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:

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

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 $\forall 1 \le j \le t$ 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:

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

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

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

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

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 sagt induktiv, dass $\sigma(B_j) = B_j \quad 1 \leq j \leq t$.

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

Da $u_j^{m_j} \in k(u_1, \ldots, u_{j-1})$, ~~Note~~

$$\subset B_{j-1}$$

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 sagt, 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:

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

Bevor wir den Hauptsatz beweisen müssen wir uns noch ein wenig mit auflösbaren Gruppen befassen.

Def. 3.9 (Siehe Algebra I) Eine Gruppe G ist auflösbar, falls es eine subnormale Reihe

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \cdots \triangleleft G_t = G$$

gibt mit G_{i+1}/G_i abelsch $\forall\, 0 \leq i \leq t-1$.

Beispiele 3.10 (Siehe Alg. I)

A_n, S_n sind auflösbar für $n \leq 4$.

A_n ist einfach (nicht abelsch) für $n \geq 5$.

~~Beweis~~

Es gibt ein Kriterium für Auflösbarkeit dass iterierte Kommutatoruntergruppen benützt. Für eine Gruppe G bezeichnet $[G,G]$ die von $\{[a,b] : a,b \in G\}$ erzeugte Untergruppe. Hier ist

$$[a,b] := aba^{-1}b^{-1}.$$

Nun ist $[G,G]$ nicht nur eine normale Untergruppe, sondern sogar eine charakteristische Untergruppe.

Def. 3.11. Eine Untergruppe $H < G$ heisst charakteristisch falls

$$\alpha(H) = H \quad \forall \alpha \in \mathrm{Aut}(G).$$

Sei induktiv $G^{(1)} := [G,G]$ und für $i \geq 1$, $G^{(i+1)} := [G^{(i)}, G^{(i)}]$.

In Algebra I wurde bewiesen:

Prop. 3.12 G ist genau dann auflösbar falls es $n \geq 1$ gibt mit $G^{(n)} = (e)$.

Wesentlich für uns ist

Prop. 3.13

(1) $H < G$; falls G auflösbar dann ist H auflösbar.

(2) $N \lhd G$: G ist genau dann auflösbar falls N und G/N auflösbar sind.

Beweis:

Wir beginnen mit einer allgemeinen Bemerkung: sei $\varphi : G \longrightarrow L$ ein Homomorphismus. Da $\forall a, b \in G$:

$$\varphi([a,b]) = [\varphi(a), \varphi(b)]$$

folgt $\varphi([G,G]) \subset [L,L]$ (*)

und falls φ surjektiv ist,

$$\varphi([G,G]) = [L,L]. \quad (**)$$

Aus (*) erhalten wir induktiv:

$$\varphi(G^{(j)}) \subset L^{(j)}$$

und falls φ surjektiv, folgt

$$\varphi(G^{(j)}) = L^{(j)}.$$

(1) Aus $H \hookrightarrow G$ folgt $H^{(j)} \subset G^{(j)}$;

falls es $n \geq 1$ gibt mit $G^{(n)} = \{e\}$

folgt, dass $H^{(n)} = \{e\}$ und somit

ist H auflösbar (Prop 3.12).

(2) Falls G auflösbar ist, ist noch

(1) $N \triangleleft G$ auflösbar; sei

$\varphi: G \to G/N$ der kanonische Homomorphismus und $n \geq 1$ mit $G^{(n)} = (e)$. Da φ surjektiv ist folgt (siehe Bemerkung)

$$(G/N)^{(n)} = \varphi(G^{(n)}) = \varphi(e) = e$$

somit ist G/N auflösbar.

Wir nehmen jetzt an, N und G/N sind auflösbar. Sei $j \geq 1$ mit $(G/N)^{(j)} = (e)$. Dann folgt:

$$\varphi(G^{(j)}) = \varphi(G)^{(j)} = (G/N)^{(j)} = e$$

und somit ist $G^{(j)} \subset N$. Sei $k \geq 1$ mit $N^{(k)} = (e)$. Dann folgt

$$G^{(j+k)} = (G^{(j)})^{(k)} \subset N^{(k)} = e$$

und somit ist G auflösbar. ∎

Theorem 3.14.

Sei $f \in k[x]$ und E ein Zerfällungskörper von f. Falls f mittels Radikalen lösbar ist, so ist $Gal(E/k)$ eine auflösbare Gruppe.

Lemma 3.15. Sei $k = K_0 \subset K_1 \subset \dots \subset K_t$ ein Turm von Erweiterungen, wobei

(1) K_t / k normale Erweiterung

(2) K_i / K_{i-1} ist eine reine Erweiterung vom Typ $\alpha_i^{p_i} \in$, p_i Primzahl, $\forall\, i$ mit $1 \leq i \leq t$.

(3) k enthält alle p_i-ten Wurzeln von 1 $1 \leq i \leq t$.

Dann ist $Gal(K_t / k)$ auflösbar.

Beweis:

Sei $G = G_0 = Gal(K_t / k)$

$G_1 = Gal(K_t / K_1)$

$\vdots$

$G_j = Gal(K_t / K_j)$

Dann gilt offensichtlich:

$\{e\} = G_t \subset G_{t-1} \subset \dots \subset G_1 \subset G$.

