kleinste’ elementen van de baan van  $F$  [1].

In dit project bestudeer je eerst [2], en daarna:

1. Stoll en Cremona geven in [2] al aan dat een variant van hun methode ook werkt voor bepaalde andere getallenringen. Werk dit uit voor  $\mathbf{Z}[\sqrt{-1}]$ .
2. Mogelijk vervolg op 1.: kun je ook bewijzen dat je de kleinste representant van de baan kan vinden, met behulp van [1]?

3. Mogelijk vervolg op 1.: nu algemene(re) imaginair kwadratische getallenringen.
4. Mogelijk vervolg op 1.: programmeer dit in het open source softwarepakket SageMath en maak het onderdeel van de standaardfunctionaliteit van SageMath.

**Referentie:**

- [1] Benjamin Hutz and Michael Stoll. Smallest representatives of  $SL(2, \mathbf{Z})$ -orbits of binary forms and endomorphisms of  $\mathbf{P}^1$ . *Acta Arith.*, 189(3):283–308, 2019.
- [2] Michael Stoll and John E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.