

# Inhalt

<b>1 Einleitung</b> .....	<b>1</b>
1.1 Was ist Computeralgebra? .....	1
1.2 Literatur .....	3
1.3 Computeralgebra-Systeme .....	4
<b>2 Grundlagen</b> .....	<b>7</b>
2.1 Algorithmen und ihre Komplexität .....	7
2.2 Kanonische Normalformen .....	12
2.3 Umformungssysteme .....	15
2.4 Ideale .....	21
2.5 Resultanten .....	30
2.6 Partialbruchzerlegungen .....	34
2.7 Einige Schranken .....	39
<b>3 Rechnen mit homomorphen Bildern</b> .....	<b>45</b>
3.1 Grundlegende Ideen .....	45
3.2 Das Chinesische Restproblem .....	47
3.3 Der Satz von Hensel .....	51
<b>4 Grundlegende algebraische Strukturen</b> .....	<b>57</b>
4.1 Ganze Zahlen .....	57
4.1.1 Darstellung .....	57
4.1.2 Addition und Subtraktion .....	61
4.1.3 Multiplikation .....	64
4.1.4 Division .....	74
4.1.5 Größter gemeinsamer Teiler .....	80
4.2 Rationale Zahlen .....	88
4.3 Algebraische Zahlen und Funktionen .....	89
4.3.1 Grundlagen und Probleme .....	89
4.3.2 Nichtverschachtelte Radikale .....	94

4.3.3	Verschachtelte Radikale	99
4.3.4	Allgemeine algebraische Ausdrücke	100
4.4	Transzendente Ausdrücke	101
4.4.1	Grundlagen und Probleme	101
4.4.2	Der Satz von Risch	102
4.5	Endliche Körper	107
4.6	Polynome	113
4.6.1	Zulässige Ordnungsrelationen	113
4.6.2	Darstellung	118
4.6.3	Addition und Subtraktion	123
4.6.4	Multiplikation	127
4.6.5	Division und Pseudodivision	132
4.6.6	Größter gemeinsamer Teiler	135
4.6.7	Der erweiterte euklidische Algorithmus	144
4.6.8	Subresultanten	145
4.6.9	Subresultanten-Ketten	147
4.6.10	Subresultanten und PRS Algorithmen	154
4.6.11	Verbesserte Subresultanten Algorithmen	160
4.6.12	Der erweiterte Subresultanten PRS-Algorithmus	164

## 5 Faktorisierung ganzer Zahlen 167

5.1	Vorbereitungen	167
5.2	Pollard- $\rho$	169
5.2.1	Der Faktorisierungsalgorithmus	169
5.2.2	Aufwandsabschätzung	175
5.3	Pollard- $(p - 1)$	176
5.3.1	Der Faktorisierungsalgorithmus	176
5.3.2	Aufwandsabschätzung	179
5.4	Elliptic Curve Method (ECM)	179
5.4.1	Pollard- $(p - 1)$ und ECM	179
5.4.2	Die Geometrie elliptischer Kurven	180
5.4.3	Multiplikation von Kurvenpunkten mit Skalaren	185
5.4.4	Der Faktorisierungsalgorithmus	189
5.4.5	Aufwandsabschätzung	193
5.5	Der Algorithmus von Morrison und Brillhart	197
5.5.1	Die Grundidee	197
5.5.2	Approximation reeller Zahlen durch Kettenbrüche	198
5.5.3	Die Kettenbruchentwicklung einer Wurzel	201
5.5.4	Der Faktorisierungsalgorithmus	204
5.5.5	Aufwandsabschätzung	211

5.6 Verwendung der Algorithmen	215
5.7 Das quadratische Sieb	217
5.7.1 Die Grundidee	217
5.7.2 Die Faktorenbasis	217
5.7.3 Das Sieben	218
5.7.4 Mehrere Polynome	223
<b>6 Polynom-Faktorisierung</b>	<b>227</b>
6.1 Motivation	227
6.2 Quadratfreie Faktorisierung	230
6.3 Der Berlekamp-Algorithmus	239
6.3.1 Grundvariante für kleine Körper	239
6.3.2 Variante für große Körper	247
6.3.3 Verbesserungen von Cantor und Zassenhaus	252
6.4 Berlekamp-Hensel Faktorisierung	264
6.4.1 Grundidee	264
6.3.1 Wie weit muss man liften?	270
6.3.2 Swinnerton-Dyer Polynome	273
<b>7 Summation in endlich vielen Termen</b>	<b>277</b>
7.1 Grundbegriffe	277
7.2 Die unbestimmte Summation	285
7.3 Die Polygamma-Funktionen	287
7.4 Shiftfreie Faktorisierung	290
7.5 Partielle Summation	292
7.6 Der Algorithmus von Moenck	293
7.7 Der Algorithmus von Gosper	298
<b>8 Gröbner-Basen</b>	<b>305</b>
8.1 Varietäten und Ideale	305
8.2 Reduktionen modulo Polynomidealen	312
8.3 Der Buchberger-Algorithmus	317
8.4 Eliminationsideale	325
<b>A Anhang CA-Systeme</b>	<b>329</b>
1. Universelle Programme	329
2. Spezialisierte Programme	335
<b>B Anhang Beispielsitzungen</b>	<b>341</b>
1. Maple	341

2. Mathematica .....	364
3. Gap .....	365
<b>Bibliographie .....</b>	<b>367</b>
1. Bücher und Zeitschriften .....	367
2. Konferenzen und zugehörigen Proceedingsbände .....	375
<b>Index .....</b>	<b>379</b>