Auflösbare Gruppen

Alexander Hölzle

16.05.2007

Inhaltsverzeichnis

1 Homomorphiesatz und Isomorphiesätze

Dieser Abschnitt dient lediglich als Auflistung wichtiger Sätze die bereits bekannt sein sollten, deshalb werden wir zum großen Teil auf Beweise verzichten.

SATZ 1.1 (Homomorphiesatz)**:** *Es seien G und H Gruppen und die Abbildung $\phi : G \to H$ sei homomorph. Dann ist*

$$\begin{aligned} \Phi : G/Kern(\phi) &\to Bild(\phi) \\ gKern(\phi) &\mapsto \phi(g). \end{aligned}$$

ein Gruppen-Isomomorphismus und damit ist $G/Kern(\phi) \cong \phi(G)$

Der Homomorphiesatz kann durch ein kommutatives Diagramm veranschaulicht werden. Dazu sei $\phi : G \to H$ ein Gruppen-Homomorphismus. Dann existiert nach dem Homomorphiesatz ein eindeutig bestimmter Homomorphismus $\Phi : G/Kern(\phi) \to H$ mit $\Phi \circ \pi = \phi$, so dass das folgende Diagramm kommutiert:

$$\begin{tikzcd} G \arrow[rr, "\pi"] \arrow[dr, "\phi"'] & & G/Kern(\phi) \arrow[dl, "\Phi"] \\ & H & \end{tikzcd}$$

Nun noch die beiden Isomorphiesätze.

SATZ 1.2 (Erster Isomorphiesatz)**:** *Sind H und K Untergruppen von einer Gruppe G. Für alle $h \in H$ gelte $hKh^{-1} = K$. Dann gilt*

(1) $H \cap K$ ist ein Normalteiler von H.

(2) $HK := \{hk | h \in H, k \in K\}$ ist eine Untergruppe von G.

(3) K ist ein Normalteiler von HK.

(4) Es besteht ein kanonischer Isomorphismus

$$H/(H \cap K) \cong HK/K.$$

***Beispiel**:*
Seien $n, m \in \mathbb{Z}$, $d := ggT(n,m)$ und $v := kgV(n,m)$. Dann gilt bekanntlich $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ bzw. $m\mathbb{Z} \cap n\mathbb{Z} = v\mathbb{Z}$. Mit dem ersten Isomorphiesatz folgt damit

$$\begin{aligned} (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} &\cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}), \\ \Rightarrow d\mathbb{Z}/n\mathbb{Z} &\cong m\mathbb{Z}/v\mathbb{Z}, \\ \Rightarrow \mathbb{Z}/\frac{n}{d}\mathbb{Z} &\cong \mathbb{Z}/\frac{v}{m}\mathbb{Z}. \end{aligned}$$

Wie wir aus der elementaren Zahlentheorie wissen, gilt für alle $n, m \in \mathbb{N}$ die Formel für das kleinste gemeinsame Vielfache $kgV(n,m) = \frac{nm}{ggT(n,m)}$, welche aus obiger Isomorphie gewonnen werden kann.

SATZ 1.3 (Zweiter Isomorphiesatz)**:** *Sind K und N zwei Normalteiler einer Gruppe G mit $K \subset N$. Dann ist N/K ein Normalteiler von G/K, und es besteht ein kanonischer Isomorphismus*

$$G/N \cong (G/K)/(N/K).$$

***Beispiel**:*
Seien $n, m \in \mathbb{Z}$ und $n\mathbb{Z}, m\mathbb{Z} \leq \mathbb{Z}$ Untergruppen von $(\mathbb{Z}, +)$. Wie wir bereits wissen gilt $n\mathbb{Z} \subseteq m\mathbb{Z}$ genau dann, wenn m ein Teiler von n ist. Es ist die Inklusion $25\mathbb{Z} \subsetneq 5\mathbb{Z}$ gültig, da 5 die Zahl 25 echt teilt und mit dem zweiten Isomorphiesatz folgt:

$$\mathbb{Z}/5\mathbb{Z} \cong (\mathbb{Z}/25\mathbb{Z})/(5\mathbb{Z}/25\mathbb{Z}) \cong (\mathbb{Z}/25\mathbb{Z})/(\mathbb{Z}/5\mathbb{Z}).$$

Zunächst mag die Isomorphie $\mathbb{Z}/5\mathbb{Z} \cong (\mathbb{Z}/25\mathbb{Z})/(\mathbb{Z}/5\mathbb{Z})$ erstaunen, betrachtet man jedoch bspw. die Restklasse $\overline{0} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$ aus $\mathbb{Z}/5\mathbb{Z}$ so erkennt man, dass darin die Restklassen $\overline{0} = \{\ldots, -30, -15, 0, 15, 30, \ldots\}$, $\overline{5} = \{\ldots, -25, -10, 5, 20, 35, \ldots\}$ und $\overline{10} = \{\ldots, -35, -20, -5, 10, 25, 40, \ldots\}$ aus $\mathbb{Z}/15\mathbb{Z}$ quasi enthalten sind.

2 Permutationsgruppen

In diesem Abschnitt werden wir zwei wichtige Arten von Gruppen repetieren und deren Kommutatorgruppen charakterisieren.

***Definition**:*
Die **symmetrische Gruppe** S_n (manchmal auch Sym_n) in $n \geq 1$ Wörtern ist eine Gruppe, die aus allen Permutationen einer Menge M mit n Elementen besteht. Dabei ist eine **Permutation** von M eine bijektive Abbildung von M in sich. Die zugehörige Verknüpfung ist die Komposition $\circ$, welche die „Hintereinanderschaltung“ zweier Abbildungen bewirkt. Das neutrale Element der Gruppe S_n ist die identische Abbildung $id(x) = x \in S_n, n \geq 1$.

Die symmetrische Gruppe besitzt $n!$ Elemente und ist im Allgemeinen nicht kommutativ. Ein Gruppenelement $\sigma \in S_n$ notieren wir durch

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

In der ersten Zeile sind die Urbilder (die n Wörter) notiert und in der zweiten Zeile die zugehörigen Bilder. Eine Verknüpfung zweier Permutationen $\sigma, \tau \in S_n$ ist wie folgt zu interpretieren: $\sigma \circ \tau := \sigma(\tau)$.

Jedes $\sigma \in S_n, n \geq 2$ kann als Produkt von Transpositionen (2-Zykel) geschrieben werden. Die Anzahl der Transpositionen in einer beliebigen Produktdarstellung eines $\sigma \in S_n$ ist unabhängig von der Darstellung entweder gerade oder ungerade. Entsprechend heißt σ **gerade** oder **ungerade**. Eine spezielle Untergruppe von S_n ist die so genannte alternierende Gruppe:

Definition:
Es sei $A_n := \{\sigma \in S_n \mid \sigma \text{ gerade } \} \subset S_n$ ist eine Untergruppe, sogar ein Normalteiler vom Index 2 in S_n. Die Untergruppe A_n heißt **alternierende Gruppe**.

Die alternierende Gruppe A_n besitzt genau $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ Elemente.

3 Das direkte Produkt

Definition:
Es seien G, H zwei beliebige Gruppen. Dann ist das kartesische Produkt

$$G \times H := \{(g,h)|g \in G, h \in H\}$$

bezüglich der Multiplikation

$$(g,h)(g',h') := (gg', hh')$$

eine Gruppe. Insbesondere ist $e = (e_G, e_H)$ das neutrale Element, wobei hier der Deutlichkeit halber e_G das neutrale Element von G und e_H das neutrale Element von H bzeichnet. Das inverse Element zu (g,h) ist entsprechend (g^{-1}, h^{-1}). Die Gruppe $G \times H$ heißt **direktes Produkt** von G und H.

Offenbar gilt stets $|G \times H| = |G| \cdot |H|$ - dies folgt unmittelbar aus der Definition. Die Abbildungen

$$i_G : G \to G \times H, g \mapsto (g, e_H)$$
$$i_H : H \to G \times H, h \mapsto (e_G, h)$$

sind injektive Gruppenhomomorphismen, also ist

$$G \cong i_G(G) = G \times \{e_H\} \text{ und } H \cong i_H(H) = \{e_G\} \times H.$$

Wir identifizieren G mit $G \times \{e_H\} \subset G \times H$, also $g \in G$ entspricht $(g, e_H) \in G \times H$. Analog identifizieren wir H mit $\{e_H\} \times H$. Auf diese Weise fassen wir die „direkten Faktoren“ G und H von $G \times H$ als Untergruppen von $G \times H$ auf.

