# 4 Galois-Theorie

## 4.1 Der Hauptsatz

### Definition + Proposition 4.1.1

Sei $L/K$ algebraische Körpererweiterung, $\bar{K}$ ein algebraischer Abschluss von $L$.

(a) $L/K$ heißt **normal**, wenn es eine Familie $\mathcal{F} \subset K[X]$ gibt, so dass $L$ Zerfällungskörper von $\mathcal{F}$ ist.

(b) Ist $L/K$ normal, so ist $\mathrm{Hom}_K(L, \bar{K}) = \mathrm{Aut}_K(L)$

**Beweis:** "$\supseteq$" gilt immer. "$\subseteq$": Sei $L = Z(\mathcal{F})$, $f \in \mathcal{F}$, $\alpha \in L$ Nullstelle von $f \Rightarrow$ Für $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ ist $\sigma(\alpha)$ auch Nullstelle von $f$. Sei $f(X) = \sum_{i=0}^{n} a_i X^i \Rightarrow$ $0 = \sigma(f(\alpha)) = \sum_{i=0}^{n} \underbrace{\sigma(a_i)}_{=a_i} \sigma(\alpha^i) = f(\sigma(\alpha)) \Rightarrow \sigma(\alpha) \in L \Rightarrow \sigma(L) \subseteq L$. $\sigma$ ist surjektiv, da $L$ von den Nullstellen der $f \in \mathcal{F}$ erzeugt wird und jedes $f \in \mathcal{F}$ endlich viele Nullstellen hat, die durch $\sigma$ permutiert werden. ■

(c) $L/K$ heißt **galoissch**, wenn $L/K$ normal und separabel ist.

(d) Ist $L/K$ galoissch, so heißt $\mathbf{Gal}(L/K) := \mathrm{Aut}_K(L)$ die **Galoisgruppe** von $L/K$.

(e) Eine endliche Erweiterung $L/K$ ist genau dann galoissch, wenn $|\mathrm{Aut}_K(L)| = [L : K]$

**Beweis:** "$\Rightarrow$" Aus (b) folgt

$$|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L, \bar{K})| = [L : K]_s \overset{3.4.5}{=} [L : K](*)$$

"$\Leftarrow$" In $(*)$ gilt stets $|\mathrm{Aut}_K(L)| \leq |\mathrm{Hom}_K(L, \bar{K})| = [L : K]_s \leq [L : K]$. Aus $|\mathrm{Aut}_K(L)| = [L : K]$ folgt also $[L : K]_s = [L : K] \Rightarrow L/K$ separabel $\overset{12}{\Rightarrow} L = K(\alpha)$ für ein $\alpha \in L$; Sei $f \in K[X]$ das Minimalpolynom von $\alpha$. Sei $\beta \in \bar{K}$ Nullstelle von $f$. Nach 3.3.1 gibt es $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ mit $\sigma(\alpha) = \beta$. Wegen $(*)$ ist $\sigma \in \mathrm{Aut}_K(L) \Rightarrow \beta \in L \Rightarrow L = \mathrm{Z}(f)$. ■

**Beispiel:** Sei $K$ Körper mit Charakteristik nicht 2, $d \in K^\times \setminus (K^\times)^2$. Dann ist $K(\sqrt{d})/K$ eine Galois-Erweiterung, denn $X^2 - d$ ist irreduzibel und separabel und zerfällt in $K(\sqrt{d})[X]$ in $(X - \sqrt{d})(X + \sqrt{d})$.

**Bemerkung 4.1.2** (a) Ist $L/K$ galoissch und $E$ ein Zwischenkörper, so ist $L/E$ galoissch und $\mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$.

**Beweis:** $L/E$ normal, da Zerfällungskörper von $\mathcal{F} \subset K[X] \subseteq E[X]$. $L/E$ separabel, da $L/K$ separabel und das Minimalpolynomm von $\alpha \in L$ über $E$ in $E[X]$ Teiler des Minimalpolynoms über $K$ ist. ■

(b) Ist in (a) zusätzlich auch $E/K$ galoissch, so ist

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K) \underset{\sigma \mapsto \sigma_{|E}}{\overset{\beta}{\to}} \mathrm{Gal}(E/K) \to 1$$

exakt.

**Beweis:** Für $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ ist $\sigma_{|E} : E \to L$, also $\sigma_{|E} \in \mathrm{Hom}_K(E, L) \subseteq \mathrm{Hom}_K(E, \bar{K}) = \mathrm{Aut}_K(E)$, da $E/K$ galoissch ist. $\Rightarrow \beta$ ist wohldefiniert.

$\beta$ **surjektiv**: Sei $\sigma \in \mathrm{Gal}(E/K)$. Nach 3.3.3 läßt sich $\sigma$ fortsetzen zu $\widetilde{\sigma} : L \to \bar{K}$, $\widetilde{\sigma} \in \mathrm{Hom}_K(L, \bar{K}) = \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$ und $\beta(\widetilde{\sigma}) = \widetilde{\sigma}_{|E} = \sigma$

$\mathrm{Kern}\,\beta = \{\sigma \in \mathrm{Gal}(L/K) : \sigma_{|E} = id_E\} = \mathrm{Aut}_E(L) = \mathrm{Gal}(L/E)$ ■

## Satz 15 (Hauptsatz der Galoistheorie)

Sei $L/K$ endliche Galois-Erweiterung.

(a) Die Zuordnungen

$$\begin{array}{ccc} \{\text{Zwischenkörper von } L/K\} & \overset{\Psi}{\longrightarrow} \\ & \underset{\Phi}{\longleftarrow} & \{\text{Untergruppen von } \mathrm{Gal}(L/K)\} \\ E & \longmapsto & \mathrm{Gal}(L/E) \\ L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in H\} & \longmapsfrom & H \end{array}$$

sind bijektiv und zueinander invers.

(b) Ein Zwischenkörper $E$ von $L/K$ ist genau dann galoissch über $K$, wenn $\mathrm{Gal}(L/E)$ Normalteiler in $\mathrm{Gal}(L/K)$ ist.

