Hochschultext

Hans Kurzweil

Endliche Gruppen

Eine Einführung in die Theorie der endlichen Gruppen

Springer-Verlag
Berlin Heidelberg New York 1977

Hans Kurzweil

Mathematisches Institut der Universität Erlangen
8520 Erlangen

AMS Subject Classification (1970): 20-01, 20A05, 20B05,
20D05, 20D10, 20D15, 20D20, 20D40, 20D45

ISBN-13: 978-3-540-08454-9 e-ISBN-13: 978-3-642-95313-2
DOI: 10.1007/978-3-642-95313-2

Library of Congress Cataloging in Publication Data. Kurzweil, Hans, 1942-. Endliche Gruppen. (Hochschultext). Bibliography: p. Includes index. 1. Finite groups.
I. Title. QA171.K987. 512'.22. 77-11623

Gesamtherstellung: fotokop wilhelm weihert KG, Darmstadt
2144/3140-543210

Vorwort

Das vorliegende Buch möchte den Leser mit den Grundlagen und Methoden der Theorie der endlichen Gruppen vertraut machen und ihn bis an aktuelle Ergebnisse heranführen. Es entstand aus einer 1-semestrigen Vorlesung, setzt nur elementare Kenntnisse der linearen Algebra voraus und entwickelt die wichtigsten Resultate auf möglichst direktem Weg. Die Theorie der p-Gruppen behandeln wir z. B. nur so weit, wie es für das Studium von p-Untergruppen beliebiger Gruppen unbedingt erforderlich ist; ähnlich verfahren wir mit den nilpotenten Gruppen. Die auflösbaren Gruppen stellen wir zusammen mit den π-auflösbaren Gruppen vor und betonen auch hier solche Aspekte, welche für die Behandlung auflösbarer Untergruppen nicht auflösbarer Gruppen wertvoll sind.

Das zentrale und bis jetzt ungelöste Problem in der Theorie endlicher Gruppen ist die Bestimmung aller einfachen Gruppen. In den letzten 20 Jahren wurden dazu eine Vielfalt tiefer Sätze bewiesen, so daß eine Lösung des Problems heute nicht mehr unmöglich erscheint. Da die Beweise oft sehr lang und kompliziert sind, entziehen sie sich weitgehend einer Darstellung in einem Lehrbuch und erst recht in diesem einführenden Text. Es haben sich jedoch eine Reihe elementarer Schlußweisen und Begriffe herausgebildet, deren Kenntnis eine Grundvoraussetzung für die Beschäftigung mit diesem Gebiet ist. Solche darzustellen, sowie auf typische Fragestellungen anzuwenden, ist ein Hauptanliegen unseres Buches. Dabei orientieren wir uns vor allem an dem Begriff des "Operierens" in seinen verschiedenen Formen. In Kap. III behandeln wir die Operation einer Gruppe auf einer Menge und leiten damit den Satz von SYLOW sowie verwandte Resultate ab. In Kap. VII untersuchen wir die Operation einer Gruppe auf einer Gruppe; hier stellen wir zum Beispiel die HALL-HIGMAN-REDUKTION vor und beweisen mit ihrer Hilfe wichtige Spezialfälle des berühmten Theorems B von HALL-HIGMAN (Kap. VII, § 6). Kap. VIII enthält den neuen, von BENDER stammenden Beweis eines klassischen Satzes von BURNSIDE, der besagt, daß Gruppen der Ordnung $p^a q^b$ (p,q Primzahlen) auflösbar sind. In diesem Beweis

ist ein minimales Gegenbeispiel eine einfache Gruppe, auf die in exemplarischer Weise die vorher entwickelten Sätze und Begriffe angewandt werden. Da deren Tragfähigkeit dabei voll zum Ausdruck kommt, möchten wir dieses Kapitel dem Leser besonders empfehlen. Wir beweisen weiter in Kap. IX, § 2 einen Satz von THOMPSON über normale p-Komplemente und zeigen mit seiner Hilfe im letzten Kapitel, daß eine Gruppe nilpotent ist, wenn sie einen fixpunktfreien Automorphismus von Primzahlordnung besitzt. Hierzu benötigen wir auch Resultate aus der linearen Darstellungstheorie, die wir bei dieser Gelegenheit mit ihren allerwichtigsten Begriffen vorstellen.

