IV Die Galois Korrespondenz.

Eine motivierende Frage für die Galois Korrespondenz ist ob die Umkehrung von Satz III. 14 gilt d.h.: angenommen $Gal(E/k)$ ist auflösbar wobei E Zerfällungskörper von $f \in k[x]$ ist, folgt dann, dass f mittels Radikalen lösbar ist? Allgemeiner, gibt es eine Korrespondenz zwischen Untergruppen von $Gal(E/k)$ und Zwischenkörper, d.h. Körper

$$k \subset B \subset E.$$

Die Antwort ist positiv falls eine zusätzliche Eigenschaft erfüllt ist, nämlich die Separabilität von E/k. Diese Korrespondenz ist das Hauptthema dieses

Kapitels.

Sei E ein Körper und $H \subset \mathrm{Aut}\, E$ eine Teilmenge. Die Menge

$$E^H := \{ a \in E : \sigma(a) = a \ \forall \sigma \in H \}$$

ist offensichtlich ein Unterkörper von E.

Def. IV. 1: E^H ist der **Fixkörper** von H.

Bemerkung IV. 2 Die Korrespondenz $H \mapsto E^H$ hat folgende Monotonieeigenschaft:

$$H_1 \subset H_2 \Longrightarrow E^{H_2} \subset E^{H_1}.$$

Beispiel IV. 3 Falls E/k eine Körpererweiterung ist, so folgt

$$k \subset E^{\mathrm{Gal}(E|k)}.$$

Das Beispiel mit $k = \mathbb{F}_p(t)$, $f(X) = X^p - t$ und E Zerfällungskörper von f zeigt

dass $k \subset E^{Gal(E|k)} = E$

da $Gal(E|k) = \{e\}$.

Das erste Ziel ist die Bestimmung des Grades der Erweiterung

$$E / E^H$$

wobei $H < Aut\, E$ eine endliche Untergruppe ~~von E~~ bezeichnet.

Sei nun G eine Gruppe und E ein Körper.

Dfn. IV.4 Ein Charakter von G in E ist ein Gruppenhomomorphismus $G \to E^\times$ von G in die Multiplikative Gruppe $E^\times$.

~~Die Menge solcher~~

Die Menge der Charaktere von G in E wird mit $\mathrm{Hom}(G, E^\times)$ bezeichnet.

Sei $F(G,E)$ der E-Vektorraum aller E-wertigen Funktionen die auf G definiert sind.

Prop. IV-5 (Dedekind) $\mathrm{Hom}(G, E^\times) \subset F(G,E)$ ist linear unabhängig.

Beweis: (Widerspruchsbeweis).

Sei $n \geq 1$ minimal so, dass es n Charaktere $\sigma_1, \dots, \sigma_n$ gibt die in $F(G,E)$ linear abhängig sind. Es gibt also $c_1, \dots, c_n$ in E $c_1 \neq 0, c_2 \neq 0, \dots, c_n \neq 0$ mit

$$(*) \quad c_1\sigma_1(x) + \dots + c_n\sigma_n(x) = 0 \quad \forall x \in G.$$

Offensichtlich ist $n \geq 2$.

Da $\sigma_1 \neq \sigma_n$ gibt es $y \in G$ mit

$\sigma_1(y) \neq \sigma_n(y)$.

Wir werten (*) in xy aus und erhalten:

$$c_1 \sigma_1(x)\sigma_1(y) + \cdots + c_n \sigma_n(x)\sigma_n(y) = 0 \quad \forall x \in G.$$

$$\Rightarrow \quad c_1 \sigma_1(x) \frac{\sigma_1(y)}{\sigma_n(y)} + \cdots + c_n \sigma_n(x) = 0$$

$$c_1 \sigma_1(x) + \cdots + c_n \sigma_n(x) = 0$$

Woraus folgt:

$$c_1 \left(\frac{\sigma_1(y)}{\sigma_n(y)} - 1\right)\sigma_1(x) + c_2\left(\frac{\sigma_2(y)}{\sigma_n(y)} - 1\right)\sigma_2(x) + \cdots$$

$$+ c_{n-1}\left(\frac{\sigma_{n-1}(y)}{\sigma_n(y)} - 1\right)\sigma_{n-1}(x)$$

$$= 0.$$

Nun ist $\frac{\sigma_1(y)}{\sigma_n(y)} - 1 \neq 0$ und wir haben

eine nicht triviale lineare Abhängigkeit

zwischen $\sigma_1, \ldots, \sigma_{n-1}$ gefunden. Ein

Widerspruch. □

Dieser Satz von Dedekind werden wir benützen um eine untere Schranke für $[E : E^G]$ zu bestimmen wobei hier $G \subset \mathrm{Aut}\, E$ eine endliche Teilmenge bezeichnet. Dafür brauchen wir zunächst

Sublemma IV – 6

Sei E ein Körper und S eine Menge. Sei $\{\sigma_1, \dots, \sigma_n\} \subset F(S, E)$ eine linear unabhängige Menge von Vektoren im E-Vektorraum $F(S, E)$. Dann gibt es $s_1, \dots, s_n$ in S so dass die n Vektoren in E^n

$$\begin{pmatrix} \sigma_1(s_1) \\ \vdots \\ \sigma_n(s_1) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_1(s_n) \\ \vdots \\ \sigma_n(s_n) \end{pmatrix}$$

linear unabhängig sind.

Beweis: Übung ☐.