**Beweis:**

(a) $L^H$ ist Zwischenkörper: ✓

"$\Psi \circ \Phi = id$": Sei $H \subseteq \mathrm{Gal}(L/K)$ Untergruppe. z.z.: $\mathrm{Gal}(L/L^H) = H$

"$\supseteq$" Nach Def. von $L^H$ "$\subseteq$": Nach 4.1.1 ist $|\mathrm{Gal}(L/L^H)| = [L : L^H]$. Es genügt also z.z.: $[L : L^H] \leq |H|$. Sei $\alpha \in L$ primitives Element von $L/L^H$, also $L = L^H(\alpha)$. Sei $f := \prod_{\sigma \in H} (X - \sigma(\alpha)) \in L[X]$; dann ist $\deg(f) = |H|$. Für jedes $\tau \in H$ ist $f^\tau = f$ (mit $\sigma$ durchläuft auch $\sigma \circ \tau$ alle Elemente von $H$) $\Rightarrow f \in L^H[X] \Rightarrow$ Das Minimalpolynom $g$ von $\alpha$ über $L^H$ ist Teiler von $f$. $\Rightarrow [L : L^H] = \deg(g) \leq \deg(f) = |H|$

"$\Phi \circ \Psi = id$": Sei $E$ Zwischenkörper, $H := \mathrm{Gal}(L/E)$. zu zeigen: $E = L^H$.

"$\subseteq$": Definition. "$\supseteq$": Da $L^H/E$ separabel ist, genügt es zu zeigen $[L^H : E]_s = 1$. Sei also $\sigma \in \mathrm{Hom}_E(L^H, \bar{K})$, $\widetilde{\sigma} \in \mathrm{Hom}_E(L, \bar{K}) = \mathrm{Aut}_E(L) = \mathrm{Gal}(L/E) = H$ Fortsetzung $\Rightarrow \underset{=\sigma}{\widetilde{\sigma}_{|L^H}} = id_{L^H}$

(b) "$\Rightarrow$": 4.1.2 b), da $\mathrm{Gal}(L/E) = \mathrm{Kern}\,\beta$. "$\Leftarrow$": Sei $H := \mathrm{Gal}(L/E)$ Normalteiler in $\mathrm{Gal}(L/K)$. Wegen 4.1.1 c) genügt es zu zeigen: Für jedes $\sigma \in \mathrm{Hom}_K(E, \bar{K})$ ist $\sigma(E) \subseteq E$. Sei also $\sigma \in \mathrm{Hom}_K(E, \bar{K})$, $\widetilde{\sigma} \in \underset{=\mathrm{Gal}(L/K)}{\mathrm{Hom}_K(L, \bar{K})}$ Fortsetzung.

Sei nun $\alpha \in E$, $\tau \in H$. Dann ist $\tau(\sigma(\alpha)) = (\tau \circ \widetilde{\sigma})(\alpha) = (\widetilde{\sigma} \circ \tau')(\alpha) = \widetilde{\sigma}(\alpha) = \sigma(\alpha)$ mit $\widetilde{\sigma}$ wie eben und $\tau' := \widetilde{\sigma}^{-1} \circ \tau \circ \widetilde{\sigma} \in H$ (nach Voraussetzung) $\Rightarrow \sigma(\alpha) \in L^H = E$ ✓ ■

## Folgerung 4.1.3

Sei $L/K$ endliche Galoiserweiterung. Dann gilt für Zwischenkörper $E, E'$ bzw. Untergruppen $H, H'$ von $\mathrm{Gal}(L/K)$:

(a) $E \subseteq E' \iff \mathrm{Gal}(L/E) \supseteq \mathrm{Gal}(L/E')$
$H \subseteq H' \iff L^H \supseteq L^{H'}$

(b) $\mathrm{Gal}(L/E \cap E') = \langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/E') \rangle$
$E \cap E' = L^{\langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/E') \rangle}$
$L^{H \cap H'} = L^H \cdot L^{H'} := K(L^H \cup L^{H'})$ (das **Kompositum** von $L^H$ und $L^{H'}$)

## Folgerung 4.1.4

Zu jeder endlichen separablen Körpererweiterung gibt es nur endlich viele Zwischenkörper.

**Beweis:** Ist $L/K$ endliche Galoiserweiterung, so entsprechen die Zwischenkörper (nach 15) bijektiv den Untergruppen der endlichen Gruppe$(L/K)$. Im allgemeinen ist $L = K(\alpha)$

(12). Sei $f$ das Minimalpolynom von $\alpha$ über $K$. $f$ ist separabel, da $L/K$ separabel. Sei $\widetilde{L}$ der Zerfällungskörper von $f$ über $K$. $\Rightarrow \widetilde{L}/K$ ist galoissch, $K \subseteq L \subseteq \widetilde{L} \Rightarrow L/K$ hat nur endlich viele Zwischenkörper. ■

### Proposition 4.1.5

Sei $L$ ein Körper, $G \subseteq \mathrm{Aut}(L)$ eine endliche Untergruppe. $K := L^G = \{\alpha \in L : \sigma(\alpha) = \alpha \; \forall \, \sigma \in G\}$

Dann ist $L/K$ Galoiserweiterung und $\mathrm{Gal}(L/K) = G$

**Beweis:**

- $L/K$ ist algebraisch und separabel. Sei dazu $\alpha \in L$. $\{\sigma(\alpha) : \sigma \in G\} = G\alpha$ ist endlich. Sei $G\alpha = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$ mit $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ für $i \neq j$ und $\sigma_1 = id_L$. Dabei ist $r$ ein Teiler von $n := |G|$. Sei $f_\alpha(X) := \prod_{i=1}^{r}(X - \sigma_i(\alpha)) \in L[X]$. Zu zeigen: $f_\alpha \in K[X]$. **denn**: für $\sigma \in G$ ist $f_\alpha^\sigma(X) = \prod_{i=1}^{r}(X - \sigma(\sigma_i(\alpha)))$ (selbe Faktoren wie $f_\alpha(X)) \Rightarrow f_\alpha = f_\alpha^\sigma \Rightarrow f_\alpha \in K[X]$

  $\Rightarrow \alpha$ algebraisch, $\alpha$ separabel (da $f_\alpha$ separabel), $[K(\alpha) : K] \leq n$ $\qquad (*)$

- $L/K$ normal: Der Zerfällungskörper von $f_\alpha$ ist in $L$ enthalten. $\Rightarrow L$ ist der Zerfällungskörper der Familie $\{f_\alpha : \alpha \in L\}$

- $L/K$ endlich: Sei $(\alpha_i)_{i \in I}$ Erzeugendensystem von $L/K$. Für jede endliche Teilmenge $I_0 \subseteq I$ ist $K(\{\alpha_i : i \in I_0\})$ endlich über $K$, also $K(\{\alpha_i : i \in I_0\}) = K(\alpha_0)$ für ein $\alpha_0 \in L \overset{(*)}{\Rightarrow} [K(\{\alpha_i : i \in I_0\}) : K] \leq n$. Sei $I_1 \subseteq I$ endlich, so dass $K_1 := K(\{\alpha_i : i \in I_1\})$ maximal unter den $K(\{\alpha_j : j \in J\})$ für $J \subseteq I$ endlich.

