

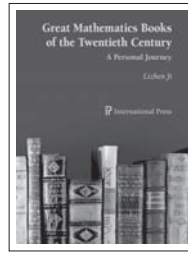
Boekbesprekingen

| Book Reviews

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



Lizhen Ji

Great Mathematics Books of the Twentieth Century A Personal Journey

International Press of Boston, 2014
 xxiv + 667 p., prijs \$ 119
 ISBN 9781571462831

For the learning of mathematics, books probably will remain indispensable. The question then is which books one should have, either for reading or for referencing. Evidently, much depends on the specific aim of the mathematician, teacher or student. The work at hand contains reviews of a virtual library of math books from the twentieth century, aimed at scholarship and learning.

This virtual library is organized according to the following chapters: 'Expository books on mathematics and mathematicians', followed by the classical trio 'Analysis', 'Algebra', 'Geometry', then 'Topology', 'Number Theory' (a long one), 'Differential Equations', 'Lie Theories' (close to the interests of the author himself), 'Mathematical Physics, Dynamical Systems and Ergodic Theory' (close to the interests of your reviewer), 'Discrete Mathematics and Combinatorics', 'Probability and Applications' with a conclusive 'Foundations of Math, Computer Science, Numerical Math'. Most of the reviews cite phrases from the *Bulletin of the AMS*, *MathSciNet* or *Zentralblatt*, but now and again the author has read the book himself and adds quotations and comments himself. Already in the chapter on expository books he gives Godfrey Hardy's famous quote from *A Mathematician's Apology*: "Beauty is the first test: there is no permanent place in the world for ugly mathematics." This test is what I would call Hardy's razor, an instrument that the author, to my opinion, has wielded quite successfully.

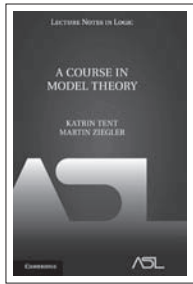
The book contains a great many pictures, portraits and brief descriptions of earlier math books and mathematicians. The book titles run from Euclid's *Elements*, via James Clerk Maxwell's *An Elementary Treatise on Electricity*, Sophus Lie's *Geometrie der Berührungstransformationen* and tome XI from Henri Poincaré's *Œuvres*, to Hassler Whitney's *Geometric Integration Theory*, just to mention a few. The library of the University of Michigan is fortunate to have such a rich collection! I should mention that also many photographs of this library have been included in the book.

Lizhen Ji's personal journey leads along many math books that I was fortunate enough to grow up with myself, both in the general learning process and in my later area of specialization. In the general category there are many references to Milnor and to Hermann Weyl and also to *The Feynman Lectures on Physics* and to Hawking & Ellis's *The Large Scale Structure of Space-Time*. In the more specialized category, among others, I found the following classics: Vladimir Arnold, *Mathematical Methods of Classical Mechanics*, Ralph Abraham and Jerrold Marsden, *Foundations of Mechanics*, René Thom, *Structural Stability and Morphogenesis*, Jürgen Moser, *Stable and Random Motions in Dynamical Systems*, Ricardo Mañé, *Ergodic Theory and Differentiable Dynamics*, and David Ruelle, *Thermodynamic Formalism*.

Of course, such a virtual library as this cannot be complete in any way. Nevertheless, I couldn't help myself from noticing that

John Oxtoby's *Measure and Category* is missing as well as P. Dirac's *The Principles of Quantum Mechanics*, definitely two classics.

Let me conclude this review. In the lead of the book a few colleague mathematicians have given a brief comment. Among them are the Fields Medalists Shing-Tung Yau and David Mumford. I like to quote the latter "An unusual idea: to write a catalog of the math books you love and/or respect. Anyone's personal list of 'great' books is bound to be idiosyncratic but can also be a useful complement for students to other entry points into the world of scholarly books." For me it was great fun to hold this book in my hands, browse it, and now and again read a bit. *Henk Broer*



Katrin Tent, Martin Ziegler
A course in Model Theory

Lecture Notes in Logic
Cambridge University Press/Association for Symbolic Logic, 2012
 $x + 248$ p., prijs £44.99
ISBN 9780521763240

