19. Die Galoisgruppe

Def. Es sei $L:K$ eine Körpererweiterung.

- Ein Isomorphismus $\sigma: L \xrightarrow{\sim} L$ mit $\sigma|_K = id.$ heißt *K-Automorphismus* von L (oder Autom. über K).
- Die K-Automorphismen von L bilden unter der Komposition als Verknüpfung eine Gruppe, die sogenannte *Galoisgruppe* $Gal(L:K)$ von L über K.

Bsp. $\mathbb{Q}(i):\mathbb{Q}$; $\mathbb{Q}$-Basis ist $\{1, i\}$; $\sigma \in \mathbb{Q}(i) \xrightarrow{\sim} \mathbb{Q}(i)$, $\sigma|_{\mathbb{Q}} = id.$

Dann gilt $(\sigma(i))^2 = \sigma(i)\cdot\sigma(i) = \sigma(i\cdot i) = \sigma(-1) = -1$.

(σ lsom.)

Somit gilt $\sigma(i) = i$ (d.h. $\sigma = id.$) oder $\sigma(i) = -i$, [andere Nullst. von X^2+1]

also $\sigma(a+ib) = a - ib$ mit $\sigma^2 = id.$

D.h. $Gal(\mathbb{Q}(i):\mathbb{Q}) \cong C_2$.

Satz 19.1 Es sei $L:K$ eine Körpererweiterung mit $G = Gal(L:K)$. Weiter sei $H \leq G$ eine Untergruppe von G. Dann ist

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

ein Unterkörper von L mit $K \subseteq L^H \subseteq L$,

Weiter gilt $H \leq Gal(L:L^H)$.

Beweis: Mit $a, b \in L^H$ ist auch $a-b$ und ab^{-1} [$b \neq 0$] in L^H.

Weiter gilt $K \subseteq L^H$, und weil jeder L^H-Autom. von L auch ein K-Autom. von L ist, ist $H \leq Gal(L:L^H)$. ⊣

Def. Der Körper $L^H \subseteq L$, der von den Autom. aus $H \leq Gal(L:K)$ (punktweise) fixiert wird, heißt *Fixkörper zur Untergruppe H*.

Satz 19.2 Sei $L:K$ eine Körpererweiterung mit $G=\mathrm{Gal}(L:K)$. Weiter sei M ein Zwischenkörper, also $K\subseteq M\subseteq L$.
Dann ist
$$G_M := \{\sigma\in G : \forall b\in M\,(\sigma(b)=b)\} = \mathrm{Gal}(L:M).$$
Insbesondere ist $G_M \leq \mathrm{Gal}(L:K)$.

Beweis: Mit $\sigma,\tau\in G_M$ ist auch $\sigma\circ\tau^{-1}\in G_M$, damit ist $G_M\leq \mathrm{Gal}(L:K)$. Weil jedes $\sigma\in G_M$ ein M-Automorphismus von L ist, und umgekehrt jeder M-Automorphismus von L in G_M ist, gilt $G_M=\mathrm{Gal}(L:M)$. ⊣

Zur Galoisgruppe einer Körpererweiterung:
Sei $L:K$ eine alg. Körpererweiterung und sei $f\in K[X]$ mit $\mathrm{grad}(f)=n$ das Min.-Poly. von einem $\alpha\in L$. Weiter sei $\sigma\in\mathrm{Gal}(L:K)$, dann gilt:
$$0=\sigma(0)=\sigma(f(\alpha))=\sigma(a_0+a_1\alpha+\dots+a_n\alpha^n) \qquad [\sigma|_K=\mathrm{id}.]$$
$$=a_0+a_1\sigma(\alpha)+\dots+a_n\sigma(\alpha)^n=f(\sigma(\alpha))$$
Mit α ist also auch $\sigma(\alpha)$ eine Nullstelle von f.

Def. Sei $L:K$ eine Körpererweiterung, sei $\alpha\in L$ alg. über K und sei $f\in K[X]$ das Min.-Poly. von α über K.
Die Nullstellen in L des Polynoms $f\in K[X]$ heissen die in L zu α konjugierten Elemente.

Bsp. $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$; $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$

Aus der Definition und den obigen Ausführungen folgt direkt

Korollar 19.3 Ist $L:K$ alg., $\alpha\in L$, $\sigma\in\mathrm{Gal}(L:K)$, so ist $\sigma(\alpha)$ in L zu α konjugiert.