An vielen Stellen finden sich Hinweise auf weitere Sätze und Entwicklungen. Neben Originalarbeiten zitieren wir dabei vor allem HUPPERTS Buch "Endliche Gruppen" (mit [H] abgekürzt), sowie GORENSTEINS Buch "Finite Groups" (mit [G] abgekürzt).

Eine Liste aller bis heute bekannten sporadischen einfachen Gruppen haben wir am Ende des Buches angefügt.

Der Text ist reichlich mit Übungen versehen, die sich in den meisten Fällen leicht aus dem jeweils behandelten Stoff ableiten lassen. Solche Übungen, die ein tieferes Eindenken erfordern, haben wir durch Unterstreichen der Übungsnummer gekennzeichnet.

Den Herren DEMPWOLFF, HUPPERT, KEGEL und STELLMACHER danke ich für wertvolle Ratschläge und ihr hilfreiches Interesse am Entstehen dieses Buches, den Herren MEIXNER und SCHNEIDER für ein aufmerksames und kritisches Lesen der Beweise und des fertigen Textes. Für die Fertigstellung des Manuskriptes bedanke ich mich bei Frau ANDERKA und Frau ROSSBACH.

Erlangen, April 1977 Hans Kurzweil

Hinweise

Ab Kapitel III ist eine Gruppe immer eine endliche Gruppe.

Die Aussagen sind mit arabischen Ziffern versehen; so ist etwa 7.21 die 21igste Aussage von Kapitel VII.

Gruppen bezeichnen wir mit großen Buchstaben A,B,..., ihre Elemente mit kleinen a,b,... .

Abbildungen schreiben wir meistens exponentiell: $x \to x^{\varphi}$; gelegentlich schreiben wir auch $\varphi(x)$.

Übungen, deren Nummern unterstrichen sind, erfordern ein tieferes Eindenken (vergleiche Vorwort).

Wir zitieren im Text zwei Gruppentheoriebücher, nämlich:

[G] GORENSTEIN: Finite Groups, Harper and Row, New York, 1968.

[H] HUPPERT: Endliche Gruppen I, Springer-Verlag, Berlin-Heidelberg, 1967.

Inhaltsverzeichnis

Kapitel I. Einführung

Wir führen hier die wichtigsten Grundbegriffe der Gruppentheorie ein. Anders als später setzen wir hier im allgemeinen nicht voraus, daß eine Gruppe endlich ist.

§ 1 Gruppen und Untergruppen

Eine Menge G heißt eine *Gruppe*, falls je zwei Elementen $x, y \in G$ ein Produkt $xy \in G$ zugeordnet ist, so daß folgende drei Gesetze*) gelten:

ASSOZIATIVGESETZ: *Für alle* $x, y, z \in G$ *gilt*

$$(xy)z = x(yz).$$

EINSELEMENT: *Es gibt ein Element* $e \in G$ *mit*

$$ex = xe = x$$

für alle $x \in G$.

INVERSES ELEMENT: *Zu jedem* $x \in G$ *gibt es ein Element* $x^{-1} \in G$ *mit*

$$xx^{-1} = e = x^{-1}x.$$

Eine Gruppe G heißt *abelsch*, falls zusätzlich noch $xy = yx$ für alle $x,y \in G$ gilt. In diesem Fall schreibt man das Produkt in G auch gerne als Summe, also $x + y$ statt xy. Das Einselement einer multiplikativ geschriebenen Gruppe werden wir immer mit dem Symbol 1 bezeichnen (bei additiver Schreibweise mit O).

---

*) Die Gruppenaxiome können leicht abgeschwächt werden; siehe [H], S.2.

