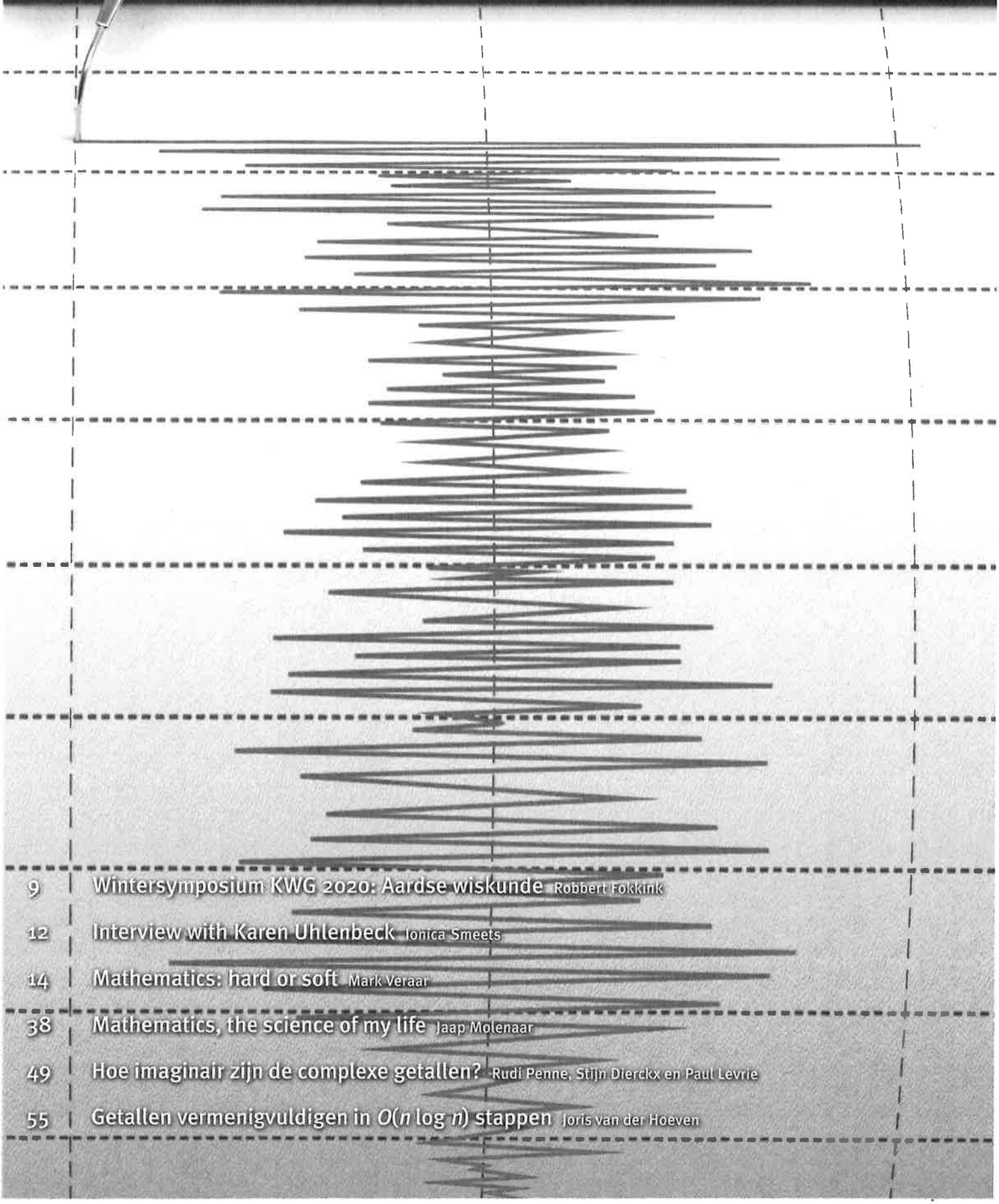
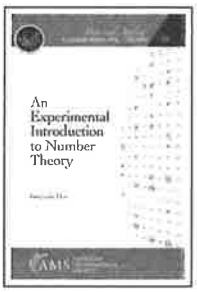
vijfde serie, deel 21, nummer 1 maart 2020 uitgave van het Koninklijk Wiskundig Genootschap

