Kap. IV. Anwendungen der Galois–Theorie

§ 14. Die Galois–Gruppe eines Polynoms

(14.1) DEF: K sei ein Körper, $f \in K[T]$ ein Polynom vom Grade ≥ 1 und $Z = \mathrm{ZFK}_K(f)$ der Zerfällungskörper von f über K. Dann heißt

$$\mathrm{Gal}_K(f) \;:=\; \mathrm{Gal}(Z:K)$$

die **Galois–Gruppe von f über K**.

(14.2) BEM: **a)** Sind Z und Z' zwei Zerfällungskörper von f über K, so gibt es nach (9.6) einen K–Isomorphismus $Z \longrightarrow Z'$, der nach Aufgabe 39 einen Gruppenisomorphismus

$$\mathrm{Gal}(Z:K) \;\cong\; \mathrm{Gal}(Z':K)$$

induziert, d.h. die Galois–Gruppe eines Polynoms ist bis auf Isomorphie eindeutig bestimmt.

b) Ist $n := \mathrm{grad}(f)$, so gilt nach Aufgabe 36)

$$[Z:K] \;\leq\; n!\,.$$

$Z:K$ ist damit eine endliche Körpererweiterung , und mit (10.12) folgt

$$|\mathrm{Gal}_K(f)| \;\leq\; [Z:K] \;\leq\; n!\,.$$

c) Ist f separabel über K, so ist $Z:K$ nach (13.8) eine Galois–Erweiterung, und es gilt insbesondere

$$|\mathrm{Gal}_K(f)| \;=\; [Z:K]\,.$$

Dies ist z.B. immer der Fall, wenn K vollkommen ist (also z.B. im Falle $\mathrm{char}(K) = 0$ oder K endlich).

(14.3) DEF: Eine Untergruppe $U \leq S_n$ heißt **transitiv**, wenn es zu $i,k \in \{1,2,\ldots,n\}$ stets ein $\pi \in U$ gibt mit $\pi(i) = k$.

(14.4) SATZ: K sei ein Körper, $f \in K[T]$ ein Polynom vom Grade ≥ 1 , $Z = \mathrm{ZFK}_K(f)$ der Zerfällungskörper von f über K und $G := \mathrm{Gal}_K(f)$ die Galois–Gruppe von f über K. Dann gilt:

a) G ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_m, wobei m die Anzahl der verschiedenen Nullstellen von f in Z ist.

b) Ist f irreduzibel und separabel über K mit $\mathrm{grad}(f) = n$, so gilt:

1) n ist ein Teiler der Gruppenordnung von G.

2) G ist isomorph zu einer **transitiven** Untergruppe von S_n.

(14.5) BEM: **a)** Die Einbettung von G in S_m hängt von der Numerierung der Nullstellen $\alpha_1, \alpha_2, \ldots \alpha_m$ von f ab. Ist $N = \{\alpha_1, \ldots \alpha_m\}$, so ist

$$\sigma(N) \;=\; \{\alpha_{i_1}, \alpha_{i_2}, \ldots \alpha_{i_m}\} \quad \text{mit} \quad \sigma(\alpha_k) = \alpha_{i_k} .$$

Die Einbettung $\omega : G \longrightarrow S_m$ ist dann definiert durch

$$\omega(\sigma) \;:=\; \begin{pmatrix} 1 & 2 & \ldots & m \\ i_1 & i_2 & \ldots & i_m \end{pmatrix} .$$

b) Ist $\omega' : G \longrightarrow S_m$ ein injektiver Gruppenhomomorphismus, der zu einer anderen Numerierung der Nullstellen gehört, so sind $U = \omega(G)$ und $V = \omega'(G)$ konjugierte Untergruppen von S_m, d.h. es existiert ein $\pi \in S_m$ mit

