§4. Der Hauptsatz der Galoistheorie

(1) Information aus LA: Wenn ein homogenes lin Gleichg system mehr ~~Gleich~~ Unbekannte als Gleichungen hat, so ist es nichttrivial lösbar.

(2) G Gruppe K Körper

Def 1 Ein Charakter $\sigma : G \to K$ ist ein Gruppenhomo $G \to K^*$, mult Gruppe von K

Bemkg. $Abb(G, K)$ ist ein K-VR. Die σ sind spezielle Abbildungen. σ_1, σ_2 Charaktere, $x_1, x_2 \in K$, dann

$$(x_1 \sigma_1 + x_2 \sigma_2)(\alpha) = x_1 \cdot \sigma_1(\alpha) + x_2 \cdot \sigma_2(\alpha)$$

Satz 1 Je endlich viele (paarweise verschiedene) Charaktere sind lin unabh $| K$.

Beweis. $\sigma_1, \ldots, \sigma_n$ Charaktere.

$n=1$: $x \cdot \sigma(\xi) \equiv 0 \leadsto x\,\sigma(\varepsilon) = x \cdot 1 = 0$

$\leadsto x = 0$ $\qquad \varepsilon$ 1-Element von G

$n-1 \leadsto n$

$$x_1 \sigma_1(\xi) + \dots + x_n \sigma_n(\xi) \equiv 0 \qquad \text{alle } \xi \in \mathcal{G}$$

Sei $\eta \in \mathcal{G}$ beliebig

$$x_1 \sigma_1(\eta\xi) + \dots + x_n \sigma_n(\eta\xi) \equiv 0$$
$$x_1 \sigma_1(\xi)\sigma_1(\eta) + \dots + x_n \sigma_n(\xi)\sigma_n(\eta) = 0$$
$$x_1 \sigma_1(\xi)\sigma_n(\eta) + \dots + x_n \sigma_n(\xi)\sigma_n(\eta) = 0$$

$$x_1 \sigma_1(\xi)[\sigma_1(\eta) - \sigma_n(\eta)] + \dots + x_{n-1}\sigma_{n-1}(\xi)[\sigma_{n-1}(\eta) - \sigma_n(\eta)] \equiv 0$$

Nach IV : $x_1[\sigma_1(\eta) - \sigma_n(\eta)] = 0$

Wähle η passend $\leadsto x_1 = 0$

Nach IV: $x_2 = \dots = x_n = 0$

(3) E, B zwei Körper, $\mathcal{G} = B^*$

Def 2 $\sigma_1, \dots, \sigma_n : B \xrightarrow{\sim} E$ Körperisos.
Der Fixkörper dieser σ ist

$$K = \{x \in B : \sigma_1(x) = \dots = \sigma_n(x)\}$$

Sonderfall: B Teilkörper $\subset E$, $\sigma_1 = \mathrm{id}$.
Dann $K = \{x \in B : \sigma_i(x) = x,\ i = 1 \dots n\}$

Damit $K \subset B \subset E$ Körpererweiterungen von K.

Def $L \subset M$ Körper. Grad (M/L)
$= [M:L] = \dim_L M \quad (\leq \infty)$

Bemerkungen 1) $L \subset M \subset N$ Körper.
Dann gilt
$$[N:L] = [N:M][M:L].$$

Denn: (Annahme: alles endlich) Wähle
Basis x_μ, $\mu = 1 \dots m$, von M/L, Basis
y_ν, $\nu = 1 \dots n$, von N/M. Verifiziere:
$x_\mu y_\nu$
Basis von N/L.

2) Ist $[M:L] < \infty$, so ist jedes $x \in M$
algebraisch über L, denn ...

Satz 2 $[B:K] \geq n = \# \sigma$

Beweis. $r = [B:K] < n$, $\omega_1, \dots, \omega_r$
Basis B über K. Betrachte lin. Gleichungssyst.

$$(L) \quad \sum_{\nu=1}^{n} x_\nu \sigma_\nu(\omega_\rho) = 0 \qquad \rho = 1 \dots r$$

hat nichttriviale Lsg, etwa $x_1, \dots, x_n$.
Sei $\omega \in B$, also
$$\omega = \sum_{\rho=1}^{r} a_\rho \omega_\rho$$
Bilde

$$\sum_{\nu=1}^{n} x_\nu \sigma_\nu(\omega_\varrho) = \sum_{\nu=1}^{n} x_\nu \sum_{\rho=1}^{r} \underbrace{\sigma_\nu(a_\rho)}_{b_\rho(\in E)} \sigma_r(\omega_\varrho)$$

$$= \sum_{\rho=1}^{r} b_\rho \sum_{\nu=1}^{n} x_\nu \sigma_\nu(\omega_\varrho) = 0$$

unabhängig von ν!

Widerspruch zu Satz 1.

