

# 数理 eBook なび No.5 2019 年 10 月号



数理学の学生を、数理関係の電子情報へナビゲートするための

パンフレットです。 首都大学東京 理学部 数理学図書委員会

SpringerLink (<https://link.springer.com/>) は、Springer Nature 社が提供する、ジャーナル、ブックなどのデータベースです。電子ジャーナルは、全学契約があり、1500 誌以上を利用可能です。電子ブックは、Math. & Stat.分野について、2010 年から毎年少しずつ契約を拡げてきました。10/1 現在、【©1929-1989、2000-2018】を利用可能です。(©年号は、図書の Copyright Year) 今年度は、強く希望が寄せられていた【©2000-2004】を契約出来たことが、数理のニュースです！

“books” “Mathematics” など  
絞り込む方法があるが、データ量が多く、  
目的の結果にたどりつくことが難しいと  
感じる場合もある。

学内からのアクセス=赤紫色  
学外からのアクセス=オレンジ色  
→【学認】を利用すると、赤紫色に

## ※アイコンの説明

Include Preview-Only content

左記のチェックを外すと、契約のあるものだけに絞り込まれる。

Download book PDF

まるごと1冊ダウンロード



契約なし

例えば、シリーズ名 “Graduate Texts in Mathematics” で検索すると、シリーズの HP がヒットします。何冊の電子ブックがあり、その内、本文を読むことが出来るのは何冊でしょうか？ (ヒント:アイコンを利用) 図書を手に取って読む、電子ブックを読む、どちらも試してみませんか？

<注意> 電子情報は、著作権の範囲内での利用、個人の研究教育を目的とする利用に限ります。違反の場合は、大学全体にペナルティが課されて利用停止になりますので、ルールを守りご利用下さい。

推薦者: 黒田茂

著者: Cox,D.A., Little,J., O'Shea,D.

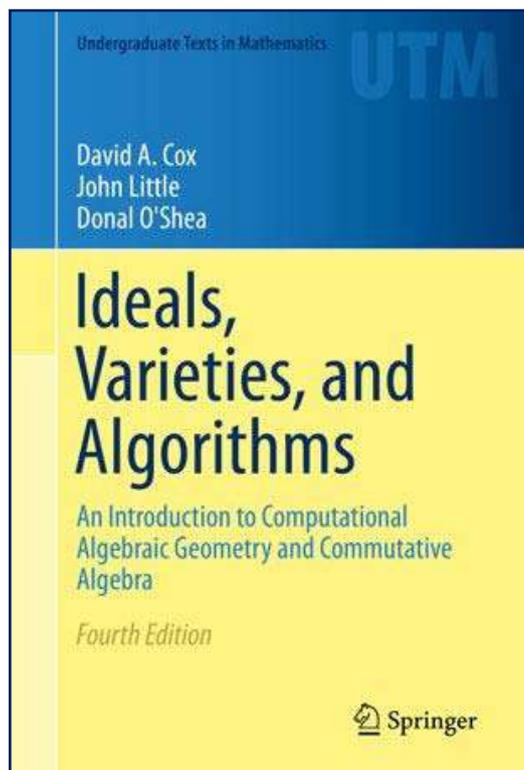
タイトル: Ideals, varieties, and algorithms : An introduction to computational algebraic geometry and commutative algebra, Fourth edition

出版社: Springer, c2015

(Undergraduate texts in mathematics)

Print ISBN : 9783319167206

Online ISBN : 9783319167213



シチジーだよ!  
全員集合

<図書>

配架場所: 数理科学図書室 洋 C

Cox,D.A.

請求番号: /414.5/C89i

資料 ID: 10004232148

<電子ブック>

<http://dx.doi.org/10.1007/978-3-319-16721-3>



推薦者: 澤野嘉宏

著者: Sawano, Y.