Nieuw Archief voor Wiskunde



Boekbesprekingen

| Book Reviews



Benjamin Hutz

An Experimental Introduction to Number Theory

American Mathematical Society, 2018
XII + 313 p., prijs $79.00
ISBN 9781470430979

Er zijn al veel boeken verschenen over getaltheorie (of getallentheorie, zoals sommigen liever zeggen). Het is een van de oudste onderwerpen in de wiskunde, diens koningin zelfs, volgens Gauss: "Die Mathematik ist die Königin der Wissenschaften und die Zahlentheorie ist die Königin der Mathematik." (Gauss vervolgt dit met zoiets als "Zij verlaagt zich vaak tot dienstverlening aan de astronomie en andere natuurwetenschappen, maar in al haar relaties verdient ze de eerste plaats.")

Valt er nog iets nieuws te bieden op dit gebied, na een standaardwerk als Hardy & Wright (*An Introduction to the Theory of Numbers*, Oxford University Press, 1938, 1e druk; 2008, 6e druk). Voor mij was dat destijds een hele kluif (die ik nooit heb opgekregen). Natuurlijk zijn er nieuwe resultaten (rond the laatste stelling van Fermat, priemtweelingen, priemwoestijnen, de vermoedens van Goldbach en van Catalan; zie ook Alex van den Brandhof, *Priemwoestijnen: Hoogtepunten uit de wiskunde van de 21e eeuw*, Prometheus, 2018, waarvan zes hoofdstukken over getaltheorie gaan), maar dat vergt allemaal behoorlijk geavanceerde wiskunde. Het hier gerecenseerde boek probeert er op een andere manier uit te springen, namelijk door de lezer aan te moedigen tot experimenteren met de computer.

Na lezing blijkt Benjamin Hutz een tamelijk traditioneel wiskundeboek over getaltheorie geschreven te hebben, in de trant van definitie, stelling, bewijs (veelal uit de hoge hoed). De lezer wordt weinig motivatie en historische achtergrond geboden. Wel beginnen nieuwe onderwerpen met een wat open 'vraag' (Question) in een kader. (Waarop de lezer op dat moment vaak geen antwoord zal kunnen geven, bijvoorbeeld: Question 1.51. Determine the function $\pi(N)$. Hier is $\pi(N)$ het aantal priemen ten hoogste N.). Dan zijn er kaders met 'onderzoekingen' (Investigation) waarbij met de hand of met de computer data verzameld moeten worden voor concrete gevallen om patronen te ontdekken en vermoedens te kunnen formuleren. Elk hoofdstuk wordt afgesloten met een ruime selectie aan oefenopgaven, ingedeeld in Computational Exercises, Theoretical Exercises en Exploration Exercises. Het boek blijkt een theoretische inleiding te zijn, maar wel doorspekt met experimenten.

Even een greep uit de inhoudsopgave: gehele getallen (met unieke priemontbinding), modulair rekenen (met kleine Fermat en de Chinese reststelling), kwadratische wederkerigheid (met primitieve wortels), verrassend genoeg wat cryptografie (symmetrisch, asymmetrisch met Diffie–Hellman en RSA, maar ook secret sharing), rekenkundige functies (Euler en Möbius, alsmede partities), algebraïsche getallen (met onder andere sommen van kwadraten), rationale en irrationale getallen (met kettingbreuken), diofantische vergelijkingen (met pythagoreïsche drietallen, de laatste stelling van Fermat, de vergelijking van Pell en het probleem van Waring), elliptische krommen, discrete dynamische systemen (met de Mandelbrot verzameling in een onderzoeking), en tot slot een beetje over

Redactie: Hans Cuypers en Hans Sterk

Review Editors NAW - MF 7.092
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven

reviews@nieuwarchief.nl
www.win.tue.nl/wgreview

polynomen. Al met al de klassieke onderwerpen met een paar uitstapjes (cryptografie en dynamische systemen).