Modeltheorie is een mooi vak en meer wiskundigen zouden er kennis van moeten nemen. Uit eigen ervaring weet ik dat handig toepassen van de Compactheids- en de Löwenheim-Skolem-stellingen tot snelle en overzichtelijke bewijzen kan leiden. Een van mijn favoriete voorbeelden bij de eerste is de stelling van De Bruyn en Erdős over het kleuren van grafen: als van een oneindige graaf elke eindige deelgraaf k -kleurbaar is, dan is de hele graaf ook k -kleurbaar. Een speciaal geval is de uitspraak dat, gegeven een afbeelding $f: X \rightarrow X$ zonder dekpunten, men X als vereniging van drie verzamelingen A_1 , A_2 en A_3 kan schrijven met $f[A_i] \cap A_i = \emptyset$ voor alle i . De Löwenheim-Skolem-stelling kun je vaak gebruiken als je binnen een grote structuur iets met transfinitie recursie zou willen maken; de stelling geeft in één klap een rijke deelstructuur waarin die recursie al gedaan is en je je in feite op de laatste stappen van je bewijs kunt concentreren. Na keuze van een geschikte taal is op deze manier een kort en krachtig bewijs van de partiëtelstelling van Erdős en Rado te geven (te vinden in Appendix C van het onderhavige boek).

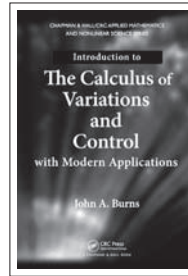
De Modeltheorie houdt niet op bij deze twee stellingen. Er is veel meer te zeggen over modellen van theorieën in het algemeen. Het onderhavige boek geeft een overzicht van een aantal begrippen die vooral in algebraïsche toepassingen van belang zijn gebleken. Hieronder vallen eliminatie van kwantoren, belangrijk voor beslisbaarheids- en volledigheidsvragen, en categoriciteit. Die laatste eigenschap van theorieën zegt dat alle modellen van een gegeven kardinaliteit, zeg κ , isomorf zijn. Hier is \aleph_0 speciaal: elke \aleph_1 -categorische theorie is categorisch in elk overaftelbaar kardinaalgetal κ , maar er zijn veel \aleph_0 -categorische theorieën die vele niet-isomorfe modellen van hogere kardinaliteit hebben. Andere noties die voorbijkomen zijn enkelvoudigheid, stabiliteit, ononderscheidbare elementen en nog veel meer.

Voor wie van algebraïsche toepassingen houdt is er redelijk veel uit het boek te halen, met twee caveats. De opgaven lijken soms onafhankelijk van de theorie in de hoofdtekst gekozen te zijn

en zijn niet zo ondersteunend als men zou willen. Daarnaast wordt het lezen hier en daar wel bemoeilijkt door storende drukfouten en onvolledige uitleg. Een van de hoogtepunten, een versie van een belangrijk tegenvoorbeeld van Hrushovski, wordt hierdoor nogal ontserd. Lezing van het oorspronkelijke artikel leert dat de gebezigde notatie AB voor de vereniging $A \cup B$ staat; dat wordt in het boek niet verteld, maar in het artikel wel en ik moet zeggen dat de uitleg daar duidelijker is dan in het boek.

Met enige voorzichtigheid lezen.

K.P. Hart



John A. Burns

Introduction to the Calculus of Variations and Control with Modern Applications

Chapman & Hall/CRC Applied Mathematics & Nonlinear Science Series
CRC Press, 2014
 $ix + 544$ p., prijs £76.99
ISBN 9781466571396

As the author writes on the first pages of his book, the calculus of variations is very strongly linked to applications. It started with the brachistochrone problem followed by many other applications. Since these problems appear in domains outside mathematics, the author has decided to assume as little 'advanced mathematics' as possible. Thus the reader may find the necessary mathematical machinery within the book. I think this is a very good idea. Working at an applied math department within a technical university, I meet many students who want to learn about variational methods, but lack the mathematical background. It is often difficult to refer them to a textbook that they could read independently. The present book, however, is such a textbook. With the many remarks and examples, it points the students to the power of the variational methods, but also to its difficulties. For instance, Perron's paradox is well explained, showing that assuming that the optimal solution exists, can already lead to wrong answers.

The chapters follow each other in a natural order. First there are the motivation examples, including some non-expected ones like on numerical approximations. After sections on mathematical background and setting up the variational problems, there is a chapter on necessary conditions followed by one on sufficient conditions. Before moving to the second part on optimal control problems, the author closes this first part with extensions and generalisations.