Sei $L_f \supseteq K$ der Zerfällungskörper eines Polynoms $f \in K[X]$.
Dh. $L_f = K(\alpha_1, \dots, \alpha_n)$ wobei $\alpha_1, \dots, \alpha_n$ die Nullstellen des Polynoms f sind. Mit Kor. 19.3 können wir jedem $\sigma \in \mathrm{Gal}(L_f : K)$ eine Permutation $\pi_\sigma \in S_n$ zuordnen, sodass die Abbildung

$$\mathrm{Gal}(L_f : K) \longrightarrow S_n$$
$$\sigma \longmapsto \pi_\sigma$$

ein Homomorphismus ist. Weil nun L_f durch K und $\alpha_1, \dots, \alpha_n$ erzeugt wird, ist dieser Homom. injektiv. Damit ist $\mathrm{Gal}(L_f : K)$ isomorph zu einer Untergruppe von S_n, wobei die n Elemente die permutiert werden die Nullstellen von f sind.

Es gilt somit folgender Satz:

Satz 19.4 Ist L_f der Zerfällungskörper von $f \in K[X]$, dann ist $\mathrm{Gal}(L_f : K)$ isomorph zu einer Untergruppe der Permutationsgruppe der Nullstellen von f.

Def. Ist L_f der Zerfällungskörper von $f \in K[X]$, so heisst $\mathrm{Gal}(L_f : K)$ die Galoisgruppe von f, bezeichnet mit $\mathrm{Gal}(f)$.

Korollar 19.5 Ist $f \in K[X]$ mit $\mathrm{grad}(f) = n$, so gilt
[Bew. in den Übungen] $\quad |\mathrm{Gal}(f)| \mid n!$

Proposition 19.6 Sei $L : K$ eine endl. Körpererweiterung.
Dann gilt $|\mathrm{Gal}(L : K)| \leq [L : K]$.

Dies folgt direkt aus

Satz 19.7 Sei $L : K$ eine endl. Körpererw. und $\varphi : K \to L'$ ein Körperhomom. Dann gibt es höchstens $[L : K]$ verschiedene Körperhomom. $\tilde{\varphi} : L \to L'$ mit $\tilde{\varphi}|_K = \varphi$.

Bem. Setzen wir $L' = L$ und $\varphi = \mathrm{id}$., so ex. höchstens $[L : K]$ versch. Körperhomom. $L \to L'$, also höchstens $[L : K]$ versch. K-Autom. von L.

[der Fall $L=K$ ist trivial]

Beweis von Satz 19.7: Wir betrachten zuerst den Fall $L = K(\alpha)$ für ein $\alpha \in L$, und zeigen, dass es höchstens $[K(\alpha):K]$ verschiedene Körperhomom. $\tilde{\varphi}: K(\alpha) \to L'$ mit $\tilde{\varphi}|_K = \varphi$ gibt:

- Sei $f = \sum_{i=0}^{n} a_i X^i$ das Min.-Polynom von α über K.
- Sei $\tilde{\varphi}: K(\alpha) \to L'$ ein Körperhomom. mit $\tilde{\varphi}|_K = \varphi$.
- Es gilt $[K(\alpha):K] = \operatorname{grad}(f) = n$.
- Für $\hat{f} := \sum_{i=0}^{n} \varphi(a_i) X^i \in L'[X]$ ist $\hat{f}(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(\underbrace{f(\alpha)}_{=0}) = 0$, und somit wird α durch $\tilde{\varphi}$ auf eine Nullstelle von $\hat{f}$ abgebildet. Da nun $\hat{f}$ höchstens n Nullstellen hat, gibt es somit höchstens n Elemente in L', auf die α durch $\tilde{\varphi}$ abgebildet werden kann.
- Andererseits ist $\tilde{\varphi}$ (siehe Übungsaufg. bzw. der Bem. am Ende der Lösung) eindeutig durch das Bild von α bestimmt.

Somit gibt es höchstens $[K(\alpha):K]$ Möglichkeiten für $\tilde{\varphi}$.

Für den allg. Fall verwenden wir Induktion nach $[L:K]$.

