7 Galoistheorie

$\bar{L}$ = alg. Abschluss von L
= " " " K.

Die Galoistheorie besteht darin, Körpererweiterungen L/K via ihrer Symmetrien, das heisst, via der Gruppe $\mathrm{Aut}_K(L)$ zu studieren.

7.1 Galoiserweiterungen

7.1.1 Definition: Eine separable normale algebraische Körpererweiterung L/K nennt man *galoissch* oder eine *Galoiserweiterung*. Die zugehörige Gruppe $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ nennt man dann die *Galoisgruppe von* L/K.

7.1.2 Proposition: Eine endliche Erweiterung L/K ist galoissch genau dann, wenn $|\mathrm{Aut}_K(L)| = [L/K]$ ist. Dann ist also $\mathrm{Gal}(L/K)$ eine endliche Gruppe der Ordnung $[L/K]$.

Beweis: L/K separabel $\Leftrightarrow |\mathrm{Hom}_K(L,\bar{L})| = |[L/K]|$

L/K normal $\Leftrightarrow \mathrm{Hom}_K(L,\bar{L}) = \mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$

Immerhin $|\mathrm{Hom}_K(L,\bar{L})| \leq [L/K]$.

und $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\bar{L})$

Ägyptisch: " $\geq$ ".

qed.

7.1.3 Beispiel: Jede Erweiterung von endlichen Körpern ℓ/k ist endlich galoissch mit zyklischer Galoisgruppe $\langle \mathrm{Frob}_{|k|} \,|\, \ell \rangle$ der Ordnung $[\ell/k]$.

$\mathrm{Aut}_k(\ell) = \langle \mathrm{Frob}_q \rangle$ für $q = |k|$.

7.1.4 Proposition-Definition: Sei L ein Körper und Γ eine Untergruppe von $\mathrm{Aut}(L)$. Dann ist

$$L^\Gamma := \{a \in L \mid \forall \gamma \in \Gamma : \gamma(a) = a\}$$

ein Unterkörper von L, genannt der *Fixkörper von* Γ.

Beweis: $0, 1 \in L^\Gamma$, denn da $a, b \in L^\Gamma$ ist $a \pm b, ab, \frac{a}{b} \in L^\Gamma$, denn $\forall \gamma \in \Gamma : \gamma(a \pm b) = \gamma(a) \pm \gamma(b) = a \pm b$. etc. qed.

7.1.5 Satz: Für jede endliche Untergruppe $\Gamma < \mathrm{Aut}(L)$ ist L/L^Γ endlich galoissch mit Galoisgruppe Γ.

Beweis: $\Gamma < \mathrm{Aut}_{L^\Gamma}(L)$. Es genügt also zu zeigen, dass $[L/L^\Gamma] = |\Gamma|$. Sehe $K := L^\Gamma$.

(1) Sei $a \in L$. Sehe $A := \{\gamma(a) \mid \gamma \in \Gamma\}$ und dann $f(X) := \prod_{a' \in A} (X - a')$. Dann ist $f \in K[X]$.

A Bahn unter Γ.

Wegen $f \neq 0$ und $f(a) = 0$ folgt a algebraisch vom Grad $\leq |A| \leq |\Gamma|$ über K.

Für alle $\gamma \in \Gamma$ ist $\gamma(f) = f$.

(2) Da f in $L[X]$ in Linearfaktoren zerfällt, enthält L einen Zerfällungskörper von f. Das Minimalpolynom von a über K ist ein Teiler von $f \Rightarrow$ separabel.

Somit L/K algebraisch und normal und separabel $\Rightarrow$ galois!

(3) Beh.: Für jeden Zwischenkörper $K \subset K' \subset L$ mit K'/K endlich ist $[K'/K] \leq |\Gamma|$.

Beweis: L/K separabel $\Rightarrow K'/K$ endlich separabel $\Rightarrow \exists a \in L : K' = K(a)$.

$\Rightarrow [K'/K] \leq |\Gamma|$ nach (1). qed.

(4) Beh. $[L/K] \leq |\Gamma|$. $\gamma(f) = \prod_{a' \in A} (X - \gamma(a')) = \prod_{a' \in A} (X - a') = f$.

Schreibe $f(X) = \sum_i b_i X^i$. $\Rightarrow \forall \gamma \in \Gamma : \gamma(f(X)) = \sum_i \gamma(b_i) X^i$. $\Rightarrow \forall i : \gamma(b_i) = b_i$, also $b_i \in K$.

Beh.: Sei K'/K endlich, $K' \subset L$, mit $[K'/K]$ maximal. (Existiert nach ③)

Sei $a \in L \Rightarrow K'(a)/K$ endlich $\Rightarrow [K'(a)/K] = [K'/K] < \infty$

$\Rightarrow K'(a) = K'$. Also $a \in K' \Rightarrow K' = L$. qed.

