



Algebra leichter gemacht

Lösungsvorschläge zu Aufgaben
des Ersten Staatsexamens
für das Lehramt an Gymnasien

von

Martina Kraupner

Oldenbourg Verlag München

Die Collage auf dem Cover zeigt Porträts des französischen Mathematikers Évariste Galois, erstellt von Kevin Danz, Philip Junk, Benedikt Meßmer, Cornelia Oczycz, Franziska Schmitt und Tobias Schulz.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© 2011 Oldenbourg Wissenschaftsverlag GmbH
Rosenheimer Straße 145, D-81671 München
Telefon: (089) 45051-0
www.oldenbourg-verlag.de

Das Werk einschließlich aller Abbildungen ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Bearbeitung in elektronischen Systemen.

Lektorat: Kathrin Mönch
Herstellung: Constanze Müller
Einbandgestaltung: hauser lacour
Gesamtherstellung: Grafik + Druck, München

Dieses Papier ist alterungsbeständig nach DIN/ISO 9706.

ISBN 978-3-486-70544-7

Vorwort

Dieses Buch richtet sich in erster Linie an alle Studenten des gymnasialen Lehramts im Fach Mathematik in Bayern. Auch Nichtbayern und Nichtlehrämter, die den Stoff der Grundvorlesungen der Algebra vertiefen wollen, sind eingeladen, sich mit den ausführlichen Lösungen zu 175 Aufgaben aus dem Bayerischen Staatsexamen zur Algebra (und Zahlentheorie) zu beschäftigen.

Erfahrungsgemäß fällt es Studenten am Anfang ihrer Vorbereitungsphase auf das Staatsexamen sehr schwer, Prüfungsaufgaben eigenständig zu lösen. Die Algebra-Vorlesungen liegen häufig bereits einige Semester zurück, Zulassungsarbeit und erziehungswissenschaftliches Staatsexamen haben die Beschäftigung mit Algebra in den Hintergrund rücken lassen. Einige wenige arbeiten sich spielend wieder in die Inhalte der Vorlesung ein und sind schnell in der Lage, Aufgaben zu lösen. Den meisten aber erscheint der Berg, den es zu besteigen gilt, schier unbezwingbar. Für die Einen wie die Anderen ist dieses Übungsbuch gedacht.

Die Lösungsvorschläge für die Prüfungstermine Herbst 2003 bis Herbst 2009 wurden während der vergangenen Semester im Zuge der Staatsexamens-Tutorien an der Universität Passau erstellt. Sie sollten nicht als Musterlösungen verstanden werden, denn an einigen Stellen ist die Beantwortung viel ausführlicher, als es im Staatsexamen verlangt wird. Vielmehr wurde versucht, die Lösungen so aufzubereiten, dass sie auch für Studenten, die am Anfang ihrer Lernphase stehen, verständlich sind. Ich hoffe, das ist gelungen, und wünsche allen, die mit diesem Buch lernen, besonders viel Erfolg im Examen.

Mein herzlichster Dank geht an Markus Kriegl, Philipp Jovanovic und Bettina Kreuzer für die hervorragende und wertvolle Korrekturarbeit an diesem Buch. Ich danke meinem wunderbaren Bürokollegen Thomas Stadler, der mir in vielen Dingen eine unschätzbare Hilfe war. Vielen Dank an Prof. Dr. Martin Kreuzer für die Betreuung in den letzten drei Jahren und die rettenden Ideen bei Aufgaben, an denen ich mir fast die Zähne ausgebissen hätte. Ebenso danke ich Herrn Peter-Paul Rast und dem Leistungskurs Kunst des Gymnasiums Neubiberg für die wunderschönen Porträts des Evariste Galois, Stefan Schuster und allen Mitarbeitern des Lehrstuhls für Symbolic Computation der Universität Passau und den vielen engagierten Studenten der Tutorien der letzten Semester.

Martina Kraupner

Inhaltsverzeichnis

Themenverzeichnis	xiii
I. Grundlagen	1
1. Gruppen	5
1.1. Zyklische Gruppen	7
1.2. Normalteiler und Faktorgruppen	8
1.3. Gruppenoperationen	11
1.4. Direkte und semidirekte Produkte	13
1.5. Die Sylow-Sätze	14
1.6. Permutationsgruppen und Diedergruppen	15
1.7. Gruppen kleinerer Ordnung	16
2. Ringe	19
2.1. Euklidische Ringe	23
2.2. Faktorielle Ringe	24
2.3. Chinesischer Restsatz	24
2.4. Irreduzibilität	24
3. Körper	27
3.1. Galoistheorie	31
3.2. Einheitswurzeln und Kreisteilungspolynome	33
3.3. Endliche Körper	34
4. Zahlentheorie	37
5. Konstruktionen mit Zirkel und Lineal	39
6. Lineare Algebra	41
II. Aufgaben und Lösungsvorschläge	45
7. Prüfungstermin Herbst 2003	49
H03-I-1	49
H03-I-2	51
H03-I-3	52

H03-I-4	53
H03-II-1	55
H03-II-2	56
H03-II-3	57
H03-II-4	58
H03-II-5	61
H03-III-1	62
H03-III-2	63
H03-III-3	65
H03-III-4	67
8. Prüfungstermin Frühjahr 2004	71
FJ04-I-1	71
FJ04-I-2	73
FJ04-I-3	74
FJ04-I-4	75
FJ04-I-5	77
FJ04-II-1	78
FJ04-II-2	80
FJ04-II-3	82
FJ04-II-4	84
FJ04-III-1	86
FJ04-III-2	87
FJ04-III-3	88
FJ04-III-4	89
9. Prüfungstermin Herbst 2004	91
H04-I-1	91
H04-I-2	93
H04-I-3	94
H04-I-4	94
H04-I-5	96
H04-II-1	98
H04-II-2	99
H04-II-3	100
H04-II-4	101
H04-II-5	103
H04-III-1	104
H04-III-2	105
H04-III-3	106
H04-III-4	107
H04-III-5	108
10. Prüfungstermin Frühjahr 2005	111
FJ05-I-1	111

