

II Gruppen : Strukturtheorie

In diesem Kapitel wird die Gruppentheorie von Kapitel I fortgeführt. Die klassischen Sätze von Sylow werden bewiesen. Wir betrachten spezielle Klassen von Gruppen (auflösbare, nilpotente). Insbesondere werden alle endlichen abelschen Gruppen beschrieben.

§ 1 Die Sätze von Sylow

Im folgenden wollen wir uns mit sogenannten p -Untergruppen endlicher Gruppen beschäftigen. Für eine Primzahl p heißt eine endliche Gruppe H eine p -Gruppe, falls die Ordnung von H eine Potenz von p ist, d.h. $|H| = p^k$ für irgendein $k \in \mathbb{N}$.

1.1. Ist G eine endliche abelsche Gruppe, und ist die Primzahl p ein Teiler von $|G|$, so gibt es ein $g \in G$ mit $\text{ord}(g) = p$. Mit Induktion über die Ordnung $|G|$ ist dies zu sehen: Der Fall $|G| = 1$ ist klar. Sonst sei $h \in G$, $h \neq e$; setze $m := \text{ord}(h)$. Gilt $p \mid m$, dann ist $h^{m'}$ mit $m' = m/p$ ein Element der Ordnung p in G . Ist p kein Teiler von m , so betrachte die von h erzeugte (zyklische) Untergruppe $\langle h \rangle$ und die zugehörige Faktorgruppe $G/\langle h \rangle$. Wegen $|G| = |\langle h \rangle| \cdot |G/\langle h \rangle|$ teilt p deren Ordnung $|G/\langle h \rangle|$. Nach Induktionsvoraussetzung existiert ein $g \in G$ mit $\text{ord}(g\langle h \rangle) = p$. Sei $n := \text{ord}(g)$; nun gilt $(g \cdot \langle h \rangle)^n = g^n \langle h \rangle = \langle h \rangle$, also $p \mid n$. Wie im ersten Fall ist $g^{n'}$ mit $n' = n/p$ ein Element der Ordnung p in G .

Die Bedingung der Kommutativität der Gruppe G ist für die gemachte Aussage nicht entscheidend. Es gilt allgemeiner:

Satz 1.2. (Cauchy) *Ist G eine endliche Gruppe und ist die Primzahl p ein Teiler der Ordnung $|G|$ von G , so enthält G ein Element der Ordnung p .*

Beweis: Wir verwenden Induktion über $|G| =: n$. Der Fall $|G| = 1$ ist klar. Sei $|G| > 1$, und sei p ein Teiler von $|G|$. Gibt es eine echte Untergruppe H von G , deren Ordnung $|H|$ durch p teilbar ist, so enthält H (und damit auch G) nach Induktionsvoraussetzung ein Element der Ordnung p . Also können wir annehmen: Die Ordnung jeder echten Untergruppe von G wird nicht von p geteilt. Für jedes $g \in G$, das nicht im Zentrum $Z(G)$ von G liegt, ist der Zentralisator $C_G(g)$ von g in G eine echte Untergruppe, und es gilt $p \nmid |C_G(g)|$. Weil aber $|G|$ von p geteilt wird, folgt: $p \mid [G : C_G(g)]$. Die Klassengleichung

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)],$$

wobei $(x_i)_{i \in I}$ ein Repräsentantensystem für die Konjugationsklassen von G ist, liefert dann, daß p auch die Ordnung $|Z(G)|$ des Zentrums teilt. Da aber nach Voraussetzung p nicht die Ordnung einer echten Untergruppe teilt, muß schon $Z(G) = G$ gelten, d.h., die Gruppe G muß abelsch sein. In diesem Fall ist die Aussage jedoch schon gezeigt. \square

Eine unmittelbare Folgerung dieses Ergebnisses ist:

Korollar 1.3. *Eine endliche Gruppe G ist genau dann eine p -Gruppe, wenn die Ordnung jedes Elements von G eine Potenz von p ist.*

Bemerkung: Diese Charakterisierung einer endlichen p -Gruppe nimmt man als Definition des Begriffes p -Gruppe im Falle unendlicher Gruppen.

