Der Hauptsatz der Galoistheorie

Satz (21.7)

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

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

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

Ergänzungen zum Hauptsatz der Galoistheorie

Satz (21.8)

(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 $\mathrm{Gal}(L|M_1) \supseteq \mathrm{Gal}(L|M_2)$.

(iii) Es gilt $L^{\{\mathrm{id}_L\}} = L$, $L^G = K$ und $\mathrm{Gal}(L|L) = \{\mathrm{id}_L\}$, $\mathrm{Gal}(L|K) = G$.

(iv) Ist M ein Zwischenkörper und $U = \mathrm{Gal}(L|M)$ die zugehörige Untergruppe, dann gilt $[L : M] = |U|$ und $[M : K] = (G : U)$.

Normalteiler und normale Teilerweiterungen

Proposition (21.9)

Sei M ein Zwischenkörper von $L|K$ und $U = \mathrm{Gal}(L|M)$ die zugehörige Untergruppe von $G = \mathrm{Gal}(L|K)$. 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 $G \to \mathrm{Gal}(M|K)$, und diese induziert einen natürlichen Isomorphismus $G/U \cong \mathrm{Gal}(M|K)$.

Die Galoisgruppe eines Polynoms

Definition (21.10)

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 $\mathrm{Gal}(L|K)$ auch als die Galoisgruppe $\mathrm{Gal}(f|K)$ des Polynoms f.

Galoisgruppen als Untergruppen von symm. Gruppen

Satz (21.11)

Sei $f \in K[x]$ ein Polynom wie in Def. (21.10) und L ein Zerfällungskörper von f über K. Seien $\alpha_1, ..., \alpha_n \in L$ die verschiedenen Nullstellen von f in L. Dann gibt es einen injektiven Homomorphismus $\phi : \mathrm{Gal}(f|K) \to S_n$ mit $\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)}$ für $1 \leq k \leq n$.

Beweis von Satz 21.11:

$f \in K[x]$ nicht-konstant mit irred. sep. Faktoren, L Zerf.-Körp. von f über K

$\Rightarrow L|K$ ist Galois-Erw., sei $G = Gal(L|K)$

Sei $n \in \mathbb{N}$ die Anzahl der verschiedenen Nullstellen von f in K und $S = \{\alpha_1, \dots, \alpha_n\} \subseteq L$ die Menge der Nullstellen.

Beh.: Es gibt einen injektiven Gruppenhom.

$\phi : G \to S_n$ mit $\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)}$ für (*)

alle $\sigma \in G$ und $1 \le k \le n$.

- Für jedes $\sigma \in G$ gilt $\sigma|_S \in \mathrm{Per}(S)$, denn:
  Da σ als K-Aut. von L jede Nullstelle von f auf eine Nullst. von f abbildet, gilt $\sigma(S) \subseteq S$
  σ ist injektiv (als Aut.) $\Rightarrow \sigma|_S$ ist inj. Abbildung $S \to S$ $\overset{|S| \text{ endlich}}{\Rightarrow}$ $\sigma|_S : S \to S$ ist bijektiv
- Für alle $\sigma, \tau \in G$ gilt $(\sigma \circ \tau)|_S = (\sigma|_S) \circ (\tau|_S)$.
  Durch $\phi_1 : G \to \mathrm{Per}(S)$, $\sigma \mapsto \sigma|_S$ ist also ein Gruppenhom. definiert. Dieser ist <u>injektiv</u>, denn: Sei $\sigma \in \ker(\phi_1) \Rightarrow \sigma|_S = \mathrm{id}_S$
  $\Rightarrow \sigma(\alpha) = \alpha \ \forall \alpha \in S \overset{L = K(S)}{\Rightarrow} \sigma = \mathrm{id}_L$
- Bekannt aus der Gruppentheorie:

Die Bijektion $L: \mathbb{M}_n \to S,\ k \mapsto \alpha_k$ liefert einen Isom. $\Psi: S_n \to \mathrm{Per}(S)$, die definiert ist durch $\Psi(\sigma) = L \circ \sigma \circ L^{-1}\ \forall \sigma \in S_n$

$$\left[S \xrightarrow{L^{-1}} \mathbb{M}_n \xrightarrow{\sigma} \mathbb{M}_n \xrightarrow{L} S\right]$$

$\Rightarrow \phi = \Psi^{-1} \circ \phi_1$ ist injektive Gruppenhom. von G nach S_n