Some authors claim that optimal control is as old as variational calculus, but as the author also writes, its birth lies around 1950. Within optimal control theory a cost, depending on the functions x and u , has to be maximised under the constraint that $\dot{x}(t) = f(x(t), u(t))$. Since in many variational problems the to-be-optimized-cost is a function of x and \dot{x} , by simply writing $\dot{x}(t) = u(t)$, these problems can be seen as optimal control problems. The Maximum Principle gives a way to calculate the optimal control as a function of the state x and the co-state. In many applications, this makes it possible to find an explicit expression for the optimal control. Maybe the best known example of this kind is the linear quadratic optimal control problem (LQ). Here the relation between x and u is given by the linear

differential equation, $\dot{x}(t) = Ax(t) + Bu(t)$, and the cost equals $\int_0^t x(t)^T Qx(t) + u(t)^T Ru(t) dt$. Here x and u are vectors and A, B, Q and R are matrices. Furthermore, $Q \geq 0$ and $R > 0$. The LQ-problem is to minimize the cost given $x(0)$. The optimal control is given as a feedback, i.e., $u(t) = P(t)x(t)$, where P satisfies the Riccati differential equation. This and much more is explained in a very detailed and readable way. As mentioned above, it is a very pleasant book to study from and/or to teach from. *Hans Zwart*



Jan Aarts

Christiaan Huygens: het Slingeruurwerk
Een studie

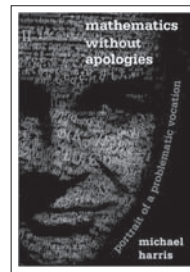
Epsilon Uitgaven, 2015
xx + 256 p., prijs €32,00
ISBN 9789050411516

Christiaan Huygens (1629–1695) was onvergelijkbaar, schreef Gottfried Wilhelm Leibniz (1646–1716) bij zijn overlijden: “Vir incomparabilis, Christianus Hugenius.” En daarmee zei hij niets te veel en niets te weinig. Huygens was inderdaad een briljante wiskundige, die een feilloze intuïtie koppelde aan een onwrikbare strengheid. Hij was ook een erg zeventiende-eeuwse wiskundige die zich de analytische benadering van de klassieke meetkunde volledig eigen had gemaakt, en inventief gebruik maakte van benaderingsmethoden en evenredigheden. Mijn kleine Archimedes noemde zijn vader hem terecht. Wis- en natuurkunde vielen in zijn werk volledig samen en in die zin was hij met zijn optica, mechanica, en musica de grootste wiskundige van zijn tijd. On-zeventiende-eeuws was daarbij zijn gebrek aan interesse voor filosofische vragen — daar duidde Leibniz ook op.

De calculus zouden zijn navolgers Leibniz en Newton ontwikkelen; Huygens dacht nog klassiek meetkundig — hij zag verhoudingen in en tussen figuren. Dat maakt zijn werk voor een hedendaagse wiskundige weliswaar taai, maar dankzij Huygens’ inventiviteit valt er meer dan genoeg te beleven. Jan Aarts heeft de mogelijkheid geschapen op avontuur te gaan door het magnum opus van Huygens: *Horologium Oscillatorium sive De Motu Pendulorum ad Horologio Aptato Demonstrationes Geometricae* (1673). Het is, zoals de titel al duidelijk maakt, Huygens ten voeten uit: een beschrijving van zijn slingeruurwerk plus de theorie van de slingerbeweging plus de onderliggende wiskunde. En dat alles grondiger dan strikt noodzakelijk voor de verantwoording van de centrale vondst, de tautochronie van de cycloïde: als de baan van een slinger een cycloïde is, is de periode onafhankelijk van de uitwijking.

