Übungsblatt 1:
Aufgabe 1

a) [Lün79]: Lüneburg: Galoisfelder etc., Hilfssatz 2.4.

b) [Lün79]: Lüneburg: Galoisfelder etc., Satz 2.1.

c) [Lün79]: Lüneburg: Galoisfelder etc., Satz 3.4.

d) [Lün79]: Lüneburg: Galoisfelder etc., Satz 3.8.

Aufgabe 2

- [vzGG99] Von zur Gathen: MCA, Algorithm 2.5
- [Win96] Winkler: Polynomial Algorithms, Theorems 2.2.1, 2.2.2, 2.2.3.

Aufgabe 3

- [Sch91] Scheid: Zahlentheorie (2. A.), Abschnitt IV.1, Satz 1, Beispiel 1.

Aufgabe 4

a) [vzGG99] Von zur Gathen: MCA, Ex. 3.14 (iv).

b) [BS] Bach: Algorithmic Number Theory I, Section 4.7 und Ex. 4.24 (Loesung im Anhang).

Übungsblatt 2:
Aufgabe 1

a) [BS] Bach: Algorithmic Number Theory I, Ex. 4.4.

b) [GCL92] Geddes et al., Theorem 2.6.

c) [BS] Bach: Algorithmic Number Theory I, Ex. 4.13.

Aufgabe 2

a) [Knu81] Knuth: TAOCP 2, pp. 270-272.

b) [Knu81] Knuth: TAOCP, Ex. 4.3.1.22.

Aufgabe 3

a) Nein, z.B. $\mathbb{Z}^2$, da $(0,1) * (1,0) = (0,0)$, d.h. $(0,1)! = (0,0)$ ist Nullteiler.

b) Trivial, s. Aufgabe 1.1.d). Restklasse wird durch den Divisionsrest durch x-5 beschrieben.

Aufgabe 4

a) [GCL92] Geddes et al., Theorem 2.11.(ii).

b) [GCL92] Geddes et al., Definition 3.4 und Skript. Definition von Aequivalenz und Vereinfachungs-Ordnung instanzieren. Begriff 'Grad' präzisieren etc.

Übungsblatt 3:
Aufgabe 1

- [Knu81] Knuth: TAOCP 2, pp. 465-468.

Aufgabe 2

a) [BS] Bach: Algorithmic Number Theory I, Section 5.4, pp. 103-104.

b) [BS] Bach: Algorithmic Number Theory I, Ex. 5.5 (Lösung im Anhang).

Aufgabe 3

- Man bemühe ein CAS.

Aufgabe 4

- Siehe Vorlesungsordner.

Übungsblatt 4:
Aufgabe 1

- [Win96] Winkler: Polynomial Algorithms, Lemma 4.1.2 ff.
- [Pet99] Pethoe: Algebraische Algorithen, Abschnitt 6.7.

Aufgabe 2

- [Bro] Bronstein: Symbolic Integration I, Section 1.3, pp. 14 ff.

Aufgabe 3

- [BS] Bach: Algorithmic Number Theory I, Ex. 5.41 (Loesung im Anhang).

Aufgabe 4

a) [Win96] Winkler: Polynomial Algorithms, Section 2.2.
[vzGG99] Von zur Gathen: MCA, Section 8.1.

b) [vzGG99] Von zur Gathen: MCA, Lemma 8.2 und Theorem 8.3.

c) [vzGG99] Von zur Gathen: MCA, Ex. 8.6.

Übungsblatt 5:
Aufgabe 1

- [Knu81] Knuth: TAOCP 2, Ex. 4.3.2.11.

Aufgabe 2

a) [Knu81] Horner-Schema, etwa Knuth: TAOCP 2, Section 4.6.4, p. 486.

[BCS97] Auch interessant: Bürgisser/Clausen/Shokrollahi: Algebraic Complexity Theory, Section 5.1, insbes. Theorem 5.6.

b) [Knu81] Knuth: TAOCP 2, Ex. 4.6.4.3.

