Hoofdstuk 19

Irrationaliteit en transcendentie

19.1 Irrationale getallen

In dit hoofdstuk zullen we aannemen dat de lezer weet wat reële getallen zijn, hoewel dat misschien niet helemaal gerechtvaardigd is. De axioma's van de reële getallen zijn vrij ingewikkeld en onbekend bij de meesten van ons. Niettemin werken we vaak met reële getallen zonder ons om deze axiomatiek druk te maken. Dit is de benadering die we ook hier kiezen. We zien de reële getallen als de gewone 'huis- tuin- en keuken' getallen waarmee we vanaf onze schooltijd gewerkt hebben. Voor het verhaal van dit hoofdstuk is het prettig, maar niet echt noodzakelijk, om ook te weten wat complexe getallen zijn.
In ieder geval, *rationale getallen* zijn die reële getallen die geschreven kunnen worden als breuk, een quotient van twee gehele getallen. Sinds de Griekse oudheid weet men dat er ook *irrationale getallen* bestaan, dat wil zeggen getallen die je niet als breuk kunt schrijven. Het beroemdste voorbeeld is $\sqrt{2}$. Stel namelijk dat $\sqrt{2} = p/q$ voor zekere natuurlijke getallen p, q. Vermenigvuldiging met q en kwadrateren geeft $2q^2 = p^2$. Links staat het getal $2q^2$. Dat heeft een oneven aantal priemfactoren 2 in zijn ontbinding. Rechts staat het getal p^2. Dat heeft een even aantal priemfactoren 2 in zijn ontbinding. Wegens de eenduidigheid van priemontbinding kunnen $2q^2$ en p^2 nooit gelijk zijn. Dus $\sqrt{2}$ is irrationaal. De ontdekking dat er ook irrationale getallen zijn was een grote slag voor Pythagoras en zijn volgelingen. Zij hadden het idee dat grootheden in de natuur en in de meetkunde als verhoudingen van gehele aantallen gezien konden worden.
Het bovenstaande argument kan gegeneraliseerd worden tot willekeurige getallen die aan een polynoomvergelijking met gehele coëfficienten voldoen.

Stelling 19.1.1 *Zij α een nulpunt van het polynoom $F(x) = x^m + c_1x^{m-1} + \cdots + c_{m-1}x + c_m$ met gehele coëfficienten c_i en $c_m \neq 0$. Dan is α ofwel irrationaal, ofwel α is geheel en deelt c_m.*

Stel namelijk $\alpha = p/q$ met p, q geheel, $q > 0$ en $\mathrm{ggd}(p, q) = 1$. Vermenigvuldig

$F(\alpha) = F(p/q) = 0$ met q^m. We vinden

$$p^m + c_1 p^{m-1} q + \cdots + c_{m-1} p q^{m-1} + c_m q^m = 0.$$

Alle termen aan de linkerkant, behalve de eerste, zijn deelbaar door q. Dus q deelt p^m. Maar we weten dat $\mathrm{ggd}(p, q) = 1$. Dit kan alleen maar als $q = 1$. Dus $\alpha = p$ is geheel. Maar dan volgt uit de gelijkheid

$$p^m + c_1 p^{m-1} + \cdots + c_{m-1} p + c_m = 0$$

dat p een deler is van c_m. $\square$

Een voorbeeld, zij α nulpunt van $x^4 - 3x + 1$. Als α rationaal zou zijn dan is α geheel en deler van 1. Dus $\alpha = \pm 1$. Een eenvoudige controle leert dat ± 1 geen nulpunt zijn van $x^4 - 3x + 1$. Dus is α irrationaal.
Neem als tweede voorbeeld het polynoom $x^m - N$ waarin N geen m-de macht is. De stelling zegt dat als een nulpunt α van $x^m - N$ rationaal is, dan is α geheel. Dus $\alpha^m = N$ in tegenspraak met het gegeven dat N geen m-de macht is. We zien dus,

Gevolg 19.1.2 *Zij $m \in \mathbb{N}$ en N een natuurlijk getal dat geen m-de macht is. Dan is $\sqrt[m]{N}$ irrationaal.*

In de analyse komen op natuurlijke wijze getallen voor waarvan we ons kunnen afvragen of ze irrationaal zijn of niet. De bekendste voorbeelden zijn π en e. We beginnen met e, de basis van de natuurlijk logaritme.

