Hauptsatz der Galoistheorie

Situation: Sei K ein Koeffizientenbereich (etwa $K = \mathbb{Q}$ oder $K = \mathbb{Q}(\sqrt[3]{2})$).
Sei $f(X) \in K[X]$ ein normiertes separables Polynom.
Seien $x_1, \ldots, x_n$ die Nullstellen von $f(X)$. Sei $E := K(x_1, \ldots, x_n)$.
Sei $G := \mathrm{Gal}_K(x_1, \ldots, x_n)$ die Galoisgruppe der Nullstellen über K.

Dann gilt: Die Zuordnung

$$\boxed{\text{Menge der Untergruppen von } G} \quad \overset{1:1}{\longleftrightarrow} \quad \boxed{\text{Menge der Zwischenerweiterungen von } E|K}$$

$$\begin{array}{rcl} H & \longmapsto & E^H := \{x \in E \mid \sigma(x) = x \text{ für alle } \sigma \in H\} \\ \mathrm{Gal}_L(x_1, \ldots, x_n) & \longmapsto & L \end{array}$$

ist eine inklusionsumkehrende Bijektion. Genauer gilt für alle Zwischenerweiterungen L, L' von $E|K$ und Untergruppen H, H' von G:

a) $E^{\mathrm{Gal}_L(x_1,\ldots,x_n)} = L$, $\quad \mathrm{Gal}_{E^H}(x_1, \ldots, x_n) = H$.

b) $L \subseteq L' \Leftrightarrow \mathrm{Gal}_L(x_1, \ldots, x_n) \supseteq \mathrm{Gal}_{L'}(x_1, \ldots, x_n)$, $\quad H \subseteq H' \Leftrightarrow E^H \supseteq E^{H'}$.

c) $|H| = [H : 1] = [E : E^H]$, $\quad [E^H : K] = [G : H] = |G| \,/\, |H|$.

d) In Algebra II werden wir eine einfache Charakterisierung dafür kennenlernen, wann H ein Normalteiler in G ist.

Wie kann man die relativen Galoisgruppen ausrechnen? Wenn $L = K(z_1, \ldots, z_m)$, gilt

$$\mathrm{Gal}_L(x_1, \ldots, x_n) = \{\sigma \in G \mid \sigma \cdot z_i = z_i \text{ für } i = 1, \ldots, m\}.$$

Wie kann man Erzeuger der Fixkörper bestimmen? Falls $H = \{\sigma_1, \ldots, \sigma_m\}$ und $E = K(t)$, gilt

$$E^H = K(e_1(\sigma_1 \cdot t, \ldots, \sigma_m \cdot t), \ldots, e_m(\sigma_1 \cdot t, \ldots, \sigma_m \cdot t)),$$

wobei die e_i die elementarsymmetrischen Funktionen in m Unbekannten seien.

Beispiel

Sei $L := \mathbb{Q}(\sqrt{2}, \mathrm{i})$ der Zerfällungskörper von $(X^2 - 2)(X^2 + 1)$ über $K := \mathbb{Q}$.

a) Die Galoisgruppe G besteht aus folgenden vier Elementen $\sigma_1, \ldots, \sigma_4$:

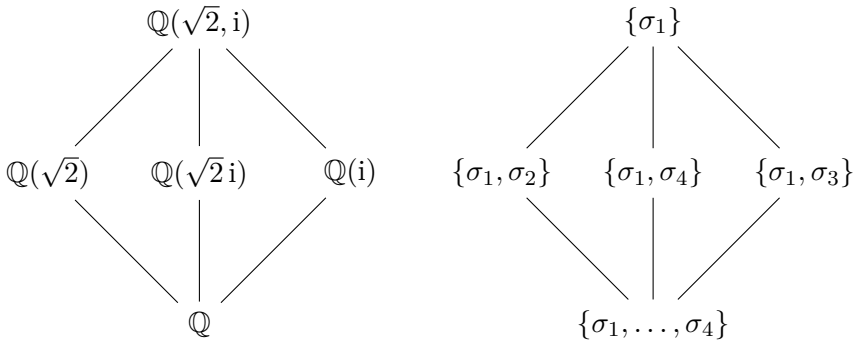
$$\begin{array}{lll} \sigma_1{:}\sqrt{2} \mapsto \sqrt{2}, & \mathrm{i} \mapsto \mathrm{i} \\ \sigma_2{:}\sqrt{2} \mapsto \sqrt{2}, & \mathrm{i} \mapsto -\mathrm{i} \\ \sigma_3{:}\sqrt{2} \mapsto -\sqrt{2}, & \mathrm{i} \mapsto \mathrm{i} \\ \sigma_4{:}\sqrt{2} \mapsto -\sqrt{2}, & \mathrm{i} \mapsto -\mathrm{i} \end{array}$$

b) Die Verknüpfungstafel ist:

$\circ$	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_1	σ_4	σ_3
σ_3	σ_3	σ_4	σ_1	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1

Dazu sind die Nebenrechnungen $\sigma_2 \circ \sigma_2 = \sigma_1$ und $\sigma_3 \circ \sigma_3 = \sigma_1$ erforderlich, den Rest kann man nach der Regel „in jeder Zeile und Spalte muss jedes Gruppenelement genau einmal vorkommen“ erschließen.

c) Tafel der Untergruppen von G und der Zwischenerweiterungen von $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ über $\mathbb{Q}$:



Im linken Diagramm steht oben die größte und unten die kleinste Zwischenerweiterung, im rechten Diagramm umgekehrt oben die kleinste und unten die größte Untergruppe der Galoisgruppe. Das ist so gemacht, dass zu einer Zwischenerweiterung an der entsprechenden Stelle rechts die zugehörige relative Galoisgruppe und zu einer Untergruppe entsprechend links der zugehörige Fixkörper steht.

d) Exemplarisch der Nachweis, dass $L^{\{\sigma_1, \sigma_4\}} = \mathbb{Q}(\sqrt{2}\,\mathrm{i})$:

Die Richtung „$\supseteq$“ ist klar, da die Zahl $\sqrt{2}\,\mathrm{i}$ von σ_4 (und von σ_1 sowieso) festgehalten wird:

$$\sigma_4(\sqrt{2}\,\mathrm{i}) = \sigma_4(\sqrt{2})\,\sigma_4(\mathrm{i}) = (-\sqrt{2})(-\mathrm{i}) = \sqrt{2}\,\mathrm{i}$$

Die andere Richtung folgt aus Gradgründen:

$$[L^{\{\sigma_1, \sigma_4\}} : \mathbb{Q}] = |G| \,/\, |\{\sigma_1, \sigma_4\}| = 4/2 = 2$$
$$[\mathbb{Q}(\sqrt{2}\,\mathrm{i}) : \mathbb{Q}] = 2$$