

Inhaltsverzeichnis

1	Aufbau, Gliederung & Voraussetzungen *	1
2	Zahldarstellungen und Fehleranalyse *	5
2.1	Zahldarstellungen und Maschinenzahlen *	7
2.2	Fehlerarten und ihre Kontrolle *	15
3	Numerische Näherungsverfahren *	21
3.1	Banachscher Fixpunktsatz in \mathbb{R} *	27
3.2	Newton-Verfahren *	33
3.3	Heron-Verfahren *	37
3.4	Sekanten-Verfahren *	42
3.5	Abstieg-Verfahren *	46
3.6	Dividierte-Differenzen-Verfahren *	53
3.7	Trapez- und Simpson-Regel *	60
3.8	Iterierte Trapez- und Simpson-Regel *	65
3.9	Normen und Folgen in \mathbb{R}^n **	69
3.10	Banachscher Fixpunktsatz in \mathbb{R}^n **	74
3.11	Gesamtschritt-Verfahren **	76
3.12	Einzel-schritt-Verfahren **	83
3.13	SOR-Verfahren **	88
3.14	Von-Mises-Geiringer-Verfahren **	90
4	Grafische Visualisierungsmethoden *	95
4.1	Polynomiale Interpolation mit Monomen *	101
4.2	Polynomiale Interpolation nach Lagrange *	105
4.3	Polynomiale Interpolation nach Newton *	111
4.4	Polynomiale Interpolation nach Aitken-Neville *	120
4.5	Polynomiale Approximation nach de Casteljau *	126
4.6	Interpolierende Subdivision nach Dubuc **	134
4.7	Approximierende Subdivision nach Chaikin **	140
4.8	Bilineare Interpolation über Rechtecken *	147
4.9	Gouraud-Schattierung über Rechtecken *	149
4.10	Phong-Schattierung über Rechtecken *	153
4.11	Transfinite Interpolation über Rechtecken **	157
4.12	Polynomiale Approximation über Rechtecken **	163

4.13	Lineare Interpolation über Dreiecken *	168
4.14	Gouraud-Schattierung über Dreiecken *	171
4.15	Phong-Schattierung über Dreiecken *	174
4.16	Transfinite Interpolation über Dreiecken **	177
4.17	Polynomiale Approximation über Dreiecken **	183
5	Kryptografische Basistechniken **	189
5.1	Gruppen *	195
5.2	Ringe *	198
5.3	Körper *	202
5.4	Galois-Feld $GF(2)=\mathbb{Z}_2$ *	206
5.5	Galois-Feld $GF(4)$ **	209
5.6	Galois-Feld $GF(8)$ ***	216
5.7	Galois-Feld $GF(16)$ ***	220
5.8	Satz von Fermat und Euler **	223
5.9	Euklidischer Algorithmus **	228
5.10	Einwegfunktionen *	237
5.11	Einwegfunktionen mit Falltür *	240
5.12	Diffie-Hellman-Verfahren *	244
5.13	RSA-Verfahren **	247
5.14	Vernam-Verfahren *	251
5.15	DES-Verfahren **	254
5.16	AES-Verfahren ***	259
5.17	Elliptische Kurven ($\text{char } K > 3$) ***	271
5.18	EC-Diffie-Hellman-Verfahren ($\text{char } K > 3$) **	279
5.19	Elliptische Kurven ($\text{char } K = 2$) ***	282
5.20	EC-Diffie-Hellman-Verfahren ($\text{char } K = 2$) **	287
	Glossar	293
	Literatur	309
	Namens- und Organisationsindex	312
	Sachindex	314
