

Satz (19.4)

Sei $L|K$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G = \text{Gal}(L|K)$, $\mathcal{U}$ die Menge der Untergruppe von G und $\mathcal{Z}$ die Menge der Zwischenkörper von $L|K$. Dann sind durch die Zuordnungen

$$\phi : \mathcal{U} \rightarrow \mathcal{Z}, U \mapsto L^U \quad \text{und} \quad \psi : \mathcal{Z} \rightarrow \mathcal{U}, M \mapsto \text{Gal}(L|M)$$

zueinander inverse Bijektionen zwischen $\mathcal{U}$ und $\mathcal{Z}$ gegeben.

Satz (19.5)

- (i) Sind $U_1, U_2 \in \mathcal{U}$ mit $U_1 \subseteq U_2$, dann folgt $L^{U_1} \supseteq L^{U_2}$.
- (ii) Sind umgekehrt $M_1, M_2 \in \mathcal{Z}$ mit $M_1 \subseteq M_2$, dann ist $\text{Gal}(L|M_1) \supseteq \text{Gal}(L|M_2)$.
- (iii) Es gilt $L^{\{\text{id}_L\}} = L$, $L^G = K$ und $\text{Gal}(L|L) = \{\text{id}_L\}$,
 $\text{Gal}(L|K) = G$.
- (iv) Ist M ein Zwischenkörper und $U = \text{Gal}(L|M)$ die zugehörige Untergruppe, dann gilt $[L : M] = |U|$ und $[M : K] = (G : U)$.

Proposition (22.6)

Sei M ein Zwischenkörper von $L|K$ und $U = \text{Gal}(L|M)$ die zugehörige Untergruppe von $G = \text{Gal}(L|K)$. Dann sind folgende Aussagen äquivalent:

- (i) Die Erweiterung $M|K$ ist normal.
- (ii) Die Untergruppe U ist Normalteiler von G .

In diesem Fall erhalten wir durch $\sigma \mapsto \sigma|_M$ eine Abbildung $G \rightarrow \text{Gal}(M|K)$, und diese induziert einen natürlichen Isomorphismus $G/U \cong \text{Gal}(M|K)$.

Beweis von Prop. 22.6

geg: endl Gal-Ers. $L|K$, M Zwischenkörper von $L|K$,
 $G = \text{Gal}(L|K)$, $U \leq G$ zu M gehörende Untergruppe, d.h.
 $U = \text{Gal}(L|M)$ und $M = L^U$

zeige zunächst $\forall \sigma \in G: \sigma U \sigma^{-1} = \text{Gal}(L|\sigma(M))$

Sei $\tau \in G$. Dann gilt die Äquivalenz:

$$\tau \in \sigma U \sigma^{-1} \iff \exists \tau_1 \in U \text{ mit } \tau = \sigma \tau_1 \sigma^{-1} \iff$$

$$\exists \tau_1 \in U \iff \sigma^{-1} \tau \sigma = \tau_1 \iff \sigma^{-1} \tau \sigma \in U \iff$$

$$\sigma^{-1} \tau \sigma \in \text{Gal}(L|M) \iff \forall \alpha \in M: (\sigma^{-1} \circ \tau \circ \sigma)(\alpha) = \alpha$$

$$\iff \forall \alpha \in M: \tau(\sigma(\alpha)) = \sigma(\alpha) \iff \forall \alpha_1 \in \sigma(M): \tau(\alpha_1) = \alpha_1$$

$$\iff \tau \in \text{Gal}(L|\sigma(M))$$

Zeige nun die Äquivalenz der Aussagen

(i) $M|K$ ist normal (ii) $U \trianglelefteq G$

"(i) $\Rightarrow$ (ii)" $U \trianglelefteq G$ ist äquivalent zu $\sigma U \sigma^{-1} = U \quad \forall \sigma \in G$,

und wie oben gezeigt, ist dies äquivalent zu $\text{Gal}(L|\sigma(M)) = \text{Gal}(L|M) \quad \forall \sigma \in G$. Nach dem Hauptsatz der Galorstheorie ist dies äquivalent zu $\sigma(M) = M \quad \forall \sigma \in G \quad (*)$

