Definition der Galois-Erweiterungen

Definition (19.13)

Eine Körpererweiterung $L|K$ wird Galois-Erweiterung genannt, wenn sie normal und separabel ist. Die Gruppe

$$\mathrm{Gal}(L|K) \quad = \quad \mathrm{Aut}_K(L)$$

wird dann die Galoisgruppe der Erweiterung $L|K$ genannt.

Ist M ein Zwischenkörper einer galois'schen Erweiterung $L|K$, dann ist auch $L|M$ galois'sch.

Charakterisierung der Galois-Erweiterungen

Satz (19.14)

Eine endliche Körpererweiterung $L|K$ ist genau dann galois'sch, wenn

$$[L : K] \quad = \quad |\mathrm{Aut}_K(L)|$$

gilt. Insbesondere ist für jede endliche Galois-Erweiterung $L|K$ also die Gleichung $|\mathrm{Gal}(L|K)| = [L : K]$ erfüllt.

Der Fortsetzungssatz für Galoisgruppen

Folgerung (19.15)

Sei $L|K$ eine Galois-Erweiterung, $f \in K[x]$ ein irreduzibles Polynom, und seien α, β zwei Nullstellen von f in L. Dann existiert ein Element $\sigma \in \mathrm{Gal}(L|K)$ mit $\sigma(\alpha) = \beta$.

Beweis von Folgerung 19.15:

geg.: endliche Galois-Erw. $L|K$, $G = Gal(L|K) = Aut_K(L)$

$f \in K[x]$ irreduzibel, $\alpha, \beta \in L$ Nullstellen von f

z.zg.: $\exists \sigma \in G$ mit $\sigma(\alpha) = \beta$

Sei $\tilde{K}$ ein alg. abgeschlossener Erweiterungskörper von L

α, β Nullst. von f $\Rightarrow$ Fortsetzungssatz 16.2 kann angewendet werden auf den Körperisom. $id_K : K \to K$

$\Rightarrow$ erhalte eine Fortsetzung $\tilde{\sigma} : K(\alpha) \to \tilde{K}$ von id_K mit $\tilde{\sigma}(\alpha) = \beta$ Da $\tilde{K}$ alg. abgeschlossen ist, existiert eine Fortsetzung von $\tilde{\sigma}$ zu einem Hom. $\sigma : L \to \tilde{K}$.

halte die Fortsetzung $\sigma : K(\alpha) \to \tilde{K}$ von id_K
mit $\sigma(\alpha) = \beta$. Da $\tilde{K}$ alg. abgeschlossen ist, existiert

Als Forts. von id_K ist dies ein K-Hom., d.h. $\sigma \in \mathrm{Hom}_K(L, \tilde{K})$.
Da $L|K$ normal ist, gilt $\mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L) = G$.
$\Rightarrow \sigma \in G$, und $\sigma|_{K(\alpha)} = \tilde{\sigma} \Rightarrow \sigma(\alpha) = \tilde{\sigma}(\alpha) = \beta$. $\square$

Beispiel für eine Galoisgruppe

Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Beh.: $L|K$ ist eine Galois-Erw., also normal und separabel

Zeige zunächst: L ist Zerf.-körper von $f = (x^2-2)(x^2-3)$ über K

Es gilt $f = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$, d.h. f zerfällt über L in Linearfaktoren.

Außerdem wird L über K durch die Nullstellen von f erzeugt, da das Erzeugenden-

System $\{\sqrt{2}, \sqrt{3}\}$ eine Teilmenge der Nullstellenmenge ist. Als Zerf.-körper eines Polynoms $f \in K[x]$ über K ist L normal über K.

Als normale Erweiterung ist $L|K$ auch algebraisch und wegen $\mathrm{char}(K) = 0$ damit auch separabel, insgesamt also galoisch.

Bestimmung der Galoisgruppe $G = \mathrm{Gal}(L|K)$:

Zunächst bestimmen wir den Erw.-grad $[L:K]$. $2 \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei $\Rightarrow$ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ Beh: $x^2 - 3 = M_{\sqrt{3}, \mathbb{Q}(\sqrt{2})}$

Das Pol. $g = x^2 - 3$ ist normiert, und $g(\sqrt{3}) = 0$.

Ang. g ist in $\mathbb{Q}(\sqrt{2})[x]$ reduzibel. Wegen

grad(g) = 2 müssten dann die Nullst. $\pm\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})$ liegen. Aber das ist lt. Vl. nicht der Fall, da 2 und 3 zwei verschiedene quadratfreie Zahlen in $\mathbb{Z}\setminus\{0,1\}$ sind. Also ist f über $\mathbb{Q}(\sqrt{2})$ irreduzibel (⇒ Beh.)