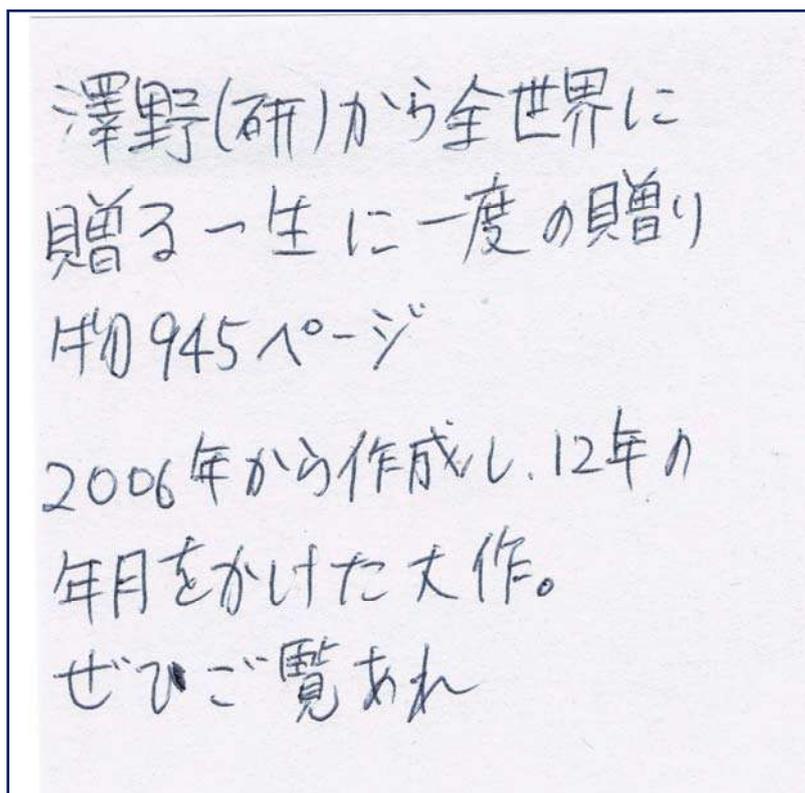
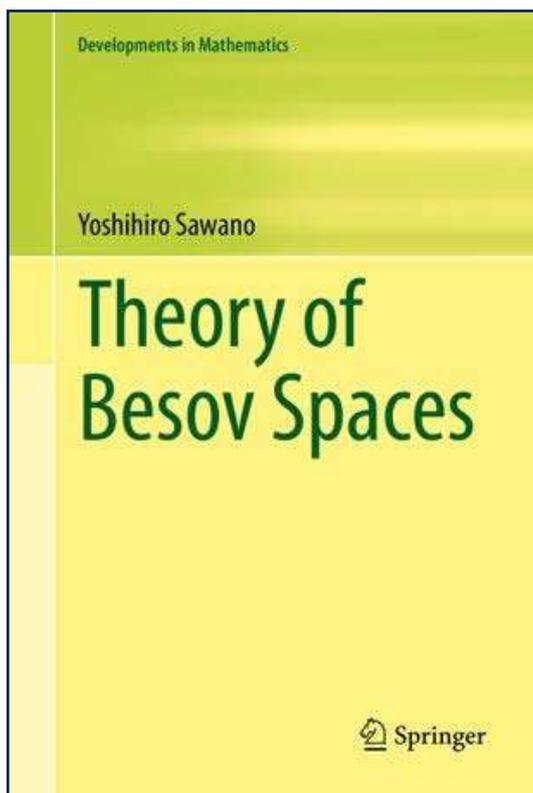
書名: Theory of Besov Spaces

出版社: Springer, 2018

(Developments in mathematics ; 56)

Print ISBN : 9789811308352

Online ISBN : 9789811308369



<図書>

配架場所: 数理科学図書室 洋 S

Sawano, Y.

請求番号: /415.5/Sa96t

資料 ID: 10005239134

<電子ブック>

<http://dx.doi.org/10.1007/978-981-13-0836-9>



推薦者: 鈴木登志雄

著者: Rautenberg, W.

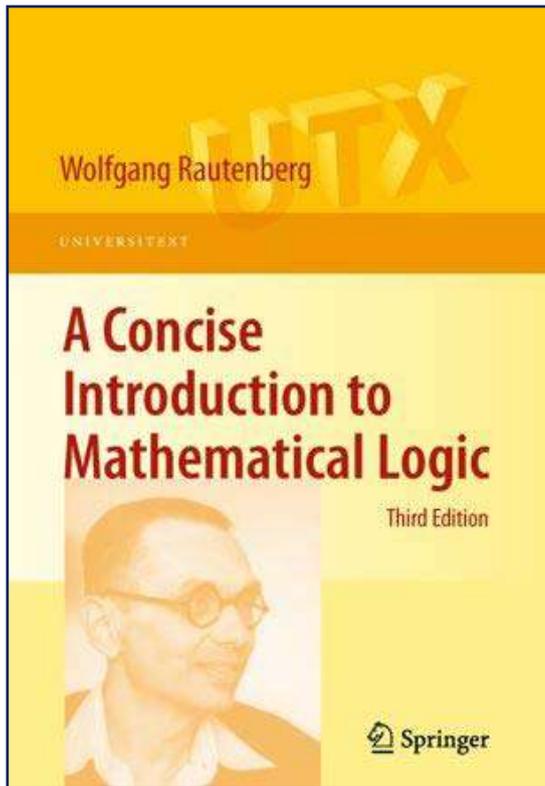
タイトル: A Concise Introduction to Mathematical Logic, Third edition