Zeige also $(*)$ unter der Voraussetzung (i). Sei $\sigma \in G$ und L^{alg} ein alg. Abschluss von L . $\rightarrow$ können σ als K -Hom. $L \rightarrow L^{\text{alg}}$ betrachten. $\Rightarrow \sigma|M$ ist ein K -Hom. $M \rightarrow L^{\text{alg}}$. Da $M|K$ normal ist, folgt $\sigma|M \in \text{Aut}_K(M) \Rightarrow \sigma(M) = M$

"(ii) $\Rightarrow$ (i)" s.o. $\rightarrow$ Aus der Vor. (ii) folgt (*).

z.zg. $M|K$ ist normal zeige dafür

$$\text{Hom}_K(M, L^{\text{alg}}) = \text{Aut}_K(M) \quad " \supseteq "$$
 offensichtlich

" $\subseteq$ " Sei $\tau \in \text{Hom}_K(M, L^{\text{alg}})$. Da $L|M$ algebraisch und L^{alg} alg. abgeschlossen ist, existiert eine Fortsetzung von τ zu einem K -Hom.

$$\exists: L \rightarrow L^{\text{alg}} \quad L|K \text{ ist normal} \Rightarrow \sigma \in \text{Aut}_K(L)$$

$$\Rightarrow \sigma \in G \stackrel{(*)}{=} \sigma(M) = M \quad \text{Wegen}$$

$$\sigma|_M = \tau \quad \text{folgt} \quad \tau(M) = M \quad \text{Daraus wieder}$$

$$\text{dann folgt} \quad \tau \in \text{Aut}_K(M)$$

Betrachte nun die Abbildung $\phi: G \rightarrow \text{Hom}_K(M, L^{\text{alg}})$
 $\sigma \mapsto \sigma|_M$. Da $M|K$ normal (und somit auch
galois'sch) ist, ist dies eine Abbr. $G \rightarrow \text{Gal}(M|K)$.

Beh. ϕ induziert einen Isom. $G/U \cong \text{Gal}(M|K)$

Damit der Hom-Satz diese Aussage liefert,
muss überprüft werden (1) ϕ ist Gruppenhom.

(2) ϕ ist surjektiv (3) $\ker(\phi) = U$

zu (1) Seien $\sigma, \tau \in G \rightarrow \phi(\sigma \circ \tau) = (\sigma \circ \tau)|_M$
 $= (\sigma|_M) \circ (\tau|_M) = \phi(\sigma) \circ \phi(\tau)$

$\uparrow \tau(M) \subseteq M$

zu (2) Sei $\sigma \in \text{Gal}(M|K)$. Da $L|M$ algebraisch und
 L^{alg} alg abgeschlossen ist, existiert eine Fortsetzung

von $\sigma_1 \in \text{Hom}_K(M, L^{\text{alg}})$ zu einem K -Hom.

$$\sigma: L \rightarrow L^{\text{alg}} \quad L|K \text{ normal} \quad \sigma \in \text{Aut}_K(L) \Rightarrow$$

$\sigma \in G$. Da σ eine Fortsetzung von σ_1 ist, folgt $\phi(\sigma) = \sigma|_M = \sigma_1$.

zu (3) Sei $\sigma \in G$. Dann gilt die Äquivalenz

$$\sigma \in \ker(\phi) \Leftrightarrow \phi(\sigma) = \text{id}_M \Leftrightarrow \sigma|_M = \text{id}_M$$

$$\Leftrightarrow \sigma(\alpha) = \alpha \quad \forall \alpha \in M \Leftrightarrow \sigma \in \text{Gal}(L|M)$$

$$\Leftrightarrow \sigma \in U.$$



Anwendungsbeispiel 1: Zwischenkörper von $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$

- Überprüfe zunächst, ob L/K mit $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ eine endl. Galois-Erweiterung ist.