FJ05-I-2	111
FJ05-I-3	113
FJ05-I-4	114
FJ05-I-5	115
FJ05-II-1	117
FJ05-II-2	118
FJ05-II-3	120
FJ05-II-4	120
FJ05-II-5	121
FJ05-III-1	122
FJ05-III-2	122
FJ05-III-3	123
FJ05-III-4	124
FJ05-III-5	125
11. Prüfungstermin Herbst 2005	127
H05-I-1	127
H05-I-2	128
H05-I-3	129
H05-I-4	132
H05-II-1	134
H05-II-2	135
H05-II-3	137
H05-II-4	137
H05-III-1	138
H05-III-2	140
H05-III-3	142
H05-III-4	143
12. Prüfungstermin Frühjahr 2006	147
FJ06-I-1	147
FJ06-I-2	148
FJ06-I-3	148
FJ06-I-4	150
FJ06-II-1	152
FJ06-II-2	152
FJ06-II-3	153
FJ06-II-4	155
FJ06-II-5	156
FJ06-II-6	157
FJ06-III-1	158
FJ06-III-2	159
FJ06-III-3	160
FJ06-III-4	161
FJ06-III-5	162

FJ06-III-6	163
13. Prüfungstermin Herbst 2006	165
H06-I-1	165
H06-I-2	166
H06-I-3	169
H06-I-4	172
H06-II-1	173
H06-II-2	175
H06-II-3	177
H06-II-4	180
H06-III-1	182
H06-III-2	183
H06-III-3	183
H06-III-4	184
14. Prüfungstermin Frühjahr 2007	187
FJ07-I-1	187
FJ07-I-2	189
FJ07-I-3	190
FJ07-I-4	192
FJ07-I-5	193
FJ07-II-1	195
FJ07-II-2	197
FJ07-II-3	198
FJ07-II-4	199
FJ07-II-5	200
FJ07-III-1	202
FJ07-III-2	202
FJ07-III-3	203
FJ07-III-4	204
FJ07-III-5	205
15. Prüfungstermin Herbst 2007	207
H07-I-1	207
H07-I-2	208
H07-I-3	209
H07-I-4	210
H07-I-5	210
H07-II-1	212
H07-II-2	212
H07-II-3	216
H07-II-4	217
H07-II-5	218
H07-III-1	218

H07-III-2	221
H07-III-3	222
H07-III-4	222
H07-III-5	223
16. Prüfungstermin Frühjahr 2008	225
FJ08-I-1	225
FJ08-I-2	225
FJ08-I-3	228
FJ08-I-4	229
FJ08-I-5	230
FJ08-II-1	231
FJ08-II-2	231
FJ08-II-3	232
FJ08-II-4	234
FJ08-III-1	235
FJ08-III-2	236
FJ08-III-3	237
FJ08-III-4	239
17. Prüfungstermin Herbst 2008	241
H08-I-1	241
H08-I-2	243
H08-I-3	244
H08-I-4	246
H08-II-1	247
H08-II-2	248
H08-II-3	249
H08-II-4	251
H08-III-1	252
H08-III-2	253
H08-III-3	254
H08-III-4	255
18. Prüfungstermin Frühjahr 2009	259
FJ09-I-1	259
FJ09-I-2	261
FJ09-I-3	264
FJ09-I-4	264
FJ09-II-1	265
FJ09-II-2	267
FJ09-II-3	268
FJ09-II-4	269
FJ09-III-1	270
FJ09-III-2	271

FJ09-III-3	272
FJ09-III-4	273
19. Prüfungstermin Herbst 2009	275
H09-I-1	275
H09-I-2	276
H09-I-3	277
H09-I-4	278
H09-II-1	279
H09-II-2	279
H09-II-3	282
H09-II-4	283
H09-III-1	286
H09-III-2	288
H09-III-3	289
H09-III-4	291
Literaturvorschläge	293
Index	295

Themenverzeichnis

Gruppen

Sylow-Gruppen

FJ04-I-3	Gruppe der Ordnung 225	74
H04-II-1	Gruppe der Ordnung pq	98
H04-III-1	Gruppe der Ordnung p^2q	104
H05-III-1	Gruppe der Ordnung 56	138
H06-I-4	nichtabelsche Gruppe der Ordnung 231	172
FJ07-I-1	Gruppe der Ordnung 2007	187
H08-III-3	einfache Gruppe der Ordnung p^2q	254
H09-II-3	p -Sylow-Untergruppen von S_n	282

Gruppenoperationen

H03-I-4	Automorphismengruppe von \mathbb{F}_{81}	53
H03-III-1	Gruppe der Ordnung p^m	62
FJ05-II-2	einfache Gruppe der Ordnung 120	118
H05-III-1	Gruppe der Ordnung 56	138
FJ07-I-1	Gruppe der Ordnung 2007	187
FJ08-III-1	$ \{g \in G \mid gU \ni x\} $	235
H08-I-2	transitive Operation	243
H09-I-3	normale Untergruppe vom Index p	277

Permutationsgruppen und Diedergruppen

H03-II-1	Definition von A_n , S_4 auflösbar	55
FJ04-II-1	Untergruppe der Ordnung 21 in S_7	78
FJ04-III-3	D_6 , A_4 , $\mathbb{Z}/3\mathbb{Z} \times_{\varphi} \mathbb{Z}/4\mathbb{Z}$	88
H04-I-1	2-Sylow-Untergruppen von S_4 , A_5 und A_6	91
FJ05-II-2	einfache Gruppe der Ordnung 120	118

H05-I-2	$G = \{\sigma \in S_n; \sigma(n) = n\}$	128
H05-II-1	zwei nichtabelsche Gruppen der Ordnung 20	134
FJ06-II-5	Diedergruppe D_4	156
H06-II-1	$\{\sigma \in S(X) : \sigma(X_1) = X_1 \text{ oder } \sigma(X_1) = X_2\}$.	173
FJ07-I-5	Element und Untergruppe der Ordnung 5 in A_4	193
FJ07-II-1	$S_4, D_{12}, D_6 \times \mathbb{Z}_2, S_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	195
FJ08-I-2	S_4 hat mindestens 24 Untergruppen	225
FJ08-II-1	$[S_n : G] \geq \binom{n}{k}$	231
H08-II-1	Elemente der Ordnung j in S_n	247
FJ09-II-1	$S_3 \times \mathbb{Z}_4, S_5$	265

