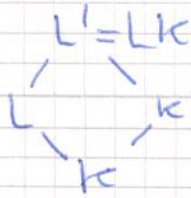
Ad §6.8: Auflösbare Körpererweiterungen



Lemma: Betrachte Körpererweiterungen der Form mit L/K galoisch. Dann ist L'/k' galoisch und wir haben einen natürlichen injektiven Homo $\mathrm{Gal}(L'/k') \hookrightarrow \mathrm{Gal}(L/k)$, $\sigma \mapsto \sigma|_L$.

Beweis: $L' = k'(L)$ und jedes Element von L ist separabel über K und ein Minimalpolynom über K zerfällt über $L \Rightarrow$ auch separabel über k' und ein Minimalpolynom über k' zerfällt über $L' \Rightarrow L'/k'$ galoisch.
Sei $\bar{L}'$ ein algebraischer Abschluss von L'. Für jedes $\sigma \in \mathrm{Gal}(L'/k')$ ist $\sigma|_L \in \mathrm{Hom}_K(L, \bar{L}')$ und da L/K galoisch ist klarlich $\sigma(L) = L$.
Also ist die Abbildung wohldefiniert. Sie ist offensichtlich ein Homomorphismus.
Ihr Kern ist $\{\sigma \mid \sigma|_L = \mathrm{id}\} \Rightarrow \sigma|_{Lk'} = \mathrm{id} \Rightarrow \sigma = \mathrm{id}$. qed.

Satz (Abel–Ruffini) Für L/K endlich galoisch der Charakteristik 0 sind äquivalent:
(a) Es existiert ein Radikalturm $K_m/\dots/K_0 = K$ mit $L \subset K_m$.
(b) $\mathrm{Gal}(L/K)$ ist auflösbar

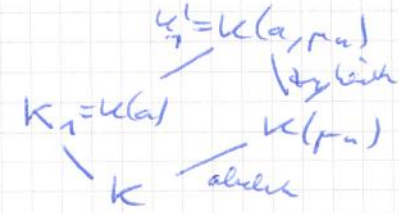
Beweis: Sei $\Gamma := \mathrm{Gal}(L/K)$ und $n := |\Gamma|$. Sei $L \subset \bar{K}$ für einen algebraischen Abschluss $\bar{K}$ von K.

(b) $\Rightarrow$ (a): Sei $1 = \Gamma_r \lhd \Gamma_{r-1} \lhd \dots \lhd \Gamma_0 = \Gamma$ eine Kompositionsreihe mit $L_i := L^{\Gamma_i}$ entspricht sie dem Körperturm $L = L_r / L_{r-1} / \dots / L_0 = K$
Nach dem Hauptsatz der Galoistheorie ist L_i/L_{i-1} galoisch mit Galoisgruppe $\cong \Gamma_{i-1}/\Gamma_i$. Nach Voraussetzung ist diese zyklisch der Ordnung ein Teiler von n.
Setze $K_0 := K$ und $K_1 := K(\mu_n)$, dann ist K_1/K_0 eine einfache Radikalerweiterung. Für jedes $i = 2..r$ setze $K_i := L_i K_1 \subset \bar{K}$.
Nach obigem Lemma ist K_i/K_{i-1} galoisch mit Galoisgruppe isomorph zu einer Untergruppe einer zyklischen Gruppe der Ordnung ein Teiler von n.
Nach §6.7 ist wegen $\mu_n \subset K_{i-1}$ die Erweiterung K_i/K_{i-1} eine einfache Radikalerweiterung.

