Bas Edixhoven
*Mathematisch Instituut*
*Universiteit Leiden*
*bas@edixhoven.net*

**Evenement** Abelprijs 2018

# Abelprijs toegekend aan Robert Langlands

**In maart 2018 werd de Abelprijs toegekend aan Robert Langlands voor zijn 'visionaire programma dat representatietheorie verbindt met getaltheorie', zie [1]. In dit artikel legt Bas Edixhoven in lekentaal uit waarom het gaat: verbanden tussen symmetrieën in de analyse en meetkunde enerzijds, en symmetrieën in de getaltheorie anderzijds.**

Sinds maart 2018 zijn al een aantal publicaties over dit onderwerp verschenen: [4] (technisch en lang, veel recent werk), [2] (biografisch, geen wiskunde), [11] (wel wiskunde maar niet voor leken), [10] (zowel tekst als video, geen wiskunde), [5] (wel voor leken, 2 pagina's, aanbevolen), [20] (2 pagina's, aanbevolen!) en [21] (4 pagina's, meer inhoudelijk, aanbevolen!), [16] (zowel historisch als wiskundig, maar lang en (wiskundig) niet zo toegankelijk). Voor het werk van Langlands zelf, inclusief de beroemde brief naar Weil, zie [14]. Ook [8] (gedeeltelijk over Langlands, maar zonder representatietheorie) is aanbevolen.

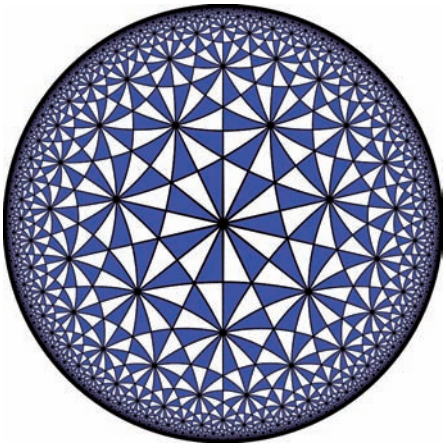
Als er dan al zoveel over geschreven is, waarom dan *nog* een artikel? Wel, ik had al in een vroeg stadium de redactie van het NAW beloofd er een te schrijven, en de bovengenoemde artikelen bekeken hebbend, vind ik dat er ruimte is voor een artikel dat iedereen die een studie wiskunde heeft afgerond een laagdrempelig inkijkje biedt in het Langlands-programma (de volgende twee paragrafen, de appetizers van dit artikel), en degene die er meer tijd in wil steken en wat wil leren een weg wijst *naar* het Langlands-programma (de overige paragrafen, de hoofdgerechten en het dessert). Ook beoog ik lezers met wat meer achtergrond te overtuigen dat het Langlands-programma wel ontdekt *moest* worden, gezien wat er al bekend was rond 1966. Ik hoop dat hiermee het aura van mystiek rond het Langlands-programma wat vervaagt en dat er wat begrip en terechte verwondering voor in de plaats komt. Het is allemaal erg mooi, indrukwekkend en wonderlijk (dat het werkt), maar eigenlijk geen wonder dat het ontdekt is.

## Symmetrieën in getaltheorie en analyse

Zo ongeveer het eenvoudigste voorbeeld van symmetrieën van getaltheoretische oorsprong in de analyse en meetkunde is dat van translaties op de reële getallenlijn $\mathbb{R}$ over gehele getallen $\mathbb{Z}$. Precies dat voorbeeld leidt tot de analytische voortzetting en de functionaalvergelijking van Riemanns zèta-functie, en dat is het onderwerp van de volgende paragraaf. Fourieranalyse, Poissons sommatieformule en de normale kansverdeling van Gauss spelen daar cruciale rollen.

In de paragraaf '$L$-functies' zien we dat Riemanns zèta-functie correspondeert met de triviale symmetriegroep in de getaltheorie. Om algemene symmetrieën uit de getaltheorie te krijgen moeten we in de analyse en meetkunde onze blik wat verruimen, en kijken naar: *harmonische analyse op lokaal compacte groepen, met randcondities van getaltheoretische oorsprong*. Zie bijvoorbeeld Figuur 1. We zien hier het schijfmodel van het hyperbolische vlak, betegeld door driehoeken met hoeken $\pi/2$, $\pi/3$ en $\pi/7$, bekend (met iets andere hoeken) van Eschers cirkellimiettekeningen. De geodeten zijn cirkels die de rand van de schijf loodrecht snijden. De lokaal compacte groep die hierbij hoort is die van complexe $2\times2$-matrices $\left(\begin{smallmatrix} a & \bar{c} \\ c & \bar{a} \end{smallmatrix}\right)$ met $|a|^2-|c|^2=1$, die op de complexe eenheidsschijf werkt door de oriëntatiebehoudende isometrieën $z \mapsto (az+\bar{c})/(\bar{c}z+a)$. Er zijn ook de oriëntatieomkerende isometrieën $z \mapsto (a\bar{z}+\bar{c})/(\bar{c}\bar{z}+a)$. De betegeling geeft een voorbeeld van randcondities van getaltheoretische oorsprong (technisch gesproken: de spiegelingen in de doorgetrokken zijden van de driehoeken brengen een aritmetische ondergroep voort).

De transformatie $z \mapsto i(1-z)/(1+z)$ brengt de eenheidsschijf naar het complexe bovenhalfvlak en identificeert de matrixgroep hierboven met $\mathrm{SL}_2(\mathbb{R})$, de groep van reële $2\times2$-matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ met determinant $1$, die werkt door $z \mapsto (az+b)/(cz+d)$. On-



**Figuur 1**

dergroepen van eindige index van $\mathrm{SL}_2(\mathbb{Z})$ geven veel voorbeelden van aritmetische ondergroepen, en dit generaliseert direct naar $\mathrm{SL}_n(\mathbb{R})$ en $\mathrm{SL}_n(\mathbb{Z})$ voor willekeurige $n$.

Het is niet verbazend dat de theorie van continue representaties van $\mathrm{SL}_n(\mathbb{R})$ op complexe Hilbertruimten *het* gereedschap is om Fourieranalyse naar deze situatie te generaliseren. Voor compacte groepen zoals bijvoorbeeld die van $n\times n$-orthogonale reële of unitaire complexe matrices is er de stelling van Peter–Weyl, die zegt dat de matrixcoëfficiënten ten opzichte van orthogonale bases van de irreducibele continue representaties (die in dit geval eindigdimensionaal zijn en een invariant inproduct hebben) een Hilbertbasis van de Hilbertruimte van kwadraatintegreerbare functies op de groep geven. Voor niet-compacte groepen, zoals $\mathrm{SL}_n(\mathbb{R})$, zijn bijna alle irreducibele continue representaties op complexe Hilbertruimten oneindig dimensionaal, en veel moeilijker te classificeren.

Onder de aritmetische ondergroepen zijn er de zogenaamde *congruentie-ondergroepen*, gegeven door congruentie-voorwaarden op de coëfficiënten, zoals bijvoorbeeld de ondergroep van elementen $g$ van $\mathrm{SL}_n(\mathbb{Z})$ waarvan de $g_{i,j}$ met $i\neq j$ deelbaar zijn door een gegeven geheel getal $m\neq 0$, en waarvan de $g_{i,i}$ rest $1$ geven na deling door $m$. Dit zijn de ondergroepen die in het Langlands-programma horen. Als men de harmonische analyse voor deze allemaal tegelijk bestudeert, dan komen er ook vanzelf matrixgroepen met *$p$-adische* lichamen $\mathbb{Q}_p$ naar voren, voor alle priemgetallen $p$, of men nu wil of niet (dit wordt duidelijk in de paragraaf 'Automorfe representaties van $\mathbf{GL}_n$ over $\mathbb{Q}$'). In de paragraaf 'Cyclotomische lichamen' laten we zien dat de $p$-adische getallen zichzelf net zo opdringen in de getaltheorie. Dit leidt ertoe dat men ook de theorie van representaties op complexe Hilbertruimten van groepen als $\mathrm{SL}_n(\mathbb{Q}_p)$ nodig heeft. Deze groepen zijn ook lokaal compact, en, net als $\mathbb{Q}_p$ zelf, 'totaal onsamenhangend'.