Direkte und semidirekte Produkte

FJ04-II-1	Untergruppe der Ordnung 21 in S_7	78
H04-II-1	Gruppe der Ordnung pq	98
H06-I-4	Gruppe der Ordnung 231	172
H07-II-2	$\mathbb{Z}/3\mathbb{Z} \times_{\varphi} \mathbb{Z}/4\mathbb{Z}$	212
H07-III-1	Gruppe der Ordnung p^3	218
FJ09-III-3	$\mathbb{Z}/n\mathbb{Z} \ltimes (\mathbb{Z}/n\mathbb{Z})^*$	272
H09-III-1	nichtabelsche Gruppe der Ordnung 155	286

Sonstiges

H03-I-1	Satz von Cayley, $n = 2u$ mit ungeradem u	49
FJ04-I-1	minimaler Normalteiler	71
FJ05-II-1	Satz von Lagrange	117
H05-II-2	$\text{Aut}(G)$ zyklisch	135
FJ06-I-3	maximale Untergruppen	148
FJ06-II-1	direkte Summe	152
FJ06-II-3	additive Gruppe von \mathbb{R}	153
FJ06-III-2	Gleichung für Gruppenindizes	159
FJ06-III-3	$G \times G, \mathcal{Q}$	160
FJ07-III-3	$G = \langle z \rangle$ mit $ G = 63$	203
H07-I-2	zyklisch, genau eine maximale Untergruppe	208
H07-II-1	Exponent	212
FJ08-II-3	Automorphismengruppe der additiven Gruppe von \mathbb{Q}	232
FJ08-III-2	$\text{tor}(G)$	236
H08-II-2	$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z}$	248

H08-III-2	$P_n = \{g^n; g \in G\}$	253
FJ09-I-1	A mit $A/B \cong \mathbb{Z}/8\mathbb{Z}$	259
FJ09-I-2	vollständige Gruppe	261
FJ09-II-2	Normalteiler vom Index 2 oder 3	267
H09-II-2	maximale Untergruppen	279

Ringe

Euklidische Ringe

H03-II-4	$\mathbb{Z}[i]$	58
FJ04-II-2	$\mathbb{Z}[\sqrt{2}]$	80
H04-I-3	größter gemeinsamer Teiler zweier Polynome	94
FJ05-I-3	größter gemeinsamer Teiler in $\mathbb{Z}[i]$	113
H05-III-2	$\mathbb{Z}[\sqrt{2}]$	140
H06-I-2	$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$	166
FJ07-II-2	$\mathbb{Z}[i\sqrt{2}]$	197
H09-III-2	$\mathbb{Z} + \mathbb{Z}\sqrt{-2}$	288

Faktorielle Ringe

H04-II-2	$\mathbb{Z}[\sqrt{-3}]$	99
H05-II-3	Hauptidealring	137
FJ06-III-4	Polynomring über einem faktoriellem Ring	161

Chinesischer Restsatz

H03-II-4	$\mathbb{Z}[i]$	58
FJ04-II-2	$\mathbb{Z}[\sqrt{2}]$	80
FJ05-III-3	Umkehrung von $\phi : \mathbb{Z}/1000\mathbb{Z} \rightarrow \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$	123

Irreduzibilität von Polynomen

H03-II-5	$X^p + pX - 1, X^4 - 42X^2 + 1 \in \mathbb{Z}[X]$	61
FJ04-I-2	$aX^4 + bX^3 + c \in \mathbb{Q}[X]$	73
H04-I-5	Anzahl normierter, irreduzibler Polynome in $\mathbb{F}_3[X]$	96

H04-II-3	$5X^3 + 63X^2 + 168 \in \mathbb{Z}[X]$, $X^4 + X + 1 \in \mathbb{F}_2[X]$, $X^9 + XY^7 + Y \in \mathbb{Z}[X, Y]$	100
FJ05-I-4	$X^4 - X^3 - 9X^2 + 4X + 2 \in \mathbb{Q}[X]$, $X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$, $Y^6 + XY^5 + 2XY^3 + 2X^2Y^2 - X^3Y + X^2 + X \in \mathbb{Q}[X, Y]$	114
H05-II-4	$X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$	137
H06-II-3	$X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$	177
FJ07-III-2	$1 + X + X^2 + X^3 + X^4 \in \mathbb{F}_2[X]$	202
FJ08-II-4	$X^3 + aX + b \in \mathbb{Q}[X]$	234
H08-I-3	$T^4 + 1 \in \mathbb{R}[T]$	244
H08-I-4	$X^p - X - 1 \in \mathbb{F}_p[X]$	246
H08-II-4	$X^5 - X - \frac{1}{16} \in \mathbb{Q}[X]$	251
FJ09-I-4	$f(x + d)$ kein Eisenstein-Polynom	264

Sonstiges

H03-III-2	Matrizenring	63
FJ04-III-4	$\{f \in \mathbb{R}[x] \mid f(a_i) = f'(a_i) = 0 \text{ für } i = 1, \dots, n\}$	89
FJ05-I-2	Äquivalenzrelation auf der Menge der Ideale	111
FJ05-II-3	Ideale in $R \times S$	120
H05-I-3	\mathbb{Z} -Basis von $\mathbb{Z}[\zeta]$	129
FJ06-II-6	maximales Ideal, R/M^n	157
H06-II-4	$\mathbb{Z}/99\mathbb{Z}$	180
H06-III-1	$\mathbb{Z}[\sqrt{13}]$	182
FJ07-I-4	in Hauptidealringen sind Primideale maximal	192
FJ07-II-3	Gauß'sches Lemma	198
H07-I-3	Einheitengruppe	209
H07-II-3	$K[X, Y]$	216
H08-III-1	Einheiten und Nullteiler	252
FJ09-I-3	Einheiten in $\mathbb{Z}/8\mathbb{Z}[t]$	264
FJ09-II-3	nilpotente Elemente	268
FJ09-III-1	Ringhomomorphismen $\mathbb{Q}[X]/(f) \rightarrow \mathbb{C}$	270
FJ09-III-2	maximales Ideal in $\mathbb{Z}[\sqrt{11}]$	271
H09-I-4	$P^3 - P + 2$ durch $X^4 - 7$ teilbar	278
H09-II-1	maximales Ideal in $\mathbb{Z}[X]$	279
H09-II-4	$\mathbb{Q}[X, Y]/I$ für $I = (X^3 - 7, (X + Y)^2 + (X + Y) + 1)$	283

