Grundlehren der
mathematischen Wissenschaften 134

A Series of Comprehensive Studies in Mathematics

B. Huppert

Endliche Gruppen I

Nachdruck der ersten Auflage

B. Huppert

Endliche Gruppen I

Nachdruck der ersten Auflage

Springer-Verlag
Berlin Heidelberg New York 1979

Bertram Huppert
Fachbereich Mathematik der Universität Mainz
Saarstraße 21
D-6500 Mainz

ISBN 3-540-03825-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-03825-6 Springer-Verlag New York Heidelberg Berlin

Library of Congress Catalog Card Number 66-18717. Printed in Germany

Satzarbeiten: Brühlsche Universitätsdruckerei, Lahn-Gießen. Druck: fotokop wilhelm weihert KG, Darmstadt. Bindearbeiten: K. Triltsch, Würzburg.
2141/3140-543210

Vorwort

Als ich im Jahre 1958 mit den Vorarbeiten zu diesem Buch begann, schien es noch möglich, eine einigermaßen vollständige Darstellung der Strukturtheorie endlicher Gruppen in einem Bande zu geben. Die stürmische Entwicklung, welche die Theorie seitdem erlebt hat (das Literaturverzeichnis gibt einen Eindruck davon), hat diese Zielsetzung unmöglich gemacht. Der vorliegende erste Band enthält neben den Grundbegriffen die Theorie der nilpotenten, p-nilpotenten und auflösbaren Gruppen sowie die gewöhnliche Darstellungstheorie. Da die Entwicklung der letzten Jahre nicht in diesen Gebieten ihren Schwerpunkt hatte, konnte hier ein ziemlich vollständiger Überblick über den gegenwärtigen Stand der Theorie gegeben werden. (Die in den allerletzten Jahren entstandene Theorie der Formationen und Fittingklassen konnte nur noch zum Teil aufgenommen werden.) Der zweite Band soll die Theorie der subnormalen Untergruppen, die feinere Theorie der p-Länge, mehrfach transitive Permutationsgruppen und einige neuere Anwendungen der Charaktertheorie enthalten. Wegen der Fülle der Ergebnisse der letzten Jahre kann dabei keine Vollständigkeit mehr angestrebt werden.

Einige Teilgebiete wurden ausgeschlossen:

1. Eine einheitliche Behandlung der heute bekannten Serien von einfachen endlichen Gruppen nach der Methode von CHEVALLEY hätte umfangreiche Vorkenntnisse über Liesche Algebren erfordert. Ich habe mich in Kap. II auf die projektiven und symplektischen Gruppen beschränkt. Die einfachen Gruppen von MATHIEU und SUZUKI werden erst in Band 2 behandelt werden.

2. Die Theorie der p-Gruppen vom Exponenten p und die dazu benötigten Zusammenhänge zwischen nilpotenten Gruppen und Lieschen Ringen wurden nicht berührt. Diese Theorie hat sachlich und methodisch nur wenige Verbindungen zu den übrigen Fragen der Strukturtheorie endlicher Gruppen, und ihre Anwendungen liegen auch weitgehend in der Theorie der unendlichen Gruppen.

3. Die Kohomologietheorie endlicher Gruppen fand bisher ihre wichtigste Anwendung in der Klassenkörpertheorie und nicht in der Strukturtheorie endlicher Gruppen. Daher habe ich in I, § 19 (unter Verzicht auf die funktorielle Beschreibung der Kohomologiegruppen) nur so viel an Kohomologietheorie entwickelt, wie für einige in diesem Buch behandelte Fragen (Erweiterungstheorie, Automorphismen von p-Gruppen, Schurscher Multiplikator) zweckmäßig erschien.

Obwohl dieses Buch keine Vorkenntnisse über Gruppen erfordert, wendet es sich doch an einen Leser mit algebraischen Grundkenntnissen. Die Grundbegriffe und elementaren Hilfsmittel der Gruppentheorie werden in Kap. I vollständig, jedoch knapp und ohne Motivierung entwickelt. Ringtheoretische Hilfsmittel, wie die Theorie der Hauptidealringe (I, § 13) und der halbeinfachen Algebren (V, § 2—4) werden vollständig dargestellt. Hingegen habe ich gelegentlich einfache Sätze über p-adische Körper und algebraische Zahlkörper ohne Beweis herangezogen.

Ich habe nicht versucht, das Buch gleichmäßig mit Aufgaben zu versehen. In Kap. I werden zahlreiche Bemerkungen und Beweisvarianten in den Aufgaben angeboten, jedoch bleiben in den späteren Kapiteln lange Strecken fast ohne Aufgaben. Die Aufgaben werden im Text nur ganz selten herangezogen.

Zahlreiche Helfer haben mich bei der Niederschrift dieses Buches unterstützt. R. Baer, N. Itô, O. H. Kegel und J. Rose haben verschiedene Fassungen einiger Kapitel kritisch gelesen. N. Blackburn und H. Lüneburg haben das vollständige Manuskript durchgesehen. Mit W. Gaschütz, F. Gross und J. Neubüser konnte ich fast alle Kapitel im Manuskript oder in der Fahnenkorrektur eingehend durchsprechen. Dies führte zu zahlreichen Verbesserungen und zur Vermeidung von Fehlern und Unklarheiten. Unveröffentlichte Ergebnisse, Beweise oder Beispiele verdanke ich N. Blackburn, R. Carter, E. Dade, W. Gaschütz, P. Hall, P. Roquette, D. Taunt, J. G. Thompson und H. Wielandt. Bei den langwierigen Korrekturen haben A. Brandis, K. Doerk, W. Gaschütz, K. D. Graf, F. Gross, B. Klaiber, J. Neubüser und A. Schlette geholfen. Allen diesen Helfern sei hier herzlich gedankt. Schließlich habe ich folgenden Institutionen zu danken, die mir Gelegenheit zur Arbeit an diesem Buch und zu fruchtbaren Gesprächen mit Kollegen gaben: dem British Council für einen Aufenthalt in Manchester 1958/59; der University of Illinois in Urbana für eine Gastprofessur 1963/64; dem California Institute of Technology in Pasadena für eine Gastprofessur im Herbst 1964. Endlich sei dem Verlag für sein großzügiges Eingehen auf meine umfangreichen Änderungswünsche

während der Korrekturen und für die gute Ausstattung des Buches gedankt.