Stelling 19.1.3 *Zij e de basis van de natuurlijke logaritme. Dan is e irrationaal.*

Stel namelijk dat e wel rationaal is met noemer d. We maken gebruik van de bekende reeks

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Zij nu $n \in \mathbb{N}$. Definieer

$$e_n = \sum_{k=0}^{n} \frac{1}{k!}$$

Dit is een rationale benadering van e met een noemer die $n!$ deelt. Bovendien $e_n < e$. Dit betekent dat het verschil een positief rationaal getal is met een noemer die $d \cdot n!$ deelt (Ga na!). Iedere positieve breuk is groter of gelijk aan 1 gedeeld door de noemer. In het bijzonder, $e - e_n \geq 1/(d \cdot n!)$. Anderzijds hebben we ook een bovengrens voor $e - e_n$. Immers,

$$\begin{aligned}
e - e_n &= \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + \cdots \\
&= \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots\right) \\
&< \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \cdots\right) \\
&= \frac{1}{n!}\frac{1}{n}
\end{aligned}$$

Zetten we ondergrens en bovengrens voor $e - e_n$ achter elkaar dan vinden we $1/(d \cdot n!) < 1/n(n!)$. En dus $n < d$. We mogen n willekeurig kiezen, en als we n groter dan d kiezen hebben we een tegenspraak. Het getal e kan dus niet rationaal zijn. $\square$

Rond 1740 gaf Euler het eerste bewijs voor de irrationaliteit van e. Het eerste irrationaliteitsbewijs voor π werd gegeven door Lambert in 1761. Dit bewijs was gebaseerd op de kettingbreuk ontwikkeling van $\tan(x)$. In de volgende paragraaf zien we een bewijs dat een variatie is op een bewijs gegeven door Hermite. Sindsdien is van een groot aantal getallen, afkomstig uit de analyse, bekend dat ze irrationaal zijn. Er blijven echter een aantal notoir moeilijke gevallen over. Zo is er de constante van Euler,

$$\gamma = \lim_{n\to\infty}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) - \log(n)$$

waarvan nog geen irrationaliteitsbewijs bekend is ondanks de vele pogingen daartoe. Merkwaardig genoeg is ook niet bekend of $e\pi$ of $e + \pi$ irrationaal zijn. Daarentegen weten we wel dat e^π irrationaal is. Gemotiveerd door de standaard reeks van e stelde P.Erdös de vraag of

$$\sum_{k=1}^{\infty} \frac{1}{k! + 1}$$

irrationaal is. Merkwaardig genoeg heeft ook hier niemand een irrationaliteitsbewijs voor kunnen geven.

19.2 Irrationaliteit van e^a en π

In deze paragraaf bewijzen we de volgende twee stellingen.

Stelling 19.2.1 *Zij $a \in \mathbb{Q}$ en $a \neq 0$. Dan is e^a irrationaal.*

Stelling 19.2.2 *Het getal π^2 is irrationaal.*

De laatste stelling impliceert dat π irrationaal is. Als namelijk π rationaal zou zijn, dan zou π^2 dat ook zijn.
Voor het bewijs van beide stellingen is het polynoom

$$P_m(t) = \frac{1}{m!}\left(\frac{d}{dt}\right)^m (t^m(1-t)^m)$$

van belang, waarin $m \in \mathbb{N}$. Deze polynomen staan bekend als de *Legendre polynomen* op het interval $[0,1]$ en hebben vele interessante eigenschappen. Voor ons is het volgende Lemma van belang.

Lemma 19.2.3 *Het polynoom $P_m(t)$ heeft gehele coëfficienten.*

Merk op dat P_m gevormd wordt door $t^m(1-t)^m$ m maal te differentiëren en vervolgens door $m!$ te delen. Doen we dit met een macht van t, bijvoorbeeld t^N, dan krijgen we,

$$\frac{1}{m!}\left(\frac{d}{dt}\right)^m t^N = \frac{N(N-1)\cdots(N-m+1)}{m!}t^{N-m} = \binom{N}{m}t^{N-m}.$$

Omdat de binomiaalcoëfficient $\binom{N}{m}$ geheel is, en $t^m(1-t)^m$ som van termen van de vorm $a_N t^N$ met a_N geheel, volgt ons Lemma. $\square$

Hier is een kort lijstje met eerste paar polynomen,

$$\begin{aligned}
P_0(t) &= 1\\
P_1(t) &= 1-2t\\
P_2(t) &= 1-6t+6t^2\\
P_3(t) &= 1-12t+30t^2-20t^3\\
P_4(t) &= 1-20t+90t^2-140t^3+70t^4\\
&\cdots
\end{aligned}$$

Hier is nog een Lemma.