Körper

H03-I-2	$\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$	51
H03-II-2	Normale Erweiterung von \mathbb{Q} mit ungeradem Grad ist Teilkörper von \mathbb{R}	56
FJ04-I-4	zueinander konjugierte Zwischenkörper	75
FJ04-I-5	$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{1}{2}\varphi(n)$	77
FJ05-III-1	endliche Körpererweiterungen sind algebraisch	122
FJ05-III-2	Körper mit 16 Teilkörpern	
H06-II-2	Minimalpolynom von $y := \frac{1}{x}$	175
H06-II-3	$\mathbb{Q}[X]/(X^4 + 2X^3 + X^2 + 2X + 1)$	177
H06-III-3	$\mathbb{Q}(\sqrt{m}) \cong \mathbb{Q}(\sqrt{n}) \Rightarrow m = n$	183
H06-III-4	Kreisteilungspolynom als Produkt von irreduziblen Polynomen	184
FJ07-II-4	\mathbb{Q} -Basis von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$	199
FJ07-III-5	Zerfällungskörper von $X^4 - 3$ über \mathbb{Q}	205
H07-III-3	d -tes Kreisteilungspolynom	222
FJ08-I-1	Zwischenkörper von $\mathbb{Q} \subset \mathbb{Q}(\sqrt[17]{19})$	225
FJ08-III-3	$[E_k : K] \leq \frac{n!}{(n-k)!}$	237
H08-II-3	Zerfällungskörper von $f_\alpha(X) = X^3 + aX^2 + bX + c$	249
FJ09-II-4	$\mathbb{Q}(\sqrt[5]{3}, \sqrt{7})$	269

Endliche Körper

H03-I-4	Automorphismen auf \mathbb{F}_{81}	53
H03-II-3	Zerlegung von $X^{p^q} - X$	57
H03-III-3	$\mathbb{F}_2[X]/(f)$	65
FJ04-II-4	\mathbb{F}_{256}	84
FJ04-III-2	Galoisgruppe von $x^4 + x^3 + x^2 + x + 1$ über \mathbb{F}_2	87
H04-I-5	\mathbb{F}_{27}	96
FJ05-II-4	Irreduzible Polynome über \mathbb{F}_p	120
H06-I-1	Inverses von $X^2 - 2X + 2$ in $(\mathbb{Q}[X]/(X^3 - X + 2))^\times$	165
FJ07-III-1	primitive Elemente von \mathbb{F}_{2^8} über \mathbb{F}_2	202
FJ07-III-2	$\mathbb{F}_2[X]/(1 + X + X^2 + X^3 + X^4)$	202
FJ07-III-4	Körper mit multiplikativer Gruppe, die $\mathbb{Z}/63\mathbb{Z}$ enthält	204
H07-II-4	irreduzible Polynome vom Grad p^2 über \mathbb{F}_q	217
H07-III-5	Abbildungen $\mathbb{F}_q \rightarrow \mathbb{F}_q$	223
FJ08-I-3	Minimalpolynome der Elemente von \mathbb{F}_8 über \mathbb{F}_2	228

FJ08-I-4	primitive Elemente von \mathbb{F}_{81} über \mathbb{F}_3	229
H08-I-1	Äquivalente Aussagen in \mathbb{F}_p	241

Galoistheorie

H03-III-4	Zwischenkörper von $\mathbb{Q}(X^2 + X^{-2}) \leq \mathbb{Q}(X)$	67
FJ04-I-3	Galoiserweiterung vom Grad 225	74
FJ04-II-3	$\text{Gal}\left(\mathbb{Q}(e^{\frac{2\pi i}{9}}) \mid \mathbb{Q}(e^{\frac{2\pi i}{3}})\right)$	82
H04-I-4	Galoisgruppe von $X^4 - 4X^3 + 4X^2 - 2$ über \mathbb{Q}	94
H04-II-5	quadratischer Teilkörper von $\mathbb{Q}(\zeta_5)$	103
H04-III-3	Galoisgruppe von $X^5 - 4X + 2$ über \mathbb{Q}	106
FJ05-I-5	Diskriminante von $X^4 + 2aX^2 + b$	115
FJ05-III-5	Galoisgruppe von $X^n - a$	125
H05-I-4	Zerfällungskörper von $X^7 + 1 - i$ über \mathbb{Q}	132
FJ06-I-1	f hat nur reelle Nullstellen, wenn die Galoisgruppe ungerade Ordnung hat	147
FJ06-II-4	Körpererweiterung mit Galoisgruppe S_n	155
FJ06-III-5	Galoiserweiterung mit Galoisgruppe $\mathbb{Z}/4\mathbb{Z}$	162
FJ06-III-6	$K\left(\bigcup_{\sigma \in G} \sigma(L)\right)$	163
H06-I-3	Galoisgruppe von $X^3 - 7$ über \mathbb{Q}	169
FJ07-I-3	Galoisgruppe von $(X^2 - 3)(X^3 + 5)$ über \mathbb{Q}	190
FJ07-II-5	Galoisgruppe von $X^3 - 3X^2 + 5$ über \mathbb{Q}	200
H07-I-4	Galoisgruppe von $M \mid K$ isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$	210
H07-I-5	Galoisgruppe von $X^3 - 3X + 1$ über \mathbb{Q}	210
H07-II-5	Galoisgruppe der Ordnung 85	218
H07-III-4	Galoisgruppe von f mit $f(X) = h(X^2)$	222
FJ08-III-4	Galoisgruppe von $E = \mathbb{Q}(\sqrt{5}) \cdot \mathbb{Q}(i\sqrt{5})$ über \mathbb{Q}	239
H08-I-3	Galoisgruppe von $T^4 + 1$ über \mathbb{Q}	244
H08-II-4	Galoisgruppe von $X^5 - X - \frac{1}{16}$	251
H08-III-4	Galoisgruppe von $\mathbb{Q}[\sqrt[p]{2}, e^{\frac{2\pi i}{p}}] \mid \mathbb{Q}$	255
FJ09-III-4	Galoisgruppe von $X^{15} - 10$ über \mathbb{Q}	273
H09-III-3	Galoisgruppe der normalen Hülle von $\mathbb{Q}\left(\sqrt{8 + 3\sqrt{7}}\right) / \mathbb{Q}$	289
H09-III-4	Galoisgruppe von $X^5 - 777X + 7$	291