Es sei G eine Gruppe, dann bezeichnen wir die triviale Untergruppe $\{e\}$ von G mit $E := \{e\}$, wobei e das neutrale Element der Gruppe G ist.

4 Normalreihen und Kompositionsreihen

4.1 Normalreihen

Betrachten wir das direkte Produkt der Gruppen G_1, G_2, also $G = G_1 \times G_2$ dann gilt $G_1 \cap G_2 = \{0\}$ bzw. $G_1 + G_2 = G$. Beachtet man dies und wendet den ersten Isomorphiesatz an, so erhält man gerade die Isomorphie $G/(G_1 \times E) \cong G_2$. Aufgrund der Isomorphie $G_2 \cong G/(G_1 \times E)$ ist die Struktur von G bestens bekannt, wenn wir den Normalteiler $G_1 \times E \cong G_1$ und die Faktorgruppe $G/(G_1 \times E)$ genau kennen.

Allerdings ist im Allgemeinen die Struktur einer beliebigen Gruppe G nicht eindeutig durch die Struktur eines Normalteilers N von G und der Faktorgruppe G/N bestimmt, wie folgendes Beispiel zeigen wird.

Beispiel:
Nach dem Struktursatz über endliche abelsche Gruppen gibt es genau zwei nicht-isomorphe Gruppen der Ordnung $4 = 2 \cdot 2$. Im einzelnen sind das die Gruppe $G := (\mathbb{Z}_4, +)$ bestehend aus den Restklassen $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ und der Kleinschen Vierergruppe $V_4 := (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ die bekanntlich aus den Tupeln $\big\{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})\big\}$ besteht.

Jede Untergruppe einer abelschen Gruppe ist Normalteiler, also kann man zu jeder Untergruppe eine Faktorgruppe erzeugen. Untergruppen, Faktorgruppen, Produkte und direkte Summen abelscher Gruppen sind wieder abelsch. Die Gruppe G besitzt also den Normalteiler $\{\overline{0}, \overline{2}\} \cong \mathbb{Z}_2$ und die Gruppe V_4 den Normalteiler $\{\overline{0}, \overline{2}\} \times E \cong \mathbb{Z}_2$. Beide Gruppen G und V_4 besitzen also einen zu $\mathbb{Z}_2$ isomorphen Normalteiler, deshalb sind die Faktorgruppen ebenfalls isomorph und dies obwohl G und V_4 zwei unterschiedliche nicht isomorphe Gruppen sind.

Gilt eine Eigenschaft $\mathcal{E}$ in einem Normalteiler N und einer Faktorgruppe G/N, so kann im Allgemeinen nicht darauf geschlossen werden, dass die Eigenschaft $\mathcal{E}$ auch in der Gruppe G gilt. Im Speziellen existieren jedoch bestimmte Eigenschaften $\mathcal{E}'$, die in G gelten, sofern bekannt ist, dass sie in einem Normalteiler N und der Faktorgruppe G/N gelten. Oftmals ist jedoch bereits die Verifiktion einer Eigenschaft recht aufwendig: Deshalb versucht man das Problem solange zu „verschieben“ und dabei die „Übertragungseigenschaft“ zu nutzen, bis es sich quasi von selbst erledigt. Will man also konkret überprüfen, ob eine Eigenschaften $\mathcal{E}'$ in einem Normalteiler N erfüllt ist, so ist es hinreichend einen Normalteiler N_1 von $N_0 := N$ und die Faktorgruppe N_0/N_1 zu untersuchen. Schließlich überträgt sich die Eigenschaft $\mathcal{E}'$ von N_1 bzw. N_0/N_1 auf die Gruppe N_0. Diese Vorgehensweise iterieren wir, bis man schließlich auf Untergruppen stößt, die offensichtlich die untersuchte Eigenschaft erfüllen. Um eine derartig elegante Problemreduktion zu erreichen, ist die Wahl der Normalteiler im Allgemeinen sehr wichtig, doch auch hier gibt es Situationen in denen denen die Wahl nicht so bedeutend ist.

Definition:
Es sei G eine Gruppe. Eine Folge von Gruppen $\{G_i\}$ heißt eine **absteigende Gruppenkette** von G, wenn gilt

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_i \supseteq G_{i+1} \supseteq \ldots$$

Die Kette heißt **normal**, wenn G_{i+1} Normalteiler in G_i ist ($i \geq 1$). Die Faktorgruppen G_i/G_{i+1} heißen die **Faktoren** der normalen Kette. Eine normale Kette heißt **zyklisch** bzw. **abelsch**, wenn alle Faktoren zyklisch bzw. abelsch sind. Eine endliche normale Kette

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{m-1} \supseteq G_m = N,$$

in der N ein Normalteiler von G ist, heißt eine **Normalreihe von** G **nach** N. Im Falle $N = \{e\}$ spricht man nur von einer Normalreihe der Länge $m-1$ von G. Zwei Normalreihen $G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m$ und $H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n$ heißen **äquivalent**, wenn $m = n$ ist, und wenn es eine Permutation der Indizes gibt $i \mapsto \pi(i)$, so dass G_i/G_{i+1} isomorph ist zu $H_{\pi(i)}/H_{\pi(i)+1}$.

Man beachte, dass in der Definition der Normalreihen nur gefordert wird, dass G_{i+1} Normalteiler von G_i ist, aber nicht notwendig Normalteiler von G.

Für das folgende Beispiel b) sollte man sich in Erinnerung rufen, dass die alternierende Gruppe A_n definiert ist durch $A_n := \{\sigma \in S_n | \sigma \text{ gerade } \}$ und eine Untergruppe von S_n ist. Da jede Untergruppe vom Index 2 ein Normalteiler ist und A_n als Untergruppe von S_n gerade Index 2 besitzt, folgt, dass A_n Normalteiler von S_n. Für alle $n \geq 3, n \neq 4$ ist A_n der einzige nicht triviale Normalteiler von S_n und für $n = 4$ ist neben A_4 noch V_4 ein Normalteiler. Als Ergänzung sei daran erinnert, dass A_n von der Ordnung $\frac{n!}{2}$ und V_4 von der Ordnung 4 ist.

Beispiel:

a) Es ist $\mathbb{Z} \supset p\mathbb{Z} \supset p^2\mathbb{Z} \supset \ldots$ eine unendliche absteigende normale Kette, da jede Untergruppe ($p^k\mathbb{Z},\ k \in \mathbb{N}$) der abelschen Gruppe $(\mathbb{Z}, +)$ ein Normalteiler von $\mathbb{Z}$ ist. Beachtet man, dass $p^i\mathbb{Z},\ i \in \mathbb{N}$ mit $i < k$ ganz $p^k\mathbb{Z}$ umfasst, so ist klar, dass $p^k\mathbb{Z}$ auch ein Normalteiler für alle $p^i\mathbb{Z},\ i \in \mathbb{N}$ mit $i < k$ ist.

b) Die Kette $S_4 \supset A_4 \supset V_4 \supset E$, mit der Kleinschen Vierergruppe V_4 und der alternierenden Gruppe A_4 ist eine Normalreihe von S_4. Es sind A_4, V_4 Normalteiler von S_4, damit ist insbesondere V_4 Normalteiler von A_4, da $A_4 \supset V_4$; es handelt sich also tatsächlich um Normalreihen. Die Kette $S_4 \supset S_4 \supset A_4 \supset A_4 \supset V_4 \supset V_4 \supset \langle(1,2)(3,4)\rangle \supset E$ ist ebenfalls eine Normalreihe.