Aus dem Assoziativgesetz folgt leicht das *verallgemeinerte Assoziativgesetz*: Jede sinnvolle Klammerung eines Ausdrucks $x_1x_2 \dots x_n$ von Elementen $x_i \in G$ ergibt dasselbe Element, wir bezeichnen es mit $x_1x_2 \dots x_n$.*)

Aus der Existenz des Einselements und des inversen Elements folgt, daß für $a,b \in G$ die Gleichungen

$$ya = b \text{ und } ax = b$$

eindeutige Lösungen

$$y = ba^{-1} \text{ und } x = a^{-1}b$$

in G besitzen.

Definieren wir $x^a := a^{-1}xa$ für $x,a \in G$, so gilt:

1.1 *Die Abbildungen* $x \to ax$, $x \to xa$, $x \to x^{-1}$ *und* $x \to x^a$ *sind bijektive Abbildungen der Gruppe* G *auf sich.*

BEWEIS: Die Abbildungen $x \to ax$ und $x \to xa$ sind nach dem eben Gesagten bijektiv. Wegen

$$(x^{-1})^{-1} = x \text{ und } (x^a)^{a^{-1}} = x$$

gilt dies auch für $x \to x^{-1}$ und $x \to x^a$. □

Eine Gruppe G heißt *endlich*, falls G nur endlich viele Elemente enthält. Deren Anzahl ist die *Ordnung* $|G|$ von G. Eine endliche Gruppe $G = \{x_1,\dots,x_n\}$ läßt sich durch eine *Gruppentafel* $T = (t_{ij})$ beschreiben; dabei ist $t_{ij} := x_ix_j \in G$, also T eine $n \times n$-Matrix über G. Zum Beispiel ist

$T =$

	x_1	x_2
x_1	x_1	x_2
x_2	x_2	x_1

die Gruppentafel einer Gruppe der Ordnung 2 und

*) Z.B. ist $x_1((x_2x_3)x_4)$, nicht aber $(x_1(x_2)x_3(x_4)$ eine sinnvolle Klammerung von $x_1x_2x_3x_4$.

$T =$

	x_1	x_2	x_3	x_4	x_5	x_6
x_1	x_1	x_2	x_3	x_4	x_5	x_6
x_2	x_2	x_3	x_1	x_6	x_4	x_5
x_3	x_3	x_1	x_2	x_5	x_6	x_4
x_4	x_4	x_5	x_6	x_1	x_2	x_3
x_5	x_5	x_6	x_4	x_3	x_1	x_2
x_6	x_6	x_4	x_5	x_2	x_3	x_1

die Gruppentafel einer nicht-abelschen Gruppe der Ordnung 6. Wir empfehlen dem Leser, an diesem konkreten Beispiel die Begriffe zu testen, die wir im folgenden einführen werden.

Eine nicht leere Untermenge U einer Gruppe G heißt eine *Untergruppe* von G (wir schreiben $U \leq G$), falls U bezüglich dem in G erklärten Produkt wieder eine Gruppe ist. Dies ist sicherlich der Fall, wenn mit $x, y \in G$ auch xy und x^{-1} in U liegen. Für endliche Gruppen gilt sogar:

1.2 *Eine nicht leere endliche Untermenge* U *einer Gruppe* G *ist schon dann eine Untergruppe von* G, *wenn mit* x, y *in* U *auch* xy *in* U *liegt.*

BEWEIS: Für $a \in U$ ist die Abbildung

$$\varphi_a : x \to xa$$

von U in sich injektiv (vergleiche 1.1), also wegen $|U| < \infty$ auch surjektiv. Demnach existiert ein $x \in U$ mit $\varphi_a(x) = a$, also $xa = a$; es folgt $x = 1 \in U$. Nun findet man ein $x \in U$ mit $\varphi_a(x) = 1$, also $xa = 1$; es folgt $x = a^{-1} \in U$. □

In jeder Gruppe G sind $U = \{1\}$ und $U = G$ Untergruppen. Statt $U = \{1\}$ schreiben wir einfach $U = 1$. Offenbar ist der Durchschnitt von beliebig vielen Untergruppen von G wieder eine Untergruppe.
Für zwei Untermengen A, B der Gruppe G sei

$$AB := \{ab \mid a \in A, b \in B\}$$

das *Komplexprodukt* von A mit B. Die so auf der Menge der nicht leeren Teilmengen von G definierte Multiplikation ist, wie die Multiplikation in G, assoziativ.