Zahlentheorie

H04-I-2	$n^2 \equiv 500 \pmod{1000}$	93
H04-III-2	$x^2 - ay^2 \equiv b \pmod{p}$	105

FJ05-I-1	$4n + 3$ als Summe zweier Quadrate	111
FJ05-III-3	Umkehrung von $\phi : \mathbb{Z}/1000\mathbb{Z} \rightarrow \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$	123
FJ05-III-4	$x^2 + 91y = 5$	124
H05-I-1	unendlich viele Primzahlen, $\text{ggT}(77n + 1, 143n + 2)$	127
FJ06-II-2	5 quadratischer Rest für $10n + k$	152
FJ06-III-1	unendlich viele $n \in \mathbb{N}$ mit $m \mid \varphi(n)$	158
H06-III-1	$\left \frac{p}{q} - \frac{x}{y} \right < \frac{1}{y^2}$	182
H07-I-1	$4^{2n+1} + 3^{n+2}$ durch 13 teilbar	207
H07-III-2	n Teiler von $(n - 1)!$	221
FJ08-I-5	$x^2 \equiv a \pmod{42}$	230
H09-I-1	$1 + 2 + 3 + \dots + n$ Teiler von $n!$	275

Konstruktionen mit Zirkel und Lineal

H03-I-3	$e^{\frac{2\pi i}{13}}$ konstruierbar	52
FJ05-II-5	Fünfeck, Siebeneck	121
H05-III-4	zu einem Dreieck flächengleiches Quadrat	143

Lineare Algebra

H05-III-3	$X^7 = \mathbb{1}_5$	142
FJ07-I-2	Eigenraum des Frobenius-Homomorphismus	189
H07-III-5	polynomiale Abbildung	223
H09-I-2	K -Vektorraum der $n \times n$ -Matrizen	276

Teil I.
Grundlagen

In diesem ersten Teil sind alle Definitionen und Sätze formuliert, deren Kenntnis in den vergangenen Jahren zur Lösung der Examensaufgaben notwendig und hilfreich war. Dabei wurden die Sätze häufig nicht in ihrer allgemeinsten Fassung, sondern so aufgeschrieben, wie sie in den in Teil II vorgestellten Lösungsvorschlägen verwendet werden.

Diese Grundlagen sollten zum größten Teil aus den Vorlesungen bekannt sein. Sie sind ohne weitere Erklärungen und anschauliche Beispiele aufgeführt. Sollte das Verständnis einer Auffrischung bedürfen, wird hier auf die Literaturvorschläge (Seite 293) verwiesen.

Sicherlich gibt es in der Algebra noch viele andere schöne Sätze und interessante Themen. Es kann auch nicht ausgeschlossen werden, dass diese in den kommenden Prüfungsterminen eine Rolle spielen. Die Sammlung erhebt insofern keinerlei Anspruch auf Vollständigkeit. Trotzdem kann wohl davon ausgegangen werden, dass ein Großteil der üblicherweise im Examen abgefragten Grundlagen von dieser Zusammenstellung abgedeckt wird.

Der erste Teil gliedert sich in sechs Kapitel zu sechs Themenblöcken, die sich inhaltlich gut voneinander abgrenzen lassen. Es empfiehlt sich, die Lernphase gemäß dieser Themenblöcke zu organisieren. Die zugehörigen Aufgaben sind im Themenverzeichnis (Seite xiii) aufgeführt.



1. Gruppen

Definition 1.1 Eine nichtleere Menge G zusammen mit einer Abbildung $\circ : G \times G \rightarrow G$ heißt eine **Gruppe**, falls gilt:

- i) Für alle $g, h, l \in G$ ist $g \circ (h \circ l) = (g \circ h) \circ l$.
- ii) Es existiert ein $e \in G$, so dass $e \circ g = g = g \circ e$ für alle $g \in G$ gilt.
- iii) Zu jedem $g \in G$ existiert ein $h \in G$ mit $g \circ h = e$.

Ist nur i) erfüllt, so heißt G eine **Halbgruppe**.

Gilt zusätzlich

- iv) $g \circ h = h \circ g$ für alle $g, h \in G$,

so heißt (G, \circ) eine **kommutative** oder **abelsche** Gruppe.

Definition 1.2 Ist (G, \circ) eine Gruppe, so heißt das Element $e \in G$, für das $e \circ g = g = g \circ e$ für alle $g \in G$ gilt, **neutrales Element** von G . Für $g \in G$ heißt das Element $h \in G$, für das $g \circ h = e$ gilt, das **zu g inverse Element** oder **Inverses von g** und wird mit g^{-1} bezeichnet.

Definition 1.3 Eine nichtleere Teilmenge U einer Gruppe G heißt **Untergruppe** von G , falls $g \circ h^{-1} \in U$ für alle $g, h \in U$ gilt.

Definition 1.4 Eine Untergruppe U einer Gruppe G heißt **maximale Untergruppe** von G , falls für alle Untergruppen $V \subseteq G$, die $U \subseteq V$ erfüllen, $U = V$ oder $V = G$ gilt.

Definition 1.5 Die Anzahl der Elemente einer Gruppe G heißt **Ordnung** von G und wird mit $|G|$ bezeichnet. Ist $|G| < \infty$, so heißt G **endlich**.

Definition 1.6 Seien (G, \cdot) und (H, \circ) Gruppen. Ein **Gruppenhomomorphismus** ist eine Abbildung $\varphi : G \rightarrow H$, die $\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$ für alle $x, y \in G$ erfüllt.

Definition 1.7 Ein Gruppenhomomorphismus $\varphi : G \rightarrow H$ heißt

- i) **Endomorphismus**, falls $H = G$ gilt.
- ii) **Isomorphismus**, falls φ bijektiv ist.
- iii) **Automorphismus**, falls $H = G$ gilt und φ bijektiv ist.