Sei auch $K_i = K_{i-1}(u_i)$ mit

$u_i^{p_i} \in K_{i-1}$, $1 \leq i \leq t$.

Sei $c_i := u_i^{p_i} \in K_{i-1}$ und

$f_i(x) = x^{p_i} - c_i \in K_{i-1}[x]$.

Aus $u_i \notin K_{i-1}$ und Lemma III.5 folgt, dass f_i irreduzibel ist, und da $K_{i-1} \supset k$ alle p_i-ten Wurzeln von 1 enthält ist K_i ein Zerfällungs-

"körper von f_i; aus Lemma III.5

folgt $Gal(K_i/K_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$ oder (e).

Nun sind K_t und K_i beides

normale Erweiterungen von K_{i-1},

und somit folgt, dass

$$G_i = Gal(K_t/K_i) \triangleleft G_{i-1} = Gal(K_t/K_{i-1})$$

und (siehe Thm II.26)

$$G_{i-1}/G_i \cong Gal(K_i/K_{i-1})$$

$$\cong \mathbb{Z}/p_i\mathbb{Z} \text{ oder (e)}.$$

Somit ist $G = G_0 = Gal(K_t/k)$

auflösbar. ∎

Beweis von Thm III.14.

Mittels Korollar III.8 können wir annehmen, dass $E \subset K$ wobei K/k radikal normal. Sei dann

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

wobei $K_i = K_{i-1}(u_i)$ eine reine Erweiterung von K_{i-1} von Primzahltyp p_i bezeichnet, $1 \le i \le t$. Insbesondere ist $u_i^{p_i} \in K_{i-1}$.

Sei $m = \prod_{i=1}^{t} p_i$; seien:

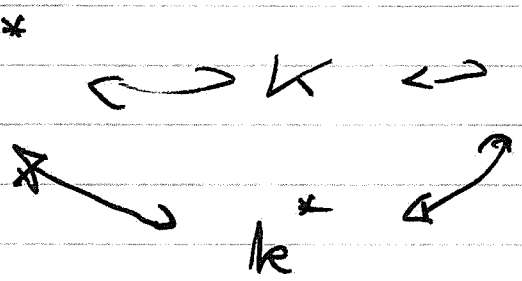
$K^* =$ Zerfällungskörper von $X^m - 1 \in K[X]$

$k^* =$ " . . . $\in k[X]$

Da K/k eine normale Erweiterung ist und $X^m - 1 \in k[X]$ folgt, dass K^*/k

auch normal ist.

Wir haben also ein Diagramm von Erweiterungen:



Wir zeigen jetzt, daß $\mathrm{Gal}(K^*/k^*)$ auflösbar ist und benützen dafür Lemma III.15:

sei $K_0^* = k^*$, $K_1^* := K_0^*(u_1)$, und induktiv $K_i^* = K_{i-1}^*(u_i)$. Nun ist $K_{i-1} \subset K_{i-1}^*$ und somit folgt

$$u_i^{p_i} \in K_{i-1} \subset K_{i-1}^*.$$

Da p_i eine Primzahl ist haben wir zwei Möglichkeiten:

(1) $K_i^* = K_{i-1}^*$ d.h. $u_i \in K_{i-1}^*$

(2) $K_i^* = K_{i-1}^*(u_i)$ ist rein vom Typ p_i.

Aus Lemma III.15 folgt dann, daß $\mathrm{Gal}(K^*/k^*)$ auflösbar ist.

Die nächste Behauptung ist, daß $\mathrm{Gal}(k^*/k)$ auflösbar ist: Sei

$$\Gamma_m(k^*) = \{\xi \in k^* : \xi^m = 1\}$$

die Menge der Nullstellen von $X^m - 1$ in k^*. Dann ist

$$\Gamma_m(k^*) < (k^*)^\times$$

eine endliche Untergruppe der multiplikativen Gruppe eines Körpers und somit zyklisch. Jedes $\sigma \in \mathrm{Gal}(k^*/k)$ gibt durch Restriktion auf $\Gamma_m(k^*)$ einen Automorphismus von $\Gamma_m(k^*)$.

Wir haben also einen Injektiven Gruppenhomomorphismus

$$Gal(k^*/k) \longrightarrow Aut\, \Gamma_m(k^*)$$

und da $\Gamma_m(k^*)$ zyklisch ist, folgt dass $Aut\, \Gamma_m(k^*)$ abelsch ist.

Somit ist $Gal(k^*/k)$ abelsch und somit auflösbar.

Nun sind $K^* \supset k^*$ beides normale Erweiterungen von k; somit ist $Gal(K^*/k^*) \lhd Gal(K^*/k)$ mit Quotient $Gal(k^*/k)$; aus Prop. III. 13. (c) folgt, dass $Gal(K^*/k)$ auflösbar ist. Da $Gal(E/k)$ Quotient von $Gal(K^*/k)$ (modulo $Gal(K^*/E)$) ist, folgt, dass $Gal(E/k)$ auflösbar ist. ∎