(4) E Körper, Γ endl. Gruppe von Autos von E

$\Gamma = \{\sigma_1 = id, \sigma_2, \dots, \sigma_n\}$

$K = \mathrm{Fix}\,\Gamma = \{x : \sigma(x) = x, \sigma \in \Gamma\}$

<u>Satz</u> 3 $[E:K] = n$. Jeder K-Auto von E gehört zu Γ.

<u>Beweis</u> 1) „≥" s. Satz 2

2) $x \in E$. $Sp\, x = \sum_{\nu=1}^{n} \sigma_\nu(x)$, $\in K$, da Γ Gruppe
„Spur"
$Sp\, x \not\equiv 0$, da σ_ν l.u.

3) „≤"

$\omega_1, \dots, \omega_{n+1} \in E$

$$(L) \quad \sum_{\rho=1}^{n+1} x_\rho \sigma_\nu(\omega_\rho) = 0 \,, \quad \nu = 1 \dots n$$

hat nichttriviale Lösung. O.E. $x_1 \neq 0$.
Sogar: $Sp\, x_1 \neq 0$, <u>denn</u>

ein Lösung kann mit $y \in E$, beliebig, multipliziert werden, weil $Sp(yx_1) \not\equiv 0$ für $y \in E$.

Wende (L) σ_ν^{-1} an:

$$\sum_{\rho=1}^{n+1} \sigma_\nu^{-1}(x_\rho)\, \omega_\rho = 0 \qquad \nu = 1 \dots n$$

$$\sum_\nu \sum_\rho \sigma_\nu^{-1}(x_\rho)\, \omega_\rho = 0$$

$$\sum_{\rho=1}^{n+1} \underbrace{\left(\sum_{\nu=1}^{n} \sigma_\nu^{-1}(x_\rho)\right)}_{Sp\, x_\rho} \omega_\rho = 0$$

nichttriviale Relation!

4) Ist σ ein weiterer K-Automorphismus, so wäre $[E:K] \geq n+1$.

Satz 4. Γ Gruppe von Autos von E, $K = \mathrm{Fix}\,\Gamma$.

1) $E \supset B \supset K$. Dann ex genau eine Untergruppe Γ_B von Γ mit $B = \mathrm{Fix}\,\Gamma_B$

2) $\varepsilon < \Delta < \Gamma$ Untergruppe. Dann ex genau ein Teilkörper B mit $B = \mathrm{Fix}\,\Delta$

Beispiele: $B = E \Rightarrow \Gamma B = \{\varepsilon\}$
$B = K \Rightarrow \Gamma K = \Gamma$
$\Delta = \varepsilon \Rightarrow B = E$
$\Delta = \Gamma \Rightarrow B = K$

Beweis 2) ist klar

1) Setze $\Gamma B = \Delta \overset{def}{=} \{\sigma \in \Gamma : \sigma | B = id\}$
Z.z.: $B = \mathrm{Fix}\,\Delta$

Sei $B' = \mathrm{Fix}\,\Delta \supset B$

$[E:K] = n = \mathrm{ord}\,\Gamma$
$[E:B'] = r = \mathrm{ord}\,\Delta$
$[B':K] = s \Rightarrow [B:K] \leq s$ $\quad (\Rightarrow n = rs)$

Z.z.: $[B:K] \geq s$.

Zwei $\sigma, \tau \in \Gamma$ stimmen auf B überein
$\Leftrightarrow \sigma^{-1}\tau = id$ auf $B \Leftrightarrow \sigma^{-1}\tau \in \Delta$,
$\Leftrightarrow \sigma, \tau \in$ derselben Nebenklasse von $\Gamma \bmod \Delta$.
Nun: $\exists!\ s$ Nebenklassen, d.h.
s Autos, die auf B verschieden wirken
$\Rightarrow [B:K] \geq s$ nach Satz 2.

⑤ Def.: $E|K$ Galois Erweiterung $\Leftrightarrow$
$\Gamma = \mathrm{Gal}(E|K) = \mathrm{Aut}_K E$ ist endlich
und hat K als genauen Fixkörper

Theorem 5 (Hauptsatz der Galoistheorie)

$E|K$ Galois mit $\Gamma = \mathrm{Gal}(E|K)$.
Triff Zuordnungen

$$\text{Untergruppe}\left\{\begin{array}{ccc} \Delta & \longmapsto & \mathrm{Fix}\,\Delta \\ \mathrm{Gal}(E|B) & \longleftarrow\!\shortmid & B \end{array}\right\}\begin{array}{c}\text{Zwischenkörper} \\ K \subset B \subset E\end{array}$$

Sind bijektiv, invers zueinander,
inklusionsumkehrend.

$\Delta \subset \Gamma$ Normalteiler $\Leftrightarrow$ $\mathrm{Fix}\,\Delta = B$ Galois.
Dann ist $\mathrm{Gal}(B|K) \cong \Gamma/\Delta$

Beweis. (Im wesentlichen in Sätzen 1–4 enthalten.)