Lemma 1.4. *Seien p eine Primzahl und G eine endliche p -Gruppe. Operiert G auf einer endlichen Menge X , so gilt für die Menge X^G der Fixpunkte, daß $|X^G| \equiv |X| \pmod{p}$.*

Beweis: Für alle $x \in X \setminus X^G$ gilt $G_x \neq G$, also ist $[G : G_x]$ durch p teilbar. Daher folgt die Behauptung aus I.6.5(2). \square

Satz 1.5. *Das Zentrum $Z(G)$ einer endlichen p -Gruppe $G \neq \{e\}$ ist nicht-trivial.*

Beweis: Man wende Lemma 1.4 auf die Operation von G auf sich selbst durch Konjugation an. In diesen Fall ist $Z(G)$ die Menge der Fixpunkte. Deshalb gilt $|Z(G)| \equiv |G| \pmod{p}$, und wegen $G \neq \{e\}$ ist $|Z(G)|$ durch p teilbar. \square

Sei p eine Primzahl. Ist G eine endliche Gruppe, so können wir die Ordnung von G in der Form $|G| = p^m \cdot q$ schreiben, wobei $q \in \mathbb{N}$ prim zu p ist. Dann nennt man eine Untergruppe S von G eine p -Sylowuntergruppe von G , wenn $|S| = p^m$ gilt. Die Existenz solcher Untergruppen ist Teil der folgenden Aussagen, die von Sylow stammen:

Satz 1.6. *Sei G eine endliche Gruppe der Ordnung $|G| = p^m \cdot q$, mit q prim zu der Primzahl p . Dann gilt:*

- (a) *Zu jedem k , $1 \leq k \leq m$, gibt es mindestens eine Untergruppe in G der Ordnung p^k .*
- (b) *Sind H eine p -Untergruppe von G und S eine p -Sylowuntergruppe von G , so gibt es ein $g \in G$ mit $H \leq gSg^{-1}$.*
- (c) *Ist s die Anzahl der (verschiedenen) p -Sylowuntergruppen von G , so gilt $s \mid q$ und $s \equiv 1 \pmod{p}$.*

Beweis: Die Behauptungen sind klar, wenn $m = 0$. Wir nehmen im folgenden an, daß $m > 0$.

(a) Wir verwenden Induktion über die Ordnung $|G|$. Man betrachte die Operation von G auf sich selbst durch Konjugation. Sei $(x_i)_{i \in I}$ ein Repräsentantensystem der nicht-zentralen Konjugationsklassen von G , d.h. mit $x_i \notin Z(G)$. Die Klassengleichung lautet

$$|G| = |Z(G)| + \sum_{i \in I} [G : C_G(x_i)].$$

Gilt $p \nmid |Z(G)|$, so existiert mindestens ein $i \in I$ mit $p \nmid [G : C_G(x_i)]$. Es folgt $|C_G(x_i)| = p^m q'$ mit $p \nmid q'$ und $C_G(x_i) \leq G$. Nach Induktionsvoraussetzung besitzt der Zentralisator $C_G(x_i)$ eine Untergruppe der Ordnung p^k .

Gilt $p \mid |Z(G)|$, so enthält $Z(G)$ nach 1.1 ein Element g mit $\text{ord}(g) = p$. Es gilt dann $\langle g \rangle \trianglelefteq G$ und $|G/\langle g \rangle| = p^{m-1} \cdot q$. Nach Induktionsvoraussetzung gibt es in $G/\langle g \rangle$ eine Untergruppe U der Ordnung $|U| = p^{k-1}$ wenn $k > 1$. Sie ist von der Form $U = V/\langle g \rangle$ mit einer Untergruppe V von G . Dann gilt $|V| = |U| \cdot |\langle g \rangle| = p^{k-1} \cdot p = p^k$.

(b) Seien H eine p -Untergruppe und S eine p -Sylowuntergruppe von G . Man betrachte die Operation von H auf der Menge der Linksnebenklassen $X = G/S$, definiert durch $(h, gS) \mapsto hgS$. Es gilt $|X| = |G|/|S| = q$. Nach Lemma 1.4 gilt $|X^H| \equiv |X| \pmod{p}$; da q prim zu p ist, folgt, daß $|X^H|$ nicht durch p teilbar ist. Daher kann X^H nicht leer sein, und wir können ein $g \in G$ mit $gS \in X^H$ finden. Dann gilt $hgS = gS$ für alle $h \in H$, also $g^{-1}hg \in S$. Damit erhalten wir $H \subset gSg^{-1}$.

