Algorithms for finite rings – Abstract

In this thesis we are interested in describing algorithms that answer questions arising in ring and module theory. Our focus is on deterministic polynomial-time algorithms and rings and modules that are finite.

The first three chapters prepare the ground for the rest of the text by introducing the underlying ring and module theory, and providing a compendium of algorithms that allow us to perform basic computations with finite abelian groups and finite rings.

The first main result of this thesis concerns the module isomorphism problem: we describe two distinct algorithms that, given a finite ring R and two finite R-modules M and N, determine whether M and N are isomorphic. If they are, the algorithms exhibit such an isomorphism.

In addition, we show how to compute a set of generators of minimal cardinality for a given module, and how to construct projective covers and injective hulls. We also describe tests for module simplicity, projectivity, and injectivity, and constructive tests for existence of surjective module homomorphisms between two finite modules, one of which is projective. As a negative result, we show that the problem of testing for existence of injective module homomorphisms between two finite modules, one of which is projective, is NP-complete.

The last part of the thesis is concerned with finding a good working approximation of the Jacobson radical of a finite ring, that is, a two-sided nilpotent ideal such that the corresponding quotient ring is "almost" semisimple. The notion we use to approximate semisimplicity is that of *separability*.