On Lattices over Number Fields

C. Fieker and M. E. Pohst

Technische Universität Berlin, Sekr. MA 8-1, FB 3 Mathematik
Straße des 17. Juni 136, D–10623 Berlin, F.R.G.
fieker@ and pohst@math.tu-berlin.de

1 Introduction

A large number of algorithms used for computations in number fields $\mathcal{E}$ over $\mathbb{Q}$ make use of the fact that there is a canonical embedding of $\mathcal{E}$ into $\mathbb{R}^n$ under which $o_\mathcal{E}$ becomes a lattice. Using this, it is possible to utilize the powerful tools of the geometry of numbers to obtain existence theorems that often can be turned into efficient algorithms.

Although it is well known that there is a generalization of the geometry of numbers to lattices over Dedekind domains (e.g. see [8], [14], [2] and [16]) there does not exist a constructive approach.

Here we present a generalization of perhaps the two most important algorithms in this context: the enumeration algorithm of Fincke and Pohst (see [6] or [13]) and the LLL–algorithm for basis reduction due to Lenstra, Lenstra and Lovács (see [11]).

References

1. Bosma, W.; Pohst, M. E.; *Computations with Finitely generated Modules over Dedekind Domains*; Proceedings ISSAC'91 (1991), 151 – 156
2. Chalk, J. H. H.; *Algebraic Lattices*; C. R. Math. Rep. Acad. Sci. Canada, Vol. II (1980)
3. Cohen, H.; *A Course in Computational Algebraic Number Theory*; Graduate Texts in Math., Vol. 138, Springer-Verlag, 1993
4. Cohen, H.; *Hermite and Smith Normal Form Algorithms over Dedekind Domains*; to appear in Math. Comp.
5. Fieker, C.; Jurk, A.; Pohst, M. E.; *On solving relative norm equations in algebraic number fields*; to appear in Math. Comp.
6. Fincke, U.; Pohst, M. E.; *Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis*; Math. Comp. 44 (1985), 463–471
7. Fincke, U.; *Ein Ellipsoidverfahren zur Lösung von Normgleichungen*; Thesis, Düsseldorf 1984
8. Humbert, P.; *Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini*; Commentarii Mathematici Helvetici, Vol. 12 (1939-1940), 263–306
9. Jurk, A.; *Über die Berechnung von Lösungen relativer Normgleichungen in algebraischen Zahlkörpern*; Thesis, Düsseldorf 1993
10. KANT group; *KANT V4*; to appear in J. Symb. Comput.
11. Lenstra, A. K.; Lenstra, H. W.; Lovász, L; *Factoring Polynomials with Rational Coefficients* Math. Ann. 261 (1982), 515–534
12. O'Meara, O. T.; *Introduction to Quadratic Forms*; Grundlehren der Mathematischen Wissenschaften, Vol. 117, Springer-Verlag 1963

13. Pohst, M. E.; Zassenhaus, H.; *Algorithmic Algebraic Number Theory*; Cambridge Univ. Press 1989
14. Rogers, K.; Swinnerton-Dyer, H. P. F.; *The Geometry of Numbers over Algebraic Number Fields*; Trans. AMS, Vol. 88 (1958), 227–242
15. Tschernikow, S.N.; *Lineare Ungleichungen*; Hochschulbücher für Mathematik, Vol. 69, Deutscher Verlag der Wissenschaften, Berlin 1971
16. Weyl, H.; *Theory of Reduction for Arithmetical Equivalence*; Trans. AMS, Vol. 48 (1940), 126–164 and Vol. 51 (1942), 203–231