(c) Sei S eine p -Sylowuntergruppe von G . Bezeichne mit X die Menge aller p -Sylowuntergruppen von G . Aus (b) folgt, daß alle Elemente in X zu S unter G konjugiert sind. Satz I.6.4 impliziert, daß $s := |X|$ gleich dem Index $[G : N_G(S)]$ ist. Aus $[G : S] = [G : N_G(S)][N_G(S) : S]$ und $[G : S] = q$ folgt nun $s \mid q$.

Betrachte die Operation von S auf X durch Konjugation. Wir wollen zeigen, daß S der einzige Fixpunkt dieser Operation ist; daraus folgt dann mit Lemma 1.4, daß $s \equiv 1 \pmod{p}$. Beachte, daß $S' \in X$ genau dann ein Fixpunkt von S ist, wenn S im Normalisator von S' enthalten ist: $S \subset N_G(S')$. Ist allgemein eine p -Untergruppe H von G im Normalisator $N_G(S')$ einer p -Sylowuntergruppe S' enthalten, so gilt schon $H \subset S'$. Denn: Da $S' \trianglelefteq N_G(S')$, ist HS' eine Untergruppe von $N_G(S')$, und es gilt $H \cdot S'/S' \cong H/H \cap S'$. Daher ist $H \cdot S'/S'$ eine p -Gruppe. Der Index $[H \cdot S' : S']$ teilt den Index $[G : S']$, der aber nicht durch p teilbar ist; also folgt $H \cdot S' = S'$, und damit $H \subset S'$. In unserer Situation bedeutet dies, daß $S \subset S'$ gilt, also $S' = S$, weil beide Gruppen Ordnung p^m haben. Damit ist S , wie behauptet, der einzige Fixpunkt der Operation von S auf X . \square

Wir halten insbesondere fest:

Korollar 1.7. *Die p -Sylowuntergruppen von G bilden eine Klasse konjugierter Untergruppen in G .*

Bemerkung: In einer beliebigen (nicht notwendig endlichen) Gruppe G heißt eine Untergruppe S eine p -Sylowuntergruppe von G , wenn S maximal in der Menge aller p -Untergruppen von G ist. Satz 1.6.b zeigt, daß diese neue Definition mit der alten im Fall einer endlichen Gruppe verträglich ist. Die Existenz von p -Sylowuntergruppen folgt im allgemeinen Fall aus dem Lemma von Zorn. Denn: Die Menge X aller p -Untergruppen ist nicht leer, da X die triviale Gruppe enthält. Eine Kette Z bestehend aus p -Untergruppen $(H_i)_{i \in I}$ in X hat in X die p -Untergruppe $\bigcup_{i \in I} H_i$ als obere Schranke. Deshalb enthält X mindestens ein maximales Element.

Satz 1.8. Seien p und q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede endliche Gruppe G der Ordnung $|G| = p \cdot q$ zyklisch, also isomorph zu $\mathbb{Z}/pq\mathbb{Z}$.

Beweis: Seien S eine p -Sylowuntergruppe und U eine q -Sylowuntergruppe von G ; dann gilt $S \cap U = \{e\}$. Sei s (bzw. r) die Anzahl der p - (bzw. q -) Sylowuntergruppen von G . Dann gilt:

$$r \equiv 1 \pmod{q}, \quad r \mid p \quad \text{und} \quad s \equiv 1 \pmod{p}, \quad s \mid q.$$

Da $p < q$ ist, folgt $r = 1$, also ist U normal in G . Für s folgt: $s = q$ oder $s = 1$. Im ersten Fall wäre jedoch $q \equiv 1 \pmod{p}$, d.h. $p \mid (q-1)$, im Widerspruch zur Voraussetzung. Also gilt $s = 1$, und S ist normal in G . Daher ist $S \cdot U$ eine Untergruppe in G , also $G = S \cdot U = S \times U$. Wähle $g \in S$ und $h \in U$, beide ungleich e . Weil $|S| = p$ und $|U| = q$ Primzahlen sind, gelten $\text{ord } g = p$ und $\text{ord } h = q$. Es folgt, da $gh = hg$, daß $\text{ord}(gh) = pq$ und daher $G = \langle gh \rangle$. \square

§ 2 Normal- und Kompositionsreihen

Sei G eine Gruppe. Eine *Normalreihe* in G ist eine endliche Folge von Untergruppen

