第15章

参考文献について

参考文献表はそれぞれの章末にありますが, 主なものを改めて紹介します.

代数幾何学の入門書

[岩澤] 岩澤 健吉, 代数函数論 増補版, 岩波書店, 1973.
[代幾] 秋月康夫・中井喜和・永田雅宜, 代数幾何学, 岩波書店
[複素代幾] 堀川 穎二, 複素代数幾何学, 岩波書店.
[デカ精] 飯高茂, 上野健爾, 浪川幸彦, デカルトの精神と代数幾何, 数学セミナー増刊「入門現代の数学」6, 日本評論社, 1980.
[代幾入門] 上野健爾, 代数幾何学入門, 岩波書店, 1997.
[A-C-G-H] E.Arbarello-M.Cornalba-P.A.Griffiths-J.Harris, *Geometry of Algebraic Curves Volume I,II*, Springer-Verlag, New York Inc, 1985
[G-H] P.Griffiths, J.Harris, Principles of Algebraic Geometry, John Wiley & Sons, Inc, 1978.
[Har] Algebraic Geometry, R. Hartshone, GTM 52, Springer, 1977.
[Matsu] H. Matsumura, Commutative ring theory, Cambridge, 1986.
[Red] D. Mumford, The Red Book of Varieties and Schemes, Springer LNM 1358, 1988.
[Sha] I. R. Shafarevich, Basic Algebraic Geometry 1, 2 2nd ed., Springer, 1994.
[Sie] Siegel, Topics in Complex Function Theory,

[岩澤] 名著です.
[デカ精] 代数幾何学の様々な話題を取り上げていて, 複素数体上の楕円曲線, Jacobi 多様体, それらの Moduli などにも触れられている.
[代幾入門] は, [デカ精] の簡易版といった感じです.
[代幾] [複素代幾] は, 標準的な教科書です.
[A-C-G-H] 代数曲線の事典のような本.
[G-H] Hodge 理論をもとに代数幾何学を展開しており, [デカ精] で省かれた証明も載っている.
[Har] は, [Sil1] でも頻繁に引用されていますが, Riemann-Roch の定理に辿り着くのにもかなりの時間がかかりますので, 他の本を先に読むのが賢明かと思います.
[Matsu] は [Har] にも引用の多い可換環論の代表的な教科書です.
[Sie] とにかく読んで.

楕円曲線に関する文献

[Ca1] J. W. S. Cassels, Lectures on Elliptic Curves, Student Texts 24, London Math. Soc., 1991.
[Ca2] J. W. S. Cassels, Diophantine Equations with Special Refernce to Elliptic Curves, J. London Math. Soc. 41 (1966), 193–291.
[Hu] D. Husemöller, Elliptic Curves, Springer GTM 111, 1986.
[Kn] A. Knapp, Elliptic curves, Mathematical notes **40**, Princeton Univ. Press, 1992.
[Mc-Mo] H. McKean and V. Moll, Elliptic Curves, Cambridge Univ. Press, 1997.

[Sil1] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer GTM 106, 1985.
[Sil2] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer GTM 151, 1994.
[S-T] J. H. Silverman and J. Tate, Rational Points of Elliptic Curves, Springer UTM, 1992.
[S-T-trans.] J. H. シルヴァーマン, J. テイト (足立恒雄, 小松啓一, 木田雅成, 田谷久雄訳) 「楕円曲線論入門」シュプリンガー, 1995.

[S-T] は, 具体例をもとに Mordel-Weil の定理などを紹介している.
[S-T-trans.] は, [S-T] の翻訳です.
[Sil1] は, 最もよく使われる教科書です. 1, 2 章の代数幾何の部分は大変ですが (ほとんど [Har] の引用), 3 章からはぐっと読み易くなります.
[Sil2] は, [Sil1] の付録に取り上げた話題を改めてまとめたものです.

[Ca1] [Ca2] [Kn] [Hu] [Mc-Mo] [Sil1] [Sil2] [S-T] については, 92 ページからの小川裕之氏による紹介も御参照下さい.

