Computeralgebra mit Gröbnerbasen
SoSe 2011
Schmale
Stand 1. Juli 2011

Inhaltsübersicht
(wird entsprechend dem Verlauf der Veranstaltung aktualisiert)

I Einleitung
Was verstehe ich unter Computeralgebra (CA) ?
Ansätze zu einer Gliederung der der CA, Problembereiche, Anwendungen, Hinweise.

II Beispiele und Hinweise zur Arithmetik
- **§ 1** Multiplikation von großen natürlichen Zahlen und von Polynomen, DFT
- **§ 2** Multiplikation großer Matrizen
- **§ 3** Division mit Rest, modulare Arithmetik, sog. chinesischer Restsatz
- **§ 4** ggT-Berechnungen, modularer Ansatz für $\mathbb{Z}[x]$, Resultante

III Faktorzerlegung von Polynomen mit rationalen Koeffizienten und in einer Variablen
- **§ 5** **(a)** Es geht in endlich vielen Schritten
  (b) Es genügt quadratfreie Polynom vom Inhalt 1 zu betrachten
- **§ 6** **(a)** Wiederholung und Ergänzungen zum Thema „endliche Körper“
  (b) Modularisierung, Quadratfreiheit, quadratfreie Zerlegung, gleichgradige Zerlegung, Swinnerton-Dyer-Polynome
- **§ 7** Primzerlegung in $\mathbb{Z}_p[x]$, p prim
  (a) Berlekamp-Verfahren für kleine Primzahlen
  (b) Berlekamp-Verfahren für große Primzahlen
  (c) Cantor-Zassenhaus-Verfahren
- **§ 8** Hebung nach $\mathbb{Z}[x]$, aber wie?
  (a) Henselsche Methode zur Hebung von Polynomprodukten von $\mathbb{Z}_p[x]$ nach $\mathbb{Z}_{p^{2^k}}[x]$
  (b) Zassenhaus-Methode zur Hebung von $\mathbb{Z}_{p^{2^k}}[x]$ nach $\mathbb{Z}[x]$ und sog. Mignotte-Schranke
  (c) Alternative zu (b): Zusammenhang mit kurzen Vektoren in speziellem $\mathbb{Z}$-Gitter
  (d) „einfacheres“ Gitter nach van Hoeij
  (e) p-adischer Hintergrund
- **§ 9** Ergänzungen
  (a) Überblick Faktorzerlegung in $\mathbb{Q}[x]$
  (b) Bemerkung zur Faktorzerlegung in $\mathbb{F}_{p^k}[x]$
  (c) Grundlagen zur Faktorzerlegung über endlichen algebraischen Erweiterungen von $\mathbb{Q}$
  (d) Bemerkungen zur Faktorzerlegung in zwei und mehr Variablen

IV Gröbnerbasen: Grundlagen

§ **10** Motivation und Orientierung

§ **11** Anordnung von Polynomen in mehreren Variablen: Monomordnungen, Wohlordnungen, geometrische Beschreibung von Monomordnungen, ordnungsabhängige Grundbegriffe

§ **12** Divisionsalgorithmus und die Folgen: Dickson-Lemma, Divisionsalgorithmus, Hilbertscher Basissatz, Gröbnerbasen,grundlegende Eigenschaften von Gröbnerbasen, Eindeutigkeit reduzierter Gröbnerbasen

§ **13** Buchberger-Kriterium und -Algorithmus: S-Polynome, Buchberger-Kriterium, Syzygien, Bezug zum Syzygiensatz, Basiskonversion, FGLM-Algorithmus.

§ **14** Ergänzungen: Wie viele reduzierte Gröbnerbasen hat ein Ideal? universelle Gröbnerbasen, Hinweise zum Gröbner-Spaziergang.

V Anwendungen:

§ **15** Dimension und Elimination

§ **16** Grundlegende Anwendungen: u.A.: erweiterter GB-Algorithmus, Rechnen in R/I, Lineare Gleichungen, Durchschnitte von Idealen und Berechnung von ggT und KgV in mehreren Variablen, Simultane Kongruenzen und Interpolation, Radikalzugehörigkeit, 0-dimensionale Radikalideale

§ **17** Gröbnerbasis-Methoden für algebraische Gleichungssystemen mit endlich vielen Lösungen: mehr zur Berechnung von Radikalen nulldimensionaler Ideale, Abschätzungen und Bestimmung der genauen Anzahl der Lösungen, reguläre Position eines Ideals, Shape-Lemma, Eigenwert- und Eigenvektormethoden zur Bestimmung der Lösungen.

Die letzten beiden Veranstaltungswochen fanden als Lese- und Seminarkurs statt.

VI L^3: Literatur [GaGe] Kapitel 16.

VII Ausgewähltes in Abhängigkeit von Interesse und Verlauf.