Johan Bosman
Mathematisch Instituut
Postbus 9512
2300 RA Leiden
jgbosman@math.leidenuniv.nl

Onderzoek

Modulaire vormen en berekeningen in Galoistheorie

Twee onderwerpen binnen de getaltheorie die van fundamenteel belang zijn bij het bestuderen van nulpunten van polynomen zijn Galoistheorie en modulaire vormen. In dit artikel geeft Johan Bosman, promovendus van Bas Edixhoven, een indruk van hun verband. In het bijzonder besteedt hij aandacht aan computationele aspecten, die optreden bij het berekenen van voorbeelden en bij het schatten van de groei van de machtreekscoëfficienten van modulaire vormen.

Op de middelbare school leert iedereen een kwadratische vergelijking $ax^2+bx+c=0$ oplossen met behulp van de abc-formule:

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

Voor vergelijkingen van graad 3 bestaat er een soortgelijke formule, in 1545 gepubliceerd door Cardano, na het gestolen te hebben van Tartaglia: de nulpunten van het polynoom ax^3+bx^2+cx+d zijn gelijk aan

$$x=\sqrt[3]{C+\sqrt{D}}+\sqrt[3]{C-\sqrt{D}}-\frac{b}{3a},$$

waarbij

$$C=\frac{-b^3}{27a^3}+\frac{bc}{6a^2}-\frac{d}{2a},$$
$$D=C^2+\left(\frac{c}{3a}-\frac{b^2}{9a^2}\right)^3$$

en de derdemachtswortels geschikt gekozen dienen te worden. We zien dat de nulpunten van tweedegraads- en derdegraadspolynomen gegeven kunnen worden als uitdrukkingen in de coëfficiënten, waarbij we de operaties $+$, $-$, $\cdot$, $/$ en $\sqrt[n]{\ }$ gebruiken. We zullen in zo'n geval zeggen dat het polynoom *oplosbaar* is. We kunnen ons afvragen of dit ook geldt voor polynomen van willekeurige graad. Ferrari, een student van Cardano, had in 1540 al aangetoond dat vierdegraadsvergelijkingen oplosbaar zijn, onder de voorwaarde dat derdegraadsvergelijkingen oplosbaar zijn.