出版社: Springer, c2010

(Universitext)

Print ISBN : 9781441912206

Online ISBN : 9781441912213



数理論理学  
(数学基礎論)  
の総合的な入門書。  
穏やかで親切な  
語り口。4年生ゼミ  
のテキストとして使用中。

<図書>

配架場所: 数理科学図書室 洋 R

Rautenberg, W.

請求番号: /410.9/R18c

資料 ID: 10002383878

<電子ブック>

<http://dx.doi.org/10.1007/978-1-4419-1221-3>



推薦者: 深谷友宏

著者: Roe, J.

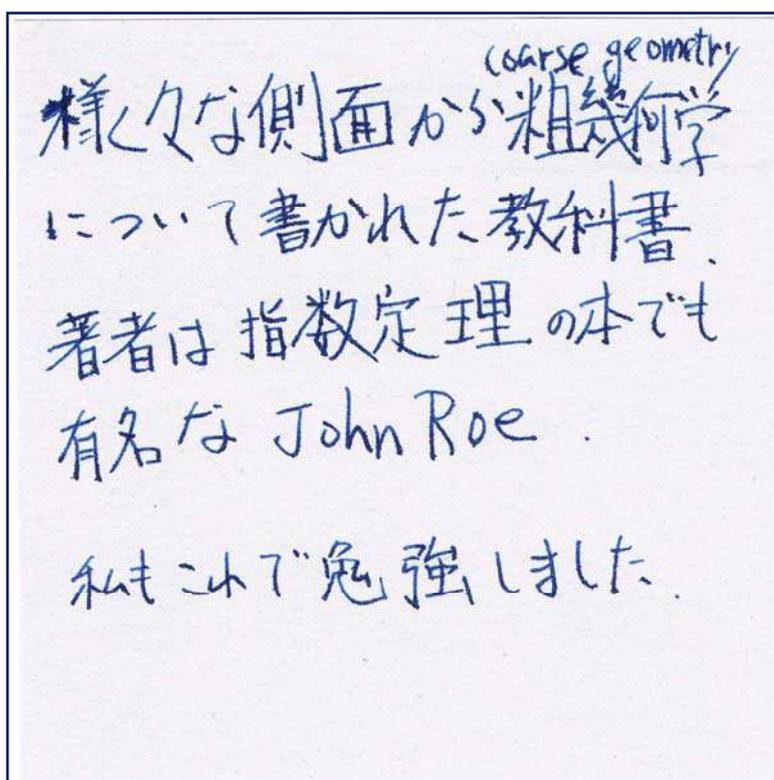
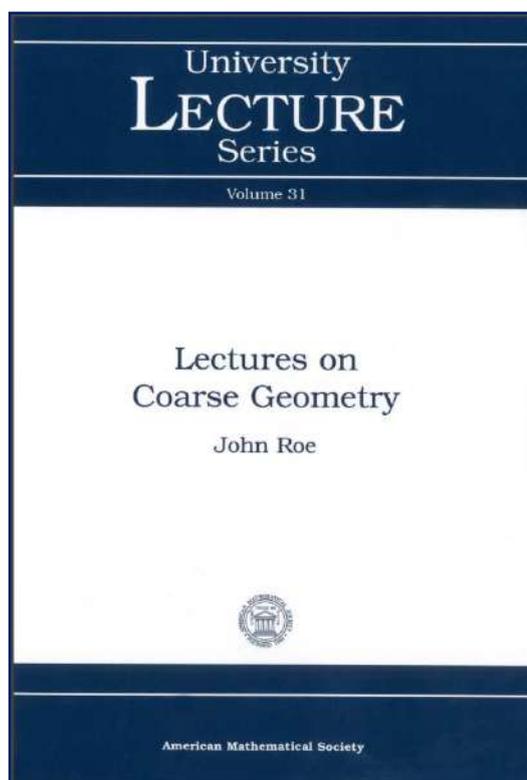
タイトル: Lectures on coarse geometry