Nu is het tijd om eens te kijken naar symmetrieën in de getaltheorie. Getaltheoretici 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, $\pi$ en $e$ zijn transcendent. In dit artikel zijn we alleen geïnteresseerd in algebraïsche getallen, en dat wil zeggen: complexe nulpunten van polynomen $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ met $n > 0$ en alle $a_i$ in $\mathbb{Q}$. 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, 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 twee zulke $\sigma$: de identiteit en de complexe conjugatie. Het is niet moeilijk te bewijzen dat dit precies de continue zijn. Met Zorns lemma is makkelijk te bewijzen dat er vreselijk veel $\sigma$ zijn, evenveel als de machtsverzameling van $\mathbb{R}$. Bijvoorbeeld kan men beginnen met de afbeelding $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (met $a$ en $b$ die $\mathbb{Q}$ doorlopen), en die uitbreiden naar $\mathbb{C}$. Een wat interessanter voorbeeld, in de stijl van Galois, is gegeven door de werking van de lichaamsautomorfismen van $\mathbb{C}$ op de nulpunten van $x^5 - 2$:

$$\begin{aligned}
&\zeta = e^{2\pi i/5},\\
&z = 2^{1/5},\\
&a \in (\mathbb{Z}/5\mathbb{Z})^\times,\\
&b \in \mathbb{Z}/5\mathbb{Z},\\
&x \in \mathbb{Z}/5\mathbb{Z},\\
&\sigma_{a,b} : \zeta^x z \mapsto \zeta^{ax+b} z.
\end{aligned}$$

Voor $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 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 $\sigma$ van $\mathbb{C}$ de elementen van $Z(f)$ permuteert. De *Galoisgroep* $\mathrm{Gal}(f)$ *van* $f$ is dan de groep van permutaties van $Z(f)$ die gegeven zijn door lichaamsautomorfismen van $\mathbb{C}$. Voor de meeste $f$ is $\mathrm{Gal}(f)$ 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 $\mathrm{Gal}(f)$ commutatief is precies dan als $Z(f)$ bestaat uit $\mathbb{Q}$-lineaire combinaties van eenheidswortels. In de paragraaf 'Cyclotomische lichamen' bestuderen we de lichaamsautomorfismen van het lichaam voortgebracht door

Évariste Galois

eenheidswortels, en dienen de $p$-adische getallen zich aan.

Groepen worden vaak bestudeerd door middel van hun representaties, want matrices zijn makkelijker dan permutaties, en zo ook voor Galoisgroepen $\mathrm{Gal}(f)$. Een complexe representatie $\rho : \mathrm{Gal}(f) \to \mathrm{GL}_d(\mathbb{C})$ (of anders gezegd een werking van de eindige groep $\mathrm{Gal}(f)$ op de complexe vectorruimte $\mathbb{C}^d$) heet een *(complexe) Galoisrepresentatie*. Voor zo'n representatie $\rho$ definieerde Artin een generalisatie van de Riemann-zèta-functie, de zogenaamde *Artin-$L$-functie van* $\rho$ (zie de paragraaf '$L$-functies'). Voor deze functies, gedefinieerd als een Dirichletreeks die convergent is voor complexe $s$ met $\Re(s) > 1$, wordt vermoed dat ze analytisch uitbreiden over $\mathbb{C}\setminus\{1\}$, en dat er een functionaalvergelijking is tussen de $L$-functie van $\rho$ in $s$ en van de $L$-functie van de duale van $\rho$ in $1 - s$.

Langlands stelde zich in 1966, optimistisch extrapolerend wat er toen al bekend was, twee vragen (zie de slotparagraaf) over dit soort $L$-functies en zogenaamde automorfe representaties. Dit leidde tot de zogenaamde Langlands-vermoedens, zowel in het globale geval (congruentie-ondergroepen enerzijds, en automorfismen van eindige lichaamsuitbreidingen van $\mathbb{Q}$ anderzijds) als het lokale geval: representatietheorie van $p$-adische matrixgroepen enerzijds en automorfismen van eindige uitbreidingen van $\mathbb{Q}_p$ anderzijds.

Sinds 1966 is er al veel bereikt, vooral wat betreft de lokale vermoedens. De globale theorie is nog niet zo ver, al is het zo dat fragmenten ervan veel hebben bij-

gedragen aan de lokale theorie. Het werk van Wiles over modulariteit van elliptische krommen over $\mathbb{Q}$ in het begin van de jaren 1990 (Abelprijs in 2016) met als gevolg daarvan de laatste stelling van Fermat, was de grootste doorbraak tot nu toe. De lokale theorie, en ook speciale waarden van $L$-functies, zijn hierin onmisbaar. Maar het belangrijkste nieuwe ingrediënt bij Wiles was de studie van Galoisrepresentaties met waarden in $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ met $p$ vast en $m$ variërend, dat wil zeggen 'deformatietheorie' van Galoisrepresentaties.

We weten nu dat de continue irreducibele representaties van $\mathrm{GL}_n(\mathbb{Q}_p)$ op complexe Hilbertruimten nauw samenhangen met $n$-dimensionale representaties van groepen van lichaamsautomorfismen van eindige uitbreidingen van $\mathbb{Q}_p$. Zowel getaltheoretici als representatietheoretici moeten hiermee hun voordeel kunnen doen, door de problemen waarmee ze worstelen te vertalen naar 'de andere kant'. Voor representatietheoretici geeft dit het inzicht dat het beschrijven van *alle* continue irreducibele representaties van $\mathrm{GL}_n(\mathbb{Q}_p)$ op complexe Hilbertruimten minstens even moeilijk is als het beschrijven van de Galoisrepresentaties aan de andere kant, en dat wat correspondeert met tam vertakte Galoisrepresentaties wel een eenvoudige systematische beschrijving toe moet laten. Voor de getaltheoretici ligt de winst meer in de globale theorie: analytische eigenschappen van de $L$-functies bij Galois-representaties en van andere generalisaties van Riemanns zèta-functie, en generalisaties van de laatste stelling van Fermat (zie [8]).

**Riemanns zèta-functie**

We beschrijven nu, in navolging van Riemann, hoe de translaties op de reële getallenlijn $\mathbb{R}$ over gehele getallen $\mathbb{Z}$ leiden tot de voortzetbaarheid en de functionaalvergelijking van de belangrijkste functie in de getaltheorie: Riemanns zèta-functie.