Lemma 19.2.4 *Zij $n \in \mathbb{Z}_{\geq 0}$ en $a \in \mathbb{R}$, $a \neq 0$. De integraal*

$$a\int_0^1 t^n e^{at}dt$$

heeft een waarde die van de vorm $A_n(1/a) + B_n(1/a)e^a$ is, waarin A_n, B_n polynomen van graad $\leq n$ zijn met gehele coëfficienten.

Het bewijs is gaat met inductie naar n. Voor $n = 0$ geldt

$$a \int_0^1 e^{at} dt = e^a - 1$$

hetgeen precies ons Lemma voor $n = 0$ is met $A_0(x) = -1, B_0(x) = 1$.
Stel nu $n > 0$. Partiële integratie levert,

$$\begin{aligned} a \int_0^1 t^n e^{at} dt &= a \left[\frac{t^n e^{at}}{a} \right]_0^1 - a\frac{n}{a} \int_0^1 t^{n-1} e^{at} dt \\ &= e^a - n \int_0^1 t^{n-1} e^{at} dt \end{aligned}$$

Uit deze gelijkheid zien we dat

$$A_n(1/a) + B_n(1/a)e^a = e^a - \frac{n}{a}(A_{n-1}(1/a) + B_{n-1}(1/a)e^a)$$

en dus $A_n(1/a) = -\frac{n}{a} A_{n-1}(1/a)$ en $B_n(1/a) = 1 - \frac{n}{a} B_{n-1}(1/a)$. Ons Lemma volgt nu door inductie naar n. □

We kunnen nu overgaan naar ons bewijs van de irrationaliteit van e^a als $a \in \mathbb{Q}$ en $a \neq 0$. Stel $a = p/q$ met $p, q \in \mathbb{Z}$ en $p > 0$. Stel dat e^a gelijk is aan een breuk r/s met $r, s \in \mathbb{Z}$ en $s > 0$.
Beschouw de integraal

$$I_n = a \int_0^1 P_n(t) e^{at} dt$$

Omdat P_n gehele coëfficienten heeft volgt uit ons vorige Lemma dat I_n van de vorm

$$R_n(1/a) + S_n(1/a)e^a$$

is waarin R_n, S_n polynomen van graad $\leq n$ zijn met gehele coëfficienten. Hierdoor zijn de getallen $R_n(1/a)$ en $S_n(1/a)$ rationale getallen waarvan de noemer een deler is van p^n. We hadden ook aangenomen dat $e^a = r/s$. Dus I_n is een rationaal getal met een noemer die sp^n deelt. Zometeen zal blijken dat $I_n \neq 0$. Dit betekent dat $|I_n| \geq 1/(sp^n)$ en hiermee hebben we, analoog aan het irrationaliteitsbewijs van e, een ondergrens.
Nu nog een bovengrens. De belangrijke opmerking is hier dat $(d/dt)^k(t^n(1-t)^n)$ een nulpunt in $t = 0$ en in $t = 1$ heeft als $k < n$. Dit komt doordat $0, 1$ n-voudige nulpunten van $t^n(1-t)^n$ zijn en bij elke differentiatie gaat deze multipliciteit met slechts 1 omlaag. Als $k = n$ dan zijn er geen nulpunten in $0, 1$ meer, maar we hebben dan wel, op de factor $n!$ na, het n-de Legendre polynoom verkregen. We gaan nu de integraal I_n n-maal herhaald partieel integreren door elke keer de factor e^{at} in de integrand te differentiëren. De randtermen van de vorm $[\ldots]_0^1$

zijn telkens nul vanwege de zojuist genoemde nulpunten van $\left(\frac{d}{dt}\right)^k t^n(1-t)^n$. We krijgen,

$$\begin{aligned} I_n &= \frac{a}{n!}\int_0^1 e^{at}\left(\frac{d}{dt}\right)^n (t^n(1-t)^n)dt \\ &= a\frac{-a}{n!}\int_0^1 e^{at}\left(\frac{d}{dt}\right)^{n-1} (t^n(1-t)^n)dt \\ &\ldots \\ &= a\frac{(-a)^n}{n!}\int_0^1 e^{at}t^n(1-t)^n dt \end{aligned}$$

