5. Anwendungen

5.1 Der Fundamentalsatz der Algebra

5.1.1 Lemma

1) $\mathbb{R}$ besitzt keine Körpererweiterung von ungeradem Grad $n > 1$.

2) $\mathbb{C}$ besitzt keine Körpererweiterung vom Grad 2.

Beweis:

1) Sei $\mathbb{R} \subset L$ eine Körpererweiterung vom Grad n. Wegen 4.5.10 ist $\mathbb{R} \subset L$ separabel. Aus dem Satz vom primitiven Element 4.7.1 folgt: $\exists\, \alpha \in L : L = \mathbb{R}(\alpha)$, und das Minimalpolynom $m_\alpha \in \mathbb{R}[X]$ ist irreduzibel von ungeradem Grad n. Dann gilt $\lim_{x \to -\infty} m_\alpha(x) = -\infty$, $\lim_{x \to \infty} m_\alpha(x) = \infty$. Aus dem

Zwischenwertsatz folgt, daß m_α eine Nullstelle in $\mathbb{R}$ hat. Da m_α irreduzibel ist, muß damit $m_\alpha = X - \alpha$ Grad 1 haben.

2) Wäre $\mathbb{C} \subset L$ vom Grad 2, so wäre wie vorher $L = \mathbb{C}(\alpha)$ und $m_\alpha = X^2 + pX + q \in \mathbb{C}[X]$. Dann hat m_α also die Nullstellen $X = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \in \mathbb{C}$ und zerfällt in Linearfaktoren ↯.

5.1.2 Lemma

Sei $K \subset L$ eine Galoiserweiterung und $p^k \mid [L:K]$ für eine Primzahl p, dann $\exists$ Zwischenkörper $K \subset N \subset L$ mit $[L:N] = p^k$.

Beweis: Nach dem Hauptsatz der Galoistheorie gilt $[L:K] = |\mathrm{Aut}_K(L)|$ also $p^k \mid |\mathrm{Aut}_K(L)|$.

Nach Satz 1.5.4 $\exists$ Untergruppe

$H \subset Aut_K(L)$ mit $|H| = p^k$, und nach dem Hauptsatz der Galoistheorie damit $N = Fix(H)$ mit $K \subset N \subset L$ und $[L:N] = |Aut_N(L)| = |H| = p^k$. □

5.1.3 Satz (Fundamentalsatz der Algebra)

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis:

Sei $f \in \mathbb{C}[X]$ ein nicht konstantes Polynom und sei L der Zerfällungskörper von f.

Es gilt $\mathbb{R} \subset \mathbb{C} \subset L$, und $\mathbb{R} \subset L$ ist endlich, separabel (4.5.10) und daher einfach (4.7.1, Satz vom primitiven Element).

$\Rightarrow L = \mathbb{R}(\alpha)$ für ein $\alpha \in L$.

Sei m_α das Minimalpolynom von α über $\mathbb{R}$ und M der Zerfällungs-

körper von M_α.
$\mathbb{R} \subset M$ ist endlich, normal (4.5.3)
und separabel (4.5.10), also eine
galoiserweiterung.

$$\mathbb{R} \subset \mathbb{C} \subset L = \mathbb{R}(\alpha) \subset M$$

$$\Rightarrow \quad 2 = [\mathbb{C} : \mathbb{R}] \mid [M : \mathbb{R}]$$

Hauptsatz
$\Leftrightarrow$
der
Galois-
theorie

$$2 \mid |\mathrm{Aut}_{\mathbb{R}}(M)|$$

Nach Satz 1.5.4 $\exists$ 2-Sylow untergruppe
$H \subset \mathrm{Aut}_{\mathbb{R}}(M)$ und nach dem
Hauptsatz der Galoistheorie
$N = \mathrm{Fix}(H)$ mit $\mathrm{Aut}_N(M) = H$
und $[M : N] = |\mathrm{Aut}_N(M)| = |H|$.

Da $\mathbb{R} \subset N \subset M$ folgt

$$[N : \mathbb{R}] \cdot [M : N] = [M : \mathbb{R}] \Rightarrow$$

$$[N : \mathbb{R}] \cdot |H| = [M : \mathbb{R}] = |\mathrm{Aut}_{\mathbb{R}}(M)|$$

Da H 2-Sylowgruppe in $\mathrm{Aut}_{\mathbb{R}}(M)$
folgt $[N : \mathbb{R}]$ ist ungrade.