Galoistheorie

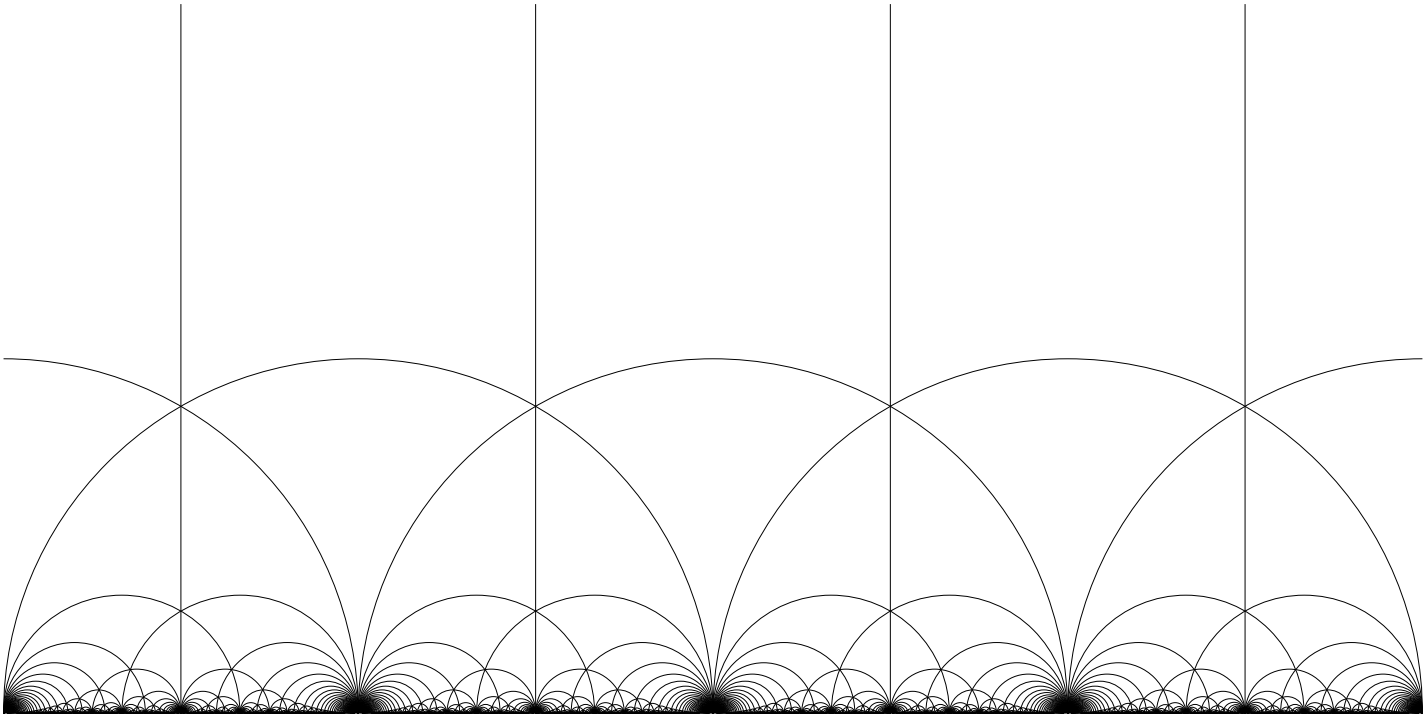
Naar een formule voor de nulpunten van polynomen van graad 5 en hoger heeft men sindsdien eeuwenlang tevergeefs gezocht. In 1799 vond de Italiaanse wiskundige Ruffini zelfs een bewijs dat zo'n formule in het algemeen niet bestaat! Niemand geloofde hem echter, totdat Abel in 1826 eveneens een bewijs vond. Zelfs vandaag de dag zijn er nog ongelovige thomassen die, uiteraard zonder succes, formules voor oplossingen van vijfdegraadsvergelijkingen proberen te vinden. Laten we hierbij wel opmerken dat het niet zo is dat geen enkele vergelijking van graad 5 of hoger opgelost kan worden. De nulpunten van x^5-x-1 kun je weliswaar niet uitdrukken in elementaire formules, maar die van x^5-2 wel: dat zijn alle waarden van $\sqrt[5]{2}$. In 1832 vond Galois een nieuw bewijs voor het feit dat vergelijkingen vanaf graad 5 niet op te lossen zijn met $+$, $-$, $\cdot$, $/$ en $\sqrt[n]{\ }$. Het bewijs van Galois is zeer interessant omdat het veel meer inzicht en structuur aan een polynoom geeft dan alleen 'ja, het kan' of 'nee, het kan niet'. Laten we eens kijken hoe Galois het deed. Kies je favoriete polynoom

$$P(x)=a_nx^n+\cdots+a_0\in\mathbf{Q}[x]$$
met nulpunten $\alpha_1,\ldots,\alpha_n\in\mathbf{C}$.

We zullen veronderstellen dat de nulpunten *verschillend* zijn; dit is geen grote belemmering want we kunnen meervoudige factoren gemakkelijk vinden. Er zijn allerlei relaties tussen de nulpunten. Zo kunnen we het product uitwerken in de identiteit

$$a_n(x-\alpha_1)\cdots(x-\alpha_n)=a_nx^n+\cdots+a_0$$

en dan vinden we bij elke coëfficiënt een sym-



Figuur 1 Bovenhalfvlak met betegeling

metrische relatie, bijvoorbeeld

$$\alpha_1 + \cdots + \alpha_n = \frac{-a_{n-1}}{a_n}$$
$$\text{en} \quad \alpha_1 \cdots \alpha_n = \frac{(-1)^n a_0}{a_n}.$$

Afhankelijk van het polynoom kunnen er meerdere relaties tussen de nulpunten zijn dan degenen die je direct uit de symmetrische relaties kunt afleiden. Galois kwam op het idee om de groep van alle permutaties van de nulpunten te bekijken die alle relaties tussen deze nulputen vasthouden; deze groep heet vandaag de dag de *Galoisgroep* van het polynoom P en noteren we met $\mathrm{Gal}(P)$. Als er geen andere relaties tussen de nulpunten zijn dan de symmetrische, dan zal $\mathrm{Gal}(P)$ uit alle mogelijk permutaties tussen de nulpunten bestaan en dus isomorf zijn met S_n, de volledige symmetrische groep van graad n. Als er echter meer relaties zijn, dan leggen deze restricties op de permutaties op en zal $\mathrm{Gal}(P)$ dus kleiner zijn.

