Corps et polynômes

relatively new schemes like XTR and NTRU. — A series of very recent results about certain important characteristics (period, distribution, linear complexity) of several commonly used pseudorandom number generators, such as the RSA generator, Blum-Blum-Shub generator, Naor-Reingold generator, inversive generator, and others. — One of the principal tools is bounds of exponential sums, which are combined with other number theoretic methods such as lattice reduction and sieving. — A number of open problems of different levels of difficulty and proposals for further research. — An extensive and up-to-date bibliography.

Corps et polynômes

Toma ALBU. — **Cogalois theory.** — Pure and applied mathematics, vol. 252. — Un vol. relié, 15,5×23,5, de XII, 341 p. — ISBN 0-8247-0949-7. — Prix: US$ 150.00. — Marcel Dekker, New York, 2003.

This volume offers a systematic, comprehensive investigation of field extensions, finite or not, that possess a cogalois correspondence. The subject, called cogalois theory, is somewhat dual to the very classical Galois theory dealing with field extensions possessing a Galois correspondence. — *Contents:* Finite cogalois theory: Preliminaries. Kneser extensions. Cogalois extensions. Strongly Kneser extensions. Galois G-cogalois extensions. Radical extensions and crossed homomorphisms. Examples of G-cogalois extensions. G-cogalois extensions and primitive elements. Applications to algebraic number fields. Connections with graded algebras and Hopf algebras. — Infinite cogalois theory: Infinite Kneser extensions. Infinite G-cogalois extensions. Infinite Kummer theory. Infinite Galois theory and Pontryagin duality. Infinite Galois G-cogalois extensions.

Christian U. JENSEN, Arne LEDET, Noriko YUI. — **Generic polynomials: constructive aspects of the inverse Galois problem.** — Mathematical Science Research Institute publications, vol. 45. — Un vol. relié, 16×24, de IX, 258 p. — ISBN 0-521-81998-9. — Prix: £45.00. — Cambridge University Press, Cambridge, 2002.

This book describes a constructive approach to the inverse Galois problem: Given a finite group G and a field K, determine whether there exists a Galois extension of K whose Galois group is isomorphic to G. Further, if there is such a Galois extension, find an explicit polynomial over K whose Galois group is the prescribed group G. The main theme of the book is an exposition of a family of "generic" polynomials for certain finite groups, which give all Galois extensions having the required group as their Galois group. The existence of such generic polynomials is discussed, and where they do exist, a detailed treatment of their construction is given. The book also introduces the notion of "generic dimension" to address the problem of the smallest number of parameters required by a generic polynomial.

Teo MORA. — **Solving polynomial equation systems I: the Kronecker-Duval philosophy.** — Encyclopedia of mathematics and its applications, vol. 88. — Un vol. relié, 16×24, de XIII, 423 p. — ISBN 0-521-81154-6. — Prix: £60.00. — Cambridge University Press, Cambridge, 2003.

Polynomial equations have been long studied, both theoretically and with a view to solving them. Until recently, manual computation was the only solution method and the theory was developed to accommodate it. With the advent of computers, the situation changed dramatically. Many classical results can be more usefully recast within a different framework

which in turn lends itself to further theoretical development tuned to computation. This first book in a trilogy is devoted to the new approach. It is a handbook covering the classical theory of finding roots of a univariate polynomial, emphasising computational aspects, especially the representation and manipulation of algebraic numbers, enlarged by more recent representations like the Duval Model and the Thom Codification. Mora aims to show that solving a polynomial equation really means finding algorithms that help one manipulate roots rather than simply computing them; to that end he also surveys algorithms for factorizing univariate polynomials.

Géométrie algébrique

David M. GOLDSCHMIDT. — **Algebraic functions and projective curves.** — Graduate texts in mathematics, vol. 215. — Un vol. relié, 16×24, de XVI, 179 p. — ISBN 0-387-95432-5. — Prix : €44.95. — Springer, New York, 2002.

This book provides a self-contained exposition of the theory of algebraic curves without requiring any of the prerequisites of modern algebraic geometry. The self-contained treatment makes this important and mathematically central subject accessible to non specialists. At the same time, specialists in the field may be interested to discover several unusual topics. Among these are Tate's theory of residues, higher derivatives and Weierstrass points in characteristic p, the Stohr-Voloch proof of the Riemann hypothesis, and a treatment of inseparable residue field extensions. Although the exposition is based on the theory of function fields in one variable, the book is unusual in that it also covers projective curves, including singularities and a section on plane curves.

Claire VOISIN. — **Hodge theory and complex algebraic geometry, vol. 1.** — Cambridge studies in advanced mathematics, vol. 76. — Un vol. relié, 15,5×23,5, de IX, 322 p. — ISBN 0-521-80260-1. — Prix : £55.00. — Cambridge University Press, Cambridge, 2002.

This first volume provides a modern introduction to Kählerian geometry and Hodge theory. It starts with basic material on complex variables, complex manifolds, holomorphic vector bundles, sheaves, and cohomology theory, the latter being treated in more theoretical way than is usual in geometry, and culminates with the Hodge decomposition theorem. In between, the author proves the Kähler identities, which leads to the hard Lefschetz theorem and the Hodge index theorem. The second part of the book investigates the meaning of these results in several directions. It introduces the notion of Hodge structure, the (logarithmic) de Rham complex, Frölicher spectral sequences, and mixed Hodge structures. The book ends with a treatment of deformations of the complex structure, Gauss-Manin connection, and variations of Hodge structure, on the one hand, and the study of algebraic cycles on the other. These topics will be further developed in the next volume.

Anneaux et algèbres

Ivan CHAJDA, Günther EIGENTHALER, Helmut LÄNGER. — **Congruence classes in universal algebra.** — Research and exposition in mathematics, vol. 26. — Un vol. broché, 17×24, de X, 217 p. — ISBN 3-88538-226-1. — Prix : €28.00. — Heldermann Verlag, Lemgo, Germany, 2003.

Congruence relations play an important role when investigating universal algebras. On the one hand, the structure of the congruence lattice of a given algebra reveals much information on