Mit Lemma 5.1.2 1) folgt dann

$N = \mathbb{R}$.

$$\Rightarrow [M:\mathbb{R}] = |H| = 2^k$$

$$\Rightarrow [M:\mathbb{C}] = \frac{[M:\mathbb{R}]}{[\mathbb{C}:\mathbb{R}]} = 2^{k-1}$$

Wäre $k \geq 2$, so wäre $\mathbb{C} \subset M$ endlich, separabel und normal (4.5.5), also Galoiserweiterung. Mit Lemma 5.1.2 $\exists$ dann Zwischenkörper $\mathbb{C} \subset N' \subset M$ mit $[N':\mathbb{C}] = 2$

↯ zu Lemma 5.1.1 1) $\Rightarrow k = 1$

$\Rightarrow M = \mathbb{C}$, da $\mathbb{R} \subset \mathbb{C} \subset L \subset M$

auch $L = \mathbb{C}$.

Damit zerfällt f also schon über $\mathbb{C}$ in Linearfaktoren und $\mathbb{C}$ ist algebraisch abgeschlossen. □

5.2 Auflösbarkeit polynomialer Gleichungen

Sei $f = x^n + a_{n-1}x^{n-1} + \dots + a_0$ ein Polynom in $\mathbb{C}[x]$.

Wir möchten die Nullstellen von f durch die Koeffizienten ausdrücken.

5.2.1 Bsp

1) $n=1$, $f = x + a_0$, $-a_0$ ist Nullstelle.

2) $n=2$ $f = x^2 + px + q$,

Nullstellen sind $-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$.

3) $n=3$, die Formeln von Cardano:

Setze $g = f\left(x - \frac{a_2}{3}\right) = x^3 + px + q$

mit $p = a_1 - \frac{a_2^2}{3}$, $q = a_0 - \frac{a_1 a_2}{3} + \frac{2a_2^3}{27}$.

Ist $p = 0$, so sind die 3. Wurzeln aus q die Nullstellen.

Ist $p \neq 0$, setze $x = u + v$ mit $u \neq 0$ und $v = -\frac{p}{3u}$.

Aus $g(x)=0$ wird

$$u^3+v^3+3uv(u+v)+p(u+v)+q=0$$

$$\Rightarrow \quad u^3+v^3+q=0$$

$$\Rightarrow \quad u^3+q-\frac{p^3}{27u^3}=0 \quad \Rightarrow$$

$$u^6+qu^3-\frac{p^3}{27}=0 \quad \Rightarrow$$

$$u^3=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}\,.$$

Sei $u \in \mathbb{C}$ eine dritte Wurzel aus der rechten Seite, so gilt mit $v=-\frac{p}{3u}$, daß $u+v$ eine Lösung von $g(x)=0$ ist.

4) $n=4$ so ähnlich.

5.2.2 Def

1) Eine Körpererweiterung $K \subset L$ heißt Radikalerweiterung, wenn $L=K(\alpha_1,\dots,\alpha_n)$ und $\alpha_i^{k_i} \in K(\alpha_1,\dots,\alpha_{i-1})$ für ein $k_i \geq 2$.

2) Eine Radikalerweiterung heißt <u>abelsch</u>, wenn $K(\alpha_1, \dots, \alpha_{i-1}) \subset K(\alpha_1, \dots, \alpha_i)$ eine galois-erweiterung mit abelscher Galoisgruppe ist $\forall\, i = 2, \dots, n$.

3) $f \in K[x]$ heißt <u>durch Radikale auflösbar</u> über K, wenn es eine Radikal-erweiterung $K \subset L$ gibt, so daß f über L in Linearfaktoren zerfällt.

<u>Bemerkung</u>:
Sei $f = a_n x^n + \dots + a_0 \in \mathbb{C}[x]$,
$K = \mathbb{Q}(a_0, \dots, a_n)$.
Genau dann, wenn $f \in K[x]$ über K durch Radikale auflösbar ist, können wir wie in Bsp. 5.2.1 die Nullstellen von f durch Wurzeln von rationalen Funktionen der Koeffizienten ausdrücken.

5.2.3 Satz

Sei $f \in K[x]$, $\operatorname{char}(K) = 0$, L der Zerfällungskörper von f. Dann:
f ist über K durch Radikale auflösbar
$\Leftrightarrow$ $\operatorname{Aut}_K(L)$ ist auflösbar

5.2.4 Lemma

Sei $\operatorname{char}(K)=0$, $\zeta_n = e^{\frac{2\pi i}{n}} \in K$.