c) Die Gruppenketten

$$\mathbb{Z}_{36} = \mathbb{Z}/36\mathbb{Z} \supset \underbrace{2\mathbb{Z}/36\mathbb{Z}}_{\cong\mathbb{Z}/18\mathbb{Z}} \supset \underbrace{12\mathbb{Z}/36\mathbb{Z}}_{\cong\mathbb{Z}/3\mathbb{Z}} \supset E$$

und

$$\mathbb{Z}_{36} \supset \underbrace{3\mathbb{Z}/36\mathbb{Z}}_{\cong \mathbb{Z}/12\mathbb{Z}} \supset \underbrace{6\mathbb{Z}/36\mathbb{Z}}_{\cong \mathbb{Z}/6\mathbb{Z}} \supset E$$

sind beide normal und zueinander äquivalent. Die an den Ketten notierte Isomorphie ergibt sich aufgrund des Isomorphimus $\phi : n\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/\frac{m}{n}\mathbb{Z}$ mit $\overline{a} \mapsto \frac{a}{n} \mod \frac{m}{n}$, falls n ein Teiler von m ist.
Bildet man nun die Faktoren G_i/G_{i+1}, also z.B. $(3\mathbb{Z}/36\mathbb{Z})/(6\mathbb{Z}/36\mathbb{Z}) \cong (\mathbb{Z}/12\mathbb{Z})/(\mathbb{Z}/6\mathbb{Z})$, so besitzt dieser Faktor die Ordnung $\frac{12}{6} = 2$ und ist als Untergruppe einer zyklischen Gruppe selbst wieder zyklisch. Da jede zyklische Gruppe abelsch ist und es (bis auf Isomorphie) nur eine abelsche Gruppe $\mathbb{Z}/2\mathbb{Z}$ gibt, muss der Faktor isomorph zu $\mathbb{Z}/2\mathbb{Z}$ sein. Analog kann man bei den übrigen Faktoren argumentieren. Es ergeben sich dann die Faktoren $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ in der jeweils angegebenen Reihenfolge. D.h. es existiert eine entsprechend Permutation, welche die Untergruppen derart umordnet, so dass die Fakoren zueinander isomorph sein müssen.

Sind in einer gegebenen Kette zwei Glieder identisch, d.h. gilt $G_i = G_{i+1}$ für wenigstens ein i, dann nenen wir diese eine **Kette mit Wiederholungen**. Ansonsten sprechen wir von einer **Kette ohne Wiederholungen**. Offenbar werden aus zwei äquivalenten Normalreihen mit Wiederholungen, durch Fortlassen der überflüssigen Terme (der Wiederholungen), zwei äquivalente Normalreihen ohne Wiederholungen. Aufgrund der Äquivalenz beider Ketten, existiert eine bijektive Zuordnung der Faktoren der einen Normalreihe zu den isomorphen Faktoren der anderen Normalreihe. Dabei werden natürlich den nicht trivialen Faktoren der einen Kette auch nicht triviale Faktoren der anderen Kette zugeordnet. Deshalb haben nach dem Weglassen der überflüssigen Terme, die dadurch entstehenden Normalreihen dieselbe Anzahl an Faktoren und damit auch dieselbe Länge. Ordnet man die Faktoren in geeigneter Reihenfolge an, so sind diese auch wieder isomorph zueinander.

SATZ 4.1: *Eine Normalreihe $G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = N$ der Gruppe G nach dem Normalteiler N ist äquivalent zu einer Normalreihe $G_1/N \supseteq G_2/N \supseteq \ldots \supseteq G_m/N = E$ der Faktorgruppe G/N.*

Beweis. Da $G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = N$ eine Normalreihe von G nach N ist, muss N gemäß Definition ein Normalteiler von G und G_{i+1} ein Normalteiler von G_i $(1 \leq i \leq m-1)$ sein. N ist als Normalteiler von G auch Normalteiler von G_i $(1 \leq i \leq m-1)$ mit der Inklusion $G_{i+1} \subseteq N$ $(1 \leq i \leq m-1)$. Wir können also den zweiten Isomorphiesatz anwenden, es ist also G_{i+1}/N Normalteiler von G_i/N und die Faktorgruppe $(G_i/N)/(G_{i+1}/N)$ ist isomorph zu G_i/G_{i+1}. Dies zeigt, dass $G_1/N \supseteq G_2/N \supseteq \ldots \supseteq G_m/N = E$ eine zu $G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = N$ äquivalente Normalreihe ist. □

Beispiel:
Die Normalreihe $S_4 \supset A_4 \supset V_4$ ist äquivalent zu $S_4/V_4 \supset A_4/V_4 \supset E$. Betrachten wir

die Gruppenordnungen der ersten Normalreihe $4! = 24 \geq \frac{4!}{2} = 12 \geq 4$ und der zweiten Normalreihe $\frac{4!}{4} = 6 \geq \frac{12}{4} = 3 \geq 1$, dann sieht man, dass die Ordnungen der entsprechenden Faktorgruppen $\frac{24}{12} = 2, \frac{12}{4} = 3$ bzw. $\frac{6}{3} = 2, \frac{3}{1} = 3$ betragen. D.h. man kann die Faktorgruppen derart umordnen, dass diese äquivalent zueinander sind.

Man betrachte weiter die Isomorphien $S_4/V_4 \cong S_3$ und $A_4/V_4 \cong S_2$, deshalb sind beide Normalreihen von oben auch zu $S_3 \supset S_2 \supset E$ isomorph.

4.2 Verfeinerungssatz, Lemma von Zassenhausen

Es wird nun untersucht, wie zwei beliebige Normalreihen zueinander liegen. Dazu eine

Definition:
Eine Normalreihe $G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m$ heißt **Verfeinerung** der Normalreihe $G_1 = H_1 \supseteq H_2 \supseteq \ldots \supseteq H_m$, wenn jeder der Gruppen H_i $(1 \leq i \leq k)$ unter den Gruppen G_j $(1 \leq j \leq m)$ vorkommt, d.h. $\{H_1, \ldots, H_k\} \subseteq \{G_1, \ldots, G_m\}$.

Das wohl bedeutendsten Ergebniss, das alle Normalreihen beherrscht, ist der folgende Verfeinerungssatz von Schreier.

SATZ 4.2 (Verfeinerungssatz)**:** *Je zwei Normalreihen einer Gruppe besitzen äquivalente Verfeinerungen.*

Für den Beweis dieses wichtigen Verfeinerungssatzes ist das so genannte Lemma von Zassenhausen von grundlegender Bedeutung.

Lemma 4.3: (Zassenhausen)
Sind A_1, A, B_1, B Untergruppen von G und A_1 Normalteiler von A, B_1 Normalteiler von B, dann gilt:

1) $A_1(A \cap B_1)$ ist Normalteiler von $A_1(A \cap B)$,

2) $B_1(A_1 \cap B)$ ist Normalteiler von $B_1(A \cap B)$,

3) $A_1(A \cap B)/A_1(A \cap B_1) \cong B_1(A \cap B)/B_1(A_1 \cap B)$.

Beweis. Das die Produkte $A_1(A \cap B_1)$ und ähnliche tatsächlich wohldefinierte Gruppen sind, folgt aus dem ersten Isomorphiesatz aus Abschnitt 1. Um den Überblick über alle vorkommenden Gruppen nicht zu verlieren, ordnen wir sie in folgenden Diagramm an.

$$\begin{tikzcd}
A \arrow[d, dash] & & B \arrow[d, dash] \\
A_1(A\cap B) \arrow[dr, dash] \arrow[dd, dash] & & B_1(A\cap B) \arrow[dl, dash] \arrow[dd, dash] \\
& A\cap B \arrow[dd, dash] & \\
A_1(A\cap B_1) \arrow[d, dash] \arrow[dr, dash] & & B_1(A_1\cap B) \arrow[d, dash] \arrow[dl, dash] \\
A_1 & (A\cap B_1)\cap(A_1\cap B) & B_1
\end{tikzcd}$$

