Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Körper- und Galoistheorie

Vorlesung 23

Polynome mit unauflösbarer Galoisgruppe

Wir möchten nun zeigen, dass gewisse Körpererweiterungen, und zwar die Zerfällungskörper von gewissen Polynomen vom Grad ≥ 5, nicht auflösbar sind. Dazu müssen wir aufgrund der Galoistheorie für auflösbare Körpererweiterungen und den gruppentheoretischen Überlegungen zu den Permutationsgruppen S_n, $n \geq 5$, (Lemma 21.9) lediglich nachweisen, dass diese Permutationsgruppen als Galoisgruppen auftreten. Dazu bedarf es einiger Vorbereitungen über Permutationsgruppen.

Zu einer Permutationsgruppe $S(M)$ auf einer Menge M liefert jede Teilmenge $T \subseteq M$ eine Untergruppe $S(T) \subseteq S(M)$. Man setzt einfach die Permutation auf T durch die Identität auf $M \setminus T$ zu einer Permutation auf ganz M fort.

Lemma 23.1. *Es sei M eine endliche Menge und $T_1, T_2 \subseteq M$ seien Teilmengen mit $T_1 \cap T_2 \neq \emptyset$. Es sei $G \subseteq S(M)$ eine Untergruppe der Permutationsgruppe, die sowohl $S(T_1)$ als auch $S(T_2)$ umfasst. Dann ist $S(T_1 \cup T_2) \subseteq G$.*

Beweis. Jedes Element $\sigma \in S(T_1 \cup T_2)$ lässt sich nach Lemma 18.7 (Lineare Algebra (Osnabrück 2017-2018)) als Produkt von Transpositionen auf $T_1 \cup T_2$ schreiben. Es muss also lediglich gezeigt werden, dass solche Transpositionen zu G gehören. Sei $\sigma \in S(T_1 \cup T_2)$ eine Transposition, und zwar vertausche σ die Elemente a und b, also $\sigma = \langle a, b \rangle$. Wenn beide Elemente zu T_1 (oder zu T_2) gehören, sind wir fertig. Sei also $a \in T_1, a \notin T_2$ und $b \in T_2, b \notin T_1$. Es sei ferner $c \in T_1 \cap T_2$, und c sei von a und b verschieden (sonst gehören beide zu einer der Teilmengen). Dann ist

$$\sigma = \langle a, b \rangle = \langle a, c \rangle \circ \langle b, c \rangle \circ \langle a, c \rangle$$

und diese drei Transpositionen gehören zu $S(T_1)$ oder zu $S(T_2)$ und damit zu G. □

Definition 23.2. Es sei M eine Menge und sei $G = S(M)$ die zugehörige Permutationsgruppe. Eine Untergruppe $H \subseteq G$ heißt *transitiv*, wenn es zu je zwei Elementen $x, y \in M$ ein $\sigma \in H$ mit $\sigma(x) = y$ gibt.

Lemma 23.3. *Es sei p eine Primzahl und S_p die Permutationsgruppe zu $\{1, \ldots, p\}$. Es sei $H \subseteq S_p$ eine transitive Untergruppe, die eine Transposition enthalte. Dann ist $H = S_p$.*

Beweis. Sei $M = \{1, \ldots, p\}$. Wir betrachten Teilmengen $T \subseteq M$ derart, dass $S(T) \subseteq H$ ist, und wollen $T = M$ zeigen. Sei dazu T_1 eine solche Teilmenge mit maximaler Elementanzahl, die wir k nennen. Da es mindestens eine Transposition in H gibt, ist $k \geq 2$. Für jedes $\sigma \in H$ ist $T_\sigma = \sigma(T_1)$ ebenfalls eine k-elementige Menge mit $S(T_\sigma) \subseteq H$. Für $\tau \in S(T_\sigma)$ ist nämlich

$$\tau = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1},$$

und $\sigma^{-1}\tau\sigma$ ist eine Permutation auf T_1, so dass sie zu H gehört und damit auch $\tau \in H$ gilt. Für Permutationen $\sigma_1, \sigma_2 \in H$ ist entweder $T_{\sigma_1} = T_{\sigma_2}$ oder $T_{\sigma_1} \cap T_{\sigma_2} = \emptyset$, da andernfalls nach Lemma 23.1 $S(T_1 \cup T_2) \subseteq H$ wäre im Widerspruch zur Maximalität von k. Sei nun $x \in M$ vorgegeben und ein $y \in T_1$ fixiert. Aufgrund der Transitivität gibt es ein $\sigma \in H$ mit $\sigma(y) = x$. Dann ist natürlich $x \in T_\sigma$. Das bedeutet, dass die Mengen T_σ, $\sigma \in H$, die Gesamtmenge M überdecken. Wegen der Gleichmächtigkeit dieser Mengen ist p ein Vielfaches von k und somit ist $p = k$, also $M = T_1$. □

