

Auflösbarkeit von Gleichungen

Im Folgenden ist wieder $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ ein Körper.

Erinnerung: Ist $L \supseteq K$ eine Galois-Erweiterung, dann ist
 $\text{Gal}(L/K) := \text{Hom}_K(L, L)$ die Galois Gruppe
von L über K .

Definition 99

Sei G eine Gruppe. Wir nennen G auflösbar, falls Folgendes gilt:

Es existiert eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{e_G\},$$

sodass G_{i+1} ein Normalteiler in G_i ist für $i=1, \dots, n-1$ und
 G_i/G_{i+1} eine abelsche Gruppe ist.

Lemma 100

Sei G eine endliche Gruppe und auflösbar. Dann finden wir eine Kette von Untergruppen $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{e_G\}$, sodass G_{i+1} ein Normalteiler in G_i ist und dass G_i/G_{i+1} zyklisch ist.

Beweis

Übung.

Definition 101

Sei $L \supset K$ eine Galois-Erweiterung. Wir nennen L über K **auflösbar**, falls $\text{Gal}(L|K)$ auflösbar ist. (im Sinne von Definition 99).

Definition 102

Sei $L \supset K$ eine endliche Körpererweiterung heißt **durch Radikale auflösbar**, falls ein Erweiterungskörper $E \supset L$ existiert, sodass eine Kette von Körpern $K = E_0 \subseteq E_1 \subseteq \dots \subseteq E_m = E$ existiert mit der Eigenschaft, dass E_i durch E_{i-1} entsteht durch Adjunktion einer Nullstelle von $X^n - a \in E_{i-1}[x]$. D.h. $E_i = E_{i-1}(\sqrt[n]{a})$, wobei $a \in E_{i-1}$.

(Insbesondere darf E_i aus E_{i-1} durch Adjunktion einer Einheitswurzel entstehen).

Bemerkung $L \supset K$ ist genau dann durch Radikale auflösbar, wenn sich jedes Element als L durch eine Formel, die nur mit $+, -, \cdot, : , \sqrt[n]{\quad}$ und Elementen aus K ausdrückt, beschreiben lässt.
(Beispiele: p-q-Formel, Cardano-Formel, Ferrari-Formel).

Lemma 103

- (1) Es sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Ist G auflösbar, dann ist auch H auflösbar. Ist H ein Normalteiler in G , so ist G genau dann auflösbar, wenn H und G/H auflösbar sind.
- (2) Seien G_1, \dots, G_n Gruppen. Dann ist $G_1 \times \dots \times G_n$ auflösbar, genau dann wenn alle G_i auflösbar sind.

Beweis

Übung.

Lemma 105

Sei $K \subseteq L \subseteq M$ eine Kette von endlichen Körpererweiterungen, so dass $M \supseteq L$, $L \supseteq K$ und $M \supseteq K$ Galois-Erweiterungen sind. Dann gilt, $M \supseteq K$ ist genau dann auflösbar, wenn $L \supseteq K$ und $M \supseteq L$ auflösbar sind.

Beweis

1. Nach dem Hauptsatz der Galois-Theorie ist $\text{Gal}(M/L)$ ein Untergruppe von $\text{Gal}(M/K)$.
 2. Nach Satz 91 gilt: $\text{Gal}(L/K) \cong \frac{\text{Gal}(M/K)}{\text{Gal}(M/L)}$.
- \Rightarrow Die Aussage von Lemma 105 ist äquivalent zur Aussage von Lemma 103.

Satz 106

Sei $L \supseteq K$ eine endliche Körpererweiterung. Falls $L \supseteq K$ durch Radikale auflösbar ist, dann existiert eine Körpererweiterung $E \supseteq L$, so dass $E \supseteq K$ eine Galois-Erweiterung ist, die auflösbar ist.

Bemerkung In Satz 106 gilt auch die Rücksichtung, nämlich, dass falls $E \supseteq K$ eine auflösbare Galois-Erweiterung ist, $L \supseteq K$ durch Radikale auflösbar ist. (Der Beweis braucht allerdings etwas mehr Arbeit)

Beweis von Satz 106

Ausgenommen $L \supseteq K$ ist durch Radikale auflösbar.

Dann finden wir nach Definition eine Körpererweiterung $E \supseteq L$, und eine Kette von Körpern $K = E_0' \subseteq E_1' \subseteq \dots \subseteq E_m' = E'$ so dass $E_i' = E_{i-1}'(b_i)$ wobei b_i eine Nullstelle von $f_i(x) = x^{n_i} - q_i \in E_{i-1}'[x]$ ist.

Für $1 \leq i \leq m$ definieren wir $E_i := ZFK(f_i)$.

