Decompositions in algebra

Gent, D.M.H. van

Summary

In this thesis entitled "*Decompositions in algebra*" we study decompositions of abelian groups equipped with several algebraic structures, and relevant algorithms.

In Chapter 1 we consider flows in undirected graphs of which the values, in contrast to the classical theory, live in not necessarily abelian groups. For abelian flows it is the case, that if for all vertices of the graph with at most one exception *Kirchhoff's law of conservation* holds, which states that the incoming flow equals the outgoing flow, then the exceptional vertex also satisfies this law. We prove the surprising result that graphs for which this implication also holds for each non-abelian flow are precisely the *planar graphs*. We also construct from a given group a decomposition into its maximal abelian subgroups, in terms of which we can decide algorithmically whether this group satisfies the conservation law for all graphs.

In Chapter 2 we generalize the theory of lattices to infinite dimension, on which the next chapter relies. Where classically a lattice forms a discrete subgroup of a Euclidean vector space, we consider discrete subgroups of Hilbert spaces, which we call *Hilbert lattices*. We prove that every Hilbert lattice has a maximal orthogonal decomposition into sublattices, and to that end study the *indecomposable vectors*. The indecomposables derive their existence from the *Voronoi polyhedron*, for which we show that it is a fundamental domain. Countable Hilbert lattices turn out to be free abelian groups. It is an open problem whether this holds generally.

In Chapter 3 we consider the integral closure of the integers in an algebraic closure of the field of rational numbers, called the *ring of algebraic integers*, equipped with the natural Hilbert lattice structure known from the theory of the geometry of numbers. We attempt to compute invariants of this lattice. In particular, we give lower and upper bounds on the *covering radius*. From this we derive a partial solution to the algorithmic counter-

part of this problem, namely the *closest vector problem.* As a test for such algorithms we propose the computation of indecomposable vectors of given degree. It turns out to be hard to compute all indecomposables of degree three, even though the number of candidates is limited, because the terms of a decomposition can have an arbitrarily large degree. For the same reason it is not even clear whether indecomposability is decidable. It is also unknown whether the lattice has isometries other than the isometries that come from the ring structure.

In Chapter 4 we decompose rings into *gradings*, a construction that generalizes the degree of a monomial in a polynomial ring. We prove that the lattice structure of the ring of algebraic integers and its subrings gives rise to the existence of a *universal grading* of such rings, and we determine their structure in several special cases. In particular, the maximal orthogonal decomposition, and hence also the universal grading, of the lattice of algebraic integers is trivial. Separate from a lattice structure, a universal grading exists under certain p-adic assumptions, and in extension to this we show that *roots of unity* and *idempotents* are 'monomials'. Furthermore, we give an algorithm to quickly compute the universal grading of rings that are additively generated by their roots of unity and idempotents.

In Chapter 5 we apply the theory of the previous chapter to the special case of *group rings.* It turns out that also for group rings over reduced orders a certain universality is satisfied: up to isomorphism there is a unique maximal way to decompose such a ring as a group ring. In terms of this we describe its automorphism group. Very surprisingly it turns out that in the connected case the subrings and subgroups that can be used to form a maximal decomposition can be chosen entirely independently. We prove this by applying the theory of modules, in particular decompositions of finite length modules, to a morphism of finite abelian groups, namely the *degree map* restricted to the group of roots of unity.

In Chapter 6 we give an efficient algorithm to take *roots of fractional ideals* in orders in number fields. We are careful in formulating this algorithm so that the output is sufficiently functorial. Here it is an obstruction that roots need not exist or be unique. We find an application of taking roots in a generalization of the coprime basis algorithm. This algorithm finds for a set of positive integers a set of pairwise coprime integers, called a *coprime basis*, where every number from the first set is a (unique) power product of numbers from the second. This power product can be seen as the best polynomial-time approximation of the prime factorization. However, it is possible to improve the coprime basis by taking roots of its elements. When we generalize the coprime basis algorithm to ideals in orders, we are able to also there make this final improvement.