We moeten dan beginnen met Jacobi's theta-functie op het complexe bovenhalfvlak $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$:

$$\theta : \mathbb{H} \to \mathbb{C}, \quad z \mapsto \sum_{n\in\mathbb{Z}} e^{\pi i z n^2}. \tag{1}$$

(Wie deze functie opzoekt op Wikipedia ziet daar een functie van twee variabelen $z$ en $\tau$; neem daar $z = 0$ en vervang dan $\tau$ door $z$.) Jacobi bewees al dat voor alle $z \in \mathbb{H}$ geldt dat

$$\theta(-1/z) = (-iz)^{1/2}\theta(z), \tag{2}$$

waarbij $(-iz)^{1/2}$ de wortel is met positief reëel deel (merk op dat $\Re(-iz) > 0$). We schetsen het bewijs van (2), omdat het zo mooi verschillende gebieden van de wiskunde verbindt; voor een gedetailleerde behandeling, zie [19, VII, §6, Proposition 16]. Het gaat hier om een gelijkheid van complex analytische functies op $\mathbb{H}$, dus het volstaat om (2) te bewijzen voor de $z = iy$ met $y \in \mathbb{R}_{>0}$. Er geldt, voor alle $y \in \mathbb{R}_{>0}$:

$$\theta(iy) = \sum_{n\in\mathbb{Z}} f_y(n),$$
$$\text{met } f_y : \mathbb{R} \to \mathbb{R},\ x \mapsto e^{-\pi x^2 y}. \tag{3}$$

We herkennen hier $f_y$, op een constante factor na, als Gauss' normale verdeling met gemiddelde $0$ en, op een constante factor na, standaardafwijking $y^{-1/2}$. De Fouriergetransformeerde hiervan is

$$\hat{f}_y : \mathbb{R} \to \mathbb{R}, \quad x \mapsto y^{-1/2} e^{-\pi x^2/y}. \tag{4}$$

Poissons sommatieformule geeft, voor alle $y \in \mathbb{R}_{>0}$:

$$\theta(iy) = \sum_{n\in\mathbb{Z}} f_y(n) = \sum_{n\in\mathbb{Z}} \widehat{f_y}(n)$$
$$= y^{-1/2}\theta(-1/iy), \tag{5}$$

waarmee het bewijs van (2) af is!

Het verband tussen $\theta$ en Riemanns zèta-functie

$$\zeta : \{s \in \mathbb{C} : \Re(s) > 1\} \to \mathbb{C}, \quad s \mapsto \sum_{n\geq 1} n^{-s}, \tag{6}$$

is de Mellintransformatie: dit is een variant van de Fouriertransformatie die grofweg gezegd $t \mapsto e^{-\pi n t}$ omzet in $s \mapsto n^{-s}$. Voor $g : \mathbb{R}_{>0} \to \mathbb{C}$ is deze gegeven, voor de $s \in \mathbb{C}$ waarvoor het nodige convergeert, door:

$$M(g) : s \mapsto \int_{t=0}^{\infty} g(t)\, t^s\, (dt)/t. \tag{7}$$

We nemen nu $g : \mathbb{R}_{>0} \to \mathbb{C}$ gegeven door

$$g(t) = \frac{\theta(it) - 1}{2} = \sum_{n>0} e^{-\pi n^2 t}. \tag{8}$$

Dan volgt uit (2) (voor details zie [9, §4.9]) dat voor $s \in \mathbb{C}$ met $\Re(s) > 1$ geldt dat

$$\xi(s) := \pi^{-s/2}\Gamma(\tfrac{s}{2})\,\zeta(s) = (M(g))\,(\tfrac{s}{2}), \tag{9}$$

dat $s \mapsto \xi(s) - s^{-1} - (1-s)^{-1}$ holomorf is op $\mathbb{C}$ en dat voor alle $s \in \mathbb{C}$:

$$\xi(1-s) = \xi(s). \tag{10}$$

Hiermee zijn de voortzetbaarheid en de functionaalvergelijking van $\zeta$ bewezen, zoals Riemann het al deed in 1859.

**Cyclotomische lichamen**

Het is weer tijd om naar symmetrieën in de getaltheorie te kijken. Het eenvoudigste voorbeeld hiervan is wellicht het lichaam $\mathbb{Q}(\sqrt{2})$: de deelverzameling van $\mathbb{C}$ van alle getallen die je kunt krijgen uit rationale getallen en $\sqrt{2}$ door optellen, aftrekken, vermenigvuldigen en delen. Omdat $\sqrt{2}$ niet rationaal is, is $\mathbb{Q}(\sqrt{2})$ een $\mathbb{Q}$-vectorruimte met basis $1$ en $\sqrt{2}$. Men gaat dan eenvoudig na dat de afbeelding $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ ($a$ en $b$ in $\mathbb{Q}$) van $\mathbb{Q}(\sqrt{2})$ naar zichzelf optelling en vermenigvuldiging behoudt, en dus een lichaamsautomorfisme is. Dit drukt uit dat, voor zover optelling en vermenigvuldiging betreft, $\sqrt{2}$ en $-\sqrt{2}$ exact dezelfde eigenschappen hebben, net als $i$ en $-i$ in $\mathbb{C}$. We herhalen nog maar eens ons motto:

*De symmetrieën in de getaltheorie zijn lichaamsautomorfismen.*

We definiëren $\bar{\mathbb{Q}}$ als de verzameling van alle complexe getallen $z$ die nulpunt zijn van een polynoom $x^n + \cdots + a_1 x + a_0$, met $n \geq 1$ en alle $a_i \in \mathbb{Q}$. Deze deelverzameling van $\mathbb{C}$ is gesloten onder $+$ en $\cdot$, is dus een lichaam, en heet de *algebraïsche afsluiting* van $\mathbb{Q}$ in $\mathbb{C}$. Het is de aftelbare vereniging van alle deellichamen van $\mathbb{C}$ die eindigdimensionaal zijn als $\mathbb{Q}$-vectorruimte.

De groep van lichaamsautomorfismen $\mathrm{Aut}(\bar{\mathbb{Q}})$ heet de *absolute Galois groep van* $\mathbb{Q}$. Deze groep werkt op $\bar{\mathbb{Q}}$, en heeft een topologische structuur die we iets nader moeten toelichten. Voor elk polynoom $f \in \mathbb{Q}[x]$ ongelijk aan $0$ permuteert $\mathrm{Aut}(\bar{\mathbb{Q}})$ de eindig vele nulpunten van $f$ in $\bar{\mathbb{Q}}$. De banen zijn de nulpuntsverzamelingen van de irreducibele factoren van $f$. In het bijzonder zijn de elementen van $\mathbb{Q}$ de enige vaste punten. Het beeld van $\mathrm{Aut}(\bar{\mathbb{Q}})$ in de permutatiegroep van de nulpunten, zeg $z_1, \ldots, z_n$, van $f$ heet de Galoisgroep van $f$; het is de automorfismengroep van het lichaam $\mathbb{Q}(z_1, \ldots, z_n)$ voortgebracht door de $z_i$. Het geven van een $\sigma \in \mathrm{Aut}(\bar{\mathbb{Q}})$ is equivalent met het geven van automorfismen van al dit soort lichamen $\mathbb{Q}(z_1, \ldots, z_n)$, compatibel op doorsneden: de beperkingen van de automorfismen tot de doorsneden moeten gelijk zijn. Dit betekent dat $\mathrm{Aut}(\bar{\mathbb{Q}})$ de *limiet* is van het diagram van de $\mathrm{Aut}(\mathbb{Q}(z_1, \ldots, z_n))$, omgekeerd geordend naar inclusies. Dit lijkt nu ingewikkeld, maar zo meteen zien we een eenvoudiger voorbeeld. Topologisch betekent dit dat als we $\mathrm{Aut}(\bar{\mathbb{Q}})$ voorzien van de grofste to-

pologie waarvoor alle stabilisatoren van elementen in $\bar{\mathbb{Q}}$ open zijn, $\mathrm{Aut}(\bar{\mathbb{Q}})$ Hausdorff, compact en totaal onsamenhangend is. Ook dit wordt straks in het voorbeeld duidelijker.