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

d.h. jede Gruppe G_i ist normal in G_{i+1} , $i = 0, \dots, n-1$. Die Faktorgruppen G_{i+1}/G_i heißen die *Faktoren der Reihe*, die Gruppen G_i deren *Terme*. Man beachte, daß die Untergruppen G_i nicht unbedingt normal in G sein müssen. Da stets $G_0 := \{e\} \trianglelefteq G =: G_1$ eine Normalreihe in G ist, hat jede Gruppe eine Normalreihe. Sind \mathbf{H} und \mathbf{G} zwei Normalreihen in G , so heißt \mathbf{H} eine *Verfeinerung von \mathbf{G}* , falls jeder Term von \mathbf{G} auch ein Term von \mathbf{H} ist. Man sagt, daß \mathbf{H} *äquivalent zu \mathbf{G}* ist, falls es eine Bijektion von der Menge der Faktoren von \mathbf{H} auf die Menge der Faktoren von \mathbf{G} gibt, so daß entsprechende Faktoren isomorph sind.

Der folgende Satz 2.2 und das vorangehende Lemma 2.1 sind nützlich, um verschiedene Normalreihen \mathbf{G} und \mathbf{H} in einer Gruppe G zu vergleichen.

Lemma 2.1. *Seien U, V Untergruppen einer Gruppe G , und seien $U' \trianglelefteq U$ bzw. $V' \trianglelefteq V$ normale Untergruppen von U bzw. V . Dann gilt $U'(U \cap V') \trianglelefteq U'(U \cap V)$ und $V'(V \cap U') \trianglelefteq V'(V \cap U)$. Die zugehörigen Faktorgruppen sind zueinander und zu $(U \cap V)/(U \cap V')(U' \cap V)$ isomorph:*

$$\begin{aligned} U'(U \cap V)/U'(U \cap V') &\cong (U \cap V)/(U \cap V')(U' \cap V) \\ &\cong V'(V \cap U)/V'(V \cap U'). \end{aligned}$$

Beweis: Es genügt, die erste Isomorphie nachzuweisen, da die zweite Faktorgruppe symmetrisch in U und V ist, man also die zweite Isomorphie durch Vertauschen von U und V in der Argumentation erhält.

Da $U \cap V$ eine Untergruppe von U und U' eine normale Untergruppe von U ist, ist $U'(U \cap V)$ eine Untergruppe von U . Die Gruppe U' ist normal in $U'(U \cap V)$, also ist die Faktorgruppe $U'(U \cap V)/U'$ erklärt. Mit I.4.3 gilt

$$U'(U \cap V)/U' \cong (U \cap V)/(U \cap V \cap U') = (U \cap V)/(U' \cap V). \quad (1)$$

Da $U \cap V'$ und $U' \cap V$ jeweils normale Untergruppen in $U \cap V$ sind, hat man mit I.4.4

$$U \cap V / (U \cap V')(U' \cap V) \cong ((U \cap V)/(U' \cap V)) / ((U \cap V')(U' \cap V)/(U' \cap V)),$$

also ist die linke Seite eine Faktorgruppe von $(U \cap V)/(U' \cap V)$. Unter Verwendung von (1) hat man deshalb einen surjektiven Homomorphismus

$$\alpha: U'(U \cap V)/U' \longrightarrow (U \cap V)/(U \cap V')(U' \cap V).$$

Der Kern von α ist gerade $U'(U \cap V')/U'$. Satz I.4.1.a impliziert dann die Isomorphie

$$U'(U \cap V)/U'(U \cap V') \cong (U'(U \cap V)/U') / \ker \alpha \cong (U \cap V)/U \cap V'(U' \cap V).$$

□

Satz 2.2. *Sind \mathbf{G} und \mathbf{H} zwei Normalreihen in einer gegebenen Gruppe G , so besitzen sie äquivalente Verfeinerungen.*

Beweis: Gegeben seien die zwei Normalreihen

$$\mathbf{G}: \{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

und

$$\mathbf{H}: \{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_m = G.$$

Dann setze man $G_{ij} := G_i(G_{i+1} \cap H_j)$ und $H_{ij} := H_j(G_i \cap H_{j+1})$ für alle i und j . Wendet man das Lemma in der Situation $U = G_{i+1}$, $U' = G_i$,

