Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Vorlesung 25

Wir haben gesehen, dass das Minimalpolynom einer aus $\mathbb{Q}$ konstruierbaren komplexen Zahl eine Zweierpotenz als Grad besitzt. Wir werden hier zeigen, dass eine komplexe algebraische Zahl genau dann konstruierbar ist, wenn der Grad des Zerfällungskörper ihres Minimalpolynoms eine Zweierpotenz ist. Dies erfordert einige einfache gruppentheoretische Vorbereitungen.

Konjugationsklassen und Klassengleichung

DEFINITION 25.1. Zu einer Gruppe G nennt man die Äquivalenzklassen zur Äquivalenzrelation, bei der zwei Elemente als äquivalent (oder *konjugiert*) gelten, wenn sie durch einen inneren Automorphismus ineinander überführt werden können, die *Konjugationsklassen*.

Zwei Elemente $a, b \in G$ sind also konjugiert, wenn es ein $x \in G$ gibt mit $b = xax^{-1}$.

Die folgende Aussage heißt *Klassengleichung*.

LEMMA 25.2. *Sei G eine endliche Gruppe und seien $K_1, \ldots, K_r$ die Konjugationsklassen von G mit mindestens zwei Elementen. Dann ist*

$$\operatorname{ord}(G) = \operatorname{ord}(Z(G)) + \sum_{i=1}^{r} \#(K_i)$$

Beweis. Die Konjugationsklassen sind Äquivalenzklassen, daher bilden sie eine Zerlegung von G. Die Summe der Anzahl der Elemente in den Konjugationsklassen ist daher gleich der Ordnung von G. Die einelementigen Konjugationsklassen entsprechen dabei den Elementen im Zentrum der Gruppe. □

Die Anzahl der Elemente in den einzelnen Konjugationsklassen unterliegt starken Einschränkungen, die das folgende Lemma beinhaltet.

LEMMA 25.3. *Sei G eine endliche Gruppe und sei $a \in G$. Dann gelten folgende Aussagen.*

(1) *Die Menge $G_a = \{x \in G | \, xax^{-1} = a\}$ ist eine Untergruppe von G.*
(2) *Sei $K = [a]$ die Konjugationsklasse zu a. Dann ist*
$$\#(K) \, = \, \operatorname{ind}_G G_a.$$
(3) *Die Elementanzahl von $K = [a]$ ist ein Teiler von* $\operatorname{ord}(G)$.

Beweis. (1). Es ist klar, dass das neutrale Element zu G_a gehört. Seien $x, y \in G_a$. Dann ist

$$xya(xy)^{-1} = xyay^{-1}x^{-1} = xax^{-1} = a,$$

also $xy \in G_a$. Bei $x \in G_a$ ist $xax^{-1} = a$, was man direkt zu $a = x^{-1}ax$ auflösen kann, was wiederum $x^{-1} \in G_a$ bedeutet. (2). Wir betrachten die Abbildung

$$G \longrightarrow K,\, x \longmapsto xax^{-1}.$$

Da K genau aus allen zu a konjugierten Elementen besteht, ist diese Abbildung surjektiv. Unter dieser Abbildung ist G_a das Urbild von a. Es gilt $xax^{-1} = yay^{-1}$ genau dann, wenn $y^{-1}xax^{-1}y = a$ ist, also genau dann, wenn $y^{-1}x \in G_a$ ist. Das bedeutet, dass die Fasern der Abbildung gerade die Linksnebenklassen zur Untergruppe G_a sind. Daher ist $\#(K)$ gleich dem Index von G_a in G. (3) folgt aus (2) und Satz 4.16. □

LEMMA 25.4. *Es sei p eine Primzahl und G eine endliche Gruppe mit p^r, $r \geq 1$, Elementen. Dann ist das Zentrum Z von G nicht trivial.*

