**Proseminar Körper- und Galois-Theorie**

# Die alternierende Gruppe und auflösbare Gruppen

Fritz Grimpen*

zum Vortrag am 19. 12. 2016†

Der Hauptsatz der Galois-Theorie [Bos13, Theorem 4.1/6] ist ein fundamentales Ergebnis der Galois-Theorie, welches eine direkte Korrespondenz zwischen den Gruppen- und Körpertheorie herstellt. Er besagt, dass zu einer gegebenen Körpererweiterung $L/K$ stets eine Bijektion zwischen den Untergruppen der Galois-Gruppe $\mathrm{Gal}(L/K)$ und den Zwischenkörpern von $L/K$ existiert. Weiter besagt er, dass ein Zwischenkörper genau dann normal und galoissch über $K$ ist, wenn die korrespondierende Untergruppe normal in $\mathrm{Gal}(L/K)$ ist.

Um nun eine endliche galoissche Körpererweiterungen $L/K$ zu untersuchen reicht es also, wenn wir die Untergruppen und insbesondere die Normalteiler von $\mathrm{Gal}(L/K)$ untersuchen. Dabei stellt sich heraus, dass wir besonders schöne Eigenschaften eines Körpers erhalten, wenn die Galoisgruppe *auflösbar* ist.

Am Rande sei angemerkt, dass sich dadurch auch viele klassische Probleme der Mathematik, wie zum Beispiel die Dreiteilung des Winkels oder die Lösbarkeit eines Polynoms beliebigen Grades alleine mit Wurzelausdrücken und Grundrechenarten, untersuchen lassen.

## 1 Die alternierende Gruppe

Zunächst betrachten wir allerdings die sogenannte alternierende Gruppe, die sich später noch als nützlich herausstellen wird, da die Galoisgruppe eines allgemeinen Polynoms $\sum_{i=1}^{n} a_n X^n \in K[X]$ mit Grad $n$, wobei $a_1, \dots, a_n \in K$ sind, gerade die symmetrische Gruppe $S_n$ ist, vgl. [Bos13, Satz 4.3/4]. Insbesondere lassen sich beliebige Gruppen nach dem Satz von Cayley als Untergruppen einer symmetrischen Gruppe betrachten (vgl. [KM13, Satz 2.15]), weswegen wir die alternierende Gruppe hier zunächst im Allgemeinen betrachten.

**Definition 1.** Sei $2 \leq n \in \mathbb{N}$ und $\mathrm{sgn} : S_n \to \{1, -1\}$ die Signum-Abbildung auf der $S_n$. Dann heißt

$$A_n = \ker \mathrm{sgn} = \{\pi \in S_n \mid \mathrm{sgn}(\pi) = 1\}$$

die *alternierende Gruppe* oder *Gruppe der geraden Permutationen*.

*Fritz Grimpen <grimpen@uni-bremen.de>

†überarbeitete Fassung vom 18. April 2018

Insbesondere ist die alternierende Gruppe $A_n$ für $2 \leq n \in \mathbb{N}$ stets normal in $S_n$. Dies folgt direkt mit der Definition über den Kern von sgn. Alternativ können wir zeigen, dass für $\pi \in A_n$ und $\rho \in S_n$ stets $\operatorname{sgn}(\rho \circ \pi \circ \rho^{-1}) = \operatorname{sgn}(\pi) = 1$ gilt und damit $\rho \circ \pi \circ \rho^{-1} \in A_n$.

**Beispiel 2.** Betrachte $A_3 \trianglelefteq S_3$. Für die $S_3$ wissen wir

$$S_3 = \{\mathrm{id}, (1\ 2), (2\ 3), (3\ 1), (1\ 2\ 3), (3\ 2\ 1)\}.$$

Weiter können wir jeden 3-Zykel in eine Verkettung von zwei Transpositionen zerlegen, sprich $(1\ 2\ 3) = (1\ 2) \circ (2\ 3)$ und $(3\ 2\ 1) = (3\ 2) \circ (2\ 1)$, also folgt $\{\mathrm{id}, (1\ 2\ 3), (3\ 2\ 1)\} \subset A_3$.