Dann haben wir folgendes Diagramm:

$$\begin{array}{c} E_1 \subseteq \dots \subseteq E_m = E \\ \cup \quad \quad \quad \cup \\ K = E_0' \subseteq E_1' \subseteq \dots \subseteq E_m' = E' \end{array}$$

Nach Konstruktion: $E_i \supseteq E_{i-1}$ ist eine Galois-Erweiterung nach Definition 81.

Die Nullstellen von f_i sind $b_i, \zeta_{n_i}^1 \cdot b_i, \zeta_{n_i}^2 \cdot b_i, \dots, \zeta_{n_i}^{n_i-1} \cdot b_i$, wobei ζ_{n_i} eine n_i -te Einheitswurzel ist mit: $\zeta_{n_i}^{n_i} = 1$ und $\zeta_{n_i}^j \neq 1$ für $1 \leq j < n_i$.

Dann definieren wir $F_i := E_{i-1}(\zeta_{n_i})$. Dann gilt: $E_i = F_i(b_i)$.

Nach der linken Voraussetzung gilt: $F_i \supseteq E_{i-1}$ ist eine Galois-Erweiterung mit abelscher Galois Gruppe $\text{Gal}(F_i/E_{i-1})$.
 $\Rightarrow F_i \supseteq E_{i-1}$ ist auflösbar.

Andererseits ist, da $E_i \supseteq E_{i-1}$ eine Galois-Erweiterung ist, auch $E_i \supseteq F_i$ eine Galois-Erweiterung. Für $\sigma \in \text{Gal}(E_i/F_i)$ gilt: $\sigma(\zeta_{n_i}^j \cdot b_i) = \zeta_{n_i}^k \cdot b_i$ für ein $0 \leq j \leq n_i-1$. Sei auch $\tau \in \text{Gal}(E_i/F_i)$ mit $\tau(\zeta_{n_i}^j \cdot b_i) = \zeta_{n_i}^l \cdot b_i$.

Dann gilt:

$$\begin{aligned} (\sigma \circ \tau)(\zeta_{n_i}^j \cdot b_i) &= \sigma(\zeta_{n_i}^l \cdot b_i) = \zeta_{n_i}^{k+l} \cdot \sigma(b_i) \\ &= \zeta_{n_i}^{k+j-1} \cdot b_i \\ &= (\tau \circ \sigma)(\zeta_{n_i}^j \cdot b_i). \end{aligned}$$

Da $(\sigma \circ \tau)$ durch $(\sigma \circ \tau)(\zeta_{n_i}^j \cdot b_i)$ eindeutig bestimmt ist, sehen wir,

dass $\text{Gal}(E/F_i)$ abelsch ist und damit auch auflösbar ist.

$\xrightarrow{\text{Lemma 105}}$ $E_i \supseteq E_{i-1}$ ist auflösbar

$\xrightarrow{\text{Lemma 105}}$ $E \supseteq K$ auflösbar ist. \square .

Im Folgenden werden wir zeigen, dass für $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$

(1). $\text{Gal}(\mathbb{Z}\text{FK}(f)/\mathbb{Q}) \cong S_5$ (= symmetrische Gruppe auf $\{1, \dots, 5\}$)

(2) S_n ist nicht auflösbar für $n \geq 5$.

Beides zusammen mit Satz 106 impliziert, dass mindestens eine Nullstelle von f nicht durch eine Formel, die nur mit $\sqrt[n]{\cdot}$, $+$, $-$, \cdot , $\%$ und Elementen aus \mathbb{Q} auskommt, dargestellt werden kann.

Korollar 107

Die allgemeine Gleichung vom Grad 5 hat keine Lösungsformel, die nur mit $+$, $-$, \cdot , $\%$, $\sqrt[n]{\cdot}$ und Zahlen aus \mathbb{Q} auskommt.

In anderen Worten: Es gibt keine p,q -Formel für Gleichungen vom Grad 5 \top .

Bemerkung Fast alle Gleichungen vom Grad $n \geq 5$ haben die Galois-Gruppe S_n .

Satz 108

S_n ist nicht auflösbar für $n \geq 5$.

Beweis

Sei G eine Gruppe. Wir definieren den Kommutator von G als

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

wobei $[a, b] := a \cdot b \cdot a^{-1} \cdot b^{-1}$.

Dann ist $[G, G]$ ein Normalteiler in G , mit der Eigenschaft, dass

(1) $\frac{G}{[G, G]}$ ist abelsch.

(2) Ist $N \trianglelefteq G$ ein Normalteiler, so dass $\frac{G}{N}$ abelsch ist, dann gilt:

$$[G, G] \subseteq N.$$

(Beweis: Übung).