出版社: AMS, c2003

(University lecture series ; 31)

Print ISBN : 9780821833322

Online ISBN : 9781470421762



<図書>

配架場所: 数理科学図書室 シリーズ

University Lecture Series 31

請求番号: /415.7/R611/2003

資料 ID: 008825559

<電子ブック>

<http://www.ams.org/books/ulect/031/>



推薦者:横田佳之

著者:Murakami,H. and Yokota,Y.

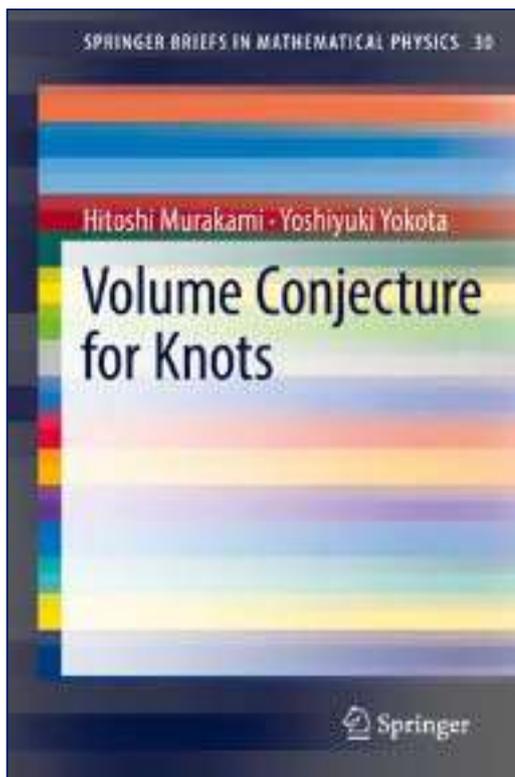
タイトル:Volume Conjecture for Knots

出版社:Springer, c2018

(Springer Briefs in Mathematical Physics ; 30)

Print ISBN : 9789811311499

Online ISBN : 9789811311505



サーストンが提唱した結び目の双曲幾何学と、  
ジョーンズやウィッテンが提唱した量子不変量  
の世界をつなぐ、話題の体積予想について、  
入門書を書いてしまいました。

不思議な図がたくさんあるので、眺めて頂けると  
幸いです。

<図書>

配架場所:数理科学図書室 洋 M

Murakami,H.

請求番号: /415.7/Mu43v

資料 ID: 10005214269

<電子ブック>

<http://dx.doi.org/10.1007/978-981-13-1150-5>



推薦者: 吉富和志

著者: Nicola, F. and Rodino, L.

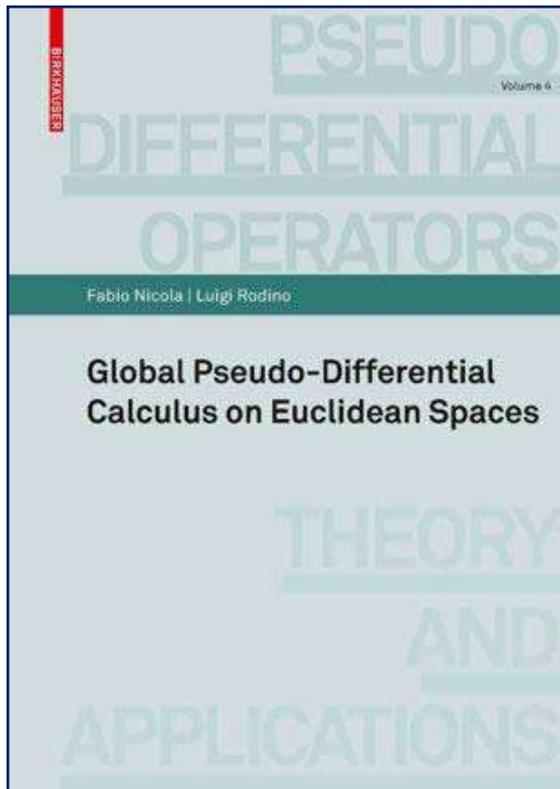
書名: Global Pseudo-differential calculus on Euclidean spaces

出版社: Birkhäuser, 2010

(Pseudo-differential operators : theory and applications ; 4)

Print ISBN : 9783764385118

Online ISBN : 9783764385125



擬微分作用素について丁寧  
に書かれた入門書です。最近  
の結果(例えば, 準楕円形  
作用素の複素巾についての, 第  
著者らによる2007年の結果)  
も扱われています。この図書は  
本年度後期の解析学特別  
講義Ⅲの教科書です。

10/1 現在、支払・登録手続き中

<図書>

配架場所: 数理科学図書室 洋N

Nicola, F.

