Drankadvies: Jus d'orange

Symmetrieën in de getaltheorie voor natuurkundigen

Bas Edixhoven *Professor Universiteit Leiden*

Wiskunde en Natuurkunde

Natuurkundigen bestuderen de wereld om ons heen, de zogenaamde echte wereld waarin (bijna) niets echt zeker is, terwijl wiskundigen een geïdealiseerde, abstracte wereld bestuderen. Sinds ongeveer 100 jaar zijn de spelregels van de wiskunde vastgelegd en niet meer veranderd: de taal waarin uitspraken gedaan worden, de axioma's (ZFC verzamelingentheorie), en de logica waarmee men nieuwe uitspraken uit al bewezen uitspraken kan afleiden. Bij het vinden van deze afleidingen zijn intuïtie en creativiteit essentieel, kunstmatige intelligentie kan er denk ik nog bijna niets. In de wiskunde is er geen onenigheid over wat er nu wel en niet bewezen is, en als er onduidelijkheid is dan vraagt men gewoon naar meer details. Er is ook een grote mate van overeenstemming met welke vragen en ontwikkelde technieken het belangrijkst zijn, zie maar de lijsten die in 1900 en in 2000 zijn geproduceerd.

In hun pogingen de echte wereld te beschrijven gebruiken natuurkundigen de wiskunde. Galileo zei al dat de wetten van de natuurkunde geschreven zijn in de taal van de wiskunde en Wigner schreef in 1960 zijn artikel 'The Unreasonable Effectiveness of Mathematics in the Natural Sciences'. De wiskunde die natuurkundigen gebruiken is meestal beperkt tot meetkunde en analyse; de ruimtetijd is meetkundig en omdat het gaat over dingen die bewegen, moet het met differentiaalvergelijkingen. Ik hoef hier niet aan natuurkundigen uit te leggen wat symmetrieën in de meetkunde en analyse zijn.

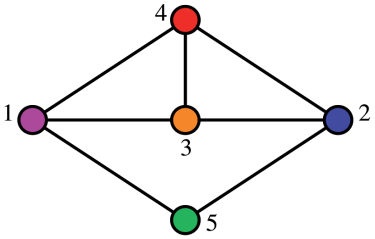
Maar er is meer wiskunde dan dat. Er is bijvoorbeeld de getaltheorie. Het zogenaamde 'Langlandsprogramma' (zie bijvoorbeeld [1], waaruit ik schaamteloos ga zelfplagiëren) gaat over verbanden tussen symmetrieën in de analyse en meetkunde enerzijds en symmetrie in de getaltheorie anderzijds. Van de 17 tot nu toe uitgereikte Abelprijzen waren er 5 voor bijdragen aan de getaltheorie, dus kennelijk is getaltheorie belangrijk voor wiskundigen.

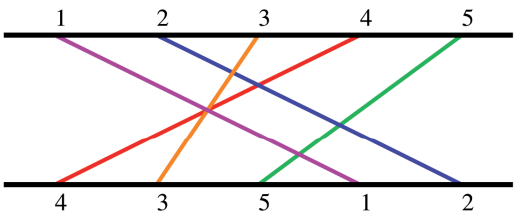
Getallen

Getaltheoretici bestuderen systemen van getallen, zoals die van de reële getallen $\mathbb{R}$, complexe getallen $\mathbb{C}$ en rationale getallen $\mathbb{Q}$, tezamen met de optelling en vermenigvuldiging op elk van deze systemen. Ze zien $\mathbb{R}$ niet altijd als een lijn, en $\mathbb{C}$ niet als een vlak, maar als het ze uitkomt ook als een $\mathbb{Q}$-vectorruimte, van oneindige (zelfs overaftelbare) dimensie. Een complex getal z is algebraïsch als de elementen $1, z, z^2, \ldots$ lineair afhankelijk zijn in de $\mathbb{Q}$-vectorruimte $\mathbb{C}$. Als z niet algebraïsch is, dan heet z transcendent. Bijvoorbeeld: $\sqrt{2}$ is algebraïsch maar niet rationaal, π en e zijn transcendent. Hier zijn we alleen geïnteresseerd in algebraïsche getallen en dat wil zeggen: complexe nulpunten van polynomen $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ met $n > 0$ en alle a_i in $\mathbb{Q}$.

Symmetrieën in de getaltheorie

De symmetrieën in de getaltheorie zijn de permutaties van de nulpunten van zulke polynomen die gegeven worden door lichaamsautomorfismen van $\mathbb{C}$. Een lichaamsautomorfisme van $\mathbb{C}$ is een afbeelding $\sigma: \mathbb{C} \to \mathbb{C}$ die bijectief is (dat wil zeggen dat voor elke z in $\mathbb{C}$ er precies één w in $\mathbb{C}$ is met $\sigma(w) = z$), en compatibel is met optelling en vermenigvuldiging in de zin dat voor alle x en y in $\mathbb{C}$ geldt dat $\sigma(x + y) = \sigma(x) + \sigma(y)$ en $\sigma(xy) = \sigma(x)\sigma(y)$. We kennen precies 2 zulke σ: de identiteit, en de complexe conjugatie. Het is niet





moeilijk te bewijzen dat dit precies de continue zijn. In een tweedejaars algebracollege kan bewezen worden dat er vreselijk veel σ zijn. Bijvoorbeeld kan men beginnen met de afbeelding $a+b\sqrt{2}\to a-b\sqrt{2}$ (met a en b die $\mathbb{Q}$ doorlopen) en die geschikt uitbreiden naar $\mathbb{C}$.