Wir wenden den ersten Isomorphiesatz, Satz 1.2, an mit

$$H := A\cap B \quad \text{und} \quad K := A_1(A\cap B_1).$$

Die Voraussetzung $hKh^{-1} \in K$ für alle $h \in H$ ist tatsächlich erfüllt, denn für alle $h \in A\cap B, a \in A_1$ und $b \in A\cap B_1$ gilt

$$h(ab)h^{-1} = (ha\underbrace{h^{-1})(h}_{=1}bh^{-1}) \in A_1(A\cap B_1),$$

weil –nach Voraussetzungen– A_1 ein Normalteiler von A und B_1 ein Normalteiler von B ist. Es sollte klar sein, dass Elemente aus $A\cap B_1$ notwendig aus B_1 sind. Da der Schnitt von Untergruppen und das Komplexprodukt von Untergruppen wieder eine Untergruppe ergibt, ist $K = A_1(A\cap B_1)$ eine Untergruppe von G, ja sogar nach Satz 1.2 ein Normalteiler von HK. Es ist

$$HK = \underbrace{(A\cap B)}_{h\in}\underbrace{A_1}_{a\in}\underbrace{(A\cap B_1)}_{b\in} = A_1(A\cap B),$$

denn für alle $h \in (A\cap B),\ a \in A_1,\ b \in (A\cap B_1) \Rightarrow hab \in (A\cap B)A_1(A\cap B_1)$ ist

$$hab = \underbrace{(hah^{-1})}_{\in A_1}\underbrace{(hb)}_{\in B} \in A_1(A\cap B),$$

da A_1 Normalteiler von A und Elemente das Element h notwendig aus A stammt. Umgekehrt gilt

$$ah = \underbrace{h}_{\in(A\cap B)} \underbrace{(h^{-1}ah)}_{\in A_1} \underbrace{1}_{\in(A\cap B_1)} \in (A\cap B)A_1(A\cap B_1).$$

Außerdem gilt

$$H \cap K = (A\cap B) \cap A_1(A\cap B_1) = (A_1 \cap B)(A\cap B_1),$$

denn für $a \in A_1,\ b \in (A\cap B_1)$ mit $ab \in A\cap B$ ist auch $a \in B$, also $ab \in (A_1\cap B)(A\cap B_1)$; die andere Inklusion ist trivial. Nach dem Isomorphiesatz gilt daher $HK/K \cong H/(H \cap K)$, also

$$A_1(A\cap B)/A_1(A\cap B_1) \cong (A\cap B)/(A_1 \cap B)(A\cap B_1).$$

Durch Vertauschen der Rollen von A und B ergibt sich

$$B_1(A\cap B)/B_1(A_1\cap B) \cong (A\cap B)/(A \cap B_1)(A_1\cap B)$$

und aufgrund der Identität $(A_1\cap B)(A\cap B_1) = (A\cap B_1)(A_1\cap B)$ steht auf der rechten Seite jeweils dasselbe. Also sind die Gruppen auf den linken Seiten isomorph. □

In der englischsprachigen Literatur ist dieses Lemma auch als „Butterfly Lemma“ (so bspw. im Buch von Serge Lang) bekannt, betrachtet man die Skizze der Untergruppen, so wird schnell klar woher der Name rührt. Betrachtet man die ersten beiden Isomorphiesätze und vergleicht diese mit dem Lemma von Zassenhausen, so könnte man auch auf die Idee kommen, dieses Lemma als dritten Isomorphiesatz zu betiteln.

Das eben bewiesene Lemma können wir sogleich hilfreich für den nachgeholten Beweis des Verfeinerungssatzes verwenden. Wir erinnern uns, dieser besagt, dass *je zwei Normalreihen einer Gruppe äquivalente Verfeinerungen besitzt.*

Beweis. Es seien $G = G_1 \supseteq G_2 \subseteq \ldots \supseteq G_m = E$ und $G = H_1 \supseteq H_2 \subseteq \ldots \supseteq H_n = E$ zwei Normalreihen der Gruppe G. Für $1 \leq i \leq m-1$ und $1 \leq j \leq n$ definieren wir

$$G_{i,j} := G_{i+1}(H_j \cap G_i).$$

Da wir Normalreihen untersuchen ist G_{i+1} Normalteiler von G_i. Zum einen ist $G_{i,1} = G_{i+1}(G \cap G_i) = \{g'g|\ g' \in G_{i+1},\ g \in G_i\} = G_i$, da $G_i \subseteq G_{i+1}$. Zum anderen gilt $G_{i,n} = G_{i+1}E = G_{i+1}$. Da H_{j+1} Normalteiler von H_j ist, können wir Teil 1) des Lemmas von Zassenhausen anwenden, deshalb ist $G_{i,j+1} = G_{i+1}(H_{j+1} \cap G_i)$ ein Normalteiler von $G_{i,j} = G_{i+1}(H_j \cap G_i)$. Wir erhalten damit durch Einschieben der $G_{i,j}$ zwischen G_i und G_{i+1} eine Verfeinerung der ersten Reihe

$$G = G_{1,1} \supseteq G_{1,2} \subseteq \ldots \supseteq G_{1,n} = G_{2,1} \supseteq G_{2,2} \supseteq \ldots G_{m-1,n} \supseteq G_m = E.$$

Entsprechend definiert man für $1 \leq j \leq n-1$ und $1 \leq i \leq m$

$$H_{j,i} := H_{j+1}(G_i \cap H_j)$$

und erhält ebenso eine Verfeinerung der zweiten Reihe

$$H = H_{1,1} \supseteq H_{1,2} \subseteq \ldots \supseteq H_{1,m} = H_{2,1} \supseteq H_{2,2} \supseteq \ldots H_{n-1,m} \supseteq H_n = E.$$

Beide Verfeinerungen haben die Länge $(n-1)(m-1)$. Außerdem haben wir für $1 \leq j \leq n-1$ und $1 \leq i \leq m-1$ die Isomorphie der Faktoren $G_{i,j}/G_{i,j+1} \cong H_{j,i}/H_{j,i+1}$, die wir erhalten, wenn wir das Lemma von ZASSENHAUSEN anwenden und $A := G_i,\ B := H_j,\ A_1 := G_{i+1},\ B_1 := H_{j+1}$ setzen. □

4.3 Beispiel zum Verfeinerungssatz

Um das nun folgenden Beispiel vollständig verstehen zu können, sollten Sie den eben erbrachten Beweis des Verfeinerungssatzes verstanden haben.

Beispiel:
Wir betrachten die Normalreihen

$$G_1 := \mathbb{Z} \supset G_2 := 2\mathbb{Z} \supset G_3 := 10\mathbb{Z} \supset G_4 := 30\mathbb{Z} \supset G_5 := \{0\}$$

und

$$H_1 := \mathbb{Z} \supset H_2 := 3\mathbb{Z} \supset H_3 := 24\mathbb{Z} \supset H_4 := \{0\}$$

von $\mathbb{Z}$. Wir basteln uns nun, wie im Beweis des Verfeinerungssatzes, neue Kettenglieder, die sich zwischen die bereits bestehenden einordnen. Beachten Sie bitte die folgenden wichtigen Aspekte

- Wir handtieren mit additiven Gruppen, deshalb ist das Komplexprodukt nun quasi die Komplexsumme.
- $n\mathbb{Z} \subset m\mathbb{Z} \ \Leftrightarrow \ m|n$.
- $d\mathbb{Z}$ ist die kleinste Untergruppe von $\mathbb{Z}$, die $n\mathbb{Z}$ und $m\mathbb{Z}$ enthält $(m, n \in \mathbb{N})$ genau dann, wenn $d = ggT(n, m)$.
- $t\mathbb{Z} = n\mathbb{Z} \cap m\mathbb{Z} \ \Leftrightarrow \ t = kgV(n, m)$.