Laat $\mathbb{C}^\times := \{z \in \mathbb{C} : z \neq 0\}$ de complexe multiplicatieve groep zijn. Voor iedere $n \in \mathbb{N}_{\geq 1}$ definiëren we het polynoom

$$\Phi_n(x) = \prod_z (x - z), \quad z \in \mathbb{C}^\times \text{ van orde } n, \quad (11)$$

waarvan de coëfficiënten in $\mathbb{Q}$ zitten omdat ze invariant zijn onder $\mathrm{Aut}(\bar{\mathbb{Q}})$. Een beetje algebra of getaltheorie leert dat $\Phi_n(x) \in \mathbb{Z}[x]$. Dit zijn de *cyclotomische polynomen*. Dedekind heeft bewezen dat alle $\Phi_n(x)$ irreducibel zijn. De nulpunten van $\Phi_n(x)$ zijn de $\exp(2\pi i/n)^a$, met $a$ geheel, $0 \leq a < n$ en $\mathrm{ggd}(a,n) = 1$. Vanwege Dedekind worden deze transitief gepermuteerd door $\mathrm{Aut}(\bar{\mathbb{Q}})$. Al deze eenheidswortels samen vormen de ondergroep $\bar{\mathbb{Q}}^\times_{\mathrm{tors}}$ van elementen van eindige orde van $\bar{\mathbb{Q}}^\times$, waarop $\mathrm{Aut}(\bar{\mathbb{Q}})$ werkt door groepsautomorfismen.

De afbeelding $\mathbb{Q} \to \bar{\mathbb{Q}}^\times_{\mathrm{tors}}$, $x \mapsto \exp(2\pi i x)$ induceert een isomorfisme van groepen van $\mathbb{Q}/\mathbb{Z}$ naar $\bar{\mathbb{Q}}^\times_{\mathrm{tors}}$. Nu is $\mathbb{Q}/\mathbb{Z}$ de vereniging van de ondergroepen $(n^{-1}\mathbb{Z})/\mathbb{Z}$ over alle $n \geq 1$. Iedere $(n^{-1}\mathbb{Z})/\mathbb{Z}$ is cyclisch, van orde $n$, en heeft daarom automorfismengroep $(\mathbb{Z}/n\mathbb{Z})^\times$: $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ werkt als $x \mapsto ax$. Voor $m$ een veelvoud van $n$ hebben we de inclusie $(n^{-1}\mathbb{Z})/\mathbb{Z} \subset (m^{-1}\mathbb{Z})/\mathbb{Z}$. De conclusie is dan dat de automorfismengroep $\mathrm{Aut}(\mathbb{Q}/\mathbb{Z})$ gelijk is aan de verzameling van collecties $(a_n)_n$ waar $n \geq 1$ en $a_n \in (\mathbb{Z}/n\mathbb{Z})^\times$, zodat als $m$ een veelvoud is van $n$, het beeld van $a_m$ onder het morfisme van ringen $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ gelijk is aan $a_n$. Al deze morfismen van groepen $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ zijn surjectief.

Om te zien wat de verzameling van deze collecties $(a_n)_n$ met $a_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ nu is, bekijken we wat eruit komt als we hetzelfde doen maar dan met $a_n \in \mathbb{Z}/n\mathbb{Z}$. De uitkomst heet dan $\hat{\mathbb{Z}}$, de *pro-eindige completering* van de ring $\mathbb{Z}$, maar dat zegt nog niet wat het is. De Chinese reststelling schiet ons te hulp. Laat, voor $n \geq 1$,

$$n = \prod_p p^{n_p} \quad (12)$$

de ontbinding van $n$ in priemfactoren zijn (bijna alle $n_p$ zijn 0, het product is eindig). Dan is *het* morfisme van ringen

$$\mathbb{Z}/n\mathbb{Z} \to \prod_p \mathbb{Z}/p^{n_p}\mathbb{Z} \quad (13)$$

een isomorfisme. Dat betekent dat we in plaats van de collecties $(a_n)_n$ met $a_n \in \mathbb{Z}/n\mathbb{Z}$ collecties $(a_{p,k})_{p,k}$ met $p$ priem en $k \geq 0$ kunnen nemen, met de eis dat voor alle $p$ en alle $k_1 \leq k_2$ geldt dat het beeld van $a_{p,k_2}$ onder $\mathbb{Z}/p^{k_2}\mathbb{Z} \to \mathbb{Z}/p^{k_1}\mathbb{Z}$ gelijk is aan $a_{p,k_1}$.

Per priemgetal $p$ is de verzameling van zulke collecties in bijectie met de verzameling $\mathbb{Z}_p$ van *$p$-adische gehele getallen* gedefinieerd als formele sommen $\sum_{i \geq 0} c_i p^i$, met de $c_i$ in $\{0, 1, \ldots, p-1\}$: hieraan koppelen we $a_{p,k} := \sum_{i=0}^{k-1} c_i p^i$. Een mooie interpretatie hiervan is om eerst natuurlijke getallen in basis $p$ te schrijven, dus als eindige rijtjes $c_k \cdots c_2 c_1 c_0$, en vervolgens $\mathbb{Z}_p$ te zien als de verzameling van oneindige rijtjes $\cdots c_2 c_1 c_0$. Optelling en vermenigvuldiging op $\mathbb{Z}_p$ werkt zoals men in het basisonderwijs leert: van rechts naar links, met 'onthouden'. Dat geeft een ring; tel bijvoorbeeld eens 1 op bij het rijtje met alle $c_i$ gelijk aan $p-1$. De volgende sectie geeft een beschrijving van $\mathbb{Z}_p$ die meer geschikt is voor analytici.

We gaan terug naar $\mathrm{Aut}(\mathbb{Q}/\mathbb{Z})$. We zien nu dat die groep gelijk is aan $\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ (we hebben de actie beschreven). Maar dan is ook $\mathrm{Aut}(\bar{\mathbb{Q}}^\times_{\mathrm{tors}})$ gelijk aan $\prod_p \mathbb{Z}_p^\times$, waarbij $(a_n)_n$ met $a_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ een element $z \in \bar{\mathbb{Q}}^\times_{\mathrm{tors}}$ met $z^m = 1$ naar $z^{a_m}$ stuurt. De actie van $\mathrm{Aut}(\bar{\mathbb{Q}})$ op $\bar{\mathbb{Q}}^\times_{\mathrm{tors}}$ geeft, en is gegeven door, een morfisme van groepen

$$\chi_{\mathrm{cycl}} : \mathrm{Aut}(\bar{\mathbb{Q}}) \to \prod_p \mathbb{Z}_p^\times \quad (14)$$

dat vanwege Dedekind surjectief is, en een open afbeelding is voor wat de topologieën betreft. Deze afbeelding is niet injectief (Galoisgroepen van polynomen zijn meestal niet abels). De stelling van Kronecker en Weber zegt dat de kern de afsluiting van de commutator-ondergroep is. Met andere woorden, voor elke $f$ in $\mathbb{Q}[x]$ waarvan de Galoisgroep abels is, is er een $n \geq 1$ zodat $f$ zijn nulpunten in $\mathbb{Q}(\exp(2\pi i/n))$ heeft.

In navolging van Galois, die eindige lichamen vond in zijn onderzoek naar groepen van automorfismen van lichamen, hebben we hier $p$-adische getallen gevonden omdat we automorfismen van cyclotomische lichamen bekeken. We hadden ook $p$-adische getallen vanuit de analyse kunnen introduceren in dit verhaal. Onze keus laat zien dat $p$-adische getallen natuurlijk en onvermijdbaar zijn in deze context.

**De lichamen $\mathbb{Q}_p$ en de adèle-ring**

We gaan weer wat analyse doen. Laat $p$ een priemgetal zijn. Dan hebben we de $p$-adische absolute waarde

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}, \quad n/m \mapsto p^{-(n_p - m_p)}, \quad (15)$$

met $n_p$ en $m_p$ zoals in (12). Kortom: $|p|_p = p^{-1}$, dus $p$ is klein en $1/p$ is groot. Net zoals men $\mathbb{R}$ krijgt door $\mathbb{Q}$ te completeren voor de gewone absolute waarde $|\cdot|$, krijgt men het breukenlichaam $\mathbb{Q}_p$ van $\mathbb{Z}_p$ door $\mathbb{Q}$ te completeren voor $|\cdot|_p$. In onze rijtjesnotatie voor $\mathbb{Z}_p$ betekent dit dat $\mathbb{Q}_p$ bestaat uit rijtjes $\cdots c_2 c_1 c_0 . c_{-1} \cdots c_{-n}$: oneindig naar links, eindig naar rechts.

