III. Auflösung durch Radikale und auflösbare Gruppen.

Als Korollar der in diesem Kapitel entwickelten Theorie werden wir den Satz von Abel–Ruffini erhalten, daß die allgemeine Gleichung 5. Grades mittels radikalen nicht lösbar ist.

Ein wichtiger Schritt besteht darin die intuitive Idee einer "Formel" für die Nullstellen eines Polynoms mittels der arithmetischen Operationen plus Wurzelzeichen präzise zu formalisieren.

Dafür führen wir die Begriffe von reiner und radikaler Erweiterung an.

Sei $K = k(u)$ eine Körpererweiterung von k. Offensichtlich ist

$$\{ n \in \mathbb{Z} : u^n \in k \}$$

eine Untergruppe von $\mathbb{Z}$ und daher der Form $m \cdot \mathbb{Z}$ für ein eindeutig bestimmtes

$$m \in \mathbb{N}.$$

Definition III.1 $k(u)/k$ ist eine reine Erweiterung vom Typ m falls

$$m\mathbb{Z} = \{ n \in \mathbb{Z} : u^n \in k \} \neq 0$$

d.h. $m \geq 1$.

Definition III.2 Eine Körpererweiterung E/k heißt radikal falls es einen Turm von Zwischenkörper gibt

$$k = K_0 \subset K_1 \subset \cdots \subset K_t = K$$

so dass K_{i+1}/K_i für jedes $0 \leq i \leq t-1$

eine reine Erweiterung ist.

Und

Definition IV.3 Ein Polynom $f \in k[X]$ ist mit Coeff. Radikalen lösbar falls ein Zerfällungskörper von f in einer radikalen Erweiterung von k enthalten ist.

Beispiel IV.4. Sei $f(x) = x^2 + bx + c \in k[X]$ und E ein Zerfällungskörper von f. Wir nehmen an $E \neq k$ und sei $R(f) = \{\alpha_1, \alpha_2\}$. Nun für $\alpha \in R(f)$:

$$0 = \alpha^2 + b\alpha + c = \left(\alpha + \frac{b}{2}\right)^2 + c - \frac{b^2}{4}$$

Definiere $u := \alpha_1 + \frac{b}{2}$; dann ist $k(u)/k$ eine reine Erweiterung von Typ 2. Wir behaupten, dass $E = k(u)$.

Offensichtlich ist $\alpha_1 = u - \frac{b}{2} \in k(u)$ und

$$\alpha_2 = -b - \alpha_1 \in k(u)$$

woraus $E = k(u)$ folgt. Also ist f mittels Radikalen auflösbar.

Folgende Bemerkung reduziert das Studium von reinen Erweiterung auf solche vom Primzahltyp: Sei $k(u)/k$ rein vom Typ $m = p_1 \cdot \ldots \cdot p_r$, wobei sich eine Primzahl mehrfach wiederholen kann. Dann haben wir einen Turm:

$$k(u) \supset k(u^{p_1}) \supset k(u^{p_1 p_2}) \supset \ldots \supset k(u^m) = k$$

wobei alle aufeinander folgenden Erweiterungen vom Primzahltyp sind.

Dies führt zum Studium von

$$X^p - c \in k[X].$$

Lemma III.5. Sei p eine Primzahl und

$$f(x) = x^p - c \in k[x].$$

(1) Folgende Dichotomie gilt

(a) f ist irreduzibel,

(b) c ist eine p-te Potenz in k.

(2) Sei E/k ein Zerfällungskörper von f. Wir nehmen an, dass k alle p-ten Wurzeln von 1 enthält. Sei $u \in R(f)$. Dann ist $E = k(u)$.

(2.1) Annahme f ist irreduzibel.

Falls $\mathrm{char}(k) \neq p$, $\mathrm{Gal}(k(u)/k) \cong \mathbb{Z}/p\mathbb{Z}$

Falls $\mathrm{char}(k) = p$, $\mathrm{Gal}(k(u)/k) \simeq (e)$.

(2.2) Annahme, f ist reduzibel

Dann ist $k(u) = k$ und $\mathrm{Gal}(k(u)/k) = (e)$.

Beweis:

(1) Sei $f = g \cdot h$ mit

$$g(x) = x^d + b_{d-1} x^{d-1} + \dots + b_0$$

und $1 \leq d < p$.

