21. Radikalerweiterungen und Lösungsformeln

Def. Seien $K \subseteq L \subseteq \mathbb{C}$ Körper. Die Körpererweiterung $L:K$ heisst Radikalerweiterung wenn $L = K(\alpha_1, \dots, \alpha_m)$ und wenn es für jedes $1 \leq j \leq m$ ein $n_j \in \mathbb{N}$ gibt mit $\alpha_j^{n_j} \in K(\alpha_1, \dots, \alpha_{j-1})$.
D.h. α_j ist Nullstelle des Polynoms $X^{n_j} - \underbrace{a}_{=\alpha_j^{n_j}}$ mit $a \in K(\alpha_1, \dots, \alpha_{j-1})$.

Bem. Radikalerweiterungen sind endl. und algebraisch, aber nicht notwendigerweise normal.

Lemma 21.1 Ist $L:K$ eine Radikalerweiterung, so ist $L = K(\beta_1, \dots, \beta_k)$ mit $\beta_j^{p_j} \in K(\beta_1, \dots, \beta_{j-1})$ und p_j prim für alle $1 \leq j \leq k$.

Beweis: Mit Induktion über k. Sei $L = K(\beta_1, \dots, \beta_{k-1})$ und sei $\alpha^n \in L$ ($\alpha \notin L$). Ist n prim, so sei $\beta_k := \alpha$.
Ist $n = p_1 \cdot \dots \cdot p_e$ für p_i prim, so sei $\beta_{k,1} := \alpha^{n/p_1}$.
Dann ist $\beta_{k,1}$ Nullstelle von $X^{p_1} - \underbrace{\beta_{k,1}^{p_1}}_{=\alpha^n \in L}$ mit p_1 prim.

Weiter sei $\beta_{k,2} := \alpha^{n/p_1 \cdot p_2}$. Dann ist $\beta_{k,2}$ Nullstelle von $X^{p_2} - \underbrace{\beta_{k,2}^{p_2}}_{=\beta_{k,1} \in L(\beta_{k,1})}$ mit p_2 prim. Analog definieren wir $\beta_{k,3}, \dots, \beta_{k,e}$.

Jedes α_j in der Radikalerweiterung $K(\alpha_1, \dots, \alpha_m)$ kann durch eine Folge $\beta_{j,1}, \dots, \beta_{j,e_j}$ ersetzt werden, sodass $L = K(\beta_{1,1}, \dots, \beta_{2,1}, \dots)$ die gewünschten Eigenschaften besitzt. ⊣

Def. Sei f ein Polynom über $K \subseteq \mathbb{C}$ und sei $L_f \supseteq K$ der Zerfällungskörper von f. Dann heisst f auflösbar durch Radikale, falls es einen Körper L gibt mit $L_f \subseteq L$, sodass $L:K$ eine Radikalerweiterung ist. [alle Nullstellen von f sind in L; durch Radikale ausdrückbar; → Lösungsformel]

[Um die Galoistheorie anzuwenden, brauchen wir (wegen der obigen Bemerkung) den Begriff der normalen Hülle.]

Def. Ist $L = K(\alpha_1, \dots, \alpha_m)$ eine Radikalerweiterung in $\mathbb{C}$, so ist die normale Hülle von $L:K$ der Zerfällungskörper $\tilde{L} \subseteq \mathbb{C}$ von $\prod_{j=1}^{m} f_j$ für f_j Minimalpolynom von α_j über K.

Lemma 21.2 Ist $L:K$ eine Radikalerweiterung in $\mathbb{C}$ und ist $\tilde{L}$ die normale Hülle von $L:K$, so ist $\tilde{L}:K$ ebenfalls eine Radikalerweiterung.

Beweis: [Übungsaufgabe 120 der Serie 25] ⊣

[Aus folgendem Lem. folgt, dass die Galoisgruppe von normalen Radikalerweiterungen auflösbar ist.]

Lemma 21.3 Sei $M \subseteq \mathbb{C}$ ein Körper, p prim und $X^p - 1$ zerfällt über M in Linearfaktoren, d.h. $X^p - 1 = \prod_{i=0}^{p-1} (X - \xi^i)$ mit $\xi \in M$ eine primitive p-te Einheitswurzel (z.B. $\xi = e^{i\frac{2\pi}{p}}$). Weiter sei $a \in M$ und $L \supseteq M$ sei der Zerfällungskörper von [Bsp. $p=5$] $X^p - a$ über M. Dann ist $\mathrm{Gal}(L:M)$ abelsch.