De stelling van Ostrowski zegt dat iedere niet-triviale absolute waarde op $\mathbb{Q}$ equivalent is met (dat wil zeggen, dezelfde topologie geeft als) $|\cdot|$ of een $|\cdot|_p$. We hoeven dus niet te zoeken naar nog meer completeringen.

Met alle completeringen in handen definieerden Artin en Whaples in 1945 de *adèlering* van $\mathbb{Q}$:

$$\begin{aligned} \mathbb{A}_{\mathbb{Q}} &:= \mathbb{R} \times \prod_p{}' \mathbb{Q}_p \\ &= \{(x, (y_p)_p) : \forall' p, y_p \in \mathbb{Z}_p\}, \end{aligned} \quad (16)$$

waar $\forall' p$ betekent: voor bijna alle $p$. Dit heet een 'beperkt product'. We nemen de volgende topologie erop: deze is translatie-invariant, en het product $\mathbb{R} \times \prod_p \mathbb{Z}_p$ is open, en de daarop geïnduceerde topologie is de producttopologie. Deze Hausdorff, lokaal compacte topologische ring $\mathbb{A}_{\mathbb{Q}}$ heeft de fantastische eigenschap dat $\mathbb{Q}$ erin zit als deelring, discreet, en co-compact ($\mathbb{Q} \backslash \mathbb{A}_{\mathbb{Q}}$ is compact)! Wat kan een analyticus nog meer wensen?

Inderdaad heeft Tate (Abelprijs in 2010) dit in 1950 in zijn proefschrift gebruikt om een generalisatie door Hecke van Riemanns resultaten over $\zeta$ opnieuw te bewijzen met Fourieranalyse op $\mathbb{A}_{\mathbb{Q}}$ en op $\mathbb{A}_{\mathbb{Q}}^\times$, de multiplicatieve groep van $\mathbb{A}_{\mathbb{Q}}$, met de topologie geïnduceerd als gesloten deelverzameling van $\mathbb{A}_{\mathbb{Q}} \times \mathbb{A}_{\mathbb{Q}}$ bestaande uit de $(x, y)$ met $xy = 1$.

Over de naam 'adèle': dit staat voor 'additieve idèle'. De idèle-groep van $\mathbb{Q}$ is onze $\mathbb{A}_{\mathbb{Q}}^\times$. Deze topologische groep was al vóór Artin en Whaples ingevoerd door Chevalley.

**Klassenlichamentheorie voor $\mathbb{Q}$**

We weten al dat $\chi_{\mathrm{cycl}} : \mathrm{Aut}(\bar{\mathbb{Q}}) \to \prod_p \mathbb{Z}_p^\times$ uit (14) het quotiënt is naar de afsluiting van de commutator-ondergroep. Dit betekent

dat het grootste Hausdorff abelse quotient $\mathrm{Aut}(\bar{\mathbb{Q}})^{\mathrm{ab}}$ van $\mathrm{Aut}(\bar{\mathbb{Q}})$ sterke gelijkenis vertoont met $\mathbb{A}_{\mathbb{Q}}^{\times}$. Inderdaad induceert $\chi_{\mathrm{cycl}}$ door samenstelling met inclusie en quotient

$$\prod_p \mathbb{Z}_p^{\times} \hookrightarrow \mathbb{A}_{\mathbb{Q}}^{\times} \twoheadrightarrow \mathbb{Q}^{\times}\backslash\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{R}_{>0}^{\times} \qquad (17)$$

een isomorfisme van topologische groepen

$$\chi_{\mathrm{cycl}} : \mathrm{Aut}(\bar{\mathbb{Q}})^{\mathrm{ab}} \xrightarrow{\simeq} \mathbb{Q}^{\times}\backslash\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{R}_{>0}^{\times}. \qquad (18)$$

De inverse afbeelding, gezien als morfisme van $\mathbb{Q}^{\times}\backslash\mathbb{A}_{\mathbb{Q}}^{\times}$ naar $\mathrm{Aut}(\bar{\mathbb{Q}})^{\mathrm{ab}}$, en op een geschikt teken na, heet de *Artin-reciprociteitsafbeelding*.

**Algemene klassenlichamentheorie**

Een hoofdresultaat in de algebraïsche getaltheorie in de eerste helft van de twintigste eeuw, bereikt door de inspanningen van velen (laten we slechts Hilbert, Artin, Takagi en Chebotarev noemen), is de generalisatie van bovenstaande naar getallenlichamen, dat wil zeggen, naar lichaamsuitbreidingen $\mathbb{Q} \to K$ van eindige dimensie.

Eerlijkheid gebiedt me te zeggen dat ik hier niet het nodige over weet, met name waar het bewijzen betreft en wie wat heeft gedaan. Daarom verwijs ik naar [7, Chapter XI] en [15]. Vooral belangrijk is dat Artins reciprociteitsafbeelding gegeneraliseerd is naar een surjectie van topologische groepen

$$\mathrm{rec}_K : K^{\times}\backslash\mathbb{A}_K^{\times} \twoheadrightarrow \mathrm{Aut}_K(\bar{\mathbb{Q}})^{\mathrm{ab}} \qquad (19)$$

waarin $\mathbb{A}_K$ de adèle-ring van $K$ is (hier zonder toelichting), en $\mathrm{Aut}_K(\bar{\mathbb{Q}})$ de (open) ondergroep van $\mathrm{Aut}(\bar{\mathbb{Q}})$ is bestaande uit die $\sigma$ die $K$ puntsgewijs vast laten. (De kern van $\mathrm{rec}_K$ is de afsluiting van het beeld van de samenhangscomponent van $1 \in (\mathbb{R}\otimes K)^{\times}$.) Een expliciete beschrijving van de bijbehorende lichaamsuitbreidingen van $K$, zoals de cyclotomische uitbreidingen van $\mathbb{Q}$, is alleen in heel speciale gevallen bekend.

Er is hier nog veel meer over te zeggen (lokale theorie, vertakking, $L$-functies en hun eigenschappen), maar ons doel is om zo snel mogelijk naar het 'niet-abelse' te gaan. De conclusie is dat klassenlichamentheorie een prachtige beschrijving geeft van het grootse Hausdorff abelse quotient van $\mathrm{Aut}_K(\bar{\mathbb{Q}})$. De groep $\mathrm{Aut}_K(\bar{\mathbb{Q}})$ zelf is veel lastiger: het wordt behelpen met representaties en $L$-functies. We beperken ons tot het geval $K = \mathbb{Q}$.

