Das Kompositum von Körpern

Proposition (24.1)

Ist $\tilde{K}$ ein Körper mit Teilkörpern L und M, dann gilt

$$L(M) \quad = \quad M(L).$$

Man bezeichnet $L \cdot M = L(M) = M(L)$ als das Kompositum der Körper L und M in $\tilde{K}$. Es handelt sich dabei um den kleinsten Teilkörper von $\tilde{K}$, der $L \cup M$ enthält.

Der Verschiebungssatz der Galoistheorie

Satz (24.2)

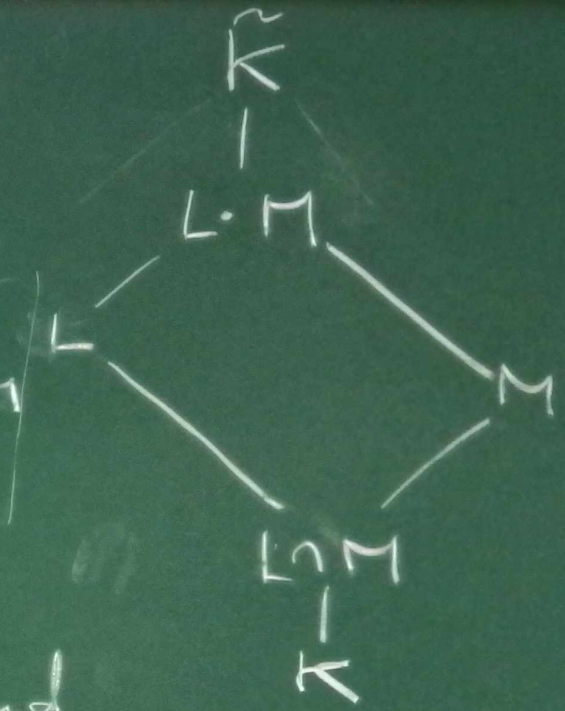
Sei $L|K$ eine endliche Galois-Erweiterung und $M|K$ eine weitere Körpererweiterung mit der Eigenschaft, dass L und M in einem gemeinsamen Erweiterungskörper $\tilde{K}$ enthalten sind. Dann sind auch $L \cdot M|M$ und $L|L \cap M$ Galois-Erweiterungen, und es gibt einen Isomorphismus

$$\phi : \mathrm{Gal}(L \cdot M|M) \longrightarrow \mathrm{Gal}(L|L \cap M)$$

von Gruppen mit $\phi(\tau) = \tau|_L$ für alle $\tau \in \mathrm{Gal}(L \cdot M|M)$.

Beweis von Satz 24.2

Vor. $L|K$ endliche Galois-Erw.
$M|K$ bel Körpererw.
$\tilde{K}$ gem. Erweiterungskörper von L und M
o.B.d.A. ist $\tilde{K}$ alg. abgeschlossen



(1) zeige: $L|L \cap M$ ist galoissch
Dies ist erfüllt, weil $L|K$ galoissch und $L \cap M$ ein Zwischenkörper von $L|K$ ist.
(2) zeige: $L \cdot M|M$ ist galoissch
$L|K$ ist endl. und separabel $\xrightarrow{\text{Satz vom prim. Element}}$ $\exists\, \alpha \in L$ mit

$L = K(\alpha)$ Seien $\alpha = \alpha_1, \ldots, \alpha_r$ die Nullstellen von $f = \mu_{\alpha, K}$ in L. $L|K$ normal $\Rightarrow \alpha_1, \ldots, \alpha_r \in L$

Beh. $LM = M(\alpha_1, \ldots, \alpha_r)$ „$\supseteq$" klar, da $\alpha_1, \ldots, \alpha_r \in L$

„$\subseteq$" zzg.: $M(L) \subseteq M(\alpha_1, \ldots, \alpha_r)$ genügt: $L \subseteq M(\alpha_1, \ldots, \alpha_r)$

Das ist wegen $L = K(\alpha_1, \ldots, \alpha_r)$ ebenfalls offensichtlich

Da α separabel über K ist ($L|K$ ist gal.), ist $f \in K[x]$ ein separables Polynom. $\mu_{\alpha_i, M}$ ist Teiler von $\mu_{\alpha_i, K} = f$ in $M[x]$ ($1 \leq i \leq r$) $\rightarrow$ $\mu_{\alpha_i, M}$ separabel ($1 \leq i \leq r$) $\Rightarrow$ α_i separabel über M ($1 \leq i \leq r$) Also ist $M(\alpha_1, \ldots, \alpha_r)$ eine separable Erweiterung. Außerdem ist $LM \overset{(*)}{=} M(\alpha_1, \ldots, \alpha_r)$ zerf. kop. von f über M. $\Rightarrow$ $LM|M$ ist normal insgesamt: $LM|M$ ist galois'sch (wegen $(*)$ darüber hinaus endlich)