Es gilt insbesondere sogar

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (3\ 2\ 1)\}.$$

Die alternierende Gruppe zur $S_3$ besteht also nur aus den 3-Zykeln der $S_3$ und der Identität. Dies lässt sich sogar verallgemeinern mit dem folgenden Satz.

**Satz 3** ([Bos13, Satz 5.3/3])**.** *Für $n \geq 3$ besteht $A_n$ aus allen Permutationen $\pi \in S_n$, welche sich als Verkettung von 3-Zykeln darstellen lassen. Insbesondere wird $A_n$ von den 3-Zykeln der $S_n$ erzeugt.*

*Beweis.* Wir zeigen, dass

$$A_n = \langle (x_1\ x_2\ x_3) \mid x_1, x_2, x_2 \in \{1, \dots, n\} \text{ paarweise disjunkt } \rangle.$$

Sei dazu zunächst $\pi \in A_n$, es existiert also eine Zerlegung $\pi = \prod_{i=1}^{2k} \pi_i$ für 2-Zykel $\pi_1, \dots, \pi_{2k} \in S_n$. Dann lässt sich aber $\pi$ durch Assoziativität anders darstellen, nämlich

$$\pi = \prod_{i=1}^{k} \pi_{2i-1} \circ \pi_{2i},$$

womit wir schließlich Paare von 2-Zykeln betrachten können.

Dazu seien nun $x_1, x_2, x_3, x_4 \in \{1, \dots, n\}$, sodass $x_1 \neq x_2$ und $x_3 \neq x_4$. Für $n = 3$ oder nicht paarweise disjunkte $x_1, \dots, x_4$ können wir nun annehmen, dass $x_2 = x_3$ und damit folgt $(x_1\ x_2) \circ (x_3\ x_4) = (x_1\ x_2) \circ (x_2\ x_4) = (x_1\ x_2\ x_4)$.

Für $n \geq 4$ und paarweise disjunkte $x_1, \dots, x_4$ gilt andererseits $(x_1\ x_2) \circ (x_3\ x_4) = (x_1\ x_2) \circ (x_2\ x_3) \circ (x_2\ x_3) \circ (x_3\ x_4) = (x_1\ x_2\ x_3) \circ (x_2\ x_3\ x_4)$, also lässt sich jede gerade Permutation als Verkettung von 3-Zykeln darstellen.

Für $x_1, x_2, x_3 \in \{1, \dots, n\}$ paarweise disjunkt gilt andererseits $(x_1\ x_2\ x_3) = (x_1\ x_2) \circ (x_2\ x_3) \in A_n$, womit aber gerade jede Verkettung von 3-Zykeln auch ungerade Permutation ist. □

Schließlich betrachten wir noch einige konkrete Permutationsgruppen, auf die wir später nochmal zurückkommen werden.

**Beispiel 4.** (1) Für $n \geq 3$ betrachten wir die Permutationen

$$\sigma = (1\ 2\ \dots\ n) \quad \text{und } \tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & n & n-1 & \cdots & 2 \end{pmatrix}.$$

Dann bezeichnen wir das Erzeugnis von $\sigma$ und $\tau$ als *Diedergruppe $D_n$*. Wir können uns $\sigma$ als eine Rotation eines regelmäßigen $n$-Ecks um den Winkel $2\pi/n$ und $\tau$ als eine Spiegelung an der Symmetrieachse vorstellen.

Es gilt $\operatorname{ord} D_n = 2n$. Insbesondere ist $\langle \sigma \rangle$ ein Normalteiler von $D_n$ mit Index 2.

(2) Weiter können wir die kleinsche Vierergruppe nach dem Satz von Cayley als Untergruppe von $S_4$ darstellen. Wir setzen

$$V = \{\mathrm{id}, (1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}.$$

Insbesondere ist $V$ ein Normalteiler von $S_4$, da Konjugation die Bahnen erhält.