Foto: abelprize.no

Robert Langlands met de Abelprijs

**Decompositie en inertie**

Het is nu tijd om wat meer te zeggen over de relatie tussen $\mathrm{Aut}(\bar{\mathbb{Q}})$ en de 'lokale theorie': de automorfismengroepen van algebraïsche afsluitingen van de $\mathbb{Q}_p$. Voor iedere $p$ heeft $\mathbb{Q}_p$ een op isomorfisme na unieke algebraïsche afsluiting, die we als $\bar{\mathbb{Q}}_p$ noteren. We laten $\mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p)$ de groep van automorfismen van $\bar{\mathbb{Q}}_p$ zijn, die $\mathbb{Q}_p$ puntsgewijs vastlaten. Omdat $\bar{\mathbb{Q}}_p$ een algebraïsch afgesloten uitbreiding van $\mathbb{Q}$ is, kan $\bar{\mathbb{Q}}$ erin ingebed worden, op vele manieren. Al deze inbeddingen

$$\iota_p : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p \qquad (20)$$

vormen één baan onder precompositie met elementen van $\mathrm{Aut}(\bar{\mathbb{Q}})$. We kiezen voor elke $p$ zo'n $\iota_p$. Elke $\sigma$ in $\mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p)$ geeft door beperking een element van $\mathrm{Aut}(\bar{\mathbb{Q}})$. Het is een makkelijk resultaat dat de hierdoor gegeven afbeelding van $\mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p)$ naar $\mathrm{Aut}(\bar{\mathbb{Q}})$ injectief is. Het beeld $D_p$ hiervan heet de *decompositiegroep bij* $p$:

$$\mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p) \xrightarrow{\simeq} D_p \subset \mathrm{Aut}(\bar{\mathbb{Q}}). \qquad (21)$$

We laten nu $\bar{\mathbb{Z}}_p$ de *gehele afsluiting* van $\mathbb{Z}_p$ in $\bar{\mathbb{Q}}_p$ zijn: de $x$ in $\bar{\mathbb{Q}}_p$ die nulpunt zijn van een polynoom $x^n + \cdots + a_1 x + a_0$ met alle $a_i$ in $\mathbb{Z}_p$. Dan is $\bar{\mathbb{Z}}_p$ een deelring van $\bar{\mathbb{Q}}_p$, invariant onder $\mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p)$ en het is een eenvoudig resultaat dat er een surjectief ringmorfisme is van $\bar{\mathbb{Z}}_p$ naar een algebraïsche afsluiting $\bar{\mathbb{F}}_p$ van $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, waarvan de kern invariant is onder $\mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p)$. Dit geeft een surjectief groepsmorfisme van $D_p = \mathrm{Aut}_{\mathbb{Q}_p}(\bar{\mathbb{Q}}_p)$ naar $\mathrm{Aut}(\bar{\mathbb{F}}_p)$, waarvan de kern $I_p$ de *inertiegroep* heet:

$$I_p \hookrightarrow D_p \twoheadrightarrow \mathrm{Aut}(\bar{\mathbb{F}}_p) \qquad (22)$$

Het leuke van ringen van karakteristiek $p$ is dat die een natuurlijk endomorfisme $\mathrm{Frob}_p$ hebben, geheten de $p$-Frobenius, gegeven door $x \mapsto x^p$. In het geval van $\bar{\mathbb{F}}_p$ is dit een automorfisme: het is injectief want $\bar{\mathbb{F}}_p$ is een lichaam, en het is surjectief omdat $\bar{\mathbb{F}}_p$ algebraïsch afgesloten is, dus elk element is een $p$-de macht. Deze $\mathrm{Frob}_p$ in $\mathrm{Aut}(\bar{\mathbb{F}}_p)$ is een 'topologische voortbrenger' en het groepsmorfisme $\mathbb{Z} \to \mathrm{Aut}(\bar{\mathbb{F}}_p)$ dat $1$ naar $\mathrm{Frob}_p$ stuurt, breidt uit tot een isomorfisme van topologische groepen $\hat{\mathbb{Z}} \to \mathrm{Aut}(\bar{\mathbb{F}}_p)$. Voor elke $p$ kiezen we een element in $D_p$ waarvan het beeld in $\mathrm{Aut}(\bar{\mathbb{F}}_p)$ gelijk is aan $\mathrm{Frob}_p$, en voor de eenvoud noemen we dat element weer $\mathrm{Frob}_p$.

**$L$-functies**

Laat nu $V$ een eindig dimensionale complexe vectorruimte zijn, en

$$\rho : \mathrm{Aut}(\bar{\mathbb{Q}}) \longrightarrow \mathrm{GL}(V) \qquad (23)$$

een continu morfisme van groepen. Al dit soort representaties zijn van de volgende vorm: men neme een $f$ in $\mathbb{Q}[x]$, met nulpunten $z_1, \ldots, z_d$ in $\bar{\mathbb{Q}}$, een (injectieve) representatie $\bar{\rho} : \mathrm{Aut}(\mathbb{Q}(z_1, \ldots, z_d)) \to \mathrm{GL}(V)$ en men stelt dit samen met de beperkingsafbeelding $\mathrm{Aut}(\bar{\mathbb{Q}}) \to \mathrm{Aut}(\mathbb{Q}(z_1, \ldots, z_d))$. Complexe Galoisrepresentaties zijn dus heel concrete objecten: het volstaat om $f$ en $\bar{\rho}$ te geven.

Als generalisatie van Riemanns zèta-functie definieert men nu de *Artin-L-functie* $s \mapsto L(\rho, s)$ (voor $\Re(s) > 1$) van $\rho$ als volgt. Het is een Euler-product, over alle priemgetallen $p$:

$$L(\rho, s) := \prod_p L_p(\rho, s), \quad \text{voor } s \in \mathbb{C} \text{ met } \Re(s) > 1. \qquad (24)$$

De factor $L_p(\rho, s)$ bij $p$ is de inverse van het inverse karakteristieke polynoom van $\rho(\mathrm{Frob}_p)$, werkend op de deelruimte $V^{I_p}$ van elementen van $V$ die invariant zijn onder $I_p$, met als variabele $p^{-s}$. In formule:

$$L_p(\rho, s) := \det\left(1 - p^{-s}\rho(\mathrm{Frob}_p), V^{I_p}\right)^{-1}. \qquad (25)$$

Dit hangt niet af van de hierboven gemaakte keuzes (de $\mathrm{Frob}_p$, de inbeddingen $\iota_p$).

Voor bijna alle $p$ geldt $V^{I_p} = V$. Men ziet dat de $L$-functie van de triviale representatie op $\mathbb{C}$ gelijk is aan Riemanns $\zeta$.

Uit de al bovengenoemde resultaten van Hecke en Tate, en wat representatietheorie van eindige groepen (Brauer), volgt dat alle $L(\rho)$ een meromorfe voortzetting hebben tot $\mathbb{C}$, en dat er een expliciete functionaalvergelijking is tussen $L(\rho,s)$ en $L(\rho^\vee,1-s)$, waarbij $\rho^\vee$ de duale representatie van $\rho$ is: $\rho^\vee(\sigma) = \rho(\sigma^{-1})^\vee$ in $\mathrm{Aut}(V^\vee)$. Als $\rho = \rho_1 \oplus \rho_2$, dan geldt $L(\rho) = L(\rho_1)L(\rho_2)$.

Artins vermoeden is dat voor irreducibele niet triviale $\rho$ de functie $L(\rho)$ analytisch is op heel $\mathbb{C}$. Het is precies hier dat het Langlands-programma een rol speelt: het idee is dat als $L(\rho)$ de $L$-functie is van een 'cuspidale automorfe representatie', dan is $L(\rho)$ analytisch en heeft de goede functionaalvergelijking, ongeveer net zo als we hebben gezien voor Riemanns $\zeta$. Het is hier misschien een geschikt moment om te vermelden dat de door Riemann gebruikte functie $\theta$ een automorf object is (het is een 'modulaire vorm').

**Automorfe representaties van $\mathrm{GL}_n$ over $\mathbb{Q}$**

Nu betreden we (opnieuw) het domein van de harmonische analyse. We hebben al een toepassing gezien van Fouriertransformatie op $\mathbb{R}$, en dat heeft te maken met representatietheorie van $\mathbb{R}$. Wie de sferisch harmonische functies op de bol $S^2$ wil begrijpen of gebruiken (denk aan de quantummechanica van het waterstofatoom) doet er goed aan de groep $\mathrm{SO}_3(\mathbb{R})$ daarop te laten werken, en de representatietheorie daarvan te gebruiken. Omdat deze groep compact is, zijn de irreducibele representaties eindigdimensionaal. De Peter–Weylstelling geeft een Hilbertbasis van de $L^2$-ruimte van kwadraat-integreerbare functies op $\mathrm{SO}_3(\mathbb{R})$, en ook voor $S^2$. Moeilijker wordt het als we groepen als $\mathrm{GL}_n(\mathbb{R})$ bekijken, want hier zijn de relevante representaties op Hilbertruimten niet noodzakelijk eindigdimensionaal. Toch is representatietheorie ook hier de manier om getaltheoretisch relevante ruimten van functies op $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R})$ aan te pakken. Bijvoorbeeld is $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R})/\mathrm{O}_n(\mathbb{R})$ de verzameling van isomorfieklassen van roosters in $n$-dimensionale euclidische ruimten.

