28. Vorlesung, 31.01.2011 (86)

(iv) Winkeldreiteilung ist i.A. unmöglich: $e^{i\pi/3} \in K(M)$ aber $e^{i\pi/9} \notin K(M)$ sonst wäre der 9-Eck konstruierbar.

4.4 Zyklische Erweiterungen

4.4.1 Def $K \subset L$ heißt zyklisch, falls sie galois ist und $Gal(L/K)$ zyklisch ist.

4.4.2 Satz Sei char $K = 0$, $K \subset L$ zyklisch, $n = [L:K]$
Enthält K eine primitive n-te Einheitswurzel so ist L Zerfällungskörper eines Pol. $X^n - b \in K[X]$

4.4.3. Lemma Seien $\varphi_1, \dots, \varphi_n \in Aut(L)$ paarweise verschieden
$\rightsquigarrow \varphi_1, \dots, \varphi_n \in Abb(K^*, K)$ linear unabhängig.

Beweis des Satzes 4.4.2 Es gilt $Gal(L/K) = \{e, \sigma, \dots, \sigma^{n-1}\}$
Sei $\zeta \in K$ primitive n-te EHW. Sei $\psi = Id_L + \zeta\sigma + \zeta^2\sigma^2 + \dots + \zeta^{n-1}\sigma^{n-1}$ $\in Aut(L)$. Lemma 4.4.3 $\rightsquigarrow \psi \neq 0$ d.h. $\exists x \in L^*: a = \psi(x) \neq 0$.

$\rightsquigarrow \sigma(a) = \sigma(\psi(x)) = \sigma(x) + \zeta\sigma^2(x) + \dots + \zeta^{n-1}\underbrace{\sigma^n(x)}_{=x} = \zeta^{-1}a$

$\rightsquigarrow \sigma(a^n) = \sigma(a)^n = \zeta^{-n}a^n = a^n \rightsquigarrow \sigma^k(a^n) = a^n, 0 \leq k \leq n-1$
$\rightsquigarrow a^n \in L^{Gal(L/K)} = K$, d.h. a ist Nst. von $X^n - a^n \in K[X]$.
Wir zeigen, dass $L = K(a)$. Sei $f \in K[X]$ Minpol. zu $a \rightsquigarrow$
$0 = \sigma^k(f(a)) = f(\sigma^k(a)) = f(\zeta^{-k}a)$, $k = 0, \dots, n-1$
$\rightsquigarrow \{a, \zeta^{-1}a, \dots, \zeta^{-n+1}a\}$ Nst. von $f \rightsquigarrow$ grad $f \geq n$
Aber $[K(a):K] = $ grad $f \geq n \rightsquigarrow K(a) = K$, grad $f = n$
Außerdem $f = (X-a)(X-\zeta a)\dots(X-\zeta a^{n-1}) = X^n - a^n$. ∎

Beweis von Lemma 4.4.3 Induktion nach k; $k=1$: $\lambda_1\varphi_1 = 0$
$\rightsquigarrow 0 = \lambda_1\varphi_1(1) = \lambda_1$ ✓ $\quad n-1 \rightsquigarrow n$: Sei $\lambda_1\varphi_1 + \dots + \lambda_n\varphi_n = 0$
$\exists a \in K^*$ mit $\varphi_1(a) \neq \varphi_n(a)$, da $\varphi_1 \neq \varphi_n$. Dann gilt:

$$\lambda_1\varphi_1(ax) + \lambda_2\varphi_2(ax) + \dots + \lambda_n\varphi_n(ax) = 0$$

$$\lambda_1\varphi_n(a)\varphi_1(x) + \lambda_2\varphi_n(a)\varphi_2(x) + \dots + \lambda_n\varphi_n(a)\varphi_n(x) = 0$$

Substraktion $\rightsquigarrow \lambda_1[\varphi_1(a)-\varphi_n(a)]\varphi_1(x)+\ldots+\lambda_{n-1}[\varphi_{n-1}(a)-\varphi_n(a)]\varphi_{n-1}(x)$ $=0$. Induktionsannahme $\rightsquigarrow \lambda_1\underbrace{[\varphi_1(a)-\varphi_n(a)]}_{\neq 0}=0 \rightsquigarrow \lambda_1=0$

$\rightsquigarrow \lambda_2\varphi+\ldots+\lambda_n\varphi_n=0 \overset{\text{I.A.}}{\rightsquigarrow} \lambda_2=\ldots=\lambda_n=0$ ▨

4.5. Lösbarkeit polynomialer Gleichungen.

Ziel der klassischen Algebra war Verfahren zur Lösung Polynomialgl. zu finden.