(a) $\Rightarrow$ (b) Sei $L \subset K_m$ für einen Radikalturm $K_m / \dots / K_0 = K$.
Wir beweisen Induktion über m. Für $m=0$ ist $L = K_m = K \Rightarrow$ trivial.
Sei also $m \geq 1$. OBdA sei $K_m \subset \bar{K}$ = algebraischer Abschluss von K.
Schreibe $K_1 = K(a)$ mit $a^n \in K \setminus \{0\}$. Für jedes i setze $K_i' := K_i(\mu_n) \subset \bar{K}$. Dann ist $K_1' = K(a, \mu_n)$ der Zerfällungskörper des Polynoms $X^n - a^n \in K[X]$, also normal und folglich galoissch über K.
Außerdem ist

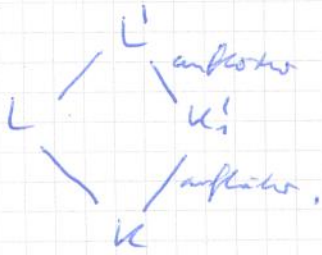
- $K(\mu_n)/K$ abelsch nach §6.6
- $K(a, \mu_n)/K(\mu_n)$ zyklisch nach §6.7

Folglich ist $K(a, \mu_n)/K$ auflösbar.



—

Weiter setze $L' := L(a, \mu_n)$. Da es sich um den Kreis-einfachen L/K und $K(a, \mu_n)/K$ erzeugt ist, ist es selbst galoissch über K.
Außerdem ist $L' \subset K_m'$ für den Radikalturm $K_m' / \dots / K_1'$.
Da dieser echt kürzer ist, ist nach Induktionsvoraussetzung L'/K_1' auflösbar. Nach dem Hauptsatz der Galoistheorie ist $\mathrm{Gal}(L'/K) / \mathrm{Gal}(L'/K_1') \cong \mathrm{Gal}(K_1'/K)$
auflösbar, auflösbar



also $\mathrm{Gal}(L'/K)$ auflösbar. Weiter ist
$\mathrm{Gal}(L'/K) / \mathrm{Gal}(L'/L) \cong \mathrm{Gal}(L/K)$
auflösbar
also $\mathrm{Gal}(L/K)$ auflösbar. qed.

—

Korollar. Für $n \geq 5$ ist die "allgemeine Gleichung n-ten Grades" nicht auflösbar durch Radikale.

Beweis: Wähle dazu in $L = K(a_1, \dots, a_n)$ rationalen Funktionenkörper über K ein Polynom $f(X) = \prod_{i=1}^{n} (X - a_i) \in K[X]$. Dann ist f eine Normalform in einem Radikalturm. Jedes $\varphi \in \mathrm{Aut}_K(\bar{K})$ bildet einen Radikalturm auf einen ebensolchen ab. Also lässt jedes a_i in einen Radikalturm. Durch Zusammensetzen von Radikaltürmen folgt, dass schon L in einem Radikalturm enthalten ist. Also ist $\mathrm{Gal}(L/K)$ auflösbar.

— Aber es gibt nicht auflösbare Polynome von Grad n, z.B.
$K(X_1, \dots, X_n) / K(S_1, \dots, S_n)$ mit $f(X) = \prod_{i=1}^{n} (X - X_i) \in K(S)[X]$.

qed.

Korollar: Für $n \geq 5$ existiert keine Formel, die für ein beliebiges Polynom vom Grad n eine Nullstelle produziert mit den 4 Grundrechenarten und beliebigen Wurzeln.

Beweis: Nach dem Satz würde eine solche Formel implizieren, dass die Galoisgruppe jedes Polynoms vom Grad n auflösbar ist. Aber das "allgemeine Polynom vom Grad n" hat Galoisgruppe S_n:
$K = \mathbb{Q}(S_1, \dots, S_n)$; S_i elementarsymmetrische Funktionen in $X_1, \dots, X_n$
$F(T) := \prod_{i=1}^{n} (T - X_i) = T^n - S_1 T^{n-1} + S_2 T^{n-2} - + \dots \in K[T]$ hat Zerfällungskörper $L = \mathbb{Q}(X_1, \dots, X_n)$ mit $\mathrm{Gal}(L/K) = S_n$.
Und S_n ist nicht auflösbar für $n \geq 5$. ged.

—

Dagegen ist S_n auflösbar für $n \leq 4$. Nach obigem Satz können wir also $X_1, \dots, X_n$ durch Formeln mit Wurzeln in Termen von $S_1, \dots, S_n$ ausdrücken. Diese Formeln liefern durch Einsetzen auch die Nullstellen jedes Polynoms vom Grad $n \leq 4$.