(3) Zeige: Durch $\tau \mapsto \tau|_L$ ist ein Gruppenhom

$Gal(LM|M) \to Gal(L|L\cap M)$ definiert (*)

Sei $\tau \in Gal(LM|M)$ $\tau \in Aut(L\cdot M)$

$\Rightarrow \tau|_L$ ist Körperhom $L \to \bar{K}$.

wegen $M \supseteq L\cap M$, $\tau(\alpha) = \alpha \ \forall \alpha \in M$ darüber hinaus

ein $L\cap M$-Hom., d.h. $\tau|_L \in Hom_{L\cap M}(L, \bar{K})$

Teil (1) $\Rightarrow$ $L|L\cap M$ ist normal $\Rightarrow$

$\tau|_L \in Aut_{L\cap M}(L)$, d.h. $\tau|_L \in Gal(L|L\cap M)$

Bezeichne die Abb (*) mit ϕ. Die Hom-eig

ist leicht zu überprüfen (vgl. §22)

(4) zeige: ϕ ist injektiv

Sei $\tau \in \ker(\phi) \Rightarrow \tau|_L = \phi(\tau) = id_L$

τ ist M-Automorphismus $\Rightarrow \tau|_M = id_M$

$\Rightarrow L, M \subseteq (L \cdot M)^{\langle \tau \rangle} \Rightarrow LM = L(M) \subseteq (L \cdot M)^{\langle \tau \rangle}$

$\Rightarrow \tau = id_{L \cdot M}$

(5) zeige: ϕ ist surjektiv

Sei $G = Gal(L \cdot M | M)$ z.zg.: $\phi(G) = Gal(L | L \cap M)$ Nach dem Hauptsatz der Galoistheorie ist dies äquivalent zu $L^{\phi(G)} = L \cap M$. „$\supseteq$" ist klar, weil $L^{\phi(G)}$ als Fixkörper einer Untergruppe von $Gal(L|L \cap M)$ ein Zwischenkörper von $L | L \cap M$ ist.

„$\subseteq$" Sei $\alpha \in L^{\phi(G)} \Rightarrow \phi(\tau)(\alpha) = \alpha \quad \forall \tau \in G$

$\Rightarrow (\tau|_L)(\alpha) = \alpha \quad \forall \tau \in G \Rightarrow \tau(\alpha) = \alpha \quad \forall \tau \in G$,

wobei $G = \mathrm{Gal}(LM|M)$. Also liegt α im Fixkörper $(LM)^G$ von G. Laut Hauptsatz der Galoistheorie ist $(L \cdot M)^G = M \Rightarrow \alpha \in M$, insg. $\alpha \in L \cap M$. $\square$

Definition der Radikalerweiterungen

Definition (24.3)

Eine Radikalerweiterung ist eine endliche Körpererweiterung $L|K$ mit folgenden Eigenschaften: Es gibt ein $r \in \mathbb{N}_0$, eine Kette von Zwischenkörpern

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L \ ,$$

natürliche Zahlen $n_1, \ldots, n_r$ und für $1 \leq i \leq r$ Elemente $\gamma_i \in L_i$, so dass jeweils $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ erfüllt ist.

Beispiel. Das Element $\alpha = \sqrt[3]{\sqrt{2+\sqrt{5}} + \sqrt{7}} \in \mathbb{R}$ ist in einer Radikalerweiterung von $\mathbb{Q}$ enthalten.

Setze $L_0 = \mathbb{Q}$

Setze $\gamma_1 = \sqrt{5}$, $n_1 = 2$, $L_1 = L_0(\gamma_1)$

Setze $\gamma_2 = \sqrt{7}$, $n_2 = 2$, $L_2 = L_1(\gamma_2)$

Setze $\gamma_3 = \sqrt{2+\sqrt{5}}$, $n_3 = 2$, $L_3 = L_2(\gamma_3)$

Setze $\gamma_4 = \sqrt[3]{\gamma_3 + \gamma_2}$, $n_4 = 3$, $L_4 = L_3(\gamma_4)$

Dann zeigt die Kette

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq L_4,$$

dass $L_4 | \mathbb{Q}$ eine Radikalerweiterung mit $\alpha = \gamma_4 \in L_4$ ist.

Auflösbarkeit eines Polynoms durch Radikale

Definition (24.4)

Man sagt, ein nicht-konstantes Polynom $f \in K[x]$ ist durch Radikale auflösbar, wenn eine Radikalerweiterung $L|K$ existiert, so dass f über L in Linearfaktoren zerfällt.