保型形式(モジュラー形式), モジュラー曲線に関する文献

[清水] 清水英男, 保型関数 I,II,III, 岩波基礎数学, 1977.
[土井-三宅] 土井 公二, 三宅 敏恒, 保型形式と整数論, 紀伊國屋数学叢書 7, 紀伊國屋書店, 1976.
[AG] G. Cornell, J. H. Silverman (ed.), "Arithmetic Geometry ", Springer-Verlag (1986)
[Ar] M. Artin, Néron Models, in [AG] 213-230 (1986)
[Antwerp] "Modular Functions of One Variable I-IV", LNM 320, 349, 350, 476 (1973-75)
[Bonn] "Modular Functions of One Variable V, VI", LNM 601, 627 (1977)
[Boston] G. Cornell, J. H. Silverman, G. Stevens (ed.), "Modular Forms and Fermat's Last Theorem ", Springer-Verlag (1997)
[BLR] S. Bosch, W. Lutkebohmert, M. Raynaud, "Néron Models", Springer-Verlag (1990)
[CMS] V. Kumar Murty (ed.), "Seminar on Fermat's Last Theorem", CMS Conference Proceedinds vol. 17, AMS (1995)
[Coh] H. Cohen, A Course in Computational Algebraic Number Teory, Springer, 1996.
[Cre] J. E. Cremona, Algorithms for Modular Elliptic Curves 2nd. Ed, Cambridge,
[D-I] F. Diamond and J. Im, Modular forms and modular curves, in [CMS] 39-133 (1995)
[Mi] T. Miyake, *Modular Forms* , Springer-Verlag, New York, 1989.
[D-R] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, in *Modular Functions of One Variable II*, Springer Lecture Notes in Mathematics 349 (1973), 143-316.
[Hecke] E. Hecke, "Mathematische Werke ", Vandenhoeck & Ruprecht (1970)
[K-M] Katz, N., Mazur, B., Arithmetic moduli of elliptic curves, Ann. of Math. Studies 108, Princeton Univ. Press, (1985)
[La] S. Lang, Elliptic Functions, 2nd ed., Springer GTM 112, 1987.
[Maz] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. IHES 47, 33-186 (1977)
[Mum] Mumford, D., The Picard groups of the moduli problem, in *Arithmetic Algebraic Geometry*, ed. O.F.G.Schilling, Harper & Row, 1965.
[Ray] M. Raynaud, Schémas en groupes de type $(p, \cdots, p)$, Bull. Soc. Math. France 102, 241-280 (1974)
[Roh] D. E. Rohrlich: Modular Curves, Hecke Correspondences, and L- Functions, in [Boston] 41-100 (1997)
[Se] Serre, J.P., Cours d'Arithmétique, Presses Universitaires de France, 1970. (英語版, A Cource in Arithmetic, GTM 7, Springer-Verlag, 1970; 日本語訳, 数論講義, 彌永健一訳, 岩波書店, 1979.)
[Sh] G. Shimura: "Introduction to the arithmetic theory of automorphic functions", Iwanami Shoten-Princeton Univ. Press (1971)
[Tate] J. Tate, Finite Flat Group Schemes, in [Boston] 121-154 (1997)

Hecke 全集 [Hecke] は聖典ですが，今では読む人はあまりいません．
[Se] は，モジュラー形式（あるいは整数論）の入門として，よく読まれています．
[Sh] は，モジュラー形式，モジュラー曲線についての基本的な文献です．
[土井-三宅] は，幾何学的な記述が少ないことを除けば，非常に便利です．
[Mi] は，[土井-三宅] の翻訳．
[清水] も，同様の本ですが，解析的なことも詳しい．
[Roh] は，非常に読みやすい解説です．他に [D-I] も参照のこと．
[Antwerp], [Bonn] には，個々の話題についての（少し古いが）多くの論文，解説が集められています．
[D-R] には，モジュラー曲線の現代的な理論が書かれていますが，決して読みやすいとはいえません．(青木氏の解説も参照のこと．)
[K-M] は，第 12 章を御覧下さい．
[Maz] は，その後の研究の基礎となった論文で，現代の整数論（数論幾何）を学ぶ上で非常に有益です．そこでは，finite group scheme の理論（とくに Raynaud [Ray]）が不可欠です．これに関しては，例えば [AG] [Tate] に解説があります．
Néron model については，[BLR] が標準的で，M. Artin の解説 [Ar] もあります．
[Coh] 数論用ソフト PARI-GP に実装される algorithm の解説がなされている．楕円曲線のために割かれた章もある．
[Cre] $\mathbf{Q}$ 上の modular な楕円曲線の data が豊富に収められている．その data を計算するための方法も解説されている．

暗号理論に関する文献

[池野-小山] 池野信一, 小山謙二, 現代暗号理論, 電子情報通信学会, 1986.
[辻井-笠原] 辻井重男, 笠原正雄, 暗号と情報セキュリティ, 昭晃堂, 1990.
[岡本] 岡本栄二, 暗号理論入門, 共立出版, 1993.
[岡本-太田] 岡本龍明, 太田和夫編, 暗号・ゼロ知識証明・数論, 共立出版, 1995.
[辻井] 辻井重男暗号-ポストモダンの情報セキュリティ, 講談社
[岡本-山本] 岡本龍明, 山本博資, 現代暗号, 産業図書, 1997
[Sal] Arto Salomaa, Public key cryptography, Springer-Verlag.
[Men1] A. J. Menezes, Elliptic Curve Public Key Cryptosystems Kluwer Academic Publishers, 1993.
[Kob] Koblitz, Introduction to number theory and cryptography, GTM. 2nd ed., Springer.
[Sti] Stinson (桜井訳), 暗号理論の基礎, 共立出版, 1996.
[Sch] Schneier, Applied cryptography, 2nd ed., John Wiley & Sons, 1996.
[Men2] Menezes, Oorschot, Vanstone, Handbook of applied cryptography, CRC Press, 1996.

暗号理論の本はとりあえず，上記の本を挙げておきます．

編集後記

第6回整数論サマースクールの準備を始めてから、はや一年。ようやく報告集出版の運びとなりました。

もし、この報告集を読みやすいと感じて頂けたのなら、それは記法を合わせ、文書のスタイルを統一したなどという些末な理由では全くなく、私以外の講演者の力量に他なりません。講演者の方々には、あらためて御礼申し上げます。

最後に、この報告集がどなたかの研究の一助になりましたら、関係者一同、甚だ幸いに存じます。

1998 年 12 月 16 日

志村 真帆呂 (早稲田大学・理工)