Mein ganz besonderer Dank geht an meinen Lehrer HELMUT WIELANDT. Seine Vorlesungen, die mich mit der Theorie der endlichen Gruppen bekannt machten, waren oftmals der Ausgangspunkt für die Niederschrift von Paragraphen und ganzen Kapiteln dieses Buches. Sie haben in Stil und Stoffauswahl meine Darstellung immer wieder beeinflußt.

Mainz, den 15. 9. 1967 Bertram Huppert

Vorwort zum Nachdruck

10 Jahre nach Erscheinen des 1. Bandes ist dieser in vielen Teilen durch die stürmische Entwicklung der Theorie der endlichen Gruppen überholt worden. Das gilt ganz besonders für das Kapitel über auflösbare Gruppen. Mit kleineren Ergänzungen und Änderungen wäre nicht viel verbessert worden, zumal der hoffentlich in naher Zukunft erscheinende zweite Band manchen Nachtrag bringen wird. Ich habe mich daher für einen ungeänderten Nachdruck mit einem Verzeichnis der mir bekanntgewordenen Fehler entschlossen. Im Text sind die betroffenen Seiten mit einem Sternchen neben der Seitenzahl versehen. Reine Schreibfehler, die der Leser leicht erkennt, habe ich nicht in das Fehlerverzeichnis aufgenommen.

Zahlreiche Kollegen haben mich auf Fehler und Versehen hingewiesen. Ihnen allen möchte ich hiermit danken. Mein ganz besonderer Dank gilt Dr. John Rose (Newcastle), der ein umfangreiches Fehlerverzeichnis mit zahlreichen, wohlbegründeten Verbesserungsvorschlägen angefertigt hat.

Mainz, Mai 1979 Bertram Huppert

Symbolverzeichnis

$p^n \top a$: p ist eine Primzahl mit $p^n \mid a$ und $p^{n+1} \nmid a$.

(a, b) ist der größte gemeinsame Teiler der ganzen rationellen Zahlen a und b.

$V(n, K)$ ist der Vektorraum der Dimension n über dem kommutativen Körper K.

V^* ist der zu V duale Vektorraum und A^* die zur linearen Abbildung A transponierte Abbildung.

$\langle v_1, \ldots, v_n \rangle$ ist der von den Vektoren v_i aufgespannte Teilraum.

$GL(n, K)$, $PGL(n, K)$, $SL(n, K)$, $PSL(n, K)$
$GL(n, p^f)$, $PGL(n, p^f)$, $SL(n, p^f)$, $PSL(n, p^f)$ (II, 6.1; S. 177)

$\mathfrak{U} \leqq \mathfrak{G}$, $\mathfrak{U} < \mathfrak{G}$ (I, 2.1; S. 4)

$\mathfrak{U} \trianglelefteqq \mathfrak{G}$, $\mathfrak{U} \lhd \mathfrak{G}$ (I, 3.1; S. 12)

$\mathfrak{U} \lhd\lhd \mathfrak{G}$ (S. 308)

$E, \mathfrak{E}$ (I, 2.1; S. 4)

$|\mathfrak{M}|$ (I, 1.7; S. 4)

$|\mathfrak{G} : \mathfrak{U}|$ (I, 2.5; S. 5)

$\langle \mathfrak{M} \rangle$ (I, 2.4; S. 5)

M^a (I, 2.14; S. 9)

$\mathfrak{M}^a$ (I, 2.15; S. 9)

$\mathfrak{M}^{\mathfrak{G}}$ (I, 3.14; S. 18)

$\mathfrak{N}_{\mathfrak{G}}(\mathfrak{M})$, $\mathfrak{C}_{\mathfrak{G}}(\mathfrak{M})$ (I, 2.17; S. 10)

$\mathfrak{C}_{\mathfrak{G}}(\mathfrak{U}/\mathfrak{M})$ (I, 4.3; S. 19)

$O(G)$, $\mathfrak{Exp}\ \mathfrak{G}$ (I, 2.8; S. 7)

$[A, B]$, $[\mathfrak{A}, \mathfrak{B}]$
$\mathfrak{G}'$, $\mathfrak{G}''$, $\mathfrak{G}^{(n)}$ (I, 8.1; S. 37)

$k(\mathfrak{G})$ (I, 8.7; S. 39)

$\mathfrak{K}_i(\mathfrak{G})$, $\mathfrak{K}_\infty(\mathfrak{G})$ (III, 2.2; S. 259)

$c(\mathfrak{G})$ (III, 2.7; S. 262)

$\mathfrak{Z}(\mathfrak{G})$ (I, 2.17; S. 10)

$\mathfrak{Z}_i(\mathfrak{G})$, $\mathfrak{Z}_\infty(\mathfrak{G})$ (III, 2.2; S. 259)

$\Phi(\mathfrak{G})$ (III, 3.1; S. 268)

$\Omega_i(\mathfrak{G})$, $\mathfrak{O}_i(\mathfrak{G})$ (III, 10.4; S. 324)

$\mathfrak{F}(\mathfrak{G})$ (III, 4.2; S. 277)

$n(\mathfrak{G})$ (III, 4.7; S. 279)

$\mathfrak{F}_p(\mathfrak{G})$ (VI, 5.4; S. 686)

$l_p(\mathfrak{G})$ (VI, 6.1; S. 688)

$\mathfrak{A}(\mathfrak{G})$ (I, 4.1; S. 18)

$\mathfrak{I}(\mathfrak{G})$ (I, 4.2; S. 18)

$\bigtimes_i \mathfrak{G}_i$ (I, 9.1; S. 45)

