

Inhaltsverzeichnis

Vorwort	v
---------------	---

I Algebra	1
1 Gruppenzwang I — Wir rechnen mit allem	3
1.1 Die graue Theorie zu Beginn	4
1.1.1 Eine Hierarchie mathematischer Strukturen	4
1.2 Die bunte Praxis.....	7
1.2.1 Beispiele für Gruppen	7
1.2.2 Gegenbeispiele	10
1.2.3 Kleingeld- und Uhrenarithmetik	12
1.3 Wieder Theorie: Ein paar Beweise als Grundlage.....	15
1.3.1 Einseitig- und Eindeutigkeit	15
1.3.2 Einfache Rechenregeln	19
1.3.3 Potenzen.....	21
1.4 Abschluss	24
2 Gruppenzwang II — Anonyme Mathematiker bieten Gruppentherapie an	25
2.1 Untergruppen	25
2.1.1 Das Untergruppenkriterium	27
2.1.2 Beispiele und Gegenbeispiele	28
2.1.3 Untergruppen von \mathbb{Z}	29
2.1.4 Erzeugendensysteme.....	29
2.2 Nebenklassen und der Satz von Lagrange	33
2.3 Normalteiler und Faktorgruppen	38
2.4 Uhrenarithmetik reloaded	41
2.5 Abschluss	42
3 Gruppenzwang III — Sensation: Homo Morphismus ist ein Gruppentier	43
3.1 Gruppenhomomorphismen	43
3.1.1 Strukturerhaltung.....	45
3.1.2 Kern und Bild	46
3.2 Mehr Homomorphismen	47
3.2.1 Isomorphismen	48
3.3 Der Homomorphiesatz	50
3.3.1 Einmal mehr zyklische Gruppen	53
3.4 Charakteristische Untergruppen	54
3.5 Direkte Produkte und direkte Summen von Gruppen	56
3.6 Abschluss	58

4 Gruppenzwang IV — Gruppencamper brauchen Iso(morphie-)matten	59
4.1 Hilfssätze und Konventionen	60
4.2 Der erste Isomorphiesatz	61
4.3 Der zweite Isomorphiesatz	63
4.4 Der dritte Isomorphiesatz	68
4.5 Eine Anwendung der Isomorphiesätze	71
4.6 Abschluss	74
5 Gruppenzwang V — Dr. Cauchy und Dr. Sylow bitte zur Gruppen-OP	75
5.1 Einführung	75
5.2 Drei grundlegende Aussagen	77
5.3 Das erste Teilziel	80
5.4 Das Große Ziel: Die Sylow-Sätze	81
5.4.1 Der erste Satz von Sylow	82
5.4.2 Der zweite Satz von Sylow	85
5.4.3 Der dritte Satz von Sylow	86
5.5 Anwendungen der Sätze von Sylow	86
5.6 Abschluss	89
6 Gruppenzwang VI — Randale: Gruppendemo musste aufgelöst werden	91
6.1 Und was hat das nun mit Gruppen zu tun?	91
6.1.1 (Sub-)Normalreihen	92
6.1.2 Faktoren von (Sub-)Normalreihen und Auflösbarkeit	93
6.2 Erste Schritte	94
6.2.1 Isomorphie von Subnormalreihen	94
6.2.2 Verfeinerungen	95
6.3 Die Sätze von Schreier und Jordan-Hölder	97
6.4 Kommutatoren	99
6.4.1 Die Kommutator-Reihe	100
6.4.2 Nützliches für Gruppentherapeuten	102
6.5 Nilpotente und p -Gruppen	104
6.6 Abschluss	106
7 Ein Spielzeug mit Gruppenstruktur	107
7.1 Einleitung	107
7.2 Speedcubing	108
7.3 Notation	109
7.4 Die Gesetze des Würfels	109
7.5 Die Cubegruppe	110
7.6 Konjugation und Kommutatoren	113
7.7 Ein paar offene Probleme	115
7.8 Weitere Informationen	115