1) Ist $L = K(\alpha)$ mit $\alpha^n \in K$, dann ist L der Zerfällungskörper von $x^n - \alpha^n$, $K \subset L$ ist Galoiserweiterung und $\operatorname{Aut}_K(L)$ ist zyklisch mit $|\operatorname{Aut}_K(L)| \mid n$.

2) Ist $K \subset L$ Galoiserweiterung mit $\operatorname{Aut}_K(L) \cong \mathbb{Z}_n$ und n prim, dann ist $L = K(\alpha)$ mit $\alpha^n \in K$.

Beweis:

1) $x^n - \alpha^n = (x - \zeta_n^0 \alpha) \cdot (x - \zeta_n \alpha) \cdot \ldots \cdot (x - \zeta_n^{n-1} \alpha)$

Da $\zeta_n \in K \Rightarrow \zeta_n^i \in K \Rightarrow \alpha \zeta_n^i \in L$

$\Rightarrow L = K(\alpha) = K(\zeta_n^0 \alpha, \zeta_n \alpha, \ldots, \zeta_n^{n-1} \alpha)$

ist der Zerfällungskörper von $x^n - \alpha^n$

$x^n - \alpha^n$ ist separabel

$\overset{4.7.11}{\Rightarrow}$ $K \subset L$ ist Galoiserweiterung

Wir setzen $\Pi: \operatorname{Aut}_K(L) \longrightarrow \mathbb{Z}_n$:

$$b_k \longmapsto k$$

wobei $b_k(\alpha) = \zeta_n^k \alpha$.

Da $\sigma_k \circ \sigma_\ell = \sigma_{k+\ell}$ ist Π ein Gruppenhomomorphismus. Π ist auch injektiv.

$\Rightarrow$ $Aut_K(L)$ ist eine Untergruppe von $\mathbb{Z}_n$ und damit selbst zyklisch mit einer Ordnung, die n teilt.

2) $Aut_K(L) = \langle \sigma \rangle$, $ord(\sigma) = n$.

Betrachte σ als K-Vektorraumendomorphismus $\sigma: L \to L$.

Da $\sigma^n = id$ muß das Minimalpolynom μ_σ $x^n - 1$ teilen.

$x^n - 1$ zerfällt über K in die Linearfaktoren $(X - \zeta_n^0) \cdots (X - \zeta_n^{n-1})$.

Da das Minimalpolynom paarweise verschiedene Linearfaktoren hat, ist σ diagonalisierbar.

Alle Eigenwerte sind n-te Einheitswurzeln.

Wäre 1 der einzige Eigenwert $\Rightarrow \sigma = id$

$\Rightarrow n = 1$ ↯ zu n prim

Sei $0 \neq \alpha \in L$ Eigenvektor zum Eigenwert $\zeta \in K$, also $\sigma(\alpha) = \zeta\alpha$

$\Rightarrow \sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n \alpha^n = \alpha^n$

$\Rightarrow \alpha^n \in Fix(Aut_K(L)) = K$

da $K \subset L$ Galoiserweiterung

Beh: $L = K(\alpha)$

„$\supset$" klar

„$\subset$" Da $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K]$

$= |\mathrm{Aut}_K(L)| = n$ und prim

folgt $[K(\alpha) : K] \in \{1, n\}$.

Wäre $[K(\alpha) : K] = 1 \Rightarrow \alpha \in K \Rightarrow$

$\sigma(\alpha) = \alpha \lightning$ zu $\sigma(\alpha) = \zeta\alpha$

mit Eigenwert $\zeta \neq 1$

$\Rightarrow [K(\alpha) : K] = n \Rightarrow [L : K(\alpha)] = 1$

$\Rightarrow L = K(\alpha)$.

□

5.2.5 Korollar:

Sei L Zwischenkörper einer Radikalerweiterung mit $\mathrm{char}(L) = 0$. Dann ist L Zwischenkörper einer abelschen Radikalerweiterung.

Beweis: Sei $K \subset L \subset M$,

$M = K(\alpha_1, \dots, \alpha_m)$, $\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.

Sei $K_i = K(\alpha_1, \dots, \alpha_i)$, dann ist

$k_i = [K_i : K_{i-1}]$. Sei $n = k_1 \cdot \ldots \cdot k_m$

Sei $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$.