$\mathfrak{A} \curlyvee \mathfrak{B}$ (I, 9.10; S. 49)

$\mathfrak{A} \curlywedge \mathfrak{B}$ (I, 9.11; S. 50)

$\mathfrak{A} \wr \mathfrak{B}$ (I, 15.1; S. 94)

$\mathfrak{A} \wr_r \mathfrak{B}$ (I, 15.5; S. 97)

$\mathfrak{A} \wr_{\mathfrak{U}} \mathfrak{B}$ (I, 15.10; S. 99)

Δ^a (I, 5.1; S. 24)

$\mathfrak{G}_a$, $\mathfrak{G}_\Delta$, $\mathfrak{G}^\Delta$, $\Delta^{\mathfrak{G}}$ (I, 5.9; S. 26)

$\operatorname{sgn} G$ (I, 5.4; S. 25)

$\mathfrak{S}[\mathfrak{G}]$ (I, 16.6; S. 105)

$\chi^{\mathfrak{G}}$, $V^{\mathfrak{G}}$, $\mathbf{D}^{\mathfrak{G}}$ (V, 16.1; S. 552)

$\chi_{\mathfrak{U}}$, $V_{\mathfrak{U}}$, $\mathbf{D}_{\mathfrak{U}}$ (V, 16.4; S. 555)

Inhaltsverzeichnis

Symbolverzeichnis XII

Kapitel I

Grundlagen

§ 1. Die Gruppenaxiome 2
§ 2. Untergruppen 4
§ 3. Normalteiler; Faktorgruppen und Homomorphismen 12
§ 4. Automorphismen 18
§ 5. Permutationsgruppen 24
§ 6. Darstellungen durch Permutationsgruppen 28
§ 7. Die Sylowschen Sätze 33
§ 8. Auflösbare Gruppen 37
§ 9. Direkte Produkte 45
§ 10. Operatorgruppen und Moduln 55
§ 11. Der Satz von Jordan-Hölder 62
§ 12. Direkte Zerlegungen 65
§ 13. Moduln über Hauptidealringen und abelsche Gruppen 70
§ 14. Erweiterungstheorie 86
§ 15. Kranzprodukte 94
§ 16. Kohomologietheorie 101
§ 17. Die Sätze von Gaschütz und Maschke 118
§ 18. Der Satz von Zassenhaus 126
§ 19. Freie Gruppen und definierende Relationen 133

Kapitel II

Permutationsgruppen und lineare Gruppen

§ 1. Primitive und mehrfach transitive Permutationsgruppen 145
§ 2. Reguläre Normalteiler mehrfach transitiver Permutationsgruppen . . . 154
§ 3. Primitive Permutationsgruppen mit abelschen Normalteilern 158
§ 4. Primitive Permutationsgruppen mit transitiven Untergruppen kleineren Grades 169
§ 5. Die symmetrischen und alternierenden Gruppen 173
§ 6. Lineare und projektive Gruppen 177
§ 7. Untergruppen von $PGL(n, p^l)$ 185
§ 8. Die Untergruppen von $PSL(2, p^l)$ 191
§ 9. Die symplektischen Gruppen 215
§ 10. Unitäre und orthogonale Gruppen 233

Kapitel III

Nilpotente Gruppen und p-Gruppen

§ 1. Kommutatoren und Kommutatorgruppen 252
§ 2. Zentralreihen und nilpotente Gruppen 259

§ 3. Die Frattinigruppe 268
§ 4. Die Fittinggruppe 276
§ 5. Minimale nichtnilpotente Gruppen 280
§ 6. Engelgruppen und engelsche Elemente 286
§ 7. Elementare Theorie der p-Gruppen 300
§ 8. Anzahlsätze 310
§ 9. Die Identitäten von P. Hall und Zassenhaus 315
§ 10. Reguläre p-Gruppen 321
§ 11. Metazyklische p-Gruppen 335
§ 12. Abelsche Normalteiler von p-Gruppen 341
§ 13. Spezielle und extraspezielle p-Gruppen 349
§ 14. p-Gruppen von maximaler Klasse 361
§ 15. Die p-Sylowgruppen der symmetrischen Gruppen $\mathfrak{S}_{p^n}$ 377
§ 16. Die p-Sylowgruppen der linearen Gruppen $GL(n, p^l)$ 381
§ 17. Binäre p-adische Gruppen 387
§ 18. Erzeugende und Relationen in p-Gruppen 395
§ 19. Automorphismen von p-Gruppen 403

Kapitel IV

Verlagerung und p-nilpotente Gruppen

§ 1. Monomiale Darstellungen und Verlagerung 412
§ 2. Einfache Anwendungen der Verlagerung 416
§ 3. Die Grünschen Sätze 422
§ 4. p-nilpotente Gruppen 427
§ 5. Minimale nicht p-nilpotente Gruppen 433
§ 6. Das p-Nilpotenzkriterium von Thompson 438
§ 7. Nilpotente Untergruppen 444
§ 8. Gruppen mit regulärer Sylowgruppe 447

Kapitel V

Darstellungstheorie

§ 1. Algebren und ihre Darstellungen 456
§ 2. Das Jacobson-Radikal 462
§ 3. Vollständig reduzible Moduln und halbeinfache Algebren 465
§ 4. Die Wedderburnschen Sätze 469
§ 5. Gruppencharaktere 474
§ 6. Charaktere abelscher Gruppen 487
§ 7. Die Sätze von Burnside, Wielandt und Frobenius 490
§ 8. Frobeniusgruppen 495
§ 9. Tensorprodukte von Moduln und Algebren 508
§ 10. Tensorprodukte von Darstellungen 515
§ 11. Zerfällungskörper 520
§ 12. Ganzzahlige Darstellungen und Konstantenreduktion 526
§ 13. Algebraisch konjugierte Charaktere 533
§ 14. Der Schursche Index 539
§ 15. Die Klassenzahl 549
§ 16. Induzierte Darstellungen 552

