Der Separabilitätsgrad einer Erweiterung

Satz (19.8)

Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann gilt

$$|\mathrm{Hom}_K(L, \tilde{K})| \leq [L : K]$$

mit Gleichheit genau dann, wenn die Erweiterung $L|K$ separabel ist.

Definition (19.9)

Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann nennt man

$$[L : K]_{\mathrm{sep}} \quad = \quad |\mathrm{Hom}_K(L, \tilde{K})|$$

den Separabilitätsgrad der Erweiterung $L|K$.

Beweis von Satz 19.8 (Rest)

zeige durch vollst. Induktion über n (etwas allgemeiner):

Ist $L|K$ eine Erweiterung vom Grad n, $\tilde{K} \supseteq L$ ein algebraisch abg. Erweiterungskörper und $\phi: K \to \tilde{K}$ ein Körperhom, dann gibt es höchstens n Fortsetzungen von ϕ auf L. Ist $L|K$ sep. dann gibt es genau n Fortsetzungen.

Ind.-Anf $n = 1$: Dann gilt $L = K$, und die Erweiterung ist separabel (weil jedes $\alpha \in K$ separabel über K). Außerdem gibt es nur eine Fortsetzung von ϕ, nämlich ϕ selbst.

Ind.-schritt: Sei $n > 1$, $L|K$ vom Grad n, $\tilde{K}$ wie oben, setze die Aussage für Werte $< n$ voraus. Sei $\alpha \in L \setminus K$ und

$m = [K(\alpha) : K]$. (Wegen $K(\alpha) \neq K$ gilt $m > 1$.) Seien $\alpha_1, \dots, \alpha_r$ die versch. Nullstellen von $f = \mu_{\alpha, K}$ im $\tilde{K}$. Dann existieren nach Folgerung 16.4 genau r Fortsetzungen $\psi_i : K(\alpha) \to \tilde{K}$ von ϕ jeweils geg. durch $\psi_i(\alpha) = \alpha_i$ für $1 \leq i \leq r$. Ist $L|K$ separabel, dann ist α separabel über K, f somit ein separables Polynom. In diesem Fall ist dann $r = m$.

Weiter gilt nach der Gradformel $[L:K(\alpha)] = \dfrac{[L:K]}{[K(\alpha):K]} < [L:K] = n$.
$\Rightarrow$ Ind.-V. anwendbar $\Rightarrow$ Für $1 \leq i \leq r$ gibt es jeweils höchstens s Fortsetzungen von ψ_i zu einem Hom. $L \to \tilde{K}$, wobei $s = [L:K(\alpha)]$. Insgesamt gibt es also höchstens rs Fortsetzungen von ϕ, und $rs \leq ms = [K(\alpha):K] \cdot [L:K(\alpha)] = [L:K] = n$

Ist nun $L|K$ separabel, dann auch die Teilerweiterung $L|K(\alpha)$ (nach Prop. 19.3). Lt. Ind.-V. gibt es in diesem Fall für jedes $\mathfrak{P}_i$ genau s Fortsetzungen, insgesamt also genau $rs = n$ Fortsetzungen von ϕ. □

Das Minimalpolynom über einem Zwischenkörper

Lemma (19.10)

Sei $L|K$ eine einfache algebraische Erweiterung, also $L = K(\alpha)$ für ein $\alpha \in L$. Sei M ein Zwischenkörper von $L|K$ und

$$f \quad = \quad \mu_{\alpha,M} \quad = \quad x^n + \sum_{i=0}^{n-1} a_i x^i \quad \in M[x]$$

das Min.-polynom von α über M. Dann gilt $M = K(a_0, ..., a_{n-1})$.