Betrachte

$$K = K_0 \subset K_0(\zeta_n) \subset K_1(\zeta_n) \subset \cdots \subset K_m(\zeta_n) = M(\zeta_n)$$

Da mit ζ_n auch die k_i-ten Einheitswurzeln in $K_0(\zeta_n)$ enthalten sind, gilt mit 5.2.4 1) angewendet auf $K_{i-1}(\zeta_n)$ und

$K_i(\zeta_n) = K_{i-1}(\zeta_n)(\alpha_i)$ mit $\alpha_i^{k_i} \in K_{i-1}(\zeta_n)$

$K_{i-1}(\zeta_n) \subset K_i(\zeta_n)$ ist Galoiserweiterung mit zyklischer, damit abelscher, Galoisgruppe.

Auch $K_0 \subset K_0(\zeta_n)$ ist Galoiserweiterung, da $K_0(\zeta_n)$ Zerfällungskörper von $x^n - 1$ ist, und die Galoisgruppe ist $\mathbb{Z}_n^*$, da für $b_k(\zeta_n) = \zeta_n^k$ (wegen $b_{ke} = b_k \circ b_e$)

$$\begin{aligned} \mathrm{Aut}_{K_0}(K_0(\zeta_n)) &\xrightarrow{\sim} \mathbb{Z}_n^* \\ b_k &\longmapsto k \end{aligned}$$

Die Einheitengruppe $\mathbb{Z}_n^*$ ist abelsch.

Da $\zeta_n^n = 1$ ist $K \subset M(\zeta_n) = K(\alpha_1, \ldots, \alpha_m, \zeta_n)$ eine abelsche Radikalerweiterung, die L als Zwischenkörper enthält. □

5.2.6 Prop (Translationssatz)

Sei $K \subset M$ eine Erweiterung, N, L Zwischenkörper, $K \subset N$ Galoiserweiterung. Dann sind auch $L \cap N \subset N$ und $L \subset L(N)$ Galoiserweiterungen mit

$$\mathrm{Aut}_{L \cap N}(N) \cong \mathrm{Aut}_L(L(N)).$$

Beweis:

$L \cap N$ ist Zwischenkörper der Galois-erweiterung $K \subset N$, damit ist $L \cap N \subset N$ auch Galoiserweiterung wegen des Hauptsatzes der Galoistheorie 4.7.9.

Wegen 4.7.11 ist N Zerfällungskörper eines separablen Polynoms $f \in K[X]$.

Seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f

$\Rightarrow N = K(\alpha_1, \dots, \alpha_n)$

$\Rightarrow L(N) = L(\alpha_1, \dots, \alpha_n)$ ist der Zerfällungskörper von f über L und damit ist $L \subset L(N)$ Galoiserweiterung wegen 4.7.11.

Sei $b \in Aut_L(L(N))$, dann hält b insbesondere K fest, und da $K \subset N$ normal ist folgt mit 4.7.6 $b|_N : N \to L(N)$ ist schon in $Aut_K(N)$.

$\Rightarrow \pi : Aut_L(L(N)) \longrightarrow Aut_K(N)$

$b \longmapsto b|_N$

ist wohldefinierter Gruppenhomomorphismus.

Da b durch die Bilder der α_i festgelegt ist und $\alpha_i \in N \ \forall i$ folgt π ist injektiv $\Rightarrow$

$Aut_L(L(N)) \cong U$ Untergruppe von $Aut_K(N)$

Dann gilt $Fix(U) = \{ \alpha \in N \mid b(\alpha) = \alpha \ \forall b \in Aut_L(L(N)) \} =$

$N \cap \{\alpha \in L(N) \mid \sigma(\alpha) = \alpha \text{ für } \sigma \in Aut_L(L(N))\}$

$= N \cap Fix(Aut_L(L(N)))$

$= N \cap L$, da $L \subset L(N)$ Galois-

erweiterung ist

$\Rightarrow U = Aut_{N \cap L}(N)$ wegen des

Hauptsatzes der Galoistheorie. □

Beweis von 5.2.3:

Erinnerung: 5.2.3 Satz

Sei $f \in K[X]$, $char(K) = 0$, L der Zerfällungskörper von f. Dann:

f ist über K durch Radikale auflösbar

$\Leftrightarrow Aut_K(L)$ ist auflösbar

Beweis:

„$\Rightarrow$" nach Def $\exists$ Radikalerweiterung

$K \subset M$, so daß f über M in Linearfaktoren zerfällt. Da L der Zerfällungskörper von f ist, ist $K \subset L \subset M$

Zwischenkörper. Da $char(L) = char(K) = 0$

folgt mit 5.2.5, daß L Zwischenkörper einer abelschen Radikalerweiterung $M' = K(\alpha_1, \dots, \alpha_m)$ ist mit $\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.