  **Ann.**: $K_1 \neq L$. Dann gibt es $i \in I$ mit $\alpha_i \notin K_1 \Rightarrow K_1(\alpha_i) \supsetneq K_1$, trotzdem endlich im Widerspruch zu Wahl von $K_1 \Rightarrow L/K$ endlich, genauer $[L : K] \leq n$ wegen $(*)$.

- $\mathrm{Gal}(L/K) = G$: "$\supseteq$": nach Definition. Nach 4.1.1 ist $n = |G| \leq |\mathrm{Gal}(L/K)| = [L : K] \leq n$

■

## 4.2 Die Galoisgruppe einer Gleichung

### Definition + Bemerkung 4.2.1

Sei $K$ ein Körper, $f \in K[X]$ ein separables Polynom.

(a) Sei $L = L(f)$ Zerfällungskörper von $f$ über $K$. Dann heißt $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$ **Galoisgruppe von f**.

(b) Ist $n = \deg(f)$, so gibt es injektiven Gruppenhomomorphismus $\mathrm{Gal}(f) \hookrightarrow S_n$ (durch Permutation der Nullstellen von $f$)

(c) Ist $L/K$ separable Körpererweiterung vom Grad $n$, so ist $\mathrm{Aut}_K(L)$ isomorph zu einer Untergruppe von $S_n$.

**Beweis:** Sei $L = K(\alpha)$, $f \in K[X]$ Minimalpolynom von $\alpha$, $\alpha = \alpha_1, \ldots, \alpha_d$ die Nullstellen von $f$ in $L \Rightarrow$ jedes $\sigma \in \mathrm{Aut}_K(L)$ permutiert $\alpha_1, \ldots, \alpha_d$. ■

## Beispiele 4.2.2

Die Galoisgruppe von $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist $S_5$.

**Bew.**:

- $f$ ist irreduzibel: Eisenstein für $p = 2$
- $f$ hat 3 relle und 2 zueinander konjugiert komplexe Nullstellen $f(-\infty) = -\infty$, $f(0) = 2, f(1) = -1, f(\infty) = \infty \Rightarrow f$ hat mindestens 3 reelle Nullstellen.
  $f'(X) = 5X^4 - 4 = 5(X^2 - \frac{2}{\sqrt{5}})(X^2 + \frac{2}{\sqrt{5}})$ hat 2 reelle Nullstellen $\Rightarrow f$ hat genau 3 reelle Nullstellen. Ist $\alpha \in \mathbb{C}$ Nullstelle von $f$, so ist $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$.
- $G = \mathrm{Gal}(f)$ enthält die komplexe Konjugation $\tau$. $\tau$ operiert als Transposition: 2 Nullstellen werden vertauscht, 3 bleiben fix.
- $G$ enthält ein Element von Ordnung 5: Ist $\alpha$ Nullstelle von $f$, so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ und $\mathbb{Q}(\alpha) \subseteq L(f) \overset{15}{\Rightarrow} 5$ teilt $|G| \overset{\text{Sylow}}{\Rightarrow}$ Beh.
- $G$ enthält also einen 5-Zyklus und eine Transposition $\overset{(!)}{\Rightarrow} G = S_5$.

## Bemerkung 4.2.3

Allgemeine Gleichung $n$-ten Grades: Sei $k$ ein Körper, $L = k(T_1, \ldots, T_n) = \mathrm{Quot}(k[T_1, \ldots, T_n])$

- $S_n$ operiert auf $L$ durch $\sigma(T_i) = T_{\sigma(i)}$
- Sei $K := L^{S_n}$. $L/K$ ist Galois-Erweiterung (nach Proposition 4.1.5) vom Grad $n!$
- $L$ ist (über $K$) Zerfällungskörper von $f(X) = \prod_{i=1}^{n}(X - T_i) \in K[X]$
- $\mathrm{Gal}(f) = S_n$
- $f(X) = \sum_{\nu=0}^{n}(-1)^\nu s_\nu(T_1, \ldots, T_n)X^{n-\nu}$ mit $s_\nu(T_1, \ldots, T_n) = \sum_{1 \le i_1 < \cdots < i_\nu \le n} T_{i_1} \cdot \ldots \cdot T_{i_\nu}$
  z.B.: $s_1(T_1, \ldots, T_n) = T_1 + \cdots + T_n$, $s_2 = T_1T_2 + T_1T_3 + \cdots + T_{n-1}T_n$, $s_n = T_1 \cdot \ldots \cdot T_n$

- $K = k(s_1, \ldots, s_n)$

## 4.3 Einheitswurzeln

### Bemerkung + Definition 4.3.1

Sei $K$ ein Körper, $\bar{K}$ algebraischer Abschluss von $K$. Sei $n$ eine positive ganze Zahl. Angenommen, $\mathrm{char}(K)$ ist entweder 0 oder teilerfremd zu $n$.

(a) Die Nullstellen von $X^n - 1$ in $\bar{K}$ heißen **n-te Einheitswurzeln**.

(b) $\mu_n(\bar{K}) := \{\zeta \in \bar{K} : \zeta^n = 1\}$ ist zyklische Untergruppe von $\bar{K}^x$ der Ordnung $n$.

**Beweis:** $\mu_n(\bar{K})$ Untergruppe ✓, also zyklisch nach 3.5.1. $f(X) = X^n - 1$ ist separabel, da $f'(X) = nX^{n-1}$ (Bem 3.4.1) ■

(c) Eine $n$-te Einheitswurzel $\zeta$ heißt **primitiv**, wenn $\langle\zeta\rangle = \mu_n(\bar{K})$

## Satz 16

(Voraussetzungen wie eben.)

(a) Die Anzahl der primitiven Einheitswurzeln in $\bar{K}$ ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^x| = \{m \in \{1, \ldots, n\} : \mathrm{ggT}(m, n) = 1\}$ ($n \mapsto \varphi(n)$ ist Eulersche $\varphi$-Funktion)

**Beweis:** Ist $\zeta$ primitive $n$-te Einheitswurzel, so ist $\mu_n(\bar{K}) = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$, $\zeta^k$ erzeugt $\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} \Leftrightarrow \mathrm{ggT}(n, k) = 1$. ■

(b) Ist $n = p_1^{\nu_1} \ldots p_r^{\nu_r}$, (Primfaktorzerlegung) so ist $\varphi(n) = \prod_{i=1}^{r} p_i^{\nu_i - 1}(p_i - 1)$

**Beweis:** Nach Satz 7 ist $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}$ (als Ringe) $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^x = (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})^x \bigoplus \cdots \bigoplus (\mathbb{Z}/p_r^{\nu_r}\mathbb{Z})^x$ (als Gruppen). Doch für jede Primzahl $p$ und jedes positive $\nu$ ist

$|(\mathbb{Z}/p^\nu\mathbb{Z})^x| = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$. ■

(c) Sind $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven Einheitswurzeln, so heißt $\Phi_n(X) := \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \bar{K}[X]$ das $n$-te **Kreisteilungspolynom**

(d) $X^n - 1 = \prod_{d|n} \Phi_d(X)$

**Beweis:** $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n \\ ord(\zeta)=d}} (X - \zeta) = \prod_{d|n} \Phi_d(X)$ ■

(e) Sei $\zeta$ primitive $n$-te Einheitswurzel. Dann ist $K(\zeta)/K$ Galois-Erweiterung.