Allereerst merken we op dat de integrand van de laatste integraal positief is. Dus $I_n \neq 0$ zoals we beloofd hadden. Verder leent de laatste integraal zich prima voor een afschatting. We gebruiken dat $|t(1-t)| < 1$ voor $t \in [0,1]$ en vinden,

$$|I_n| < \frac{|a|^{n+1}}{n!}e^{|a|}$$

Zetten we nu onze ongelijkheden achter elkaar, dan vinden we

$$1/(sp^n) < |a|^{n+1}e^{|a|}/n!$$

Na vermenigvuldiging met p^{n+1} krijgen we $p/s < |pa|^{n+1}e^{|a|}/n!$. Laten we nu $n \to \infty$ gaan, dan gaat de rechterkant van de ongelijkheid naar nul. Dus $p/s \leq 0$ hetgeen onmogelijk is omdat p, s positief geheel zijn. We hebben weer een tegenspraak en e^a kan niet rationaal zijn. □

Het irrationaliteitsbewijs voor π loopt op vrijwel precies dezelfde manier. We gebruiken nu het volgende Lemma.

Lemma 19.2.5 *Zij $n \in \mathbb{Z}_{\geq 0}$. Dan is*

$$\pi \int_0^1 t^n \sin \pi t \ dt$$

een polynoom in $1/\pi^2$ met gehele coëfficienten en graad $\leq [n/2]$.

Dit volgt wederom door volledige inductie. Voor $n = 0$ en $n = 1$ berekenen we gemakkelijk

$$\pi \int_0^1 \sin \pi t \ dt = 2 \qquad \pi \int_0^1 t \sin \pi t \ dt = 1.$$

Stel nu $n > 1$. Door tweevoudige partiële integratie vinden we dat

$$\pi \int_0^1 t^n \sin \pi t \ dt = 1 - \frac{n(n-1)}{\pi}\int_0^1 t^{n-2} \sin \pi t \ dt.$$

Hieruit volgt op recursieve wijze ons Lemma. □

Nu het irrationaliteitsbewijs voor π^2. Neem aan dat $\pi^2 = r/s$ met $r, s \in \mathbb{N}$. We beschouwen de integraal

$$I_{2n} = \pi \int_0^1 P_{2n}(t) \sin \pi t \; dt.$$

Volgens bovenstaand Lemma is dit een polynoom van graad $\leq 2n/2 = n$ in $1/\pi^2$ met gehele coëfficienten. Dit betekent dat I_{2n} een rationaal getal is met een noemer die r^n deelt. Zometeen laten we zien dat $I_{2n} \neq 0$ en dus, $|I_{2n}| \geq 1/r^n$. Anderzijds kunnen we I_{2n} van boven afschatten door een $2n$-voudige partiële integratie uit te voeren waarbij we in elke stap $\sin \pi t$ differentiëren. We vinden,

$$I_{2n} = \pi(-1)^n \frac{\pi^{2n}}{(2n)!} \int_0^1 \sin \pi t \; t^{2n}(1-t)^{2n} dt$$

Allereerst, omdat de laatste integrand positief is, geldt $I_{2n} \neq 0$ zoals beloofd. Verder geldt,

$$|I_{2n}| < \frac{\pi^{2n+1}}{(2n)!}.$$

Combinatie van de onder- en bovengrens geeft $1/r^n < \pi^{2n+1}/(2n)!$. Na vermenigvuldiging met r^n, $1 < r^n \pi^{2n+1}/(2n)!$. Laat nu $n \to \infty$ dan gaat de rechterzijde van de ongelijkheid naar 0 en we houden over dat $1 < 0$. Duidelijk een tegenspraak. Dus π^2 is irrationaal. □

19.3 Transcendentie

In dit hoofdstuk zijn er qua benaming een aantal parallellen te trekken met termen uit de psychologie. Hebben het in voorgaande paragrafen over (ir)rationaliteit gehad, hier gaan we nog een stapje verder met het begrip transcendent. Overigens zijn er ook nog andere wiskunde termen met een synoniem in de psychologie. Bijvoorbeeld: complex, karakter, eigenwaarde, etc.

