Review of the book

Algebraic Number Theory, second edition

by Richard A. Mollin

CRC Press, Taylor & Frances Group 2011

ISBN: 978-1-4398-4598-1

Fan Junjie, Bertrand
National University of Singapore

29 November 2011

1 Overview of Book

This is the second edition of an introductory text in algebraic number theory written by a well-known leader in algebra and number theory. This new edition is completely reorganized and rewritten from the first edition. Suitable for advanced undergraduates and beginning graduate students in mathematics, this text offers a good introduction to the fundamentals of algebraic number theory. But unlike standard texts of this level, this text also touches on some applications of algebraic number theory, such as its use in the number field sieve algorithm as well as in primality testing. Numerous extensive biographical sketches of relevant mathematicians are also scattered throughout the book.

2 Book Summary

The first chapter is a standard and mostly algebraic introduction to integral domains, ideals and unique factorization. It also covers standard material on Noetherian and principal ideal domains as well as Dedekind domains. It ends by introducing algebraic numbers and number fields, with an emphasis on quadratic fields. The background material for this chapter can be found in Appendix A: Abstract Algebra, which the reader may use to recall some concepts and notations. The reader would note that some of the exercises involve material from later parts of the book. For example, in exercise 1.27 on page 19, the notation for the norm of an element of the number field is used, but it is only defined on page 65 in chapter 2.

Chapter 2 covers field extensions. It starts with standard material on automorphims and fixed points, cumulating in the proof of the fundamental theorem of galois theory. It continues with material on norms and traces on algebraic number fields, integral bases of the ring of integers of a number field and the discriminant of Q-bases of a number field. Stickelberger's theorem is then proved, followed by a brief section on norms of ideals and discriminants.

Chapter 3 covers material on class groups. It starts off with material about binary quadratic forms. It then delves into ideals and composition of forms, Dirichlet composition, and proving theorems about ideal class groups and class numbers of forms. The third section talks about Minkowski's geometry of numbers which is used to prove the finiteness of the ideal class group as well as Hermite's theorem on discriminants. The next section covers standard material on units in number rings, which cumulates in the proof of Dirichlet's unit theorem.

Chapter 4 explains some applications of the above material to the solutions of some Diophantine equations and to integer factorization algorithms, something which not many books of this level have. It starts off with some brief discussions on prime power representation, before covering unique factorization in certain quadratic domains in order to find the solutions of some Bachet equations. The next section proves in detail special cases of Fermat's last theorem, such as the case when the exponent is 3 and when it is a regular prime. This section also covers Bernoulli numbers and polynomials and their relations to the Riemann Zeta function. The last 2 sections talk in some detail about some integer factorization algorithms such as the quadratic sieve algorithm, Pollard's algorithm and finally the number field sieve algorithm.

Chapter 5 extends the ideal decomposition concepts developed for quadratic fields in chapter 1 to arbitrary number fields. The chapter starts with a discussion on ramification, inertia and decomposition numbers as well as relative norms and traces of elements of a number field. These cumulate in a theorem about the norms of ideals generated by norms of elements. The next section discusses the relations between the dual basis, the different and the discriminant of an extension of number fields. This discussion cumulates in the fundamental theorem of the different. Ramified and unramified extensions of number fields are then covered, leading to the prime factorization theorem in cyclotomic extensions. Using Galois theory concepts developed in chapter 2, Galois and Kummer extensions are then explained leading towards class field theory and the Kronecker-Weber theorem. This theorem, together with concepts related to Artin symbols, are used in Lenstra's primality test, which is described in some detail at the close of this chapter.

The final chapter covers higher reciprocity laws, extensions of Gauss' classical quadratic reciprocity laws. The chapter begins with a detailed discussion of cubic reciprocity laws, leading to its proof and that of a theorem on prime representation and cubic residuacity. The next section proves in detail a range of results, including the biquadratic reciprocity law, a theorem connecting quartic reciprocity and prime representation as well as Burde's rational quartic reciprocity law. Finally, the Stickelberger relation is discussed in some detail, leading to the proof of the Eisenstein reciprocity law, which generalizes the laws covered in the chapter.

3 Reviewer's Comments

This book offers a good self-contained coverage of algebraic number theory. The reader following the book would have attained a comprehensive view of the basics of algebraic number theory. To this reviewer's knowledge, another book with a similar coverage is Marcus' 'Number Fields'. These books allow the student to transition from the more introductory books, such as Alaca and William's 'Introductory Algebraic Number Theory' and Stewart and Tall's 'Algebraic Number Theory and Fermat's Last Theorem', to the more advanced texts, the likes of Neukrich's 'Algebraic Number Theory' and Lang's 'GTM: Algebraic Number Theory'.

While most material in this book are concise and come with detailed proofs, the reader may want to supplement his reading by browsing the more introductory texts listed above should he find parts of the text challenging. Doing the exercises also reinforces the reader's understanding of the material covered. A plus point about this text is that solutions to odd-numbered exercises are sketched at the back of the book, so that the interested reader can be helped along quickly in better understanding concepts in the text.

There are a few misspellings in the text, and as mentioned in the summary for chapter 1 above, some exercises there require concepts introduced only later in the text. But these are minor inconveniences which should not deter the motivated reader. The use of biological sketches of relevant mathematicians sprinkled throughout the text is also a plus point. It breathes more life into the mathematics by talking about the people who did most of the important mathematics which became the basic and foundational material of today.

4 Reviewer's Recommendation

I recommend this book to advanced undergraduates and beginning graduate students interested in algebraic number theory and wishing to read more advanced texts on this topic, but he should be ready to supplement his reading with more elementary texts should he find certain parts challenging.

The reviewer is a math graduate student at the National University of Singapore