**Beweis:** $K(\zeta)$ ist Zerfällungskörper von $X^n - 1$ über $K$, also normal. $X^n - 1$ ist separabel (4.3.1) ■

(f)

$$\chi_n : \begin{array}{ccc} \mathrm{Gal}(K(\zeta)/K) & \to & (\mathbb{Z}/n\mathbb{Z})^x \\ \sigma & \mapsto & \chi_n(\sigma) \end{array}$$

ist injektiver Gruppenhomomorphismus, wobei
$\sigma(\zeta) = \zeta^{\chi_n(\sigma)}$. ($\chi_n$ heißt **zyklotomischer Charakter**)

**Beweis:** $\chi_n(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^x$, da $\sigma(\zeta)$ primitive Einheitswurzel sein muß.

$\chi_n$ ist Gruppenhomomorphismus: $\sigma_1, \sigma_2 \in \mathrm{Gal}(K(\zeta)/K) \Rightarrow \sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{\chi_n(\sigma_2)}) = (\sigma_1(\zeta))^{\chi_n(\sigma_2)} = \zeta^{\chi_n(\sigma_1)\chi_n(\sigma_2)}$

$\chi_n$ injektiv: $\chi_n(\sigma) = 1 \Rightarrow \sigma(\zeta) = \zeta \Rightarrow \sigma = id$ ■

(g) $\Phi_n(X) \in K[X]$, genauer $\Phi_n(X) \in \begin{cases} \mathbb{Z}[X] \text{ (primitiv)} & : \mathrm{char}(K) = 0 \\ \mathbb{F}_p[X] & : \mathrm{char}(K) = p \end{cases}$

**Beweis:** Induktion über $n$: $n = 1$ ✓

$n > 1$: $\underbrace{X^n - 1}_{(*)} \overset{(d)}{=} \Phi_n(X) \underbrace{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}_{(**)}$

$\mathrm{char}(K) = p$ : $(*) \in \mathbb{F}_p[X]$, $(**) \in \mathbb{F}_p[X]$ nach IV $\Rightarrow \Phi_n(X) \in \mathbb{F}_p[X]$ : (weil Polynomdivision zweier Polynome in $\mathbb{F}_p[X]$ nie die Koeffizienten aus dem Körper $\mathbb{F}_p$ herausführt).

$\mathrm{char}(K) = 0$ : $(*) \in \mathbb{Z}[X]$ (primitiv), $(**) \in \mathbb{Z}[X]$ primitiv nach IV

$\overset{\text{Lemma von Gauß}}{\Rightarrow} \Phi_n(X) \in \mathbb{Z}[X]$ primitiv. ■

(h) Ist $K = \mathbb{Q}$, so ist $\Phi_n$ irreduzibel und $\chi_n$ ein Isomorphismus. $\mathbb{Q}(\zeta)$ heißt $n$-ter **Kreisteilungskörper**.

**Beweis:** Es genügt zu zeigen: $\Phi_n$ irreduzibel (dann folgt $\chi_n$ Isomorphismus aus (e) und (f))

Sei $f \in \mathbb{Q}[X]$ Minimalpolynom von $\zeta$, $f \in \mathbb{Z}[X]$ wegen (g)

**Beh.**: $f(\zeta^p) = 0$ für jede Primzahl $p$ mit $p \nmid n$.

Dann ist auch $f(\zeta^m) = 0$ für jedes $m$ mit $\mathrm{ggT}(m, n) = 1 \Rightarrow f(\zeta_i) = 0$ für jede primitive Einheitswurzel $\zeta_i \Rightarrow \Phi_n | f \Rightarrow \Phi_n = f$

**Bew.**: Sei $X^n - 1 = f \cdot h$. Wäre $f(\zeta^p) \neq 0 \Rightarrow h(\zeta^p) = 0$ dh. $\zeta$ Nullstelle von $h(X^p) \Rightarrow h(X^p)$ ist Vielfaches von $f \Rightarrow \exists\, g \in \mathbb{Z}[X]$ mit $h(X^p) = f \cdot g$
$\overset{mod\ p}{\Rightarrow} \bar{f}\bar{g} = \bar{h}^p$ in $\bar{\mathbb{F}}_p[X] \Rightarrow \bar{f}$ und $\bar{h}$ haben gemeinsame Nullstellen in $\bar{\mathbb{F}}_p \Rightarrow$ $X^n - \bar{1} = \bar{f}\bar{h}$ hat doppelte Nullstelle $\lightning$ zu $X^n - 1$ separabel. ■

**Beispiele:** $\Phi_1(X) = 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ für $p$ prim.

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_2 \cdot \Phi_1} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1$$

$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_3 \Phi_2 \Phi_1} = \cdots = X^2 - X + 1$$

$$\Phi_8(X) = X^4 + 1$$

Für $n < 105$ sind alle Koeffizienten $0, 1$ oder $-1$.

## Folgerung 4.3.2

Das regelmäßige $n$-Eck ist genau dann mit Zirkel und Lineal (aus $\{0, 1\}$) konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

**Beweis:** z.z.: $\zeta_n$ (primitive $n$-te Einheitswurzel) $\in K(\{0, 1\}) \Leftrightarrow \varphi(n) = 2^l$ für ein $l \geq 1 \Leftrightarrow \underbrace{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]}_{\varphi(n)} = 2^l$ und es gibt Kette $\mathbb{Q}(M) = L_0 \subset L_1 \subset \cdots \subset L_n = \mathbb{Q}(\zeta_n)$ und $[L_i : L_{i-1}] = 2$.

"$\Leftarrow$": $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ ist abelsch von Ordnung $2^l$. Dazu gehört Kompositionsreihe mit Faktoren $\mathbb{Z}/2\mathbb{Z}$ $\overset{\text{Hauptsatz d. Galoistheorie}}{\Rightarrow}$ ■

## 4.4 Norm, Spur und Charaktere

### Definition + Proposition 4.4.1

Sei $G$ eine Gruppe, $K$ ein Körper.