Beweis. Wir gehen von der Klassengleichung aus, also von

$$\operatorname{ord}(G) = \operatorname{ord}(Z) + \sum_{j \in J} n_j,$$

wobei n_j den Index der zu den mehrelementigen Konjugationsklassen C_j gehörenden echten Untergruppen (im Sinne von Lemma 25.3) $G_j \subseteq G$ bezeichnet. Jedes n_j ist nach Lemma 25.3 ein Vielfaches von p. Daher ist auch $\operatorname{ord}(Z)$ ein Vielfaches von p. Somit ist Z nicht trivial. □

Galoistheoretische Charakterisierung von konstruierbaren Zahlen

LEMMA 25.5. *Es sei $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$ eine Kette von quadratischen Körpererweiterungen in $\mathbb{C}$. Dann gibt es eine endliche Galoiserweiterung $K \subseteq M$ in $\mathbb{C}$, die L enthält, und die ebenfalls eine Kette von quadratischen Körpererweiterungen besitzt.*

Beweis. Wir führen Induktion über r, wobei die Fälle $r = 0, 1$ klar sind. Sei also eine Kette von quadratischen Körpererweiterungen

$$K = L_0 \subset L_1 \subset \ldots \subset L_r \subset L_{r+1} = L$$

gegeben. Nach Induktionsvoraussetzung gibt es einen Körper M, $L_r \subseteq M \subseteq \mathbb{C}$, derart, dass $K \subseteq M$ eine Galoiserweiterung ist, die eine Kette von quadratischen Körpererweiterungen besitzt. Als Galoiserweiterung über K ist M nach Satz 15.6 der Zerfällungskörper eines (separablen) Polynoms $F \in K[X]$. Wir können $L_{r+1} = L_r(x)$ mit $x^2 = a \in L_r$ schreiben. Wir betrachten das Polynom

$$H = \prod_{\varphi \in \operatorname{Gal}(M|K)} \left(X^2 - \varphi(a)\right).$$

Die Koeffizienten dieses Polynoms sind invariant unter der Galoisgruppe $\mathrm{Gal}\,(M|K)$ und gehören daher wegen Satz 15.6 zu K. Sei M' der Zerfällungskörper von H über M in $\mathbb{C}$. Dieser ist insgesamt der Zerfällungskörper vom Produkt FH über K, so dass $K \subseteq M'$ insbesondere eine Galoiserweiterung ist. Nach Konstruktion ist x eine Nullstelle von H, woraus sich $L = L_r(x) \subseteq M'$ ergibt. Nach Induktionsvoraussetzung gibt es eine Kette von quadratischen Körpererweiterungen

$$K = M_0 \subset M_1 \subset \ldots \subset M_s = M\,.$$

Diese erweitern wir sukzessive zu einer Kette

$$M = M_s \subset M_{s+1} \subset \ldots \subset M_t = M'$$

von quadratischen Körpererweiterungen, wobei $M_{s+i+1} = M_{s+i}(\sqrt{\varphi_i(a)})$ sei und φ_i die Automorphismen von $\mathrm{Gal}\,(M|K)$ durchlaufe. □

Satz 25.6. *Es sei $K \subseteq \mathbb{C}$ ein Unterkörper und $z \in \mathbb{C}$. Dann sind folgende Aussagen äquivalent.*

(1) *Die komplexe Zahl z ist aus K konstruierbar.*
(2) *Es gibt in $\mathbb{C}$ eine Körperkette aus quadratischen Körpererweiterungen*
$$K = L_0 \subset L_1 \subset \ldots \subset L_r = L$$
mit $z \in L$.
(3) *Das Element z ist algebraisch über K, und der Grad des Zerfällungskörpers von z über K ist eine Zweierpotenz.*
(4) *Das Element z ist algebraisch über K, und die Ordnung der Galoisgruppe des Zerfällungskörpers von z über K ist eine Zweierpotenz.*
(5) *Es gibt eine endliche Galoiserweiterung $K \subseteq M$ (in $\mathbb{C}$) mit $z \in M$, deren Grad eine Zweierpotenz ist.*