- $[L:K] = 1$ ist klar.
- Für $[L:K] > 1$ wählen wir $\alpha \in L$ mit $\operatorname{grad}(\alpha) = r > 1$, wobei $\operatorname{grad}(\alpha) := \operatorname{grad}(f)$ für f Min.-Poly. von α über K.
- Für jeden Körperhom. $\tilde{\varphi}: L \to L'$ mit $\tilde{\varphi}|_K = \varphi$ betrachten wir $\tilde{\varphi}|_{K(\alpha)}$.
- Aus dem obigen Fall erhalten wir höchstens $[K(\alpha):K]$ solche Restriktionen $\tilde{\varphi}|_{K(\alpha)}$. (Ind.-Voraus. / obiger Fall (Restriktion))
- Mit dem Gradsatz $[L:K] = [L:K(\alpha)] \cdot [K(\alpha):K]$ und der Ind.-Voraussetzung erhalten wir dann, dass es höchstens $[L:K]$ versch. Körperhom. $\tilde{\varphi}: L \to L'$ mit $\tilde{\varphi}|_K = \varphi$ gibt.

Ist die Körpererweiterung $L:K$ endl., normal und separabel (d.h. L ist der Zerfällungskörper eines separablen Polynoms), so erhalten wir eine stärkere Aussage:

Proposition 19.8 Ist L_f der Zerfällungskörper eines separablen Polynoms $f \in K[X]$, so ist

$$|Gal(L_f; K)| = [L_f : K].$$

Dies folgt direkt aus dem folgenden Satz und der anschliessenden Bemerkung.

Satz 19.9. Sei L_f der Zerfällungskörper des sep. Polynoms $f \in K[X]$ und sei $\varphi: K \to L'$ ein Körperhom., sodass $\varphi(f)$ über L' in Linearfaktoren zerfällt. Dann gibt es genau $[L_f : K]$ Körperhom. $\tilde{\varphi}: L_f \to L'$ mit $\tilde{\varphi}|_K = \varphi$.

Beweis: Wie im Beweis von Satz 19.7; wir verwenden, dass f sep. ist (irred. Faktoren von f haben versch. Nullstellen in L_f bzw. L') und zeigen den Satz wieder für einfache Körpererweiterungen und mit Induktion nach $[L_f : K]$.

[Fortsetzung siehe S. 124b]

Aus dem folgenden Satz wird folgen, dass jede endliche Körpererweiterung $L:K$, wobei $\mathrm{char}(K)=0$, einfach ist.

Satz 19.10. (Satz über primitive Elemente) Eine endliche Körpererweiterung $L:K$ mit $|K| = \infty$ ist einfach genau dann, wenn es nur endlich viele Zwischenkörper M mit $K \subseteq M \subseteq L$ gibt.

- Für $[L_f : K] = 1$ ist nichts zu beweisen.

  Es sei $[L_f : K] > 1$. Wir wählen einen irred. Faktor g von f mit $\text{grad}(g) = r > 1$.

- Da f separabel ist, sind es auch g und $\varphi(g)$.

- Sei α eine Nullstelle von g. Für jede Nullstelle α_j' $(1 \leq i \leq r)$ von $\varphi(g)$ existiert ein Körperhomom. $\varphi_j : K(\alpha) \to L'$ mit $\varphi_j|_K = \varphi$ und $\varphi_j(\alpha) = \alpha_j'$.

- Mit Induktion, angewandt auf die Körpererw. $L_f : K(\alpha)$, folgt, dass sich jedes φ_j auf genau $[L_f : K(\alpha)]$ Arten zu einem Körperhom. $\tilde{\varphi} : L_f \to L'$ mit $\tilde{\varphi}|_{K(\alpha)} = \varphi_j$ erweitern lässt.

- Weil $[K(\alpha) : K] = r$, ist damit die Existenz von $[L_f : K(\alpha)] \cdot r = [L_f : K(\alpha)] \cdot [K(\alpha) : K] = [L_f : K]$ verschiedenen Körperhomom. $\tilde{\varphi} : L_f \to L'$ mit $\tilde{\varphi}|_K = \varphi$ gezeigt.

- Mit Satz 19.7 gibt es aber höchstens $[L_f : K]$ solche Körperhom. $\tilde{\varphi}$, womit der Satz bewiesen ist.