Nu kan men te werk gaan met discrete ondergroepen van Liegroepen zoals $\mathrm{GL}_n(\mathbb{Z})$ in $\mathrm{GL}_n(\mathbb{R})$, maar dat leidt tot Heckeoperatoren bij alle priemgetallen (zoals in [8]), terwijl het voor *dit* verhaal essentieel is dat we alles uitdrukken in representatietheorie, ook van groepen als $\mathrm{GL}_n(\mathbb{Q}_p)$. Daarom bekijken we ruimten van functies op $\mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$. Het verband tussen $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R})$ en $\mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ is als volgt:

$$\begin{aligned}&\mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})/\mathrm{GL}_n(\hat{\mathbb{Z}})\\ &\quad = \mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R}),\end{aligned} \tag{26}$$

hetgeen men kan bewijzen door te gebruiken dat de actie van $\mathrm{GL}_n(\mathbb{Q})$ op $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty)/\mathrm{GL}_n(\hat{\mathbb{Z}})$ transitief is, waarbij $\mathbb{A}_\mathbb{Q}^\infty$ de *eindige adèle-ring* is:

$$\mathbb{A}_\mathbb{Q}^\infty = \prod_p{}'\mathbb{Q}_p \text{ en } \mathbb{A}_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\infty \times \mathbb{R}. \tag{27}$$

Daarom zijn functies op de ruimte $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R})$ rechts $\mathrm{GL}_n(\hat{\mathbb{Z}})$ invariante functies op $\mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$.

De laatste stap naar automorfe vormen komt voort uit de wens een 'algebraïsche' theorie te hebben: alleen eindige sommen, geen limieten. Bijvoorbeeld, in plaats van de ruimte van $L^2$-functies op de cirkel $S^1 = \mathbb{Z}\backslash\mathbb{R}$ willen we de *eindige* $\mathbb{C}$-lineaire combinaties van de elementen van de Hilbertbasis. Dit zijn precies de functies waarvan de getransleerden in een eindigdimensionale vectorruimte liggen. Het probleem dat hier optreedt komt alleen van de factor $\mathrm{GL}_n(\mathbb{R})$, want de factor $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty)$ heeft een cofinaal systeem van open compacte ondergroepen, bijvoorbeeld de kernen van de groepsmorfismen $\mathrm{GL}_n(\hat{\mathbb{Z}}) \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, met $m \geq 1$.

We bekijken dus functies

$$\begin{aligned}&f : \mathrm{GL}_n(\mathbb{A}_\mathbb{Q})\\ &\quad = \mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty) \to \mathbb{C}\end{aligned} \tag{28}$$

die voldoen aan:

1. $f$ is invariant onder linkstranslaties met elementen van $\mathrm{GL}_n(\mathbb{Q})$;
2. $f$ is invariant onder rechtstranslaties met elementen van een open ondergroep (die van $f$ af mag hangen) van $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty)$;
3. voor alle $g$ in $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty)$ is de beperking van $f$ tot $\{g\} \times \mathrm{GL}_n(\mathbb{R})$ glad;
4. de rechtsgetransleerden van $f$ onder $\mathrm{O}_n(\mathbb{R})$ liggen in een eindig dimensionale vectorruimte;
5. $f$ is *cuspidaal*;
6. $f$ is een eigenvector van het centrum van de algebra van links-invariante differentiaaloperatoren op $\mathrm{GL}_n(\mathbb{R})$;
7. $\exists a \in \mathbb{R}$ zodat $g \mapsto |f(g)| \cdot \|\det(g)\|^a$ begrensd is.

Een aantal van deze voorwaarden verdienen nog toelichting. Voor complete details zie [22] (sterk aanbevolen, juist omdat daar complete definities en precieze vermoedens staan). Voorwaarde (7): voor $x \in \mathbb{A}_\mathbb{Q}$ is $\|x\|$ gedefinieerd als $|x_\infty| \cdot \prod_p |x_p|_p$. Voorwaarde (7) betekent intuïtief dat $f$ niets te maken heeft met $\mathrm{GL}_m$ voor $m < n$, en technisch dat voor elke partitie $n = n_1 + n_2$ met $n_1, n_2 > 0$, en voor elke $g$ in $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$,

$$\int_{u \in U_{n_1,n_2}(\mathbb{Q})\backslash U_{n_1,n_2}(\mathbb{A}_\mathbb{Q})} f(ug)\,du = 0,$$

waarin $U_{n_1,n_2}$ de ondergroep van $\mathrm{GL}_n$ is bestaande uit matrices van de vorm

$$\begin{pmatrix} 1_{n_1} & * \\ 0 & 1_{n_2} \end{pmatrix}.$$

Voorwaarden (1)–(5) zijn lineair: de verzameling van $f$ die eraan voldoen is een complexe deelruimte. De keuze van de maximaal compacte ondergroep $\mathrm{O}_n(\mathbb{R})$ in voorwaarde (4), die slechts uniek is op conjugatie na, heeft als gevolg dat de groep $\mathrm{GL}_n(\mathbb{R})$ *niet* werkt, door rechtstranslaties, op de ruimte van functies die aan de eerste vier voorwaarden voldoen. Maar de algebra van differentiaaloperatoren uit voorwaarde (6), voortgebracht door de *infinitesimale* rechtstranslaties, werkt er nog wel op. Het is geen moeilijk resultaat dat het centrum $\mathfrak{z}_n$ van deze algebra een polynoomalgebra in $n$ variabelen is (coëfficienten van het minimumpolynoom). Een eigenvector $f \neq 0$ als in (6) geeft dan een $\mathbb{R}$-algebra-morfisme $H : \mathfrak{z}_n \to \mathbb{C}$ dat voor elke $D \in \mathfrak{z}_n$ de eigenwaarde van $D$ op $f$ geeft, en de verzameling van zulke morfismen is in een natuurlijke bijectie met $\mathbb{C}^n$. Laat nu $H : \mathfrak{z}_n \to \mathbb{C}$ een morfisme zijn. Dan heet

$$\begin{aligned}\mathcal{A}^\circ_{n,H} := \{f\colon f \text{ voldoet aan } (1)-(7)\\ \text{en } (6) \text{ met } H\}\end{aligned}$$

de ruimte van *cuspidale automorfe vormen op* $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ *met infinitesimaal karakter* $H$.