§ 17. Einschränkung von irreduziblen Darstellungen auf Normalteiler . . . 564
§ 18. Monomiale Darstellungen . . . 578
§ 19. Die Sätze von R. Brauer . . . 586
§ 20. Charaktere von Permutationsgruppen . . . 597
§ 21. Permutationsgruppen von Primzahlgrad . . . 607
§ 22. Involutionen . . . 618
§ 23. Schurscher Multiplikator und Darstellungsgruppen . . . 628
§ 24. Projektive Darstellungen . . . 638
§ 25. Berechnung des Schurschen Multiplikators . . . 641

Kapitel VI

Auflösbare Gruppen

§ 1. Hallgruppen auflösbarer Gruppen . . . 658
§ 2. Sylowsysteme auflösbarer Gruppen . . . 664
§ 3. Gruppen mit vielen Sylowsystemen . . . 667
§ 4. Produkte von nilpotenten Gruppen . . . 674
§ 5. Hauptreihen . . . 685
§ 6. Elementare Theorie der p-Länge . . . 688
§ 7. Formationen . . . 696
§ 8. Rang und Frattinigruppe . . . 711
§ 9. Überauflösbare Gruppen . . . 716
§ 10. Produkte von zyklischen Gruppen . . . 722
§ 11. Systemnormalisatoren auflösbarer Gruppen . . . 726
§ 12. Cartergruppen auflösbarer Gruppen . . . 736
§ 13. Gruppen, in denen die Systemnormalisatoren Cartergruppen sind . . . 743
§ 14. Auflösbare Gruppen mit lauter abelschen Sylowgruppen . . . 751
§ 15. Sylowsysteme und Cartergruppen . . . 761

Literaturverzeichnis . . . 769
Namenverzeichnis . . . 786
Sachverzeichnis . . . 789
Errata . . . 794

Kapitel I

Grundlagen

In Kapitel I entwickeln wir zunächst in knapper, aber vollständiger Form die Grundbegriffe der Gruppentheorie (§ 1–4). Diese Paragraphen enthalten zahlreiche elementare Sätze und Hilfssätze, welche später immer wieder herangezogen werden; dies trifft ganz besonders zu für den Produktsatz 2.12a), die Dedekind-Identität 2.12c), Hilfssatz 2.13 und die Sätze 4.5, 4.8 und 4.9. Die Darstellungen einer Gruppe als Permutationsgruppe (§ 6) liefern als wichtigste Folgerung die grundlegenden Sylowschen Sätze (§ 7). Einige elementare Auflösbarkeitskriterien werden aus den Sylowschen Sätzen in § 8 hergeleitet werden.

Die weiteren Paragraphen von Kapitel I sind vornehmlich den konstruktiven Verfahren der Theorie der endlichen Gruppen gewidmet: Direkte Produkte (§ 9 und 12), Erweiterungstheorie (§ 14), Kranzprodukte (§ 15). Neben das direkte Produkt stellen wir gleich zwei daraus abgeleitete Konstruktionen, nämlich das direkte Produkt mit vereinigten zentralen Untergruppen (9.10) und das direkte Produkt mit vereinigten Faktorgruppen (9.11). Auf die wichtige Frage, unter welchen Umständen sich eine vorgegebene Gruppe aus einfacheren Gruppen mittels eines der angegebenen Verfahren aufbauen läßt, gehen wir mehrfach ein. So gewinnen wir in § 13 als Spezialfall der Untersuchung von Moduln über Hauptidealringen den Fundamentalsatz für endlich erzeugbare, abelsche Gruppen. Von grundlegender Wichtigkeit für die ganze Theorie der endlichen Gruppen ist der Satz von Zassenhaus (§ 18), welcher gewisse Erweiterungen als semidirekte Produkte nachweist. Die Kohomologietheorie behandeln wir in § 16 nur in dem Umfang, welcher für die späteren Untersuchungen der Automorphismen von p-Gruppen (III, § 19) und die Behandlung des Schurschen Multiplikators (V, § 23) nützlich erscheint.

An mehreren Stellen war es zweckmäßig oder sogar notwendig, die Beschränkung auf endliche Gruppen aufzuheben. Die in den Paragraphen 9–13 entwickelte Theorie der direkten Produkte, Kompositionsreihen und direkten Zerlegungen von Gruppen mit Operatoren und von Moduln ist so angelegt, daß viele der in der Darstellungstheorie (Kapitel V) benötigten Sätze über Moduln als Spezialfälle darin enthalten sind. Bei der Beschreibung von Gruppen durch definierende Relationen in § 19 schließlich war ein Eingehen auf freie Gruppen völlig unvermeidlich.

Dem wenig erfahrenen Leser sei empfohlen, sich zuerst auf die Paragraphen 1—9 und 18 zu beschränken; einen Beweis von 17.5 ohne Verwendung der Hilfsmittel der Kohomologietheorie findet er in Aufgabe 70 skizziert.

§ 1. Die Gruppenaxiome

1.1 Gruppenaxiome. *Die nichtleere Menge $\mathfrak{G}$ heißt eine Gruppe, wenn folgende Bedingungen erfüllt sind:*

a) *Jedem geordneten Paar $\{A, B\}$ von Elementen A und B aus $\mathfrak{G}$ ist eindeutig ein drittes Element C aus $\mathfrak{G}$ zugeordnet. Wir schreiben $C = AB$ und nennen C das Produkt von A und B.*

b) *Für alle A, B, C aus $\mathfrak{G}$ gilt das assoziative Gesetz*

$$(AB)C = A(BC).$$

c) *Es gibt ein Element E aus $\mathfrak{G}$ mit $EA = A$ für alle A aus $\mathfrak{G}$. Wir nennen E ein Einheitselement von $\mathfrak{G}$. (Es wird sich zeigen, daß es nur ein solches Element gibt.)*

d) *Zu jedem Element A aus $\mathfrak{G}$ gibt es ein Element B aus $\mathfrak{G}$ mit $BA = E$.*

