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

Körper- und Galoistheorie

Vorlesung 20

In den nächsten drei Vorlesungen möchten wir auflösbare Körpererweiterungen galoistheoretisch charakterisieren und insbesondere zeigen, dass nicht jede Körpererweiterung auflösbar ist, also sich nicht jedes Polynom durch (sukzessive) Radikale (auf)lösen lässt. In dieser Vorlesung bereiten wir dazu das gruppentheoretische Fundament.

Auflösbare Gruppen

Definition 20.1. Eine Gruppe G heißt *auflösbar*, wenn es eine Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G$$

gibt derart, dass G_i ein Normalteiler in G_{i+1} ist und die Restklassengruppe G_{i+1}/G_i abelsch ist (für jedes $i = 0, \ldots, k-1$).

Die in dieser Definition auftretende Filtrierung nennt man auch eine *auflösende Filtrierung*. Eine kommutative Gruppe ist natürlich auflösbar, wie die triviale Filtrierung $\{e\} \subseteq G$ zeigt.

Lemma 20.2. *Es sei G eine auflösbare Gruppe. Dann ist auch jede Untergruppe $H \subseteq G$ auflösbar.*

Beweis. Wir gehen von einer auflösenden Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G$$

aus, d.h., dass die G_i Normalteiler in G_{i+1} und die Restklassengruppen G_{i+1}/G_i kommutativ sind. Die Untergruppe $H \subseteq G$ besitzt durch $H_i = H \cap G_i$ eine induzierte Filtrierung. Dabei liegt das kommutative Diagramm

$$\begin{array}{ccc} H \cap G_i & \longrightarrow & H \cap G_{i+1} \\ \downarrow & & \downarrow \\ G_i & \longrightarrow & G_{i+1} \end{array}$$

vor. Wir betrachten den Homomorphismus

$$f : H \cap G_{i+1} \longrightarrow G_{i+1}/G_i .$$

Der Kern von f ist offenbar $H \cap G_i$. Daher ist H_i nach Lemma 5.6 ein Normalteiler in H_{i+1}, und der Quotient H_{i+1}/H_i ist nach Satz 5.12 eine Untergruppe von G_{i+1}/G_i und damit kommutativ. Also bilden die H_i eine auflösende Filtrierung von H. $\square$

Lemma 20.3. *Es sei G eine Gruppe, $N \subseteq G$ ein Normalteiler und G/N die zugehörige Restklassengruppe. Dann ist G genau dann auflösbar, wenn dies für N und G/N gilt.*

Beweis. Sei zunächst G auflösbar. Nach Lemma 20.2 ist $N \subseteq G$ auflösbar. Betrachten wir also die Restklassengruppe $H = G/N$ und fixieren wir eine auflösende Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G\,.$$

Es sei

$$q : G \longrightarrow H$$

der Restklassenhomomorphismus. Wir setzen $H_i = q(G_i)$, dies ist eine Filtrierung von H mit Untergruppen. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} G_i & \longrightarrow & G_{i+1} \\ \downarrow & & \downarrow \\ H_i & \longrightarrow & H_{i+1} \end{array} ,$$

wobei die vertikalen Homomorphismen surjektiv sind. Wir behaupten, dass H_i ein Normalteiler in H_{i+1} ist, und ziehen dazu

Lemma 5.4 heran. Sei also $h \in H_i$ und $x \in H_{i+1}$, die wir durch $\tilde{h} \in G_i$ bzw. $\tilde{x} \in G_{i+1}$ repräsentieren. Dann ist $xhx^{-1} = q(\tilde{x}\tilde{h}\tilde{x}^{-1})$ und wegen der Normalität von G_i ist $\tilde{x}\tilde{h}\tilde{x}^{-1} \in G_i$ und somit $xhx^{-1} \in H_i$. Wir betrachten die zusammengesetzte surjektive Abbildung

$$G_{i+1} \longrightarrow H_{i+1} \longrightarrow H_{i+1}/H_i\,.$$

Da G_i zum Kern dieser Abbildung gehört, gibt es aufgrund von Satz 5.10 eine surjektive Abbildung

$$G_{i+1}/G_i \longrightarrow H_{i+1}/H_i,$$

weshalb H_{i+1}/H_i ebenfalls kommutativ ist.