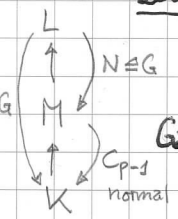
(ξ ist primitiv ⇔ jede Lösung von X^p-1 ist eine Potenz von ξ)

Beweis:
- Ist $\alpha_0 \in M$ eine Nullstelle von $X^p - a$, so zerfällt $X^p - a$ über M in Linearfaktoren $(X - \alpha_0 \xi^i)$, denn $X^p - a = \prod_{i=0}^{p-1} (X - \alpha_0 \xi^i)$, d.h. $\mathrm{Gal}(L:M) = \{\mathrm{id}\}$, also abelsch.
- Seien nun $\alpha_0, \beta \in L \setminus M$ zwei versch. Nullstellen von $X^p - a$. Dann ist $\left(\frac{\beta}{\alpha_0}\right)^p = \frac{\beta^p}{\alpha_0^p} = \frac{a}{a} = 1$. D.h. $\xi := \frac{\beta}{\alpha_0}$ ist eine p-te Einheitswurzel, und weil $\xi \neq 1$ ($\beta \neq \alpha_0$) und p prim, ist ξ eine primitive p-te Einheitswurzel.

- Insbesondere ist $\beta = \alpha_0 \xi$ und die p paarweise versch. Nullstellen von $X^p - a$ sind: $\alpha_0 = \alpha_0 \cdot \xi^0, \alpha_0 \cdot \xi^1, \dots, \alpha_0 \cdot \xi^{p-1}$.
- Weil $\xi \in M$ ist, ist $L = M(\alpha_0)$ und die Körpererw. $L:M$ ist einfach.
- Ist σ ein M-Autom. von L, so ist $\sigma(\alpha_0) = \alpha_0 \cdot \xi^k$ für $0 \le k < p$ und σ ist bestimmt durch $\sigma(\alpha_0)$; denn für $\beta = \alpha_0 \xi^\ell$ ist
$$\sigma(\beta) = \sigma(\alpha_0 \xi^\ell) = \sigma(\alpha_0) \cdot \underbrace{\sigma(\xi^\ell)}_{= \xi^\ell \in M} = \sigma(\alpha_0) \cdot \xi^\ell = (\alpha_0 \cdot \xi^k) \cdot \xi^\ell = \alpha_0 \cdot \xi^{k+\ell}.$$
- Seien nun $\sigma, \tau \in \mathrm{Gal}(L:M)$, z.B. $\sigma(\alpha_0) = \alpha_0 \xi^r$, $\tau(\alpha_0) = \alpha_0 \xi^s$ für $0 \le r, s < p$. Dann gilt:
$$\sigma\circ\tau(\alpha_0) = \sigma(\tau(\alpha_0)) = \sigma(\alpha_0 \xi^s) = (\alpha_0 \cdot \xi^r)\cdot \xi^s = (\alpha_0 \cdot \xi^s)\cdot \xi^r = \dots = \tau\circ\sigma(\alpha_0)$$
(r & s vertauschen; rückwärts)
Somit gilt $\sigma\circ\tau = \tau\circ\sigma$, und weil $\sigma, \tau \in \mathrm{Gal}(L:M)$ beliebig waren, ist $\mathrm{Gal}(L:M)$ abelsch. ⊣

Korollar 21.4 Sei $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ ein Körper, p prim, $a \in K$, $M \supseteq K$ der Zerfällungskörper von $X^p - 1$ über K, und $L \supseteq K$ der Zerfällungskörper von $X^p - a$ über K. Weiter sei $G := \mathrm{Gal}(L:K)$ und $N := \mathrm{Gal}(L:M)$. Dann ist $N \trianglelefteq G$, $G/N \cong \mathrm{Gal}(M:K) \cong C_{p-1}$, und N und G/N sind abelsch.