Wir ziehen aus den Axiomen zunächst ein paar einfache Folgerungen:

1.2 Folgerung. *Die Produktbildung in einer Gruppe ist unabhängig von der Beklammerung; genauer gesagt:*

Für irgendwelche Elemente $A_1, A_2, \ldots$ aus $\mathfrak{G}$ definieren wir die Teilmengen $\mathfrak{P}_k(A_1, \ldots, A_k)$ von $\mathfrak{G}$ rekursiv durch

$$\mathfrak{P}_1(A_1) = \{A_1\}, \qquad \mathfrak{P}_2(A_1, A_2) = \{A_1 A_2\}$$

und

$$\mathfrak{P}_k(A_1, \ldots, A_k) = \{XY \mid X \in \mathfrak{P}_m(A_1, \ldots, A_m),\ Y \in \mathfrak{P}_n(A_{m+1}, \ldots, A_{m+n}),\ k = m + n\}.$$

(Die Elemente aus $\mathfrak{P}_k(A_1, \ldots, A_k)$ sind also gerade die Produkte $A_1 \ldots A_k$ mit sinnvoller Beklammerung.) Wir behaupten: Für jedes k enthält $\mathfrak{P}_k(A_1, \ldots, A_k)$ genau ein Element. Dieses Element bezeichnen wir mit $A_1 \ldots A_k$.

Beweis. Wir beweisen durch Induktion nach k, daß jedes $\mathfrak{P}_k(A_1, \ldots, A_k)$ genau ein Element enthält. Für $k = 1, 2$ ist dies auf Grund der Definition klar. Sei $k \geqq 3$ und $G = XY \in \mathfrak{P}_k(A_1, \ldots, A_k)$ mit $X \in \mathfrak{P}_m(A_1, \ldots, A_m)$ und $Y \in \mathfrak{P}_n(A_{m+1}, \ldots, A_k)$. Nach unserer Induktionsannahme ist $X = A_1 Z$ mit $Z = A_2 \ldots A_m$; für $m = 1$ ist dabei $Z = E$ wegzulassen. Nun folgt mit 1.1 b)

$$G = XY = (A_1 Z)Y = A_1(ZY).$$

Dabei ist nach unserer Induktionsannahme

$$ZY \in \mathfrak{P}_{k-1}(A_2, \ldots, A_k) = \{A_2 \ldots A_k\},$$

und wir sind fertig. q.e.d.

1.3 Folgerung. a) *Ist E ein Einheitselement der Gruppe $\mathfrak{G}$, so gilt auch $AE = A$ für alle A aus $\mathfrak{G}$.*

b) *Aus $BA = E$ folgt $AB = E$.*

c) *Aus $AX = AY$ oder $XA = YA$ folgt $X = Y$.*

Beweis. a) Nach 1.1 d) gibt es Elemente X und Y in $\mathfrak{G}$ mit $XA = E$ und $YX = E$. Dann folgt

$$YE = Y(XA) = (YX)A = EA = A\,.$$

Wegen $EE = E$ erhalten wir weiter

$$A = YE = Y(EE) = (YE)E = AE\,,$$

was zu zeigen war.

b) Nach 1.1 d) gibt es in $\mathfrak{G}$ ein Element X mit $XB = E$. Unter Beachtung von 1.2 folgt dann

$$E = XB = XEB = X(BA)B$$
$$= (XB)\,(AB) = E\,(AB) = AB\,.$$

c) Sei $BA = E$. Dann haben wir auch $AB = E$ und

$$X = EX = (BA)X = B(AX) = B(AY) = (BA)Y = EY = Y$$

bzw.

$$X = XE = X(AB) = (XA)B = (YA)B = Y(AB) = YE = Y\,.$$

q.e.d.

1.4 Folgerung. *Ist $\mathfrak{G}$ eine Gruppe, so gibt es zu gegebenen Elementen A und B aus $\mathfrak{G}$ genau ein Element X aus $\mathfrak{G}$ mit $AX = B$. Ebenso gibt es genau ein Element Y mit $YA = B$.*

Beweis. Sei C ein nach 1.1 d) existierendes Element mit $CA = E$. Nach 1.3 b) ist dann auch $AC = E$. Nun ist $X = CB$ ein Element der gesuchten Art, denn wir haben

$$AX = A(CB) = (AC)B = EB = B\,.$$

Sind X_1 und X_2 Elemente mit $AX_1 = AX_2 = B$, so liefert 1.3 c) sofort $X_1 = X_2$. q.e.d.

Aus 1.4 folgt unmittelbar, daß $\mathfrak{G}$ nur ein Einheitselement E besitzt. Ferner ergibt sich noch:

1.5 Folgerung. a) *Zu vorgegebenem A aus $\mathfrak{G}$ gibt es genau ein X aus $\mathfrak{G}$ mit $XA = E$. Dann ist auch $AX = E$. Wir nennen X das Inverse zu A und schreiben $X = A^{-1}$.*

b) *Stets gilt $(AB)^{-1} = B^{-1}A^{-1}$ und $(A^{-1})^{-1} = A$.*

Beweis. Die Aussage unter a) ist eine Folgerung aus 1.4 und 1.3 b). Die Aussage b) ergibt sich dann mit 1.2 aus

$$(B^{-1}A^{-1})\,(AB) = (B^{-1}(A^{-1}A))B = B^{-1}B = E\,, \qquad AA^{-1} = E$$

und der Eindeutigkeit des inversen Elementes. q.e.d.

1.6 Definition. Wir definieren die Potenzen des Elementes G aus der Gruppe $\mathfrak{G}$ rekursiv durch $G^0 = E$ und $G^{i+1} = G^i G$; für $i < 0$ setzen wir $G^i = (G^{-i})^{-1}$. Man beweist leicht die Gültigkeit von $G^{i+j} = G^i G^j$ für alle ganzen rationalen Zahlen i und j.

