

Wolfram Koepf

Computeralgebra

Eine algorithmisch orientierte Einführung



Springer

Inhaltsverzeichnis

1	Einführung in die Computeralgebra	
1.1	Was können Computeralgebrasysteme?	3
1.2	Ergänzende Bemerkungen	21
1.3	Übungsaufgaben	22
2	Programmieren in Computeralgebrasystemen	
2.1	Interne Darstellung von Ausdrücken	27
2.2	Mustererkennung	28
2.3	Kontrollstrukturen	30
2.4	Rekursion und Iteration	32
2.5	Rememberprogrammierung	36
2.6	Divide-and-Conquer-Programmierung	39
2.7	Programmierung durch Mustererkennung	40
2.8	Ergänzende Bemerkungen	43
2.9	Übungsaufgaben	43
3	Zahlsysteme und Ganzzahlarithmetik	
3.1	Zahlsysteme	51
3.2	Langzahlarithmetik: Addition und Multiplikation	53
3.3	Langzahlarithmetik: Division mit Rest	64
3.4	Der erweiterte Euklidische Algorithmus	68
3.5	Eindeutige Faktorzerlegung	73
3.6	Rationale Arithmetik	79
3.7	Ergänzende Bemerkungen	80
3.8	Übungsaufgaben	80
4	Modulare Arithmetik	
4.1	Restklassenringe	87

4.2	Modulare Quadratwurzeln	93
4.3	Chinesischer Restsatz	96
4.4	Der kleine Satz von Fermat	99
4.5	Modulare Logarithmen	104
4.6	Pseudoprime Zahlen	107
4.7	Ergänzende Bemerkungen	116
4.8	Übungsaufgaben	116
5	Codierungstheorie und Kryptographie	
5.1	Grundbegriffe der Codierungstheorie	121
5.2	Präfixcodes	124
5.3	Prüfzeichenverfahren	130
5.4	Fehlerkorrigierende Codes	131
5.5	Asymmetrische Verschlüsselungsverfahren	136
5.6	Ergänzende Bemerkungen	146
5.7	Übungsaufgaben	146
6	Polynomarithmetik: Rechnen mit Polynomen und rationalen Funktionen	
6.1	Polynomringe	153
6.2	Multiplikation: Der Karatsuba-Algorithmus	159
6.3	Schnelle Multiplikation mit FFT	162
6.4	Division mit Rest	173
6.5	Polynominterpolation	178
6.6	Der erweiterte Euklidische Algorithmus	181
6.7	Eindeutige Faktorzerlegung	185
6.8	Quadratfreie Faktorisierung	192
6.9	Rationale Funktionen	197
6.10	Ergänzende Bemerkungen	199

6.11	Übungsaufgaben	199
7	Algebraische Zahlen	
7.1	Restklassenpolynomringe.....	205
7.2	Chinesischer Restsatz für Polynome.....	210
7.3	Algebraische Zahlen.....	212
7.4	Endliche Körper	227
7.5	Resultanten	234
7.6	Polynomiale Gleichungssysteme.....	243
7.7	Ergänzende Bemerkungen	251
7.8	Übungsaufgaben	252
8	Faktorisierung in Polynomringen	
8.1	Vorbereitende Betrachtungen	261
8.2	Effiziente Faktorisierung in $\mathbb{Z}_p[x]$	265
8.3	Quadratfreie Faktorisierung von Polynomen über endlichen Körpern	274
8.4	Effiziente Faktorisierung in $\mathbb{Q}[x]$	276
8.5	Hensel-Lifting.....	282
8.6	Multivariate Faktorisierung	287
8.7	Ergänzende Bemerkungen	291
8.8	Übungsaufgaben	291
9	Vereinfachung und Normalformen	
9.1	Normalformen und kanonische Formen	297
9.2	Normalformen und kanonische Formen für Polynome	302
9.3	Normalformen für rationale Funktionen.....	304
9.4	Normalformen für trigonometrische Polynome	305
9.5	Ergänzende Bemerkungen	310
9.6	Übungsaufgaben	311

10	Potenzreihen	
10.1	Formale Potenzreihen.....	31
10.2	Taylorpolynome	32
10.3	Berechnung formaler Potenzreihen.....	32
10.3.1	Holome Differentialgleichungen	33
10.3.2	Holome Rekursionsgleichungen	34
10.3.3	Hypergeometrische Funktionen	34
10.3.4	Effiziente Berechnung von Taylorpolynomen holonomer Funktionen	357
10.4	Algebraische Funktionen.....	359
10.5	Implizite Funktionen	364
10.6	Ergänzende Bemerkungen	373
10.7	Übungsaufgaben	374
11	Algorithmische Summation	
11.1	Bestimmte Summation.....	387
11.2	Differenzenrechnung	396
11.3	Unbestimmte Summation	399
11.4	Unbestimmte Summation hypergeometrischer Terme	404
11.5	Bestimmte Summation hypergeometrischer Terme ...	419
11.6	Ergänzende Bemerkungen	433
11.7	Übungsaufgaben	434
12	Algorithmische Integration	
12.1	Der Bernoulli-Algorithmus für rationale Funktionen ...	441
12.2	Algebraische Vorbereitungen	443
12.3	Rationaler Teil	449
12.4	Logarithmischer Teil	456
12.5	Ergänzende Bemerkungen	478

12.6	Übungsaufgaben	478
	Literaturverzeichnis	481
	Symbolverzeichnis	487
	<i>Mathematica</i> Stichwortverzeichnis	489
	Stichwortverzeichnis	497