21. Radikalerweiterungen und Lösungsformeln

Def. Seien $K \subseteq L \subseteq \mathbb{C}$ Körper. Die Körpererweiterung $L:K$ heisst <u>Radikalerweiterung</u> 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. $\dashv$

Def. Sei f ein Polynom über $K \subseteq \mathbb{C}$ und sei $L_f \supseteq K$ der Zerfällungskörper von f. Dann heisst f <u>auflösbar durch Radikale</u>, falls es einen Körper L gibt mit $L_f \subseteq L$, sodass $L:K$ eine Radikalerweiterung ist.

[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 <u>normale Hülle</u> von $L:K$ der Zerfällungskörper $L^* \subseteq \mathbb{C}$ 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 123 der Serie 25] $\dashv$

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

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

ξ ist primitiv $\Leftrightarrow$ jede Lösung von X^p-1 ist ξ^i für ein i.

Beweis: • Ist $\alpha_0 \in K$ eine Nullstelle von $X^p - a$, so zerfällt $X^p - a$ über K in Linearfaktoren $(X - \alpha_0 \xi^i)$, denn $X^p - a = \prod_{i=0}^{p-1} (X - \alpha_0 \xi^i)$, d.h. $\mathrm{Gal}(L:K) = \{\iota\}$, also abelsch.

• Seien nun $\alpha_0, \beta \in L \setminus K$ 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: $\alpha_0 = \alpha_0 \cdot \xi^0, \alpha_0 \cdot \xi^1, \ldots, \alpha_0 \cdot \xi^{p-1}$.
- Weil $\xi \in K$ ist, ist $L = K(\alpha_0)$ und die Körpererw. $L:K$ ist einfach.
- Ist σ ein K-Autom. von L, so ist $\sigma(\alpha_0) = \alpha_0 \cdot \xi^k$ für $0 \leq k < p$ und σ ist bestimmt durch $\sigma(\alpha_0)$; denn für $\beta = \alpha_0 \xi^l$ ist

$$\sigma(\beta) = \sigma(\alpha_0 \cdot \xi^l) = \sigma(\alpha_0) \cdot \underbrace{\sigma(\xi^l)}_{= \xi^l \in K} = \sigma(\alpha_0) \cdot \xi^l = (\alpha_0 \cdot \xi^k) \cdot \xi^l = \alpha_0 \cdot \xi^{k+l}.$$

- Seien nun $\sigma, \tau \in \mathrm{Gal}(L:K)$, z.B. $\sigma(\alpha_0) = \alpha_0 \xi^r$, $\tau(\alpha_0) = \alpha_0 \xi^s$ für $0 \leq r, s < p$. Dann gilt:

$$\sigma \circ \tau(\alpha_0) = \sigma(\tau(\alpha_0)) = \sigma(\alpha_0 \xi^s) = (\alpha_0 \cdot \xi^r) \cdot \xi^s = (\alpha_0 \cdot \xi^s) \cdot \xi^r = \ldots = \tau \circ \sigma(\alpha_0).$$

Somit gilt $\sigma \circ \tau = \tau \circ \sigma$, und weil $\sigma, \tau \in \mathrm{Gal}(L:K)$ beliebig waren, ist $\mathrm{Gal}(L:K)$ abelsch. $\dashv$

<u>Korollar 21.4</u> 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.

<u>Beweis:</u> Aus Aufgabe 124 folgt, dass $G/N \cong C_{p-1}$, und weil L Zerfällungskörper über K ist (von $X^p - a$), ist $L:K$ normal und $N \trianglelefteq G$. Somit ist $N \cong \mathrm{Gal}(L:M)$ und mit Lem. 21.3 ist N abelsch. $\dashv$

<u>Erinnerung:</u>
- 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 $H_i \leq G$ existiert mit $\{e\} = H_0 \leq \ldots \leq H_n = G$, sodass für alle $0 \leq i \leq n-1$ gilt:

$$H_i \trianglelefteq H_{i+1} \text{ und } H_{i+1}/H_i \text{ abelsch bzw. zykl. mit Ordnung } p.$$

[siehe Serie 7, insbes. Aufg. 51]

Korollar 21.5 Seien $K \subseteq M \subseteq L$ wie in Korollar 21.4.
Dann ist $Gal(L:K)$ 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 $Gal(L:K)$ 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 $grad(f) \geq 2$, und weil $char(K) = 0$ 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 $1 = \frac{\alpha_1^{p_1}}{\beta^{p_1}} = \xi^{p_1}$]
- 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.