- Nachweis von (*): Sei $\sigma \in G$ und $k \in \mathbb{M}_n$. Sei $l \in \mathbb{M}_n$ geg. durch $\sigma(\alpha_k) = \alpha_l$. z.zg. $l = \phi(\sigma)(k)$ Tatsächlich gilt

$$\phi(\sigma)(k) = (\Psi^{-1} \circ \phi_1)(\sigma)(k) = \Psi^{-1}(\sigma|_S)(k) = (L^{-1} \circ (\sigma|_S) \circ L)(k)$$

$= (\iota^{-1} \circ (\partial|_S))(\alpha_k) = \iota^{-1}(\alpha_1) = l$ $\square$

Klausurtermin: Di. 21. Juli, $9^{30} - 10^{30}$

Beispiel: Galoisgruppe von $f = x^3 - 2 \in \mathbb{Q}[x]$

Sei $\alpha = \sqrt[3]{2}$, $\delta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Nullstellen von f in $\mathbb{C}$: $\alpha_1 = \alpha$, $\alpha_2 = \delta\alpha$, $\alpha_3 = \delta^2\alpha$

Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$:

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha, \delta)$$

bereits bekannt: $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, $[L : \mathbb{Q}(\alpha)] = 2$

$$\Rightarrow |G| = [L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Das Polynom f ist irreduzibel über $\mathbb{Q}(\delta)$, denn:

$\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-3}) \Rightarrow [\mathbb{Q}(\beta):\mathbb{Q}] = 2$ (da $-3 \in 2\mathbb{Z}+1 \setminus 0, 1$ quadratfrei) Ang. f ist reduzibel über $\mathbb{Q}(\beta)$ $\Rightarrow$ $M_{\alpha,\mathbb{Q}(\beta)}$ ist echter Teiler von f $\Rightarrow$ $[L:\mathbb{Q}] = [L:\mathbb{Q}(\beta)] \cdot$ $[\mathbb{Q}(\beta):\mathbb{Q}] = \operatorname{grad}(M_{\alpha,\mathbb{Q}(\beta)}) \cdot 2 < 3 \cdot 2 = 6$ ↯

außerdem: $\alpha, \beta\alpha$ sind Nullstellen von f in L $\Rightarrow$

$\exists \sigma \in \operatorname{Gal}(L|\mathbb{Q}(\beta))$ mit $\sigma(\alpha) = \beta\alpha$ $\Rightarrow$ $\sigma \in G$, $\sigma(\alpha) = \beta\alpha$, und $\sigma(\beta) = \beta$

Es gilt $\sigma(\alpha_1) = \sigma(\alpha) = \beta\alpha = \alpha_2$, $\sigma(\alpha_2) = \sigma(\beta\alpha) =$

$\sigma(\beta)\sigma(\alpha) = \beta(\beta\alpha) = \beta^2\alpha = \alpha_3$, $\sigma(\alpha_3) = \sigma(\beta^2\alpha) =$

$\sigma(\beta)^2\sigma(\alpha) = \beta^2(\beta\alpha) = \beta^3\alpha = 1 \cdot \alpha = \alpha = \alpha_1$

$\Rightarrow \sigma$ entspricht dem Element $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \in S_3$

Ebenso liefert die Anwendung des Fortsetzungssatzes ein $\tau \in G$ mit $\tau(\alpha) = \alpha$, $\tau(\sigma) = \sigma^2$

$\tau(\alpha_1) = \tau(\alpha) = \alpha = \alpha_1$, $\tau(\alpha_2) = \tau(\sigma\alpha) =$

$\tau(\sigma)\tau(\alpha) = \sigma^2\alpha = \alpha_3$, $\tau(\alpha_3) = \tau(\sigma^2\alpha) =$

$\tau(\sigma)^2\tau(\alpha) = (\sigma^3)^2\alpha = \sigma^4\alpha = \sigma\alpha = \alpha_2$
$\uparrow \sigma^3 = 1$

$\Rightarrow \tau$ entspricht dem Element $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$ in S_3