Den zweiten Punkt nennt man im Speziellen auch Lemma von Bézout und im Allgemeinem ist dies eine Folgerung aus dem Hauptsatz über den größten gemeinsamen Teiler.

$$\begin{aligned}
G_{1,1} &= G_2 + (G_1 \cap H_1) = 2\mathbb{Z} + (\mathbb{Z} \cap \mathbb{Z}) = \mathbb{Z}, \\
G_{1,2} &= G_2 + (G_1 \cap H_2) = 2\mathbb{Z} + (\mathbb{Z} \cap 3\mathbb{Z}) = 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}, \\
G_{1,3} &= G_2 + (G_1 \cap H_3) = 2\mathbb{Z} + (\mathbb{Z} \cap 24\mathbb{Z}) = 2\mathbb{Z} + 24\mathbb{Z} = 2\mathbb{Z}, \\
G_{1,4} &= G_2 + (G_1 \cap H_4) = 2\mathbb{Z} + (\mathbb{Z} \cap \{0\}) = 2\mathbb{Z}.
\end{aligned}$$

$$\begin{aligned}
G_{2,1} &= G_3 + (G_2 \cap H_1) = 10\mathbb{Z} + (2\mathbb{Z} \cap \mathbb{Z}) = \mathbb{Z}, \\
G_{2,2} &= G_3 + (G_2 \cap H_2) = 10\mathbb{Z} + (2\mathbb{Z} \cap 3\mathbb{Z}) = 10\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}, \\
G_{2,3} &= G_3 + (G_2 \cap H_3) = 10\mathbb{Z} + (2\mathbb{Z} \cap 24\mathbb{Z}) = 10\mathbb{Z} + 24\mathbb{Z} = 2\mathbb{Z}, \\
G_{2,4} &= G_3 + (G_2 \cap H_4) = 10\mathbb{Z} + (2\mathbb{Z} \cap \{0\}) = 10\mathbb{Z}.
\end{aligned}$$

$$\begin{aligned}
G_{3,1} &= G_4 + (G_3 \cap H_1) = 30\mathbb{Z} + (10\mathbb{Z} \cap \mathbb{Z}) = 30\mathbb{Z} + 10\mathbb{Z} = 10\mathbb{Z}, \\
G_{3,2} &= G_4 + (G_3 \cap H_2) = 30\mathbb{Z} + (10\mathbb{Z} \cap 3\mathbb{Z}) = 30\mathbb{Z} + 30\mathbb{Z} = 30\mathbb{Z}, \\
G_{3,3} &= G_4 + (G_3 \cap H_3) = 30\mathbb{Z} + (10\mathbb{Z} \cap 24\mathbb{Z}) = 30\mathbb{Z} + 120\mathbb{Z} = 30\mathbb{Z}, \\
G_{3,4} &= G_4 + (G_3 \cap H_4) = 30\mathbb{Z} + (10\mathbb{Z} \cap \{0\}) = 30\mathbb{Z}.
\end{aligned}$$

$$\begin{aligned}
G_{4,1} &= G_5 + (G_4 \cap H_1) = \{0\} + (30\mathbb{Z} \cap \mathbb{Z}) = \{0\} + 30\mathbb{Z} = 30\mathbb{Z}, \\
G_{4,2} &= G_5 + (G_4 \cap H_2) = \{0\} + (30\mathbb{Z} \cap 3\mathbb{Z}) = \{0\} + 30\mathbb{Z} = 30\mathbb{Z}, \\
G_{4,3} &= G_5 + (G_4 \cap H_3) = \{0\} + (30\mathbb{Z} \cap 24\mathbb{Z}) = \{0\} + 120\mathbb{Z} = 120\mathbb{Z}, \\
G_{4,4} &= G_5 + (G_4 \cap H_4) = \{0\} + (30\mathbb{Z} \cap \{0\}) = \{0\}.
\end{aligned}$$

Wir konnte also lediglich die zusätzliche Untergruppe $G_{4,3} = 120\mathbb{Z}$ als zusätzliches Kettenglied berechnen. Analog berechnet man auch die zusätzlichen Faktoren zur zweiten Gruppenkette. Letztlich erhalten wir die beiden Verfeinerungen (ohne Wiederholungen)

$$\begin{gathered}
\mathbb{Z} \supset 2\mathbb{Z} \supset 10\mathbb{Z} \supset 30\mathbb{Z} \supset 120\mathbb{Z} \supset \{0\}, \\
\mathbb{Z} \supset 3\mathbb{Z} \supset 6\mathbb{Z} \supset 24\mathbb{Z} \supset 120\mathbb{Z} \supset \{0\},
\end{gathered}$$

mit den Faktoren

$$\begin{gathered}
\mathbb{Z}_2, \mathbb{Z}_5, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}; \\
\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}.
\end{gathered}$$

Man sieht, dass wir eine bijektive Abbildung angeben können, d.h. die Normalreihen sind äquivalent.

4.4 Kompositionsreihen

Aufgrund des Verfeinerungssatzes ist es naheliegend nur noch diejenigen Normalreihen zu untersuchen, die nicht verfeinert werden können, ohne dass Wiederholungen auftreten. Der erste Teil der nun folgenden Definition sollte Sie an die analoge Definition der maximalen Ideale erinnern. Beim zweiten Teil sollten Sie sich in Erinnerung rufen, dass die trivialen Untergruppen $\{e\}$ und G von G stets Normalteiler sind.

Definition:

1. Ein Normalteiler M einer Gruppe G heißt **maximal**, wenn M von G verschieden ist und wenn für jeden Normalteiler N von G mit $M \subseteq N \subseteq G$ stets $M = N$ oder $N = G$ folgt.

2. Eine Gruppe $G \neq \{e\}$ heißt **einfach**, wenn $\{e\}$ und G die einzigen Normalteiler von G sind.

Die einfachen Gruppen sind also genau diejenigen, in denen $\{e\}$ der maximale Normalteiler ist – dies folgt ganz einfach aufgrund des Mangels an Normalteilern. Als Verallgemeinerung hiervon ist das folgende einfache Ergebnis anzusehen.

Lemma 4.4: *Es ist $M \subseteq G$ genau dann ein maximaler Normalteiler, wenn G/M einfach ist.*

Beweis. Wir betrachten den kanonischen Epimorphismus $\pi : G \to G/N$ eines beliebigen Normalteilers. Wir wissen, dass die Abbildung π jedem Gruppenelement g seine Nebenklasse gN zuweist. Da die Abbildung π ein surjektiver Homomorphismus ist bildet sie Normalteiler aus G auf Normalteiler in G/N ab. Es gilt sogar für Normalteiler U von G:

$$U \mapsto \pi(U)$$

ist eine bijektive Abbildung, d.h. $\pi(U)$ ist genau dann Normalteiler in G/N, wenn U Normalteiler von G ist. Außerdem stimmen die Indizes $[G : U] = [G/N : \pi(U)]$ überein. Es ist z.B. $M \neq G$ äquivalent zu $G/M \neq E$. Zwischen G und N liegen also genau dann keine weiteren Normalteiler, wenn $G/G = E$ und G/N keine weiteren Normalteiler liegen. Dies ist genau dann der Fall, wenn G/N einfach ist. □

Beispiel:
Jeder Normalteiler N von G, dessen Index in G eine Primzahl p ist, ist maximal, denn die Gruppe G/N hat die Ordnung $\frac{|G|}{|N|} = p$ (nach Lagrange). Ein Gruppe von Primzahlordnung besitzt nur die trivialen Normalteiler, d.h. sie ist einfach.

Wir konkretisieren und betrachten die Gruppe $G := (\mathbb{Z}/6\mathbb{Z}, +)$ und die Untergruppe $U := \{\overline{0}, \overline{2}, \overline{4}\}$ von G. Nach Lagrange gilt $|G| = |U| \cdot [G : U]$, d.h. es muss also $6 = 3 \cdot 2$ gelten, wobei $[G : U] = 2$ eine Primzahl ist. Es ist also G ein maximaler Normalteiler.

Nun haben wir die nötigen Begriffe, um die Normalreihen zu charakterisieren, die nicht mehr verfeinert werden können, ohne das Wiederholungen auftreten.

Definition:
Eine Normalreihe $G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = E$ heißt eine **Kompositionsreihe** von G, wenn G_{i+1} maximaler Normalteiler in G_i ist $(1 \leq i < m)$. Die Faktoren einer Kompositionsreihe heißen **Kompositionsfaktoren**.

Mit dem eben gezeigten ist klar, dass eine Normalreihe genau dann eine Kompositionsreihe ist, wenn die Faktoren G_i/G_{i+1} einfache Gruppen sind.

