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

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

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

ist eine inklusionsumkehrende Bijektion. Der Rechenbereich E^H wird auch als *Fixkörper* bezüglich der Untergruppe H bezeichnet. Genauer gelten für alle Zwischenerweiterungen L, L' von $E|K$ und Untergruppen H, H' von G folgende Aussagen.

Hin und zurück

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

Der Fixkörper zur Galoisgruppe einer Zwischenerweiterung L ist wieder L. Die Galoisgruppe über dem Fixkörper einer Untergruppe H ist wieder H. Die erste Aussage umfasst die bekannte Tatsache, dass eine Zahl aus E, welche invariant unter der Wirkung der Galoisgruppe $\mathrm{Gal}_L(x_1, \ldots, x_n)$ ist, schon in L liegen muss. Wieso?

Größer und kleiner

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

Je größer der Koeffizientenbereich, desto kleiner ist die zugehörige Galoisgruppe; und umgekehrt: Je größer die Untergruppe, desto kleiner ist der zugehörige Fixkörper. Wieso sind beide Aussagen anschaulich?

Grade und Indizes

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

Die *Ordnung* einer Untergruppe H ist durch den Grad $[E : E^H]$ gegeben. Der *Index* einer Untergruppe H ist durch den Grad $[E^H : K]$ gegeben. Wieso passt das mit dem inklusionsumkehrenden Charakter zusammen?

Normalität

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 $L = K(z_1, \dots, z_m)$, gilt

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

Wie kann man Erzeuger der Fixkörper bestimmen?

Falls $H = \{\sigma_1, \dots, \sigma_m\}$ und $E = K(t)$, gilt

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

wobei die e_i die elementarsymmetrischen Funktionen in m Unbekannten sind.

Wozu ist der Hauptsatz gut?

- Der Hauptsatz klärt die Struktur der Zwischenerweiterungen, durch Rückführung auf die zugänglichere Struktur der Untergruppen.
- Informationen über Grade liefern Informationen über Indizes und umgekehrt; manchmal ist das eine leichter zu berechnen als das andere.
- Der Hauptsatz geht wesentlich im Beweis der fundamentalen Äquivalenz

  $$\boxed{\text{Gleichung } f(X) = 0 \text{ auflösbar}} \iff \boxed{\text{Galoisgruppe } \mathrm{Gal}_K(x_1, \dots, x_n) \text{ auflösbar}}$$

  ein: Unter geeigneten Voraussetzungen an den Koeffizientenbereich K bilden die Galoisgruppen zu den einzelnen Stufen eines Turms aus Radikalerweiterungen (nach Streichen mehrfach vorkommender Untergruppen) eine Normalreihe der vollen Galoisgruppe über K.
- Der Hauptsatz ist ein erstes Beispiel für tiefe Dualitätsresultate, von denen es noch viele weitere gibt.