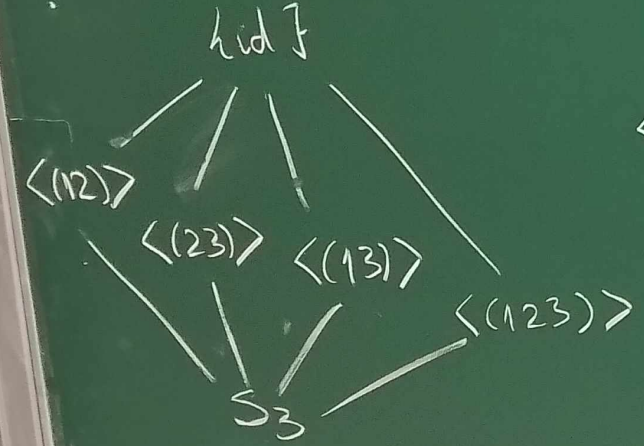
Nach Satz 21.11 ist G isomorph zu einer 6-elementigen Untergr. von S_3 $\xRightarrow{|S_3| = 6}$

$G \cong S_3$

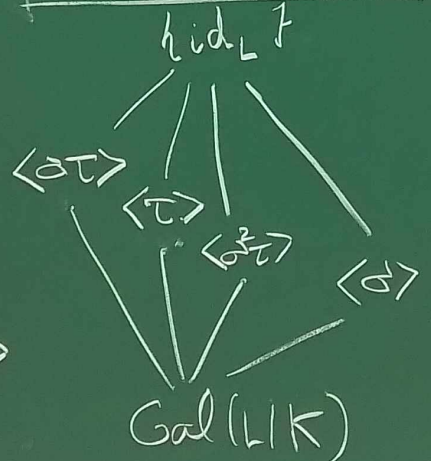
Sei $\alpha = \sqrt[3]{2}$, $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha, \zeta)$.

Bereits gesehen: $G = \mathrm{Gal}(L|K)$ ist gegeben durch $\langle \sigma, \tau \rangle$, wobei $\sigma(\alpha) = \zeta\alpha$, $\sigma(\zeta) = \zeta$ bzw. $\tau(\alpha) = \alpha$, $\tau(\zeta) = \zeta^2$.

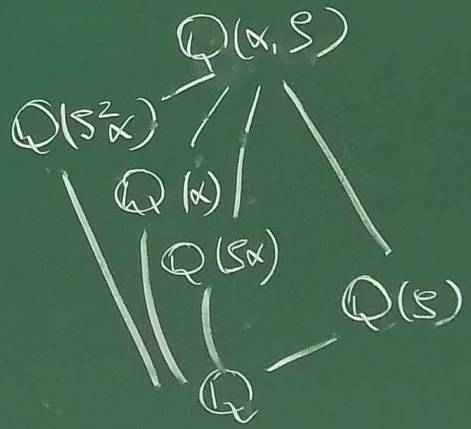
Untergruppen von S_3



Untergruppen von G



Zwischenkörper von $L|K$



$(\sigma\tau)(\alpha_1) = \sigma(\tau(\alpha_1)) = \sigma(\alpha_1) = \alpha_2$

$(\sigma\tau)(\alpha_2) = \sigma(\tau(\alpha_2)) = \sigma(\alpha_3) = \alpha_1$

$(\sigma\tau)(\alpha_3) = \sigma(\tau(\alpha_3)) = \sigma(\alpha_2) = \alpha_3$

$\Rightarrow \sigma\tau$ entspricht dem Element $(12) \in S_3$

Frage: Sind die Zwischenkörper im Diagramm rechts wirklich alle verschieden?

$[\mathbb{Q}:\mathbb{Q}] = 1$, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6$, $[\mathbb{Q}(\beta):\mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}):\mathbb{Q}] = 2$,

$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\beta\alpha):\mathbb{Q}] = [\mathbb{Q}(\beta^2\alpha):\mathbb{Q}] = 3$

$\Rightarrow$ nur Übereinstimmungen zwischen $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta\alpha)$, $\mathbb{Q}(\beta^2\alpha)$ möglich

aber: $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, aber $\mathbb{Q}(\beta\alpha), \mathbb{Q}(\beta^2\alpha) \not\subseteq \mathbb{R}$

$\Rightarrow$ nur $\mathbb{Q}(\beta\alpha) = \mathbb{Q}(\beta^2\alpha)$ möglich

aber: Angenommen $\mathbb{Q}(\beta\alpha) = \mathbb{Q}(\beta^2\alpha)$.