Beweis. Die Äquivalenz von (1) und (2) ergibt sich wie in Satz 24.4. Sei (2) erfüllt. Nach Lemma 25.5 gibt es eine endliche Galoiserweiterung $K \subseteq M$, die L und damit z enthält und die eine Kette von quadratischen Körpererweiterungen besitzt. Nach Satz 2.8 ist dann der Grad von $K \subseteq M$ eine Zweierpotenz. Es sei L' der Zerfällungskörper von z über K. Da M galoissch ist, gilt $L' \subseteq M$, und daher ist auch der Grad von $K \subseteq L'$ eine Zweierpotenz. Die Implikation von (3) nach (4) und von (4) nach (5) sind klar aufgrund von Satz 15.6. (5) $\Longrightarrow$ (2). Sei nun (5) erfüllt, und eine Galoiserweiterung $K \subseteq M$ in $\mathbb{C}$ mit $z \in M$ gegeben, deren Grad eine Zweierpotenz 2^r ist. Wir zeigen durch Induktion nach r, dass es eine Filtration der Körpererweiterung durch quadratische Körpererweiterungen gibt (also ohne direkten Bezug auf ein z). Dabei ist der Fall $r = 0$ trivial. Sei also $\mathrm{grad}_K\, M = 2^r$ $(r \geq 1)$ und die Existenz von Körperketten für kleinere Exponenten bereits bewiesen. Nach Satz 15.6 ist dann auch die Ordnung der Galoisgruppe $G = \mathrm{Gal}\,(M|K)$ gleich 2^r. Aufgrund von Lemma 25.4 gibt es ein nichttriviales Zentrum $Z \subseteq G$, so

dass es nach dem Hauptsatz für endliche abelsche Gruppen auch eine Untergruppe $H \subseteq Z$ mit zwei Elementen gibt. Als Untergruppe des Zentrums ist H ein Normalteiler in G. Wir betrachten $L = \mathrm{Fix}\,(H) \subseteq M$. Nach Satz 15.6 ist $\mathrm{grad}_L\, M = 2$ und nach Satz 16.4 ist $K \subseteq L$ eine Galoiserweiterung der Ordnung 2^{r-1} und besitzt nach Induktionsvoraussetzung eine Filtration aus quadratischen Körpererweiterungen. Diese Filtration wird durch $L \subset M$ zu einer solchen Gesamtfiltration ergänzt wird. □

Bemerkung 25.7. Wir betrachten die konstruierbare Zahl $u = \sqrt{1+\sqrt{3}}$ und knüpfen dabei an Beispiel 14.9 an. Dort wurde gezeigt, dass u das Minimalpolynom $X^4 - 2X^2 - 2$ besitzt, welches über $L = \mathbb{Q}[u]$ die Primfaktorzerlegung

$$X^4 - 2X^2 - 2 \;=\; (X-u)(X+u)(X^2 - 1 + \sqrt{3})$$

besitzt. Insbesondere ist L nicht normal, der Zerfällungskörper ist vielmehr $Z = L[\sqrt{1-\sqrt{3}}]$ und hat den Grad 8 über $\mathbb{Q}$. Seine Galoisgruppe ist nicht abelsch, denn andernfalls wäre jeder Zwischenkörper nach Satz 16.4 eine Galoiserweiterung von $\mathbb{Q}$, was aber für L nicht zutrifft.

Abschließend bemerken wir, dass es algebraische Elemente $z \in \mathbb{C}$ gibt, deren Minimalpolynom zwar den Grad 4 besitzt, wo der Grad des Zerfällungskörpers aber keine Zweierpotenz ist. Für ein hinreichend kompliziertes Polynom vom Grad 4 ist nämlich die Galoisgruppe des Zerfällungskörpers gleich der symmetrischen Gruppe S_4 und daher ist der Grad des Zerfällungskörpers gleich 12.