Für $X \subseteq G$ sei $X^{-1} = \{x^{-1} \mid x \in X\}$. Dann gilt

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Besteht A nur aus einem Element a, so schreiben wir aB statt AB.

Eine nicht leere Teilmenge U von G ist offenbar genau dann eine Untergruppe von G, wenn $UU = U$ und $U^{-1} = U$ gilt.

1.3 *Sind* A *und* B *Untergruppen der Gruppe* G, *so ist* AB *genau dann eine Untergruppe von* G, *wenn* $AB = BA$ *gilt.*

BEWEIS: Aus $AB \leq G$ folgt

$$AB = (AB)^{-1} = B^{-1}A^{-1} = BA.$$

Gilt dagegen $AB = BA$, so erhält man

$$(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB$$

und

$$(AB)^{-1} = B^{-1}A^{-1} = BA = AB,$$

also $AB \leq G$. □

1.4 *Für zwei Untergruppen* A, B *der endlichen Gruppe* G *gilt*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

BEWEIS: Für $a_1, a_2 \in A$ und $b_1, b_2 \in B$ gilt $a_1b_1 = a_2b_2$ genau dann, wenn $a_2^{-1}a_1 = b_2b_1^{-1}$ (=: $d \in A \cap B$), also ein $d \in A \cap B$ existiert mit $a_1 = a_2d$ und $b_2 = db_1$. □

Ist $G = AB$ das Produkt zweier Untergruppen A, B mit $A \cap B = 1$, so heißt A ein *Komplement* von B in G.

Sei U eine Untergruppe von G und $x \in G$. Dann ist

$$Ux = \{ux \mid u \in U\} \text{ bzw. } xU = \{xu \mid u \in U\}$$

eine *Rechtsnebenklasse* bzw. *Linksnebenklasse* von U in G. Weil $u \to ux$ ($u \to xu$) eine Bijektion von U auf Ux (xU) ist, besitzt jede Rechtsnebenklasse (Links-) genauso viele Elemente wie U. Wegen $x = 1x \in Ux$ überdecken die Rechtsnebenklassen (Links-) ganz G. Für $y = ux \in Ux$ folgt mit 1.1

$$Uy = \{wy \mid w \in U\} = \{wux \mid w \in U\} = Ux.$$

Also sind zwei Rechtsnebenklassen (Links-) von U in G gleich oder haben leeren Durchschnitt. Eine Untermenge V von G heißt *Rechtsvertretersystem (Links-)* von U in G, falls V aus jeder Rechtsnebenklasse (Links-) von U in G genau ein Element enthält. Für ein solches V ist

$$G = \bigcup_{x \in V} Ux$$

eine Partition von G.

Weil $Ux \to (Ux)^{-1} = x^{-1}U$ eine bijektive Abbildung der Rechtsnebenklassen auf die Linksnebenklassen ist, enthält G gleichviele Rechts- wie Linksnebenklassen von U; ihre Anzahl heißt der *Index* von U in G und wird mit $|G:U|$ bezeichnet.

Aus dem Vorigen folgt unmittelbar:

1.5 SATZ VON LAGRANGE:
Für eine Untergruppe U *der endlichen Gruppe* G *gilt:*

$$|G| = |U| \cdot |G:U|.$$

Insbesondere sind $|U|$ *und* $|G:U|$ *Teiler von* $|G|$.

Eine Folgerung von 1.5 ist:

1.6 *Für zwei Untergruppen* U_1, U_2 *der endlichen Gruppe* G *mit* $U_1 \subseteq U_2$ *gilt*

$$|G:U_1| = |G:U_2| \cdot |U_2:U_1|.$$

BEWEIS: Nach 1.5 gilt

$$|U_1| \cdot |G:U_1| = |G| = |U_2| \cdot |G:U_2| = |U_1| \cdot |U_2:U_1| \cdot |G:U_2|. \quad \square$$

Man kann ohne Schwierigkeit 1.6 auch für unendliches G beweisen, falls $|G:U_1| < \infty$.