⊣

<u>Bemerkung:</u> Ist $L' = L_f$, so gibt es genau $[L_f : K]$ K-Automorphismen $\tilde{\varphi} : L_f \to L_f$ (insbes. $\tilde{\varphi}|_K = \text{id}$.):

- Jeder Körperhom. $\varphi : L_f \to L_f$ ist injektiv, denn $\ker(\varphi)$ ist ein Ideal in L_f und L_f hat nur die Ideale L_f und (0). $L_f/(0) \cong L_f$ und L_f/L_f ist kein Körper; also ist $\ker(\varphi) = (0)$, d.h. φ ist injektiv.

- $\tilde{\varphi}$ bildet die Nullstellen von f injektiv auf die Nullstellen von $\tilde{\varphi}(f) = f$ ab, und weil $\text{grad}(f) < \infty$ ist die Inj. eine Bijektion.

- Somit ist $\tilde{\varphi}[L_f]$ Zerfällungskörper von f über K, also $L_f \cong \tilde{\varphi}[L_f]$.

  Es gibt somit $[L_f : K]$ versch. K-Autom. $\tilde{\varphi} : L_f \to L_f$ und $|\text{Gal}(L_f : K)| = [L_f : K]$.

Beweis: ($\Leftarrow$) Weil $L:K$ endlich ist, können wir L schreiben als $L = K(\alpha_1, \dots, \alpha_n)$ für $\alpha_i \in L$.

Der Beweis ist mit Induktion über n.

- Der Fall $n=1$ ist klar. ($L : K(\alpha_1)$ ist einfach)
- Ist $M = K(\alpha_1, \dots, \alpha_{n-1})$, dann ist $K \subseteq M \subseteq L$ ein Zwischenkörper und mit Induktionsvoraussetzung ist $M = K(\beta)$ für ein β. ($M:K$ ist einfach)
- Dann ist $L = K(\alpha_n, \beta) = K(\alpha_1, \dots, \alpha_n)$.
- Für jedes $a \in K$ definieren wir $M_a := K(\alpha_n + a\beta)$. Dann ist $K \subseteq M_a \subseteq L$ ein Zwischenkörper. (für alle $a \in K$)
- Weil es nach Voraussetzung nur endl. viele Zwischenkörper gibt aber K unendlich ist, finden wir $a, b \in K$ mit $a \neq b$ und $M_a = M_b$. (insbes. ist $\alpha_n + a\beta \in M_b$)
- Somit gilt
$$\beta = \frac{(\alpha_n + b\beta) - (\alpha_n + a\beta)}{b-a} \in M_b.$$
- Weiter haben wir $\alpha_n = \underbrace{(\alpha_n + b\beta)}_{\in M_b} - \underbrace{b\beta}_{\in M_b} \in M_b$ und somit ist $L = K(\alpha_n, \beta) = M_b = K(\alpha_n + b\beta)$, also ist $L:K$ einfach. (weil $b \in K \subseteq M_b$ und $\beta \in M_b$; $\alpha_n, \beta \in M_b$)

($\Rightarrow$): Sei nun $L = K(\alpha)$ für ein $\alpha \in L$ und sei M ein Zwischenkörper, also $K \subseteq M \subseteq L$.

- Dann ist $L = M(\alpha)$. Sei f das Min. Poly. von α über K und g das Min.-Poly. von α über M. Dann gilt $g \mid f$.
- Sei $g = a_0 + a_1 X + \dots + X^r$ und sei $M_0 := K(a_0, \dots, a_{r-1}) \subseteq M$. Dann ist $g \in M_0[X]$ und für $\tilde{g}$ das Min.-Poly. von α über M_0 gilt $\tilde{g} \mid g$, ⊛
- Somit haben wir $[L:M] = \operatorname{grad}(g) = \operatorname{grad}(\tilde{g}) = [L:M_0]$
$$= [L:M] \cdot [M:M_0] \implies [M:M_0] = 1.$$
- Also gilt $M = M_0$ und M ist durch g (mit $g \mid f$) bestimmt, und weil f nur endl. viele normierte Teiler hat, ex. nur endl. viele Zw.-Körper. [im Zerfällungskörper von f]

⊛ weil $g \in M_0[X]$. Andererseits gilt auch $\deg \tilde{g}$ weil $M_0 \subseteq M$ und somit ist $\deg g = \deg \tilde{g}$, insbes. ist $\operatorname{grad}(g) = \operatorname{grad}(\tilde{g})$.