§ 15 Auflösbarkeit durch Radikale

$f \in \mathbb{Q}[T]$ sei ein normiertes Polynom vom Grade ≥ 1. Wir wollen die Frage untersuchen, ob sich die Nullstellen von f formelmäßig berechnen lassen. Nach dem Fundamentalsatz der Algebra ist klar, daß f Nullstellen in $\mathbb{C}$ besitzt, genauer: es gibt $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ und natürliche Zahlen $m_j \geq 1$ mit

$$f = (T-\alpha_1)^{m_1} \cdot \ldots \cdot (T-\alpha_r)^{m_r} \quad \text{und} \quad \sum_{j=1}^{r} m_j = \mathrm{grad}(f)$$

Hierbei sind $\alpha_1, \ldots, \alpha_r$ die verschiedenen Nullstellen von f, und m_j ist die Vielfachheit der Nullstelle α_j.

$$Z := \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$$

ist dann der Zerfällungskörper von f über $\mathbb{Q}$. Nach (13.8) ist $Z : \mathbb{Q}$ eine Galois–Erweiterung.

Wir schauen uns jetzt einmal Polynome vom Grade 1,2,3 und 4 etwas genauer an:

grad(*f*)=1 : $\quad f = T + q \in \mathbb{Q}[T]$

Die einzige Nullstelle ist $\alpha_1 = -q \in \mathbb{Q}$, also $\mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha_1) = \mathbb{Q}$.

grad(*f*)=2 : $\quad f = T^2 + pT + q \in \mathbb{Q}[T]$

Aus der Schulzeit ist sicher noch die folgende Formel für die Nullstellen von f bekannt, die man durch quadratische Ergänzung erhält. In Spezialfällen kommt sie schon bei den Babyloniern ca. 1900 v.Chr. vor!

$$\alpha_{1,2} \;=\; -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

Die Nullstellen von f lassen sich also aus den Koeffizienten von f durch rationale Rechenoperationen und Wurzelziehen berechnen. Dabei ist $D := \dfrac{p^2}{4} - q \in \mathbb{Q}$ die sog. **Diskriminante** von f, von der es abhängt, ob f zwei verschiedene reelle Nullstellen, eine doppelte Nullstelle oder zwei nichtreelle konjugiert komplexe Nullstellen besitzt.
Wegen $\alpha_{1,2} \;=\; -\dfrac{p}{2} \pm \sqrt{D}$ folgt $\quad \mathrm{ZFK}_{\mathbb{Q}}(f) = \mathbb{Q}(\sqrt{D})$.

grad(*f*)=3 : Durch die Substitution $T = T - \dfrac{a}{3}$ wird aus dem Polynom $T^3 + aT^2 + bT + c \in \mathbb{Q}[T]$ ein Polynom der Form

$$f = T^3 + pT + q\,,$$

in dem das quadratische Glied verschwindet. Für die Nullstellenbestimmung ist dies unbedeutend, da man anschließend die Substitution wieder rückgängig machen kann.

(15.1) SATZ: Cardano (1545), Tartaglia (1515)

Die Nullstellen $\alpha_1, \alpha_2, \alpha_3$ des Polynoms $f = T^3 + pT + q$ lassen sich folgendermaßen angeben:

$\alpha_1 = a + b$, $\alpha_2 = \varepsilon^2 a + \varepsilon b$, $\alpha_3 = \varepsilon a + \varepsilon^2 b$

mit $a = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$, $b = \frac{p}{3a}$ und $\varepsilon = -\frac{1}{2} + \frac{1}{2} i\sqrt{3}$ $(\varepsilon^3 = 1)$.

Es ist dann $Z := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ der Zerfällungskörper von f. Wir wollen jetzt körpertheoretisch die Eigenschaft beschreiben, daß sich die Nullstellen von f formelmäßig angeben lassen.

Für $\beta_1 := \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$ gilt $\beta_1^2 = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \in \mathbb{Q} =: K_0$

β_1 liegt in $K_1 := \mathbb{Q}(\beta_1) = K_0(\beta_1)$ mit $\beta_1^2 \in K_0$.

Für $\beta_2 := \sqrt[3]{-\frac{q}{2} + \beta_1}$ gilt $\beta_2^3 = -\frac{q}{2} + \beta_1 \in \mathbb{Q}(\beta_1) = K_1$

β_2 liegt in $K_2 := K_1(\beta_2)$ mit $\beta_2^3 \in K_1$.

$a = \beta_2 \in K_2 \implies b = -\frac{p}{3a} \in K_2 \implies \alpha_1 = a + b \in K_2$.

Adjungiert man jetzt noch $\beta_3 := \varepsilon$ zu K_2, so liegen alle Nullstellen von f in $K_3 := K_2(\beta_3)$, wobei wieder gilt $\beta_3^3 = \varepsilon^3 = 1 \in K_2$.