1.7 Definition. Die Kardinalzahl einer Menge $\mathfrak{M}$ bezeichnen wir stets mit $|\mathfrak{M}|$. Ist $\mathfrak{G}$ eine Gruppe, so nennen wir $|\mathfrak{G}|$ die Ordnung von $\mathfrak{G}$. Wir nennen $\mathfrak{G}$ eine endliche Gruppe, wenn $|\mathfrak{G}|$ eine endliche Kardinalzahl ist.

Wir interessieren uns oft nicht für die Natur der Elemente einer Gruppe, sondern nur für die algebraischen Beziehungen zwischen den Elementen. Um dem Rechnung zu tragen, führen wir den folgenden Äquivalenzbegriff ein:

1.8 Definition. Zwei Gruppen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ heißen isomorph, wenn es eine umkehrbar eindeutige Abbildung π von $\mathfrak{G}_1$ auf $\mathfrak{G}_2$ gibt mit

$$(GH)^\pi = G^\pi H^\pi$$

für alle Elemente G und H aus $\mathfrak{G}_1$. Wir schreiben dann $\mathfrak{G}_1 \cong \mathfrak{G}_2$. Die Isomorphie ist offenbar ein Äquivalenzbegriff. Unter einer Gruppeneigenschaft verstehen wir eine Eigenschaft, welche mit $\mathfrak{G}$ auch jeder zu $\mathfrak{G}$ isomorphen Gruppe zukommt.

Wir vermerken:

1.9 Folgerung. *Ist π ein Isomorphismus von $\mathfrak{G}_1$ auf $\mathfrak{G}_2$ und E_i das Einheitselement von $\mathfrak{G}_i$, so gilt $E_1^\pi = E_2$. Ferner gilt für alle G in $\mathfrak{G}_1$ stets $(G^{-1})^\pi = (G^\pi)^{-1}$.*

Beweis. Die Aussage $E_1^\pi = E_2$ folgt aus der für alle G aus $\mathfrak{G}_1$ gültigen Gleichung

$$E_1^\pi G^\pi = (E_1 G)^\pi = G^\pi$$

zusammen mit der Eindeutigkeitsaussage in 1.4. Aus

$$(G^{-1})^\pi G^\pi = (G^{-1} G)^\pi = E_1^\pi = E_2$$

folgt ebenso $(G^{-1})^\pi = (G^\pi)^{-1}$. **q.e.d.**

1.10 Definition. Die Gruppe $\mathfrak{G}$ heißt abelsch (oder auch kommutativ), wenn für alle Elemente A und B aus $\mathfrak{G}$ gilt $AB = BA$. Dann ist jedes Produkt $A_1 \ldots A_n$ mit $A_i \in \mathfrak{G}$ unabhängig von der Anordnung der A_i.

§ 2. Untergruppen

2.1 Definition. Die Teilmenge $\mathfrak{U}$ der Gruppe $\mathfrak{G}$ heißt eine Untergruppe von $\mathfrak{G}$, wenn $\mathfrak{U}$ bezüglich der auf $\mathfrak{G}$ definierten Produktbildung eine Gruppe ist. Das heißt also:

Liegen U_1 und U_2 in $\mathfrak{U}$, so liegt auch $U_1 U_2$ in $\mathfrak{U}$; mit U liegt U^{-1} in $\mathfrak{U}$; das Einheitselement E von $\mathfrak{G}$ liegt in $\mathfrak{U}$. (Natürlich ist E dann das Einheitselement von $\mathfrak{U}$.)

Wir schreiben $\mathfrak{U} \leqq \mathfrak{G}$, falls $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$ ist; ist $\mathfrak{U}$ eine von $\mathfrak{G}$ verschiedene Untergruppe von $\mathfrak{G}$, so schreiben wir $\mathfrak{U} < \mathfrak{G}$. Jede Gruppe enthält die nur aus dem Einheitselement E bestehende Untergruppe $\mathfrak{E} = \{E\}$. Wir bezeichnen gelegentlich die Gruppen $\mathfrak{E}$ und $\mathfrak{G}$ als die trivialen Untergruppen von $\mathfrak{G}$.

Nützlich ist oft:

2.2 Hilfssatz. *Ist $\mathfrak{U}$ eine endliche Teilmenge der Gruppe $\mathfrak{G}$, und gilt für U_1, U_2 aus $\mathfrak{U}$ stets auch $U_1 U_2 \in \mathfrak{U}$, so ist $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$.*

Beweis. Sei U_0 irgendein Element aus $\mathfrak{U}$. Die Produkte UU_0 mit $U \in \mathfrak{U}$ sind dann nach 1.3 c) alle verschieden und liefern genau $|\mathfrak{U}|$ Elemente aus $\mathfrak{U}$. Also ist $\mathfrak{U} = \{UU_0 \mid U \in \mathfrak{U}\}$. Insbesondere gibt es ein U_1 aus $\mathfrak{U}$ mit $U_1 U_0 = U_0 = EU_0$. Nach 1.3 c) ist dann $U_1 = E$. Ferner gibt es ein U_2 aus $\mathfrak{U}$ mit $U_2 U_0 = E$, daher liegt $U_2 = U_0^{-1}$ auch in $\mathfrak{U}$. q.e.d.

2.3 Satz. *Sind die $\mathfrak{U}_i$ mit i aus der Indexmenge I Untergruppen von $\mathfrak{G}$, so ist auch der Durchschnitt $\bigcap_{i \in I} \mathfrak{U}_i$ eine Untergruppe von $\mathfrak{G}$.*

Beweis. Liegen A und B beide in allen Untergruppen $\mathfrak{U}_i$, so liegen auch A^{-1} und AB in allen $\mathfrak{U}_i$, daher auch in $\bigcap_{i \in I} \mathfrak{U}_i$. Offenbar liegt auch E in $\bigcap_{i \in I} \mathfrak{U}_i$. q.e.d.