Met een vertaling en af en toe bewerking van een groot deel van de oorspronkelijke tekst laat Jan Aarts zien hoe Huygens zijn betoog opbouwt en zijn bewijsvoering uitwerkt. De vertaling is hier en daar vrij, soms wat ongelukkig (waarom geweld in plaats van gewoon hol voor ‘cava’, p. 76). Keuzes die gemaakt worden voor selectie uit en aanpassingen van de oorspronkelijke tekst worden jammer genoeg niet verantwoord, daarvoor moet het origineel erbij gehaald worden. De lezer loopt daardoor de aanbiedingsbrief mis — aan Lodewijk XIV, midden in het rampjaar! — alsmede Huy-

gens’ inleidende woorden. Jammer is ook dat de originele figuren vervangen zijn door nieuwe, die weinig toevoegen en hier en daar zelfs afdoen aan de heldere lijn van Huygens’ diagrammen. Veel historische context krijgt de lezer er niet bij, bijvoorbeeld over de state of the art van midden-zeventiende-eeuwse wiskunde. Tot mijn verrassing blijft de grootste vondst van Huygens impliciet: het slingeruurwerk uit 1656, waarmee hij kans zag de regelmaat van de slinger te gebruiken om een klok te regelen. Op dezelfde manier ziet Aarts schijnbaar over het hoofd dat Huygens met zijn conische slinger in staat was een eerste nauwkeurige bepaling van g te maken, iets waarvan Newton dankbaar gebruik maakte. Daartegenover staat echter zijn aanstekelijke enthousiasme voor Huygens’ prestaties, dat uitnodigt om daadwerkelijk in de wiskunde van *Het Slingeruurwerk* te duiken. *Fokko Jan Dijksterhuis*



Michael Harris

Mathematics without Apologies
Portrait of a Problematic Vocation

Princeton University Press, 2015
xxii + 438 p., prijs \$29.95
ISBN 9780691154237

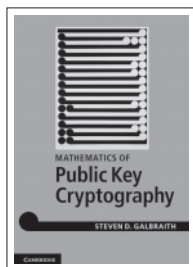
Het leek een intrigerend boek, de 21ste-eeuwse tegenhanger van Hardy’s klassieker, dat ik als student gelezen had en dus bood ik aan het boek te recenseren. Nadat het boek gearriveerd was, bladerde ik het door, las hier een alinea, daar een bladzijde en ik stuitte op zinnen als deze: “The Cole brothers’ use of citation indices to quantify visibility and influence is characteristic of the Mertonian school that dominates what, taking a hint from philosopher David Corfield, one might call the encyclopedic tendency in sociology of science. Corfield borrowed the term to adapt Alasdair MacIntyre’s tripartite division of ‘moral inquiry’ to the philosophy of mathematics.” Wat staat hier? En hoe vallen zinnen als deze (en het boek staat er vol van) te rijmen met de ambitie van de auteur om wiskunde uit te leggen aan “those whose lives are not necessarily bound up with mathematics”, wat toch het overgrote deel van de mensheid is? En draagt dit soort proza bij aan wat volgens de auteur het eigenlijke onderwerp van het boek is, namelijk “how it feels to live a mathematician’s double life: one life within this framework of professional autonomy, answerable only to our colleagues, and the other life in the wild at large.”

Het boek, kortom, staat vol met verwijzingen (en verwijzingen binnen verwijzingen) naar, uiteraard, wiskundigen, maar ook naar filosofen (Kant, Nietzsche, Lacan) en sociologen (Kuhn). Het effect is dat er bakken geleerdheid en belezenheid over de lezer worden uitgestort, die, althans voor deze recensent, maar niet willen bekijken. Verward ging ik op zoek naar andere recensies, in de hoop, ik geef het toe, lotgenoten te vinden, die net als ik moeite hadden de weg in dit labyrint te vinden. Een bloemlezing: “...his style is very different, favoring density, indirectness, the post or post-post modern”, “If math has mystics, Michael Harris is one”, “It is so boring! Uses a lot of pseudo sociological arguments”, “Perhaps the goal was to ramble, but I did not get it”, “Are you thinking to

become a mathematician? If you are, then this book is for you". Het is natuurlijk een teken van zwakte om in een recensie naar andere recensies te verwijzen, maar verdient een post-postmodern boek niet een dito bespreking?