Laten we als voorbeeld het polynoom $P = x^4 + x^3 + x^2 + x + 1$ bekijken. De nulpunten in $\mathbf{C}$ zijn de vijfdemachts eenheidswortels (behalve 1 zelf):

$$P = (x - \alpha_1) \cdots (x - \alpha_4)$$
$$\text{waarbij } \alpha_k = e^{2\pi ik/5}.$$

We zien onmiddelijk de relaties $\alpha_k = \alpha_1^k$. Als $\sigma \in \mathrm{Gal}(P)$ deze relaties wil behouden dan zal dus moeten gelden

$$\sigma(\alpha^k) = \sigma(\alpha_1)^k.$$

Dit betekent dat σ vastligt op het moment dat we $\sigma(\alpha_1)$ kennen. Nu moet α_1 naar een van de andere vier nulpunten worden gestuurd, dus $\mathrm{Gal}(P)$ zal in dit geval hooguit 4 elementen hebben. Het kan ook bewezen worden dat elk nulpunt kan optreden als beeld van α_1 dus de Galoisgroep heeft 4 elementen en is dus niet de groep van alle permutaties van de 4 nulpunten die 24 elementen heeft.

De oplosbaarheid van een polynoom P kan nu worden uitgedrukt in abstracte eigenschappen van de Galoisgroep $G = \mathrm{Gal}(P)$. We gaan een rij

$$G = G_1 \supset G_2 \supset \cdots$$

van ondergroepen van G maken aan de hand van het volgende recept: Begin met $G_1 = G$ en neem daarna telkens de *commutator ondergroep*:

$$G_{i+1} = [G_i, G_i] := \langle ghg^{-1}h^{-1} : g, h \in G \rangle.$$

Men kan laten zien dat P oplosbaar is dan en slechts dan als ergens in deze rij de triviale groep voorkomt. We hevelen de terminologie over en zeggen dat een groep G die hieraan voldoet *oplosbaar* is.

Als G zelf bijvoorbeeld commutatief is, dan is $[G, G]$ triviaal, dus polynomen met een commutatieve Galoisgroep zijn oplosbaar. Permutatiegroepen van graad hooguit 4 blijken allemaal oplosbaar te zijn, maar voor $n \geq 5$ bestaan er niet-oplosbare groepen: de groep S_n is hier een voorbeeld van.

Een groep die erg cruciaal is in deze context is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, de automorfismengroep van het lichaam van algebraïsche getallen. Het is een topologische groep waarin de Galoisgroepen van alle polynomen in $\mathbf{Q}[x]$ gecodeerd zitten. Voor eindige groepen G is het geven van een polynoom met Galoisgroep G (grofweg) equivalent met het geven van een continu surjectief homomorfisme $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to G$. De groep $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is binnen deze theorie dus een soort allesomvattend object en daarmee ook meteen heel moelijk te begrijpen.

Modulaire vormen en Galoisrepresentaties

Modulaire vormen spelen een belangrijke rol in de getaltheorie. Voor een goed overzichtsartikel met over de materie verwijzen wij graag naar [2] en de vele referenties die daarin staan. Grofweg zijn modulaire vormen holomorfe functies op het complexe bovenhalfvlak die aan bepaalde groeivoorwaarden en aan bepaalde symmetrierelaties ten aanzien van transformaties van de vorm

$$z \mapsto \frac{az + b}{cz + d}$$

voldoen. Een belangrijk voorbeeld van een

modulaire vorm die vele wiskundigen heeft beziggehouden is de functie

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}, \quad \text{waarbij } q = e^{2\pi iz}. \tag{1}$$

De groeivoorwaarde voor deze functie is $\lim_{\Im z\to\infty}\Delta(z) = 0$ en de symmetrierelatie luidt in dit geval dat $\Delta(z)$ voldoet aan

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z)$$

voor alle $z \in$ en $a,b,c,d \in \mathbf{Z}$ met $ad-bc=1$. We kunnen deze transformaties visualiseren in een plaatje dat laat zien hoe het complexe bovenhalfvlak in driehoeken wordt opgedeeld; zie figuur 1.