2.4 Definition. Sei $\mathfrak{M}$ eine Teilmenge der Gruppe $\mathfrak{G}$. Als Erzeugnis $\langle \mathfrak{M} \rangle$ von $\mathfrak{M}$ bezeichnen wir den Durchschnitt aller Untergruppen von $\mathfrak{G}$, welche die Menge $\mathfrak{M}$ enthalten. Offenbar ist dann $\langle \mathfrak{M} \rangle$ die kleinste Untergruppe von $\mathfrak{G}$, welche $\mathfrak{M}$ enthält. Setzen wir $\mathfrak{M}^{-1} = \{M^{-1} \mid M \in \mathfrak{M}\}$, so gilt

$$\langle \mathfrak{M} \rangle = \{E, X_1 \ldots X_s \mid X_i \in \mathfrak{M} \cup \mathfrak{M}^{-1},\ s = 1, 2, \ldots\}.$$

Ist $\mathfrak{M} = \{A, B, \ldots\}$, so schreiben wir auch $\langle \mathfrak{M} \rangle = \langle A, B, \ldots \rangle$. Ist $\mathfrak{G} = \langle \mathfrak{M} \rangle$, so nennen wir die Menge $\mathfrak{M}$ ein Erzeugendensystem von $\mathfrak{G}$. Eine Gruppe, welche sich mit einem Element erzeugen läßt, nennen wir zyklisch. Setzen wir stets $A^0 = E$, so besteht $\langle A \rangle$ gerade aus den Elementen A^i mit $i = 0, \pm 1, \pm 2, \ldots$, welche aber nicht notwendig alle verschieden sind.

2.5 Satz. *Sei $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$. Die Mengen*

$$G\mathfrak{U} = \{GU \mid U \in \mathfrak{U}\} \quad (\text{mit } G \in \mathfrak{G})$$

bezeichnen wir als Linksnebenklassen von $\mathfrak{U}$ in $\mathfrak{G}$. Für irgendwelche Elemente G und H aus $\mathfrak{G}$ gilt dann stets $G\mathfrak{U} \cap H\mathfrak{U} = \emptyset$ oder $G\mathfrak{U} = H\mathfrak{U}$. Die Gruppe $\mathfrak{G}$ ist die disjunkte Vereinigung aller verschiedenen Linksnebenklassen $G\mathfrak{U}$. Enthält die Menge $\mathfrak{R}$ aus jeder Linksnebenklasse von $\mathfrak{U}$ genau ein Element, so nennen wir $\mathfrak{R}$ ein System von Linksnebenklassenvertretern von $\mathfrak{U}$ in $\mathfrak{G}$ (transversal *im Englischen*). *Die Zerlegung*

$$\mathfrak{G} = \bigcup_{R \in \mathfrak{R}} R\mathfrak{U}$$

nennen wir die Zerlegung von $\mathfrak{G}$ in Linksnebenklassen nach $\mathfrak{U}$. Alle Nebenklassen von $\mathfrak{U}$ haben die gleiche Kardinalzahl $|\mathfrak{U}|$. Wir nennen die Kardinalzahl $|\mathfrak{R}|$ von $\mathfrak{R}$ den Index von $\mathfrak{U}$ in $\mathfrak{G}$ und schreiben dafür $|\mathfrak{G} : \mathfrak{U}|$.

(Entsprechende Aussagen gelten natürlich für die Rechtsnebenklassen $\mathfrak{U}G$.)

Beweis. Wir führen auf $\mathfrak{G}$ eine Äquivalenzrelation ein durch die Festsetzung $X \sim Y$, falls $X^{-1}Y$ in $\mathfrak{U}$ liegt. Dies ist wirklich eine Äquivalenzrelation:

Wegen $X^{-1}X = E \in \mathfrak{U}$ gilt $X \sim X$, also ist die Relation reflexiv. Ist $X \sim Y$, also $X^{-1}Y \in \mathfrak{U}$, so folgt $(X^{-1}Y)^{-1} = Y^{-1}X \in \mathfrak{U}$, daher $Y \sim X$, und unsere Relation ist symmetrisch. Aus $X \sim Y$ und $Y \sim Z$ folgt $X^{-1}Y \in \mathfrak{U}$ und $Y^{-1}Z \in \mathfrak{U}$, daher auch

$$X^{-1}Z = (X^{-1}Y)\,(Y^{-1}Z) \in \mathfrak{U}$$

und dann $X \sim Z$. Daher ist die Relation auch transitiv.

Bekanntlich läßt sich nun $\mathfrak{G}$ schreiben als die disjunkte Vereinigung der Äquivalenzklassen nach unserer Relation. Die Klasse der zu G äquivalenten Elemente aus $\mathfrak{G}$ ist offenbar gerade die Linksnebenklasse $G\mathfrak{U}$. Die restlichen Behauptungen sind nun klar. **q.e.d.**

2.6 Satz. a) *Sei $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$. Ist $\mathfrak{G} = \bigcup_{R \in \mathfrak{R}} \mathfrak{U}R$ die Zerlegung von $\mathfrak{G}$ in Rechtsnebenklassen nach $\mathfrak{U}$, so ist $\mathfrak{G} = \bigcup_{R \in \mathfrak{R}} R^{-1}\mathfrak{U}$ die Zerlegung von $\mathfrak{G}$ in Linksnebenklassen nach $\mathfrak{U}$. (Insbesondere haben wir nicht zwischen einem Links- und Rechtsindex von $\mathfrak{U}$ in $\mathfrak{G}$ zu unterscheiden.)*

b) *Ist $\mathfrak{G} = \bigcup_{R \in \mathfrak{R}} \mathfrak{U}R$ die Zerlegung von $\mathfrak{G}$ in Rechtsnebenklassen nach der Untergruppe $\mathfrak{U}$ und ist $\mathfrak{U} = \bigcup_{S \in \mathfrak{S}} \mathfrak{V}S$ die Zerlegung von $\mathfrak{U}$ nach $\mathfrak{V}$, so ist $\mathfrak{G} = \bigcup_{S \in \mathfrak{S}, R \in \mathfrak{R}} \mathfrak{V}SR$ die Zerlegung von $\mathfrak{G}$ in Rechtsnebenklassen nach $\mathfrak{V}$. Insbesondere gilt $|\mathfrak{G} : \mathfrak{V}| = |\mathfrak{G} : \mathfrak{U}|\,|\mathfrak{U} : \mathfrak{V}|$.*