## 2 Kommutatoren und auflösbare Gruppen

**Definition 5.** Seien $G$ eine Gruppe und $a, b \in G$. Dann heißt $[a, b] = aba^{-1}b^{-1}$ *Kommutator von a und b*. Für Untergruppen $H, H' \leq G$ wird mit $[H, H']$ die von allen Kommutatoren $[h, h']$ mit $h \in H$, $h' \in H'$ erzeugte Untergruppe bezeichnet. Für $H = H' = G$ wird diese auch als *Kommutatorgruppe von G* bezeichnet.

Wir beweisen zunächst folgende Bemerkung um eine Aussage über die Struktur der Kommutatorgruppe zu erhalten.

**Bemerkung 6** ([Bos13, Bemerkung 5.4/1])**.**

*(i) Die Kommutatorgruppe $[G, G]$ ist genau dann trivial, wenn $G$ abelsch ist.*

*(ii) Das Inverse eines Kommutators ist ebenfalls ein Kommutator. Insbesondere besteht $[G, G]$ aus allen endlichen Produkten von Kommutatoren aus $G$.*

*(iii) Weiter ist die Kommutatorgruppe $[G, G]$ normal in $G$ und es ist $G/[G, G]$ abelsch.*

*(iv) Für einen Normalteiler $N \trianglelefteq G$ mit abelschen $G/N$ gilt $[G, G] \subseteq N$. Weiter gilt $[G, G] = N$, wenn $N \subseteq [G, G]$, also ist $[G, G]$ der kleinste Normalteiler in $G$, sodass die Faktorgruppe abelsch ist.*

*Beweis.*

(i) Für triviales $[G, G]$ gilt $aba^{-1}b^{-1} = 1$ für alle $a, b \in G$. Dies ist aber gerade $ab = ba$, also ist $G$ abelsch.

Für abelsches $G$ gilt stets $[g, h] = ghg^{-1}h^{-1} = 1$ mit $g, h \in G$ und es folgt somit $[G, G] = \{1\}$.

(ii) Seien $a, b \in G$. Dann gilt

$$[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a],$$

womit die Inversen von Kommutatoren sind wieder Kommutatoren. Also existiert für jedes $k \in [G, G]$ eine Zerlegung $k = [g_1, g_1'] \cdots [g_n, g_n']$ mit $n \in \mathbb{N}$ und $g_i, g_i' \in G, i \in [n]$.

(iii) Für $a, b, g \in G$ gilt

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1} \in [G, G],$$

also für $k \in [G, G]$ und eine Zerlegung $k = \prod_{i=1}^{n} [h_i, h_i']$ mit $n \in \mathbb{N}$ und $h_i, h_i' \in G, i \in [n]$ gilt

$$gkg^{-1} = g\left(\prod_{i=1}^{n} [h_i, h_i']\right)g^{-1} = \prod_{i=1}^{n} g[h_i, h_i']g^{-1} \in [G, G].$$

Damit ist $[G, G]$ normal in $G$.

Bezeichne nun $\overline{x}$ die Nebenklasse von $x \in G$ in $G/[G, G]$. Dann gilt für beliebige $x, y \in [G, G] \leq G$ stets $\overline{x}\ \overline{y}\ \overline{x^{-1}}\ \overline{y^{-1}} = \overline{xyx^{-1}y^{-1}} = \overline{1}$, da $xyx^{-1}y^{-1} = [x, y] \in [G, G]$. Dies ist aber äquivalent zu $\overline{xy} = \overline{yx}$, also ist $G/[G, G]$ abelsch.

(iv) Seien $g, h \in G$. Da $G/N$ abelsch ist, gilt auch $(gh)N = gNhN = (hg)N$. Dies ist allerdings äquivalent mit $(ghg^{-1}h^{-1})N = N$, also gilt $[g,h] \in N$. Damit gilt aber $[G,G] \subseteq N \subseteq [G,G]$, also Gleichheit.

□

**Beispiel 7.**

(1) Für die kleinsche Vierergruppe $V$ gilt $[V,V] = \{\mathrm{id}\}$.