請求番号: /413.6/N71g

資料ID:

<電子ブック>

<http://dx.doi.org/10.1007/978-3-7643-8512-5>





1970年代に起こった情報通信に関する研究における革命的な出来事の一つに、公開鍵暗号の概念の提案がある。ディフィーとヘルマンによる論文「New Directions in Cryptography」では、公開鍵暗号やデジタル署名等が提案されており、数千年とも考えられる暗号の歴史の中でも特筆すべきものである。勿論、これらの概念は突如として出てきたものではなく、1960年代に始まったアーパネット（インターネットの基になるもの）の研究等と無関係ではない。そもそも暗号技術は軍事や外交の道具であり、時には国家機密に属するもので歴史の表舞台に出てくることはなかった。一方、公開鍵暗号はインターネットのような技術的に盗聴などが可能で、安全でないネットワークをユーザーが安全に利用するために必要な技術として提案されたものであり、それまでの考え方とは全く異なるものである。公開鍵暗号の概念の提案以降、現代暗号とも呼ばれるこの分野には様々な研究分野から多くの研究者が参入し、現在でも国際的に活発に研究が行われている。ビットコインに代表される暗号資産やその中心的技術であるブロックチェーンも現代暗号の研究なくしては現れなかったと言っても過言ではない。

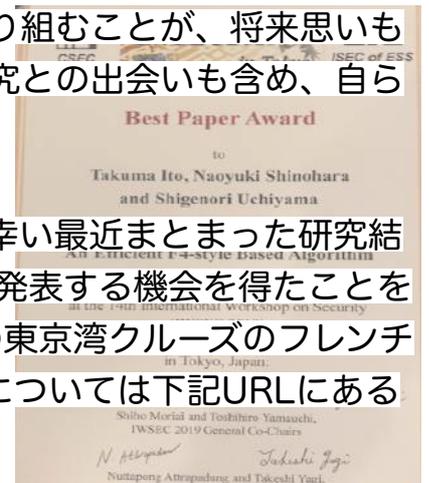
公開鍵暗号と数論の密接な関係については、RSA暗号等をご存知であればここに記すまでもないかもしれないが、公開鍵暗号の発明は暗号技術に対する我々の見方を変えただけでなく、同時に数論という純粋数学の一分野を国家機密をも担う応用数理へと変貌させてしまったとも言えよう。

学生時代に代数的整数論を専攻していた私は、偶然の出会いと縁あって学位取得後すぐにNTT研究所に入社し現代暗号の研究に携わって以来20年以上になる。職場を大学に移してからこの10年間ほどは、量子計算機と呼ばれる近未来型の計算機を用いた攻撃からも安全と期待されている公開鍵暗号方式の安全性評価の研究をこつこつとやっている。“Connecting the dots.” (点と点をつなげ) はスティーヴ・ジョブズの2005年のスタンフォード大学の卒業式でのスピーチにおける有名な言葉。何かの役に立つのか? 等考えずに、自らが興味あること、面白いと思うことに一生懸命取り組むことが、将来思いもよらないことに繋がるかもしれないという意味だが、暗号研究との出会いも含め、自らの狭い経験に基づいても大いに実感させられる。

そろそろ与えられた紙面も尽きてきたようなので、最後に、幸い最近まとまった研究結果が出て2019年8月末に開催された国際会議IWSEC2019で発表する機会を得たことを紹介して、この小文を終えたい。(IWSEC2019では2時間の東京湾クルーズのフレンチビュッフェのバンケットを楽しんだ。) 研究概要や関連情報については下記URLにある記事を参照頂きたい：

<https://www.tmu.ac.jp/news/topics/22145>

<https://www.tmu.ac.jp/news/topics/22325.html>



耐量子計算機暗号の安全性評価の世界記録達成 および

IWSEC2019 : Best Paper Award受賞 おめでとうございます！