$V = H_{j+1}$, $V' = H_j$ an, so erhält man $G_{ij} \trianglelefteq G_{i,j+1}$ und $H_{ij} \trianglelefteq H_{i+1,j}$ und einen Isomorphismus der Faktorgruppen

$$G_{i,j+1}/G_{ij} \cong H_{i+1,j}/H_{ij}$$

für alle i und j . Es gilt jeweils $G_{im} = G_{i+1,0}$ und $H_{nj} = H_{0,j+1}$ sowie $G_{n-1,m} = G = H_{n,m-1}$. Die G_{ij} mit $i = 0, \dots, n-1$; $j = 0, \dots, m$ und die H_{ij} mit $i = 0, \dots, n$; $j = 0, \dots, m-1$ bilden dann zwei Normalreihen in G , die äquivalente Verfeinerungen von \mathbf{G} bzw. \mathbf{H} sind. \square

Eine Normalreihe \mathbf{G} von G heißt *Kompositionsreihe*, falls \mathbf{G} keine echte Verfeinerung besitzt. Eine endliche Gruppe G besitzt stets eine Kompositionsreihe. Diese erhält man, indem man eine gegebene Normalreihe durch Einfügen von Termen verfeinert. Da G endlich ist, ergibt sich nach endlich vielen Schritten eine Kompositionsreihe.

Satz 2.3. *Eine Normalreihe \mathbf{G} in G ist genau dann eine Kompositionsreihe, wenn jeder der Faktoren in \mathbf{G} eine einfache Gruppe ist.*

Beweis: Ist einer der Faktoren G_{i+1}/G_i der Normalreihe \mathbf{G} in G nicht einfach, so besitzt er eine nicht-triviale normale Untergruppe der Form N/G_i mit $G_{i+1} \supsetneq N \supsetneq G_i$. Die Gruppe N ist normal in G_{i+1} . Fügt man den Term N in die Normalreihe \mathbf{G} ein, so erhält man eine echte Verfeinerung von \mathbf{G} . Deshalb ist \mathbf{G} keine Kompositionsreihe.

Besitzt umgekehrt die Normalreihe \mathbf{G} eine echte Verfeinerung, so gibt es einen Index i und eine Untergruppe K in G mit $G_i \triangleleft K \triangleleft G_{i+1}$. Dann ist die Faktorgruppe K/G_i eine nicht-triviale normale Untergruppe in G_{i+1}/G_i , also ist diese Gruppe nicht einfach. \square

Diese Charakterisierung einer Kompositionsreihe kann auch so ausgesprochen werden: Eine Normalreihe

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_n = G$$

in G ist eine Kompositionsreihe, falls für jedes $i = 0, \dots, n-1$ die Gruppe G_i maximal normal in G_{i+1} ist.

Als leichte Folgerung von Satz 2.2 erkennt man:

Satz 2.4. (Jordan–Hölder) *Ist G eine Gruppe mit einer Kompositionsreihe \mathbf{G} , so ist jede Kompositionsreihe \mathbf{H} in G zu \mathbf{G} äquivalent.*

Beispiele: (1) Die zyklische Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ der Ordnung $n > 0$ besitzt als endliche Gruppe eine Kompositionsreihe. Ist $n = m_1 m_2 \dots m_k$ eine Zerlegung von n in positive Faktoren, so erhält man eine zugehörige Normalreihe

$$\begin{aligned} \{e\} &= m_1 m_2 \dots m_k \mathbb{Z} / n\mathbb{Z} \triangleleft m_2 \dots m_k \mathbb{Z} / n\mathbb{Z} \triangleleft \dots \\ &\triangleleft m_{k-1} m_k \mathbb{Z} / n\mathbb{Z} \triangleleft m_k \mathbb{Z} / n\mathbb{Z} \triangleleft \mathbb{Z} / n\mathbb{Z}. \end{aligned}$$

Die Faktoren dieser Reihe sind zu $\mathbb{Z}/m_i\mathbb{Z}$ mit $1 \leq i \leq k$ isomorph. Wählt man alle m_i als (nicht notwendig verschiedene) Primzahlen, so ist diese Normalreihe eine Kompositionsreihe, da $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p einfach ist. Die Äquivalenz zweier solcher Kompositionsreihen gemäß Satz 2.4 entspricht der Eindeutigkeit der Primfaktorzerlegung der Zahl n bis auf Reihenfolge.

(2) Ist p eine Primzahl, so besitzt eine zyklische Gruppe der Ordnung $q = p^\nu$ mit $\nu \in \mathbb{N}$ genau eine Kompositionsreihe.

