Blick auf den Berchtesgadener Hochthron



Seitenansicht des Barmstein-Südgrats



Gratturm der Südgrat-Normalroute und Gipfel



Einstiegswand der Normalroute



Letzter Abschnitt der Route vor dem Gipfel



Die Galoisgruppe der reinen Gleichung

Satz (22.6)

Sei $n \in \mathbb{N}$ mit $n \geq 2$ und K ein Körper mit $\mathrm{char}(K) \nmid n$, was $\mathrm{char}(K) = 0$ einschließt. Wir setzen voraus, dass K eine primitive n-te Einheitswurzel ζ enthält. Weiter sei $a \in K^\times$, L ein Erweiterungskörper von K und $\alpha \in L$ eine n-te Wurzel von a.

(i) Die Erweiterung $K(\alpha)|K$ ist eine Galois-Erweiterung.

(ii) Sei G die Galoisgruppe von $K(\alpha)|K$. Dann gibt es einen Teiler d von n mit der Eigenschaft, dass G isomorph zu $\mathbb{Z}/d\mathbb{Z}$ ist.

(iii) Es gilt $G \cong \mathbb{Z}/n\mathbb{Z}$ genau dann, wenn das Polynom $f = x^n - a$ in $K[x]$ irreduzibel ist.

Zyklische Galois-Erweiterungen und Wurzeln

Satz (22.9)

Sei $n \in \mathbb{N}$, K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält, und $L|K$ eine Galois-Erweiterung vom Grad n mit zyklischer Galoisgruppe G. Dann gibt es ein Element $\vartheta \in L$ mit $L = K(\vartheta)$ und $\vartheta^n \in K$.

Der Verschiebungssatz der Galoistheorie

Satz (23.2)

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 23.2 (Forts.)

geg. endl. Gal.-Erw. $L|K$, bel. Erw. $M|K$

bereits gezeigt: $LM|M$, $L|L\cap M$ sind Galois-Erw.

noch z.zg.: Die Abb. $\phi: Gal(LM|M) \to Gal(L|L\cap M)$, $\tau \mapsto \tau|_L$ ist ein Isom. von Gruppen.

zu überprüfen (i) $\tau|_L \in Gal(L|L\cap M)$ $\forall \tau \in G$, wobei $G = Gal(LM|M)$

(ii) ϕ ist Gruppenhom

(iii) ϕ ist injektiv (iv) ϕ ist surjektiv

zu (i) Nach Def. ist $\tau|_L$ ein Körperhom. $L \to \bar{K}$.

(O.B.d.A. können wir annehmen, dass $\bar{K}$ alg. abg. ist.)

$L|K$ ist normal $\Rightarrow \tau|_L \in \mathrm{Aut}_K(L)$

noch zu überprüfen: $(\tau|_L)(\alpha) = \alpha \quad \forall \alpha \in L \cap M$

Wegen $\tau \in G$ gilt $\tau(\alpha) = \alpha \quad \forall \alpha \in M$. Daraus folgt direkt $(\tau|_L)(\alpha) = \alpha \quad \forall \alpha \in L \cap M$

zu (ii) klar, da $(\sigma \circ \tau)|_L = \sigma|_L \circ \tau|_L$ für alle $\sigma, \tau \in G$

zu (iii) Sei $\tau \in \ker(\phi)$ z.zg.: $\tau = \mathrm{id}_{LM}$

$\tau \in \ker(\phi) \Rightarrow \phi(\tau) = \mathrm{id}_L \Rightarrow \tau|_L = \mathrm{id}_L \Rightarrow \tau(\alpha) = \alpha \quad \forall \alpha \in L$

$\tau \in G, G = \mathrm{Gal}(LM|M) \Rightarrow \tau(\alpha) = \alpha \quad \forall \alpha \in M$

Wegen $L \cdot M = L(M)$ folgt daraus $\tau = \mathrm{id}_M$

zu (iv) z.zg.: $\phi(G) = \mathrm{Gal}(L|L \cap M)$ Nach dem Hauptsatz der Galoistheorie genügt es z.zg., dass $L^{\phi(G)} = L \cap M$

Die Inklusion „⊇" ist offensichtlich, da $L^{\phi(G)}$ nach dem Hauptsatz der Galoistheorie ein Zwischenkörper von $L|L\cap M$ ist.