(2) Betrachte die Diedergruppe $D_4 \leq S_4$, vgl. Beispiel 4 (1), welche durch

$$D_4 = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3) \circ (2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 2) \circ (3\ 4), (1\ 3), (1\ 4) \circ (2\ 3)\}$$

gegeben ist. Wir wissen bereits, dass $\langle\sigma\rangle$ normal in $D_4$ und $D_4/\langle\sigma\rangle$ abelsch ist, also muss $[D_4, D_4] \subset \langle\sigma\rangle$ gelten. Weiter ist nun $(1\ 2\ 3\ 4) \notin [D_4, D_4]$, da für $\pi_1, \pi_2 \in D_4$ stets $\mathrm{sgn}([\pi_1, \pi_2]) = \mathrm{sgn}(\pi_1 \circ \pi_2 \circ \pi_1^{-1} \circ \pi_2^{-1}) = \mathrm{sgn}(\mathrm{id}) = 1$ gilt.

Schließlich gilt

$$\begin{aligned}[(1\ 2\ 3\ 4), (2\ 4)] &= (1\ 2\ 3\ 4) \circ (2\ 4) \circ (1\ 2\ 3\ 4)^{-1} \circ (2\ 4)^{-1} \\ &= (1\ 2\ 3\ 4) \circ (2\ 4) \circ (4\ 3\ 2\ 1) \circ (2\ 4) = (1\ 3) \circ (2\ 4) \in [D_4, D_4],\end{aligned}$$

also $[D_4, D_4] = \{\mathrm{id}, (1\ 3) \circ (2\ 4)\} = \{\mathrm{id}, \sigma\}$.

Schließlich lässt sich über die symmetrischen und alternierenden Gruppen eine umfassende Aussage über deren Kommutatorgruppen treffen.

**Bemerkung 8** ([Bos13, Bemerkung 5.4/2]). *Es gilt für $n \in \mathbb{N}$, $n \geq 2$ stets $[S_n, S_n] = A_n$. Weiter gilt für die alternierenden Gruppen, dass*

$$[A_n, A_n] = \begin{cases} \{1\} & \text{für } n = 2, 3, \\ V & \text{für } n = 4, \\ A_n & \text{für } n \geq 5. \end{cases}$$

*Beweis.* Es ist $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ abelsch und mit Bemerkung 6 folgt, dass $[S_n, S_n] \subseteq A_n$ gelten muss. Insbesondere gilt weiter $A_2 = \{1\}$ und es folgt, dass $[S_2, S_2] = A_2$. Für $n \geq 3$ betrachte einen beliebigen 3-Zyklus $(x_1\ x_2\ x_3) \in S_n$. Dann gilt aber

$$\begin{aligned}(x_1\ x_2\ x_3) &= (x_1\ x_3) \circ (x_2\ x_3) \circ (x_1\ x_3) \circ (x_2\ x_3) \\ &= (x_1\ x_3) \circ (x_2\ x_3) \circ (x_1\ x_3)^{-1} \circ (x_2\ x_3)^{-1} \in [S_n, S_n],\end{aligned}$$

also $A_n \subseteq [S_n, S_n]$ und damit $A_n = [S_n, S_n]$.

Weiter ist $A_2$ von Ordnung 1 und $A_3$ von Ordnung 3 und damit abelsch, also gilt $[A_2, A_2] = [A_3, A_3] = \{1\}$.

Sei weiter $n \geq 5$ und $(x_1\ x_2\ x_3) \in A_n$ ein 3-Zyklus und $x_4, x_5 \in [n]$, sodass $x_1, \dots, x_5$ paarweise verschieden sind. Dann erhalten wir

$$(x_1\ x_2\ x_3) = (x_1\ x_2\ x_4) \circ (x_1\ x_3\ x_5) \circ (x_1\ x_2\ x_4)^{-1} \circ (x_1\ x_3\ x_5)^{-1} \in [A_n, A_n],$$

also $A_n \subseteq [A_n, A_n]$ und damit $A_n = [A_n, A_n]$.