$\Rightarrow \beta\alpha, \beta^2\alpha \in \mathbb{Q}(\beta\alpha) \Rightarrow \beta = \frac{\beta^2\alpha}{\beta\alpha} \in \mathbb{Q}(\beta\alpha)$

$\Rightarrow \frac{\beta\alpha}{\beta} = \alpha \in \mathbb{Q}(\beta\alpha)$ msg.: $[\alpha, \beta] \leq$

$\mathbb{Q}(\beta\alpha) \Rightarrow \mathbb{Q}(\alpha, \beta) \leq \mathbb{Q}(\alpha\beta) \Rightarrow$

$\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha, \beta)$ ↯ da $[\mathbb{Q}(\beta\alpha) : \mathbb{Q}]$

$= 3$ und $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$

Der Frobenius-Automorphismus endlicher Körper

Erinnerung: Sei p eine Primzahl.

- Für jeden Ring R mit $\mathrm{char}(R) = p$ ist durch $x \mapsto x^p$ ein Endomorphismus von R gegeben, der sog. Frobenius-Endomorphismus.
- Ist K darüber hinaus ein endlicher Körper, dann ist dieser Endomorphismus auf K sogar ein Automorphismus.

Sei nun $r \in \mathbb{N}$ und $q = p^r$.

Definition (22.1)

Sei $n \in \mathbb{N}$ und φ der Frobenius-Automorphismus von $\mathbb{F}_{q^n}$. Dann bezeichnen wir $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q} = \varphi^r$ als den Frobenius-Automorphismus der Körpererweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$.

Bem. Sei p eine Primzahl, und seien $r, n \in \mathbb{N}$. Setze $q = p^r$. zur Erinnerung:
Der Körper $\mathbb{F}_q$ ist nach Def. des eindeutig bestimmte Zwischenkörper von $\mathbb{F}_p^{alg} \mid \mathbb{F}_p$ mit q Elementen.
Sei φ der Frobenius-Automorphismus von $\mathbb{F}_{q^n}$ geg. durch $\varphi(\alpha) = \alpha^p \quad \forall \alpha \in \mathbb{F}_{q^n}$.
Setze $\varphi_{\mathbb{F}_{q^n} \mid \mathbb{F}_q} = \varphi^r$. Dann gilt $\varphi_{\mathbb{F}_{q^n} \mid \mathbb{F}_q}(\alpha)$
$= \varphi^r(\alpha) = \alpha^{p^r} = \alpha^q$ für alle $\alpha \in \mathbb{F}_{q^n}$.
Daher gilt $\varphi_{\mathbb{F}_{q^n} \mid \mathbb{F}_q}(\alpha) = \alpha \quad \forall \alpha \in \mathbb{F}_q$

(Grund: Die Elemente von $\mathbb{F}_q$ sind genau die Nullstellen von $x^q - x$ in $\mathbb{F}_p^{alg}$, erfüllen also $x^q = x$). Also ist $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ ein $\mathbb{F}_q$-Automorphismus von $\mathbb{F}_{q^n}|\mathbb{F}_q$.

Satz (22.2)

Sei $n \in \mathbb{N}$.

(i) Die Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ ist eine Galois-Erweiterung.

(ii) Die Galois-Gruppe $G = \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ wird vom Frobenius-Automorphismus $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ der Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ erzeugt.

(iii) Durch $\mathbb{Z}/n\mathbb{Z} \to G$, $a + n\mathbb{Z} \mapsto \varphi^a_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ ist ein Isomorphismus von Gruppen definiert.

p beliebige Primzahl, $\varphi = \varphi_{\mathbb{F}_{p^6}|\mathbb{F}_p}$

Untergruppen von $(\mathbb{Z}/6\mathbb{Z}, +)$	Untergruppen von $\mathrm{Gal}(\mathbb{F}_{p^6}|\mathbb{F}_p)$	Zwischenkörper von $\mathbb{F}_{p^6}|\mathbb{F}_p$
$\{\bar{0}\}$	$\{\mathrm{id}_{\mathbb{F}_{p^6}}\}$	$\mathbb{F}_{p^6}$
$\langle\bar{3}\rangle$	$\langle\varphi^3\rangle$	$\mathbb{F}_{p^3}$
$\langle\bar{2}\rangle$	$\langle\varphi^2\rangle$	$\mathbb{F}_{p^2}$
$\mathbb{Z}/6\mathbb{Z}$	$\langle\varphi\rangle$	$\mathbb{F}_p$