$n = 2$, $\mathrm{char}(K) \neq 2$: $aX^2 + bX + c = 0$ hat bekanntlich die Lösungen $\frac{-b \pm \sqrt{b^2 - 4ac}}{2}$. (Mitternachtsformel).

$n = 3$. Annahme: $\mathrm{char}(K) \neq 2, 3$ (sonst verschieden vom Grad jeder Zwischenerweiterung)

OBdA sei f normiert, also $f(X) = X^3 + a_1 X^2 + a_2 X + a_3$.
Die Variablentransformation $X + \frac{a_1}{3} = Y$ (ähnliche Ergänzung — wie quadratische Ergänzung) bringt das Polynom in die Gestalt $Y^3 + \left(a_2 - \frac{a_1^2}{3}\right) Y + \left(a_3 - \frac{a_1 a_2}{3} + \frac{2a_1^3}{27}\right)$. Um Nenner zu vermeiden, schreiben wir das oBdA f in der Form

$$f(X) = X^3 + 3pX - 2q \qquad \text{für } p, q \in K.$$

—

Dann ist die Diskriminante $D = \dots = -4 \cdot 27 \cdot (p^3 + q^2)$, und die Galoisgruppe von f über $K(\sqrt{D})$ ist schon in A_3 enthalten (↘ §12). Wir haben also nur noch eine zyklische Gleichung vom Grad 3 zu lösen. Dafür brauchen wir nach §11 die dritten Einheitswurzeln.
Sei $\zeta := \frac{-1 + \sqrt{-3}}{2}$ eine solche $\neq 1$.

Mit $f(X) = (X-x_1)(X-x_2)(X-x_3)$ wollte es nach §12 also z.B. der Ansatz $\underline{a := x_1 + \zeta x_2 + \zeta^2 x_3}$ tun.

Wir rechnen kombiniert:

$$a^3 = x_1^3 + x_2^3 + x_3^3 + 3\cdot\zeta\cdot(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 6x_1x_2x_3 + 3\cdot\zeta^2\cdot(x_1x_2^2 + x_2x_3^2 + x_3x_1^2)$$

$$= x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3\cdot\frac{\zeta+\zeta^2}{2}\cdot(x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2^2 + x_2x_3^2 + x_3x_1^2) + 3\cdot\frac{\zeta-\zeta^2}{2}\cdot(x_1^2x_2 + x_2^2x_3 + x_3^2x_1 - x_1x_2^2 - x_2x_3^2 - x_3x_1^2)$$

Hier sind die ersten beiden Teile symmetrisch, d.h. S_3-invariant. Wir können sie also durch eine kleine Rechnung in Termen der Koeffizienten von f ausdrücken. Beachte dabei $\frac{\zeta+\zeta^2}{2} = -\frac{1}{2}$.

In der dritten Zeile ist $\frac{\zeta-\zeta^2}{2} = \frac{\sqrt{-3}}{2}$ und der Term in Klammern ist $= (x_1-x_2)(x_1-x_3)(x_2-x_3) = \sqrt{D}$. Also folgt

$$a^3 = +27q + 3\cdot\underbrace{\frac{\sqrt{-3}}{2}\cdot\sqrt{D}}_{\sqrt{\frac{(-3)}{4}\cdot(-4)\cdot 27\cdot(p^3+q^2)} \;=\; 9\cdot\sqrt{p^3+q^2}}$$

$$= 27\cdot\left(+q + \sqrt{p^3+q^2}\right).$$

Analog erhalten wir für $\underline{a' := x_1 + \zeta^2 x_2 + \zeta x_3}$:

$$a'^3 = 27\cdot\left(+q - \sqrt{p^3+q^2}\right)$$

(da dies genau den Wechsel von $\sqrt{-3}$ zu $-\sqrt{-3}$ entspricht!)

Weiter ist $\underline{a'' := x_1 + x_2 + x_3} = 0$.