Es folgt: $\alpha_2 = \varepsilon^2 a + \varepsilon b \in K_3$ und $\alpha_3 = \varepsilon a + \varepsilon^2 b \in K_3$. Insgesamt also $\alpha_1, \alpha_2, \alpha_3 \in K_3$ und damit $Z = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq K_3$.

Der Körper K_3 wird also schrittweise durch Adjunktion von Wurzeln aus Elementen eines darunterliegenden Körpers aufgebaut:

$$\begin{array}{ccccccc} K_0 = \mathbb{Q} & \subseteq & K_1 = K_0(\beta_1) & \subseteq & K_2 = K_1(\beta_2) & \subseteq & K_3 = K_2(\beta_3) \\ & & \beta_1^2 \in K_0 & & \beta_2^3 \in K_1 & & \beta_3^3 \in K_2 \end{array}$$

grad(f)=4: Durch die Substitution $T = T - \frac{a}{4}$ wird aus dem Polynom $T^4 + aT^3 + bT^2 + cT + d \in \mathbb{Q}[T]$ ein Polynom der Form

$$f = T^4 + pT^2 + qT + r \in \mathbb{Q}[T].$$

Die Nullstellen dieses Polynoms lassen sich formelmäßig bestimmen, wobei dieser Fall auf den kubischen Fall zurückgeführt wird. Eine erste Lösung stammt von **Ferrari (1540)**.

grad(f) $\geq$ 5: Es wurde lange Zeit vergeblich versucht, auch für Gleichungen vom Grade ≥ 5 allgemeine Lösungsformeln zu finden, bis sich herausstellte, daß dies unmöglich ist.

Abel (1802–1829) bewies **1824**, daß es für allgemeine Gleichungen vom Grade ≥ 5 keine Lösungsformel geben kann.

Galois (1811–1832) gab **1832** konkrete Beispiele für solche Gleichungen an.

Wir wollen im folgenden versuchen, diese Zusammenhänge richtig zu verstehen. Motiviert durch die Überlegungen im Falle grad(f)=3 kommen wir zu der folgenden Definition:

(15.2) DEF: Eine Körpererweiterung $L : \mathbb{Q}$ heißt eine **Radikalerweiterung (abgekürzt RE)**, wenn eine Körperkette

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{r-1} \subseteq K_r = L \subseteq \mathbb{C}$$

und Elemente $\beta_j \in L \ (j = 1, 2, \ldots, r)$ existieren, so daß gilt:

i) $K_j = K_{j-1}(\beta_j) \quad (j = 1, 2, \ldots, r)$

ii) Es gibt ein $n_j \in \mathbb{N}$ mit $\beta_j^{n_j} \in K_{j-1} \quad (j = 1, 2, \ldots, r)$.

(15.3) BEM: **a)** $\beta_j^{n_j} \in K_{j-1}$ bedeutet, daß β_j eine n_j–te Wurzel aus einem Element aus K_{j-1} ist. Damit ist β_j algebraisch über K_{j-1}, und es gilt $\mathrm{grad}_{K_{j-1}}(\beta_j) \leq n_j$.

b) Da $K_j : K_{j-1}$ endlich ist, ist auch $L : \mathbb{Q}$ nach dem Gradsatz endlich und damit algebraisch.

c) Ist $L : \mathbb{Q}$ eine Radikalerweiterung, so gibt es einen Erweiterungskörper $R \supseteq L$, so daß $R : \mathbb{Q}$ eine Radikalerweiterung ist, die gleichzeitig eine Galois–Erweiterung ist. Einen Beweis hierfür erhält man durch Induktion nach $[L : \mathbb{Q}]$.

Liegen nun alle Nullstellen eines Polynoms $f \in \mathbb{Q}[T]$ in einer Radikalerweiterung $L : \mathbb{Q}$, d.h. $\mathrm{ZFK}_{\mathbb{Q}}(f) \subseteq L$, so lassen sich die Nullstellen von f formelmäßig darstellen. Man definiert daher

(15.4) DEF: Ein Polynom $f \in \mathbb{Q}[T]$ heißt **durch Radikale auflösbar**, wenn es eine Radikalerweiterung $L : \mathbb{Q}$ gibt, so daß f über L in Linearfaktoren zerfällt (d.h. $\mathrm{ZFK}_{\mathbb{Q}}(f) \subseteq L$).

Wir wollen uns jetzt überlegen, welche Konsequenzen diese Eigenschaft auf die Galois–Gruppe von $\mathrm{ZFK}_{\mathbb{Q}}(f) : \mathbb{Q}$ hat.