De hoofdstukken van het boek laten zich lezen (als dat het goede woord is) als opzichzelfstaande essays en een grondiger recensie dan hier ruimte voor is, zou elk hoofdstuk afzonderlijk de revue laten passeren. In plaats daarvan een willekeurige greep: Hoofdstuk 4, getiteld 'Megaloprepeia' (!), is leesbaar. Het exploreert "the common border between mathematics and morality": hoe de wiskunde via de financiële wiskunde haar onschuld verloren heeft in de crash van 2008. Tegenstanders ("Finance is criminality") van financiële wiskunde en voorstanders komen aan het woord. Niets blijkt wat het lijkt te zijn: de wiskundige James Simons, die miljarden verdiende met 'high frequency trading', waarvan het sociale nut dubieus is, steunt via de Simons Foundation beurzen, conferenties en wetenschappelijke instituten in een 'exponentially virtuous circle': wiskunde-instituten brengen superrijken voort, die op hun beurt de zuivere wiskunde in stand houden. Hoofdstuk 5 ("Bonus Chapter 5"), getiteld 'An Automorphic Reading of Thomas Pynchon's *Against the Day*' was voor mij onleesbaar, maar ik moet bekennen, dat ik *Against the Day* niet gelezen heb. Hoofdstuk 8, 'The Science of Tricks', begint met de onthulling "I am a trickster", verwijzend naar 'Harris's tensor product trick' en onderzoekt de status van 'tricks' in de wiskunde. De auteur betreft ook de verhouding van wiskundigen tot muziek in zijn beschouwingen en poneert, dat tricks in de wiskunde zich verhouden tot wiskunde als popmuziek tot klassieke muziek. Ten slotte een woord over de wiskunde, verspreid over een aantal hoofdstukken (genummerd α , β , $\beta.5$, γ en δ) en gezamenlijk getiteld 'How to Explain Number Theory at a Dinner Party'. De auteur begint met te bewijzen, dat de wortel uit 2 irrationaal is en voert de lezer via vergelijkingen (kegelsneden, Fermats 'two square theorem'), derdegraadsvergelijkingen (met als oplossingen de drie zusters Olga, Masha en Irina) en congruenties naar afsluitende beschouwingen over elliptische krommen: voor wiskundigen waarschijnlijk te weinig en voor niet-wiskundigen te veel. Samenvattend: een bizar boek, hier en daar ondoordringbaar als een oerwoud, maar ook met zo nu en dan een verrassend vergezicht. Betreden op eigen risico!

Arjen Sevenster



Steven D. Galbraith

Mathematics of Public Key Cryptography

Cambridge University Press, 2012

xiv + 615 p., prijs £44.99

ISBN 9781107013926

One of the key inventions of modern cryptography is public-key (or asymmetric) cryptography. In contrast to classical symmetric cryptography, in public-key cryptography two distinctly different keys are used for encrypting and for decrypting: a *public-key* that is known to all the users in the system is used for encrypting a message, and a *secret-key* that is known exclusively to the le-

gitimate receiver is needed for decrypting the obtained ciphertext. This is comparable to a padlock: everyone can lock it, but only the owner of the key can open it. This distinguishing feature is crucial in ad-hoc networks like the Internet, where it is not clear ahead of time who will want to communicate (securely) with whom. Also, public-key cryptography gives rise to electronic signatures for digitally approving messages, like contracts, in a nonrepudiative way.

It is no big surprise that it is possible to effectively garble a message when (part of) the garbling process is secret; who hasn't thought about simple schemes for secret communication as a kid? — of course, designing schemes that withstand sophisticated cryptanalytic attacks is a different league — but how is it possible to garble a message so that it becomes unreadable even for someone who *knows precisely* how it was garbled? This sounds almost contradictory. The answer is: thanks to mathematics.

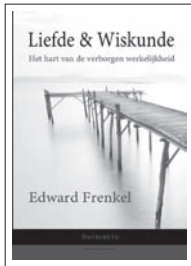
The book *Mathematics of Public Key Cryptography* by Steven D. Galbraith provides a broad and in-depth treatment of mathematical techniques that are related to and motivated by public-key cryptography. The basic ideas of public-key cryptography and simple schemes like RSA are of course easily explained; this book goes way beyond: it covers basic and advanced mathematical techniques that are essential for a deep understanding of public-key encryption (and signature) schemes and their security. This ranges from (hyper)elliptic curves to computing short vectors in lattices. The main topics of the book are: algebraic groups, factoring and discrete logarithms, and lattices — all with a focus on computational aspects and applications to cryptography — plus a discussion of various concrete (classes of) cryptographic schemes. Throughout, it is enlivened with historical remarks and anecdotes.