U vraagt zich misschien af hoe dat experimenteren met de computer wordt ondersteund. De auteur was zich er terdege van bewust dat elke keuze van een specifieke programmeertaal twee problemen zou geven. Ten eerste gaat het daarmee op een informaticaboek lijken en ten tweede is die keuze altijd fout en veroudert het boek veel sneller. Daarom staan er alleen wat algoritmes in pseudocode in, en wordt de rest aan (de fantasie van) de lezer overgelaten. En juist voor getaltheorie zouden wat aanwijzingen nuttig zijn, want rekenen met grotere getallen geeft vaak problemen (denk aan afronden en overloop). Dit maakt dat het boek voor zelfstudie door bijvoorbeeld een middelbare scholier niet geschikt is, want de drempel tot echt zelf experimenteren is hoog. Die scholier (of geïnteresseerde leek) is veel beter af met het boek van Frits Beukers, *Getaltheorie voor beginners* (Epsilon Uitgaven, 6e druk, 2018), dat nagenoeg dezelfde stof afdekt, zij het iets minder formeel.

Ik wil het boek van Hutz nog even vergelijken met twee andere boeken over getaltheorie die ik de laatste jaren onder ogen heb gekregen en die ook iets hebben dat ze 'anders' maakt.

Michael Rassias schreef in 2011 zijn afstudeerverslag over 'computational number theory', dat vervolgens uitgegeven werd als *Problem-Solving and Selected Topics in Number Theory: In the Spirit of the Mathematical Olympiads* (Springer, 2011). Rassias won als 15-jarige een zilveren medaille bij de Internationale Wiskunde Olympiade in 2003, wat de ondertitel van zijn boek verklaart. Het boek van Rassias biedt veel problemen van olympiadeniveau, (wat voor mij de reden was om het aan te schaffen). Dit zijn veelal geen gewone oefenopgaven maar uitdagingen die enige creativiteit vergen. Daarbij wordt een stuk getaltheorie systematisch opgebouwd. Bovendien bevat het wat originele wiskunde, zoals het vermoeden van Rassias: voor elk priemgetal $p > 2$, bestaan er twee priemgetallen p_1, p_2 met $p = \frac{p_1 + p_2 + 1}{p_1}$. Helaas moest ik al snel constateren dat de uitgever deze jonge auteur beter in bescherming had moeten nemen, want ondanks lovende woorden schiet het boek tekort. De presentatie is vaak didactisch onbeholpen en onvolledig. Zo worden belangrijke begrippen gebruikt zonder ze eerst netjes te definieren, zoals $n!$, $a \mid b$ en (a,b) in de betekenis van ggd. Het lijkt erop dat de lezer al een olympiadetraining achter de rug moet hebben.

Het laatste boek over getaltheorie dat ik hier wil noemen is *An Illustrated Theory of Numbers* van Martin Weissman (AMS, 2017). Het is anders omdat het visualisatie centraal stelt. Waar Hutz maar één esthetische afbeelding bevat (Fig. 7.1. Rational points on the unit sphere), staat het boek van Weissman vol met aantrekkelijke afbeeldingen, veelal in kleur. Het is in een fraai groot formaat uitgegeven, met ruime marges die benut worden voor illustraties en extra uitleg (helaas niet als e-book). In 'Illustrating the Theory of Numbers', *Proceedings of Bridges 2018: Mathematics, Art, Music, Architecture, Education, Culture* (Tesselations Publishing, pp. 211–218, 2018, http://archive.bridgesmathart.org/2018/bridges2018-211.pdf) beschrijft Weissman hoe hij zijn uitdaging om getaltheorie over te brengen aan zijn studenten door middel van visualisaties heeft aangepakt en welke principes hij daarbij heeft gehanteerd. Hij werd daardoor in zekere zin ook (wis)kunstenaar. Wiskundig reikt zijn boek minder ver dan dat van Hutz, maar dit wordt ruimschoots gecompenseerd door het diepere inzicht dat geboden wordt.

Tom Verhoeff

Yann Bugeaud

Linear Forms in Logarithms and Applications

European Mathematical Society, 2018
xvi + 224 p., prijs € 38,00
ISBN 9783037191835

The linear form $L(a,b) := a\log 2 + b\log 3$ in the variables a and b is a basic example of a linear form in logarithms. Certainly $L(a,b) \neq 0$ for any integers $(a,b) \neq (0,0)$, as equality would lead to the impossible identity $2^a = 3^{-b}$. Starting in the late 1960s Alan Baker (1939–2018) obtained some ground breaking estimates for how small linear forms in logarithms such as $L(a,b)$ as a function of N can be as we range over the integers $-N \leq a \leq N$ and $-N \leq b \leq N$. In 1970 he won the Fields Medal for this work. In this very basic set-up Baker's work gives $\log |L(a,b)| > -C\log N$, with some explicit C. It allows one to prove (Theorem 3.1 in the book) that for all positive integers m and n, we have $|2^m - 3^n| > 2^m (em)^{-8.4\cdot 10^8}$, showing that the distance between a power of 2 and the power of 3 closest to it, tends to infinity when the power of 2 tends to infinity. More generally one would consider the linear form

$$\Lambda_n := \beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n,$$

with the α_i non-zero algebraic numbers such that $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals and the β_i are also algebraic numbers, not all zero.