Nun zur angekündigten Unteren Schranke:

Lemma IV-7 Sei $H = \{\sigma_1, \ldots, \sigma_n\} \subset \mathrm{Aut}\, E$ eine Teilmenge mit n Elementen. Dann gilt: $[E : E^H] \geq n$.

Bem. IV-8: Falls $\langle H \rangle :=$ die von H erzeugte Untergruppe von $\mathrm{Aut}\, E$, so ist $E^H = E^{\langle H \rangle}$

und deswegen darf man im Lemma IV-7 keine präzisere Aussage erwarten.

Beweis: $\sigma_1|_{E^\times}, \dots, \sigma_n|_{E^\times}$ sind n Charaktere von $E^\times$ in $E^\times$, also (Prop IV-5) linear unabhängig in $F(E^\times, E)$.

Es gibt also (Sublemma IV-6)

$$\{y_1, \dots, y_n\} \subset E^\times$$

mit

$$\begin{pmatrix} \sigma_1(y_1) \\ \vdots \\ \sigma_n(y_1) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_1(y_n) \\ \vdots \\ \sigma_n(y_n) \end{pmatrix}$$

linear unabhängig in E^n.

Wir betrachten jetzt E als Vektorraum über E^H. Das Lemma folgt dann aus folgender Behauptung:

Behauptung: $\{y_1, \dots, y_n\} \subset E$ sind linear unabhängig über E^H.

Seien $c_1, \dots, c_n$ in $\overline{E}^H$ mit

$$\sum_{i=1}^{n} c_i y_i = 0 .$$

Daraus folgt:

$$\sum_{i=1}^{n} c_i \sigma_j(y_i) = 0 \qquad j = 1, 2, \dots, n$$

d.h.

$$\begin{pmatrix} \sigma_1(y_1) & \cdots & \sigma_1(y_n) \\ \vdots & & \vdots \\ \sigma_n(y_1) & \cdots & \sigma_n(y_n) \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

Da der Rang dieser Matrix n ist,

folgt $c_1 = \dots = c_n = 0$. □

Jetzt können wir folgendes schließen:

Prop IV-9: Sei $G < \mathrm{Aut}\, E$ eine endliche Untergruppe. Dann gilt

$$[E : E^G] = |G|.$$

Beweis: ~~Widerspruchsbeweis~~

Aus Lemma IV-7 folgt mit $n := |G|$

$$[E : E^G] \geq n.$$

Annahme $[E : E^G] > n$.

Seien also $b_1, \dots, b_m$ in E, linear unabhängig über E^G mit $m > n$.

Wir betrachten nun die lineare Abbildung:

$$T: E^m \longrightarrow E^n$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \longmapsto \begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_m) \\ \vdots & & \\ \sigma_n(b_1) & \cdots & \sigma_n(b_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

Dann folgt (1) $\operatorname{Ker} T \neq (0)$

(2) $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \operatorname{Ker} T$

$$\Longrightarrow \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_m) \end{pmatrix} \in \operatorname{Ker} T.$$

Ersteres folgt aus $m > n$ und die zweite Aussage folgt aus der Tatsache dass $\sigma \sigma_i = \sigma_{s(i)}$ wobei $s \in S_n$.

Sei nun $r := \min \{ k : v \in \operatorname{Ker} T \setminus (0)$ besitzt k Koordinaten verschieden von Null$\}$

Sei $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \operatorname{Ker} T$ mit r Koordinaten $\neq 0$; OEDA sei $x_1 \neq 0$.

Dann folgt $\forall \sigma \in G$:

$$\frac{1}{\sigma(x_1)} \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_m) \end{pmatrix} - \frac{1}{x_1} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \operatorname{Ker} T$$

$$= \begin{pmatrix} 0 \\ \sigma\left(\frac{x_2}{x_1}\right) - \frac{x_2}{x_1} \\ \vdots \\ \sigma\left(\frac{x_m}{x_1}\right) - \frac{x_m}{x_1} \end{pmatrix} = 0$$

↑ Definition von σ.

d. h.

$$\begin{pmatrix} 1 \\ x_2/x_1 \\ \vdots \\ x_m/x_1 \end{pmatrix} \in \operatorname{Ker} T \cap \left(E^{\sigma}\right)^m.$$

Aus $\sum_{j=1}^{m} \sigma_i(b_j) \frac{x_j}{x_1} = 0$

angewandt auf $\sigma_i = id$ folgt

$$\sum_{j=1}^{m} b_j \frac{x_j}{x_1} = 0.$$

d.h. $b_1 + b_2 \frac{x_2}{x_1} + \dots + b_m \frac{x_m}{x_1} = 0$

also eine nicht triviale lineare Relation über E^G, Widerspruch mit der Annahme. ∎

Korollar IV-10. *Seien G, H endliche Untergruppen von $\mathrm{Aut}E$. Dann gilt*

$$E^G \subset E^H \iff H < G$$

Beweis:

($\Longleftarrow$) Klar.

($\Longrightarrow$) Wir nehmen an: $E^G \subset E^H$.

Falls $H \not\subset G$ gibt es $\sigma \in H$ mit $\sigma \notin G$. Aber σ fixiert jedes Element aus E^H, folglich auch aus E^G.

Daraus folgt $E^G = E^{G \cup \sigma}$.

Und somit mit Prop. IV_9 und Lemma IV_1:

$$|G| = [E : E^G] = [E : E^{\{\sigma\} \cup G}]$$

$$\geq |\{\sigma\} \cup G| = |G| + 1.$$

Ein Widerspruch. ⚡