Als we het product in (1) uitwerken dan krijgen we een machtreeks

$$\begin{aligned}\Delta(z) &= q - 24q^2 + 252q^3 - 1472q^4 \\ &\quad + 4830q^5 - 6048q^6 + \cdots \\ &= \sum_{n\geq 1}\tau(n)q^n,\end{aligned}$$

met $\tau(n)$ geheel. De op deze manier gedefinieerde functie $\tau : \mathbf{Z}_{>0} \to \mathbf{Z}$ heet de *Ramanujan-taufunctie*. Ramanujan merkte een aantal merkwaardige eigenschappen van zijn tau functie op. Onder andere waren daar de volgende drie eigenschappen, die hij niet kon bewijzen:

- Als m en n ondeelbaar zijn dan geldt $\tau(mn) = \tau(m)\tau(n)$ (ofwel τ is *multiplicatief*).
- Voor priemmachten geldt de recurrente betrekking $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$.
- Voor priemgetallen hebben we een ongelijkheid $|\tau(p)| \leq 2p^{11/2}$.

De eerste twee eigenschappen zijn in 1917 door Mordell bewezen, maar de derde is lange tijd onopgelost geweest.

Behalve de bovengenoemde eigenschappen vond Ramanujan ook nog congruenties voor $\tau(n)$ modulo (machten van) de priemgetallen $2, 3, 5, 7, 23$ en 691, bijvoorbeeld

$$\tau(n) \equiv 1 + n^{11} \quad \text{voor alle } n.$$

Serre begon zich af te vragen waarom zulke congruenties niet bestaan modulo andere priemgetallen. In 1968 formuleerde hij een vermoeden waarin werd gesteld dat $\tau(p)$ uit te drukken is in termen van 2-dimensionale Galoisrepresentaties, dat wil zeggen continue homomorfismen $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(K)$ waarbij K een zeker lichaam is. Hij bracht op die manier het modulo ℓ gedrag van $\tau(p)$ in verband met de grens $|\tau(p)| \leq 2p^{11/2}$. Het lukte Deligne in 1969 om het bestaan van zulke representaties aan te tonen en in 1974 slaagde hij erin om hiermee $|\tau(p)| \leq 2p^{11/2}$ te bewijzen. Het bewijs van Deligne gebruikt diepe resultaten uit de algebraische meetkunde; het totale aantal pagina's dat je krijgt als je alles helemaal vanaf het begin zou uitschrijven wordt geschat op 2000. Het zal dus duidelijk zijn dat we in dit korte artikel niet op de details kunnen ingaan.

De vorm Δ is niet uniek hierin. Eigenschappen die vergelijkbaar zijn met die voor de vorm Δ gelden voor veel meer modulaire vormen. De modulaire vormen in kwestie heten *eigenvormen* omdat het eigenvectoren zijn voor bepaalde lineaire operatoren op ruimten van modulaire vormen, de zogenaamde Hecke-operatoren. Bij elke eigenvorm blijken er Galoisrepresentaties gemaakt te kunnen worden. De afgelopen decennia is het verband tussen eigenvormen en Galoisrepresentaties zeer intensief bestudeerd. Een van de grote resultaten die hieruit voortkwam is Wiles' bewijs voor de Laatste Stelling van Fermat. Een ander groot resultaat, dat sterk in verband staat met het werk van Wiles, is het bewijs voor (het grootste deel van) het Serre-vermoeden, gegeven door Khare en Wintenberger. Dit Serre-vermoeden stelt dat een representatie $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(K)$ met K een eindig lichaam slechts aan een paar hele milde voorwaarden hoeft te voldoen om al van een eigenvorm afkomstig te zijn.

Het berekenen van $\tau(n)$

Een vraag die René Schoof aan Bas Edixhoven stelde is of het mogelijk is om $\tau(n)$ efficiënt uit te rekenen. Als we $\tau(p)$ kunnen uitrekenen voor priemgetallen p en n kunnen factoriseren in priemgetallen dan kunnen we, wegens de observaties van Ramanujan, $\tau(n)$ uitrekenen. Als we nu $\tau(p) \mod \ell$ uitrekenen voor zo veel priemgetallen ℓ dat hun product groter dan $4p^{11/2}$ is, dan ligt, gezien de grens voor $|\tau(p)|$ hiermee $\tau(p)$ zelf vast. Met dit in het achterhoofd is Edixhoven een project gestart waarin hij het probleem tracht aan te pakken door de bijbehorende Galoisrepresentaties uit te rekenen.