- Quadratische Gleichung (ca. 1700 v. Chr. in Babylon)

  Sei K Körper, char $K\neq 2$, $f=aX^2+bX+c\in K[X]$

  $f(x)=0 \Leftrightarrow g(x)=0$ wobei $g=X^2+pX+q$, $p=\frac{b}{a}, q=\frac{c}{a}$

  Quadratische Ergänzung: $x^2+px+\left(\frac{p}{2}\right)^2=-q+\left(\frac{p}{2}\right)^2$

  $\rightsquigarrow \left(x+\frac{p}{2}\right)^2=\frac{p^2-4q}{4} \rightsquigarrow x_1,x_2=\frac{-p\pm\sqrt{p^2-4q}}{2}$

  Dabei ist $\Delta=p^2-4q=(x_1-x_2)^2$ die Diskriminante von f.
  Ist Δ ein Quadrat in K, so gilt $x_1,x_2\in K$.
  Sonst liegen $x_{1,2}$ in $\overline{K}$.

- Kubische Gleichung (dal Ferro, Tartaglia ca. 1515, Cardano 1545 in „Ars Magna")

  Sei $K\subset\mathbb{R}$ ($\rightsquigarrow$ char $K=0$), $f=a_3X^3+a_2X^2+a_1X+a_0\in K[X]$

  Reduktion auf die vereinfachte Form: Multiplikation mit $a_3^{-1} \rightsquigarrow g=X^3+\alpha X^2+\beta X+\gamma$. Variabelsubstitution $y=x+\frac{\alpha}{3} \rightsquigarrow h=X^3+pX+q$

  Ansatz von dal Ferro und Tartaglia zur Lösung von $x^3+px+q=0$: suche x in der Form $x=u+v$

  $\rightsquigarrow (u+v)^3=-p(u+v)-q \underset{\text{Formel}}{\overset{\text{Binom.}}{\rightsquigarrow}} u^3+v^3+3uv(u+v)=-p(u+v)-q$

  Suche u,v, so dass $\begin{cases} u^3+v^3=-q \\ 3uv=-p \end{cases}$

Setze $v = -p/3u$ in der ersten Gl. und multipliziere mit $u^3 \rightsquigarrow$
$(u^3)^2 + q(u^3) - \frac{p^3}{27} = 0$; quadratische Resolvente: $y^2 + qu - \frac{p^3}{27} = 0$
(Die Diskr. der quadr. Resolv. ist $q^2 + 4\frac{p^3}{27} = \frac{4p^3+27q^2}{27} = \frac{-\Delta}{27}$
wobei $\Delta = -4p^3 - 27q^2 = (x-x_1)^2(x_2-x_3)^2(x_3-x_1)^2$ die Diskr. von $h = X^3 + pX + q$ ist.)

$\rightsquigarrow y_{1,2} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \rightsquigarrow u^3 = y_1$ oder y_2

Aus $u^3 + v^3 = -q$ sieht man: $u^3 = y_1 \rightsquigarrow v^3 = y_2$, $u^3 = y_2 \rightsquigarrow v^3 = y_1$.
Wir lösen nun $u^3 = y_1$, $v^3 = y_2$, $uv = -3p$. Dabei muss man berücksichtigen, dass $U^3 - y = 0$ drei Nullstellen haben kann.
Es gibt eine Fallunterscheidung:

(i) $\Delta < 0 \rightsquigarrow y_{1,2} \in \mathbb{R}$. Jede reelle Zahl hat genau eine reelle dritte Wurzel ($\mathbb{R} \ni x \mapsto x^3 \in \mathbb{R}$ bijektiv) $\rightsquigarrow$ man kann $u^3 = y_1$, $v^3 = y_2$ eindeutig in $\mathbb{R}$ lösen. Sind die Lösungen u_1, v_1 so ist

$$x_1 = \underbrace{\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}}_{u_1} + \underbrace{\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}}_{v_1}$$