(15.5) BEM: Sei $f \in \mathbb{Q}[T]$ durch Radikale auflösbar. Man kann dann einen Erweiterungskörper R von L konstruieren, so daß $R : K$ sowohl eine Galois–Erweiterung als auch eine Radikalerweiterung ist.

$$\underbrace{\overbrace{\underbrace{\mathbb{Q} \subseteq Z}_{GE} \subseteq L}^{RE} \subseteq R}_{GE\,+\,RE}$$

Diese Konstruktion kann so vorgenommen werden, daß die zu der Radikalerweiterung gehörige Körperkette

$$(\star) \quad \mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{r-1} \subseteq K_r = R \subseteq \mathbb{C}$$

folgende Eigenschaften besitzt:

1) $K_{i+1} : K_i$ ist eine Galois–Erweiterung mit zyklischer Galois–Gruppe $(i = 1, 2, \ldots, r-1)$

2) $K_1 : K_0$ ist eine Galois–Erweiterung mit abelscher Galois–Gruppe.

Geht man nun von $(\star)$ mit Hilfe der Abbildung η aus dem Hauptsatz zu den Untergruppen der Galois–Gruppe H von $R : \mathbb{Q}$ über, so erhält man

$$\begin{array}{ccccccccc} \mathrm{Gal}(R:\mathbb{Q}) & \supseteq & \mathrm{Gal}(R:K_1) & \supseteq & \mathrm{Gal}(R:K_2) & \supseteq \ldots \supseteq & \mathrm{Gal}(R:K_{r-1}) & \supseteq & \mathrm{Gal}(R:K_r) \\ \| & & \| & & \| & & \| & & \| \\ U_0 & & U_1 & & U_2 & & U_{r-1} & & U_r \end{array}$$

mit $U_0 = H$ und $U_r = \{id\}$. Für $1 \le i \le r-1$ haben wir die Galois–Erweiterungen

$$\overbrace{R \ \supseteq \ \underbrace{K_{i+1} \ \supseteq \ K_i}_{GE}}^{GE} \supseteq \mathbb{Q}\,.$$

Nach dem Teil II des Hauptsatzes ist dann

$$U_{i+1} = \mathrm{Gal}(R : K_{i+1}) \text{ Normalteiler in } U_i = \mathrm{Gal}(R : K_i)\,,$$

wobei die Gruppe

$$\mathrm{Gal}(K_{i+1} : K_i) \ \cong \ U_i/U_{i+1}$$

zyklisch und damit abelsch ist. Es bleibt der Fall $i = 0$:

$$\overbrace{R \ \supseteq \ \underbrace{K_1 \ \supseteq \ K_0 = \mathbb{Q}}_{GE}}^{GE}$$

Wieder ist

$$U_1 = \mathrm{Gal}(R : K_1) \text{ Normalteiler in } U_0 = \mathrm{Gal}(R : K_0)\,,$$

wobei die Gruppe

$$\mathrm{Gal}(K_1 : K_0) \ \cong \ U_0/U_1$$

abelsch ist. Insgesamt gibt es also in H eine Kette

$$H = U_0 \supseteq U_1 \supseteq U_2 \supseteq \ldots \supseteq U_{r-1} \supseteq U_r = \{id\}$$

von Untergruppen U_i , wobei U_{i+1} Normalteiler in U_i ist und die Faktorgruppe U_i/U_{i+1} abelsch ist.

Wir nehmen dieses Ergebnis zum Anlaß , **auflösbare** Gruppen zu definieren

Einschub: Auflösbare Gruppen

(15.6) DEF: G sei eine Gruppe. Eine Folge $(U_j)_{j=0,1,\ldots,r}$ von Untergruppen von G heißt **Normalreihe in** G, wenn gilt:

i) $\{e\} = U_r \subseteq U_{r-1} \subseteq \ldots \subseteq U_1 \subseteq U_0 = G$

ii) Für jedes $j = 1, 2, \ldots, r$ ist U_j Normalteiler in U_{j-1} .

Die Faktorgruppen U_{j-1}/U_j heißen die **Faktoren** der Normalreihe $(U_j)_{j=0,1,\ldots,r}$.

(15.7) DEF: Eine Gruppe G heißt **auflösbar**, wenn es in G eine Normalreihe mit abelschen Faktoren gibt.

(15.8) BEISPIELE: **a)** Jede abelsche Gruppe G ist auflösbar (es ist nämlich $\{e\} \subseteq G$ eine Normalreihe mit abelschen Faktoren), aber nicht umgekehrt (s.b)).

b) S_3 und S_4 sind auflösbar. Im ersten Fall ist $\{id\} \subseteq A_3 \subseteq S_3$ eine Normalreihe mit abelschen Faktoren, und im zweiten Fall $\{id\} \subseteq V \subseteq A_4 \subseteq S_4$ eine solche.

c) Die Diedergruppe D_n ist für $n \geq 2$ auflösbar. Eine Normalreihe mit abelschen Faktoren ist $\{id\} \subseteq < d > \subseteq D_n$, wobei $d \in D_n$ eine Drehung der Ordnung n ist.