Definition 1.8 Die identische Abbildung $\text{id} : G \rightarrow G$ mit $\text{id}(x) = x$ wird auch **trivialer Automorphismus** genannt.

Definition 1.9 Zwei Gruppen G und H heißen **isomorph**, falls es einen Isomorphismus $\varphi : G \rightarrow H$ gibt. Wir schreiben dann $G \cong H$.

Definition 1.10 Ist $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus und e das neutrale Element von H , so heißt $\{g \in G \mid \varphi(g) = e\}$ der **Kern** von φ und wird mit $\ker(\varphi)$ oder auch $\text{Kern}(\varphi)$ bezeichnet.

Die Menge $\{h \in H \mid \varphi(x) = h \text{ für ein } x \in G\}$ heißt das **Bild** von φ und wird mit $\text{Bild}(\varphi)$ oder auch $\text{im}(\varphi)$ bezeichnet.

Ist X eine Teilmenge von H , so heißt die Menge $\{g \in G \mid \varphi(g) \in X\}$ das **Urbild von X** unter φ und wird mit $\varphi^{-1}(X)$ bezeichnet.

Satz 1.11 Ein Gruppenhomomorphismus $\varphi : G \rightarrow H$ ist genau dann injektiv, wenn der Kern von φ nur aus dem neutralen Element von G besteht.

Satz 1.12 Sei G eine endliche Gruppe und $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist $\text{im}(\varphi)$ eine Untergruppe von H , $\ker(\varphi)$ eine Untergruppe von G und es gilt $|G| = |\text{im}(\varphi)| \cdot |\ker(\varphi)|$.

Satz 1.13 Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus, sei e_G das neutrale Element von G und e_H das neutrale Element von H . Dann ist $\varphi(e_G) = e_H$ und das zu einem Element $g \in G$ inverse Element g^{-1} wird durch φ auf das Inverse des Bildes von g abgebildet.

Definition 1.14 Sei G eine Gruppe und X eine nichtleere Teilmenge von G . Die Menge

$$\langle X \rangle := \{x_1 \cdot \dots \cdot x_l \mid l \in \mathbb{N}, x_i \in X \vee x_i^{-1} \in X, 1 \leq i \leq l\}$$

ist eine Untergruppe von G und heißt **die von X erzeugte Untergruppe**. Ist U eine Untergruppe von G und X eine Teilmenge von G mit $U = \langle X \rangle$, so heißt X ein **Erzeugendensystem von U** .

Definition 1.15 Sei G eine Gruppe. Die Untergruppe $\{\{ghg^{-1}h^{-1} \mid g, h \in G\}\}$ heißt **Kommutatorgruppe von G** .

Satz 1.16 Sei G eine Gruppe und X ein Erzeugendensystem von G .

- a) Gilt $ab = ba$ für alle $a, b \in X$, so ist G abelsch.
- b) Stimmen zwei Gruppenhomomorphismen $\varphi, \psi : G \rightarrow H$ auf X überein, so gilt $\varphi = \psi$.

1.1. Zyklische Gruppen

Definition 1.17 Sei G eine Gruppe und g ein Element in G . Die Ordnung der von $\{g\}$ erzeugten Untergruppe heißt **Ordnung von g** . Man schreibt dafür $\text{ord}(g)$. Die von $\{g\}$ erzeugte Untergruppe wird mit $\langle g \rangle$ bezeichnet. Falls es ein $g \in G$ gibt mit $G = \langle g \rangle$, heißt G **zyklisch**.

Satz 1.18 Sei G eine Gruppe mit neutralem Element e und sei $g \in G$. Gibt es ein $a \in \mathbb{N} \setminus \{0\}$ mit $g^a = e$, so ist $\text{ord}(g)$ ein Teiler von a .

Satz 1.19 Ist p eine Primzahl und G eine Gruppe der Ordnung p , so ist G zyklisch.

Satz 1.20 Untergruppen zyklischer Gruppen sind zyklisch.

Satz 1.21 Ist $G = \langle z \rangle$ eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$, so ist

$$\begin{aligned} \varphi : \mathbb{Z}/n\mathbb{Z} &\rightarrow G \\ a + (n) &\mapsto z^a \end{aligned}$$

ein Isomorphismus von Gruppen. Bis auf Isomorphie gibt es also genau eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$.

Satz 1.22 Zyklische Gruppen sind abelsch.

Definition 1.23 Sei $n \in \mathbb{N}$. Die Anzahl der zu n teilerfremden Zahlen $m \in \mathbb{N}$ mit $1 \leq m \leq n$ wird mit $\varphi(n)$ bezeichnet. Die Funktion $\varphi : \mathbb{N} \rightarrow \mathbb{N}$, $n \mapsto \varphi(n)$ heißt **Eulersche Phi-Funktion**.

Satz 1.24 Sei φ die Eulersche Phi-Funktion.

- a) Für eine Primzahl p und eine natürliche Zahl $k > 0$ gilt

$$\varphi(p^k) = p^k - p^{k-1}.$$

- b) Für die Primfaktorzerlegung einer natürlichen Zahl $n = p_1^{k_1} \cdots p_l^{k_l}$ gilt

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_l^{k_l}).$$

- c) Es gilt die Summenformel

$$n = \sum_{d|n, d \geq 1} \varphi(d).$$

Satz 1.25 Sei G eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ und φ die Eulersche Phi-Funktion. Dann hat G genau $\varphi(n)$ erzeugende Elemente, also $\varphi(n)$ Elemente der Ordnung n .

Satz 1.26 Sei G eine endliche Gruppe. Ist G abelsch, so gibt es zu jedem Teiler der Gruppenordnung eine Untergruppe dieser Ordnung. Ist G zyklisch, so gibt es zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung.

Definition 1.27 Sei G eine Gruppe. Die Menge aller Automorphismen auf G mit der Hintereinanderausführung als Verknüpfung ist eine Gruppe und heißt **Automorphismengruppe** von G . Sie wird mit $\text{Aut}(G)$ bezeichnet.

Satz 1.28 Die Automorphismengruppe der zyklischen Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ist isomorph zur Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$ (vgl. 2.11).

