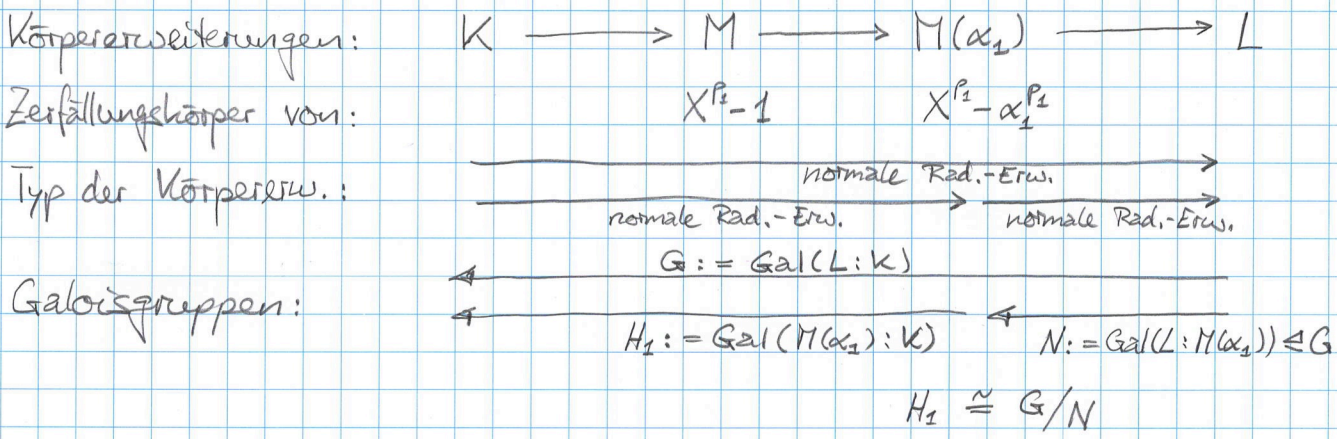
Mit Kor. 21.4 & 21.5 ist $H_1 := \mathrm{Gal}(M(\alpha_1):K)$ auflösbar.

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 50 (Serie 7) auch $G = \mathrm{Gal}(L:K)$ auflösbar. ⊣

Bem. zu Aufgabe 50: $\{e\} = K_m \trianglelefteq \dots \trianglelefteq K_0 = H_1 \cong G/N$ mit K_i/K_{i+1} abelsch.
Für $\bar{K}_i := \{kn : k \in K_i \wedge n \in N\}$ ist dann $\{\bar{e}\} = \bar{K}_m \trianglelefteq \dots \trianglelefteq \bar{K}_0 = G/N$ und es gilt $K_i/K_{i+1} \cong \bar{K}_i/\bar{K}_{i+1}$, also ist G auflösbar.

Satz 21.7 Sei f ein Polynom über K ($\mathbb{Q} \subseteq K \subseteq \mathbb{C}$).
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 50), dass auch $\tilde{G}/N \cong \mathrm{Gal}(f)$ auflösbar ist.
bzw. denselben Argumenten ⊣

Bem. • Polynome $f \in \mathbb{Q}[X]$ vom Grad $n = 2, 3, 4$ sind durch Radikale auflösbar (es ex. Lösungsformeln mit Wurzeln).

• Ist $\text{grad}(f) = n$, so ist $\text{Gal}(f)$ isom. zu einer Untergruppe von S_n.

• Für $n \geq 5$ ist S_n nicht auflösbar (Aufgabe 127. (b)).

$\Rightarrow$ Ist $\text{grad}(f) = n \geq 5$ und $\text{Gal}(f) \cong S_n$, 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 $\text{grad}(f) = p$ welches über $\mathbb{C}$ genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$ hat. Dann ist $\text{Gal}(f) \cong S_p$. Insbesondere ist für $p \geq 5$ das Polynom f nicht auflösbar.

[ein solches Polynom mit $\text{grad}(f) = 5$ ist z.B. $X^5 - 6X + 3$; Afg. 125]

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 $\text{grad}(f) = p$ und f das Minimalpolynom von α ist, ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$.

• Weiter ist $|\text{Gal}(L_f : \mathbb{Q})| = |\text{Gal}(f)| = [L_f : \mathbb{Q}] = [L_f : \mathbb{Q}(\alpha)] \cdot p$, woraus $p \mid |\text{Gal}(f)|$ folgt.

• Mit dem Satz von Cauchy hat $\text{Gal}(f)$ ein Element ρ der Ordnung p. Weil $\text{Gal}(f)$ 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 46.(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 127.(b) 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 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.