Computer-assisted exploration of Gröbner bases theory in Theorema

Alexander Maletzky
RISC, Johannes Kepler University Linz, Austria

In this talk we give an overview of the formal, computer-supported exploration of the theory of Gröbner bases [1] in the mathematical assistant system Theorema 2.0 [2] we carried out in the frame of our studies. Gröbner bases play a central role in many areas of symbolic computation, as they allow to effectively solve a whole range of non-trivial ideal-theoretic problems.

The core component of our formal treatment are so-called reduction rings, introduced by Buchberger more than 30 years ago. Reduction rings generalize the original setting of Gröbner bases in polynomial rings over fields to a much wider class of algebraic structures, namely essentially commutative rings with multiplicative identity and a couple of further functions and relations, satisfying a handful of non-trivial axioms. We represented the central aspects of this theory in Theorema and proved all results correct using the automated- and interactive proving facilities of the system. Moreover, we also implemented Buchberger's algorithm for actually computing Gröbner bases in a completely generic and directly executable manner and proved it totally correct. In addition, we even formalized the analysis of the complexity of the algorithm in a very special setting, namely in bivariate polynomial rings over fields, following a pencil-and-paper elaboration carried out by Buchberger in the early 1980s. The result of all this is now available as a collection of 16 Theorema theories, consisting in total of roughly 2240 formulas, that may serve as the basis for future theory explorations in Theorema; this, in particular, holds for eight theories exclusively dealing with elementary mathematical concepts that are themselves absolutely independent of Gröbner bases, reduction rings and Buchberger's algorithm.

Although the mathematical theories we formalized are by no means novel, we nevertheless managed to contribute to them as well, by (drastically) simplifying one proof, generalizing various definitions and results, and, most importantly, correcting a subtle error in the theory of reduction rings related to the notion of *irrelativity* introduced in [3]. These improvements definitely give evidence to the claim that mathematics profits from being treated formally in software systems and hence constitutes another motivation for our work in particular and for computer-assisted theory exploration in general.

This research was funded by the Austrian Science Fund (FWF): grant no. W1214-N15, project DK1.

[1] B. Buchberger, An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal, PhD thesis, University of Innsbruck, Austria (1965).

[2] B. Buchberger, T. Jebelean, T. Kutsia, A. Maletzky, W. Windsteiger, Theorema 2.0: Computer-Assisted Natural-Style Mathematics, *J. Formalized Reasoning* **9**(1) (2016), 149–185.

[3] S. Stifter, A Generalization of Reduction Rings, *J. Symb. Comp.* **4**(3) (1988), 351–364.