Hinreichendes Kriterium für die Auflösbarkeit

Satz (24.5)

Sei $f \in K[x]$ ein nicht-konstantes Polynom mit auflösbarer Galoisgruppe $G = \mathrm{Gal}(f|K)$. Dann ist f durch Radikale auflösbar.

Beweis von Satz 24.5

geg: $f \in K[x]$, K Körper der Charakteristik 0

Vor: f hat eine auflösbare Galoisgruppe G

z.zg: f ist durch Radikale auflösbar

Sei L ein Zerfällungskörper von f über K, so dass $G = Gal(L|K)$ ist. G ist auflösbar $\Rightarrow$

$\exists$ Kette von Untergr. $G = U_0 \supseteq U_1 \supseteq \dots \supseteq U_r = \{id_L\}$

so dass $U_i \trianglelefteq U_{i-1}$ und U_{i-1}/U_i zyklisch für $1 \leq i \leq r$. Sei $n_i = (U_{i-1} : U_i)$ für $1 \leq i \leq r$.

Kette von Untergr. $G = U_0 \supseteq U_1 \supseteq \dots \supseteq U_r = \{id_L\}$
so dass $U_i \trianglelefteq U_{i-1}$ und U_{i-1}/U_i zyklisch für

Setze $L_i = L^{U_i}$ für $0 \le i \le r$. Galoistheorie $\Rightarrow$
$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = L$. Für $0 \le i \le r$ gilt
jeweils $U_i = \mathrm{Gal}(L|L_i)$, außerdem: $U_i = \mathrm{Gal}(L|L_i)$
ist Normalteiler von $U_{i-1} = \mathrm{Gal}(L|L_{i-1})$ Galoistheorie
$\Rightarrow L_i|L_{i-1}$ ist normale Teilerweiterung von $L|L_{i-1}$, und
$\mathrm{Gal}(L_i|L_{i-1}) \cong \mathrm{Gal}(L|L_{i-1})/\mathrm{Gal}(L|L_i) = U_{i-1}/U_i$ $(1 \le i \le r)$
Um das Ergebnis aus §23 anwenden zu können, definiere
$n = \mathrm{kgV}(n_1, \dots, n_r)$ und wähle in einem alg. Abschluss $\tilde{L}$ von L
eine primitive n-te Einheitswurzel ζ. Setze $K' = K(\zeta)$,
$L' = L(\zeta)$ und $L_i' = L_i(\zeta)$ für $0 \le i \le r$. Die Erweiterung
$L_i'|L_{i-1}'$ erfüllt dann die Voraussetzungen des Satzes aus §23,

denn: Sei $m_i = [L_i' : L_{i-1}']$. Es gilt $L_i' = L_i \cdot K' = L_i K(\zeta)$. Nach dem Vorschiebungssatz der Galoistheorie gilt $\mathrm{Gal}(L_i' | L_{i-1}') \cong \mathrm{Gal}(L_i | K' \cap L_i)$.
$\Rightarrow \mathrm{Gal}(L_i' | L_{i-1}')$ ist damit isomorph zu einer Untergp. der zyklischen Gruppe $\mathrm{Gal}(L_i | L_{i-1})$ und somit ebenfalls zyklisch, und $m_i | n_i$. Da L_{i-1} eine primitive n-te Einheitswurzel ζ enthält, enthält sie mit ζ^{n/m_i} auch eine prim. m_i-te Einheitswurzel.

§23 ⟹ $\exists \gamma_i \in L_i'$ mit $L_i' = L_{i-1}'(\gamma_i)$ und $\gamma_i^{m_i} \in L_{i-1}'$. Die Körperkette

$$K \subseteq K' = K(\beta) = L_0' \subseteq L_1' \subseteq \ldots \subseteq L_r' = L'$$

zeigt, dass $L'|K$ eine Radikalerweiterung ist. Weil f über L in Linearfaktoren zerfällt, zerfällt f erst recht über L'. $\Rightarrow$ f ist durch Radikale auflösbar. □

Das Kompositum normaler Erweiterungen

Lemma (24.6)

Seien $L_1|K$ und $L_2|K$ zwei normale Erweiterungen desselben Körpers K.

- Dann ist auch die Erweiterung $L_1 \cap L_2|K$ normal.
- Sind L_1 und L_2 in einem gemeinsamen Erweiterungskörper M enthalten, dann ist auch $L_1 \cdot L_2|K$ eine normale Erweiterung, wobei $L_1 \cdot L_2$ das Kompositum von L_1 und L_2 in M bezeichnet.

Eigenschaften von Radikalerweiterungen

Proposition (24.7)

(i) Sei $L|K$ eine Radikalerweiterung, $\tilde{K}$ ein algebraischer Abschluss von K und $\sigma : L \to \tilde{K}$ ein K-Homomorphismus. Dann ist auch $\sigma(L)|K$ eine Radikalerweiterung.