Beweis: Aus Aufgabe folgt, dass $\mathrm{Gal}(M:K) \cong C_{p-1}$ ([$M:K$ ist normal]), und weil L Zerfällungskörper über K ist (von $X^p - a$), ist $L:K$ normal und $\mathrm{Gal}(L:M) = N \trianglelefteq G$ und $\mathrm{Gal}(M:K) \cong G/N$. Somit ist mit Lem. 21.3 auch N abelsch. ($G/N \cong C_{p-1}$ abelsch)



⊣

Erinnerung:
- Mit dem Hauptsatz über endl. erzeugte abelsche Gruppen ist jede endl. abelsche Gruppe ein Produkt von zyklischen Gruppen.
- Eine Gruppe G heisst <u>auflösbar</u>, falls eine Folge von Untergruppen $H_i \le G$ existiert mit $\{e\} = H_0 \le \dots \le H_n = G$, sodass für alle $0 \le i \le n-1$ gilt:
$$H_i \trianglelefteq H_{i+1} \text{ und } H_{i+1}/H_i \text{ abelsch bzw. zykl. mit Ordnung } p.$$

[siehe Aufgabe 123.(a)]

Korollar 21.5 Seien $K \subseteq M \subseteq L$ wie in Korollar 21.4.
Dann ist $\mathrm{Gal}(L:K)$ auflösbar.

Beweis: Für N und G wie Korollar 21.4, sind N und G/N abelsch, also auflösbar, und somit ist auch G auflösbar. ⊣

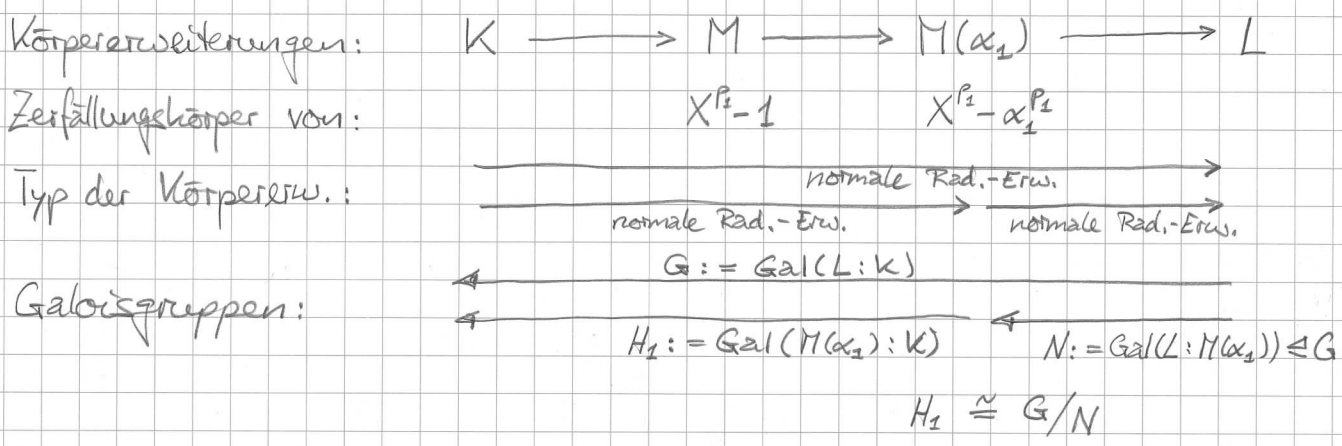
Lemma 21.6 Sei $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$ und sei $L:K$ eine normale Radikalerweiterung. Dann ist $\mathrm{Gal}(L:K)$ auflösbar.

Beweis: Mit Lem. 21.1 dürfen wir annehmen $L = K(\alpha_1, \dots, \alpha_n)$, $\alpha_j^{p_j} \in K(\alpha_1, \dots, \alpha_{j-1})$ mit $\alpha_j \notin K(\alpha_1, \dots, \alpha_{j-1})$ und p_j prim. Der Beweis ist mit Induktion über n, wobei für $n=0$ nichts zu beweisen ist.