ÜBUNGEN

Es seien A, B und C Untergruppen der endlichen Gruppe G.

1. Aus $B \subseteq A$ folgt $|A:B| \geq |C \cap A : C \cap B|$.

2. $|G: A \cap B| \leq |G:A| \cdot |G:B|$.

3. Sei $B \subseteq A$. Ist $x_1,\ldots,x_n$ ein Linksvertretersystem von A in G, und $y_1,\ldots,y_m$ ein Linksvertretersystem von B in A, so ist $\{x_i y_j\}_{\substack{i = 1,\ldots,n \\ j = 1,\ldots,m}}$ ein Linksvertretersystem von B in G.

4. A ∪ B ist nur dann eine Untergruppe von G, wenn $A \subseteq B$ oder $B \subseteq A$ gilt.

5. Sei die Ordnung von G eine Primzahl. Dann sind 1 und G die einzigen Untergruppen von G.

6. Ist die Ordnung von G gerade, so enthält G ein Element y mit $yy = 1 \neq y$.

7. Gilt $yy = 1$ für alle $y \in G$, so ist G abelsch.

8. Ist $|G| = 4$, so ist G abelsch und besitzt eine Untergruppe der Ordnung 2 (verwende Aufg. 6 und 7).

§ 2 Homomorphismen und Normalteiler

Ein *Homomorphismus* φ einer Gruppe G ist eine Abbildung $x \to x^{\varphi}$ von G in eine Gruppe H, so daß für alle $x,y \in G$ gilt:

$$(xy)^{\varphi} = x^{\varphi}y^{\varphi}.$$

Der Homomorphismus φ heißt *Epimorphismus*, falls φ surjektiv und *Isomorphismus*, falls φ bijektiv ist. Im letzteren Fall schreiben wir $G \cong H$. Ein Isomorphismus von G auf G heißt *Automorphismus*. Ein *Endomorphismus* ist schließlich ein Homomorphismus von G in G.

Sei φ ein Homomorphismus von G in H. Folgende Bemerkungen ergeben sich unmittelbar:

a) $1^{\varphi} = 1 \quad (\in H)$

b) $(x^{-1})^{\varphi} = (x^{\varphi})^{-1} \quad (x \in G)$

c) *Ist* U *Untergruppe von* G, *so ist* U^{φ} *Untergruppe von* H; *insbesondere ist* G^{φ} *Untergruppe von* H.

d) *Ist* $\bar{U}$ *Untergruppe von* H, *so ist* $U := \{x \in G \mid x^{\varphi} \in \bar{U}\}$ *Untergruppe von* G.

Demnach ist

$$\mathit{Kern}\ \varphi := \{x \in G \mid x^{\varphi} = 1\}$$

eine Untergruppe von G. Für $y \in \mathit{Kern}\ \varphi$, $x \in G$ gilt

$$(x^{-1}yx)^{\varphi} = (x^{\varphi})^{-1}\, y^{\varphi}x^{\varphi} = (x^{\varphi})^{-1}x^{\varphi} = 1,$$

und daher für $N := \mathit{Kern}\ \varphi$

$$x^{-1}Nx = N \qquad \text{für alle } x \in G.$$

Eine Untergruppe N von G mit dieser Eigenschaft oder mit der dazu äquivalenten Eigenschaft

$$Nx = xN \qquad \text{für alle } x \in G$$

heißt *Normalteiler* von G oder *normal* in G; wir schreiben $N \trianglelefteq G$.