Definitie 19.3.1 *Een getal α heet algebraïsch als het een nulpunt is van een niet triviaal polynoom P met gehele coëfficienten. Een getal heet transcendent als het niet algebraïsch is.*

Ter herinnering, een triviaal polynoom is het polynoom dat alleen coëfficienten nul heeft. Het is duidelijk dat rationale getallen ook algebraïsch zijn. De breuk $\alpha = p/q$ is immers nulpunt van $qx - p$. Om transcendentie van een getal α aan te tonen moeten we laten zien dat $P(\alpha) \neq 0$ voor elk niet-triviaal polynoom P met gehele coëfficienten. Dit is veel meer werk dan het aantonen van irrationaliteit van α waarin we alleen maar polynomen P van graad 1 hoeven te bekijken.

Het mag dan ook geen verbazing wekken dat het lang heeft geduurd voor men van natuurlijk voorkomende getallen de transcendentie kon aantonen. Dat er überhaupt transcendente getallen bestaan werd voor het eerst door Liouville in 1844 aangetoond. We zullen hier niet de hele theorie behandelen, maar slechts één voorbeeld eruit lichten.

Stelling 19.3.2 *Het getal*

$$\alpha = \sum_{k=0}^{\infty} \frac{1}{2^{k!}}$$

is transcendent.

De reden dat we van dit getal transcendentie kunnen aantonen is dat de reeks $\sum_{k=0}^{\infty} 1/2^{k!}$ waanzinnig snel convergeert. De afgebroken reeks $\alpha_n = \sum_{k=0}^{n} 1/2^{k!}$ geeft voor kleine n al een zeer goede benadering. Om nu transcendentie van α aan te tonen, nemen we het tegendeel aan, namelijk dat α voldoet aan een polynoomvergelijking. Stel dat $P(\alpha) = 0$ waarin P een polynoom met gehele coëfficienten is. We gaan nu zowel een boven- als onderafschatting voor $|P(\alpha_n)|$ geven en krijgen een tegenspraak als $n \to \infty$. Merk allereerst op dat α_n een rationaal getal met noemer $2^{n!}$ is.
Zij d de graad van P. Dan is $P(\alpha_n)$ een breuk met noemer die $2^{dn!}$ deelt. Verder kan $P(\alpha_n)$ slechts voor eindig veel n nul worden omdat P niet meer dan d nulpunten heeft. Door n voldoende groot te kiezen zorgen we er dus voor dat $P(\alpha_n) \neq 0$. Maar dan geldt $|P(\alpha_n)| \geq 1/2^{dn!}$. Dit was de ondergrens die, evenals bij irrationaliteitsbewijzen, altijd in transcendentiebewijzen voorkomt.
Voor de bovengrens stellen we $Q(x) = P(x)/(x - \alpha)$ en M het maximum van $|Q(x)|$ als $x \in [0, \alpha]$. Dan geldt voor elke $x \in [0, \alpha]$ dat $|P(x)| = |Q(x)| \cdot |x - \alpha| \leq M \cdot |x - \alpha|$. In het bijzonder geldt dit voor $x = \alpha_n$. Het verschil $\alpha - \alpha_n$ kunnen we afschatten met

$$\begin{aligned} |\alpha - \alpha_n| &= \frac{1}{2^{(n+1)!}} + \frac{1}{2^{(n+2)!}} + \frac{1}{2^{(n+3)!}} + \cdots \\ &< \frac{1}{2^{(n+1)!}} \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) \\ &= \frac{2}{2^{(n+1)!}} \end{aligned}$$

Dus $|P(\alpha_n)| < M|\alpha_n - \alpha| < 2M/2^{(n+1)!}$. Zetten we onder- en bovengrens achter elkaar, $1/2^{dn!} < M/2^{(n+1)!}$. Na vermenigvuldiging met $2^{(n+1)!}$ wordt dit $2^{(n+1-d)n!} < 2M$. De linkerzijde van de ongelijkheid gaat echter naar oneindig als $n \to \infty$. We hebben dus een tegenspraak, en α is transcendent. $\square$

