Ad § 6.2: Galoiskorrespondenz

<u>Hauptsatz der Galoistheorie</u>: Sei L/K endlich galoisch mit Galoisgruppe Γ. Dann gibt es natürliche zueinander inverse Bijektionen

$$\{\text{Zwischenkörper von } L/K\} \rightleftarrows \{\text{Untergruppen von } \Gamma\}$$

$$K' \longmapsto \mathrm{Gal}(L/K')$$

$$L^{\Gamma'} \longleftarrow\!\shortmid \ \Gamma'$$

Weiter gilt für beliebige einander entsprechende K' aus Γ' und K'' aus Γ'':

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

(b) $K' \subset K'' \iff \Gamma' \supset \Gamma''$.

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

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

(e) K'/K galoisch genau, wenn $\Gamma' \triangleleft \Gamma$ und dann ist (d) ein natürlicher Iso $\Gamma/\Gamma' \xrightarrow{\sim} \mathrm{Gal}(K'/K)$.

<u>Beweis</u>: Ist $\Gamma' < \Gamma$ gegeben, setze $K' := L^{\Gamma'}$. Nach § 6.1 ist dann L/K' galoisch mit $\mathrm{Gal}(L/K') = \Gamma'$. Also ist $\circlearrowleft$ die Identität.

Ist $K' \subset L$ gegeben, setze $\Gamma' := \mathrm{Gal}(L/K')$. Dann ist $K' \subset L^{\Gamma'}$.

Andererseits gilt $[L/K'] \underset{\text{da } L/K' \text{ galoisch}}{=} |\Gamma'| \underset{\text{nach § 6.1}}{=} [L/L^{\Gamma'}]$.

Also gilt $K' = L^{\Gamma'}$. Dies zeigt dann $\circlearrowleft$ die Identität ist.

(a) Wir wissen schon $[L/K'] = |\Gamma'|$, und daraus folgt

$$[K'/K] = \frac{[L/K]}{[L/K']} = \frac{|\Gamma|}{|\Gamma'|} = [\Gamma : \Gamma'].$$

(b) folgt direkt aus der Definition der Abbildungen.

(c) Für alle $\delta \in \Gamma$ gilt

$$\begin{aligned} \delta \in \Gamma' = \mathrm{Gal}(L/K') &\iff \delta|_{K'} = id \\ &\iff \gamma\delta\gamma^{-1}|_{\gamma(K')} = id \\ &\iff \gamma\delta\gamma^{-1} \in \mathrm{Gal}(L/\gamma(K')) \end{aligned}$$

(d) Nach (c) gilt für jedes $\gamma\in\Gamma$: $\left\{\begin{matrix} K' \text{ entspricht } \Gamma' \\ \gamma(K') \text{ entspricht } {}^{\gamma}\Gamma' \end{matrix}\right\}$.

Also gilt $\gamma(K')=K' \iff {}^{\gamma}\Gamma'=\Gamma' \iff \gamma\in \mathrm{Norm}_\Gamma(\Gamma')$.

Somit haben wir eine wohldefinierte Abbildung

$$\mathrm{Norm}_\Gamma(\Gamma') \longrightarrow \mathrm{Aut}_K(K'),\quad \gamma\mapsto \gamma|K'.$$

Dies ist offenbar ein Gruppenhomomorphismus. Weiter gilt

$\gamma\in\mathrm{Ker} \iff \gamma|K'=\mathrm{id} \iff \gamma\in \mathrm{Gal}(L/K')=\Gamma'$.

Somit faktorisiert der Homomorphismus durch einen injektiven Homo

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

Betrachte $\varphi\in\mathrm{Aut}_K(K')$. Sei $\bar{L}$ ein algebraischer Abschluss von L. Dann besitzt φ eine Fortsetzung $\psi\in\mathrm{Hom}_K(L,\bar{L})$. Da L/K normal ist, gilt $\psi(L)=L$, also $\psi\in\mathrm{Gal}(L/K)=\Gamma$ mit $\psi|K'=\varphi$. Daher ist der obige Homo surjektiv.

$$\begin{tikzcd}
& \bar{L} \arrow[d, dash] \\
L \arrow[ur, dashed, "\psi"] \arrow[d, dash] & L \arrow[d, dash] \\
K' \arrow[r, "\sim", "\varphi"'] \arrow[dr, dash] & K' \arrow[d, dash] \\
& K
\end{tikzcd}$$

(e) Es ist K'/K galoisch $\iff |\mathrm{Aut}_K(K')| = [K':K]$

$$\begin{aligned}
&\qquad\ \ \overset{(d)}{\|} \qquad\qquad\qquad \overset{(a)}{\|}\\
&[\mathrm{Norm}_\Gamma(\Gamma'):\Gamma'] \quad [\Gamma:\Gamma']\\
\iff\ & \mathrm{Norm}_\Gamma(\Gamma') = \Gamma\\
\iff\ & \Gamma' \lhd \Gamma.
\end{aligned}$$

Der Rest folgt aus (d). qed.