„⊆" Sei $\alpha \in L^{\phi(G)} \Rightarrow \alpha \in L$ und

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

$\forall \tau \in G \Rightarrow \tau(\alpha) = \alpha \quad \forall \tau \in G \rightarrow$

$\alpha \in (L M)^{\mathrm{Gal}(LM|M)} \Rightarrow \alpha \in M$

insgesamt: $\alpha \in L \cap M$ □

Definition der Radikalerweiterungen

Definition (23.3)

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 für eine Radikalerweiterung

$\mathbb{Q}(\alpha)|\mathbb{Q}$ mit $\alpha = \sqrt[3]{\sqrt{2+\sqrt{5}} + \sqrt{7}}$

Setze $\alpha_1 = \sqrt{5}$, $\alpha_2 = \sqrt{7}$, $\alpha_3 = \sqrt{2+\sqrt{5}}$,
$\alpha_4 = \sqrt[3]{\sqrt{2+\sqrt{5}} + \sqrt{7}}$

und $K_0 = \mathbb{Q}$, $K_1 = K_0(\alpha_1)$, $K_2 = K_1(\alpha_2)$,
$K_3 = K_2(\alpha_3)$, $K_4 = K_3(\alpha_4)$. Dann ist
$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq K_4 = \mathbb{Q}(\alpha)$
eine Körperkette wie in Def. 23.3 angegeben, und folglich ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine Radikalerweiterung.

Auflösbarkeit eines Polynoms durch Radikale

Definition (23.4)

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 (23.5)

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 23.5.

geg: K Körper, $\mathrm{char}(K) = 0$, $f \in K[x]$
mit auflösbarer Galoisgruppe $G = \mathrm{Gal}(f|K)$
Sei L ein Zerf.körp. von f über K $\rightarrow$ o.Bd.A.
$G = \mathrm{Gal}(L|K)$ z.zg: $\mathrm{Gal}(f|K)$ ist eine Radikalerweiterung
$\mathrm{Gal}(L|K)$ auflösbar $\rightarrow \exists$ Kette von Untergruppen
$G = \mathrm{Gal}(L|K) = U_0 \supseteq U_1 \supseteq \dots \supseteq U_r = \{\mathrm{id}_L\}$
wobei $U_i \trianglelefteq U_{i-1}$ für $1 \leq i \leq r$, U_{i-1}/U_i zyklisch von Ordnung n_i. Der Hauptsatz der Galoistheorie liefert eine Folge $K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = L$

von Zwischenkörpern von $L|K$, wobei jeweils $U_i = \mathrm{Gal}(L|L_i)$ für $0 \leq i \leq r$. Dabei gilt jeweils $\mathrm{Gal}(L_i|L_{i-1}) \cong \mathrm{Gal}(L|L_{i-1}) / \mathrm{Gal}(L|L_i) = U_{i-1}/U_i$, denn wegen $U_i \leq U_{i-1}$ ist $L_i|L_{i-1}$ jeweils galoissch.

Sei $n = \mathrm{kgV}(n_1, \dots, n_r)$ und ζ eine primitive n-te Einheitswurzel in einem alg. Abschluss von L (existiert, da $\mathrm{char}(L) = \mathrm{char}(K) = 0$). Setze $L_i' = L_i(\zeta)$ für $0 \leq i \leq r$, $L' = L(\zeta)$ und $K' = K(\zeta)$. Dann enthält L_{i-1}' für $1 \leq i \leq r$ jeweils eine primitive n_i-te Einheitswurzel. Außerdem ist $\mathrm{Gal}(L_i'|L_{i-1}')$ ist zyklisch, denn auf Grund des Verschiebungssatzes der Galoistheorie gilt $\mathrm{Gal}(L_i'|L_{i-1}') \cong \mathrm{Gal}(L_i|L_{i-1} \cap K')$, und als Untergr. der zyklischen Gruppe $\mathrm{Gal}(L_i|L_{i-1})$ ist auch $\mathrm{Gal}(L_i|L_{i-1} \cap K)$ zyklisch (mit einer Ordn., die n_i teilt).

($L_i' = L_i(\zeta) = L_i \cdot K'$)

Satz 22.9 $\Rightarrow$ Für $1 \le i \le r$ existiert jeweils ein $\gamma_i \in L_i'$ und ein $m_i | n_i$ mit $\gamma_i^{m_i} \in L_{i-1}'$ und $L_i' = L_{i-1}'(\gamma_i)$.