Beh. L ist Zerf.-korp. des Polynoms $f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ über $\mathbb{Q}$

Dies ist genau dann der Fall, wenn $L = \mathbb{Q}(N)$ mit

$N = \{\pm\sqrt{2}, \pm\sqrt{3}\}$ erfüllt ist. Offenbar gilt $N \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

und $\{\sqrt{2}, \sqrt{3}\} \subseteq \mathbb{Q}(N)$, also gilt $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(N)$

d.h. $L = \mathbb{Q}(N)$ ist erfüllt ($\Rightarrow$ Beh.)

Beh. $\Rightarrow L/K$ ist endl. alg. Erweiterung, außerdem normal.

$L|K$ algebraisch, das $K = \mathbb{Q} \rightarrow L|K$ ist separabel
insg. also $L|K$ ist endl. Galois-Erweiterung

Sei nun $G = \text{Gal}(L|K)$

- zeige: $[L:K] = 4$ (siehe Skript)

Daraus folgt $|G| = 4$. 4 ist Primzahlquadrat $\Rightarrow G$ ist abelsch
Hauptsatz über endl. erz. abelsche Gruppen $\rightarrow G \cong \mathbb{Z}/4\mathbb{Z}$
oder $G \cong (\mathbb{Z}/2\mathbb{Z})^2$

- Ang. $G \cong \mathbb{Z}/4\mathbb{Z}$, d.h. G ist zyklisch. Dann hätte G genau eine
Untergruppe der Ordnung 2. $|G| = 4 \rightarrow G$ hätte genau eine Untergr.
von Index 2. Aus der Galois-theorie würde folgen, dass L genau
einen Zwischenkörper M mit $[M:K] = 2$ hat. Aber $L|K$ hat mind.
zwei solche Zwischenkörper, nämlich $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$

- Also muss $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ gelten.

Die Gruppe $(\mathbb{Z}/2\mathbb{Z})^2$ hat genau drei Gruppen von Ordn. 2 (und Index 2), nämlich $\langle (\bar{1}, \bar{0}) \rangle$, $\langle (\bar{0}, \bar{1}) \rangle$ und $\langle (\bar{1}, \bar{1}) \rangle$. Wegen der Isomorphie gilt dasselbe für G . Wegen $|G| = 4$ gilt $|U| = 2$ für jede Untergr. U von G mit $\text{id}_L \notin U \subsetneq G$.

- Aus dem Hauptsatz der Galoistheorie folgt nun, dass $L|K$ genau drei echte Zwischenkörper besitzt. Zwei davon

sind $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, ein dritter ist $\mathbb{Q}(\sqrt{6})$
(da $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$). Da 2, 3, 6 verschiedene
quadratfreie Zahlen in $\mathbb{Z} \setminus \{0, 1\}$ sind, sind
 $\mathbb{Q}(\sqrt{d})$ für $d=2, 3, 6$ tatsächlich drei verschiedene
echte Zwischenkörper von $L|K$.

Ergebnis: $L|K$ hat genau fünf Zwischen-
körper, nämlich $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$ und
 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Bestimmung der Elemente von $G = \text{Gal}(L|K)$.

Jedes $\sigma \in G$ ist ein K -Automorphismus von L ,
muss also die Nullstelle $\sqrt{2}$ von $X^2 - 2 \in K[X]$

auf eine Nullstelle von $x^2 - 2$ abbilden, d.h.
es gilt $\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}$ ebenso: $\sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}$

Wegen $|G| = 4$ folgt daraus $G = \{id_L, \sigma, \tau, \sigma\tau\}$
wobei σ, τ durch $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ und
 $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$ festgelegt sind.

