

La Théorie Algorithmique des Nombres

Exposé Quatrième:
Primalité et Factorisation

Conférence:	École de Recherche CIMPA UNESCO Maroc
Sujet:	Théorie des Nombres et ses Applications
Place:	Université Mohammed Premier, Faculté des Sciences (FSO)
Venue:	Oujda, Region Oriental, Maroc
Date:	Jeudi, Mai 28, 2015
Temps:	10:15 – 11:15, a.m.
Auteur:	Daniel C. Mayer (Autriche)

Our Top-Recent Trilogy.

- [T1] D.C. Mayer,
Periodic bifurcations in
descendant trees of finite p -groups,
Adv. Pure Math., **5** (2015), no. 4, 162–195,
Special Issue on Group Theory.
- [T2] D.C. Mayer,
Index- p abelianization data of
 p -class tower groups,
Adv. Pure Math., **5** (2015), no. 5, 286–313,
Special Issue on Number Theory
and Cryptography.
(29th Journées Arithmétiques 2015,
University of Debrecen, Hungary, Jul. 2015.)
- [T3] D.C. Mayer,
Periodic sequences of p -class tower groups,
J. Appl. Math. Phys.
(International Conference on
Groups and Algebras 2015,
Shanghai, Jul. 2015.)

Our Most Recent Presentations.

- [P1] D.C. Mayer and M.F. Newman,
*Finite 3-groups
as viewed from class field theory*,
Groups St Andrews 2013,
Univ. of St Andrews, Fife, Scotland, Aug. 2013.
- [P2] D.C. Mayer, M.R. Bush, and M.F. Newman,
3-class field towers of exact length 3,
18th ÖMG Congress and
123rd Annual DMV Meeting 2013,
Univ. of Innsbruck, Tyrol, Austria, Sep. 2013.
- [P3] D.C. Mayer, M.R. Bush, and M.F. Newman,
*Class towers and capitulation
over quadratic fields*,
West Coast Number Theory 2013,
Asilomar Conference Center, Pacific Grove,
Monterey, California, USA, Dec. 2013.

Our Modern Tetralogy.

- [MT1] D.C. Mayer,
The second p -class group of a number field,
Int. J. Number Theory **8** (2012),
no. 2, 471–505.
- [MT2] D.C. Mayer,
Transfers of metabelian p -groups,
Monatsh. Math. **166** (2012),
no. 3–4, 467–495.
- [MT3] D.C. Mayer,
Principalization algorithm
via class group structure,
J. Théor. Nombres Bordeaux **26** (2014),
no. 2, 415–464.
- [MT4] D.C. Mayer,
The distribution of second p -class groups
on coclass graphs,
J. Théor. Nombres Bordeaux **25** (2013),
no. 2, 401–456.
(27th Journées Arithmétiques 2011,
Faculty of Mathematics and Informatics,
University of Vilnius, Lithuania, Jul. 2011.)

Our Classical Tetralogy.

- [CT1] D.C. Mayer,
Lattice minima and units
in real quadratic number fields,
Publ. Math. Debrecen **39** (1991),
no. 1–2, 19–86.
- [CT2] D.C. Mayer,
Multiplicities of dihedral discriminants,
Math. Comp. **58** (1992),
no. 198, 831–847 and S55–S58.
(Westcoast Number Theory Conference 1990,
Asilomar Conference Grounds, Pacific Grove,
Monterey, California, USA, Dec. 1990).
- [CT3] D.C. Mayer,
Discriminants of metacyclic fields,
Canad. Math. Bull. **36** (1) (1993), 103–107.
- [CT4] D.C. Mayer,
Quadratic p -ring spaces
for counting dihedral fields,
Int. J. Number Theory **10** (2014),
no. 8, 2205–2242.

References.

- [1] H. Cohen,
A course in computational algebraic number theory,
Graduate texts in mathematics **138**,
Springer, 1996.
- [2] H. Cohen,
Advanced topics in computational number theory,
Graduate texts in mathematics **193**,
Springer, 2000.
- [3] M. Pohst and H. Zassenhaus,
Algorithmic algebraic number theory,
Encyclopedia of mathematics and its applications,
Cambridge University Press, 1990.
- [4] S.S. Wagstaff, Jr.,
The Joy of Factoring,
Student Mathematical Library (STML), Vol. **68**,
American Mathematical Society (AMS), 2013.

Information Technology.

- [1] The GAP Group,
*GAP – Groups, Algorithms, and Programming —
a System for Computational Discrete Algebra*,
Version 4.7.7,
Aachen, Braunschweig, Fort Collins, St. Andrews, 2015,
(<http://www.gap-system.org>).
- [2] The MAGMA Group,
MAGMA Computational Algebra System, Version 2.21-3,
Sydney, 2015,
(<http://magma.maths.usyd.edu.au>).
- [3] Oracle,
JDK 7u80, Java SE, and NetBeans, Version 8.0.2,
Redwood City, CA, 2015,
(<http://www.oracle.com>).
- [4] The PARI Group,
PARI/GP, Version 2.7.3,
Bordeaux, 2015,
(<http://pari.math.u-bordeaux.fr>).

Further References.

- [1] E. Artin, Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, *Abh. Math. Sem. Univ. Hamburg* **7** (1929), 46–51.
- [2] J.R. Brink, *The class field tower for imaginary quadratic number fields of type (3, 3)* (Dissertation, Ohio State University, 1984).
- [3] J.R. Brink and R. Gold, Class field towers of imaginary quadratic fields, *manuscripta math.* **57** (1987), 425–450.
- [4] G. Frei, P. Roquette, and F. Lemmermeyer, *Emil Artin and Helmut Hasse. Their Correspondence 1923–1934*, Universitätsverlag Göttingen, 2008.
- [5] F.-P. Heider und B. Schmithals, Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen, *J. Reine Angew. Math.* **336** (1982), 1–25.
- [6] H. Kisilevsky, Number fields with class number congruent to 4 mod 8 and Hilbert’s theorem 94, *J. Number Theory* **8** (1976), 271–279.
- [7] D.C. Mayer, Principalization in complex S_3 -fields, *Congressus Numerantium* **80** (1991), 73–87.
(Proceedings of the 20th Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, Canada, Sep. 1990).
- [8] A. Scholz und O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm, *J. Reine Angew. Math.* **171** (1934), 19–41.
- [9] I.R. Shafarevich, Extensions with prescribed ramification points, *Publ. Math., Inst. Hautes Études Sci.* **18** (1963), 71–95 (Russian). English transl. by J.W.S. Cassels: *Am. Math. Soc. Transl.*, II. Ser., **59** (1966), 128–149.
- [10] O. Taussky, A remark concerning Hilbert’s Theorem 94, *J. Reine Angew. Math.* **239/240** (1970), 435–438.