Wir definieren nun zusätzlich: $D^0 G := G$ und $D^i G := [D^{i-1} G, D^{i-1} G]$.
für $i \geq 1$.

Falls G auflösbar ist, so existiert eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{e_G\},$$

so dass $\frac{G_i}{G_{i+1}}$ abelsch ist.

$$\Rightarrow D^{i+1} G \subseteq G_{i+1}.$$

$$\Rightarrow D^n G = \{e_G\}.$$

Wir zeigen jetzt, dass $D^m S_n \neq \{\text{id}\}$ für alle $m \in \mathbb{N}$ ist. Dies impliziert dann, dass S_n nicht auflösbar ist.

Es ist $[S_n, S_n] = A_n$, die alternierende Gruppe, denn

$$\begin{array}{c} \sigma, \tau \in S_n \\ \text{sgn } [\sigma, \tau] = \text{sgn}(\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1}) = \text{sgn}(\sigma \circ \sigma^{-1}) \cdot \text{sgn}(\tau \circ \tau^{-1}) = 1 \\ \Rightarrow [\sigma, \tau] \in A_n \Rightarrow [S_n, S_n] \subseteq A_n. \end{array}$$

(2) Andererseits: $\sigma \in A_n$ lässt sich schreiben als Produkt von Dreierzyklen und für $x_1, x_2, x_3 \in \{1, \dots, n\}$ gilt:

$$(x_1 x_2 x_3) = [(x_1 x_3), (x_2 x_3)]$$

$$\Rightarrow A_n \subseteq [S_n, S_n]$$

Weiterhin ist: $[A_n, A_n] = A_n$. (d.h. $D^1 S_n = A_n$ und $D^n S_n = A_n$ für $n \geq 2$)

Seien $x_1, \dots, x_5 \in \{1, \dots, n\}$. Dann gilt: (hierfür brauchen wir $n \geq 5$)

$$(x_1 x_2 x_3) = [(x_1 x_2 x_4), (x_1 x_3 x_5)] \quad (*)$$

Da jedes $\sigma \in A_n$ als Produkt von Dreierzyklen geschrieben werden kann impliziert (*), dass $A_n \subseteq [A_n, A_n] \subseteq A_n \Rightarrow A_n = [A_n, A_n]$ □

Die Galoisgruppe von $f(x) = x^5 - 4x + 2$

(alle Nullstellen sind paarweise verschieden)

Beobachtung: f hat zwei nicht-reelle Nullstellen und drei reelle Nullstellen.

(das kann man z.B. mit Hilfe einer Kurvendiskussion zeigen.)

$\Rightarrow G := \text{Gal}(ZFK(f)/\mathbb{Q})$ hat ein Element der Ordnung 2, nämlich die komplexe Konjugation eingeschränkt auf $ZFK(f)$.

G ist isomorph zu einer Untergruppe von S_5 , die auf $\{1, \dots, 5\}$ transitiv operiert. D.h. es gibt etwa Orbit $G \cdot 1$ von G in $\{1, \dots, 5\}$.
 Bahngleichung $5 = \frac{|G|}{|G_1|}$ (G_1 = Stabilisator von 1 in G). $\Rightarrow 5$ teilt $|G|$.

Andererseits sei $X = \{5\text{-elementigen Teilmengen von } G\} \rightarrow |X| = \binom{|G|}{5}$
 und G operiert auf X und daher haben wir mit der Bahnungsgleichung,

$$\binom{|G|}{5} = \sum_{I \in \mathcal{I}} \frac{|G|}{|G_{\text{fix}}|}, \quad (*)$$

wobei $(U_i)_{i \in I}$ ein Repräsentationsystem von der Wirkung von G auf X ist, und $G_{U_i} = S$ -stabilisator von U_i . Aber G_{U_i} wirkt auf U_i und da $|U_i| = 5$ gilt: $|G_{U_i}| \in \{1, 5\}$

Falls alle $|G_{U_i}| = 1$, gilt nach (x): $\binom{|G|}{S} = |I|^I \cdot |G|!$

Aber S füllt $|G|$ und weil $|G| = |S_5| = 5!$ füllt, gilt:

(a) S teilt $|H| \cdot |G|$ und (b) $\binom{|G|}{S}$ ist teilerfremd zu S . \diamond

(a) + (b) \rightarrow $\exists i \in I$ mit $|G_{U_i}| = 5 \Rightarrow G$ hat eine Untergruppe von Ordnung 5.

D.h.: (1) G hat eine Untergruppe von Ordnung 2. $\int \Rightarrow G = S_3$
 (2) G hat eine Untergruppe von Ordnung 5.