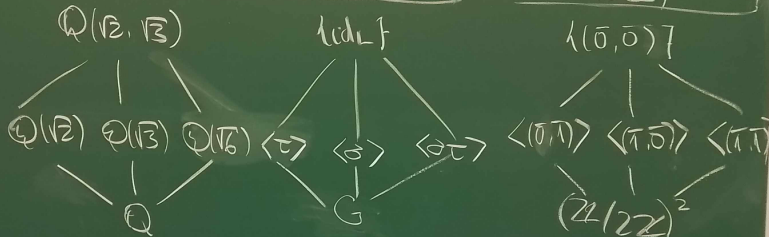
leicht zu sehen: Es gibt einen Isom. $(\mathbb{Z}/2\mathbb{Z})^2 \cong G$
mit $(1, 0) \mapsto \sigma$, $(0, 1) \mapsto \tau$, $(1, 1) \mapsto \sigma\tau$

Damit erhält man die folgenden Korrespondenzen:

Zwischenkörper
von L/K

Untergruppen
von $\text{Gal}(L/K)$

Untergruppen von
 $(\mathbb{Z}/2\mathbb{Z})^2$



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

$$\begin{aligned} \Rightarrow (\sigma \circ \tau)(\sqrt{6}) &= \sigma(\tau(\sqrt{2} \cdot \sqrt{3})) = \sigma(\tau(\sqrt{2}) \cdot \tau(\sqrt{3})) \\ &= \sigma(\sqrt{2} \cdot (-\sqrt{3})) = -\sigma(\sqrt{2} \cdot \sqrt{3}) = -\sigma(\sqrt{2}) \cdot \sigma(\sqrt{3}) \\ &= -(-\sqrt{2}) \cdot \sqrt{3} = \sqrt{2} \cdot \sqrt{3} = \sqrt{6} \Rightarrow \sqrt{6} \in L^{\langle \sigma \tau \rangle} \end{aligned}$$

Die Galoisgruppe eines Polynoms

Definition (22.7)

Sei K ein Körper und $f \in K[x]$ ein nicht-konstantes Polynom, dessen irreduzible Faktoren alle separabel sind, und sei L ein Zerfällungskörper von f über K . Dann bezeichnet man $\text{Gal}(L|K)$ auch als die Galoisgruppe $\text{Gal}(f|K)$ des Polynoms f .

Satz (22.8)

Sei $f \in K[x]$ ein Polynom wie in Def. 22.7 und L ein Zerfällungskörper von f über K . Seien $\alpha_1, \dots, \alpha_n \in L$ die verschiedenen Nullstellen von f in L . Dann gibt es einen injektiven Homomorphismus $\phi : \text{Gal}(f|K) \rightarrow S_n$ mit

$$\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)} \quad \text{für} \quad 1 \leq k \leq n.$$

Beispiel: Anwendung von Satz 22.8 auf die
Galois-Erweiterung $L|K$ aus dem Beispiel oben

Es gilt $\text{Gal}(L|K) = \text{Gal}(f|K)$ mit dem
Polynom $f = (x^2 - 2)(x^2 - 3)$. Die Nullstellen von diesem
Polynom sind $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$.

$$\sigma(\alpha_1) = \sigma(\sqrt{2}) = -\sqrt{2} = \alpha_2, \quad \sigma(\alpha_2) = \sigma(-\sqrt{2}) = -\sigma(\sqrt{2}) \\ = -(-\sqrt{2}) = \sqrt{2} = \alpha_1, \quad \sigma(\alpha_3) = \alpha_3, \quad \sigma(\alpha_4) = \alpha_4$$

$$\Rightarrow \sigma \text{ entspricht der Permutation } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$$

Ebenso zeigt man, dass τ dem Element (34) ent-

$$\sigma(\alpha_1) = \sigma(\sqrt{2}) = -\sqrt{2} = \alpha_2, \quad \sigma(\alpha_2) = \sigma(-\sqrt{2}) = -\sigma(\sqrt{2})$$

spricht, und damit entspricht $\sigma\tau$ dem Element $(12)(34)$

Das Diagramm der Untergruppen von $G = \text{Gal}(L/K)$ entspricht also dem folgenden Untergruppen diagramm in S_4 .