Beweis. a) Die Abbildung α mit $G^{\alpha} = G^{-1}$ ist eine umkehrbar eindeutige Abbildung von $\mathfrak{G}$ auf sich mit $(\mathfrak{U}R)^{\alpha} = R^{-1}\mathfrak{U}$.

b) Aus $\mathfrak{V}S_1R_1 = \mathfrak{V}S_2R_2$ folgt durch Multiplikation mit $\mathfrak{U}$ von links $\mathfrak{U}R_1 = \mathfrak{U}R_2$. Also ist $R_1 = R_2$ und dann $S_1 = S_2$. Trivialerweise gilt $\mathfrak{G} = \bigcup_{S \in \mathfrak{S}, R \in \mathfrak{R}} \mathfrak{V}SR$. **q.e.d.**

Grundlegend für die Theorie der endlichen Gruppen ist der folgende Satz von Lagrange, der ein arithmetisches Element in die Theorie hineinbringt:

2.7 Hauptsatz (LAGRANGE). *Sei $\mathfrak{G}$ eine endliche Gruppe und $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$. Dann gilt $|\mathfrak{G}| = |\mathfrak{U}|\,|\mathfrak{G} : \mathfrak{U}|$. Insbesondere sind also Ordnung und Index einer Untergruppe einer endlichen Gruppe stets Teiler der Gruppenordnung.*

Beweis. Dies ist der Sonderfall $\mathfrak{V} = \mathfrak{E}$ von 2.6 b). **q.e.d.**

2.8 Definition. Sei G ein Element der Gruppe $\mathfrak{G}$. Die kleinste natürliche Zahl n mit $G^n = E$ nennen wir die Ordnung $O(G)$ von G; gibt es keine natürliche Zahl n mit $G^n = E$, so schreiben wir $O(G) = \infty$. Das kleinste gemeinsame Vielfache der Ordnungen $O(G)$ der Elemente G aus $\mathfrak{G}$ nennen wir, falls es existiert, den Exponenten Exp $\mathfrak{G}$ von $\mathfrak{G}$.

2.9 Satz. *Sei $\mathfrak{G}$ eine Gruppe. Sei $G \in \mathfrak{G}$ mit $O(G) = n < \infty$. Dann gilt:*

a) *Aus $G^m = E$ folgt $n \mid m$.*

b) *Es gilt*

$$\langle G \rangle = \{E, G, G^2, \ldots, G^{n-1}\}$$

und $|\langle G \rangle| = O(G) = n$. Insbesondere ist $O(G)$ für endliches $\mathfrak{G}$ ein Teiler von $|\mathfrak{G}|$.

c) *Ist k eine ganze rationale Zahl, so gilt $O(G^k) = \frac{n}{(n,k)}$.*

Beweis. a) Sei $m = nr + s$ mit $0 \leqq s < n$. Dann ist

$$E = G^m = G^{nr+s} = (G^n)^r G^s = G^s.$$

Wegen der Minimalität von $n = O(G)$ erzwingt das $s = 0$, somit $n \mid m$.

b) Sei $i + j = nr + s$ mit $0 \leqq s < n$. Dann ist $G^{i+j} = G^s$. Also ist die endliche Menge $\{G^s \mid 0 \leqq s < n\}$ nach 2.2 eine Gruppe, ist somit gleich $\langle G \rangle$. Angenommen, es sei $G^i = G^j$ mit $0 \leqq i \leqq j < n$. Dann ist $G^{j-i} = E$. Nach a) folgt $n \mid j - i$, also ist $i = j$. Somit sind die G^i mit $0 \leqq i \leqq n - 1$ paarweise verschieden. Wegen $G^{nk+r} = G^r$ bleibt

$$\langle G \rangle = \{E, G, G^2, \ldots, G^{n-1}\}.$$

Nach 2.7 ist daher $O(G) = |\langle G \rangle|$ ein Teiler von $|\mathfrak{G}|$.

c) Aus $n \mid k\frac{n}{(n,k)}$ folgt

$$G^{k\frac{n}{(n,k)}} = E.$$

Nach a) ist also $O(G^k) \mid \frac{n}{(n,k)}$. Aus $G^{kt} = E$ folgt umgekehrt mit a) $n \mid kt$, daher $\frac{n}{(n,k)} \mid t$. Also ist $O(G^k) = \frac{n}{(n,k)}$. q.e.d.

2.10 Satz. *Jede Gruppe von Primzahlordnung ist zyklisch.*

Beweis. Sei $|\mathfrak{G}| = p$ eine Primzahl und sei G ein von E verschiedenes Element aus $\mathfrak{G}$. Wir setzen $\mathfrak{U} = \langle G \rangle$. Dann ist $|\mathfrak{U}|$ nach 2.7 ein Teiler von $|\mathfrak{G}| = p$. Wegen $1 < |\mathfrak{U}|$ folgt daraus $|\mathfrak{U}| = |\mathfrak{G}|$, also $\mathfrak{U} = \mathfrak{G}$, und $\mathfrak{G}$ ist zyklisch. q.e.d.

Satz 2.10 ist nur der allererste einer langen Reihe von Sätzen, welche aus der Primfaktorzerlegung von $|\mathfrak{G}|$ Aussagen über $\mathfrak{G}$ herleiten.

2.11 Definition. Sind $\mathfrak{A}$ und $\mathfrak{B}$ Teilmengen der Gruppe $\mathfrak{G}$, so setzen wir

$$\mathfrak{A}\mathfrak{B} = \{AB \mid A \in \mathfrak{A}, B \in \mathfrak{B}\}.$$