Sei $E > k$ ein Zerfällungskörper von f und $u \in R(f)$. Dann ist

$$R(f) = \{ u \cdot \zeta : \zeta^p = 1, \zeta \in E \}$$

und $b_0 = u^d \cdot \zeta$ wobei $\zeta \in E$ und

$$\zeta^p = 1.$$

Daraus folgt: $b_0^p = u^{d \cdot p} = c^d$.

Da d und p Teilerfremd sind seien $r, s \in \mathbb{Z}$ mit $rp + sd = 1$. Dann folgt:

$$c = c^{rp} \cdot c^{sd} = c^{rp} b_0^{ps}$$

$$= (c^r b_0^s)^p .$$

Dies zeigt (1).

(2) Die erste Aussage ist klar.

Falls $\mathrm{char}\, k \neq p$, ist f separabel und falls f irreduzibel ist ist $[k(u):k] = p$; da $k(u)$ auch Zerfällungskörper von f folgt aus Satz II.17:

$$|\mathrm{Gal}(k(u)/k)| = p$$

Aber dann muss $\mathrm{Gal}(k(u)/k) \cong \mathbb{Z}/p\mathbb{Z}$.

Falls $\mathrm{char}\, k = p$:

$$X^n - c = X^n - u^n = (X-u)^p$$

woraus $\mathrm{Gal}(k(u)/k) \cong \{e\}$ folgt.

Falls f reduzibel folgt c ist eine p-te Potenz und da k alle p-ten Wurzeln von 1 enthält folgt $k(u) = k$. ∎

Um das Problem der Lösbarkeit eines Polynoms mittels Radikalen mit Gruppentheorie in Verbindung zu setzen werden wir anhand der nächsten Lemmas zeigen, dass eine radikale Erweiterung immer in einer normalen radikalen Erweiterung enthalten ist.

Dies führt dann zu folgender Situation:

Sei $f \in k[x]$ auflösbar mittels Radikalen, E Zerfällungskörper von f und

$$k \subset E \subset K$$

wobei K/k eine radikale Erweiterung ist.

Falls es jetzt $k \subset E \subset K \subset F$ F/k radikale normale Erweiterung gibt dann folgt aus Thm 2.26, dass wir eine exakte Sequenz von Galois Gruppen

haben:

$$\to Gal(F/E) \longrightarrow Gal(F/k) \longrightarrow Gal(E/k) \to (e)$$

Falls wir dann zeigen können, dass eine radikale normale Erweiterung F/k eine auflösbare Galoisgruppe besitzt, folgt aus Standardfakten über auflösbare Gruppen, dass dann $Gal(E/k)$ als Quotient von $Gal(F/k)$ auch auflösbar ist.

Der Kontext der folgenden zwei Lemmas ist der Folgende: sei

$$B = k(u_1, \dots, u_t)$$

eine endliche Erweiterung von k,

$p_i = irr(u_i, k)$ das Minimalpolynom von u_i über k und $f = p_1 \cdot \dots \cdot p_t \in k[X]$.

Sei E ein Zerfällungskörper von f und

$G = G_{-1}(E|k)$.

Lemma 3.6. $E = k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G)$.

Beweis: Da E Zerfällungskörper von f folgt $R(p_i) \subset E$ $\forall$ $1 \le i \le t$.

Seien u, u' in $R(p_i)$. Dann gibt es (Lemma 2.15) einen Isomorphismus

$$\varphi : k(u) \to k(u')$$

der id_k erweitert. Nun ist $f \in k(u)[X]$ und $\varphi_*(f) = f$; zudem ist E auch Zerfällungskörper von $f \in k(u)[X]$. Aus Satz 2.16 folgt, dass φ sich zu einem Isomorphismus $\overline{\Phi} : \overline{E} \to \overline{E}$ erweitert. Da $\overline{\Phi}|_k = id_k$ folgt $\overline{\Phi} \in G_{-1}(E|k)$ und da $\overline{\Phi}|_{k(u)} = \varphi$ folgt $\overline{\Phi}(u) = u'$.

Es folgt, dass $R(f) = \bigcup_{i=1}^{t} R(p_i) \subset k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G)$

Woraus $k(\sigma(u_1), \ldots, \sigma(u_t) : \sigma \in G) = E$

folgt. ∎

26.3.2021

Lemma 3.7. Im Kontext von Lemma 3.6 nehmen wir an, dass:

$$u_1^{m_1} \in k, \quad u_2^{m_2} \in k(u_1), \quad \ldots, \quad u_t^{m_t} \in k(u_1, \ldots, u_{t-1}).$$

Dann ist E/k eine radikale Erweiterung.