Beispiel:

a) $\mathbb{Z}_{24} \supset \mathbb{Z}_8 \supset \mathbb{Z}_4 \supset \mathbb{Z}_2 \supset \{0\}$,
$\mathbb{Z}_{24} \supset \mathbb{Z}_{12} \supset \mathbb{Z}_4 \supset \mathbb{Z}_2 \supset \{0\}$,
$\mathbb{Z}_{24} \supset \mathbb{Z}_{12} \supset \mathbb{Z}_6 \supset \mathbb{Z}_2 \supset \{0\}$,
sind Kompositionsreihen, denn die Faktoren sind Gruppen von Primzahlordnung. Dazu betrachte man schlicht den Quotienten der Ordnungen $\frac{|G_i|}{|G_{i+1}|}$ zweier aufeinanderfolgender Gruppen innerhalb der Kette.

b) $\mathbb{Z}_4 \supset \mathbb{Z}_2 \supset \{0\}$ und $\mathbb{Z}_2 \times \mathbb{Z}_2 \supset \{0\}$ haben die gleichen Faktoren, nämlich $\mathbb{Z}_2$. Das zeigt, dass nichtisomorphe Gruppen durchaus äquivalente Kompositionsreihen besitzen können.

c) Ist $G = N_1 N_2 \ldots N_k$ inneres Produkt einfacher Normalteiler N_i $(1 \leq i \leq k)$, dann ist $G \supset N_2 \ldots N_k \supset N_3 \ldots N_k \supset \ldots \supset N_k \supset E$ eine Kompositionsreihe mit den Faktoren $N_1, N_2, \ldots, N_k$.

4.5 Satz von Jordan-Hölder

Der französische Mathematiker Camille JORDAN (1838-1922) bewies zunächst, dass in einer Kompositionsreihe die Ordnung der Faktoren G_i/G_{i+1} nur von G (nicht von der Kompositionsreihe) abhängen; der deutsche Mathematiker Otto HÖLDER (1859-1937) zeigte dann, dass die Faktorgruppe selbst (bis auf Isomorphie und Reihenfolge) nur von G abhängen.

SATZ 4.5: (JORDAN-HÖLDER)
Besitzt eine Gruppe Kompositionsreihen, so sind je zwei Kompositionsreihen dieser Gruppe äquivalent.

Beweis. Der zu beweisende Satz ist eine unmittelbare Folgerung des Verfeinerungssatzes über Normalreihen. Hat nämlich G überhaupt eine Kompositionsreihe $\{G_i\}$, und ist $\{H_i\}$ eine zweite Kompositionsreihe von G, so besitzen diese nach dem Satz von SCHREIER äquivalente Verfeinerungen. Kompositionsreihen können jedoch nach Definition nicht mehr verfeinert werden, also sind beide Kompositionsreihen äquivalent. □

5 Kommutatorgruppen

Der Struktursatz zeigt, dass die endlichen bzw. endlich erzeugten abelschen Gruppen vollständig klassifiziert sind. Im Folgenden wollen wir Gruppen untersuchen, die als Verallgemeinerung der abelschen Gruppen angesehen werden können.

5.1 Einfache Kommutatorgruppen

Wir betrachten zunächst die Kommutatorgruppe einer Gruppe, die man als Maß für die Kommutativität einer Gruppe ansehen kann.

Definition:
Es sei G eine Gruppe. Für $a, b \in G$ wird das Produkt

$$[a, b] := aba^{-1}b^{-1}$$

als **Kommutator von** a und b bezeichnet. Die von allen Kommutatoren erzeugte Untergruppe $K(G)$ von G heißt **Kommutatorgruppe von** G,

$$K(G) := \langle \{[a, b] \mid a, b \in G\} \rangle .$$

Gelegentlich wird die Kommutatorgruppe auch abgeleitete Untergruppe genannt. Da $[a, b]^{-1} = (a^{-1}b^{-1})^{-1}(ab)^{-1} = bab^{-1}a^{-1} = [b, a]$ ist das Inverse eines Kommutators wieder ein Kommutator und damit besteht $K(G)$ aus allen endlichen Produkten von Kommutatoren. Man beachte jedoch, dass ein Produkt von Kommutatoren im Allgemeinen nicht wieder als Kommutator geschrieben werden kann, d.h. die Elemente von $K(G)$ sind also selbst nicht unbedingt Kommutatoren, sondern nur Produkte von diesen.

Wegen $gh = [g, h]hg$ für $g, h \in G$ gibt $[g, h]$ den „Unterschied“ zwischen gh und hg an. Offensichtlich gilt

$$[g, h] = e \Leftrightarrow g \text{ ist mit } h \text{ vertauschbar.}$$

Oder mit anderen Worten: *G ist genau dann abelsch, wenn $K(G) = \{e\}$ gilt.*
Vergleichen Sie bitte auch mit den Eigenschaften des Zentrums einer Gruppe.

SATZ 5.1: *Die Kommutatorgruppe $K(G)$ einer Gruppe G ist ein Normalteiler von G.*

Beweis. Gemäß Definition ist $K(G)$ die kleinste Untergruppe, die alle Kommutatoren von G enthält. Wir müssen also nur noch zeigen, dass $K(G)$ ein Normalteiler von G ist oder was dazu äquivalent ist, dass $\forall g \in G, k \in K$ liegt $gK(G)g^{-1} \in K(G)$. □

Der Kommutator ist also (wie das Zentrum) auch ein Normalteiler der zu Grunde gelegten Gruppe G. Der nun folgende Satz ist für alles weitere von großer Bedeutung.

SATZ 5.2: *Es sei G eine Gruppe mit Untergruppe N von G. Dann gilt die Äquivalenz*

$$N \text{ ist Normalteiler mit ablescher Faktorgruppe } G/N \Leftrightarrow K(G) \subseteq N.$$

Beweis. „$\Rightarrow$" Es sei N ein Normalteiler mit abelscher Faktorgruppe G/N. Es sei $\pi : G \to G/N$ die kanonische Projektion. Weil G/N abelsch ist, gilt $\pi(g)\pi(h) = \pi(h)\pi(g)$ für alle $g, h \in G$, also

$$\pi(ghg^{-1}h^{-1}) = \pi(g)\pi(h)\pi(g)^{-1}\pi(h)^{-1} = e.$$

Jeder Kommutator liegt also in $Kern(\pi) = N$, und da der Kern eines Homomorphismus eine Untergruppe (sogar ein Normalteiler) von G ist, liegt auch jedes endliche Produkt der Kommutatoren innerhalb von N, d.h. $K(G) \subseteq N$.

„$\Leftarrow$" Es sei nun $K(G) \subseteq N$, dann gilt für $g \in G, n \in N$

$$gng^{-1} = [g, n]n \in N,$$

also ist N schon ein Normalteiler von G. Wegen $h^{-1}g^{-1}hg \in K(G) \subseteq N$ für $g, h \in G$ gilt

$$(gN)(hN) = (gh)N = gh\underbrace{(h^{-1}g^{-1}hg)}_{\in K(G) \subseteq N}N = hgN = (hN)(gN).$$

Man beachte, dass N in der Faktorgruppe G/N das neutrale Element ist, deshalb gilt obige Gleichung. Damit ist ist also die Faktorgruppe G/N abelsch. □

Folgerung 5.3: *Die Faktorgruppe $G/K(G)$ ist abelsch.*

Beweis. Da jeder Kommutator $K(G)$ ein Normalteiler von G ist und offensichtlich $K(G) \subseteq K(G)$ erfüllt ist folgt die Behauptung unmittelbar. □

Das heißt, die Kommutatorgruppe ist der kleinste Normalteiler, für den die Faktorgruppe abelsch ist. Die abelsche Gruppe $G/K(G)$ heißt **Faktorkommutatorgruppe** von G. Oft nennt man diese Gruppe auch die „*abelsch gemachte Gruppe von G*" oder „*abelisierung der Gruppe*". Die Ausdrucksweise erklärt sich durch obige Beweisführung, denn beim Übergang von G zu $K(G)$ ist es legitim alle Produkte $ghg^{-1}h^{-1} = [g, h] \in K(G)$

als neutrales Element der Faktorgruppe $G/K(G)$ zu interpretieren. Damit erzwingt man das Kommutativgesetz $gh = hg$.

Beispiel:

a) Kommutatoren von ableschen Gruppen, wie bspw. Untergruppen von $(\mathbb{Z}, +)$, sind stets $\{e\}$.

b) Interessant wird es also, wenn man sich Kommutatoren von nicht ableschen Gruppen, wie S_3 betrachtet. Es stellt sich heraus, dass die alternierende Gruppe A_3 dem Kommutator $K(S_3)$ entspricht.

Konkrete Beispiele und Erläuterungen zu Kommutatorgruppen nicht ablescher Gruppen werden wir im übernächsten Unterabschnitt kennenlernen.