Setze $K_i = K(\alpha_1, \dots, \alpha_i)$.

Wir zeigen per Induktion über m, daß $\mathrm{Aut}_K(L)$ auflösbar ist.

Für $m=0$ gilt $K = L = M'$ und $\mathrm{Aut}_K(L) = \{e\}$.

Sei $m > 0$. $L(K_1)$ ist der Zerfällungskörper von $f \in K_1[X]$ und ist Zwischenkörper der abelschen Radikalerweiterung $K_1 \subset M'$. Per Induktion können wir annehmen, daß $\mathrm{Aut}_{K_1}(L(K_1))$ auflösbar ist. Es gilt

$$\mathrm{Aut}_{K_1}(L(K_1)) \overset{\text{Translations-satz 5.26}}{\cong} \mathrm{Aut}_{K_1}(K_1(L)) = \mathrm{Aut}_{K_1 \cap L}(L),$$

(da $K \subset L$ Galois-erweiterung ist, da f separabel wegen $\mathrm{char}(K) = 0$, 4.5.11.)

$\Rightarrow \mathrm{Aut}_{K_1 \cap L}(L)$ ist auflösbar. (*)

Da $K \subset M$ abelsche Radikalerweiterung ist, ist $K \subset K_1$ Galoiserweiterung und $\mathrm{Aut}_K(K_1)$ abelsch.

Da $K \subset L \cap K_1 \subset K_1$ Zwischenkörper ist $\mathrm{Aut}_{L \cap K_1}(K_1)$ Untergruppe von $\mathrm{Aut}_K(K_1)$, damit Normalteiler, und aus dem Hauptsatz der Galoistheorie 4.7.9 folgt $K \subset K_1 \cap L$ ist Galoiserweiterung und

$$\frac{\mathrm{Aut}_K(K_1)}{\mathrm{Aut}_{K_1 \cap L}(K_1)} \cong \mathrm{Aut}_K(K_1 \cap L),$$

wobei letztere als Faktorgruppe einer abelschen Gruppe auch abelsch ist.

Da $K \subset L \cap K_1 \subset L$ Zwischenkörper ist und $K \subset L \cap K_1$ Galoiserweiterung folgt wieder mit dem Hauptsatz

4.7.9 $\mathrm{Aut}_{L\cap K_1}(L)$ Normalteiler in $\mathrm{Aut}_K(L)$ und

$$\frac{\mathrm{Aut}_K(L)}{\mathrm{Aut}_{L\cap K_1}(L)} \cong \mathrm{Aut}_K(L\cap K_1)$$

und diese Gruppe ist abelsch und damit auflösbar.

$\Rightarrow$ Der Normalteiler $\mathrm{Aut}_{L\cap K_1}(L)$ ist auflösbar (*), die Faktorgruppe $\mathrm{Aut}_K(L)/\mathrm{Aut}_{L\cap K_1}(L)$ ist auflösbar

1.6.5 $\Rightarrow$ $\mathrm{Aut}_K(L)$ ist auflösbar.

"$\Leftarrow$" Sei $\mathrm{Aut}_K(L)$ auflösbar.

Sei $n = [L:K]$.

1. Fall: Sei $\zeta_n \in K$.

Da $\mathrm{Aut}_K(L)$ auflösbar, $\exists$ nach Satz 1.6.9 eine Kompositionsreihe, i.e.

$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_0 = \mathrm{Aut}_K(L)$,

so daß $G_i \subset G_{i-1}$ Normalteiler und

G_{i-1}/G_i zyklisch von Primzahlordnung p_i.

Betrachte die Zwischenkörper

$$K \subset K_i := \mathrm{Fix}(G_i) \subset L.$$

Da $K \subset L$ Galoiserweiterung (f separabel, 4.5.11 und 4.7.11) ist auch

$K_{i-1} \subset L$ Galoiserweiterung mit

$$\mathrm{Aut}_{K_{i-1}}(L) = \mathrm{Aut}_{\mathrm{Fix}(G_{i-1})}(L) = G_{i-1}$$

nach dem Hauptsatz der Galoistheorie 4.7.9.