Aufgabe 3

a) SS 1997, Aufgabe 2.3.a).

b) SS 1997, Aufgabe 2.3.b).

Aufgabe 4

a)-e) SS 1997, Aufgabe 2.4.

Übungsblatt 6:
Aufgabe 1

a) [Win96] Winkler: Polynomial Algorithms, Ex. 3.1.5 und Theorem 3.1.2 plus Corollary.

b) [Win96] Winkler: Polynomial Algorithms, Ex. 3.1.6 und Theorem 3.1.4.

Aufgabe 2

a)-c) SS 1997, Aufgabe 6.4.
[Knu81] Siehe auch Knuth: TAOCP 2, Section 4.3.2, pp. 288-290 und Ex. 4.3.2.7.

Aufgabe 3

- SS 1997, Aufgabe 7.2.

Aufgabe 4

a) SS 1997, Aufgabe 6.2.b).

b) SS 1997, Aufgabe 6.3.a).

c) SS 1997, Aufgabe 6.3.b).

d) SS 1997, Aufgabe 6.3.c).

e) SS 1997, Aufgabe 6.3.d).

f) SS 1997, Aufgabe 6.3.e).

Übungsblatt 7:
Aufgabe 1

- [vzGG99] Von zur Gathen: MCA, Theorem 9.4.
- [vzGG99] Von zur Gathen: MCA, Ex. 9.6.
- [vzGG99] Von zur Gathen: MCA, Ex. 9.10.

Aufgabe 2

- [vzGG99] Von zur Gathen: MCA, Theorem 9.27.

Aufgabe 3

- SS 1997, Aufgabe 7.4.

Aufgabe 4

- [GCL92] Geddes et al., Section 7.6.

Übungsblatt 8:
Aufgabe 1

- Je nach Fassung: SS 1997, Aufgabe 7.3 oder
  [vzGG99] Von zur Gathen: MCA, Algorithm 15.10 und Theorem 15.11.

Aufgabe 2

- Rechenübung.

Aufgabe 3

a) [vzGG99] Von zur Gathen: MCA, Theorem 6.31.

b) [vzGG99] Von zur Gathen: MCA, Theorem 6.32.

c) [vzGG99] Von zur Gathen: MCA, Corollary 6.33.

Aufgabe 4

- [Zip93] Zippel: Effective Polynomial Computation, Section 21.1 (Ende).

Übungsblatt 9:
Aufgabe 1

a,b) [vzGG99] Von zur Gathen: MCA, Ex. 14.23.

Aufgabe 2

- SS 1997, Aufgabe 10.2.

Aufgabe 3

- SS 1997, Aufgabe 9.3.
  Siehe auch [Win96] Winkler: Polynomial Algorithms, Ex. 5.2.3.

Aufgabe 4

- [Knu81] Knuth: TAOCP 2, Section 4.6.2, insbesondere pp. 441-442 (und dort B4).
- [PZ89] Pohst/Zassenhaus: Algorithmic Algebraic Number Theory, pp. 83 unten bis 85, insbesondere p. 85.
- [Poh93] Pohst: Computational Algebraic Number Theory, pp. 7-8 (insbes. 8 Mitte).

Aufgabe 5

a)-c) [BS] Bach: Algorithmic Number theory I, Ex. 7.36.

Übungsblatt 10:
Aufgabe 1

- [BS] Bach: Algorithmic Number Theory I, Ex. 7.17.

Aufgabe 2

a) [vzGG99] Von zur Gathen: MCA, Lemma 14.46.

b) [vzGG99] Von zur Gathen: MCA, p. 389 oben.

c) [vzGG99] Von zur Gathen: MCA, Lemma 14.47 und Ex. 14.45.

d) [vzGG99] Von zur Gathen: MCA, Algorithm 14.48 und Theorem 14.49.
Zusatzfrage: Folgt aus [vzGG99] von zur Gathen: MCA, Lemma 14.47 oder direkt nach [Lün79] Lüneburg: Galoisfelder etc., Satz 11.1.c).