8	Endliche Körper	117
8.1	Wiederholung muss sein	118
8.2	Körper haben Charakter	120
8.3	Frobenius mischt sich ein	123
8.4	Polynomringe	125
8.5	Adjunktion	127
8.6	Symbolische Adjunktion von Nullstellen	129
8.7	Existenz und Eindeutigkeit endlicher Körper	135
8.8	Zusammenfassung, Literatur und Ausblick	137
II	Diskrete Mathematik	139
9	Über die Anzahl von Sitzordnungen am runden Tisch	141
9.1	Die Frage	141
9.2	Der Weg	141
9.3	Versteh das Problem	142
9.3.1	Beispiel	142
9.3.2	Erste, aber falsche Lösung	143
9.3.3	Systematisches Probieren	143
9.4	Suche Zusammenhänge, ersinne einen Plan und führe ihn aus	144
9.4.1	Suche im Internet	144
9.4.2	Eine Wertetabelle	145
9.4.3	Ein Plan	146
9.5	Überprüfe die Lösung	147
9.5.1	Das Burnside-Lemma	147
9.5.2	Anwendung des Polya-Burnside-Lemmas	147
9.5.3	Die $T(n, k)$ -Formel	149
9.5.4	Versteh die Formel	150
9.5.5	Gruppe der Rotationen	152
9.5.6	Unterscheidungen bei der Fragestellung	152
9.6	Am Ziel	156
9.6.1	Zwei verschiedene Berechnungsweisen?	156
9.6.2	Zusammenfassung und Lösung der Aufgabe	156
9.6.3	Konstruktiver Algorithmus?	157
9.6.4	Nachbetrachtung	157
10	Summenzerlegungen	159
10.1	Zählen kann doch jeder	162
10.2	Äquivalente und verwandte Fragen	162
10.3	Die Anzahl der Summenzerlegungen von n	163
10.4	Rekursive Ansätze	164
10.4.1	Summenzerlegungen nach Größe der Summanden	164
10.4.2	Summenzerlegungen nach Anzahl der Summanden	166

10.5	Dualität	168
10.6	Leere Behälter.....	169
10.7	Erzeugende Funktionen	171
10.7.1	Die Brücke	172
10.7.2	Über die Brücke gehen.....	173
10.7.3	Der Bauplan ist klar	174
10.7.4	Zurück zu Summenzerlegungen	175
10.8	Ausblick und Schluss	175
11	Pentagon, Kartenhaus und Summenzerlegung	177
11.1	Pentagonalzahlen	178
11.2	Kartenhaus-Zahlen	178
11.3	Erstes Wunder	179
11.4	Verallgemeinerte Pentagonalzahlen	179
11.5	Euler und Kartenhäuser?	180
11.6	Zweites Wunder	180
11.7	Nachlese	182
12	Das Heiratsproblem	183
12.1	Kleine mathematische Hilfe für potentielle Schwiegermütter	183
12.2	Ein Dorf will heiraten	184
12.3	Die graphentheoretische Darstellung	185
12.4	Graphentheoretischer Algorithmus für das Problem des gewichtsmaximalen Matchings	188
12.4.1	Beispiel: Unser Dorf	189
12.4.2	Suche ein optimales Matching	190
12.4.3	Der graphentheoretische Algorithmus kurz und knapp	194
12.5	Lösungsweg mit linearer Optimierung	194
12.5.1	Ein schönerer Lösungsweg?	194
12.5.2	Ansatz mit linearer Optimierung	194
12.5.3	Formulierung der konkreten linearen Optimierungsaufgabe ..	195
12.5.4	Ganzzahlige Lösungen	197
12.6	Zurück ins Dorf.....	200
13	Über die Anzahl surjektiver Abbildungen	203
14	Potenzsummen	211
15	Berechnung großer Binomialkoeffizienten	215
15.1	Rechnen gemäß Definition	215
15.2	Rekursive Berechnung	216
15.3	Multiplizierte in günstiger Reihenfolge	216
15.4	Teile und (be-)herrsche	217
15.5	Der Satz von Legendre	218
15.6	Algorithmische Berechnung	218
15.7	Weiteres Anwendungsbeispiel.....	219

16 Über Permanente, Permutationen und Fixpunkte	221
16.1 Einführung	221
16.2 Das Prinzip der Inklusion und Exklusion	221
16.3 Permanente	223
16.4 Das Rencontre-Problem	226
17 Zählen mit Permanente	231
17.1 Definitionen und Vorbereitungen	231
17.2 Zählen mit Permanente und Determinanten	233
17.3 Der Satz	235
17.4 Beweis der Aussagen (17.1) und (17.2)	236
17.5 Beweis des Satzes	237
18 Binomialmatrizen und das Lemma von Gessel-Viennot	239
18.1 Die Binomialmatrix	239
18.2 Pfade und Pfadsysteme	241
18.3 Das Lemma von Gessel-Viennot	243
18.4 Die Determinante der Binomialmatrix	244
18.5 LU-Zerlegung der Binomialmatrix	246
18.6 Ein weiteres Beispiel — Spinne und Feind	249
III Geometrie und Konstruierbarkeit	253
19 Mathematik des Faltens — Winkeldreiteilung und der Satz von Haga	255
19.1 Winkeldreiteilung	255
19.2 Satz von Haga und Verallgemeinerung	257
19.3 Konstruktion eines Silbernen Rechtecks	261
19.4 Schlussbemerkung	264
20 Das regelmäßige Siebzehneck	265
20.1 Das Problem und die Rechnung	265
20.2 Die Konstruktion	270
21 Ein Satz von Carnot	273
21.1 Satz von Carnot	273
21.2 Umkehrsatz von Carnot	275
22 Die Kardioide als Hüllkurve	277
IV Elliptische Kurven und Kryptographie	281
23 Das Gruppengesetz elliptischer Kurven	283
23.1 Motivation	283
23.2 Definition elliptischer Kurven	284
23.3 Singuläre Punkte	285