eine Lösung von $x^3 + px + q = 0$. Dies ist Cardanos Formel.
Weitere Lösungen von $u^3 = y_1$, $v^3 = y_2$ sind $\{u_1\zeta, u_1\zeta^2\}$ und $\{v_1\zeta, v_1\zeta^2\}$ mit $\zeta = e^{2\pi i/3}$. Wegen $3uv = -p$ finden wir noch zwei Lösungen von $x^3 + px + q = 0$, nämlich

$$x_2 = \zeta u_1 + \zeta^2 v_1, \quad x_3 = \zeta^2 u_1 + \zeta v_1.$$

(ii) $\Delta = 0 \rightsquigarrow y_1 = y_2 = -\frac{q}{2}$; sei $u_1 = v_1 = \sqrt[3]{-\frac{q}{2}} \in \mathbb{R}$. Dann
$x_1 = u_1 + v_1 = 2\sqrt[3]{-\frac{q}{2}}$, $x_2 = \zeta u_1 + \zeta^2 v_1 = \zeta^2 u_1 + \zeta u_1 = x_3$
Übrigens $\zeta + \zeta^2 = -1$ also $x_2 = x_3 = (\zeta + \zeta^2)u_1 = -u_1$.
Alle Nst. sind also reel. Ist $q \neq 0 \rightsquigarrow x_1$ einfach, x_2 doppelte Nst.
$q = 0 \rightsquigarrow x_1 = x_2 = x_3 = 0$ dreifache Nst.

(iii) $\Delta > 0 \rightsquigarrow y_1, y_2 \notin \mathbb{R}$ (Casus irreducibilis)

Seien δ_1, δ_2 die Wurzeln von $-\frac{\Delta}{27}$ ($\overline{\delta_1} = \delta_2$). Dann gilt

$y_1 = \frac{-q+\delta_1}{2}$, $y_2 = \frac{-q+\delta_2}{2}$ ($\overline{y_1} = y_2$).

Wähle nun eine 3-Wurzel von $y_1 = |y_1| e^{i\varphi}$ z.B. $z = \sqrt[3]{|y_1|}\, e^{i\varphi/3}$

Dann sind $\rho z, \rho^2 z$ die anderen 3-Wurzeln, und $\overline{z}, \rho\overline{z}, \rho^2\overline{z}$ die 3-Wurzeln von $y_2 = \overline{y_1}$. Wegen $3uv = -p$ ergeben sich die Lösungen $(u_1, v_1) = (z, \overline{z})$, $x_1 = z + \overline{z} = 2\operatorname{Re} z$

$(u_2, v_2) = (\rho z, \rho^2 \overline{z}) = (\rho z, \overline{\rho z}) \rightsquigarrow x_2 = 2\operatorname{Re}(\rho z)$

$(u_3, v_3) = (\rho^2 z, \rho\overline{z}) = (\rho^2 z, \overline{\rho^2 z}) \rightsquigarrow x_3 = 2\operatorname{Re}(\rho^2 z)$

Ironischerweise sind alle drei Wurzeln von $x^3 + px + q = 0$ <u>reell</u> obwohl die Wurzel der Resolvente nicht reell sind.

- <u>Gleichung vierten Grades</u> Auch hier lässt sich eine Formel herleiten (mit Hilfe der kubischen Resolvente), sie ist allerdings sehr kompliziert.
- Abel (1826) bewies (nach Vorarbeiten von Ruffini), dass keine allgemeine Lösung der Gleichung 5. Grades gibt.
- Schließlich gab Galois (1832) eine umfassende und genauere Antwort, wann Polynomialgleichungen "durch Radikale" lösbar sind.

<u>4.4.1 Def.</u> Eine Körpererw. $K \subset L$ heißt <u>Radikalerweiterung</u> wenn es eine Kette $K = L_0 \subset L_1 \subset \dots \subset L_r = L$ gibt mit $L_i = L_{i-1}(a_i)$ mit $a_i \in L_i$, $a_i^{n_i} \in L_{i-1}$

(d.h. L_i entsteht aus L_{i-1} durch Adjunktion einer Nst. eines Pol. $X^{n_i} - b_i \in L_{i-1}[X]$)

Ein Polynom $f \in K[X]$ heißt <u>durch Radikale lösbar</u> wenn es eine Radikalerw. $E \supset K$ gibt, so dass $K \subset L \subset E$, wobei L der Zerfällungskörper von f ist.