Schließlich erhalten wir x_1, x_2, x_3 aus a^0, a', a'' durch Lösen des entsprechenden linearen Gleichungssystems:

$$x_1 = \frac{a + a' + a''}{3} = \sqrt[3]{q - \sqrt{p^3+q^2}} + \sqrt[3]{q + \sqrt{p^3+q^2}}$$

$$x_2 = \frac{\zeta^2 a + \zeta a' + a''}{3} = \zeta^2\cdot\sqrt[3]{q - \sqrt{p^3+q^2}} + \zeta\cdot\sqrt[3]{q + \sqrt{p^3+q^2}}$$

$$x_3 = \frac{\zeta a + \zeta^2 a' + a''}{3} = \zeta\cdot\sqrt[3]{q - \sqrt{p^3+q^2}} + \zeta^2\cdot\sqrt[3]{q + \sqrt{p^3+q^2}}$$

Dabei ist noch zu beachten, dass die beiden dritten Wurzeln so gewählt werden, dass ihr Produkt

$$\sqrt[3]{q - \sqrt{p^3+q^2}}\cdot\sqrt[3]{q + \sqrt{p^3+q^2}} = \sqrt[3]{q^2 - (p^3+q^2)} = \sqrt[3]{-p^3} = -p \text{ ist}$$

folgt aus der Berechnung von $a\cdot a'$.

$n=4$: Für die "allgemeine Gleichung" $F(T)=\prod_{i=1}^{4}(T-X_i)$ mit Galoisgruppe S_4 über $K=\mathbb{Q}(S_1,\dots,S_4)$ entsprechen die normalen Untergruppen der S_4 folgenden Zwischenkörper:

1		$L=\mathbb{Q}(X_1,\dots,X_4)$
Kleinsche Vierergruppe $\hookrightarrow$	$H=\langle(12)(34),(13)(24)\rangle$	$K(t_1,t_2,t_3)$
	A_4	$K(\sqrt{D})$
	S_4	K

wobei $\sqrt{D}=\prod_{1\le i<j\le 4}(X_i-X_j)$ Quadratwurzel der Diskriminante ist und

$$t_1 := X_1X_4+X_2X_3$$
$$t_2 := X_1X_3+X_2X_4$$
$$t_3 := X_1X_2+X_3X_4$$

- In der Tat liegen diese offensichtlich im Fixkörper L^H, und ihr gemeinsamer Stabilisator (punktweise) ist wieder H; also ist tatsächlich $K(t_1,t_2,t_3)=L^H$.
- Die t_1,t_2,t_3 bilden eine Bahn unter der Operation von S_4; also ist das Polynom $G(u):=\prod_{i=1}^{3}(u-t_i)$ symmetrisch in den X_i. Konkret berechnet es sich zu
$$G(u)=u^3-S_2\cdot u^2+(S_1S_3-4S_4)\cdot u-(S_1^2S_4-4S_2S_4+S_3^2)$$
Wir erhalten daher t_1,t_2,t_3 konkret in Termen von Quadrat- und dritten Wurzeln wie im Fall $n=3$.
- Schließlich erhalten wir $X_1,\dots,X_4$ über $K(t_1,t_2,t_3)$ durch Quadratwurzeln, da H abelsch vom Exponenten 2 ist. Konkret ist

H-invariant:
$$\begin{cases}(X_1+X_2-X_3-X_4)^2=\dots=S_1^2-4t_1-4t_2\\ (X_1-X_2+X_3-X_4)^2=\dots=S_1^2-4t_1-4t_3\\ (X_1-X_2-X_3+X_4)^2=\dots=S_1^2-4t_2-4t_3\end{cases}$$

Aus diesen und $S_1=X_1+X_2+X_3+X_4$ erhält man $X_1,\dots,X_4$ durch Lösen eines LGS.

(Die Quadratwurzeln müssen so gewählt werden, dass $\underbrace{(X_1+X_2-X_3-X_4)\cdot(X_1-X_2+X_3-X_4)\cdot(X_1-X_2-X_3+X_4)}_{S_4\text{-invariant!}}=\dots=S_1^3-4S_1S_2+8S_3$ ist.)