Sei N ein Normalteiler von G. Dann gilt auch UN = NU für jede Untermenge U von G; mit U ist also auch UN eine Untergruppe von G (1.3). Für $x,y \in G$ gilt

$$(Nx)(Ny) = N(xN)y = N(Nx)y = Nxy.$$

Somit ist das Produkt zweier Nebenklassen des Normalteilers N wieder eine Nebenklasse von N. Die Menge G/N der Nebenklassen Nx, $x \in G$, von N in G bildet bezüglich der Komplexmultiplikation sogar eine Gruppe: Das Assoziativgesetz für G/N folgt aus dem für G, das Einselement von G/N ist N = N1, und das zu Nx inverse Element ist Nx^{-1}. Die Gruppe G/N heißt die *Faktorgruppe* von G nach N. Die Abbildung

$$\varphi : x \to Nx$$

ist offenbar ein Epimorphismus von G auf G/N mit *Kern* $\varphi = N$, man spricht von dem *kanonischen* Epimorphismus auf G/N. Weil umgekehrt, wie oben erwähnt, der Kern eines Homomorphismus ein Normalteiler ist, sind die Normalteiler von G genau die Kerne der Homomorphismen von G. Es gilt der wichtige

1.7 HOMOMORPHIE-SATZ: *Sei* φ *ein Epimorphismus der Gruppe* G *auf die Gruppe* H *und* N := *Kern* φ. *Dann ist*

$$Nx \to x^{\varphi}$$

ein Isomorphismus von G/N *auf* H.

BEWEIS: Für $x, y \in G$ gilt

$$x^{\varphi} = y^{\varphi} \Leftrightarrow x^{\varphi}(y^{\varphi})^{-1} = 1 \Leftrightarrow (xy^{-1})^{\varphi} = 1 \Leftrightarrow xy^{-1} \in N \Leftrightarrow Nx = Ny.$$

Somit ist die Abbildung $\alpha: Nx \to x^{\varphi}$ wohldefiniert und bijektiv. Weil φ ein Homomorphismus ist, gilt schließlich auch

$$(NxNy)^{\alpha} = (Nxy)^{\alpha} = (xy)^{\varphi} = x^{\varphi}y^{\varphi} = (Nx)^{\alpha}(Ny)^{\alpha}. \quad \square$$

Für $N \subseteq A \subseteq G$ sei

$$A/N := \{Na \mid a \in A\} \ (\subseteq G/N).$$

Zwei direkte Folgerungen aus 1.7 sind die *Isomorphiesätze:*

1.8 *Sei* U *eine Untergruppe und* N *ein Normalteiler der Gruppe* G. *Dann ist die Abbildung*

$$\varphi : u \to Nu$$

von U *auf* NU/N *ein Epimorphismus mit Kern* $\varphi = U \cap N$. *Also gilt* $U/(U \cap N) \cong NU/N$.

1.9 *Seien* N *und* M *zwei Normalteiler der Gruppe* G *mit* $N \subseteq M$. *Dann ist die Abbildung*

$\varphi : Nx \to Mx$

von G/N *auf* G/M *ein Epimorphismus mit Kern* $\varphi = M/N$. *Also gilt* $(G/N)/(M/N) \cong G/M$.

Es ist wichtig, ein klares Bild über die Untergruppen einer Faktorgruppe G/N zu haben. Weil die Abbildung $x \to Nx$ ein Epimorphismus von G auf G/N ist, folgt aus den entsprechenden Aussagen über Homomorphismen (oder auch direkt), daß die Untergruppen von G/N von der Form U/N sind, wobei U eine Untergruppe von G ist, die N enthält. Dabei ist U/N normal in G/N genau dann, wenn U normal in G ist. Für eine beliebige Untergruppe U von G ist $\bar{U} := UN/N$ das Bild von U in G/N, also UN ein Urbild von $\bar{U}$ in G.

1.10 *Sei* N *ein Normalteiler und* U *eine Untergruppe der Gruppe* G *mit* $N \subseteq U$. *Dann gilt*

$|G/N : U/N| = |G:U|$.

BEWEIS: Wegen $N \subseteq U$ gilt für $x, y \in G$

$$Ux = Uy \Leftrightarrow xy^{-1} \in U \Leftrightarrow Nxy^{-1} \subseteq U \Leftrightarrow (Nx)(Ny)^{-1} \in U/N. \quad \square$$

Folgende Bemerkung ist oft nützlich:

1.11 *Sind* N *und* M *Normalteiler der Gruppe* G *mit* $N \cap M = 1$, *so gilt* $xy = yx$ *für alle* $x \in N$ *und* $y \in M$.