(ii) Ein Kompositum zweier Radikalerweiterungen ist eine Radikalerweiterung.

(iii) Ist $L|K$ eine separable Radikalerweiterung, so gibt es einen Erweiterungskörper M von L mit der Eigenschaft, dass $M|K$ eine Galois-Erweiterung und zugleich eine Radikalerweiterung ist.

Beweis von Kap. 24.7

zu i) geg.: Radikalerw. $L|K$, $\tilde{K} \supseteq L$ alg. abg. Erweiterungskörper, $\sigma \in \mathrm{Hom}_K(L, \tilde{K})$

z.zg.: $\sigma(L)|K$ ist Radikalerw.

$L|K$ Radikalerw. $\Rightarrow$ $\exists$ Kette von Zwischenkörp.

$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_{r-1} \subseteq L_r = L$ und

$n_1, \ldots, n_r \in \mathbb{N}$, $\gamma_i \in L_i$ mit $L_i = L_{i-1}(\gamma_i)$,

$\gamma_i^{n_i} \in L_{i-1}$ für $1 \leq i \leq r$ Wende σ auf die Kette an, erhalte

$\sigma(K) = K \subseteq \sigma(L_1) \subseteq \ldots \subseteq \sigma(L_{r-1}) \subseteq$

$\sigma(L_r) = \sigma(L)$ für $1 \leq i \leq r$ gilt jeweils
$\sigma(\gamma_i)^{n_i} = \sigma(\gamma_i^{n_i}) \in \sigma(L_{i-1})$ und
$\sigma(L_{i-1})(\sigma(\gamma_i)) = \sigma(L_{i-1}(\gamma_i)) = \sigma(L_i)$
Dies zeigt, dass $\sigma(L)|K$ eine Radikalerw. ist.

zu (ii) Seien $L|K$, $M|K$ Radikalerw., wobei L und M Teilkörper eines Körpers $\tilde{K}$ sind
z.Zg.: $L \cdot M | K$ ist Radikalerw.

Vor. $\Rightarrow$ ∃ Körperketten $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$
und $K = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_s = M$, $m_1, \ldots, m_r$,
$n_1, \ldots, n_s \in \mathbb{N}$, $\gamma_i \in L_i$, $\delta_j \in M_j$ mit
$\gamma_i^{m_i} \in L_{i-1}$, $L_i = L_{i-1}(\gamma_i)$ für $1 \leq i \leq r$ und
$\delta_j^{n_j} \in M_{j-1}$, $M_j = M_{j-1}(\delta_j)$ für $1 \leq j \leq s$

$\Rightarrow$ erhalte eine neue Körperkette

$L = M_0' \subseteq M_1' \subseteq \dots \subseteq M_s' = L \cdot M$ durch

$M_j' = L \cdot M_j$ für $0 \leq j \leq s$. leicht zu überprüfen:

$M_j' = M_{j-1}'(\delta_j)$, $\delta_j^{n_j} \in M_{j-1}'$ für $1 \leq j \leq s$

zu (iii) Sei $L|K$ eine sep. Radikalerw. zzg. 7 Radikalerweiterung $M|K$ mit $M \supseteq L$, die außerdem galois'sch ist

$L|K$ endl. sep. Erw. $\xrightarrow[\text{Element}]{\text{Satz vom prim.}}$ $\exists x \in L$ mit $L = K(x)$

Sei $f = \mathrm{Mx}_{\cdot K}$ und M ein Zerfällungskörper von f über K mit $M \supseteq L$. Dann ist $M|K$ eine Galois-Erw.

Element

Sei $f = M_{\alpha, K}$ und M ein Zerfällungskörper von f über K.

Seien $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ die Nullstellen von f in M.

$\Rightarrow M = K(\alpha_1, \dots, \alpha_n)$, nach Def des Zerfällungskörpers.

Fortsetzungssatz $\rightarrow \exists \sigma_i \in \mathrm{Hom}_K(K(\alpha), M)$ mit $\sigma_i(\alpha) = \alpha_i$.

Dieser liefert einen Isom. zwischen $K(\alpha)$ und $K(\alpha_i) \mid K$, d.h.

$K(\alpha_i) = \sigma_i(K(\alpha))$ $\quad L = K(\alpha) \Rightarrow K(\alpha) \mid K$ ist Radikalerw.

$\overset{ii)}{\Longrightarrow} K(\alpha_i) \mid K$ ist Radikalerw.

Leicht zu sehen: $M = K(\alpha_1, \dots, \alpha_r)$ ist Kompositum von $K(\alpha_1), \dots, K(\alpha_r)$ $\overset{iii)}{\Longrightarrow}$ $M \mid K$ ist Radikalerw. $\square$