Seien nun N und $H = G/N$ auflösbar, sei $q : G \to G/N$ der Restklassenhomomorphismus und seien

$$\{e\} = N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots \subseteq N_{k-1} \subseteq N_k = N$$

und

$$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq H_{\ell-1} \subseteq H_\ell = H$$

auflösende Filtrierungen. Wir ergänzen die Filtrierung von N durch die Urbilder $G_j = q^{-1}(H_j)$ zu einer Filtrierung von G. Die surjektive Abbildung

$$G_{j+1} \longrightarrow H_{j+1} \longrightarrow H_{j+1}/H_j$$

besitzt den Kern G_j und zeigt, dass G_j ein Normalteiler in G_{j+1} mit kommutativer Restklassengruppe ist. $\square$

Die Definition einer auflösbaren Gruppe legt nicht nahe, wie man eine solche Filtrierung finden könnte. Ein systematischer Weg, eine solche Filtrierung zu finden, falls es denn eine gibt, wird durch iterierte Kommutatorgruppen gegeben. Ein Kommutator ist ein Element der Form $aba^{-1}b^{-1}$.

Definition 20.4. Zu einer Gruppe G heißt die von allen Kommutatoren $aba^{-1}b^{-1}$, $a, b \in G$, erzeugte Untergruppe die *Kommutatorgruppe* von G. Sie wird mit $K(G)$ bezeichnet.

Lemma 20.5. *Es sei G eine Gruppe und $K(G)$ ihre Kommutatorgruppe. Dann gelten folgende Aussagen.*

(1) *$K(G)$ ist ein Normalteiler in G.*
(2) *Die Restklassengruppe $G/K(G)$ ist abelsch.*
(3) *Die Gruppe G ist genau dann abelsch, wenn $K(G)$ trivial ist.*

Beweis. (1). Es ist zu zeigen, dass für jedes $x \in G$ der Automorphismus

$$G \longrightarrow G,\ g \longmapsto xgx^{-1},$$

die Untergruppe $K(G)$ in sich selbst überführt. Für einen Kommutator $aba^{-1}b^{-1}$ ist

$$\begin{aligned} xaba^{-1}b^{-1}x^{-1} &= (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1}) \\ &= (xax^{-1})(xbx^{-1})(xax^{-1})^{-1}(xbx^{-1})^{-1} \end{aligned}$$

wieder ein Kommutator. Daher wird auch jedes Produkt von Kommutatoren auf ein Produkt von Kommutatoren abgebildet und somit ist $xK(G)x^{-1} \subseteq K(G)$. (2). In der Restklassengruppe $G/K(G)$ ist

$$[a][b] = [a][b][b^{-1}a^{-1}ba] = [a][b][b^{-1}][a^{-1}][b][a] = [b][a].$$

(3). Eine Gruppe ist genau dann abelsch, wenn sämtliche Kommutatoren trivial sind. □

Definition 20.6. Es sei G eine Gruppe. Die i-te *iterierte Kommutatoruntergruppe* wird induktiv durch

$$K^0(G) = G \text{ und } K^i(G) = K(K^{i-1}(G))$$

definiert.

Die erste Kommutatorgruppe ist einfach die Kommutatorgruppe, die zweite Kommutatorgruppe ist die Kommutatorgruppe der Kommutatorgruppe, u.s.w. Dies ergibt insgesamt eine absteigende Filtrierung

$$G \supseteq K(G) \supseteq K^2(G) \supseteq K^3(G) \supseteq \ldots \supseteq .$$

Diese Filtrierung kann unendlich absteigend sein oder aber stationär werden, d.h. es kann $K^i(G) = K^{i+1}(G)$ gelten. Die Auflösbarkeit einer Gruppe kann mit dieser Filtrierung folgendermaßen charakterisiert werden.