To the uninitiated the above set-up might appear to be of very limited interest. However, the reality is very different! With the help of Baker's theorems lots of Diophantine problems can be attacked. Baker for example used his method to solve the Gauss's celebrated class number one and later the class number two problem (this problem can be reduced to solving a Diophantine equation). Tijdeman used Baker's method to show that the Catalan equation $x^p - y^q = 1$ has only finitely many solutions with $x,p,y,q > 1$. The method also allows one to make some (modest) progress on the very important abc-conjecture (see below).

In practice many problems can be reduced to lower bounds for linear forms in two or three logarithms. Whereas for linear forms in two logarithms rather sharp lower bounds are available, this is not the case for three logarithms. As a rule of thumb, when a Diophantine problem can be reduced to linear forms in only two logarithms, then it often can be completely solved. If more logarithms are needed one typically ends up with huge bounds on the size of the solutions. However, sometimes using the so-called LLL-algorithm (not discussed in this book, but, e.g., in the book of Evertse and Győry discussed below), a complete solution is possible here.

This book is an introduction to Baker's theory of linear forms in the logarithms of algebraic numbers, with a special emphasis on a large variety of its applications, mainly to Diophantine problems. Its aim is to train the reader how to apply results from the theory of linear forms in complex and p-adic logarithms. In order not to complicate this process too much, often neither the results used, nor the applications that are established, are stated in the greatest possible generality.

After a brief introduction to linear forms in logarithms, the author lists in Chapter 2 several estimates for linear forms in complex and p-adic logarithms, which are used throughout the book. This is the toolbox, so to say, and in the rest of the book the author demonstrates how to use it. He starts doing so in Chapter 3, which is devoted to Diophantine problems from which one can very simply derive a linear form in complex algorithms and then apply an appropriate result from Chapter 2.

In Chapter 4 the author considers applications to classical families of Diophantine equations. For many of these there were early fundamental results by Thue and Siegel showing that these equations have at most finitely many solutions. Unfortunately, the early works did not yield upper bounds for the solutions and so were of little help for the complete resolution of the equation. Baker's method allows one, at least in principle, to completely solve some of these equations. A more extensive discussion can be found in a book from 1986 by Shorey and Tijdeman (see below).

Chapter 5 is concerned with the situation where the $\alpha_1,\ldots,\alpha_n$ in the linear form Λ_n are all rational numbers very close to 1. In this situation sharper bounds are available leading to, e.g., effective irrationality measures for quotients of logarithms of rational numbers.

For a non-rational number x, let $\nu_p(x)$ denote the exponent of p in the decomposition of x as a product of prime powers. In the theory of p-adic linear forms in logarithms, one seeks to find a non-trivial upper bound for quantities like $\nu_p(2^a\cdot 3^b-1)$ as we range over the integers $-N\le a\le N$ and $-N\le b\le N$ and N is large. Here we have $Cp\log N$ as upper bound, with C a constant. The linear dependency on p is quite unsatisfactory and it is a major open problem to improve on this dependency. In Chapter 6, among other results these estimates are used to extend the effective estimates for the size of the solutions of classical families of Diophantine equations obtained in Chapter 4 to S-integers. A rational number whose numerator and denominator are composed of only prime numbers from a given finite set S, is said to be an S-unit.

The abc-conjecture claims that, for every $\epsilon>0$, for all positive coprime integers a, b and c with $a+b=c$, there exists a number $C(\epsilon)$ depending only on ϵ, such that $c<C(\epsilon)m^{1+\epsilon}$, with m the squarefree kernel of abc, that is $m=\prod_{p\mid abc}p$ is the product of all distinct prime divisors p of abc. It implies for example that if we add two powers of smallish numbers, the resulting sum cannot also be a high power of a smallish integer. In particular, Fermat's Last Theorem is a relatively straightforward consequence of the abc-conjecture. Arguably the abc-conjecture is the mother of all Diophantine problems and states in essence that the operation of adding does not respect the multiplicative structure of integers. Apart from implying Fermat's Last Theorem, it has lots of other consequences. In Chapter 8 the author, following Stewart and Yu, proves, combining complex and p-adic linear forms in logarithms, a much weaker version of the abc-conjecture.