Es folgt $[L:\mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})] = \text{grad}(g) = 2$ und mit der Gradformel $[L:k] = [L:\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):k] = 2\cdot 2 = 4$. Da L|K galois'sch ist, folgt $|G| = [L:k] = 4$

Als Gruppe von Primzahlquadratordnung ist G abelsch.

Hauptsatz über endl. abelsche Gruppen ⇒ G ist isomorph zu einem Produkt zyklischer Gruppen ⇒ $G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Mit L|K ist auch die Erweiterung $L|\mathbb{Q}(\sqrt{2})$ galois'sch.

s.o. ⇒ $g = x^2 - 3$ ist irred. über $\mathbb{Q}(\sqrt{2})$, $\pm\sqrt{3}$ sind Nullstellen von g in L. Folgerung 19.15 ⇒ $\exists \tau \in \text{Gal}(L|\mathbb{Q}(\sqrt{2}))$ mit $\tau(\sqrt{3}) = -\sqrt{3}$

Wegen $\tau \in \mathrm{Gal}(L|\mathbb{Q}(\sqrt{2}))$ gilt $\tau(\sqrt{2}) = \sqrt{2}$.

Mit $L|K$ ist auch $L|\mathbb{Q}(\sqrt{3})$ galoisch.

Beh. $h = x^2 - 2$ ist irred. über $\mathbb{Q}(\sqrt{3})$ Ang. h ist reduzibel über $\mathbb{Q}(\sqrt{3})$ $\overset{\text{grad}(h)=2}{\Rightarrow}$ Die Nullst. $\sqrt{2}$ von h liegt in $\mathbb{Q}(\sqrt{3})$.

$\Rightarrow L = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{3}) \Rightarrow [L:K] = [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$

↯ zu $[L:K] = 4$ $\quad L\sqrt{2} \in \mathbb{Q}(\sqrt{3})$ $(\Rightarrow$ Beh.$)$

h irred. über $\mathbb{Q}(\sqrt{3})$, $\pm\sqrt{2}$ sind Nullst. von h in L

$\overset{\text{Folgerung 19.15}}{\Rightarrow}$ $\exists\, \sigma \in \mathrm{Gal}(L|\mathbb{Q}(\sqrt{3}))$ mit $\sigma(\sqrt{2}) = -\sqrt{2}$ und $\sigma(\sqrt{2}) = \sqrt{3}$. Mit $\sigma, \tau \in G$ liegt auch $\sigma \circ \tau$ in G.

$(\sigma \circ \tau)(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$, $(\sigma \circ \tau)(\sqrt{3}) = \sigma(-\sqrt{3})$

$= -\sigma(\sqrt{3}) = -\sqrt{3} \Rightarrow \sigma \circ \tau \notin \{\mathrm{id}_L, \sigma, \tau\}$

Wegen $|G| = 4$ ist somit $G = \{\mathrm{id}_L, \sigma, \tau, \sigma \circ \tau\}$

Es gilt $\sigma^2(\sqrt{2}) = \sigma(\sigma(\sqrt{2})) = \sigma(-\sqrt{2}) = -\sigma(\sqrt{2}) =$
$-(-\sqrt{2}) = \sqrt{2}$ und $\sigma^2(\sqrt{3}) = \sigma(\sigma(\sqrt{3})) = \sigma(\sqrt{3}) = \sqrt{3}$.
Da jedes Element von G durch die Bilder von $\sqrt{2}$ und $\sqrt{3}$
eindeutig bestimmt ist (wegen $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$), folgt
daraus $\sigma^2 = \mathrm{id}_L$. Aus $\sigma \neq \mathrm{id}_L$ und $\sigma^2 = \mathrm{id}_L$ folgt $\mathrm{ord}(\sigma) = 2$.
Genauso überprüft man $\mathrm{ord}(\tau) = 2$.
Im Fall $G \cong \mathbb{Z}/4\mathbb{Z}$ wäre G eine zyklische Gruppe der Ordnung 4
und würde als solche nur ein Element der Ordnung 2 enthalten.
Also muss $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gelten.

§ 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.

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.