Es bleibt noch zu zeigen, dass $[A_4, A_4] = V$ ist. Mit $\operatorname{ord} A_4 = 12$ und $\operatorname{ord} V = 4$ folgt, dass $[A_4 : V] = 3$ gilt, also $A_4/V$ abelsch ist, da $V$ insbesondere normal in $[A_4, A_4]$ ist. Damit ist aber $[A_4, A_4] \subseteq V$ nach Bemerkung 6. Weiter gilt für paarweise verschiedene $x_1, x_2, x_3, x_4 \in \{1, \dots, 4\}$, dass

$$(x_1\ x_2) \circ (x_3\ x_4) = (x_1\ x_2\ x_3) \circ (x_1\ x_2\ x_4) \circ (x_1\ x_2\ x_3)^{-1} \circ (x_1\ x_2\ x_4)^{-1} \in [A_4, A_4]$$

und damit $V \subseteq [A_4, A_4]$, womit die Behauptung gezeigt ist. □

**Definition 9** ([Bos13, Definition 5.4/3]). Sei $G$ eine Gruppe. Eine endliche Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

heißt eine *Normalreihe von $G$*, wenn $G_{i+1}$ normal in $G_i$ für $i \in \{0, \dots, n-1\}$ ist.

Die Faktorgruppen $G_i/G_{i+1}$ für $i \in \{0, \dots, n-1\}$ werden als *Faktoren* der Normalreihe bezeichnet.

Eine Gruppe $G$ heißt *auflösbar*, wenn es eine Normalreihe gibt, sodass die Faktoren dieser abelsch sind.

**Beispiel 10.**

(1) Die kleinsche Vierergruppe ist auflösbar.

(2) Die Kette

$$D_4 \supseteq \langle\sigma\rangle \supseteq \{\mathrm{id}\}$$

ist eine Normalreihe mit abelschen Faktoren. Insbesondere ist $D_4$ damit auflösbar.

(3) Weiter ist jede Diedergruppe $D_n$ für $n \geq 3$ auflösbar, da $D_n \supseteq \langle\sigma\rangle \supseteq \{\mathrm{id}\}$ Normalreihe ist, denn es gelten $D_n/\langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$ und $\langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$, womit aber gerade die Faktoren abelsch sind.

**Bemerkung 11** ([Bos13, Bemerkung 5.4/5]). *Die symmetrischen Gruppen $S_n$ für $n \leq 4$ sind auflösbar, für $n \geq 5$ allerdings nicht.*

*Beweis.* Für $n \leq 4$ existieren nach Bemerkung 8 folgende Normalreihen

$$\begin{aligned} S_2 &\supseteq \{\mathrm{id}\} \\ S_3 &\supseteq A_3 \supseteq \{\mathrm{id}\} \\ S_4 &\supseteq A_4 \supseteq V \supseteq \{\mathrm{id}\} \end{aligned}$$

Die Faktoren $S_3/A_3$ und $S_4/A_4$ sind abelsch, da diese stets von Ordnung 2 sind. Weiter ist $A_4/V$ von Ordnung 3, also ebenfalls abelsch, und es sind $V$ und $S_2$ bereits abelsch.

Für $n \geq 5$ gilt nach Bemerkung 8, dass $[S_n, S_n] = A_n$ und $[A_n, A_n] = A_n$, also kann $S_n$ nicht auflösbar sein, da kein echt kleinerer Normalteiler von $A_n$ mit abelscher Faktorgruppe existiert und $A_n$ selbst nicht abelsch, also nicht trivial auflösbar, ist. □

Bei Betrachtung der Kette

$$S_4 \supseteq A_4 \supseteq V \supseteq \{\mathrm{id}\}$$

merken wir, dass $A_4 = [S_4, S_4]$ und $V = [A_4, A_4]$ gelten, also lässt sich die Normalreihe auch anders darstellen:

$$S_4 \supseteq [S_4, S_4] = A_4 \supseteq [A_4, A_4] = V \supseteq [V, V] = \{\mathrm{id}\}$$

Hierbei sind also die Untergruppen der Kette die Kommutatorgruppen der übergeordneten Gruppe, wie wir mit $[A_4, A_4] = [[S_4, S_4], [S_4, S_4]]$ leicht feststellen. Analog können wir die Normalreihen der auflösbaren Symmetriegruppen darstellen, womit folgende Definition motiviert ist.