Hiermee hebben we nu het belangrijkste object aan de analysekant van dit verhaal. Op deze $\mathbb{C}$-vectorruimte werken $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty)$, $\mathrm{O}_n(\mathbb{R})$, en de Lie-algebra $\mathrm{M}_n(\mathbb{R})$. De eerste hiervan commuteert met de andere twee, die samen een eenvoudige commutatieregel hebben. De belangrijkste vraag is nu hoe $\mathcal{A}^\circ_{n,H}$ eruit ziet als representatie voor $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q}^\infty) \times (\mathrm{O}_n(\mathbb{R}), \mathrm{M}_n(\mathbb{R}))$. Het is bekend (en vast niet zo makkelijk) dat $\mathcal{A}^\circ_{n,H}$ een directe som is van simpele representa-

ties $\pi$ (op een vectorruimte $V_\pi$), elk met multipliciteit $1$. Verder is elk zo'n simpele representatie op unieke manier van de vorm $\pi = \pi_\infty \otimes \otimes'_p \pi_p$, met $\pi_\infty$ een irreducibele representatie van het paar $(\mathrm{O}_n(\mathbb{R}), \mathrm{M}_n(\mathbb{R}))$, elke $\pi_p$ een irreducibele representatie van $\mathrm{GL}_n(\mathbb{Q}_p)$, en $\otimes'_p \pi_p$ het *beperkt tensorproduct* van de $\pi_p$ (zie [22]), een notie die weerspiegelt dat $\mathbb{A}_\mathbb{Q}$ een beperkt product is. Weer verder is voor bijna alle $p$ de representatie $\pi_p$ gegeven door een ongeordend $n$-tal complexe getallen $\lambda_i \neq 0$ zodat voor alle $i$ en $j$ geldt dat $\lambda_j \neq p\lambda_i$. Dit heeft van alles te maken met de groep $\mathbb{Q}_p^{\times,n}$ van diagonale matrices. Gezien de paragraaf '$L$-functies' ligt het voor de hand om voor zulke $p$ te definiëren:

$$L_p(\pi, s) := \prod_i (1 - \lambda_i p^{-s})^{-1}.$$

De $\pi$ die voorkomen in $\mathcal{A}^\circ_{n,H}$ heten *cuspidale automorfe representaties*. De eis dat automorfe vormen linksinvariant zijn onder $\mathrm{GL}_n(\mathbb{Q})$ legt sterke beperkingen van getaltheoretische aard op aan de collectie van lokale factoren $(\pi_p)_p$ van een automorfe $\pi$. Zonder deze eis is het chaos.

**De cruciale twee vragen**

We hebben nu aan beide kanten wat structuur gezien. Laat nu $\rho : \mathrm{Aut}(\bar{\mathbb{Q}}) \to \mathrm{GL}_n(\mathbb{C})$ een irreducibele continue representatie zijn. Dan hebben we voor iedere $p$ waarvoor $\rho_p$ onvertakt is, het $n$-tal eigenwaarden van $\rho(\mathrm{Frob}_p)$, en dus de daarbij horende representatie $\pi(\rho)_p$ van $\mathrm{GL}_n(\mathbb{Q}_p)$. De vraag rijst dan of er een cuspidale automorfe $\pi(\rho)$ bestaat waarvan, voor onvertakte $p$, de lokale factoren de $\pi(\rho)_p$ zijn, en welke cuspidale automorfe representaties van Galoisrepresentaties komen. En ook rijst de vraag of er voor een cuspidale automorfe $\pi$ een $L$-functie $L(\pi)$ te definiëren is, product van lokale $L(\pi_\infty)$ en $L(\pi_p)$ met lokale functionaalvergelijkingen, die analytisch voortzetbaar is en de productfunctionaalvergelijking heeft. Een positief antwoord op de eerste en op de laatste vraag bewijst Artins vermoeden.

Langlands stelde zich waarschijnlijk deze vragen in 1966. Mijn punt is dat dit toen wel in de lucht hing (volgens [16, §3.1] zegt Langlands dit zelf ook). Er was al werk over modulariteit van elliptische krommen over $\mathbb{Q}$ (Shimura–Taniyama, Weil in [23]), de theorie van automorfe representaties was al in ontwikkeling, zie [12] en werk van Harish–Chandra, en denk eens aan het geval $n = 1$, en ook aan functielichamen. De eerste vraag is nog steeds open, maar de tweede is met ja beantwoord in [13].

In ieder geval heeft Langlands een enorm onderzoeksterrein geopend: kijk naar $\ell$-adische representaties, vervang $\mathbb{Q}$ door een getallenlichaam, $\mathrm{GL}_n$ door een andere groep. U staat nu voor de poort naar een gebied met mooie tuinen, maar ook enorme bouwterreinen. Een optimistische onderzoekende houding is nu voldoende, en het hele Langlands-programma, inclusief 'duale groepen' en 'functorialiteit', zal vanzelf voor u opdoemen.

Wie wil aansluiten bij huidig onderzoek, wordt Scholzes voordracht op ICM 2018 [17] aanbevolen (zie ook Moonens stuk in dit NAW-nummer), en ook [6] en [3]. In [18] kondigt Scholze een artikel aan, van hem en Fargues, waarin 'de natuur' (cohomologie van 'locale Shimura-variëteiten') de locale Langlands-correspondentie voor willekeurige reductieve $p$-adische groepen realiseert. Ruim vijftig jaar na de start van het Langlandsprogramma is dit een zeer belangrijke mijlpaal. Nu nog de globale theorie!

**Referenties**


1 http://www.abelprize.no/seksjon/vis.html?tid=73018.

2 AMS communication, Robert Langlands Awarded Abel Prize, *Notices Amer. Math. Soc.* 65(6) (2018), 670–672.

3 J. Arthur, A note on the automorphic Langlands group – Dedicated to Robert V. Moody, *Canad. Math. Bull.* 45(4) (2002), 466–482.

4 A.-M. Aubert, Around the Langlands program, *Jahresber. Dtsch. Math.-Ver.* 120(1) (2018), 3–40,

5 A. Bellos, A glimpse of the Laureate's work, http://www.abelprize.no/c73016/binfil/download.php?tid=73020.

6 K. Buzzard en T. Gee, The conjectural connections between automorphic representations and Galois representations, *Automorphic Forms and Galois Representations. Vol. 1*, London Math. Soc. Lecture Note Ser. 414, Cambridge University Press, 2014, pp. 135–187.

7 J.W.S. Cassels en A. Fröhlich., eds., *Algebraic Number Theory*, Second edition, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union, papers from the conference held at the University of Sussex, Brighton, 1–17 September 1965, London Mathematical Society, 2010. Including a list of errata.

8 S. Dahmen en A. Kret, Andrew Wiles and the Abel Prize, *NAW* 5/18(2) (2017), 88–98.

9 F. Diamond en J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer, 2005.

10 B. Dundas en C. Skau, Interview with Abel laureate Robert Langlands, *Eur. Math. Soc. Newsl.* 109 (2018), 19–27. Video at http://www.abelprize.no/artikkel/vis.html?tid=73440.

11 S. Friedberg, What is... the Langlands program? *Notices Amer. Math. Soc.* 65(6) (2018), 663–665.

12 I.M. Gel'fand, M.I. Graev en I.I. Piatetski-Shapiro, Representations of adèle groups, *Dokl. Akad. Nauk SSSR* 156 (1964) 487–490. In Russian.

13 R. Godement en H. Jacquet, *Zeta Functions of Simple Algebras*, Lecture Notes in Mathematics, Vol. 260, Springer, 1972.

14 R.P. Langlands, The work of Robert Langlands, http://publications.ias.edu/rpl.

15 P. Stevenhagen en H.W. Lenstra, Chebotarëv and his density theorem, *Math. Intelligencer* 18(2) (1996), 26–37.

16 J. Mueller, On the genesis of Robert P. Langlands' conjectures and his letter to André Weil, *Bull. Amer. Math. Soc. (N.S.)* 55(4) (2018), 493–528.

17 P. Scholze, $p$-adic geometry, arXiv:1712.03708.

18 P. Scholze, Etale cohomology of diamonds, http://www.math.uni-bonn.de/people/scholze/EtCohDiamonds.pdf.

19 J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, No. 7. Springer, 1973.

20 A. Sletsjøe, 17 handwritten pages that shaped a whole area of mathematical research, http://www.abelprize.no/c73016/binfil/download.php?tid=73037.

21 A. Sletsjøe, *From quadratic reciprocity to Langlands' program*, http://www.abelprize.no/c73016/binfil/download.php?tid=73038.

22 R. Taylor, Galois representations, *Ann. Fac. Sci. Toulouse Math. (6)* 13(1) (2004), 73–119.

23 A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.* 168 (1967) 149–156.