Bovenstaand bewijs is het enige transcendentie bewijs dat binnen het bestek van dit boek valt. De verwante reeksen $\sum_{k=1}^{\infty} 2^{-2^n}$ en $\sum_{k=1}^{\infty} 2^{-n^2}$ convergeren weliswaar minder snel, maar zien er op het oog verder hetzelfde uit. Echter,

schijn bedriegt. Pas in 1930 bewees K.Mahler dat de eerste transcendent is en de transcendentie van de tweede is een resultaat van Nishioka en Duverney als gevolg van recente ontwikkelingen in de transcendentietheorie in 1996.
De bovenstaande reeksen zijn tamelijk gekunsteld en komen niet vaak op natuurlijke wijze in bijvoorbeeld de analyse voor. We zijn uiteraard meer geïnteresseerd in getallen zoals e en π. Hiervoor heeft het transcendentiebewijs relatief lang op zich laten wachten. In 1873 bewees Hermite de transcendentie van e en in 1882 volgde de transcendentie van π door Lindemann. Met dit laatste was meteen het bewijs geleverd van de onmogelijkheid van het klassieke Griekse probleem van de *kwadratuur van de cirkel*. Dit probleem is één van de vele constructieproblemen uit de klassieke Griekse meetkunde. Het gaat erom, uitgaande van een lijnstuk met lengte 1, met passer en liniaal een vierkant te construeren waarvan de oppervlakte gelijk is aan de oppervlakte van de cirkel met straal 1. Dit betekent in het bijzonder dat we een lijnstuk met lengte $\sqrt{\pi}$ moeten construeren, de zijde van zo'n vierkant. Het is echter bekend dat constructies die uitgaan van een lijnstuk met lengte 1 alleen nieuwe lijnstukken kunnen opleveren die algebraïsch zijn. Omdat π, en dus ook $\sqrt{\pi}$, transcendent is kan de gevraagde cirkel niet geconstrueerd worden. Meer details kan de lezer in het boekje van Martinus Riemersma [Rie] vinden.
In deze eeuw heeft de transcendentietheorie zich langzaam maar zeker verder ontwikkeld tot een aparte discipline. We zullen er niet te diep op ingaan maar vermelden wel *Hilbert's 7de probleem*. In 1900 hield de beroemde Duitse wiskundige David Hilbert een voordracht voor het wereldcongres van wiskundigen over de wiskundige problemen die in de komende eeuw een rol zouden kunnen spelen in de ontwikkeling van de wiskunde. Hij behandelde een lijst van 23 problemen en de zevende bestond uit de vraag of α^β transcendent is als α en β algebraïsch zijn. Dus bijvoorbeeld, is $2^{\sqrt{2}}$ transcendent ?
Zeer verrassend werd in 1934 al het antwoord gegeven door, onafhankelijk van elkaar, A.O.Gel'fond en Th.Schneider. Hier is de stelling.

Stelling 19.3.3 (Gel'fond, Schneider, 1934) *Zij α, β een tweetal algebraïsche getallen en stel dat $\alpha \neq 0, 1$ en $\beta \notin \mathbb{Q}$. Dan is α^β transcendent.*

Dus, als toepassing, de getallen $2^{\sqrt{2}}$ en, voor wie complexe getallen kent, $(-1)^i = e^\pi$ zijn transcendent.

19.4 Aftelbaarheid

In de vorige paragraaf zagen we dat het bewijzen van transcendentie van een getal over het algemeen een moeizame zaak is. Daarentegen weet men wel dat bijna alle reële getallen transcendent zijn. Dit volgt uit een aantal briljante ideeën van G.Cantor, de wiskundige die rond het eind van de 19e eeuw het denken over verzamelingen in gang zette en daarmee een nieuwe ontwikkeling in de wiskunde. Van hem is het begrip *aftelbare verzameling*. Een informele, maar hopelijk duidelijke, omschrijving van dit begrip is het volgende. Een verzameling V noemen we aftelbaar als we de elementen een nummering kunnen geven zó dat elk element van V een nummer krijgt. Dit betekent dat we met de elementen van V in een rij kunnen vormen waarin elk element van V minstens éénmaal voorkomt. Het is daarbij toegestaan dat een element herhaalde malen in de rij voorkomt. Uiteraard zijn de natuurlijke getallen aftelbaar want de elementen van $\mathbb{N}$ hebben zichzelf als nummer en kunnen in de rij $1, 2, 3, 4, \ldots$ gezet worden. De gehele getallen zijn ook aftelbaar, de elementen van $\mathbb{Z}$ kunnen in de rij $0, 1, -1, 2, -2, 3, -3, \ldots$ gezet worden. Zelfs de positieve rationale getallen zijn aftelbaar. We maken in dat geval een rij door voor $N = 2, 3, 4, \ldots$ alle breuken op te schrijven waarvan de som van teller en noemer gelijk is aan N. Op deze manier weten we zeker dat elke breuk in onze rij aan bod komt. We krijgen de rij