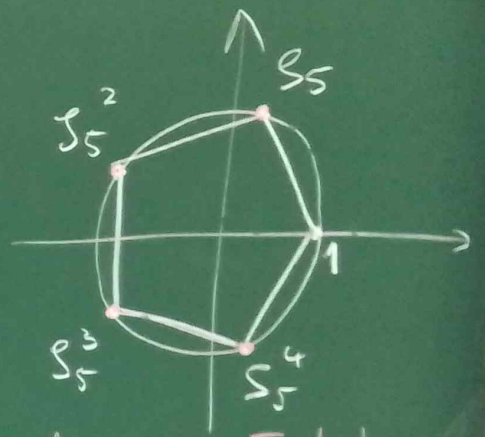
Notation: $\zeta_n = e^{2\pi i/n}$

Beispiele für Kreisteilungspolynome:

(i) $\Phi_5 = (x-\zeta_5)(x-\zeta_5^2)(x-\zeta_5^3)(x-\zeta_5^4)$

$= x^4 + x^3 + x^2 + x + 1$

↳ Begründung folgt

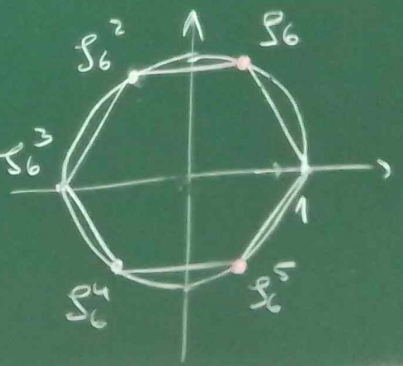


primitive 5-te Einheitswurzeln

(ii) $\Phi_6 = (x-\zeta_6)(x-\zeta_6^5) = x^2 - x + 1$

↳ s.u

primitive 6-te Einheitswurzeln



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.

Satz (20.5)

Es gilt $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$.

primitive

$-1 = \zeta_6^3$

Beweis von Lemma 20.4

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

Beide Polynome haben in $\mathbb{C}$ nur einfache Nullstellen, denn die Nullstellen von $x^n - 1$ sind die n Elemente von μ_n, jedes Φ_d hat nach Def. nur einfache Nullstellen, und da für jedes d die Nullstellen von Φ_d jeweils die Elt. der Ordnung d in $\mathbb{C}^\times$ sind, haben auch Φ_d und $\Phi_{d'}$ für zwei verschiedene Teiler d, d' von n keine gemeinsame Nullstelle.

Es genügt deshalb zu überprüfen, dass beide Polynome in der Gleichung (*) dieselbe Nullstellenmenge haben. Ist ζ eine Nullst. von $x^n - 1$, dann gilt $\zeta^n = 1 \Rightarrow \operatorname{ord}(\zeta) \mid n$ für $\zeta \in \mathbb{C}^\times \Rightarrow \exists d \in \mathbb{N}, d \mid n$ mit $\operatorname{ord}(\zeta) = d \rightarrow \zeta$ ist germ. d-te Einheitswurzel $\Rightarrow \Phi_d(\zeta) = 0$

Also ist ζ auch eine Nullstelle des Produkts rechts.

Ist umgekehrt ζ eine Nullstelle des Produkts, dann gilt $\Phi_d(\zeta) = 0$ für ein $d \in \mathbb{N}$ mit $d \mid n$.

$\Rightarrow \zeta$ ist primitive d-te Einheitswurzel $\Rightarrow \zeta^d = 1$

$d \mid n \Rightarrow \exists k \in \mathbb{N} : n = kd \Rightarrow \zeta^n = (\zeta^d)^k = 1^k = 1$

$\Rightarrow \zeta$ ist Nullstelle von $x^n - 1$ $\square$

z

(iii)

Anwendungen von Lemma 20.4.

(i) Ist p eine Primzahl, dann gilt

$$x^p - 1 = \Phi_p \Phi_1 = \Phi_p \cdot (x-1) \longrightarrow$$

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

(ii) Ist p eine Primzahl und $r \in \mathbb{N}$, dann gilt allgemeiner $x^{p^r} - 1 = \prod_{k=0}^{r} \Phi_{p^k} =$

$$\Phi_{p^r} \prod_{k=0}^{r-1} \Phi_{p^k} = \Phi_{p^r} \left(x^{p^{r-1}} - 1 \right) \longrightarrow$$

$$\Phi_{p^r} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \frac{\left(x^{p^{r-1}}\right)^p - 1}{x^{p^{r-1}} - 1} =$$

$$x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \dots + x^{p^{r-1}} + 1$$

z.B. $\Phi_9 = x^6 + x^3 + 1$

(iii) $x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6 \Rightarrow \Phi_6 = \dfrac{x^6 - 1}{\Phi_1 \Phi_2 \Phi_3}$

$= \dfrac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$