(15.9) BEM: **a)** Untergruppen und Faktorgruppen von auflösbaren Gruppen sind wieder auflösbar.

b) Eine endliche Gruppe ist genau dann auflösbar, wenn es eine Normalreihe mit zyklischen Faktoren gibt. Eine Normalreihe mit abelschen Faktoren läßt sich in diesem Falle zu einer Normalreihe mit zyklischen Faktoren "verfeinern".

c) Eine Gruppe G ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}$ gibt, so daß die n–te Ableitung trivial ist. Die **Ableitung** G' einer beliebigen Gruppe G ist die Untergruppe von G, die von allen **Kommutatoren** $aba^{-1}b^{-1}$ $(a, b \in G)$ erzeugt wird. G' ist Normalteiler in G, und die Faktorgruppe G/G' ist abelsch. G ist genau dann abelsch, wenn G' trivial ist. Für $n \in \mathbb{N}_0$ ist die n–te Ableitung $G^{(n)}$ rekursiv definiert als Ableitung der $(n-1)$–ten Ableitung $(n \geq 1)$, wobei $G^{(0)} := G$ gesetzt wird. Gilt $G^{(n)} = \{e\}$, so ist $G^{(n)} \subseteq G^{(n-1)} \subseteq \ldots \subseteq G^{(2)} \subseteq G^{(1)} \subseteq G^{(0)} = G$ eine Normalreihe mit abelschen Faktoren.

d) Die symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist.

Man kann zeigen: $S_n' = A_n \quad (\forall\, n \geq 2)$ und $A_n' = A_n \quad (\forall\, n \geq 5)$. Daraus folgt für $n \geq 5$

$$S_n^{(k)} \neq \{id\} \quad (\forall\, k \in \mathbb{N})$$

Also ist S_n für $n \geq 5$ **nicht** auflösbar. Nach (15.8) sind S_1, S_2, S_3 und S_4 auflösbar.

Kommen wir jetzt wieder zum Problem der Auflösbarkeit zurück.

(15.10) SATZ: Für ein Polynom $f \in \mathbb{Q}[T]$ sind folgende Aussagen äquivalent:

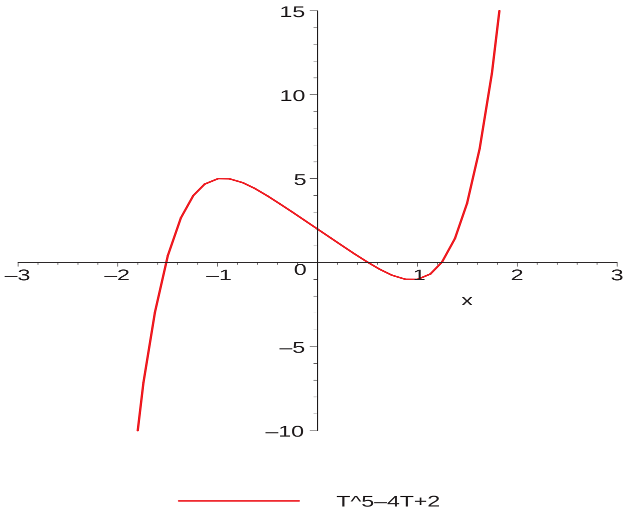
a) f ist durch Radikale auflösbar

b) Die Galoisgruppe von f ist auflösbar.

(15.11) KOROLLAR: Jedes Polynom $f \in \mathbb{Q}[T]$ vom Grade ≤ 4 ist durch Radikale auflösbar.

(15.12) BEM: Man kann zeigen, daß es zu jedem $n \in \mathbb{N}$ ein irreduzibles Polynom $f_n \in \mathbb{Q}[T]$ vom Grade n gibt mit $\mathrm{Gal}_{\mathbb{Q}}(f_n) \cong S_n$. Da S_n für $n \geq 5$ nicht auflösbar ist, gibt es also zu jedem $n \geq 5$ ein irreduzibles Polynom über $\mathbb{Q}$ vom Grade n, das nicht durch Radikale auflösbar ist. Folglich kann es keine allgemeingültigen Lösungsformeln für die Nullstellen von Polynomen vom Grade ≥ 5 geben.

(15.13) BEISPIELE: **a)** Nach (14.7) ist die Galoisgruppe des irreduziblen Polynoms $f := T^5 - 4T + 2 \in \mathbb{Q}[T]$ isomorph zu S_5 und daher nicht auflösbar. Folglich ist auch f **nicht** durch Radikale auflösbar.



b) Die Galoisgruppe des irreduziblen Polynoms $g := T^5 - 5T + 2 \in \mathbb{Q}[T]$ ist isomorph zu D_5 und daher nach (15.8c) auflösbar. Folglich ist g durch Radikale auflösbar.