Da G_i in G_{i-1} Normalteiler ist, gilt

$$G_{i-1}/G_i = \frac{\mathrm{Aut}_{K_{i-1}}(L)}{\mathrm{Aut}_{K_i}(L)} \cong \mathrm{Aut}_{K_{i-1}}(K_i)$$

und $K_{i-1} \subset K_i$ ist Galoiserweiterung mit zyklischer Galoisgruppe G_{i-1}/G_i.

Da $K = K_0 \subset K_1 \subset \cdots \subset K_m = L$ und

$[L:K] = [K_m : K_{m-1}] \cdot \ldots [K_i : K_{i-1}] \cdot \ldots [K_1 : K_0]$

und $[K_i : K_{i-1}] = |\mathrm{Aut}_{K_{i-1}}(K_i)|$

$= |G_{i-1}/G_i| = p_i$ folgt

$p_i \mid n$.

Damit ist auch $\zeta_{p_i} = e^{\frac{2\pi i}{p_i}} = e^{\frac{2\pi i}{n} \cdot \frac{n}{p_i}}$

$= \zeta_n^{\frac{n}{p_i}} \in K$.

Damit können wir 5.2.4 2) anwenden

und erhalten $K_i = K_{i-1}(\alpha_i)$ mit

$\alpha_i^{p_i} \in K_{i-1}$.

Damit ist $L = K(\alpha_1, \ldots, \alpha_m)$ eine Radikalerweiterung.

2. Fall $\zeta_n \notin K$.

Verwende den Translationssatz 5.2.6 für $K \subset L(\zeta_n)$, Zwischenkörper L, $K(\zeta_n)$ mit $K \subset L$ Galoiserweiterung, dann ist $L \cap K(\zeta_n) \subset L$ und

$K(\zeta_n) \subset L(\zeta_n)$ Galoiserweiterung

mit $\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n)) \cong \mathrm{Aut}_{L \cap K(\zeta_n)}(L)$.

Dann ist $k := [L(\zeta_n) : K(\zeta_n)] = |\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n))| = |\mathrm{Aut}_{L \cap K(\zeta_n)}(L)|$

$= [L : L \cap K(\zeta_n)] \mid [L : K] = n$

$\Rightarrow \zeta_k = \zeta_n^{\frac{n}{k}} \in K(\zeta_n)$

Da $\mathrm{Aut}_K(L)$ auflösbar ist auch die Untergruppe $\mathrm{Aut}_{L \cap K(\zeta_n)}(L)$ auflösbar, also $\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n))$ auflösbar.

Damit erfüllt $K(\zeta_n) \subset L(\zeta_n)$ die Voraussetzungen von Fall 1.

Der Zerfällungskörper $L(\zeta_n)$ von f über $K(\zeta_n)[x]$ ist wegen Fall 1 eine Radikalerweiterung

$L(\zeta_n) = K(\zeta_n)(\alpha_1, \dots, \alpha_m)$ mit $\alpha_i^{k_i} \in K(\zeta_n)(\alpha_1, \dots, \alpha_{i-1})$. Da $\zeta_n^n = 1 \in K$ ist auch $K \subset L(\zeta_n)$

Radikalerweiterung, über der f zerfällt
$\Rightarrow$ f ist durch Radikale auflösbar. □

5.2.7 Korollar

Sei $f \in K[X]$ vom Grad höchstens 4, K ein Teilkörper von $\mathbb{C}$, L der Zerfällungskörper von f.
Wegen 4.4.8 ist $Aut_K(L) \subset S_4$ Untergruppe und wegen Bsp 2) nach 1.6.4 ist S_4 auflösbar $\Rightarrow$ f ist durch Radikale auflösbar (wußten wir schon wegen der Formeln von Cardano 5.2.1 3)).

5.2.8 Bsp Sei $f = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1 \in \mathbb{Q}[X]$.
Man kann zeigen, daß f das Minimalpolynom von $\alpha = \zeta_{11} + \zeta_{11}^{-1}$ ist.
Dann ist $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_{11})$ und $Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11})) = \mathbb{Z}_{11}^*$ (siehe Beweis von 5.2.5), $\mathbb{Z}_{11}^* \cong \mathbb{Z}_{10}$

ist zyklisch, daher ist jede Untergruppe ein Normalteiler und damit $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ Galoiserweiterung.

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) \cong \frac{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11}))}{\mathrm{Aut}_{\mathbb{Q}(\alpha)}(\mathbb{Q}(\zeta_{11}))}$$

ist Faktorgruppe einer zyklischen Gruppe und damit selbst zyklisch.

Da $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ folgt

$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \mathbb{Z}_5$.