5.2 Höhere Kommutatorgruppen

Im Hinblick auf die Auflösbarkeit von Gruppen liegt es nahe, den Prozess der Bildung der Kommutatorgruppen zu iterieren, also die Kommutatorgruppe der Kommutatorgruppe zu betrachten.

Definition:
Es sei G eine Gruppe und $K_1(G) := K(G)$ die Kommutatorgruppe von G. Dann definieren wir induktiv

$$K_{i+1}(G) := K(K_i(G)) \quad \text{für } i = 1, 2, \dots \, .$$

Die Gruppe $K_i(G)$ heißt **i-te Kommutatorgruppe von** G. Es ist zweckmäßig $K_0(G) := G$ zu setzen. Man hat also eine absteigende Folge von Untergruppen

$$G = K_0(G) \supseteq K_1(G) \supseteq K_2(G) \dots \, .$$

Wir zeigen zunächst einige Rechenregeln für diese „höheren Kommutatorgruppen“.

SATZ 5.4: *Es sei U eine Untergruppe, N ein Normalteiler von G und H eine weitere Gruppe. Dann gilt für alle $n \geq 0$.*

i) $K_n(U) \subseteq K_n(G)$

ii) $K_n(G/N) = (K_n(G)N)/N \cong K_n(G)/(K_n(G) \cap N)$

iii) $K_n(G \times H) = K_n(G) \times K_n(H)$.

Beweis. Ad i): Da U eine Untergruppe von G und damit Teilmenge von G ist, folgt die Beziehung unmittelbar.

Ad ii): Wir beweisen die Behauptung mit Induktion nach n.
Für $n = 0$ ist zu zeigen, dass $G/N = (GN)/N \cong G/(G \cap N)$. Die zu zeigende Identität folgt durch $GN = \{gn \mid g \in G, n \in N\} = G$. Das $(GN)/N \cong G/(G \cap N)$ folgt mit Hilfe des ersten Isomorphiesatzes.
Es gelte nun die Induktionsvoraussetzung für alle $1 \leq k \leq n$ und wir betrachten $K_{n+1}(G)$. Aus der Definition und der Induktionsvoraussetzung folgt

$$K_{n+1}(G/N) = K(K_n(G/N)) = K((K_n(G)N)/N). \tag{1}$$

Die Elemente von $(K_n(G)N)/N$ sind von der Form kN mit $k \in K_n(G)$, da $gN = N$ für $g \in N$ gilt. Damit wir $K((K_n(G)N)/N)$ erzeugt von

$$\{k_1Nk_2Nk_1^{-1}Nk_2^{-1}N = [k_1, k_2]N \mid k_1, k_2 \in K_n(G)\}.$$

Dieses ist aber auch ein Erzeugendensystem für $(K_{n+1}(G)N)/N$. Das ergibt die Gleichugn (1). Die angegebene Isomorphie folgt wieder mit dem ersten Isomorphiesatz.

Add iii): Es genügt zu zeigen, dass sich die Kommutatoren von $[g, g'] \times [h, h']$ mit $g, g' \in G$ und $h, h' \in H$ und $[(g, h), (g', h')]$ entsprechen. Dies folgt jedoch unmittelbar aus den Definitionen, da

$$\begin{aligned}[g, h] \times [g', h'] &= \underbrace{(gg'g^{-1}g'^{-1})}_{=:x \in G} \times \underbrace{(hh'h^{-1}h'^{-1})}_{=:y \in H} = (x, y) \\ &= (g, h) \cdot (g', h') \cdot (g, h)^{-1} \cdot (g', h')^{-1} = [(g, h), (g', h')] .\end{aligned}$$

□

5.3 Kommutatoren von Permutationsgruppen

SATZ 5.5:

a) *Für $n \geq 5$ ist A_n eine einfache Gruppe, d.h. A_n hat keinen Normalteiler $\neq \{e\}$ bzw. $\neq A_n$.*

b) *$K(S_n) = A_n$ für $n \geq 2$.*

c) *$K(A_n) = A_n$ für $n \geq 5$ und $K(A_4) = V_4$.*

d) *Für $n \geq 3, n \neq 4$ ist A_n der einzige nichttriviale Normalteiler von S_n.*

Für die abelsche Gruppe S_2 ist $A_2 = \{id\}$.

Beispiel:
Es ist $K(S_3) = A_3$ und $K(A_3) = \{id\}$ und $K(A_4) = V_4$ sowie $K(V_4) = \{id\}$. Mit diesen Ergebnissen können wir $K_3(S_4)$ bestimmen. Dazu nutzen wir die Definition der höheren Kommutatorgruppen aus: Konkret, $K_3(S_4) = K(K(K(S_4))) = K(K(A_4)) = K(V_4) = \{id\}$.

Aufgrund der letzten Sätze ist folgendes Ergebnis klar.

SATZ 5.6: *Die symmetrische Gruppe S_n ist für $n \geq 5$ **nicht** auflösbar.*

Beweis. Es ist $K_t(S_n) = A_n$ für alle $t \geq 2$, insbesondere sind alle Kommutatorgruppen $K_t(S_n)$, $t \geq 0$, von der trivialen Gruppe $\{id\}$ verschieden. □

Bei den symmetrischen Gruppen können wir also recht gut übersehen, welche dieser Gruppen auflösbar ist und welche nicht. Im Übrigen ist der letzte Satz letztendlich der Grund dafür, dass algebraische Gleichungen vom Grade 5 oder höher im Allgemeinen nicht durch Radikale (also durch sukzessives Wurzelziehen) gelöst werden können.

6 Auflösbare Gruppen

6.1 Grundlagen

Nun können wir den zentralen Begriff dieses Dokuments definieren.

Definition:
Eine Gruppe G heißt **auflösbar**, wenn es ein $m \in \mathbb{N}$ gibt mit $K_m(G) = \{e\}$.

Die auflösbaren Gruppen können, wie bereits angesprochen, als Verallgemeinerung der abelschen Gruppen aufgefasst werden, denn jede abelsche Gruppe G ist wegen $K(G) = \{e\}$ unmittelbar auflösbar. Aber auch nicht abelsche Gruppen (wie z.B. S_4, $K_3(S_4) = \{e\}$) können auflösbar sein.

Die auflösbaren Gruppen verdanken ihren Namen der Tatsache, dass sie in enger Beziehung zur Auflösbarkeit algebraischer Gleichungen stehen. Die Kenntnis der Auflösbarkeit bzw. Nichtauflösbarkeit gewisser Gruppen wird insbesondere in der Galois-Theorie benötigt, um algebraische Gleichungen zu lösen (aufzulösen).

Um von anderen Klassen von Gruppen zu entscheiden, ob sie auflösbar sind oder nicht, werden wir erst einige Konsequenzen aus der Definition ziehen und andere Auflösbarkeitskriterien herleiten.

SATZ 6.1: *1. Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*

2. *Ist G' auflösbar und $f : G \to G'$ ein surjektiver Homomorphismus, so ist G' auflösbar. Insbesondere ist jede Faktorgruppe einer auflösbaren Gruppe auflösbar.*

3. *Es sei N ein Normalteiler einer Gruppe G. Sind N und G/N auflösbar, so ist auch G auflösbar.*

4. *Jedes endliche direkte Produkt auflösbarer Gruppen ist auflösbar.*

Beweis. Ad 1. Ist H Untergruppe von G, so ist jeder Kommutator in H auch ein Kommutator in G. Also gilt $K(H) \subseteq K(G)$, daraus erhalten wir induktiv $K_i(H) \subseteq K_i(G)$ für $i \in \mathbb{N}$. Ist $K_n(G) = \{e\}$, so ist also auch $K_n(H) = \{e\}$ und das bedeutet, dass die Untergruppe H auflösbar ist.