**Definition 12.** Für eine Gruppe $G$ und $i \in \mathbb{N}$ definieren wir den *$i$-ten iterierten Kommutator $D^iG$* induktiv durch

$$D^0G = G \text{ und } D^{i+1}G = [D^iG, D^iG].$$

Hiermit erhalten wir zu einer beliebigen Gruppe $G$ eine Kette

$$G = D^0G \supseteq D^1G \supseteq D^2G \supseteq \dots .$$

Insbesondere ist diese Kette sogar Normalreihe mit abelschen Faktoren, wenn es ein $n \in \mathbb{N}$ mit $D^nG = \{1\}$ gibt, da nach Bemerkung 6 stets $[D^i, D^i] = D^{i+1}$ normal in $D^i$ für $i \in \mathbb{N}$ und die Faktorgruppe abelsch ist.

Schließlich stellt sich mit dem folgenden Satz heraus, dass die Existenz einer solchen natürlichen Zahl sogar äquivalent mit der Auflösbarkeit einer Gruppe ist.

**Satz 13** ([Bos13, Satz 5.4/4]). *Eine Gruppe $G$ ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}$ gibt, so dass $D^nG = \{1\}$ die triviale Gruppe ist. Insbesondere ist dann*

$$G = D^0G \supseteq D^1G \supseteq \cdots \supseteq D^nG = \{1\}$$

*eine Normalreihe mit abelschen Faktoren.*

*Beweis.* Sei zunächst $G$ auflösbar, also es existiert eine Normalreihe

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

und es ist $G_i/G_{i+1}$ abelsch für $i \in \{0, \dots, n-1\}$.

Zunächst gilt nun $D^0G = G \subset G_0$. Sei nun $i \in \{0, \dots, n-1\}$ mit $D^iG \subset G_i$. Weiter gilt $[G_i, G_i] \subset G_{i+1}$ aufgrund der Auflösbarkeit von $G$ und gilt schließlich

$$D^{i+1}G = [D^iG, D^iG] \subset [G_i, G_i] \subset G_{i+1}.$$

Damit folgt nun aber induktiv, dass $D^nG \subset G_n = \{1\}$.

Existiert umgekehrt ein $n \in \mathbb{N}$ mit $D^nG = \{1\}$, dann ist

$$G = D^0G \supseteq D^1G \supseteq \cdots \supseteq D^nG = \{1\}$$

eine Normalreihe mit abelschen Faktoren. □

Mit dieser Aussage haben wir ein direkt anwendbares Kriterium zur Auflösbarkeit einer Gruppe $G$ erhalten. Wir können nun die iterierten Kommutatoren von $G$ berechnen; sollte nun ein $n \in \mathbb{N}$ mit $D^nG = D^{n+1}G \neq \{1\}$ existieren, so wissen wir, dass $G$ nicht auflösbar sein kann.

Schließlich gilt noch folgender Satz, welcher nochmals ein äquivalentes Kriterium zur Auflösbarkeit und ein schwächeres Kriterium zur Nichtauflösbarkeit liefert.

**Satz 14** ([Bos13, Satz 5.4/7]). *Es sei $G$ eine Gruppe und $H \leq G$ eine Untergruppe. Wenn $G$ auflösbar ist, dann ist auch $H$ auflösbar.*

*Wenn weiter $H$ normal in $G$ ist, dann ist $G$ genau dann auflösbar, wenn $H$ und $G/H$ auflösbar sind.*

*Beweis.* Sei zunächst $G$ auflösbar. Es gilt nun $[H,H] \subset [G,G]$ und es folgt damit induktiv, dass $D^iH \subset D^iG$. Also muss für $n \in \mathbb{N}$ mit $D^nG = \{1\}$ nun auch $D^nH = \{1\}$ gelten.