23.4	Das Gruppengesetz	288
23.4.1	Der unendlich ferne Punkt	289
23.4.2	Die anderen Fälle	291
23.4.3	Zusammenfassung der Definition	293
23.5	Die Assoziativität	294
23.5.1	Vorbereitung	294
23.5.2	Ausschluss der einfachen Fälle	295
23.5.3	Der letzte Fall	298
23.6	Andere Ansätze	301
23.6.1	Projektive Geometrie	301
23.6.2	Divisoren	303
23.7	Abschluss	303
24	ECC — Elliptic Curves Cryptography	305
24.1	Einführung	305
24.2	Das Problem des diskreten Logarithmus	306
24.3	Schlüsseltausch nach Diffie-Hellman	308
24.4	Public-Key-Verschlüsselung nach ElGamal	309
24.5	Signierung nach ElGamal und mit ECDSA	310
24.5.1	ElGamal-Signatur-Algorithmus	310
24.5.2	ECDSA	312
24.6	Index Calculus	313
24.7	Abschluss	315
25	Primzahlen und elliptische Kurven	317
25.1	Mathematisches über elliptische Kurven	317
25.1.1	Hasses Satz	317
25.1.2	Elliptische Kurven mod n	318
25.2	ECM — Faktorisierung mit elliptischen Kurven	319
25.3	Zertifizierung von Primzahlen	322
25.3.1	Was ist eigentlich ein Zertifikat?	322
25.3.2	Das Goldwasser-Kilian-Zertifikat	322
25.3.3	Am Beispiel der vierten Fermat-Zahl	324
25.4	Abschluss	325
26	Primzahlen mit Abstand	327
26.1	Der Abstand zwischen 2 Primzahlen wird beliebig groß	327
26.2	In jeder unbegrenzten arithmetischen Progression gibt es unendlich viele Primzahlen	328
26.3	Es gibt arithmetischen Progressionen beliebiger Länge, die nur aus Primzahlen bestehen	329
27	Faktorisierungsverfahren	331
27.1	Einführung	331
27.2	Probiedivision	332

27.3	Fermat-Faktorisierung	333
27.4	Lehman-Algorithmus	335
27.5	Pollard-Rho-Verfahren	337
27.6	$(p - 1)$ -Verfahren	341
27.7	Elliptische-Kurven-Methode	345
27.8	Quadratisches Sieb	352
V	Ausblick auf Weiteres	361
28	Fouriertransformation	363
28.1	Motivation	363
28.2	Zeit und Frequenzbereich	364
28.3	Der Weg zur Fouriertransformation	365
28.3.1	Von den Fourierreihen zur Transformation	366
28.3.2	Tabelle zur Fouriertransformation von Zeitsignalen	367
28.4	Beispiele mit dem Oszilloskop	368
28.4.1	Die Sinusfunktion	368
28.4.2	Die Rechteckfunktion	370
28.4.3	Die Dreieckfunktion	371
28.4.4	Gauß	372
28.5	Die Faltung	372
28.6	Systeme	375
28.7	Was es sonst noch gibt	377
29	Das Brachistochronenproblem	379
29.1	Einleitung	379
29.2	Formalisierung des Problems	381
29.3	Ein mächtiges Werkzeug: Variationskalkül	382
29.4	Bestimmen der optimalen Lösung	384
29.5	Abschluss	387
30	Repunits, geometrische Summen und Quadratzahlen	389
30.1	Einige Spezialfälle	390
30.2	Hilfsmittel	392
30.2.1	Die Pellsche Gleichung	392
30.2.2	Rekursive Folgen	394
30.3	Der Fall $q = 3$	395
30.3.1	m geradzahlig	395
30.3.2	m ungeradzahlig	396
30.4	Ausblick	404
31	Irrationalität von e und π	405
31.1	Einleitung	405
31.2	Die Irrationalität von e	406
31.3	Die Irrationalität von π	408

32 Transzendenz von e und π	411
32.1 Einleitung	411
32.2 Die Transzendenz von e	412
32.3 Die Transzendenz von π	416
32.3.1 Vorbereitungen	418
32.3.2 Konjugierte von $i \cdot \pi$	421
32.3.3 Zwei konträre Abschätzungen	424
Literaturverzeichnis	429
Index	435