- Sei das Lemma bewiesen für ein $n \geq 0$. Sei f das Minimalpolynom von α_1 über K. Weil $L:K$ normal ist (nach Voraussetzung) und $f(\alpha_1) = 0$, zerfällt f in L in Linearfaktoren.
- Weil $\alpha_1 \notin K$, ist $\mathrm{grad}(f) \geq 2$, und weil $\mathrm{char}(K) = 0$ und f irred., hat f keine mehrfachen Nullstellen (f ist separabel).
- Somit hat f in L mind. zwei versch. Nullstellen. Sei $\beta \neq \alpha_1$ eine weitere Nullstelle von f.
- Dann gilt für $\xi := \frac{\alpha_1}{\beta}$, dass $\xi \in L$, $\xi \neq 1$ (weil $\beta \neq \alpha_1$), und $\xi^{p_1} = 1$ (α_1 ist Nullstelle von $X^{p_1} - \alpha_1^{p_1}$, und weil $f(\alpha_1) = 0$ gilt $f \mid X^{p_1} - \alpha_1^{p_1}$, und wegen $f(\beta) = 0$ ist $\beta^{p_1} = \alpha^{p_1}$). [also $1 = \frac{\alpha_1^{p_1}}{\beta^{p_1}} = \xi^{p_1}$]
  ⇒ β ist Nullstelle von $X^{p_1} - \alpha_1^{p_1}$
- Weil p_1 prim ist, ist $\xi \in L$ eine primitive p_1-te Einheitswurzel und $X^{p_1} - 1$ zerfällt in L in Linearfaktoren.
- Sei $M \subseteq L$ ein Zerfällungskörper von $X^{p_1} - 1$ über K. Dann ist $K \subseteq M \subseteq M(\alpha_1) \subseteq L$ und $M(\alpha_1)$ ist ein Zerfällungskörper von $X^{p_1} - \alpha_1^{p_1}$ über K. Insbesondere ist $M(\alpha_1):K$ normal.

analog zu Lem. 21.3

Mit Kor. 21.4 & 21.5 ist $H_1 := \mathrm{Gal}(M(\alpha_1):K)$ auflösbar.
Wir haben folgende Situation:



Nach Induktionsvoraussetzung ist N auflösbar, und weil $L:M(\alpha_1)$ normal ist, ist $N \trianglelefteq G$. Somit sind $H_1 \cong G/N$ und N auflösbar, und damit ist mit Aufgabe 33.(a) Serie 5 auch $G = \mathrm{Gal}(L:K)$ auflösbar. ⊣

Satz 21.7 Sei f ein Polynom über K ($\mathbb{Q} \leq K \leq \mathbb{C}$).
Ist f auflösbar durch Radikale, so ist auch $\mathrm{Gal}(f)$ auflösbar.
[es gilt auch die Umkehrung]

Beweis: Sei L_f der Zerfällungskörper von f über K und sei $L \supseteq L_f$ so, dass $L:K$ eine Radikalerweiterung ist (L ex. nach Def. von "auflösbar durch Radikale"). Mit Lem. 21.2 ex. $\tilde{L} \supseteq L$, sodass $\tilde{L}:K$ eine normale Radikalerweiterung ist ($\tilde{L}$ ist normale Hülle von L). Mit Lem. 21.6 ist $\tilde{G} := \mathrm{Gal}(\tilde{L}:K)$ auflösbar. Es gilt $\mathrm{Gal}(f) = \mathrm{Gal}(L_f:K)$ und weil $L_f:K$ normal ist (L_f ist Zerf.-Körper), ist $N := \mathrm{Gal}(\tilde{L}:L_f)$ ein Normalteiler von $\tilde{G}$ und $\mathrm{Gal}(f) \cong \tilde{G}/N$. Weil $N \trianglelefteq \tilde{G}$ und $\tilde{G}$ auflösbar ist, folgt (mit Aufgabe 123), dass auch $\tilde{G}/N \cong \mathrm{Gal}(f)$ auflösbar ist.

[$N \trianglelefteq G \wedge G$ auflösbar $\Rightarrow G/N$ auflösbar]

⊣

Bem. • Polynome $f \in \mathbb{Q}[X]$ vom Grad $n = 2, 3, 4$ sind durch Radikale auflösbar (es ex. Lösungsformeln mit Wurzeln).
• Ist $\operatorname{grad}(f) = n$, so ist $\mathrm{Gal}(f)$ kom. zu einer Untergruppe von S_n.
• Für $n \geq 5$ ist S_n nicht auflösbar (Aufgabe 124. (c)).
$\Rightarrow$ Ist $\operatorname{grad}(f) = n \geq 5$ und $\mathrm{Gal}(f) \cong S_n$, so ist f nicht durch Radikale auflösbar.

