4.3 Auflösbarkeit von Gleichungen

Fragen:

1) Kann man die Nullstellen eines Polynoms $f \in \mathbb{Q}[X]$ immer in der Form „was mit Wurzeln" schreiben?

2) Gibt es für geschlossene Formeln?

ZB

$X^3 + pX + q$ hat Nullst.

$$\alpha - \frac{p/3}{\alpha}, \quad \alpha = \sqrt[3]{-\frac{q}{2} + \sqrt[2]{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Hier: Frage 1.

Exkurs: Einheitswurzeln

K: Körper, $\zeta \in K^*$ heißt

- <u>n-te Einheitswurzel</u> $(n > 0)$, falls $\zeta^n = 1$.
- <u>primitive n-te Einheitswurzel</u>, falls $\operatorname{ord} \zeta = n$.

Sei

$$\mu_n(K) = \{ \zeta \in K^* \mid \zeta \text{ ist n-te Einh.wurzel} \}$$

ZB. $\mu_n(\mathbb{C}) = \{ e^{2\pi i k/n} \mid k \in \mathbb{Z} \}$

... Einheitswurzeln

$\mu_n(K) = \{ \zeta \in K^* \mid \zeta$ ist n-te Einh.wurzel $\}$

Bem.:

1) $\zeta \in \mu_n(K) \Leftrightarrow \zeta$ ist Nullst. von $X^n - 1$

2) $\mu_n(K)$ ist eine Untergruppe von K^*. (Warum?)

- Wegen 1) ist $\mu_n(K)$ endlich.
- 2.5, Satz 4 : $\mu_n(K)$ ist zyklisch

Radikale

<u>**Def.:**</u> L/K Körpererw., $a \in K^*$.

Eine Nullstelle von $X^n - a$ $(n>0)$ heißt ein <u>Radikal von a über K</u>. Schreibe $\sqrt[n]{a}$.

⚠ $\sqrt[n]{a}$ ist nur bis auf n-te Einheitswurzeln bestimmt:

u, v Nullst. von $X^n - a$

$\Rightarrow$ u/v Nullst. von $X^n - 1$

$\Rightarrow$ $v = \zeta u$, $\zeta \in \mu_n(K)$.

... Radikale

<u>Def.:</u>

Eine Körpererw. L/K heißt <u>durch Radikale auflösbar</u>, falls es Körpererw.

$$K = K_0 \subset K_1 \subset \cdots \subset K_k$$

gibt mit

- $L \subset K_k$
- $K_i = K_{i-1}(a_i)$ mit $u_i \in K_i$, $u_i^{m_i} \in K_{i-1}$

(sei $a_i = u_i^{m_i}$, dann $K_i = K_{i-1}(\sqrt[m_i]{a_i})$)

... Radikale

<u>Def.:</u>

Für ein Polynom $f \in K[X] \setminus K$ sagt man, <u>die Gleichung $f(X) = 0$ sei durch Radikale auflösbar</u>, falls der Zerfällungskörper L/K von f durch Radikale auflösbar ist

Kann man die Nullstellen eines Polynoms $f \in \mathbb{Q}[X]$ immer in der Form „was mit Wurzeln" schreiben?

$\leadsto$ Ist für jedes $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ $f(X) = 0$ durch Radikale auflösbar?

Satz 1 K : Körper

$N \in \mathbb{Z}_{>0}$ s.d. $\operatorname{char} K \nmid N$ falls $\operatorname{char} K \neq 0$.

K enthalte eine primitive N-te Einheitswurzel.

Für eine endliche Körpererw. L/K sind äquiv.:

1) $L = K(\sqrt[n]{a})$ für ein $a \in K$ und ein $n > 0$ mit $n \mid N$

2) L/K galoisch und $G(L/K)$ zyklisch mit $|G(L/K)| \mid N$.

Bem. 2 (Notation aus Satz 1)

- K enthält prim. N-te Einheitswurzel

  $\Rightarrow$ K —"—— n-te —"—— (Warum?)