Ad 2. Wir zeigen zunächst, dass $f(K(G)) = K(G')$ gilt. Dazu sei $f : G \to G'$ ein surjektiver Gruppenhomomorphismus. Für einen Kommutator $k = [g, h] \in G$ gilt

$$f(k) = f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = [f(g), f(h)] \in K(G').$$

Für ein Produkt $k_1 \cdot \ldots \cdot k_n$ von Kommutatoren in G ist

$$f(k_1 \cdot \ldots \cdot k_n) = f(k_1) \cdot \ldots \cdot f(k_n) \in K(G'),$$

also gilt $f(K(G)) \subseteq K(G')$. Da f surjektiv ist und $k' = [g', h']$ mit $g', h' \in G'$ ein Kommutator in G', so gibt es $g, h \in G$ mit $f(g) = g',\ f(h) = h'$, also ist

$$k' = [f(g), f(h)] = f([g, h]) \in f(K(G)).$$

Die Untergruppe $f(K(G))$ (der sogar ein Normalteiler ist) enthält also alle Kommutatoren in G', daraus folgt $K(G') \subset f(K(G))$ und damit $K(G') = f(K(G))$.

Wir führen den Beweis nun mit Induktion nach der Länge der Auflösungskette n. Der Induktionsanfang gilt wegen dem eben Bewiesenen. Es gelte also die erweiterte Induktionsvoraussetzung $f(K_i(G)) = K_i(G')$ für alle $i \leq n$, wobei das n so gewählt wurde, dass $K_n(G) = \{e\}$ gilt. Dieses n muss existieren, da G nach Voraussetzungen auflösbar ist. Wir müssen nun zeigen, dass $f(K_{n+1}(G)) = K_{n+1}(G')$ gilt. Wir wenden wieder die Definition an und erhalten dadurch $f(K_{n+1}(G)) = f(K(\{e\})) = f(\{e\}) = \{e\}$.

Ad 3. Es sei $\pi : G \to G/N$ die kanonische Projektion. Weil N und G/N auflösbar sind, gibt es $n, m \in \mathbb{N}$ mit $K_n(N) = \{e\}$ und $K_m(G/N) = \{e\}$. Wie in 2. gilt

$$\pi(K_m(G)) = K_m(G/N) = \{e\},$$

also ist $K_m(G) \subseteq Kern(\pi) = N$. Daraus folgt

$$K_{n+m}(G) = K_n(K_m(G)) \subseteq K_n(N) = \{e\},$$

also ist $K_{n+m}(G) = \{e\}$. Damit ist G auflösbar.

Ad 4. Man wende induktiv Satz 5.4 iii) an. □

Wenn G eine auflösbare Gruppe ist, $K_m(G) = \{e\}$, dann ist $G = K_0(G) \supseteq K_1(G) \supseteq \ldots \supseteq K_m(G) = \{e\}$ eine abelsche Normalreihe von G, denn eine Kommutatorgruppe $K(G)$ ist stets ein Normalteiler von G (vgl. Satz 5.1). Damit ist also $K_i(G)$ ein Normalteiler zu $K_{i-1}(G)$, da $K_i(G) = K(K_{i-1}(G))$ nach Definition gilt. Daher sind die Faktoren $K_{i-1}(G)/K_i(G)$ nach Satz 5.2 abelsch. Es gilt sogar allgemeiner der

SATZ 6.2: *Eine Gruppe ist genau dann auflösbar, wenn sie eine abelsche Normalreihe besitzt.*

Beweis. Wie wir gerade gesehen haben, bildet die Kette der Kommutatoren (die sog. abgeleitete Reihe) einer auflösbaren Gruppe eine abelsche Normalreihe. Die Umkehrung beweisen wir mit Induktion nach der Länge n der Normalreihe. Es sei $n := 1$, dann ist $G = G_1 \supseteq G_2 = \{e\}$ eine abelsche Normalreihe, dann ist $G \cong G/\{e\} = G_1/G_2$ gemäß Voraussetzungen abelsch, also auflösbar. Es seien nun alle Gruppen mit abelscher Normalreihe der Länge $< n$ auflösbar und sei $G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{n+1} = \{e\}$ eine abelsche Normalreihe von G der Länge n. Dann ist $G_2 \supseteq G_3 \supseteq \ldots \supseteq G_{n+1} = \{e\}$ eine abelsche Normalreihe von G_2 der Länge $n-1$, also gemäß erweiterter Induktionsvoraussetzung auflösbar. Es ist G_2 Normalteiler in $G_1 = G$ mit abelscher also auflösbarer Faktorgruppe G/G_2. Nach Satz 6.1, 3., ist damit G auflösbar. □

6.2 Auflösbarkeit und Kompositionsreihen

Wir wollen uns nun noch ansehen, welche Konsequenzen die Auflösbarkeit einer Gruppe G auf eine Kompositionsreihe von G hat, sofern sie existiert.

Lemma 6.3: *Jede Verfeinerung einer abelschen Normalreihe ist abelsch.*

Beweis. Es sei $G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r\{e\}$ eine abelsche Normalreihe. Da wir jede Verfeinerung erhalten, indem wir endlich oft je eine passende Untergruppe einschieben, genügt es zu zeigen, dass eine Verfeinerung $\ldots \supseteq G_i \supseteq H \supseteq G_{i+1} \supseteq \ldots$ auch G_i/H und H/G_{i+1} abelsch sind. Der Rest folgt dann durch Induktion. Als Untergruppe der abelschen Gruppe G_i/G_{i+1} wird H/G_{i+1} sofort als abelsch erkannt. Die Gruppe G_i/H ist nach dem zweiten Isomorphiesatz isomorph zur Faktorgruppe $(G_i/G_{i+1})/(H/G_{i+1})$ einer abelschen Gruppe und damit selbst abelsch. □

Ist G also auflösbar mit einer Kompositionsreihe, dann besitzt G auch eine abelsche Normalreihe. Beide Reihen können nun nach dem Satz von SCHREIER zu äquivalenten Normalreihen verfeinert werden, welche selbst abelsch sind. Da aber Verfeinerung einer Kompositionsreihe nur durch Wiederholungen erzielt wird, ist die Kompositionsreihe selbst bereits abelsch. Die Kompositionsfaktoren sind dann einfache abelsche Gruppen und als solche zyklisch und von Primzahlordnung. Damit ist unter Berücksichtigung von Satz 6.2

SATZ 6.4: *Es sei G eine Gruppe mit Kompositionsreihe. G ist genau dann auflösbar, wenn die Kompositionsfaktoren von G Primzahlordnung haben.*

Folgerung 6.5: *Eine auflösbare Gruppe G besitzt genau dann eine Kompositionsreihe, wenn G endlich ist.*

Beweis. Jede endliche Gruppe besitzt stets eine Kompositionsreihe. Es sei G auflösbar und $G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{e\}$ eine Kompositionsreihe. Nach dem letzten Satz ist $|G_i| = |G_i/G_{i+1}||G_{i+1}| = p_i|G_{i+1}|$ mit einer Primzahl p_i $(1 \leq i < m)$. Folglich gilt $|G| = p_1|G_2| = p_1p_2|G_3| = \ldots = p_1p_2 \ldots p_{m-1}$. □

Über die Größe der Klasse der auflösbaren endlichen Gruppen kann man sich nach den folgenden Sätzen eine gute Vorstellung machen.

SATZ 6.6: *Jede endliche p-Gruppe (p Primzahl) ist auflösbar.*

Beweis. Nach Definition haben die endlichen p-Gruppen die Ordnunge p^n. Wir führen Induktion nach n durch. Der Fall $n = 0$ ist trivial. Es sei $|G| = p^n$ und $n \geq 1$. Nach Folgerung 3.2 aus verlinktem PDF-Dokument ist das Zentrum $Z(G)$ nicht trivial und von der Ordnung $p^r,\ r \geq 1$. Wegen $|G/Z(G)| = p^{n-r}$ und $n - r < n$ ist $G/Z(G)$ nach Induktionsvoraussetzung auflösbar. Insgesamt folgt die Auflösbarkeit von G. □

Abschließend führen wir noch zwei weitere berühmte Sätze auf, werden diese aber nicht beweisen.

SATZ 6.7: (von Burnside)
Alle Gruppen der Ordnung p^aq^b mit Primzahlen p, q und $a, b \in \mathbb{N}$ sind auflösbar.

SATZ 6.8: (von Feit-Thompson)
Alle Gruppen ungerader Ordnung sind auflösbar.

Der letzte Satz wurde im Jahr 1963 von Feit udn Thompson bewiesen, der Originalbeweis ist inklusive aller Hilfssätze 274 Seiten lang. Ein kurzer Beweis dieses Satzes wird nach wie vor dringend gesucht.