Lemma 23.4. *Sei p eine Primzahl und $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad p, das genau $p-2$ reelle Nullstellen besitzt. Dann ist die Galoisgruppe des Zerfällungskörpers $\mathbb{Q} \subseteq Z(F)$ gleich der Permutationsgruppe S_p. Bei $p \geq 5$ ist diese Körpererweiterung nicht auflösbar.*

Beweis. Es seien $\alpha_1, \ldots, \alpha_{p-2}$ die reellen Nullstellen und α_{p-1}, α_p die beiden nichtreellen komplexen Nullstellen. Nach Lemma 14.2 ist die Galoisgruppe $\mathrm{Gal}\,(Z(F)|\mathbb{Q})$ in natürlicher Weise eine Untergruppe der Permutationsgruppe der Nullstellen. Wir zeigen, dass es sich um die volle Permutationsgruppe handelt. Die komplexe Konjugation induziert einen $\mathbb{Q}$-Automorphismus auf L, der die reellen Nullstellen unverändert lässt und die beiden nichtreellen Nullstellen α_{p-1} und α_p ineinander überführt. Daher bewirkt dieser Automorphismus auf den Nullstellen eine Transposition. Da F über $\mathbb{Q}$ irreduzibel ist, ist F für jede Nullstelle das Minimalpolynom und daher sind alle Nullstellen zueinander konjugiert. Nach Satz 14.5 gibt es somit für je zwei Nullstellen α und β einen Automorphismus φ mit $\varphi(\alpha) = \beta$. Damit sind die Voraussetzungen von Lemma 23.3 erfüllt und somit ist die Galoisgruppe die volle Permutationsgruppe. □

Korollar 23.5. *Sei a eine Primzahl und sei*

$$F = X^5 + a^2X^4 - a \in \mathbb{Q}[X].$$

Dann gelten folgende Aussagen.

(1) *Das Polynom F ist irreduzibel in $\mathbb{Q}[X]$.*
(2) *F besitzt drei reelle Nullstellen und darüber hinaus zwei komplexe nichtreelle Nullstellen.*
(3) *Die Galoisgruppe des Zerfällungskörpers $\mathbb{Q} \subseteq Z(F)$ ist die Permutationsgruppe S_5.*
(4) *Die Körpererweiterung $\mathbb{Q} \subseteq Z(F)$ ist nicht auflösbar.*

Beweis. (1) ergibt sich aus dem Kriterium von Eisenstein. (2). Wir berechnen einige Funktionswerte von F. Es ist

$$F\left(-a^2\right) = -a^{10} + a^{10} - a = -a < 0,$$
$$F(-1) = -1 + a^2 - a = -1 + a(a-1) > 0,$$
$$F(0) = -a < 0$$

und schließlich

$$F(1) = 1 + a^2 - a > 0.$$

Nach dem Zwischenwertsatz gibt es daher mindestens drei reelle Nullstellen. Die Ableitung von F ist

$$F' = 5X^4 + 4a^2X^3 = 5X^3\left(X + \frac{4}{5}a^2\right)$$

und besitzt die beiden reellen Nullstellen 0 und $-\frac{4}{5}a^2$. Nach dem Mittelwertsatz der Differentialrechnung kann somit F nicht mehr als drei reelle Nullstellen besitzen, da zwischen zwei Nullstellen stets eine Nullstelle der Ableitung liegt. Die Nullstellen der Ableitung sind wegen

$$F\left(-\frac{4}{5}a^2\right) \neq 0$$

(wegen der Irreduzibilität von F über $\mathbb{Q}$) keine Nullstelle von F, so dass F keine mehrfache Nullstelle besitzen kann. Daher muss es zwei weitere komplexe nichtreelle Nullstellen geben. (3) und (4) folgen aus (1), (2) und Lemma 23.4. □

Paolo Ruffini (1765-1822)

Niels Henrik Abel (1802-1829)

Das erste Beispiel für ein solches Polynom ist $X^5 + 4X^4 - 2$. Durch die Existenz solcher Polynome folgt die allgemeine Unauflösbarkeit für algebraische

Gleichungen vom Grad 5 und höher. Diese Aussage heißt *Satz von Abel-Ruffini*.

SATZ 23.6. *Für $n \geq 5$ gibt es polynomiale Gleichungen (über $\mathbb{Q}$) vom Grad n, die nicht auflösbar sind.*

Beweis. Für $n = 5$ folgt dies direkt aus Korollar 23.5, und für $n \geq 6$ kann man ein unauflösbares Polynom vom Grad 5 einfach mit einem beliebigen Polynom vom Grad $n - 5$ multiplizieren. □

Abbildungsverzeichnis