$$U \;=\; \pi^{-1} \circ V \circ \pi .$$

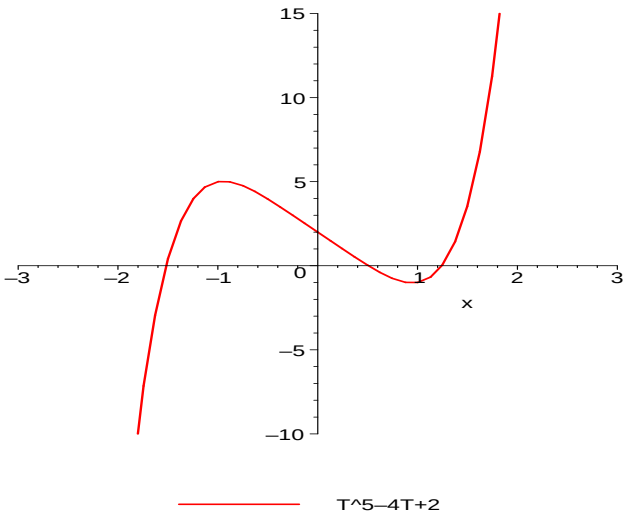
Insbesondere sind U und V isomorph zueinander.

c) Ist $f \in \mathbb{Q}[T]$ irreduzibel vom Grade n, so kommen als Galois–Gruppe von f nur transitive Untergruppen von S_n in Frage. Es ergibt sich also das Problem, alle transitiven Untergruppen von S_n zu bestimmen.

(14.6) SATZ: *p sei eine Primzahl, und $f \in \mathbb{Q}[T]$ sei ein irreduzibles Polynom vom Grade p. f besitze in dem Zerfällungskörper $Z = \mathrm{ZFK}_{\mathbb{Q}}(f) \subseteq \mathbb{C}$ genau 2 nichtreelle Nullstellen. Dann gilt*

$$\mathrm{Gal}_{\mathbb{Q}}(f) \;\cong\; S_p .$$

(14.7) BEISPIEL: Die Galois–Gruppe des Polynoms $T^5 - 4T + 2 \in \mathbb{Q}[T]$ ist isomorph zu S_5.



Zwei Probleme der Galois–Theorie

(14.8) PROBLEM Gegeben sei ein irreduzibles Polynom $f \in \mathbb{Q}[T]$ vom Grade n. Bestimmt werden soll die Galoisgruppe $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ von f, d.h. die Galoisgruppe des Zerfällungskörpers von f über $\mathbb{Q}$.

Jeder Automorphismus $\sigma \in G$ permutiert die Nullstellen von f, so daß G zu einer transitiven Untergruppe U von S_n isomorph ist. Es gibt nun Verfahren, die **ohne** explizite Kenntnis der Nullstellen von f die richtige Untergruppe U herausfiltern können, zu der G isomorph ist. Ein **Problem** besteht nun darin, **algorithmische Verfahren** für die Bestimmung der Galoisgruppe zu entwickeln. So gibt es z.B. in dem Computeralgebra–System MAPLE die Prozedur "galois", die die Galois–Gruppe eines irreduziblen Polynoms vom Grade ≤ 9 bestimmt.

(14.9) PROBLEM Im Jahre 1892 hat David Hilbert (1862–1943) das sog. **Umkehrproblem der Galois–Theorie** gestellt:

> G sei eine beliebige endliche Gruppe.
> Gibt es dann ein Polynom $f \in \mathbb{Q}[T]$
> mit $\mathrm{Gal}_{\mathbb{Q}}(f) \cong G$?

Dieses Problem ist bis heute nicht gelöst worden, es gibt nur Teillösungen. So ist z.B. die Frage zu bejahen, wenn

G eine endliche **abelsche** Gruppe ist oder wenn

G eine endliche **auflösbare** Gruppe ist

(Letzteres hat Shafarevich im Jahre 1954 bewiesen).

Für spezielle Gruppen, etwa $\mathbb{Z}_n$, A_n , S_n $(n \in \mathbb{N})$, ist das Umkehrproblem gelöst.