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \ldots$$

We zien dat hierin herhalingen voorkomen, bijvoorbeeld $\frac{1}{1}$ en $\frac{2}{2}$, maar dit is niet erg. De belangrijke voorwaarde is dat elk positief rationaal getal minstens éénmaal in deze rij voorkomt. Op soortgelijke manier kunnen we ook laten zien dat $\mathbb{Q}$ aftelbaar is. Het is aardig om je te realiseren dat, hoewel $\mathbb{Q}$ een veel 'grotere' verzameling dan $\mathbb{N}$ is, de verzameling $\mathbb{Q}$ toch afgeteld kan worden en in die zin gelijkmachtig is, zoals men zegt, met $\mathbb{N}$. We gaan nog één stap verder.

Stelling 19.4.1 *De verzameling van algebraïsche getallen is aftelbaar.*

De aftelling gaat als volgt. Elk algebraïsch getal is nulpunt van een polynoom met gehele coëfficienten. Dit betekent dat we de algebraïsche getallen kunnen aftellen door de polynomen met gehele coëfficienten af te tellen. Beschouw een willekeurig polynoom $P(x) = p_m x^m + p_{m-1}x^{m-1} + \ldots, +p_1 x + p_0$ met $p_i \in \mathbb{Z}$ en $p_m \neq 0$. Dan is m de graad van $P(x)$. We geven $P(x)$ een maat $M(P) = m + |p_0| + |p_1| + \cdots + |p_{m-1}| + |p_m|$. De belangrijke opmerking is dat voor gegeven M_0 er slechts eindig veel polynomen P met maat M_0 bestaan. Immers de graad van P kan niet groter dan M_0 zijn en de coëfficienten worden ook elk in absolute waarde begrensd door M_0. De aftelling van polynomen kunnen we tot stand brengen door achtereenvolgens voor $N = 0, 1, 2, 3, \ldots$ alle polynomen op te schrijven met maat N. $\square$

Voordat de lezer misschien gaat denken dat alle verzamelingen aftelbaar zijn geven we ook de volgende stelling.

Stelling 19.4.2 (Cantor) *De verzameling reële getallen is niet aftelbaar.*

Het is voldoende om te laten zien dat de reële getallen in het interval $]0, 1[$ niet aftelbaar zijn. Stel dat dit interval wel aftelbaar is, en beschouw een aftelling.

Stel dat in deze aftelling het n-de reële getal een decimale ontwikkeling heeft die we aangeven met $0.a_{n1}a_{n2}a_{n3}\ldots$ waarin $a_{nm} \in \{0,1,2,3,4,5,6,7,8,9\}$. De rij ziet er dus uit als

$$
\begin{array}{c}
0.a_{11}a_{12}a_{13}a_{14}\ldots \\
0.a_{21}a_{22}a_{23}a_{24}\ldots \\
0.a_{31}a_{32}a_{33}a_{34}\ldots \\
\ldots \\
0.a_{n1}a_{n2}a_{n3}a_{n4}\ldots \\
\ldots
\end{array}
$$

Kies nu voor elke i een cijfer b_i dat ongelijk is aan a_{ii} beschouw het reële getal β met decimale onwtikkeling $0.b_1b_2b_3\ldots$. Dit getal zou ook in onze aftelling moeten voorkomen. Zeg dat β het m-de getal in onze aftelling is. Dan geldt dat $0.b_1b_2b_3\ldots = 0.a_{m1}a_{m2}a_{m3}\ldots$. In het bijzonder volgt hieruit dat $b_m = a_{mm}$, hetgeen in flagrante tegenspraak is met onze constructie waarin we $b_m \neq a_{mm}$ namen. Blijkbaar komt β niet in de aftelling voor, en dit betekent dat $[0,1]$ geen aftelbare verzameling kan zijn. $\square$

De procedure waarmee we *overaftelbarheid* van $\mathbb{R}$ aantoonden staat bekend als de *diagonaalprocedure* van Cantor en wordt in vele situaties in de wiskunde aangewend.

Omdat $\mathbb{R}$ een overaftelbare (=niet aftelbare) verzameling is, en de algebraïsche getallen aftelbaar, volgt dat de transcendente getallen een overaftelbare verzameling vormen. Kortom, er zijn genoeg transcendente getallen. Dit maakt het des te ironischer dat de transcendentie van natuurlijk voorkomende getallen zoals e en π pas tegen het eind van de 19e eeuw met veel moeite aangetoond kon worden.