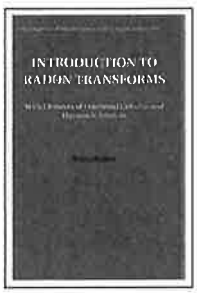
In Chapters 7, 9 and 10 the author considers, respectively, primitive divisors of certain linear recurrences, simultaneous linear forms in logarithms and applications, and multiplicative dependence between algebraic numbers.

In Chapters 11 and 12 the author presents complete proofs of versions of some of the basic results in Chapter 2, with the same dependence in the parameters, but with larger numerical constants (as that leads to some simplification of the proofs).

Finally, in Chapter 13 the author lists some open questions and conjectures related to the theory of linear forms in logarithms.

I will end this review by comparing Bugeaud's book to two other ones covering partly the same ground. As to applications of Baker's method in the theory of Diophantine equations, these are treated in a book by Shorey and Tijdeman (*Exponential Diophantine Equations*, Cambridge Tracts in Mathematics 87, Cambridge University Press, 1986) in much greater generality. There is also some overlap with the monograph of Evertse and Győry (*Unit Equations in Diophantine Number Theory*, Cambridge Studies in Advanced Mathematics 146, Cambridge University Press, 2015) that I also recently discussed here (*NAW* 5/19(1), 2018, pp. 62–63). The latter book focuses more on presenting the state of the art and filling some gaps in the literature. The present book, in contrast, is focused on training the reader in Baker's method. In my opinion it does a good job in that, and an impressive range of different applications is covered. Thus this book has its own place and is a helpful stepping stone to actively understanding more theoretical books.

Pieter Moree



Boris Rubin

Introduction to Radon Transforms
With Elements of Fractional Calculus and Harmonic Analysis

Cambridge University Press, 2015
xvii + 576 p., prijs £135.00
ISBN 9780521854597

Dit veelomvattende boek behandelt, met een weelde aan details, de harde (functionaal)analyse van diverse typen *Radon-transformaties*. Heel algemeen: Een R-transformatie is een integraaltransformatie, die een functie op een 'meetkundige' ruimte $\mathbb{X}$ overvoert in een functie op een ruimte $\mathbb{Y}$, met als kenmerkende bijzonderheid dat $\mathbb{Y}$ bestaat uit een klasse meetkundige objecten, die zich in $\mathbb{X}$ bevindt. Denk aan rechte lijnen in $\mathbb{R}^3$ of aan grote cirkels in $\mathbb{S}^2$.

R-transformaties hebben belangrijke toepassingen in de medische wereld, waar vooral het praktisch realiseren van de *inverse R-transformatie* cruciaal is.

Dit boek is elegant opgebouwd. Alleen al de hoofdstukken 'Preliminaries', 'Fractional Integration' en 'Riesz Potentials' samen met de appendix 'Harmonic Analysis on the Unit Sphere' zouden een schitterend inleidend boek over 'Analyse op $\mathbb{R}^n$' kunnen vormen. Een stiefkindje in veel opleidingen!

Het grootste hoofdstuk behandelt de traditionele R-transformatie, waarbij $\mathbb{X}=\mathbb{R}^n$ en $\mathbb{Y}$ een collectie hypervlakken in $\mathbb{R}^n$ is. Vooral de relatie tot fractionele integralen en sferische harmonischen wordt uitgediept, evenals de functionaalanalyse van dualen en inversen in relatie tot een grote schaar van functieruimten.

Dan de standaard R-transformatie op de eenheidssfeer. Daarbij wordt uitgegaan van $\mathbb{X}=\mathbb{S}^{n-1}$. De $\mathbb{Y}$-ruimte kan dan bestaan uit 'grote cirkels' van dimensie $n-2$, de Funk-transformatie. Bij andere, in extenso behandelde, gevallen bestaat $\mathbb{Y}$ uit 'hemisferen', of ook wel kleinere 'kapjes', rondom een bepaald punt op $\mathbb{S}^{n-1}$. Ook een stel andere convolutie-achtige transformaties komt aan bod.