Voor $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ met $n > 0$ en de a_i in $\mathbb{Q}$ laten we $Z(f)$ de verzameling van complexe nulpunten van f zijn. Dan is het eenvoudig in te zien dat elk lichaamsautomorfisme σ van $\mathbb{C}$ de elementen van $Z(f)$ permuteert. De Galoisgroep Gal(f) van f is dan de verzameling van permutaties van $Z(f)$ die gegeven zijn door lichaamsautomorfismen van $\mathbb{C}$; als we twee van deze permutaties samenstellen dan is het er weer één, dus het is een groep.

Een voorbeeld, in de stijl van Galois, is gegeven door $x^7 - 2$. De nulpunten zijn dan de $\zeta^x z$, met $\zeta = e^{2\pi i/7}$, $z = 2^{1/7}$, en x in {0,1,2,3,4,5,6} (de hoekpunten van een regelmatige 7-hoek op de cirkel om 0 met straal $2^{1/7}$ in het complexe vlak). Laat nu σ een lichaamsautomorfisme van $\mathbb{C}$ zijn. Dan $\sigma(\zeta)^7 = \sigma(\zeta^7) = \sigma(1) = 1$, dus is er een a in {1,2,3,4,5,6} met $\sigma(\zeta) = \zeta^a$. En $\sigma(z)^7 = \sigma(z7) = \sigma(2) = \sigma(1 + 1) = \sigma(1) + \sigma(1) = 2$, dus is er een b in {0,1,2,3,4,5,6} met $\sigma(z) = \zeta^b z$. Dan geldt voor elke x in {0,1,2,3,4,5,6} dat $\sigma(\zeta^x z) = \sigma(\zeta)^x\sigma(z) = (\zeta^a)x(\zeta^b z) = \zeta^{ax+b}z$, waarbij de $ax + b$ modulo 7 genomen moet worden, bijvoorbeeld $2 \cdot 3 + 5 = 4$. Dit getalssysteem 'gehele getallen modulo 7' wordt als $\mathbb{Z}/7\mathbb{Z}$ genoteerd en de vermenigvuldiggroep van elementen ongelijk 0 als $(\mathbb{Z}/7\mathbb{Z})^\times$. Gauss liet al zien dat er voor alle a in $(\mathbb{Z}/7\mathbb{Z})^\times$ en b in $\mathbb{Z}/7\mathbb{Z}$ er een lichaamsautomorfisme $\sigma_{a,b}$ van $\mathbb{C}$ is zodat voor alle x in $\mathbb{Z}/7\mathbb{Z}$ geldt dat $\sigma_{a,b} : \zeta^x z \to \zeta^{ax+b}z$. Kennelijk is Gal($x^7 - 2$) de groep van affiene transformaties $x \to ax + b$ van $\mathbb{Z}/7\mathbb{Z}$.

$\zeta = e^{2\pi i/7}$
$z = 2^{1/7}$
$a \in (\mathbb{Z}/7\mathbb{Z})^\times$
$b \in \mathbb{Z}/7\mathbb{Z}$
$x \in \mathbb{Z}/7\mathbb{Z}$
$\sigma_{a,b}: \zeta^x z \to \zeta^{ax+b}z$

Voor de meeste f is Gal(f) de groep van alle permutaties van $Z(f)$ en dus isomorf met S_n, maar het vermoeden (onopgelost) is dat alle eindige groepen voorkomen als Galoisgroep. Voor commutatieve eindige groepen (en algemener voor oplosbare eindige groepen) is dit bekend. De stelling van Kronecker-Weber zegt dat Gal(f) commutatief is precies dan als $Z(f)$ bestaat uit Q-lineaire combinaties van eenheidswortels.

Kan natuurkunde bijdragen aan getaltheorie? Mijn hoop is van wel, maar op dit moment schiet mij alleen te binnen dat Ngo Bao Chau een Fieldsmedaille heeft gekregen voor zijn bewijs van het *fundamentele lemma* in het Langlandsprogramma en dat zijn methode Hitchin vezelingen gebruikt die geïnspireerd zijn door integreerbare systemen uit de klassieke mechanica.

Prof. Bas Edixhoven is docent en onderzoeker van de Arithmetic Geometry research group aan de Universiteit Leiden en geeft daarnaast vele colleges en lezingen. Contact: edix@math.leidenuniv.nl

Referenties

[1] Edixhoven, Bas. Abelprijs toegekend aan Robert Langlands. Nieuw Arch. Wiskd. (5) 20 (2019), no. 1, 12–18. http://pub.math.leidenuniv.nl/~edixhovensj/publications/2019/nieuw_archief_langlangds.pdf