Aufgabe 3

a) [Win96] Winkler: Polynomial Algorithms, p. 121.
[vzGG99] Von zur Gathen: MCA, Ex. 16.16.(i).

b) [Win96] Winkler: Polynomial Algorithms, Lemma 5.2.4.

c) [Win96] Winkler: Polynomial Algorithms, p. 122.
[vzGG99] Von zur Gathen: MCA, Ex. 16.16.(ii) und (iii).

d) Rechenaufgabe, [vzGG99] von zur Gathen: MCA, Ex. 16.16.(iv).

Übungsblatt 11:
Aufgabe 1

a) [Win96] Winkler, Polynomial Algorithms, Lemma 8.2.3.a.

b) [BW93] Becker/Weispfenning: Gröbner Bases, Lemma 5.17.

Aufgabe 2

a) [Win96] Winkler: Polynomial Algorithms, Lemma 8.2.5.d und Ex. 8.2.2 (Lösung im Anhang).

b) [Win96] Winkler: Polynomial Algorithms, Theorem 8.2.6 und Ex. 8.2.3 (Lösung im Anhang).
[BW93] Becker/Weispfenning: Gröbner Bases, Lemma 5.26.

Aufgabe 3

- [Win96] Winkler: Polynomial Algorithms, Aufgabe 8.4.4.

Aufgabe 4

a) [Win96] Winkler: Polynomial Algorithms, Theorem 8.4.9.c.
[CLO97] Cox/Little/O'Shea: Ideals, Varieties, and Algorithms, Theorem 4.3.11.
Siehe auch [BW93] Becker/Weispfenning: Gröbner Bases, pp. 259-260.
Siehe auch [Mis93] Mishra: Algorithmic Algebra, Section 3.7.4.

b) [Win96] Winkler: Polynomial Algorithms, Theorem 8.4.9.d.
[CLO97] Cox/Little/O'Shea: Ideals, Varieties, and Algorithms, Proposition 4.4.10.(3) und (5).
Siehe auch [BW93] Becker/Weispfenning: Gröbner Bases, pp. 264-269.
Siehe auch [Mis93] Mishra: Algorithmic Algebra, Section 3.7.5.

- [CLO97] Cox/Little/O'Shea: Ideals, Varieties, and Algorithms: Bemerkungen auf p. 187 und p. 195.

Literatur

[BCS97] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory.* Springer, 1997.

[Bro] Manuel Bronstein. *Symbolic integration.* Springer, ??

[BS] Eric Bach and Jeffrey Shallit. *Algorithmic number theory.* Cambridge, Mass. : MIT Press, ??

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases: a computational approach to commutative algebra.* Springer, 1993.

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra.* Springer, 1997.

[GCL92] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for computer algebra.* Kluwer Acad. Publ., 1992.

[Knu81] Donald E. Knuth. *The art of computer programming 2.* Addison-Wesley, 1981.

[Lün79] Heinz Lüneburg. *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen.* Bibliogr. Inst., 1979.

[Mis93] Bhubaneswar Mishra. *Algorithmic algebra.* Springer, 1993.

[Pet99] Attila Pethö. *Algebraische Algorithmen.* Vieweg, 1999.

[Poh93] Michael E. Pohst. *Computational algebraic number theory.* Birkhäuser, 1993.

[PZ89] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory.* Cambridge Univ. Pr., 1989.

[Sch91] Harald Scheid. *Zahlentheorie.* BI-Wiss.-Verl., 1991.

[vzGG99] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra.* Cambridge University Press, 1999.

[Win96] Franz Winkler. *Polynomial algorithms in computer algebra.* Springer, 1996.

[Zip93] Richard Zippel. *Effective polynomial computation.* Kluwer Academic, 1993.