$\Rightarrow L'|K'$ ist eine Radikalerw., ebenso $K'|K$ (da $K' = K(\zeta)$ mit $\zeta^n = 1$) Damit ist gezeigt, dass $L'|K$ eine Radikalerweiterung ist. Der Zerf.-körp. L von f über K ist also in einer Radikalerw. enthalten, und damit ist f durch Radikale auflösbar. $\square$

Das Kompositum normaler Erweiterungen

Lemma (23.6)

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.

Beweis von Prop. 23.6

geg. zwei normale Erweiterungen $M_1 | K$, $M_2 | K$

Sei $\tilde{K}$ ein alg. abg. gemeinsamer Erw.-körp. von M_1 und M_2

zu zeigen: (1) $M_1 \cap M_2 | K$ (2) $M_1 \cdot M_2 | K$

zu (1) Es genügt z.zg.: $\mathrm{Hom}_K(M_1 \cap M_2, \tilde{K}) = \mathrm{Aut}_K(M_1 \cap M_2)$

„$\supseteq$" ist offensichtlich „$\subseteq$" Sei $\phi \in \mathrm{Hom}_K(M_1 \cap M_2, \tilde{K})$.

zu überprüfen: $\phi(M_1 \cap M_2) \subseteq M_1 \cap M_2$ Sei $\alpha \in M_1 \cap M_2$.

z.zg. $\phi(\alpha) \in M_1 \cap M_2$ $M_1 | M_1 \cap M_2$ ist alg. Erw., $\tilde{K}$ alg. abg.

$\Rightarrow$ $\exists$ Forts. $\phi_1 : M_1 \to \tilde{K}$ von ϕ $M_1 | K$ ist normal

$\Rightarrow$ $\phi_1 \in \mathrm{Aut}_K(M_1)$ $\Rightarrow$ $\phi(\alpha) = \phi_1(\alpha) \in M_1$

Der Nachweis von $\phi(K) \in M_2$ läuft analog.

zu (2) zzg: $\mathrm{Hom}_K(M_1 \cdot M_2, \hat{K}) = \mathrm{Aut}_K(M_1 \cdot M_2)$.

„$\supseteq$" ist offensichtlich „$\subseteq$" Sei $\phi \in \mathrm{Hom}_K(M_1 \cdot M_2, \hat{K})$.

zzg: $\phi(M_1 \cdot M_2) \subseteq M_1 \cdot M_2$. $\phi|_{M_1} \in \mathrm{Hom}_K(M_1, \hat{K})$

(da $M_1|K$ normal) $\Rightarrow \phi(M_1) \subseteq M_1$, ebenso $\phi(M_2) \subseteq M_2$

$\Rightarrow M_1 M_2$ enthält $\phi(M_1) \cup \phi(M_2)$, damit auch $\phi(M_1 \cdot M_2)$. □

Hinweis:

Das aus $M_1M_2 \supset \phi(M_1) \cup \phi(M_2)$ die Inklusion $M_1M_2 \supseteq \phi(M_1M_2)$ folgt, hätte genauer ausgeführt werden müssen. Aus der Voraussetzung erhält man zunächst, dass $M_1 \cup M_2 \subseteq \phi^{-1}(M_1M_2)$ gilt. Weil die Urbildmenge eines Teilkörpers unter einem Körperhomomorphismus wiederum ein Teilkörper ist, folgt daraus, dass der Teilkörper $M_1M_2 = M_1(M_2)$ in $\phi^{-1}(M_1M_2)$ enthalten ist, und damit wiederum ist $\phi(M_1M_2) \subseteq M_1M_2$.

Die Aussage bezüglich Urbildern unter Körperhomomorphismen wurde in der Vorlesung bereits einmal verwendet, nämlich im Beweis von Lemma 16.6. Man sollte diese Aussage als eigenständiges Lemma formulieren, das wiederholt angewendet werden kann. Ich habe das Skript entsprechend geändert.

Eigenschaften von Radikalerweiterungen

Proposition (23.7)

(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 Proposition 23.7:

zu (i) geg. Radikalerw. $L|K$, $\hat{K}$ alg. Abschluss von K, $\sigma: L \to \hat{K}$ K-Hom.