④ Also L/K endlich, $|\mathrm{Aut}_K(L)| \geq |\Gamma| \geq [L/K] \Rightarrow |\mathrm{Aut}_K(L)| = [L/K]$.

qed.

7.1.6 Proposition: Für jede Galoiserweiterung L/K und jeden Zwischenkörper K' ist auch L/K' galoissch, und $\mathrm{Gal}(L/K')$ ist eine Untergruppe von $\mathrm{Gal}(L/K)$.

Bew.: L/K separabel $\Rightarrow$ L/K' separabel. L/K normal $\Rightarrow$ L/K' normal $\Big\} \Rightarrow L/K'$ galoissch.

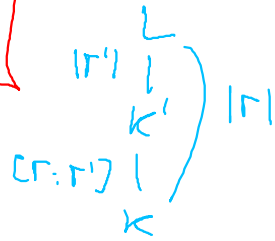
L
|
K'
|
K

$\mathrm{Gal}(L/K') = \mathrm{Aut}_{K'}(L) < \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$. geht.

7.2 Galoiskorrespondenz

7.2.1 Hauptsatz der Galoistheorie: Sei L/K endlich galoissch mit Galoisgruppe Γ. Dann haben wir natürliche zueinander inverse Bijektionen

$$\begin{array}{ccc} \{\text{Zwischenkörper von } L/K\} & \underset{\sim}{\rightleftarrows} & \{\text{Untergruppen von } \Gamma\} \\ K' & \longmapsto & \mathrm{Gal}(L/K') \\ L^{\Gamma'} & \longmapsfrom & \Gamma' \end{array}$$



Weiter gilt für beliebige einander entsprechende $K' \leftrightsquigarrow \Gamma'$ und $K'' \leftrightsquigarrow \Gamma''$:

(a) $[L/K'] = |\Gamma'|$ und $[K'/K] = [\Gamma : \Gamma']$.

(b) $K' \subset K'' \iff \Gamma' > \Gamma''$. inklusionsumkehrend!

(c) Für jedes $\gamma \in \Gamma$ entspricht der Zwischenkörper $\gamma(K')$ der Untergruppe ${}^{\gamma}\Gamma'$.

(d) Es existiert ein natürlicher Isomorphismus

$$\mathrm{Norm}_\Gamma(\Gamma')/\Gamma' \xrightarrow{\sim} \mathrm{Aut}_K(K'),\ \gamma\Gamma' \mapsto \gamma|_{K'}.$$

(e) K'/K ist galoissch genau dann, wenn Γ' normal in Γ ist, und dann ist die Abbildung in (d) ein natürlicher Isomorphismus

$$\Gamma/\Gamma' \xrightarrow{\sim} \mathrm{Gal}(K'/K).$$

Beweis: Zu $\Gamma' < \Gamma$ sehe $K' := L^{\Gamma'}$. Dann ist L/K' galoissch mit $\mathrm{Gal}(L/K') = \Gamma'$ nach 7.1.5. Also ist $\Gamma' \mapsto K'$ die Identität.

Zu K' Zwischenkörper setze $\Gamma' := \mathrm{Gal}(L/K')$. Dann ist $K' \subset L^{\Gamma'}$ und $[L/K'] = |\Gamma'| = [L/L^{\Gamma'}]$.

$\Rightarrow [L^{\Gamma'}/K'] = 1 \Rightarrow L^{\Gamma'} = K'$. Also ist $K' \mapsto \Gamma'$ die Identität.

(a) $[L/K'] = |\Gamma'|$ o.B.d.A. und $\underbrace{[L/K']}_{=|\Gamma'|} \cdot [K'/K] = [L/K] = |\Gamma| = |\Gamma'| \cdot [\Gamma : \Gamma']$.

$\Rightarrow [K'/K] = [\Gamma : \Gamma']$.

(b) $K' \subset K'' \Rightarrow \Gamma' = \mathrm{Aut}(L/K') \geq \mathrm{Aut}(L/K'') = \Gamma''$

$\Gamma' \geq \Gamma'' \Rightarrow K' = L^{\Gamma'} \subset L^{\Gamma''} = K''$.

(c) Für alle $\delta \in \Gamma$ gilt:

$\delta \in \Gamma' \iff \delta|_{K'} = \mathrm{id} \iff \forall x \in K' : \delta(x) = x \iff \forall x \in K' : \gamma\delta\gamma^{-1}(\gamma(x)) = \gamma(x)$

$\iff \gamma\delta\gamma^{-1}|_{\gamma(K')} = \mathrm{id} \iff \gamma\delta\gamma^{-1} \in \mathrm{Gal}(L/\gamma(K'))$.