Sei nun $H$ normal in $G$ und betrachte den kanonischen Homomorphismus

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\longmapsto gH \end{aligned}$$

Wähle nun $n \in \mathbb{N}$ mit $D^nG = \{1\}$. Für $g, g' \in G$ gilt nun

$$[gH, g'H] = gHg'Hg^{-1}Hg^{-1}H = (gg'g^{-1}g'^{-1})H = [g,g']H,$$

also $[\pi(G), \pi(G)] = [G/H, G/H] = \pi([G,G])$. Damit folgt induktiv aber weiter $D^n(\pi(G)) = \pi(D^nG)$ und somit $D^n(G/H) = \{H\}$.

Seien nun andererseits $G/H$ und $H$ auflösbar mit $D^nH = \{1\}$ und $D^n(G/H) = \{1\}$. Nun gilt aber $D^n(\pi(G)) = \pi(D^nG) = \{1\}$, also $D^nG \subset H$ und weiter $D^{2n}G = D^n(D^nG) \subset D^nH = \{1\}$, also $G$ auflösbar. □

Schließlich lässt sich die Nichtauflösbarkeit von $S_5$ mit Hilfe dieses Satzes nochmals begründen. Dazu betrachten wir den Normalteiler $A_5 \trianglelefteq S_5$. Wir wissen, dass $S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$ auflösbar ist, also ist $S_5$ genau dann auflösbar, wenn $A_5$ auflösbar ist. Nun ist aber $A_5$ nicht auflösbar, da $[A_5, A_5] = A_5$ gilt, also ist auch die ganze $S_5$ nicht auflösbar.

Im Allgemeinen müssen wir für eine Gruppe $G$ nun nur noch eine Untergruppe $H \leq G$ finden, welche nicht auflösbar ist, um die Nichtauflösbarkeit von $G$ zu zeigen.

**Beispiel 15.**

(1) Es ist $\langle\sigma\rangle$ Normalteiler von $D_4$. Es gelten weiter $\operatorname{ord}\sigma = 4$ und $\operatorname{ord}(D_4/\langle\sigma\rangle) = 2$, also beide abelsch und damit auflösbar. Damit ist aber $D_4$ gerade auflösbar.

(2) Sei $n \in \mathbb{N}$ und $\mathrm{GL}(n,\mathbb{R})$ die allgemeine lineare Gruppe. Sei weiter $\det : \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ die Determinantenabbildung und bezeichne $\mathrm{SL}(n,\mathbb{R})$ den Kern von det.

    Mit dem Homomorphiesatz für Gruppen folgt nun, dass $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R})$ isomorph zur Einheitengruppe von $\mathbb{R}$ ist, also auflösbar ist. Damit ist also $\mathrm{GL}(n,\mathbb{R})$ genau dann auflösbar, wenn $\mathrm{SL}(n,\mathbb{R})$ auflösbar ist.

    Schließlich lässt sich mit Methoden der linearen Algebra zeigen, dass $\mathrm{SL}(n,\mathbb{R})$ von den sogenannten Elementarmatrizen erster Art erzeugt wird, vgl. [Lan02, Chapter XIII, Proposition 9.1]. Damit lässt sich schließlich zeigen, dass $\mathrm{SL}(n,\mathbb{R})$ für $n \geq 3$ nicht auflösbar ist, vgl. [Lan02, Chapter XIII, Theorem 9.2].

# Literatur


[Bos13] Siegfried Bosch. *Algebra*. 8. Aufl. Springer Berlin Heidelberg, 2013.

[KM13] C. Karpfinger und K. Meyberg. *Algebra*. 3. Aufl. Springer Spektrum, 2013.

[Lan02] Serge Lang. *Algebra*. 3. Aufl. Graduate Texts in Mathematics. Springer New York, 2002.