Folge: Jede endliche separable Erweiterung L/K besitzt nur endlich viele Zwischenkörper.

Beweis: Sei N/K eine normale Hülle von L/K. Dann ist N/K endlich galoisch. Nach dem Hauptsatz haben wir dann eine natürliche Bijektion

$$\left\{\begin{matrix}\text{Zwischenkörper}\\ K\subset K'\subset L\end{matrix}\right\} \xleftrightarrow{1:1} \left\{\begin{matrix}\text{Untergruppen}\\ \mathrm{Gal}(N/L)<\Gamma'<\mathrm{Gal}(N/K)\end{matrix}\right\}.$$

Aber rechts gibt es nur endlich viele. qed.

Folge: Jedes Element von L, welches in keinem dieser endlich vielen Zwischenkörper $K\subset K'\subsetneq L$ liegt, ist ein primitives Element von L/K.

Sei nun $f\in K[X]$ separabel vom Grad n mit den Nullstellen $a_1,\dots,a_n \in K(a_1,\dots,a_n)=L$. Betrachte die Linksoperation von $\Gamma := \mathrm{Gal}(L/K)$ auf $\{1,\dots,n\}$ durch $\gamma(a_i) := a_{\gamma i}$.

Prop.: Die Bahnen dieser Operation entsprechen genau den normierten irreduziblen Faktoren von f in $K[X]$. Insbesondere ist die Operation transitiv g.d.w. f irreduzibel ist.

Beweis: Für jede Teilmenge $A\subset\{1,\dots,n\}$ setze $f_A(X) := \prod_{i\in A}(X-a_i) \in L[X]$. Für alle $\gamma\in\Gamma$ rechnen wir

$$\gamma f_A(X) = \prod_{i\in A}(X-\gamma(a_i)) = \prod_{i\in A}(X-a_{\gamma i}) = f_{\gamma(A)}(X).$$

Also gilt $f_A(X)\in K[X] \iff \forall\gamma\in\Gamma: \gamma f_A = f_A$
$\iff \forall \gamma\in\Gamma: \gamma(A)=A$.

Also entsprechen die normierten Faktoren von f_A in $K[X]$ genau den Γ-invarianten Teilmengen von $\{1,\dots,n\}$. Die irred. Faktoren entsprechen folglich den minimalen nichtleeren Γ-invarianten Teilmengen, also den Bahnen.

qed.

Beispiel: $f(X)=X^3-2\in\mathbb{Q}[X]$ irred. mit Nullstellen $a, \zeta a, \zeta^2 a$ für $a:=\sqrt[3]{2}\in\mathbb{R}$ und $\zeta \in e^{\frac{2\pi i}{3}} \in \mathbb{C}\setminus\mathbb{R}$
$\Rightarrow \Gamma$ transitiv $< S_3$ und komplexe Konjugation $\mapsto (2\,3)\in\Gamma$
$\Rightarrow \Gamma = S_3$.

Beispiel: $f(X)=X^4-2\in\mathbb{Q}[X]$ irred. mit Nullstellen $a,-a,ia,-ia$ für $a:=\sqrt[4]{2}\in\mathbb{R}$. Die komplexe Konjugation operiert durch $(3\,4)\in S_4$. Wegen der Transitivität existiert $\gamma\in\Gamma$ mit $\gamma(a)=-a$, also $\gamma1=2$ und $\gamma2=1$. Wegen $(3\,4)\in\Gamma$ folgt $(1\,2)\in\Gamma$. Weiter existiert $\gamma\in\Gamma$ mit $\gamma(a)=ia$, also $\gamma(-a)=-ia$ und somit $\gamma1=3$ und $\gamma2=4$. Wegen $(3\,4)\in\Gamma$ folgt z.B. $(1\,3)(2\,4)\in\Gamma$. Aber

$$\langle(12),(34),(13)(24)\rangle = D_4 < S_3,$$

und $8=|D_4|\le|\Gamma| = [\mathbb{Q}(a,i)/\mathbb{Q}] = 8$ impliziert $\Gamma=D_4$.