Beweis: Sei $G = \{\sigma_1, \ldots, \sigma_e\}$

Dann folgt aus Lemma 3.6:

$$E = k\begin{pmatrix} \sigma_1(u_1), \ldots, \sigma_e(u_1) \\ \vdots \\ \sigma_1(u_t), \ldots, \sigma_e(u_t) \end{pmatrix}.$$

Sei

$$B_1 = k(\sigma_1(u_1), \ldots, \sigma_e(u_1))$$

und allgemein

$$B_j = B_{j-1}(\sigma_1(u_j), \ldots, \sigma_e(u_j)),$$

$$2 \leq j \leq t.$$

Wir erhalten einen Turm von Erweiterungen:

$k \subset B_1 \subset B_2 \subset \dots \subset B_t = E$

und zeigen $j \in \{1, \dots, t\}$, dass B_j eine radikale Erweiterung von B_{j-1} ist $\forall 1 \leq j \leq t$ wobei $B_0 := k$. Es folgt dann (Übung), dass E eine radikale Erweiterung von k ist.

Für B_1 haben wir den Turm von Erweiterungen:

~~$k \subset k(\sigma_1(u_1)) \subset k(\sigma_1(u_1))(\sigma_2(u_1)) \subset k(\sigma_1(u_1), \sigma_2(u_1))(\sigma_j(u_1))$~~

~~$k(\sigma_1(u_1), \sigma_2(u_1))$~~

$k \subset k(\sigma_1(u_1)) \subset k(\sigma_1(u_1), \sigma_2(u_1)) \subset k(\sigma_1(u_1), \sigma_2(u_1), \sigma_3(u_1))$

$\dots = k(\sigma_1(u_1), \dots, \sigma_e(u_1)) = B_1$.

$\sigma_1(u_1)^{m_1} = \sigma_1(u_1^{m_1}) = u_1^{m_1} \in k$.

Also ist $k(\sigma_1(u_1))$ reine Erweiterung von k.

Allgemein sei $2 \leq j \leq t$. Dann ist

$$k(\sigma_1(u_1), \ldots, \sigma_{j-1}(u_1), \sigma_j(u_1)) =$$

$$= k(\sigma_1(u_1), \ldots, \sigma_{j-1}(u_1))(\sigma_j(u_1))$$

Und $\sigma_j(u_1)^{m_1} = \sigma_j(u_1^{m_1}) = u_1^{m_1} \in k$

$$\in k(\sigma_1(u_1), \ldots, \sigma_{j-1}(u_1))$$

Woraus folgt, dass B_1 eine radikale Erweiterung von k ist.

Als nächstes bemerken wir, dass

$$\sigma(B_j) = B_j \qquad 1 \leq j \leq t.$$

Für $B_1 = k(\sigma_1(u_1), \ldots, \sigma_t(u_1))$

ist es klar, da $\forall \sigma \in G$:

$$\sigma\sigma_1(u_1), \ldots, \sigma\sigma_t(u_1)$$

eine Permutation der

$$\sigma_1(u_1), \ldots, \sigma_t(u_1) \text{ ist.}$$

Das selbe Argument zeigt induktiv, dass $\sigma(B_j) = B_j \quad 1 \le j \le t$.

Nun: $B_j = B_{j-1}(\sigma_1(u_j), \dots, \sigma_\ell(u_j))$.

Da $u_j^{m_j} \in k(u_1, \dots, u_{j-1}) \subset B_{j-1}$,

folgt $\sigma(u_j)^{m_j} = \sigma(u_j^{m_j}) \in \sigma(B_{j-1}) = B_{j-1}$

$\forall \sigma \in G$.

Das selbe Argument wie für B_1/k zeigt, dass B_j eine radikale Erweiterung von B_{j-1} ist. □

Aus Lemmas 3.6 und 3.7 folgt:

Korollar 3.8: Sei E Zerfällungskörper von $f \in k[X]$, $E \subset K$ wobei K/k radikal. Dann gibt es F/k radikale normale Erweiterung von k mit:

$$k \subset E \subset K \subset F.$$