Beweis von Lemma 19.10:

geg: einfache alg. Erw. $L = K(\alpha)$

M Zwischenkörper von $L|K(\alpha)$

Sei $f = M_{\alpha, M} = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

und $M_0 = K(a_0, a_1, \ldots, a_{n-1})$. Beh: $M_0 = M$

Wegen $f \in M[x]$ gilt $a_0, \ldots, a_{n-1} \in M$ und somit $M_0 = K(a_0, \ldots, a_{n-1}) \subseteq M$

Beh: $f = M_{\alpha, M_0}$ Grund: $f \in M_0[x]$,

$f(\alpha) = 0_K$, und da f über M irreduzibel ist,

ist f auch in $M_0[x]$ irreduzibel.

außerdem: $L = K(\alpha) \Rightarrow L = M_0(\alpha) = M(\alpha)$

L
|
M
|
M_0
|
K

$\Rightarrow$
$=$
M
$\Rightarrow$
$[M:$

$\Rightarrow [L : M_0] = [M_0(\alpha) : M] = \text{grad}(f) = [M(\alpha) : M]$
$= [L : M]$

M ist Zwischenkörper von $L | M_0$, Gradformel

$\Rightarrow [L : M_0] = [L : M] \cdot [M : M_0] \Rightarrow$
$[L : M] = [L : M_0]$

$[M : M_0] = 1 \overset{M_0 \subseteq M}{\Rightarrow} M = M_0.$ □

Charakterisierung der einfachen Erweiterungen

Satz (19.11)

Eine endliche Erweiterung $L|K$ besitzt genau dann nur endlich viele Zwischenkörper, wenn sie einfach ist.

Folgerung (19.12)

Jede endliche, separable Erweiterung $L|K$ besitzt nur endlich viele Zwischenkörper.

Beweis von Satz 19.11.

geg: endliche Erweiterung $L|K$

Beh: $L|K$ ist einfach ($\exists\, \alpha \in L$ mit $L = K(\alpha)$) $\iff$ $L|K$ hat nur endlich viele Zwischenkörper

„$\Rightarrow$" Vor. $\Rightarrow \exists\, \alpha \in L$ mit $L = K(\alpha)$

Sei $f = \mu_{\alpha,K} \in K[x]$. Bereits früher haben wir festgestellt, dass für jeden Zwischenkörper M das Minimalpolynom $\mu_{\alpha,M}$ ein normierter Teiler in $M[x]$ ist. Nach Lemma 19.10 ist der Zwischenkörper M durch diesen Teiler ein -

deutig festgelegt: Ist $M_{\alpha,K} = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, dann $M = K(a_0, \dots, a_{n-1})$. Da f in $L[x]$ nur endlich viele normierte Teiler besitzt, gibt es auch nur endl. viele Zwischenkörper.

„$\Leftarrow$" Ist K endlich ist, dann ist jede endliche Erweiterung $L|K$ einfach (da $L^\times$ eine zykl. Gruppe ist; für jeden Erzeuger α von $L^\times$ gilt $L = K(\alpha)$). Weil L endlich ist, hat $L|K$ auch nur endlich viele Zwischenkörp. Die Implikation „$\Leftarrow$" gilt also, weil beide Teilaussagen wahr sind.

Setze nun voraus, dass K unendlich ist

Zeige durch vollst. Ind. über r: Ist $L|K$ eine Körpererw. mit nur

auch nur endlich viele Zwischenkörper. Die Implikation „⟸" gilt also, weil beide Teilaussagen wahr sind.

endl. vielen Zwischenkörpern und gilt $L = K(\alpha_1, \dots, \alpha_r)$ mit $\alpha_j \in L$ für $1 \le j \le r$, dann ist $L|K$ einfach. Daraus folgt die Aussage, weil jede endl. Erw. ein endliches Erz.-system (als Körpererw.) hat

Ind.-Anf. $r = 1$: nichts zu zeigen

Ind.-Schritt $r \mapsto r+1$: Vor. $\Rightarrow L = K(\alpha_1, \dots, \alpha_{r+1})$

Setze $L_0 = K(\alpha_1, \dots, \alpha_r)$. $L|K$ hat nur endl. viele Zw.-körper $\Rightarrow$ $L_0|K$ hat nur endl. viele Zw. $\overset{\text{Ind. Vor.}}{\Rightarrow}$ $\exists \alpha \in L_0$ mit $L_0 = K(\alpha)$