Insbesondere ist $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ auflösbar, und da f über $\mathbb{Q}(\alpha)$ schon zerfällt, gilt f ist durch Radikale auflösbar.

Die Radikalausdrücke für die Nullstellen von f kennen wir dadurch aber nicht.

5.2.9 Prop Sei p eine Primzahl, $\tau \in S_p$ eine Transposition und σ ein p-Zykel, dann gilt $S_p = \langle \tau, \sigma \rangle$.

Beweis: $\exists \quad \tau = (12)$.

Ist $\beta = (123 \cdots p)$, so gilt

$(i \; i+1) = (\beta^{i-1}(1) \; \beta^{i-1}(2)) =$

$\beta^{i-1} \circ (12) \; \beta^{-(i-1)} \quad \in \langle \tau, \beta \rangle$

$\forall \; i = 1, \ldots, p-1$. Da S_p von Nachbartranspositionen erzeugt wird, folgt die Behauptung.

Ist β ein beliebiger p-Zykel, so sind seine Potenzen auch p-Zykel (da p prim) und wir können eine Potenz wählen, so daß

$\beta^i = (1 2 a_3 \cdots a_p)$

Für $\beta' = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & p \\ 1 & 2 & a_3 & a_4 & \cdots & a_p \end{pmatrix}$ gilt

$\beta'^{-1} \circ \beta^i \circ \beta' = (1 \cdots p)$ und

$\beta'^{-1} \circ (12) \circ \beta' = (12)$, so daß

für $U = \langle \tau, \beta \rangle$ gilt

$S_p = \langle \tau, (1 \cdots p) \rangle \subset \beta'^{-1} U \beta' \subset S_p$

$\Rightarrow \quad b'^{-1} U b' = S_p \quad \Rightarrow$

$U = b' S_p b'^{-1} = S_p$ □

5.2.10 Satz (Abel-Ruffini)

Sei $f \in \mathbb{Q}[x]$ irreduzibel vom ungeraden Primzahlgrad p mit genau 2 nicht-reellen Nullstellen, sei L der Zerfällungskörper von f, dann gilt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong S_p$.

Beweis: Sei $\lambda \in \mathbb{C}$ eine Nullstelle von f, so gilt $f(\bar{\lambda}) = \overline{f(\lambda)} = \bar{0} = 0$

$\Rightarrow$ die komplexe Konjugation $j: \mathbb{C} \to \mathbb{C}$ permutiert die Nullstellen von f

$\Rightarrow j|_L : L \to L \subset \mathrm{Aut}_{\mathbb{Q}}(L)$

Da f genau $p-2$ reelle Nullstellen hat, ist $j|_{\text{Nullstellen}}$ eine Transposition.

Sei α eine Nullstelle von f,

dann gilt

$p = [\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [L : \mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(L)|$,

da $\mathbb{Q} \subset L$ Galoiserweiterung wegen 4.7.11 und 4.5.11 (char $\mathbb{Q} = 0$, also f separabel).

Damit enthält $\mathrm{Aut}_{\mathbb{Q}}(L)$ p-Sylowgruppen der Ordnung p, also einen p-Zykel.

Mit 5.2.9 folgt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong S_p$. □

5.2.11 Korollar

$f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist über $\mathbb{Q}$ nicht durch Radikale auflösbar.

Beweis:

Wegen des Eisensteinkriteriums 4.3.9 ist f irreduzibel über $\mathbb{Z}$ und wegen 4.3.10 auch über $\mathbb{Q}$.

Es gilt für $t \in \mathbb{R}$:

t	-2	-1	1	2
$f(t)$	-22	5	-1	26

Aus dem Zwischenwertsatz folgt dann, daß f mindestens 3 reelle Nullstellen besitzt.

$f' = 5x^4 - 4$

besitzt zwei reelle Nullstellen

$x = \pm \sqrt[4]{\frac{4}{5}}$, daher gibt es

nur 2 lokale Extrema und

daher höchstens 3 reelle Nullstellen.

Damit hat f genau zwei nicht-reelle Nullstellen.

Aus Abel-Ruffini 5.2.10 folgt,

daß für den Zerfällungskörper L

von f gilt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong S_5$.

Wegen 1.6.6 ist $\mathrm{Aut}_{\mathbb{Q}}(L)$ nicht

auflösbar. Wegen 5.2.3 ist f

nicht durch Radikale auflösbar.