(3) Die additive Gruppe $(\mathbb{Z}, +)$ besitzt keine Kompositionsreihe, da jede Normalreihe als kleinsten Term ungleich $\{0\}$ eine unendliche zyklische Gruppe aufweist und weil diese nicht einfach ist.

(4) Es ist $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$ eine Kompositionsreihe in S_3 , da $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ und $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Die symmetrische Gruppe S_4 hat mehrere Kompositionsreihen, vgl. Übung 18. Für $n \geq 5$ kann man zeigen, daß A_n eine einfache Gruppe ist; also ist dann $\{e\} \trianglelefteq A_n \trianglelefteq S_n$ eine Kompositionsreihe in S_n .

§ 3 Auflösbare Gruppen

Eine *abelsche Normalreihe* in einer Gruppe G ist eine Normalreihe $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$, in der alle Faktoren G_{i+1}/G_i abelsch sind. Eine Gruppe G heißt *auflösbar*, wenn G eine abelsche Normalreihe besitzt.

Beispiele 3.1. (1) Jede abelsche Gruppe ist auflösbar.

(2) Die Gruppe $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k) \mid c = 0 \right\}$, k ein Körper, ist auflösbar. Wegen

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix}$$

definiert $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d)$ einen Homomorphismus $\alpha: G \rightarrow k^* \times k^*$ mit $\ker \alpha = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in GL_2(k) \right\}$. Die Gruppe $G_1 := \ker \alpha$ ist normal in G , und G_1 ist zur additiven Gruppe von k isomorph. Man erhält die abelsche Normalreihe

$$\{e\} = G_0 \trianglelefteq G_1 = \ker \alpha \trianglelefteq G_2 = G.$$

(3) Die symmetrische Gruppe S_4 ist auflösbar. Man erhält eine abelsche Normalreihe mit $G_1 = \{e, (12)(34), (13)(24), (14)(23)\}$ und $G_2 = A_4$ und $G_3 = S_4$.

Satz 3.2. Die Klasse der auflösbaren Gruppen ist abgeschlossen unter der Bildung von Untergruppen, homomorphen Bildern und Erweiterungen.

Beweis: Sei $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ eine abelsche Normalreihe in einer auflösbaren Gruppe G .

Ist $U \leq G$ eine Untergruppe, so bilden die $U \cap G_i$ ($i = 0, \dots, n$) eine abelsche Normalreihe in U , und U ist auflösbar. Denn jedes $U \cap G_i$ ist normal in $U \cap G_{i+1}$, und $(U \cap G_{i+1})/(U \cap G_i)$ ist zu $(U \cap G_{i+1})G_i/G_i \leq G_{i+1}/G_i$ isomorph (nach Satz I.4.3), also abelsch.

Ist $\varphi: G \rightarrow G'$ ein surjektiver Homomorphismus, so bilden die $\varphi(G_i)$ mit $0 \leq i \leq n$ eine abelsche Normalreihe in G' , und G' ist auflösbar. Denn jedes $\varphi(G_i)$ ist normal in $\varphi(G_{i+1})$, und die Abbildung $G_{i+1} \rightarrow \varphi(G_{i+1})/\varphi(G_i)$ mit $g \mapsto \varphi(g)\varphi(G_i)$ induziert einen surjektiven Homomorphismus von G_{i+1}/G_i auf $\varphi(G_{i+1})/\varphi(G_i)$; daher ist $\varphi(G_{i+1})/\varphi(G_i)$ abelsch.

Sei nun $1 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \rightarrow 1$ eine Erweiterung von N durch H , bei der N und H auflösbar sind. Es seien $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = H$ eine abelsche Normalreihe in H und $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_m = N$ eine abelsche Normalreihe in N . Wir setzen

$$G_i := \begin{cases} N_i & \text{für } i = 0, \dots, m, \\ \pi^{-1}(H_{i-m}) & \text{für } i = m+1, \dots, m+n. \end{cases}$$

Dann ist jedes G_i normal in G_{i+1} ($i = 1, \dots, m+n-1$), und für $i \geq m$ gilt $G_{i+1}/G_i \cong H_{i+1-m}/H_{i-m}$. Also ist (G_i) eine abelsche Normalreihe von G . \square

Korollar 3.3. *Das Produkt zweier normaler auflösbarer Untergruppen einer Gruppe G ist auflösbar.*