Satz 1.29 Seien $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$. Dann gilt

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m \cdot n)\mathbb{Z}.$$

Satz 1.30 (Hauptsatz über endliche abelsche Gruppen)

Sei G eine endliche abelsche Gruppe. Dann gibt es zyklische Untergruppen Z_1, \dots, Z_r von G mit $G \cong Z_1 \times \dots \times Z_r$. Die Ordnungen der Z_i sind Primzahlpotenzen. Die Anzahl der zyklischen Untergruppen einer gegebenen Ordnung ist dabei eindeutig bestimmt.

1.2. Normalteiler und Faktorgruppen

Definition 1.31 Sei G eine Gruppe und U eine Untergruppe von G . Die Menge $gU := \{gu \mid u \in U\}$ heißt **Linksnebenklasse von g bezüglich U** . Die Menge $Ug := \{ug \mid u \in U\}$ heißt **Rechtsnebenklasse von g bezüglich U** . Die Anzahl der Linksnebenklassen ist gleich der Anzahl der Rechtsnebenklassen bezüglich U und heißt **Index von U in G** . Der Index wird mit $[G : U]$ bezeichnet.

Definition 1.32 Sei Y eine endliche Menge, seien X_1, \dots, X_n Teilmengen von Y . Man sagt, X_1, \dots, X_n bilden eine **Partition** von Y , falls die Teilmengen paarweise disjunkt sind und $Y = X_1 \cup \dots \cup X_n$ gilt.

Satz 1.33 Sei G eine endliche Gruppe und U eine Untergruppe von G . Dann bilden die Rechtsnebenklassen (bzw. die Linksnebenklassen) von U eine Partition von G .

Satz 1.34 (Lagrange)

Ist U Untergruppe einer endlichen Gruppe G , dann gilt $|G| = [G : U] \cdot |U|$.

Definition 1.35 Sei G eine Gruppe und U eine Teilmenge von G . Die Menge U heißt **Normalteiler** von G , wenn U eine Untergruppe von G ist und eine der folgenden äquivalenten Bedingungen erfüllt ist:

- i) Für alle $g \in G$ gilt $gUg^{-1} \subseteq U$.

- ii) Für alle $g \in G$ gilt $gUg^{-1} = U$.
- iii) Für alle $g, h \in G$ gilt $(gU)(hU) = ghU$.
- iv) Für alle $g \in G$ gilt $gU = Ug$.

Satz 1.36 Jede Gruppe G hat mindestens zwei Normalteiler, nämlich $\{e\}$ und G . Diese beiden Normalteiler werden als triviale Normalteiler bezeichnet.

Satz 1.37 Ist G eine abelsche Gruppe, so ist jede Untergruppe von G Normalteiler von G .

Satz 1.38 Ist N Normalteiler einer Gruppe G , so bilden die Nebenklassen von N mit der Verknüpfung

$$(gN)(hN) = ghN$$

eine Gruppe. Sie heißt **Faktorgruppe von G modulo N** und wird mit G/N bezeichnet.

Satz 1.39 Sei G eine endliche Gruppe und N ein Normalteiler von G . Dann gilt $|G| = |N| \cdot |G/N|$.

Definition 1.40 Sei G eine Gruppe und N ein Normalteiler von G . Dann ist die Abbildung $\varepsilon : G \rightarrow G/N$ definiert durch $g \mapsto gN$ ein surjektiver Homomorphismus. Er heißt der **kanonische Epimorphismus** von G auf G/N .

Definition 1.41 Eine Gruppe G , die keine Normalteiler außer $\{e\}$ und G hat, heißt **einfach**.

Satz 1.42 Sei G eine Gruppe und $(N_i)_{i \in I}$ eine Familie von Normalteilern von G . Dann ist $\bigcap_{i \in I} N_i$ ein Normalteiler von G .

Satz 1.43 Sei G eine Gruppe und U eine endliche Untergruppe von G . Ist U die einzige Untergruppe der Ordnung $|U|$ von G , dann ist U ein Normalteiler von G .

Satz 1.44 Sei G eine endliche Gruppe und U eine Untergruppe von G . Ist U vom Index 2 in G , dann ist U ein Normalteiler von G .
Allgemeiner gilt: Ist p der kleinste Primteiler von $|G|$ und U eine Untergruppe vom Index p in G , dann ist U ein Normalteiler von G .

Satz 1.45 Sei G eine endliche Gruppe und U eine echte Untergruppe von G . Ist $|G|$ kein Teiler von $[G : U]!$, so besitzt G einen nichttrivialen Normalteiler, ist also nicht einfach.

Definition 1.46 Sei G eine Gruppe und X eine nichtleere Teilmenge von G . Die Menge $N_G(X) := \{g \in G \mid gXg^{-1} = X\} = \{g \in G \mid gX = Xg\}$ heißt **Normalisator** von X in G .

Satz 1.47 Sei G eine Gruppe. Für eine Teilmenge X von G ist $N_G(X)$ eine Untergruppe von G . Für eine Untergruppe U ist $N_G(U)$ die größte Untergruppe von G , von der U Normalteiler ist. Für einen Normalteiler N von G ist $N_G(N) = G$.

Definition 1.48 Sei G eine Gruppe. Für eine nichtleere Teilmenge X und eine Untergruppe H von G heißt $Z_H(X) := \{g \in H \mid gx = xg \text{ für alle } x \in X\}$ **Zentralisator** von X in H und $Z(G) := \{g \in G \mid gh = hg \text{ für alle } h \in G\}$ heißt **Zentrum** von G . Das Zentrum heißt **trivial**, wenn $Z(G) = \{e\}$ gilt.

Satz 1.49 Sei G ein Gruppe. Für eine Teilmenge X und eine Untergruppe H von G ist der Zentralisator $Z_H(X)$ eine Untergruppe von G . Das Zentrum von G ist ein Normalteiler von G .

Satz 1.50 Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus.

- Ist U eine Untergruppe von G , so ist $\varphi(U)$ eine Untergruppe von H . Ist $U = \langle X \rangle$, so ist $\varphi(U) = \langle \varphi(X) \rangle$.
- Ist V eine Untergruppe von H , so ist $\varphi^{-1}(V)$ eine Untergruppe von G .
- Ist φ surjektiv und N ein Normalteiler von G , so ist $\varphi(N)$ ein Normalteiler von H .
- Ist N ein Normalteiler von H , so ist $\varphi^{-1}(N)$ ein Normalteiler von G .
- Der Kern von φ ist ein Normalteiler von G .