BEWEIS: Da mit x bzw. y auch $y^{-1}xy$ bzw. $x^{-1}y^{-1}x$ in N bzw. M liegt, folgt

$$x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) = (x^{-1}y^{-1}x)y \in M \cap N = 1,$$

also $xy = yx$. $\square$

Eine Gruppe G heißt *einfach*, falls die trivialen Untergruppen 1 und G die einzigen Normalteiler von G sind. Ist zum Beispiel Y unter den echten Normalteilern der Gruppe X maximal, also ein *maximaler* Normalteiler von X, so ist X/Y einfach. Eine gute Übung für die Anwendung von 1.8 ist:

1.12 *Sei* X *eine Untergruppe der Gruppe* G, Y *ein maximaler Normalteiler von* X *und* N *ein Normalteiler von* G. *Dann gilt* $XN = YN$ *genau dann, wenn* $X \cap N \neq Y \cap N$ *ist. Im Falle* $X \cap N \neq Y \cap N$ *ist* X/Y *isomorph zu* $(X \cap N)/(Y \cap N)$ *und im Falle* $X \cap N = Y \cap N$ *zu* XN/YN.

BEWEIS: Aus $Y \leq (N \cap X)Y \trianglelefteq X$ und der Einfachheit von X/Y folgt entweder $(N \cap X)Y = Y$, d.h. $N \cap X = N \cap Y$ oder $(N \cap X)Y = X$, d.h. $NX = NY$. Im Falle $N \cap X = N \cap Y$ gilt $YN \cap X = Y$ und 1.8 ergibt

$$XN/YN = (X(YN))/YN \cong X/(YN \cap X) = X/Y.$$

Im Falle $(N \cap X)Y = X$ folgt aus 1.8

$$X/Y = (N \cap X)Y \,/\, Y \cong N \cap X \,/\, (Y \cap (N \cap X)) = N \cap X \,/\, N \cap Y. \qquad \square$$

Eine endliche Reihe von Untergruppen

$$1 =: A_k \trianglelefteq A_{k-1} \trianglelefteq \cdots \trianglelefteq A_i \trianglelefteq A_{i-1} \trianglelefteq \cdots \trianglelefteq A_o := G$$

der Gruppe G heißt eine *Kompositionsreihe* der *Länge* k, falls A_i ein maximaler Normalteiler von A_{i-1} ist $(i = 1,\ldots,k)$; im Falle $G = 1$ sei $k = 0$. Die einfachen Gruppen A_{i-1}/A_i heißen die *Faktoren* der Kompositionsreihe. In unendlichen Gruppen existieren nicht immer Kompositionsreihen, während eine endliche Gruppe G stets solche besitzt: Man wähle etwa nacheinander A_1, A_2, ... als einen maximalen Normalteiler von $A_o := G$, A_1 ... . Die wichtigste Aussage über Kompositionsreihen ist der Satz von JORDAN-HÖLDER, der besagt, daß zwei Kompositionsreihen einer Gruppe G im "wesentlichen" gleich sind. Dies verdeutlicht die zentrale Stellung der einfachen Gruppen, insbesondere in der Theorie endlicher Gruppen. Weil die Aussage des JORDAN-HÖLDERschen Satzes jedoch bei endlichen Gruppen in den meisten vorkommenden Fällen von vornherein klar ist und wir ihn deshalb später nicht benötigen, verweisen wir seinen Beweis in einen Anhang zu diesem Abschnitt.

ANHANG: DER SATZ VON JORDAN-HÖLDER

Zwei Kompositionsreihen

$$1 = A_k \lneq \cdots \lneq A_o = G$$

$$1 = B_n \lneq \cdots \lneq B_o = G$$

der Länge k und n einer Gruppe G heißen *isomorph*, falls k = n und es eine Permutation (i',...,k') von (1,...,k) gibt mit

$$A_{i-1}/A_i \cong B_{i'-1}/B_{(i-1)'} \quad (i = 1,\ldots,k).$$

SATZ VON JORDAN-HÖLDER: *Zwei Kompositionsreihen einer Gruppe sind isomorph.*

BEWEIS: Seien $\{A_i\}$ und $\{B_j\}$ zwei Kompositionsreihen wie oben und $N := A_1 \cap B_1$. Aus $A_1 \trianglelefteq G$, $B_1 \trianglelefteq G$ folgt $N \trianglelefteq G$.