(a) Ein **Charakter** von $G$ (mit Werten in $K$) ist ein Gruppenhomomorphismus $\chi : G \to K^x$

(b) $X_K(G) := \{\chi : G \to K^x,\ \chi \text{ Charakter}\} = \mathrm{Hom}(G, K^x)$ heißt **Charaktergruppe** von $G$ (mit Werten in $K$)

(c) (Lineare Unabhängigkeit der Charaktere, E.Artin) $X_K(G)$ ist linear unabhängige Teilmenge des $K$-Vektorraums $\mathrm{Abb}(G, K)$

**Beweis:** Angenommen $X_K(G)$ ist linear abhängig. Dann sei $n > 0$ minimal, so dass es in $X_K(G)$ $n$ paarweise verschieden linear abhängige Elemente gibt. Es gebe also paarweise verschiedene Charaktere $\chi_1, \ldots, \chi_n \in X_K(G)$ und Körperelemente $\lambda_1, \ldots, \lambda_n \in K$ mit $\sum_{i=1}^{n} \lambda_i \chi_i = 0$. Dazu muß $n \geq 2$ sein. Ferner sind die Körperelemente $\lambda_1, \ldots, \lambda_n \in K$ von 0 verschieden, da sonst $n$ nicht minimal wäre.

Sei $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Dann gilt für alle $h \in G$:

$$0 = \sum_{i=1}^{n} \lambda_i \underbrace{\chi_i(gh)}_{=\chi_i(g)\chi_i(h)} = \sum_{i=1}^{n} \underbrace{\lambda_i \chi_i(g)}_{=:\mu_i \in K^x} \chi_i(h) = \sum_{i=1}^{n} \mu_i \chi_i(h) \Rightarrow \sum_{i=1}^{n} \mu_i \chi_i = 0$$

Sei $\nu_i := \mu_i - \lambda_i \chi_1(g),\ i = 1, \ldots, n$. Dann ist $\sum_{i=1}^{n} \nu_i \chi_i = 0$ (da $\sum_{i=1}^{n} \mu_i \chi_i = 0$ und $\sum_{i=1}^{n} \lambda_i \chi_i = 0$ ist). Da $\nu_1 = \lambda_1 \chi_1(g) - \lambda_1 \chi_1(g) = 0$ ist, bedeutet dies: $\sum_{i=2}^{n} \nu_i \chi_i = 0$. Wegen $\nu_2 = \lambda_2 \chi_2(g) - \lambda_2 \chi_1(g) = \underbrace{\lambda_2}_{\neq 0} \underbrace{(\chi_2(g) - \chi_1(g))}_{\neq 0} \neq 0$ sind also $\chi_2, \ldots, \chi_n$ linear abhängig. Dies steht im Widerspruch zur Minimalität von $n$. ■

Es sei angemerkt, daß der Begriff eines "Charakters" in der Mathematik in sehr vielen, teilweise stark unterschiedlichen Bedeutungen anzutreffen ist. So bedeutet "Charakter" in der Darstellungstheorie von Gruppen etwas anderes als in der obigen Definition 4.4.1.

### Definition + Bemerkung 4.4.2

Sei $L/K$ endliche Körpererweiterung, $q := \frac{[L:K]}{[L:K]_s}$ $(= p^r,\ p = \mathrm{char}(K))$, $n := [L : K]_s$, $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_n\}$

(a) Für $\alpha \in L$ heißt $\mathrm{tr}_{L/K}(\alpha) := q \cdot \sum_{i=1}^{n} \sigma_i(\alpha) \in \bar{K}$ die **Spur** von $\alpha$ (über $K$)

(b) $\forall \alpha \in L : \mathrm{tr}_{L/K}(\alpha) \in K$

**Beweis:** Œ$L/K$ separabel. Ist $L/K$ normal, also galoissch, so ist $\mathrm{Hom}_K(L, \bar{K}) = \mathrm{Gal}(L/K) =: G$ und $\mathrm{tr}_{L/K}(\alpha) \in L^G = K$ (da invariant unter allen $\sigma_i$). Andernfalls sei $\widetilde{L}$ normale Erweiterung von $K$ mit $L \subset \widetilde{L}$. Für $\tau \in \mathrm{Hom}_K(\widetilde{L}, \bar{K}) = \mathrm{Gal}(\widetilde{L}/K)$ und jedes $i = 1, \ldots, n$ ist $\tau \circ \sigma_i \in \mathrm{Hom}_K(L, \bar{K})$ (da $\sigma_i(L) \subseteq \widetilde{L}$) $\Rightarrow \mathrm{tr}_{L/K}(\alpha) \in \widetilde{L}^{\mathrm{Gal}(\widetilde{L}/K)} = K$ ■

(c) $\mathrm{tr}_{L/K}$ ist $K$-linear.

(d) Für $\alpha \in L$ heißt $N_{L/K}(\alpha) = \left( \prod_{i=1}^{n} \sigma_i(\alpha) \right)^q$ die **Norm** von $\alpha$ (über $K$).

(e) $N_{L/K}(\alpha) \in K$

(f) $N_{L/K} : L^x \to K^x$ ist Gruppenhomomorphismus

**Beweis:**

(e) Ist $L/K$ separabel, so argumentiere wie in (b). Sonst siehe Bosch.

■

## Bemerkung 4.4.3

Sei $L/K$ endliche Körpererweiterung. Für $\alpha \in L$ sei $m_\alpha : L \to L,\ x \mapsto \alpha x$. $m_\alpha$ ist $K$-linear und es gilt:

$$\mathrm{tr}_{L/K}(\alpha) = \mathrm{Spur}(m_\alpha),\ N_{L/K}(\alpha) = \det(m_\alpha)$$

**Beweis:** Ist $L/K$ separabel, so sei $L = K(\alpha)$. Dann ist $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ eine $K$-Basis von $L$, $[L : K] = n$. Weiter sei $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \in K[X]$ das Minimalpolynom von $\alpha$ über $K$. Dann ist die Abbildungsmatrix von $m_\alpha$ bezüglich der Basis $1, \ldots, \alpha^{n-1}$

$$D = \begin{pmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & & \vdots & -c_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \ldots 0 & 1 & -c_{n-1} \end{pmatrix}$$

$\Rightarrow \text{Spur}(m_\alpha) = -c_{n-1}$, $\det(m_\alpha) = (-1)^n c_0$.

