

BOOK REVIEW

Algorithmic algebraic number theory, by M. Pohst and H. Zassenhaus. Cambridge University Press, Cambridge, 1989, pp. 465, \$89.50. ISBN 0-521-33060-2

Suppose that $f \in \mathbf{Q}[T]$ is a polynomial with rational coefficients. If f is irreducible, then the quotient ring $\mathbf{Q}[T]/(f(T))$ is a *number field*, i.e., it is a finite extension of \mathbf{Q} . Conversely, it is well known that every number field can be obtained in this way. Multiplying $f(T)$ or T by a rational number if necessary, we may and do assume that $f(T)$ is, in fact, a monic irreducible polynomial with integral coefficients.

The basic arithmetical invariants of the number field $F = \mathbf{Q}[T]/(f(T))$ are its ring of integers, the unit group of this ring, and its ideal class group. Another important invariant, perhaps algebraic rather than arithmetic, is the Galois group G of f or, more precisely, the Galois group of a normal closure of F over \mathbf{Q} . The group G is a transitive subgroup of the group of permutations of the roots of f .

In a first course in algebraic number theory it is usually first proved that the ring of integers, i.e., the integral closure R of \mathbf{Z} in F , is a Dedekind ring. This ring is not, in general, a principal ideal ring or even a unique factorization domain. Next, one introduces the *ideal class group* $\text{Cl}(R)$ of R ; this is the group of fractional R -ideals modulo the subgroup of principal fractional ideals. By means of Minkowski's techniques of geometry of numbers, one shows that $\text{Cl}(R)$ is a finite abelian group. The class group is trivial precisely when R is a principal ideal ring or, what boils down to the same thing, a unique factorization domain. Finally, it is shown that the unit group R^* is finitely generated. This last theorem is due to Dirichlet and is usually proved by applying Minkowski's results to a lattice that one obtains by taking logarithms of the absolute values of the units in R^* .

The question arises, given the polynomial f , how to *compute* the Galois group G , the ring of integers R , its class group $\text{Cl}(R)$, and the unit group R^* . Moreover, this question can be asked in a variety of ways. For instance, can these invariants be computed *in principle*? They can. Most textbooks do not even discuss this fundamental question. Wanting more, one could ask for *efficient* algorithms to calculate the invariants. This question can be studied asymptotically, i.e., for the parameters of the polynomial f such as the degree and the size of its coefficients, tending to infinity. This is Lenstra's point of view in his recent paper in this *Bulletin* [2]. The question can also be considered from a more *practical* point of view: one is interested in algorithms that can actually be programmed on a computer and that give answers in a "reasonable" amount of time for polynomials f of a "reasonable" size. This is the point of view of the authors of the book under consideration.

The book under review is a six-chapter course in algebraic number theory with special attention for the computational aspects. Chapter 1 provides an introduction. The authors introduce their often original and usually rather cumbersome notation and conventions. They insist, for instance, in also dealing with rings without a multiplicative unit element 1. The usual rings are here called “unital”. The decision is motivated by pointing out that most ideals are rings without 1, while ideals are, of course, just modules that happen to be contained in the ring itself. In this chapter the authors also discuss, in a somewhat mysterious way, one of the foundational principles of their subject:

The “permanence principle” as established by Peacock and his British contemporaries implies that any number system should satisfy the axioms of a commutative ring. In general terms the task of constructive algebra assumes the following form. Let a commutative ring R be given in such a way that for any two of its elements a, b

- (i) there is a clearcut answer whether a is equal to b ($a = b$) or whether a, b are distinct ($a \neq b$);
- (ii) there are elements $a + b, a - b, ab$ of R explicitly known (viz. sum, difference, product of a, b) such that the axioms of a commutative ring are satisfied.

Then we say that the commutative ring R is given constructively. For example, the rational integer ring Z as introduced in customary high school mathematics is constructively given.

In Chapter 2 the authors prove the main results of Galois theory and explain how to compute the Galois group of a given polynomial. A useful list of transitive permutation groups of degree ≤ 12 , together with the relevant invariant polynomials, is given at the end of the book.

Many of the objects considered in algebraic number theory, such as rings of integers, ideals, and the unit groups modulo torsion, have, in a natural way, the structure of *lattices*; i.e., they can be viewed as free abelian groups that span vector spaces equipped with a scalar product. For computational purposes it is important to have good algorithms to do calculations in lattices available; these are discussed in Chapter 3, which deals with the geometry of numbers. It includes a discussion of Minkowski’s convex body theorem and the more recent algorithm due to Lenstra, Lenstra, and Lovász to find a “good” basis for a given lattice.

The ring $\mathbf{Z}[T]/(f(T))$ is contained in the ring of integers of $F = \mathbf{Q}[T]/(f(T))$. Its index in the ring of integers R is finite. In Chapter 4 methods to compute R starting from $\mathbf{Z}[T]/(f(T))$ are described. Dirichlet’s Unit Theorem is proved in Chapter 5. The proudly announced “logarithm free” proof appears to be the usual proof with the exponential function applied to it. Finally, the class group is discussed in Chapter 6. In this chapter we also find the often-repeated and probably untrue story in which Dirichlet pointed out a mistake in a proof by Kummer of Fermat’s Last Theorem. See Edwards’s text [1] for a more reliable account.

Needless to say, the last two chapters contain descriptions of algorithms to compute unit groups and class groups respectively. The book ends with a series of tables of number fields of low degree and small discriminant together with their rings of integers, unit groups, and class groups. Curiously, the complex quadratic

fields are omitted.

REFERENCES

- [1] H. M. Edwards, *Fermat's last theorem, a genetic introduction to algebraic number theory*, Graduate Texts in Math., vol. 50, Springer-Verlag, Berlin, Heidelberg, and New York, 1977.
- [2] H. W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211–244.

RENÉ SCHOOF
UNIVERSITÀ DI TRENTO
E-mail address: SCHOOF@ITNVAX.CINECA.IT