Beh.: $\sigma(L)|K$ ist eine Radikalerw.

$L|K$ Radikalerw. $\Rightarrow$ Es gibt eine Kette von Zwischenkörpern $K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = L$ und $n_i \in \mathbb{N}$, $\gamma_i \in L_i$ mit $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ für $1 \leq i \leq r$. Anwendung von σ liefert $K = \sigma(K) = \sigma(L_0) \subseteq \sigma(L_1) \subseteq \dots \subseteq \sigma(L_r) = \sigma(L)$, außerdem $\sigma(L_i) = \sigma(L_{i-1}(\gamma_i)) = \sigma(L_{i-1})(\sigma(\gamma_i))$ und $\sigma(\gamma_i)^{n_i} = \sigma(\gamma_i^{n_i}) \in \sigma(L_{i-1}) \Rightarrow \sigma(L)|L$ ist Radikalerw.

zu (ii) Sei $\tilde{K}$ ein gem. alg. abg. Erw. von L und M, wobei $M|K$ und $L|K$ Radikalerw., $L \cdot M$ das Kompositum von L und M in $\tilde{K}$. z.zg.: $LM|K$ ist Radikalerw.

$L|K$ Radikalerw. $\Rightarrow \exists$ Zwischenkörper $K = L_0 \subseteq \dots \subseteq L_r = L$, $K = M_0 \subseteq \dots \subseteq M_s = M$ $(r, s \in \mathbb{N})$ und $\gamma_i \in L_i$, $\delta_j \in M_j$, $m_i, n_j \in \mathbb{N}$ mit $L_i = L_{i-1}(\gamma_i)$, $M_j = M_{j-1}(\delta_j)$, $\gamma_i^{m_i} \in L_{i-1}$, $\delta_j^{n_j} \in M_{j-1}$ für $1 \le i \le r$, $1 \le j \le s$.

Setze $M_j' = L \cdot M_j$ für $0 \le j \le s$. $\Rightarrow M_0' = L$, $M_s' = L \cdot M_s = L \cdot M \Rightarrow K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = L = M_0' \subseteq \dots \subseteq M_s' = M$

Aus $M_j = M_{j-1}(\delta_j)$ folgt jedoch $M_j' = M_{j-1}'(\delta_j)$, und $\delta_j^{n_j} \in M_{j-1} \subseteq M_{j-1}'$.

Also zeigt die Kette der Länge $r+s$, dass $L \cdot M / K$ eine Radikalerweiterung ist.

zu (iii) geg.: separable Radikalerw. L/K zz: Es gibt eine endl. Galois-Erw. M/K mit $M \supseteq L$. leicht zu sehen. L/K ist endl. Erw. Satz vom prim. El. $\Rightarrow \exists \alpha \in L$ mit $L = K(\alpha)$

Sei $f = \mu_{\alpha, K}$ und $M \supseteq L$ ein Zerf.körp. von f über K, d.h. $M = K(\alpha_1, \dots, \alpha_r)$, wobei $\alpha = \alpha_1, \dots, \alpha_r$ die Nullst. von f in M sind.

Der Körper M ist Kompositum der Körper $M_j = K(\alpha_j)$ $(1 \le j \le r)$.

klar: M/K ist Galoiserw. f irred. $\Rightarrow \exists \sigma_j \in \mathrm{Gal}(M/K)$ mit $\sigma_j(\alpha) = \alpha_j$. Ter(ii) $\Rightarrow$ Mit L/K ist auch $\sigma_j(L)/K$ eine Radikalerw., und $\sigma_j(L) = \sigma_j(K(\alpha)) = K(\sigma_j(\alpha)) = K(\alpha_j) = M_j$. Mit M_j/K für $1 \le j \le r$ ist nach Teil auch M/K Radikalerw., da M Kompositum von $M_1, \dots, M_j$. $\square$

„Radikalerweiterung $\Rightarrow$ auflösbare Gruppe“

Proposition (23.8)

Ist $L|K$ eine galoissche Radikalerweiterung, dann ist $G = \mathrm{Gal}(L|K)$ eine auflösbare Gruppe.

Satz (23.9)

Sei $f \in K[x]$ ein nicht-konstantes, durch Radikale auflösbares Polynom. Dann ist $\mathrm{Gal}(f|K)$ eine auflösbare Gruppe.