In $\bar{K}[X]$ zerfällt $f$ in Linearfaktoren:

$f = \prod_{i=1}^{n}(X - \sigma_i(\alpha)) \Rightarrow c_{n-1} = -\sum_{i=1}^{n}\sigma_i(\alpha)$, $c_0 = (-1)^n \prod_{i=1}^{n}\sigma_i(\alpha)$

Ist $L \neq K(\alpha)$, so sei $b_1, \ldots, b_m$ eine $K(\alpha)$-Basis von $L$. Dann ist $B = \{b_i\alpha^j,\ i = 1, \ldots, m,\ j = 0, \ldots, n-1\}$ eine $K$-Basis von $L$. Dann ist die Darstellungsmatrix von $m_\alpha$ bezüglich $B$:

$$\widetilde{D} = \begin{pmatrix} D & 0 & \ldots & 0 \\ 0 & D & & \\ & & \ddots & \\ 0 & 0 & & D \end{pmatrix}$$

$\Rightarrow \text{Spur}(m_\alpha) = m(-c_{n-1})$, $\det(m_\alpha) = ((-1)^n c_0)^m$

Für jedes $\sigma_i \in \text{Hom}_K(L, \bar{K})$ ist $\sigma_i(\alpha)$ Nullstelle von $f$. Jede Nullstelle von $f$ wird dabei gleichoft angenommen, nämlich $m = [L : K(\alpha)]$-mal $\Rightarrow \text{tr}_{L/K}(\alpha) = m \cdot \text{tr}_{K(\alpha)/K}(\alpha) = m(-c_{n-1})$ und $N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}\right)^m = ((-1)^n c_0)^m$ ■

## **Satz 17** ("Hilbert(s Satz) 90")

Sei $L/K$ zyklische Galois-Erweiterung. (dh. $\text{Gal}(L/K) = \langle\sigma\rangle$ für ein $\sigma$)

(a) Ist $\beta \in L$ mit $N_{L/K}(\beta) = 1$, so gibt es ein $\alpha \in L^x$ mit $\beta = \frac{\alpha}{\sigma(\alpha)}$

**Beweis:** $n := [L : K]$. Nach 4.4.1 sind die Charaktere $id, \sigma, \ldots, \sigma^{n-1} : L^x \to L^x$ linear unabhängig über $L$.

Nun ist $f = id + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \cdots + \beta\sigma(\beta)\ldots\sigma^{n-2}(\beta)\sigma^{n-1}$ nicht die Nullabbildung $\Rightarrow \exists\gamma \in L$ mit $\alpha := f(\gamma) \neq 0$

$$\beta\sigma(\alpha) = \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \cdots + \underbrace{\beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)}_{N_{L/K}(\beta)=1}\underbrace{\sigma^n(\gamma)}_{=\gamma} = \alpha$$ ■

(b) Sei $L/K$ zyklische Galoiserweiterung, $n = [L : K]$, $\sigma \in \text{Gal}(L/K)$ ein Erzeuger. Zu $\beta \in L$ mit $\text{tr}_{L/K}(\beta) = 0$ gibt es $\alpha \in L$ mit $\beta = \alpha - \sigma(\alpha)$

**Beweis:** Sei $\gamma \in L$ mit $\text{tr}_{L/K}(\gamma) \neq 0$ und
$\alpha := \frac{1}{\text{tr}_{L/K}(\gamma)} \cdot [\beta\sigma(\gamma) + (\beta + \sigma(\beta))\sigma^2(\gamma) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-1}(\gamma)]$
$\Rightarrow \sigma(\alpha) = \frac{1}{\text{tr}_{L/K}(\gamma)}[\sigma(\beta)\sigma^2(\gamma) + (\sigma(\beta) + \sigma^2(\beta))\sigma^3(\gamma) + \cdots + (\sigma(\beta) + \cdots +$

$\sigma^{n-1}(\beta))\sigma^n(\gamma)]$
$\Rightarrow \quad (\alpha - \sigma(\alpha))\mathrm{tr}_{L/K}(\gamma) = \beta\sigma(\gamma) + \beta\sigma^2(\gamma) + \cdots + \beta\sigma^{n-1}(\gamma) - \underbrace{(\sigma(\beta) + \cdots + \sigma^{n-1}(\beta))}_{-\beta}\gamma = \beta \cdot \mathrm{tr}_{L/K}(\gamma)$ ■

## Folgerung 4.4.4

Voraussetzungen wie in Satz 17.

(a) Ist $\mathrm{char}(K)$ kein Teiler von $n = [L : K]$ und enthält $K$ eine primitive $n$-te Einheitswurzel $\zeta$, so gibt es ein primitives Element $\alpha \in L$, so dass das Minimalpolynom von $\alpha$ über $K$ von der Form

$$X^n - \gamma$$

ist für ein $\gamma \in K$. (*"Kummer-Erweiterung"*)

(b) Ist $\mathrm{char}(K) = [L : K] = p$, so gibt es ein primitives Element $\alpha \in L$, so dass das Minimalpolynom von $\alpha$ über $K$ die Form

$$X^p - X - \gamma$$

hat für ein $\gamma \in K$. (*"Artin-Schreier-Erweiterung"*)

**Beweis:**

(a) Es ist $N_{L/K}(\zeta) = \zeta^n = 1 = N_{L/K}(\zeta^{-1}) \overset{\text{Satz } 17}{\Rightarrow}$ es gibt $\alpha \in L^x$ mit $\sigma(\alpha) = \zeta\alpha \Rightarrow \sigma^i(\alpha) = \zeta^i\alpha,\ i = 1, \ldots, n-1 \Rightarrow$ Das Minimalpolynom von $\alpha$ über $K$ hat $n$ verschiedene Nullstellen $\Rightarrow L = K(\alpha)$.

Außerdem ist $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n \Rightarrow \gamma := \alpha^n \in K \Rightarrow$ Das Minimalpolynom von $\alpha$ ist $X^n - \gamma$

(b) $\mathrm{tr}_{L/K}(1) = 1 + \cdots + 1 = p = 0 \overset{\text{Satz } 17}{\Rightarrow}$ es gibt $\alpha \in L$ mit $\sigma(\alpha) = \alpha + 1 \Rightarrow \sigma^i(\alpha) = \alpha + i,\ i = 0, \ldots, n-1 \Rightarrow K(\alpha) = L$

$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = \alpha^p + 1 - (\alpha + 1) = \alpha^p - \alpha \Rightarrow \alpha^p - \alpha =: \gamma \in K$ und $X^p - X - \gamma$ ist Minimalpolynom von $\alpha$. ■

## Proposition 4.4.5

Sei $L/K$ einfache Körpererweiterung, $L = K(\alpha)$

(a) Ist $\alpha$ Nullstelle eines Polynoms $X^n - \gamma$ für ein $\gamma \in K$ und enthält $K$ eine primitive $n$-te Einheitswurzel $\zeta$, so ist $L/K$ galoissch, $\mathrm{Gal}(L/K)$ zyklisch, $d := [L : K]$ ist Teiler von $n$, $\alpha^d \in K$, $X^d - \alpha^d$ ist Minimalpolynom von $\alpha$

(b) Ist $\mathrm{char}(K) = p > 0$ und $\alpha \in L \setminus K$ Nullstelle eines Polynoms $X^p - X - \gamma$ für ein $\gamma \in K$, so ist $L/K$ galoissch und $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$

**Beweis:**

(a) Die Nullstellen von $X^n - \gamma$ sind $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha \Rightarrow L$ ist Zerfällungskörper von $X^n - \gamma$, also normal und separabel, also galoissch.

Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(\alpha) = \zeta^{\nu(\sigma)}\alpha$ für ein $\nu(\sigma) \in \mathbb{Z}/n\mathbb{Z}$.

$\sigma \mapsto \nu(\sigma)$ ist injektiver Gruppenhomomorphismus $\mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z} \Rightarrow \mathrm{Gal}(L/K)$ ist zyklisch, da Untergruppe von $\mathbb{Z}/n\mathbb{Z} \Rightarrow d = [L : K]$ teilt $n$.

Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(\alpha^d) = \left(\zeta^{\nu(\sigma)}\right)^d \alpha^d = \alpha^d \Rightarrow \alpha^d \in K$; $X^d - \alpha^d$ ist Minimalpolynom, da $L = K(\alpha)$ und $[K(\alpha) : K] = d$.

(b) Für $i \in \mathbb{F}_p$ ist $(\alpha + i)^p - (\alpha + i) - \gamma = \alpha^p + \underbrace{i^p}_{=i} - \alpha - i - \gamma = 0 \Rightarrow X^p - X - \gamma$ hat $p$ verschieden Nullstellen $\Rightarrow L$ ist Zerfällungskörper von $X^p - X - \gamma$ und $L/K$ ist separabel. Außerdem folgt: $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$ ■

## 4.5 Auflösung von Gleichungen durch Radikale

### Definition 4.5.1

Sei $K$ ein Körper.

(a) Eine einfache Körpererweiterung $L = K(\alpha)$ heißt **elementare (oder einfache) Radikalerweiterung**, wenn entweder

(i) $\alpha$ ist eine Einheitswurzel.

(ii) $\alpha$ ist Nullstelle von $X^n - \gamma$ für ein $\gamma \in K$ und $\mathrm{char}(K) \nmid n$

(iii) $\alpha$ ist Nullstelle von $X^p - X - \gamma$ für $\gamma \in K$, $\mathrm{char}(K) = p$

(b) Eine endliche Körpererweiterung $L/K$ heißt **Radikalerweiterung**, wenn es eine Körpererweiterung $L'/L$ gibt und eine Kette $K = L_0 \subset L_1 \subset \cdots \subset L_n = L'$ von Zwischenkörpern, so dass $L_{i+1}/L_i$ elementare Radikalerweiterung ist für $i = 0, \ldots, n-1$

(c) Ist $f \in K[X]$ separabel, nicht konstant, so heißt die Gleichung $f(X) = 0$ **durch Radikale auflösbar**, wenn der Zerfällungskörper von $f$ Radikalerweiterung ist.

**Beispiel:** $K = \mathbb{Q}$, $f(X) = X^3 - 3X + 1$

**Beh.**: Ist $\alpha$ Nullstelle von $f$, so ist $\mathbb{Q}(\alpha)$ Zerfällungskörper von $f$, hat also Grad 3 über $\mathbb{Q}$. $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist **keine** einfache Radikalerweiterung.

Die Nullstellen von $f$ sind:

$$\alpha_1 = e^{2\pi i/9} + e^{16\pi i/9}$$
$$\alpha_2 = e^{8\pi i/9} + e^{10\pi i/9}$$
$$\alpha_3 = e^{14\pi i/9} + e^{4\pi i/9}$$

Es ist $\alpha_1^2 = e^{4\pi i/9} + e^{14\pi i/9} + 2 = \alpha_3 + 2 \Rightarrow \alpha_3 \in \mathbb{Q}(\alpha_1) \Rightarrow \alpha_2 = -\alpha_1 - \alpha_3 \in \mathbb{Q}(\alpha_1)$

## Satz 18

Sei $K$ ein Körper, $f \in K[X]$ separabel, nicht konstant.

(a) Die Gleichung $f(X) = 0$ ist genau dann durch Radikale auflösbar, wenn ihre Galoisgruppe auflösbar ist (dh. $G$ hat Normalreihe $G = G_0 \rhd \cdots \rhd G_n = \{e\}$ mit $G_i/G_{i+1}$ abelsch).

(b) Eine endliche Körpererweiterung $L/K$ ist genau dann Radikalerweiterung, wenn es eine endliche Galoiserweiterung $L'/K$ gibt mit $L \subseteq L'$, so dass $\mathrm{Gal}(L'/K)$ auflösbare Gruppe ist.

**Beispiel:** $X^5 - 4X + 2$ hat Galoisgruppe $S_5$ und ist deshalb nicht durch Radikale auflösbar, denn $S_5 \supset A_5 \supset \{e\}$ ist Kompositionsreihe. Nach Jordan-Hölder tritt $A_5$ in jeder Kompositionsreihe für $S_5$ als Faktorgruppe auf.

**Beweis:** "⇒": Sei $K = L_0 \subset L_1 \subset \cdots \subset L_m$ Kette wie in Def. 4.5.1 (b) mit $L \subseteq L_m$.

**Induktion über m:**

**m=1:** Ist $L_1/K$ vom Typ (i), so ist $L_1 = K(\zeta)$ für eine primitive $n$-te Einheitswurzel $\zeta$ und $\mathrm{Gal}(K(\zeta)/K) \subseteq (\mathbb{Z}/n\mathbb{Z})^x$, also auflösbar.

Ist $L_1/K$ vom Typ (iii), so ist $L_1/K$ galoissch und $\mathrm{Gal}(L_1/K) = \mathbb{Z}/p\mathbb{Z}$.

Sei $L_1/K$ vom Typ (ii). Enthält $K$ eine primitive $n$-te Einheitswurzel, so ist $K(\alpha)/K$ galoissch und $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}/n\mathbb{Z}$

Andernfalls sei $F = K(\zeta)$ der Zerfällungskörper von $X^n - 1$ über $K$ und $L_1' = L_1(\zeta) = F(\alpha) = F \cdot L_1$ das "**Kompositum**" von $F$ und $L_1$.