Beweis: Sind N_1, N_2 zwei normale auflösbare Untergruppen in G , so gilt $N_1N_2/N_2 \cong N_1/(N_1 \cap N_2)$. Mit 3.2 ist die rechte Seite auflösbar und damit auch N_1N_2 . \square

Korollar 3.4. *Sei p eine Primzahl. Jede endliche p -Gruppe ist auflösbar.*

Beweis: Wir benützen Induktion über $|G|$. Der Fall $|G| = 1$ ist trivial. Ist $|G| > 1$, so ist das Zentrum $Z(G)$ nicht-trivial nach Satz 1.5. Daher ist $G/Z(G)$ eine p -Gruppe mit $|G/Z(G)| < |G|$, also auflösbar nach Induktion. Da auch $Z(G)$ als kommutative Gruppe auflösbar ist, folgt die Behauptung aus Satz 3.2. \square

Satz 3.5. *Sei G eine endliche auflösbare Gruppe. Dann besitzt G eine abelsche Normalreihe $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$, so daß jedes G_{i+1}/G_i ($i = 0, \dots, n-1$) zyklisch von Primzahlordnung ist.*

Beweis: Wir haben in § 2 bemerkt, daß jede endliche Gruppe G eine Kompositionsreihe $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ besitzt; alle Faktoren G_{i+1}/G_i sind hier einfach. Wenn nun G auflösbar ist, so sind nach Satz 3.2 auch alle G_{i+1}/G_i auflösbar. Es reicht daher zu zeigen, daß eine einfache auflösbare Gruppe zyklisch von Primzahlordnung ist.

Sei also H eine einfache und auflösbare Gruppe. Weil $\{e\}$ und H die einzigen Normalteiler in H sind, kann eine abelsche Normalreihe von H nur aus $\{e\}$ und H bestehen, also muß H kommutativ sein. Für jedes $h \in H$, $h \neq e$ ist $\langle h \rangle$ eine nicht-triviale normale Untergruppe von H , also gleich H . Daher ist H zyklisch, und Satz I.1.13 impliziert, daß $|H|$ eine Primzahl sein muß. \square

3.6. Sei G eine Gruppe. Man nennt $[a, b] := aba^{-1}b^{-1}$ den *Kommutator* zweier Elemente $a, b \in G$. Die *Kommutatoruntergruppe* (oder *derivierte Gruppe*) von G ist definiert als

$$D(G) = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle.$$

Allgemeiner nennt man für zwei Untergruppen U, V von G die Untergruppe

$$[U, V] = \langle aba^{-1}b^{-1} \mid a \in U, b \in V \rangle$$

die *gegenseitige Kommutatorgruppe* von U und V . (Es gilt also $D(G) = [G, G]$.) Sind U und V normal in G , so auch $[U, V]$. Insbesondere ist $D(G)$ eine normale Untergruppe von G . Die Gruppe $G/D(G)$ ist abelsch und wird *Faktorkommutatorgruppe* von G genannt. Ist N ein Normalteiler in G , so ist G/N genau dann abelsch, wenn $D(G) \leq N$ gilt.

Man definiert $D^n(G)$ für alle $n \in \mathbb{N}$, indem man $D^0(G) = G$ und induktiv $D^n(G) = D(D^{n-1}(G)) = [D^{n-1}(G), D^{n-1}(G)]$ für $n \geq 1$ setzt. Man erhält die sogenannte *abgeleitete Reihe*

$$G = D^0(G) \supseteq D^1(G) \supseteq D^2(G) \supseteq D^3(G) \supseteq \dots$$

von G . Die Faktorgruppen sind abelsche Gruppen. Die abgeleitete Reihe kann zur Charakterisierung auflösbarer Gruppen herangezogen werden:

Satz 3.7. *Eine Gruppe G ist genau dann auflösbar, wenn es $m \in \mathbb{N}$ mit $D^m(G) = \{e\}$ gibt.*

Beweis: Gilt $D^m(G) = \{e\}$, so bilden die $G_i = D^{m-i}(G)$ eine abelsche Normalreihe von G , und G ist auflösbar.