Lemma 20.7. *Eine Gruppe ist genau dann auflösbar, wenn es ein i gibt derart, dass die i-te iterierte Kommutatorgruppe $K^i(G)$ trivial wird.*

Beweis. Wenn die Filtrierung der iterierten Kommutatorgruppen trivial wird, sagen wir

$$G \supseteq K(G) \supseteq K^2(G) \supseteq \ldots \supseteq K^{i-1}(G) \supseteq K^i(G) = \{e\},$$

so liegt unmittelbar eine auflösende Filtrierung vor, da ja

$$K^{j+1}(G) = K(K^j(G)) \subseteq K^j(G)$$

nach Lemma 20.5 ein Normalteiler ist mit einer abelschen Restklassengruppe. Sei nun G auflösbar. Wir zeigen durch Induktion über die Anzahl k der beteiligten Untergruppen in einer auflösenden Filtrierung von G, dass die Filtrierung der iterierten Kommutatorgruppen trivial wird. Dabei sind die Fälle $k = 0, 1$ klar. Wir betrachten die Untergruppe $G_{k-1} \subset G_k = G$ in der Filtrierung. Da die Restklassengruppe G/G_{k-1} kommutativ ist, wird die Kommutatorgruppe $K(G)$ unter der Restklassenabbildung auf 0 abgebildet und daher ist $K(G) \subseteq G_{k-1}$. Dabei besitzt natürlich G_{k-1} eine auflösende Filtrierung mit $k-1$ Untergruppen, und der Beweis zu Lemma 20.2 zeigt, dass dies auch für die Untergruppe $K(G)$ gilt. Nach Induktionsvoraussetzung wird also die Filtrierung von $K(G)$ durch die iterierten Kommutatorgruppen trivial. □

Lemma 20.8. *Für $n \leq 4$ sind die Permutationsgruppen S_n auflösbar.*

Beweis. Siehe Aufgabe 20.9. □

Lemma 20.9. *Für $n \geq 5$ sind die Permutationsgruppen S_n nicht auflösbar.*

Beweis. Wir betrachten eine Filtrierung

$$G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = S_n$$

derart, dass die $G_i \subseteq G_{i+1}$ Normalteiler sind mit kommutativen Restklassengruppen. Wir werden zeigen, dass jedes G_i sämtliche Dreierzykel (also Permutationen, bei denen drei Elemente zyklisch vertauscht werden, und alle übrigen festgelassen werden), enthält. Daher kann diese Filtrierung nicht bei der trivialen Gruppe enden, also ist $G_0 \neq \{e\}$. Die Aussage über die Dreierzykel beweisen wir durch absteigende Induktion, wobei der Fall $G_k = S_n$ klar ist. Sei also vorausgesetzt, dass G_{i+1} alle Dreierzykel enthält. Sei $\langle z_1, z_2, z_3 \rangle$ ein Dreierzyklus (mit verschiedenen Elementen $z_1, z_2, z_3 \in \{1, \ldots, n\}$.) Wegen $n \geq 5$ gibt es noch zwei weitere Elemente $x, y \in \{1, \ldots, n\}$, die von z_1, z_2, z_3 und untereinander verschieden sind. Nach Induktionsvoraussetzung gehören die Dreierzykel

$$\sigma = \langle z_1, z_2, x \rangle \text{ und } \tau = \langle z_1, z_3, y \rangle$$

zu G_{i+1}. Eine elementare Überlegung zeigt

$$\langle z_1, z_2, z_3 \rangle \;=\; \langle z_3, y, z_2 \rangle \circ \langle z_1, y, z_3 \rangle \;=\; (\sigma\tau\sigma^{-1}) \circ \tau^{-1} \;=\; \sigma\tau\sigma^{-1}\tau^{-1}.$$

Dieses Element wird unter der Restklassenabbildung

$$G_{i+1} \longrightarrow G_{i+1}/G_i$$

auf das neutrale Element abgebildet, da ja die Restklassengruppe kommutativ ist. Also ist $\langle z_1, z_2, z_3 \rangle \in G_i$. $\square$