$L_1'$ ist galoissch über $K$ (Zerfällungskörper von $X^n - \gamma$ über $K$) und es gibt exakte Sequenz

$$1 \to \underbrace{\mathrm{Gal}(L_1'/F)}_{\text{zyklisch}} \to \mathrm{Gal}(L_1'/K) \to \underbrace{\mathrm{Gal}(F/K)}_{\text{abelsch}} \to 1$$

$\Rightarrow \mathrm{Gal}(L_1'/K)$ auflösbar.

**m>1:** Eine endliche Körpererweiterung heißt **auflösbar**, wenn es eine endliche Erweiterung $L'/L$ gibt, so dass $L'/K$ galoissch und $\mathrm{Gal}(L'/K)$ auflösbar ist.

Nach Induktionsvoraussetzung ist $L_{m-1}/K$ auflösbar. Außerdem ist $L_m/L_{m-1}$ auflösbar. (m=1)

zu zeigen also: Sind $K \subset \underbrace{L}_{=L_{m-1}} \subset \underbrace{M}_{=L_m}$ Körpererweiterungen und ist $L/K$ auflösbar und $M/L$ auflösbar, so ist $M/K$ auflösbar.

Seien dazu $L'/L$ und $M'/M$ Erweiterungen wie in Def.:

**Beh.**: $L'M'/L'$ ist galoissch und $\mathrm{Gal}(L'M'/L)$ ist auflösbar.

**denn**: Nach Voraussetzung ist $M'/L$ galoissch, also Zerfällungskörper eines Polynoms $f \in L[X] \Rightarrow M'L'$ ist Zerfällungskörper von $f \in L'[X]$ über $L'$.

Außerdem: $\mathrm{Gal}(L'M'/L') \to \mathrm{Gal}(M'/L)$, $\sigma \mapsto \sigma_{|M'} \overset{(!)}{\in} \mathrm{Gal}(M'/L)$ ist wohldefiniert und injektiv: Ist $\sigma_{|M'} = id_{M'}$, so ist $\sigma = id_{L'M}$, da $\sigma_{|L'} = id_{L'}$ nach Voraussetzung.

Also Œ$L = L'$, $L'M' = M$.

**m>1 (Forts.)** Ist $M/K$ galoissch, so ist $\mathrm{Gal}(M/K)$ auflösbar, da dann

$$1 \to \underbrace{\mathrm{Gal}(M/L)}_{\text{auflösbar}} \to \mathrm{Gal}(M/K) \to \underbrace{\mathrm{Gal}(L/K)}_{\text{auflösbar}} \to 1$$

exakt ist.

Andernfalls sei $\widetilde{M}/M$ (minimale) Erweiterung, so dass $\widetilde{M}/K$ galoissch ist. $\widetilde{M}$ wird (über $K$) erzeugt von den $\sigma(M)$, $\sigma \in \mathrm{Hom}_K(M, \bar{K})$. ($\bar{K}$ fest gewählter algebraischer Abschluss von $K$) Für jedes $\sigma \in \mathrm{Hom}_K(M, \bar{K})$ ist $\sigma(M)$ Galoiserweiterung von $\sigma(L) = L$.

Dann ist

$$\begin{array}{ccc} \mathrm{Gal}(\widetilde{M}/L) & \to & \prod_{\sigma \in \mathrm{Hom}_K(M,\bar{K})} \mathrm{Gal}(\sigma(M)/L) \\ \tau & \mapsto & (\tau_{|\sigma(M)})_\sigma \end{array}$$

injektiver Gruppenhomomorphismus.

Für jedes $\sigma \in \mathrm{Hom}_K(M, \bar{K})$ ist $\mathrm{Gal}(\sigma(M)/L) \cong \mathrm{Gal}(M/L)$, also auflösbar $\Rightarrow$ $\prod_\sigma \mathrm{Gal}(\sigma(M)/L)$ ist auflösbar. (!) $\Rightarrow \mathrm{Gal}(\widetilde{M}/L)$ auflösbar (als Untergruppe einer auflösbaren Gruppe) $\Rightarrow \mathrm{Gal}(\widetilde{M}/K)$ ist auflösbar wegen $1 \to \mathrm{Gal}(\widetilde{M}/L) \to \mathrm{Gal}(\widetilde{M}/K) \to \mathrm{Gal}(L/K) \to 1$ exakt.

"$\Leftarrow$":
$G := \mathrm{Gal}(L'/K)$ sei auflösbar, $G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$ Normalreihe, so dass $G_{i+1}$ Normalteiler in $G_i$ und $G_i/G_{i+1} \cong \mathbb{Z}/p_i\mathbb{Z}$ mit Primzahlen $p_i$, $i = 0, \ldots, m-1$ ist.

Dazu gehört eine Kette von Zwischenkörpern $K = K_0 \subset K_1 \subset \ldots K_m = L'$, in der $K_i/K_{i-1}$ Galoiserweiterung ist und $\mathrm{Gal}(K_i/K_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$.

Fall 1: Ist $p_i = \mathrm{char}(K)$, so ist $K_i/K_{i-1}$ elementare Radikalerweiterung vom Typ (iii), also Minimalpolynom der Form $X^{p_i} - X - \gamma$.

Fall 2: Ist $p_i \neq \mathrm{char}(K)$, so ist $K_i/K_{i-1}$ vom Typ (ii), **falls** $K_{i-1}$ eine primitive $n$-te Einheitswurzel $\zeta$ enthält.

Fall 3: $p_i \neq \mathrm{char}(K)$, $K_{i-1}$ enthält keine primitive Einheitswurzel. Sei also

$$d := \prod_{\substack{p \text{ prim} \\ p \mid |G|}} p$$

und $F$ der Zerfällungskörper von $X^d - 1$ über $K$. $\Rightarrow F/K$ ist Erweiterungskörper vom Typ (i).

Sei $\widetilde{L} = FL' \Rightarrow \widetilde{L}/F$ ist Galoiserweiterung (siehe hier ausgelassenes Diagramm). Die Abbildung $\mathrm{Gal}(\widetilde{L}/F) \to \mathrm{Gal}(L'/K)$, $\sigma \mapsto \sigma|_{L'}$, ist injektiver Gruppenhomomorphismus, also ist $\mathrm{Gal}(\widetilde{L}/F)$ auflösbar und $|\mathrm{Gal}(\widetilde{L}, F)|$ teilt $|G|$. Erhalte Kette $K \subset F \subset F_1 \subset \cdots \subset F_r = \widetilde{L}$ von Zwischenkörpern, $F_i/F_{i-1}$ Galoiserweiterung, $\mathrm{Gal}(F_i/F_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$ elementare Radikalerweiterung vom Typ (ii). ■