Sei umgekehrt $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ eine abelsche Normalreihe von G . Für alle $r > 0$ gilt $[G_r, G_r] \subset G_{r-1}$, da $[G_r, G_r]$ der kleinste Normalteiler N von G_r ist, so daß die Faktorgruppe G_r/N abelsch ist. Wir behaupten, daß $D^i(G) \leq G_{n-i}$ für alle $i \leq n$. Offensichtlich ist $D^0(G) = G \leq G_n$. Nehmen wir induktiv an, daß $D^i(G) \leq G_{n-i}$ für ein $i < n$ gilt, so folgt $D^{i+1}(G) = [D^i(G), D^i(G)] \subset [G_{n-i}, G_{n-i}] \subset G_{n-(i+1)}$. Wir erhalten nun $D^n(G) \subset G_{n-n} = G_0 = \{e\}$. \square

Beispiel 3.8. Wir wollen zeigen, daß $D(S_n) = D(A_n) = A_n$ für alle ganzen Zahlen $n \geq 5$. Sind a, b, c, d, e fünf verschiedene Zahlen in $\{1, 2, \dots, n\}$, so gilt für die Dreierzyklen $x := (abd)$ und $y := (ace)$, daß $xyx^{-1}y^{-1} = (abc)$. Dies zeigt, daß jeder Dreierzyklus in A_n zu $D(A_n)$ gehört. Nach I.3.4 wird A_n von seinen Dreierzyklen erzeugt. Daraus folgt $A_n = D(A_n)$ und dann auch $A_n \leq D(S_n)$. Da $S_n/A_n \cong \{\pm 1\}$ abelsch ist, gilt aber auch $D(S_n) \leq A_n$; es folgt, daß $D(S_n) = A_n$.

Diese Beschreibung von $D(S_n)$ und $D(A_n)$ zeigt nach Satz 3.7, daß S_n und A_n für $n \geq 5$ nicht auflösbar sind. Man kann genauer zeigen, daß A_n für $n \geq 5$ *einfach* ist, also keine normale Untergruppen außer $\{e\}$ und A_n selbst hat.

§ 4 Nilpotente Gruppen

Eine Normalreihe

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

in einer Gruppe G heißt *zentrale Normalreihe* von G , wenn

- (1) jedes G_i normal in G ist ($0 \leq i \leq n$), und
- (2) jedes G_{i+1}/G_i im Zentrum von G/G_i enthalten ist ($0 \leq i < n$).

Satz 4.1. Sei \mathbf{G} eine Normalreihe in einer Gruppe G . Ist jeder Term G_i von \mathbf{G} normal in G , so ist \mathbf{G} genau dann eine zentrale Normalreihe, wenn

$$[G_{i+1}, G] \leq G_i$$

für jedes $i = 0, \dots, n-1$ gilt.

Beweis: Ist die Normalreihe \mathbf{G} zentral, so gilt $G_{i+1}/G_i \subset Z(G/G_i)$. Dies ist äquivalent mit der Aussage: Für alle $\gamma \in G_{i+1}$, $g \in G$ und alle $i = 0, \dots, n-1$ gilt $[\gamma G_i, g G_i] = e G_i$. Eine leichte Rechnung zeigt, daß dies jedoch gleichbedeutend mit $[\gamma, g] G_i = e G_i$, also mit $[\gamma, g] \in G_i$ ist. \square

4.2. Eine Gruppe G heißt *nilpotent*, falls es in G eine zentrale Normalreihe gibt. Die Länge einer kürzesten zentralen Normalreihe in einer nilpotenten Gruppe G wird auch die *Klasse von G* genannt. Eine nilpotente Gruppe G ist offenbar auflösbar, da die Faktoren in einer zentralen Normalreihe abelsch sind.

Beispiele: (1) Sei p eine Primzahl. Dann ist jede p -Gruppe G nilpotent. Wir können dazu annehmen, daß $G \neq \{e\}$. Dann ist nach Satz 1.5 auch das Zentrum $Z(G)$ nicht-trivial. Nach Induktion über $|G|$ besitzt $G/Z(G)$ eine zentrale Normalreihe (Z_i) . Mit Hilfe der Projektion $\pi: G \rightarrow G/Z(G)$ erhält man durch

$$\{e\} \trianglelefteq Z(G) \trianglelefteq \pi^{-1}(Z_1) \trianglelefteq \dots \trianglelefteq G$$



<http://www.springer.com/978-3-642-40532-7>

Algebra

Jantzen, J.C.; Schwermer, J.

2014, X, 458 S., Softcover

ISBN: 978-3-642-40532-7