Also ist $\mathrm{Gal}(L/\gamma(K')) = \gamma\Gamma'\gamma^{-1} = {}^{\gamma}\Gamma'$.

(d) Für jedes $\gamma \in \Gamma$ entspricht $\gamma(K')$ der Untergruppe ${}^{\gamma}\Gamma'$ nach (c).

Also ist $\gamma(K') = K' \iff {}^{\gamma}\Gamma' = \Gamma' \iff \gamma \in N_\Gamma(\Gamma')$.

$\rightsquigarrow$ natürlicher Homo $N_\Gamma(\Gamma') \longrightarrow \mathrm{Aut}_K(K')$, $\gamma \mapsto \gamma|_{K'}$.

Dabei ist $\gamma|_{K'} = \mathrm{id} \iff \gamma \in \mathrm{Aut}_{K'}(L) = \Gamma'$. Also ist der Kern gleich Γ'

$\Rightarrow$ injektiver Homo $N_\Gamma(\Gamma')/\Gamma' \hookrightarrow \mathrm{Aut}_K(K')$.

Sei $\tau \in \mathrm{Aut}_K(K')$. Dann existiert ein Fortsetzung $\gamma \in \mathrm{Hom}_K(L, \bar{L})$.

L/K normal $\Rightarrow \gamma(L) = L$. $\Rightarrow \gamma \in \mathrm{Aut}_K(L) = \Gamma$ mit $\gamma|_{K'} = \tau$.

Wegen $\gamma(K') = K'$ ist $\gamma \in N_\Gamma(\Gamma')$. Also ist der Homo surjektiv.

(e) K/K' galois $\iff |\mathrm{Aut}_K(K')| = [K'/K]$

(d) $[N_\Gamma(\Gamma') : \Gamma']$ (a) $[\Gamma : \Gamma']$

$\iff N_\Gamma(\Gamma') = \Gamma \iff \Gamma' \trianglelefteq \Gamma$.

Rest Spezialfall von (d).

qed.

K'/K

7.2.2 Satz: Jede endliche separable Erweiterung hat nur endlich viele Zwischenkörper.

Bem.: Sei K'/K endlich separabel, und L/K' eine normale Hülle über K.
$\Rightarrow L/K$ endlich, normal, separabel.
$\Rightarrow L/K$ galoissch

7.2.1 $\Rightarrow L/K$ hat nur endlich viele Zwischenkörper.
$\Rightarrow K'/K$ also. qed.

L
$|$
K'
$|$
K

K' K'

7.2.3 Bemerkung: Jedes Element von L, das in keinem von K verschiedenen Zwischenkörper liegt, ist ein primitives Element von ~~L/K~~ K'/K.

$*$ $\forall \gamma, \delta \in \Gamma: \gamma\delta(a_i) = \gamma(\delta(a_i))$
$\gamma\delta(a_i) = a_{\gamma\delta(i)}$, $\gamma(\delta(a_i)) = \gamma(a_{\delta(i)}) = a_{\gamma(\delta(i))}$
$\Downarrow$
$\gamma\delta(i) = \gamma(\delta(i))$

Sei nun $f \in K[X]$ ein separables Polynom vom Grad $n \geqslant 0$. Seien $a_1, \ldots, a_n$ die Nullstellen von f in einem Zerfällungskörper $L = K(a_1, \ldots, a_n)$ von f über K. Dann ist L/K galoissch, und wir nennen seine Galoisgruppe $\mathrm{Gal}(L/K)$ auch die *Galoisgruppe von f über K*.

7.2.4 Proposition: Es existiert eine eindeutige Linksoperation von Γ auf $\{1, \ldots, n\}$ mit der Eigenschaft

$$\forall \gamma \in \mathrm{Gal}(L/K)\ \forall 1 \leqslant i \leqslant n\colon\ \gamma(a_i) = a_{\gamma i}.$$

Diese ist treu, entspricht also einem injektiven Homomorphismus $\mathrm{Gal}(L/K) \hookrightarrow S_n$.

Dadurch können wir $\mathrm{Gal}(L/K)$ mit einer Untergruppe von S_n identifizieren. Die Identifikation hängt allerdings von der gewählten Reihenfolge der Nullstellen ab. Jede andere Reihenfolge hat die Form $a_{\sigma 1}, \ldots, a_{\sigma n}$ für eine Permutation $\sigma \in S_n$, und die Umordnung ändert den Homomorphismus ab um den inneren Automorphismus int_σ von S_n und sein Bild somit um Konjugation mit σ.

7.2.5 Proposition: Die Bahnen der Operation von $\mathrm{Gal}(L/K)$ auf $\{1, \ldots, n\}$ entsprechen genau den normierten irreduziblen Faktoren von f in $K[X]$. Insbesondere ist die Operation transitiv genau dann, wenn f irreduzibel ist.