

# Computer Algebra

Lecture Notes

Johannes Kepler Universität Linz  
Wintersemester 2017/18

Prof. Franz Winkler  
Institut für Symbolisches Rechnen  
(RISC)

# Contents

References	
1. What is Computer Algebra ?	1
2. Gröbner Bases	5
2.1. Introduction	5
2.2. Gröbner bases at Work	9
2.3. The notion of a Gröbner basis	13
2.4. Solving ideal problems by Gröbner bases	27
3. Greatest common divisors of polynomials	43
3.1 Gröbner bases and GCDs	43
3.2 A modular GCD algorithm	49
3.3 Squarefree factorization	55
4. Resultants	57
5. Factorization	65
5.1. Factorization over finite fields	65
5.2. Factorization over the integers	69
5.3. Factorization over algebraic extension fields	75
6. Appendix: Arithmetic in basic domains	79

The material in these lecture notes is largely taken from

F. Winkler, “Polynomial Algorithms in Computer Algebra”, Springer-Verlag Wien  
New York (1996)

where also proofs of the theorems can be found.

## References

- [AdL94] W.W. Adams, P. Lounstaunau, *An Introduction to Gröbner Bases*, Amer. Math. Soc., Graduate Studies in Math., vol.3 (1994)
- [BeW93] T. Becker, V. Weispfenning, *Gröbner Bases — A Computational Approach to Commutative Algebra*, Springer (1993)
- [BCL83] B. Buchberger, G.E. Collins, R. Loos, *Computer Algebra — Symbolic and Algebraic Computation (2nd ed.)*, Springer (1983)
- [BuW98] B. Buchberger, F. Winkler, *Gröbner Bases and Applications*, Cambridge Univ. Press, London Math. Soc. Lecture Notes 251 (1998)
- [Coh93] A.M. Cohen, *Computer Algebra in Industry*, Wiley (1993)
- [CGL95] A.M. Cohen, L. van Gastel, S.V. Lunel, *Computer Algebra in Industry 2*, Wiley (1995)
- [CLO97] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms (2nd ed.)*, Springer (1997)
- [GaG99] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge Univ. Press (1999)
- [GCL92] K.O. Geddes, S.R. Czapor, G. Labahn, *Algorithms for Computer Algebra*, Kluwer Acad. Publ. (1992)
- [GKW03] J. Grabmeier, E. Kaltofen, V. Weispfenning, *Handbook of Computer Algebra: Foundation, Applications, Systems*, Springer (2003)
- [Gro68] W. Gröbner, *Algebraische Geometrie I*, BI Hochschultaschenbücher
- [Gro70] W. Gröbner, *Algebraische Geometrie II*, BI Hochschultaschenbücher
- [Mis93] B. Mishra, *Algorithmic Algebra*, Springer (1993)
- [SWP08] J.R. Sendra, F. Winkler, S. Pérez-Díaz, *Rational Algebraic Curves — A Computer Algebra Approach*, Springer (2008)
- [vdW70] B.L. van der Waerden, *Algebra I, II*, Springer (1991)
- [Win96] F. Winkler, *Polynomial Algorithms in Computer Algebra*, Springer (1996)