The book distinguishes itself from the typical cryptography textbook in that it has an opposite balance: it does the mathematics in-depth and very carefully, but keeps the cryptography rather simple (and sometimes a bit high-level). As such, it is very well suited for cryptographers that want to extend on their mathematical background and skills, or as a reference book, as well as for pure mathematicians that are interested in computational aspects and connections to cryptography. Also, with its many examples and exercises, it should serve well as basis for a course on, say, mathematical methods in cryptography.

The *Mathematics of Public Key Cryptography* is not meant to be read linearly, and this is a bit its weakness. I personally find: there is no continuous red line or natural focus — but this is maybe unavoidable given the intention of the book and its broadness. Altogether, I very much appreciate the rigorous and in-depth treatment of various aspects of public-key cryptography. Topics that are merely touched upon and/or explained in brief come along with plenty of pointers to the existing literature for further details. Certainly a book that stays in my shelf and should serve me well in the future.

Serge Fehr

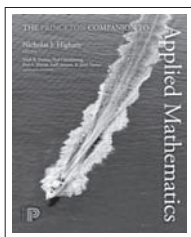
Recent verschenen publicaties. Als u een van deze boeken wilt bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.



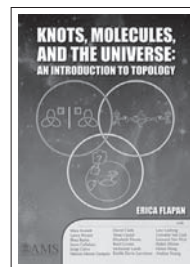
Edward Frenkel
Liefde & Wiskunde
 Uitgeverij Novencentio, 2015
 ISBN 9789491126048
novecentio-uitgeverij.nl/product/liefde-wiskunde



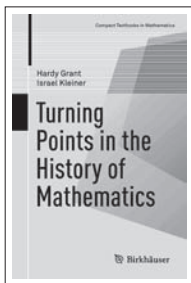
Dana Mackenzie, Barry Cipra
What's Happening in the Mathematical Sciences
 Volume 10
 American Mathematical Society, 2015
 ISBN 9781470422042
bookstore.ams.org/happening-10



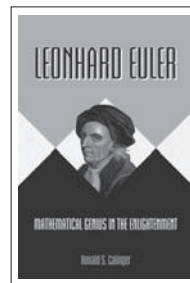
Nicholas J. Higham (ed.)
The Princeton Companion to Applied Mathematics
 Princeton University Press, 2015
 ISBN 9780691150390
press.princeton.edu/titles/10592.html



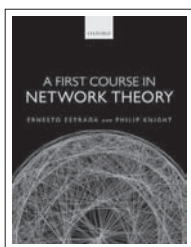
Erica Flapan
Knots, Molecules, and the Universe
 An Introduction to Topology
 American Mathematical Society, 2016
 ISBN 9781470425357
bookstore.ams.org/mkb-96



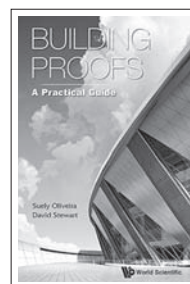
Hardy Grant, Israel Kleiner
Turning Points in the History of Mathematics
 Springer, 2016
 ISBN 9781493932634
www.springer.com/9781493932634



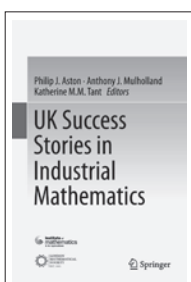
Ronald S. Calinger
Leonhard Euler
 Mathematical Genius in the Enlightenment
 Princeton University Press, 2015
 ISBN 9780691119274
press.princeton.edu/titles/10531.html



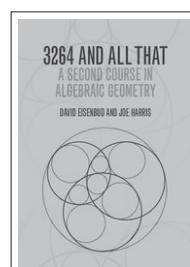
Ernesto Estrada, Philip Knight
A First Course in Network Theory
 Oxford University Press, 2015
 ISBN 9780198726463
global.oup.com/academic/product/a-first-course-in-network-theory-9780198726463



Suelly Oliveira, David Stewart
Building Proofs
 World Scientific, 2015
 ISBN 9789814641296
www.worldscientific.com/worldscibooks/10.1142/9418



Philip J. Aston, Anthony J. Mulholland, Katherine M.M. Tant (eds.)
UK Success Stories in Industrial Mathematics
 Springer, 2016
 ISBN 9783319254524
www.springer.com/9783319254524



David Eisenbud, Joe Harris
3264 and All That
 A Second Course in Algebraic Geometry
 Cambridge University Press, 2016
 ISBN 9781107602724
www.cambridge.org/9781107602724