Lemma 21.8 Sei p prim, $f \in \mathbb{Q}[X]$ ein über $\mathbb{Q}$ irred. Polynom mit $\operatorname{grad}(f) = p$ welches über $\mathbb{C}$ genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$ hat. Dann ist $\mathrm{Gal}(f) \cong S_p$. Insbesondere ist für $p \geq 5$ das Polynom f nicht auflösbar.
[ein solches Polynom mit $\operatorname{grad}(f) = 5$ ist z.B. $X^5 - 6X + 3$; Afg. 122]

Beweis: • f zerfällt über $\mathbb{C}$ in Linearfaktoren und hat, weil f irred. ist, p verschiedene Nullstellen.
• Um den Zerfällungskörper $L_f \subseteq \mathbb{C}$ von f über $\mathbb{Q}$ zu konstruieren, adjungieren wir eine dieser p Nullstellen zu $\mathbb{Q}$. Sei $\alpha \in \mathbb{C}$ eine dieser p Nullstellen. Weil $\operatorname{grad}(f) = p$ und f das Minimalpolynom von α ist, ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$.
• Weiter ist $|\mathrm{Gal}(L_f : \mathbb{Q})| = |\mathrm{Gal}(f)| = [L_f : \mathbb{Q}] = [L_f : \mathbb{Q}(\alpha)] \cdot p$, woraus $p \mid |\mathrm{Gal}(f)|$ folgt.
(Aufg. 38, Serie 7)
• Mit dem Satz von Cauchy hat $\mathrm{Gal}(f)$ ein Element ρ der Ordnung p. Weil $\mathrm{Gal}(f)$ isomorph ist zu einer Untergruppe von S_p, ist ρ isomorph zu einem Element $\tilde{\rho} \in S_p$ der Ordnung p. Die einzigen solchen Elemente in S_p sind p-Zyklen; also ist

$$\rho \cong \tilde{\rho} = (i_1, \ldots, i_p) \in S_p.$$

- Die komplexe Konjugation ist ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$ und induziert einen $\mathbb{Q}$-Autom. σ von L_f, welcher die $p-2$ reellen Nullstellen von f punktweise festhält (f hat $p-2$ Nullstellen in $\mathbb{R}$ und 2 Nullstellen in $\mathbb{C}\setminus\mathbb{R}$), und die beiden Nullstellen in $\mathbb{C}\setminus\mathbb{R}$ vertauscht.
  Bem. Ist $\beta \in \mathbb{C}\setminus\mathbb{R}$ eine Nullstelle von f, so ist auch $\bar{\beta}$ eine Nullstelle von f.

- Der $\mathbb{Q}$-Autom. σ ist isomorph zu einem Element $\tilde{\sigma} = (j_1, j_2) \in S_p$, d.h. σ ist isomorph zu einer Transposition.

- Nach Umnummerierung dürfen wir annehmen $\tilde{\sigma} = (1\ 2)$ und für ein $k \geq 1$ ist $\tilde{\rho}^k = (1\ 2\ j_3 \dots j_p)$.

- Mit Aufgabe 43.(c) [jede Permutation $\pi \in S_p$ ist ein Produkt von $\tilde{\sigma}$ und $\tilde{\rho}^k$] gilt $\langle \tilde{\sigma}, \tilde{\rho}^k \rangle = S_p$. Insbesondere ist $\langle \sigma, \rho^k \rangle = \mathrm{Gal}(f)$, und somit ist $\mathrm{Gal}(f) \cong S_p$.

- Mit Aufgabe 124.(c) ist für $n \geq 5$ die Gruppe S_n nicht auflösbar. Für $p \geq 5$ ist somit die Gruppe $\mathrm{Gal}(f)$ nicht auflösbar, und mit Satz 21.7 ist auch das Polynom f nicht durch Rad. auflösbar. ⊣

Folgerung: Für Polynome $f \in \mathbb{Q}[X]$ mit $\mathrm{grad}(f) \geq 5$ existieren [Abel-Ruffini] im Allgemeinen für die Nullstellen von f keine Lösungsformeln mit Wurzelausdrücken, da sonst f durch Radikale auflösbar wäre – das ist aber bereits für $\mathrm{grad}(f) = 5$ im Allgemeinen nicht der Fall.