Het basisidee van de berekeningen komt uit de meetkunde: de Galoisrepresentatie die bij $\tau(p) \mod \ell$ hoort voor een gegeven ℓ kan worden gerealiseerd in een variëteit die $J_1(\ell)$ genoemd wordt en dimensie $(\ell-5)(\ell-7)/24$ heeft. Jean-Marc Couveignes had het idee om hierbij numerieke berekeningen te gebruiken. Om deze ideeën hard te maken lijkt het echter onvermijdelijk om *Arakelovmeetkunde* te gebruiken; op dit punt kon Robin de Jong zijn steentje bijdragen aan het project. Hierbij is gebruikgemaakt van een resultaat van Franz Merkl, iemand uit de kansrekening. Voor details zie [3].

Er is echter één nadeel aan het algoritme van Edixhoven, Couveignes en De Jong: het is praktisch onuitvoerbaar. Zo is de rekenprecisie veel te hoog en ook kunnen we niet gebruikmaken van de variëteit $J_1(\ell)$ maar moeten we naar $J_1(5\ell)$ gaan, waarvan de dimensie $(\ell-2)^2$ is. In de praktijk kunnen we deze bezwaren negeren en gewoon gaan rekenen. We krijgen polynomen met coëfficiënten van een hoge precisie (denk hier aan enkele duizenden decimalen). We weten dat de coëfficiënten benaderingen zijn van rationale getallen. Als de benadering sterk genoeg is, dan gokken we dat de rationale getallen waar ze dichtbij liggen de daadwerkelijke coëfficienten zijn van de polynomen die bij de representaties horen. We moeten dan wel nog achteraf nagaan dat het verkregen polynoom correct is. Dankzij het feit dat het Serrevermoeden nu bewezen is, is dit allemaal goed te doen.

Uiteraard geldt ook hier dat we niet tot de taufunctie beperkt zijn. De rekenmethoden werken met eigenvormen in het algemeen. Dit heeft leuke toepassingen in de computationele inverse Galoistheorie.

Computationele inverse Galoistheorie

Een van de grote problemen in de algebraïsche getaltheorie is de vraag of er voor elke eindige groep G een polynoom met rationale coëfficiënten bestaat waarvan de Galoisgroep isomorf is met G. Men vermoedt dat elke eindige groep voorkomt als Galoisgroep van een polynoom, maar een bewijs hiervoor lijkt voorlopig nog niet in zicht. Voor een aantal soorten groepen is het echter al wel bekend: zo heeft Shafarevich in 1954 bijvoorbeeld bewezen dat elke *oplosbare* groep optreedt als Galoisgroep van een polynoom over $\mathbf{Q}$. De beruchte lijst sporadische simpele groepen is op één groep na (de zogenaamde Matthieugroep M_{23}) gerealiseerd als Galoisgroep. Een andere vraag die je in deze context kunt stellen is of je voor een gegeven eindige groep ook een polynoom kunt *uitrekenen* met deze Galoisgroep. Dit is de favoriete sport van Jürgen Klüners en Gunter Malle, zie [5]. Zij hebben verscheidene technieken ontwikkeld en daarmee is het ze gelukt om voor alle transitieve permutatiegroepen tot en met graad 15 een polynoom te produceren. Al hun

technieken zijn erop gefocust om geparametriseerde families van polynomen te produceren.

Er zijn soorten groepen die niet behandeld kunnen worden met de technieken van Klüners en Malle. De eenvoudigste groep waarvoor ze geen polynoom konden maken is $\mathrm{SL}_2(\mathbf{F}_{16})$, de groep van 2-bij-2 matrices met determinant 1 over het lichaam van 16 elementen. Deze groep heeft 4080 elementen en treedt op als permutatiegroep van graad 17: ze permuteert de elementen van $\mathbf{P}^1(\mathbf{F}_{16}) = \mathbf{F}_{16} \cup \{\infty\}$ door gebroken lineaire transformaties:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x := \frac{ax+b}{cx+d}.$$