Sei zunächst N = 1: Im Falle $A_1 = B_1$ ist $A_1 = B_1 = 1$ und die Aussage trivial. Im Falle $A_1 \neq B_1$ gilt $A_1 \lneq A_1B_1 \leq G$, wegen $A_1B_1 \trianglelefteq G$ sogar $A_1B_1 = G$. Aus 1.8 folgt

$$G/A_1 = A_1B_1 \,/\, A_1 \cong B_1 \,/\, A_1 \cap B_1 \cong B_1,$$

und genauso $G/B_1 \cong A_1$. Es ist also n = k = 2 und die Faktoren sind, wie behauptet, zueinander isomorph.

Sei nun $N \neq 1$. Aus 1.12 folgt, daß

$$1 = A_k \cap N \subseteq A_{k-1} \cap N \subseteq \cdots \subseteq A_o \cap N = N$$

$$1 = A_kN \,/\, N \subseteq A_{k-1}N \,/\, N \subseteq \cdots \subseteq A_oN \,/\, N = G/N$$

Kompositionsreihen (mit eventuellen Wiederholungen) von N und G/N sind, daß die Summe ihrer Längen gleich k ist, und daß ihre Faktoren zu denen der ursprünglichen Reihe isomorph sind. Dasselbe gilt auch für die zwei Kompositionsreihen

$$1 = B_n \cap N \subseteq B_{n-1} \cap N \subseteq \cdots \subseteq B_o \cap N = N$$

$$1 = B_nN \,/\, N \subseteq B_{n-1}N \,/\, N \subseteq \cdots \subseteq B_oN \,/\, N = G/N.$$

Wegen $A_1 \cap N = N = B_1 \cap N \neq 1$ haben die Reihen $\{A_i \cap N\}$ bzw. $\{B_j \cap N\}$, also auch $\{A_iN/N\}$ bzw. $\{B_jN/N\}$ höchstens die Länge (k-1) bzw. (n-1). Die behauptete Isomorphie der beiden Reihen $\{A_i\}$ und $\{B_j\}$ ergibt sich somit durch Induktion nach (n+k). □

Übungen

Es sei G eine Gruppe.

1. Eine Untergruppe vom Index 2 in G ist normal in G.

2. Es gibt genau zwei nicht-isomorphe Gruppen der Ordnung 4; bestimme ihre Gruppentafeln (verwende Aufg. 8, S. 6).

3. Sei N ein Normalteiler von G mit $|G:N| = 4$. Dann besitzt G einen Normalteiler M von G mit $|G:M| = 2$ (verwende Aufg. 2).

4. Sei N ein minimaler Normalteiler von G und M eine maximale Untergruppe von G mit $N \not\subseteq M$. Dann gilt $G = MN$ und, falls N abelsch, $N \cap M = 1$.

5. Sei G einfach, $|G| \neq 2$ und φ ein Homomorphismus von G in die Gruppe H. Besitzt H einen Normalteiler A vom Index 2, so liegt G^φ in A.

6. Sei N ein Normalteiler von G und G/N endlich von ungerader Ordnung. Ein Element $y \in G$ mit $yy = 1 \neq y$ liegt in N.

§ 3 Automorphismen

Die Menge *Aut* G aller Automorphismen einer Gruppe G ist bezüglich der Multiplikation

$$\alpha\beta : x \to (x^\alpha)^\beta \qquad (x \in G)$$

eine Gruppe, wobei das Einselement die identische Abbildung von G, und α^{-1} die zu α inverse Abbildung ist.

Eine Untergruppe U von G heißt *charakteristisch* in G, falls $U^\alpha = U$ für alle $\alpha \in Aut\ G$ gilt; wir schreiben U *char* G. Offenbar sind die trivialen Untergruppen 1 und G charakteristisch. Zum Beispiel ist auch das Zentrum