$\Rightarrow L = K(\alpha, \beta)$ mit $\beta = \alpha_{r+1}$. Betrachte die Elt. $\gamma_c = \alpha + c\beta$, mit $c \in K$. Da K unendlich ist, $L|K$ aber nur endl. viele Zwischenkörper hat, gibt es $c, d \in K$ mit $c \neq d$ mit $K(\gamma_c) = K(\gamma_d)$ Beh.: $K(\alpha, \beta) = K(\gamma_c)$

„⊇" klar „⊆" $\gamma_d, \gamma_c \in K(\gamma_c) \Rightarrow \gamma_d - \gamma_c = (d-c)\beta \in K(\gamma_c) \overset{d-c \in K^\times}{\Rightarrow}$

$\beta \in K(\gamma_c) \Rightarrow \gamma_c - c\beta = \alpha \in K(\gamma_c)$ insg.: $\{\alpha, \beta\} \subseteq K(\gamma_c)$

also $K(\alpha, \beta) \subseteq K(\gamma_c)$. □

§ 20. Kreisteilungspolynome

Definition (20.1)

Sei $n \in \mathbb{N}$. Eine *n*-te Einheitswurzel in $\mathbb{C}$ ist ein Element $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$. Mit μ_n bezeichnen wir die Menge aller n-ten Einheitswurzeln. Es handelt sich um eine Untergruppe von $\mathbb{C}^\times$.

Lemma (20.2)

Sei $k \in \mathbb{Z}$. Genau dann gilt $\mu_n = \langle \zeta_n^k \rangle$, wenn $\mathrm{ggT}(k, n) = 1$ ist.

Ergänzung: Sei $n \in \mathbb{N}$

$$\mu_n = \{ \zeta \in \mathbb{C}^\times \mid \zeta^n = 1 \}$$

Die Elemente von μ_n sind genau die komplexen Nullstellen des Polynoms $X^n - 1$. Da das Polynom $f_n = x^n - 1$ teilerfremd zu seiner Ableitung ist ($ggT(f_n, f_n') = ggT(x^n - 1, n \cdot x^{n-1}) = 1$), besitzt f_n in $\mathbb{C}^\times$ genau n (verschiedene) Nullstellen.

Diese sind gegeben durch ζ_n^k, $0 \le k < n$ mit $\zeta_n = e^{2\pi i/n}$

($\zeta_n^n = (e^{2\pi i/n})^n = e^{2\pi i} = 1 \Rightarrow \zeta_n \in \mu_n$, somit auch $\zeta_n^k \in \mu_n$ auf Grund der Gruppeneigenschaft)

Die Zahl $n \in \mathbb{N}$ minimal mit $\zeta_n^n = 1 \Rightarrow \operatorname{ord}(\zeta_n) = n$

Korrektur: Beweis von Lemma 20.2

$\zeta_n \in \mu_n$ auf gewisse Gruppenaxiome

Die Zahl $n \in \mathbb{N}$ minimal mit $\zeta_n^n = 1 \Rightarrow \operatorname{ord}(\zeta_n) = n$

Daraus folgt, dass $\mu_n = \langle \zeta_n \rangle$ gilt.

Beweis von Lemma 19.2:

Aus der Gruppentheorie ist bekannt: Ist G eine Gruppe, $n \in \mathbb{N}$, $g \in G$ mit $n = \operatorname{ord}(g)$, dann gilt für alle $k \in \mathbb{Z}$ die Äquivalenz

$\operatorname{ord}(g^k) = n \iff \operatorname{ggT}(k, n) = 1$.

Wende dies an auf $G = \mathbb{C}^\times$, $g = \zeta_n$. Wir erhalten

$\langle \zeta_n^k \rangle = \mu_n \iff \operatorname{ord}(\zeta_n^k) = n \iff \operatorname{ggT}(k, n) = 1$

□

Definition der Kreisteilungspolynome

Definition (20.3)

Sei $n \in \mathbb{N}$, $n \geq 2$.