Satz 1.51 (Universelle Eigenschaft der Faktorgruppe)

Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus und sei N ein Normalteiler von G mit $N \subseteq \ker(\varphi)$. Dann gibt es genau einen Homomorphismus $\bar{\varphi} : G/N \rightarrow H$ mit $\bar{\varphi} \circ \varepsilon = \varphi$, wobei $\varepsilon : G \rightarrow G/N$ den kanonischen Epimorphismus von G auf G/N bezeichne.

Satz 1.52 (Homomorphiesatz)

Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist

$$\begin{aligned} \bar{\varphi} : G / \ker(\varphi) &\rightarrow H \\ g \ker(\varphi) &\mapsto \varphi(g) \end{aligned}$$

injektiv. Insbesondere ist $G / \ker(\varphi) \cong \text{im}(\varphi)$.

Satz 1.53 (Erster Isomorphiesatz)

Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler von G . Dann ist HN eine Untergruppe von G mit Normalteiler N und $H \cap N$ ist ein Normalteiler von H . Weiter ist $H / (H \cap N) \cong HN / N$.

Satz 1.54 (Zweiter Isomorphiesatz)

Sei G eine Gruppe und seien N, H Normalteiler von G mit $N \subseteq H$. Dann ist N ein Normalteiler von H , H/N ein Normalteiler von G/N und es gilt $(G/N)/(H/N) \cong G/H$.

Satz 1.55 (Dritter Isomorphiesatz)

Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus, M ein Normalteiler von H und $N := \varphi^{-1}(M)$. Dann gibt es einen injektiven Homomorphismus $\Phi : G/N \rightarrow H/M$. Falls φ surjektiv ist, ist Φ ein Isomorphismus.

Satz 1.56 (Korrespondenzsatz)

Sei G eine Gruppe und N ein Normalteiler von G . Die Untergruppen (bzw. Normalteiler) von G/N entsprechen bijektiv den Untergruppen (bzw. Normalteilern) von G , die N enthalten. Der zugehörige Isomorphismus ist der kanonische Epimorphismus $\varepsilon : G \rightarrow G/N$.

Definition 1.57 Eine endliche Gruppe G heißt **auflösbar**, wenn es Untergruppen U_0, \dots, U_l von G gibt, für die gilt:

- i) $G = U_0 \supset U_1 \supset \dots \supset U_l = \{e\}$,
- ii) U_{i+1} ist ein Normalteiler von U_i für $i = 0, \dots, l-1$ und
- iii) U_i/U_{i+1} ist abelsch für alle $i = 0, \dots, l-1$.

Satz 1.58 Abelsche Gruppen sind auflösbar.

Satz 1.59 Ist eine Gruppe G auflösbar, so ist jede Untergruppe und jede Faktorgruppe von G auflösbar.

Satz 1.60 Sei N ein Normalteiler einer Gruppe G . Die Gruppe G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

1.3. Gruppenoperationen

Definition 1.61 Sei G eine Gruppe und M eine Menge. Man sagt, G **operiert auf M mittels γ** , falls es eine Abbildung $\gamma : G \times M \rightarrow M$ gibt, für die gilt:

- i) $\gamma(e_G, m) = m$ für alle $m \in M$;
- ii) $\gamma(g, \gamma(h, m)) = \gamma(gh, m)$ für alle $g, h \in G$ und $m \in M$.

Eine solche Abbildung heißt **(Gruppen-)Operation** von G auf M .

Satz 1.62 Die Gruppenoperationen $G \times M \rightarrow M$ entsprechen bijektiv den Gruppenhomomorphismen $G \rightarrow S_M$. Genauer gilt:

a) Ist $\gamma : G \times M \rightarrow M$ eine Gruppenoperation, so ist

$$\begin{aligned}\varphi : G &\rightarrow S_M \\ g &\mapsto \gamma_g\end{aligned}$$

mit $\gamma_g : M \rightarrow M, m \mapsto \gamma(g, m)$ ein Gruppenhomomorphismus.

b) Ist $\varphi : G \rightarrow S_M$ ein Gruppenhomomorphismus, so definiert

$$\begin{aligned}\gamma : G \times M &\rightarrow M \\ (g, m) &\mapsto \varphi(g)(m)\end{aligned}$$

eine Gruppenoperation von G auf M .

Definition 1.63 Man spricht von einer trivialen Operation $G \times M \rightarrow M$, wenn $(g, m) \mapsto m$ für alle $(g, m) \in G \times M$ gilt, also wenn der zur Operation gehörige Gruppenhomomorphismus $G \rightarrow S_M$ konstant ist.

Satz 1.64 (Satz von Cayley)

Jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n .

Definition 1.65 Sei G eine Gruppe, M eine Menge und $\gamma : G \times M \rightarrow M$ eine Gruppenoperation.

- a) Für $m \in M$ heißt $B_m = \{\gamma(g, m) \mid g \in G\}$ die **Bahn von m** unter γ .
- b) Die Operation γ heißt **transitive Operation**, falls es nur eine Bahn gibt, d.h. falls $B_m = M$ für alle $m \in M$ gilt.
- c) Für $m \in M$ ist die Menge $G_m = \{g \in G \mid \gamma(g, m) = m\}$ eine Untergruppe von G . Sie heißt **Fixgruppe** oder **Stabilisator von m** .

Satz 1.66

Sei G eine endliche Gruppe und $\gamma : G \times M \rightarrow M$ eine Gruppenoperation. Für alle $m \in M$ gilt $|G| = |B_m| \cdot |G_m|$.

Satz 1.67 (Bahnengleichung)

Eine Gruppe G operiere auf einer Menge M durch γ . Seien B_{m_1}, \dots, B_{m_l} die verschiedenen Bahnen unter γ . Dann bilden die Bahnen B_{m_1}, \dots, B_{m_l} eine Partition von M und es gilt $|M| = \sum_{j=1}^l |B_{m_j}|$.

Satz 1.68 Eine Gruppe G operiert genau dann transitiv auf einer Menge M durch γ , wenn es für alle $m_1, m_2 \in M$ ein $g \in G$ gibt mit $\gamma(g, m_1) = m_2$.