Het bestaan van een polynoom voor $\mathrm{SL}_2(\mathbf{F}_{16})$ was al wel aangetoond door Mestre, maar een expliciet voorbeeld ontbrak nog. Op dit punt komen berekeningen met Galoisrepresentaties voor modulaire vormen van pas. We weten dat een polynoom met Galoisgroep $\mathrm{SL}_2(\mathbf{F}_{16})$ grofweg hetzelfde is als een continu surjectief homomorfisme $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{SL}_2(\mathbf{F}_{16})$ en dat we bij modulaire vormen Galoisrepresentaties $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(K)$ kunnen maken met K een zeker lichaam. Als we nu een modulaire vorm kunnen vinden waarbij we zo'n representatie kunnen maken met $K = \mathbf{F}_{16}$ waarvan het beeld $\mathrm{SL}_2(\mathbf{F}_{16})$ is dan weten we dus al dat zo'n polynoom bestaat.

Een eenvoudige search met de computer laat al snel zien dat zulke modulaire vormen bestaan. We kunnen met deze vormen gaan rekenen en daarmee polynomen produceren. Laten we ook inderdaad een polynoom met Galoisgroep $\mathrm{SL}_2(\mathbf{F}_{16})$ geven (voor details zie [1]):

$$\begin{aligned} & x^{17} - 5x^{16} + 12x^{15} - 28x^{14} + 72x^{13} \\ & - 132x^{12} + 116x^{11} - 74x^9 + 90x^8 \\ & - 28x^7 - 12x^6 + 24x^5 - 12x^4 \\ & - 4x^3 - 3x - 1. \end{aligned}$$

Een aardige bijkomstigheid is dat John Jones en David Roberts een soortgelijke sport als Klüners en Malle beoefenen. In plaats van naar polynomen met gegeven Galoisgroep zijn zij op zoek naar polynomen waarvan het splijtlichaam een zogenoemde kleine worteldiscriminant hebben, zie [4]. Als we uitgaan van de gegeneraliseerde Riemannhypothese, dan zijn dit soort getallenlichamen zeer dun gezaaid en daarom is het interessant om ernaar te zoeken. David Roberts maakte de auteur erop attent dat het bovenstaande polynoom aan hun lijst ontbrak. Een andere groep die ontbrak in de tabellen van Klüners en Malle is de groep $\mathrm{PSL}_2(\mathbf{F}_{25})$, de groep van gebroken lineaire transformaties met determinant 1 en coëfficiënten in $\mathbf{F}_{25}$. Deze groep heeft 7800 elementen en permuteert $\mathbf{P}^1(\mathbf{F}_{25})$. Het volgende polynoom heeft haar als Galoisgroep:

$$\begin{aligned} & x^{26} + 25x^{24} - 90x^{23} + 410x^{22} \\ & - 2174x^{21} + 7915x^{20} - 24445x^{19} \\ & + 82385x^{18} - 174360x^{17} + 340352x^{16} \\ & - 596725x^{15} + 606925x^{14} - 845215x^{13} \\ & + 2199840x^{12} - 1523031x^{11} + 203295x^{10} \\ & - 2102590x^9 + 1804065x^8 - 28770x^7 \\ & - 35747x^6 + 674760x^5 - 134800x^4 \\ & + 150735x^3 - 2885x^2 + 64x - 5. \end{aligned}$$

We sluiten niet uit dat er in de nabije toekomst nog een paar andere groepen aan het lijstje worden toegevoegd.

Referenties

1 J. G. Bosman, 'A polynomial with Galois group $\mathrm{SL}_2(\mathbf{F}_{16})$', *LMS J. Comput. Math.* **10** (2007) 378–388.

2 F. Diamond en J. Im, 'Modular forms and modular curves', *Seminar on Fermat's Last Theorem* (Toronto, ON, 1993-1994) CMS Conf. Proc., **17**, Amer. Math. Soc., Providence, RI, 1995, 39–133.

3 S. J. Edixhoven, J.-M. Couveignes, R. S. de Jong, F. Merkl, J. G. Bosman, 'On the computation of coefficients of a modular form', eprint, 2006, arXiv reference math.NT/0605244v1.

4 J. W. Jones en D. P. Roberts, 'Galois number fields with small root discriminant', *J. Number Theory* **122** (2007) 379–407.

5 J. Klüners en G. Malle, 'Explicit Galois realization of transitive groups of degree up to 15', *J. Symbolic Comput.* **30** (2000) no. 6, 675–716.