Bemerkung:

Daraus folgt, daß es für Polynome

vom Grad ≥ 5 keine allgemeinen Formeln für die Nullstellen wie die Cardano-Formeln geben kann.
Auch wenn für einzelne Polynome (siehe 5.2.6) solche Formeln gibt, so gibt es aber auch welche, für die es keine gibt (5.2.11), so daß es keine allgemeingültigen geben kann.

Notizen zoom-meeting 24.7.

zu Gruppen:

1. Operationen $G \times M \to M$

2. Konjugation $G \times G \to G : (g,h) \mapsto ghg^{-1}$

3. Konjugation M = Menge (aller) Untergruppen von G
$G \times M \to M : (g,U) \mapsto gUg^{-1}$

2. + 3. sind Spezialfälle von 1.

Operation	Stabilisator	Bahn
2. Konjugation	Zentralisator	Konjugationsklasse
3. "	Normalisator	"

$$\text{Zentrum} = \{g \mid hg = gh \ \forall h \in G\}$$

Bsp: $G = S_3$ 2. Konjugationsklasse von $(12) = \{(12),(23),(13)\}$

3. $A_3 = \{id, (123), (132)\}$ Konjugationsklasse von $A_3 =$

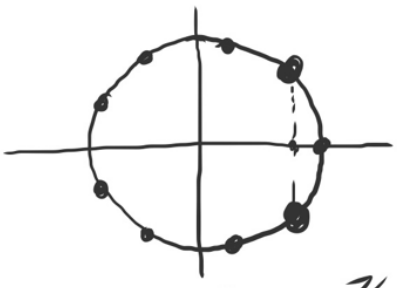
$\{A_3\}$

Zu Körpern:

K Zfkp von $x^9 - 1$ / $\mathbb{Q}$.

$\mathbb{Q} \subset K$ Galoiserweiterung

$K = \mathbb{Q}(\zeta) \qquad \zeta = e^{\frac{2\pi i}{9}}$



$\varphi_k : \zeta \mapsto \zeta^k$ invertierbar $\Leftrightarrow$ k Einheit in $\mathbb{Z}_9$

$\varphi_k \mapsto k$, $\mathrm{Aut}_{\mathbb{Q}}(K) \cong \mathbb{Z}_9^*$

$(\mathbb{Z}_9^*, \cdot) = \{1, 2, 4, 5, 7, 8\} \cong (\mathbb{Z}_6, +) = \langle 1 \rangle$

$(2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 = 7,\ 2^5 = 14 = 5,\ 2^6 = 10 = 1)$

$\langle 2 \rangle$

1

$2 = 1+1$

$3 = 1+1+1$

2

$2 \cdot 2 = 4$

$2 \cdot 2 \cdot 2 = 8$

$\mathbb{Z}_6$

$\mathbb{Z}_2 \cong \langle 3 \rangle$ $\qquad$ $\mathbb{Z}_3 \cong \langle 2 \rangle$

$\langle 0 \rangle$

$\mathbb{Z}_6 \cong \mathrm{Aut}_{\mathbb{Q}}(K)$

$\mathbb{Z}_2 \cong \langle \varphi_8 \rangle = U_2$ $\qquad$ $\langle \varphi_4 \rangle \cong \mathbb{Z}_3 = U_1$

$\{id\}$

(*) Minpoly$(a) = x^3 - 3x + 1$ (Nullstellensatz) $\Rightarrow \mathbb{Q}(a) = F_2$

$\mathbb{Q}$

$\mathrm{Fix}(U_2) = F_2$ $\qquad$ $F_1 = \mathrm{Fix}(U_1)$

K

$U_1 = \mathrm{Aut}_{F_1}(K)$

$[K : F_1] = |U_1| = 3 \Rightarrow [K : F_1] \cdot [F_1 : \mathbb{Q}] = [K : \mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(K)| = |\mathbb{Z}_6| = 6$

$3 \qquad 2$

$\varphi_4(\zeta^3) = (\zeta^3)^4 = \zeta^{12} = \zeta^3 = e^{2\pi i/3}$

$\Rightarrow F_1 = \mathbb{Q}(\zeta^3)$ Minpoly$(\zeta^3) = \frac{x^3 - 1}{x - 1}$

$[F_2 : \mathbb{Q}] = 3. \qquad (\zeta^8)^8 = \zeta^{64} = \zeta$ Sei

$a = \zeta + \zeta^8 \Rightarrow \varphi_8(a) = a \Rightarrow \mathbb{Q}(a) \subset F_2$ (*)