- Sei $\zeta \in K$ prim. n-te Einheitswurzel. Dann:

  $$\{ \zeta^k \sqrt[n]{a} \mid k = 0, 1, \dots, n-1 \}$$

  sind die n Nullst. von $X^n - a$.

Satz 1 K : Körper

$N \in \mathbb{Z}_{>0}$ s.d. $\operatorname{char} K \nmid N$ falls $\operatorname{char} K \neq 0$.

K enthalte eine primitive N-te Einheitswurzel.

Für eine endliche Körpererw. L/K sind äquiv.:

1) $\cancel{L = K(\sqrt[n]{a})}$ für ein $a \in K$ und
L ist Zerfällungskörper von $X^n - a$ ein $n > 0$ mit $n \mid N$

2) L/K galoisch und $G(L/K)$ zyklisch mit $|G(L/K)| \mid N$.

Lem. 3 (ohne Beweis – siehe Jantzen, Schwermer, VI.3.3)

K : Körper

$\sigma_1, \dots, \sigma_n \in \mathrm{Aut}\, K$ paarw. verschieden.

Dann ist

$$\{\sigma_1, \dots, \sigma_n\} \subset \mathrm{Abb}(K, K)$$

linear unabhängig.

K-Vektorraum

(allg.: für eine Menge M ist $\mathrm{Abb}(M, K)$ ein K-VR)

Satz 4

L/K endl. Körpererw., char $K = 0$

Es sind äquivalent:

1) L/K ist durch Radikale auflösbar.

2) Es gibt $K \subset L \subset M$ mit M/K endl. & gal., so dass $G(M/K)$ auflösbar.

Erinnerung (Kap 1.7):

auflösbare Gruppe $\overset{\text{Def}}{=}$ hat abelsche Normalreihe

Kor. 5

und galois'sch

L/K endl. Körpererw., char $K = 0$

Es sind äquivalent:

1) L/K ist durch Radikale auflösbar.

2) ~~Es gibt $K \subset L \subset M$ mit M/K endl. & gal., so dass $G(M/K)$ auflösbar.~~
$G(L/K)$ ist auflösbar.

Bem.: K : Körper, $\operatorname{char} K = 0$

$f \in K[X] / K$

L/K : Zerfällungskörper von f

Dann.:

1) L/K ist endl. & galois'sch

endl. : ✓
normal : 4.1, Satz 1
separabel : 4.1, Kor. 5

2) $\{b_1, \dots, b_n\} \subset L$ Nullst. von f. Dann

$$s : G(L/K) \longrightarrow S_n$$
$$\varphi \longmapsto s_\varphi \text{ s.d. } \varphi(b_i) = b_{s_\varphi(i)}$$

... Bem.: K : Körper, $\operatorname{char} K = 0$

$f \in K[X] / K$

L/K : Zerfällungskörper von f

2) $\{b_1, \dots, b_n\} \subset L$ Nullst. von f. Dann ist

$$s : G(L/K) \longrightarrow S_n$$
$$\varphi \longmapsto s_\varphi \text{ s.d. } \varphi(b_i) = b_{s_\varphi(i)}$$

injektiver Gr. hom.

- b Nullst. von $f \Rightarrow \varphi(b)$ Nullst. von f (Warum?)
- $L = K(b_1, \dots, b_n)$, also φ durch Wirkung auf b_i festgelegt ($\Rightarrow s$ inj)
- s Gr. Hom: nachrechnen (Details?)

Auflösbarkeit von Gleichungen

- $f \in K[X] \setminus K$ (char $K = 0$)
  $N = \{b_1, \dots, b_n\} \subset \overline{K}$ Nullst. von f.
- $K(N)$ durch Radikale auflösbar
  $\Leftrightarrow$ $G(K(N)/K) \hookrightarrow S_n$ auflösbar
- 1.7, Lem 2 : UG von aufl. Gr. sind auflösbar
  1.7, Bsp. , Satz 1, Lem 2. :

  $\boxed{S_n \text{ auflösbar} \quad \Leftrightarrow \quad n \leq 4}$
- ZB. $X^5 - 4X - 1 \in \mathbb{Q}[X]$ hat $G(L/\mathbb{Q}) \simeq S_5$