- Eine primitive n-te Einheitswurzel ist ein Element $\zeta \in \mu_n$ mit $\mu_n = \langle \zeta \rangle$.
- Wir bezeichnen mit $\mu_n^\times \subseteq \mu_n$ die Menge der primitiven n-ten Einheitswurzeln.
- Das Polynom $\Phi_n \in \mathbb{C}[x]$ gegeben durch

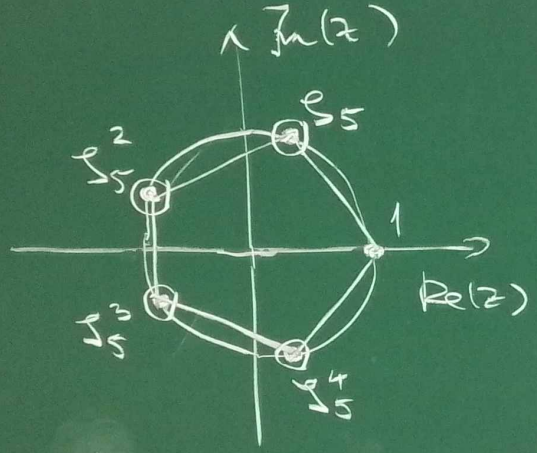
$$\Phi_n \quad = \quad \prod_{\zeta \in \mu_n^\times} (x - \zeta)$$

wird das n-te Kreisteilungspolynom genannt.

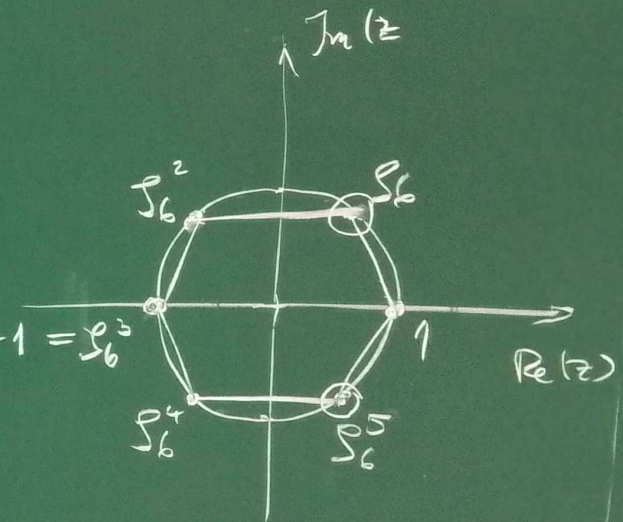
Beispiel: n-te Einheitswurzeln und primitive n-te Einheitswurzeln für

$n = 5, 6$

$\underline{n=5}$



$\varphi(5) = 4$



$\varphi(6) = 2$

Die Ganzzahligkeit der Kreisteilungspolynome

- Aus technischen Gründen setzen wir $\Phi_1 = x - 1$, obwohl wir für $n = 1$ keine primitiven n-ten Einheitswurzeln definiert haben.
- Für alle $n \in \mathbb{N}$ ist $\varphi(n) = \operatorname{grad} \Phi_n$.

Lemma (20.4)

Für alle $n \in \mathbb{N}$ gilt $x^n - 1 = \prod_{d|n} \Phi_d$, wobei d die natürlichen Teiler von n durchläuft.

Beweis von Lemma 20.4:

Sei $n \in \mathbb{N}$. Beh.: $x^n - 1 = \prod_{d \mid n} \Phi_d$

S.O. $\Rightarrow$ $x^n - 1$ hat in $\mathbb{C}$ keine mehrfachen Nullstellen. Dasselbe gilt für das Polynom auf der rechten Seite, denn: Nach Def. hat jeder Faktor Φ_d nur einfache Nullstellen. Außerdem können verschiedene Faktoren keine gem. Nullstelle haben, denn alle Nullst. von Φ_d sind jeweils Elemente der Ordnung d in $\mathbb{C}^\times$

Es genügt also z.zg., dass die Nullstellenmengen auf beiden Seiten gleich sind. Die Nullstellen links sind genau die Elemente mit $\zeta^n = 1$, also genau die Elemente $\zeta \in \mathbb{C}^\times$ mit $\mathrm{ord}(\zeta) = d$ für ein Teiler d von n. Ebenso ist $\zeta \in \mathbb{C}$ genau eine Nullstelle des Polynoms rechts, wenn $\zeta \in \mathbb{C}^\times$ gilt und $\mathrm{ord}(\zeta) = d$ für einen Teiler d von n gilt. □