Überblick zum Thema Galoisgruppen

Vorbemerkung: Ein Teil der hier aufgeführten Aussagen gehören in der Regel nicht zum Stoff einer einsemestrigen Algebra-Vorlesung, und werden für die Lösung der Staatsexamensaufgaben auch nicht unbedingt benötigt. Man kann sie aber auf jeden Fall verwenden, um die eigene Lösung zu kontrollieren.

(1) Häufig verwendete allgemeine Aussagen

- Ist K ein endlicher Körper oder gilt $\mathrm{char}(K) = 0$, dann ist jede algebraische Erweiterung von K separabel.
- Ist K ein Körper und L Zerfällungskörper eines Polynoms $f \in K[x]$ über K, dann ist $L|K$ eine normale Erweiterung.
- Ist $L|K$ eine Galois-Erweiterung vom Grad n, dann ist $\mathrm{Gal}(L|K)$ eine Gruppe der Ordnung n.

(Die ersten beiden Aussagen werden häufig verwendet, um zu zeigen, dass eine konkret vorgegebene Körpererweiterung eine Galois-Erweiterung ist. Die dritte Aussage liefert zumindest eine erste Information über die Struktur der Galoisgruppe.)

(2) Galoisgruppen als Untergruppen der S_n

- Sei K ein Körper, $\tilde{K}$ ein algebraischer Abschluss von K und $f \in K[x]$ ein Polynom, dessen irreduzible Faktoren alle separabel sind, mit genau n verschiedenen Nullstellen in $\tilde{K}$. Dann ist die Galoisgruppe $\mathrm{Gal}(f|K)$ des Polynoms f isomorph zu einer Untergruppe von S_n. (Die Bedingung an die irreduziblen Faktoren ist immer erfüllt, wenn K endlich ist oder $\mathrm{char}(K) = 0$ gilt.)
- Ist das Polynom f irreduzibel, dann ist $\mathrm{Gal}(f|K)$ isomorph zu einer transitiven Untergruppe von S_n. In diesem Fall ist n ein Teiler der Gruppenordnung $\mathrm{Gal}(f|K)$. (Dabei heißt eine Untergruppe U von S_n *transitiv*, wenn die Operation von U auf $M_n = \{1, ..., n\}$ transitiv ist. Dies ist gleichbedeutend damit, dass für beliebig vorgegebene $i, j \in M_n$ jeweils ein $\sigma \in U$ mit $\sigma(i) = j$ existiert.)
- Ist die Diskriminante $d(f)$ von f ein Quadrat in K, dann ist $\mathrm{Gal}(f|K)$ zu einer Untergruppe von A_n, der alternierenden Gruppe.

Für $d(f)$ existieren Formeln, die man sich allerdings nur bei Grad 2 und 3 gut merken kann:

$$d(f) = p^2 - 4q \quad \text{für} \quad f = x^2 + px + q \qquad \text{und} \qquad d(f) = -4p^3 - 27q^2 \quad \text{für} \quad f = x^3 + px + q.$$

Ist $f \in K[x]$ ein beliebiges Polynom vom Grad 3, $f = x^3 + ax^2 + bx + c$ mit $a, b, c \in K$, dann definiert man $g(x) = f(x - \frac{1}{3}a)$. Der zweithöchsten Koeffizient von g ist Null, somit kann $d(g)$ mit der angegebenen Formel ausgerechnet werden. Außerdem gilt $\mathrm{Gal}(f|K) = \mathrm{Gal}(g|K)$, weil f und g dieselben Zerfällungskörper besitzen.

(3) Polynome vom Grad 3, 4 und 5

- Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom vom Grad 3. Ist $d(f)$ in K ein Quadrat, dann gilt $\mathrm{Gal}(f|K) \cong A_3$, ansonsten $\mathrm{Gal}(f|K) \cong S_3$.
- Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom vom Grad 4. Ist $d(f)$ in K ein Quadrat, dann ist $\mathrm{Gal}(f|K)$ isomorph zu V_4 (Kleinsche Vierergruppe) oder zu A_4. Ansonsten ist $\mathrm{Gal}(f|K)$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$, zu D_4 (Diedergruppe) oder zu S_4.
- Ist $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad 5 mit genau drei reellen und zwei nicht-reellen Nullstellen, dann gilt $\mathrm{Gal}(f|\mathbb{Q}) \cong S_5$. Insbesondere ist $\mathrm{Gal}(f|\mathbb{Q})$ dann nicht auflösbar.

Das Ergebnis im zweiten Punkt kommt folgendermaßen zu Stande: Die Untergruppen S_4, A_4, V_4 sowie die zu D_4 und $\langle(1\ 2\ 3\ 4)\rangle$ konjugierten Untergruppen sind genau die transitiven Untergruppen von S_4. Mit Hilfe der Signumsfunktion überprüft man leicht, dass dabei nur V_4, A_4 Untergruppen von A_4 sind. Den dritten Punkt hatten wir im Kurs anhand einer passenden Übungsaufgabe besprochen.

(4) Endliche Körper

- Ist $E|F$ eine Körpererweiterung bestehend aus endlichen Körpern E und F und ist $n = [E : F]$, dann ist $E|F$ automatisch eine Galois-Erweiterung, und es gilt $\mathrm{Gal}(E|F) \cong \mathbb{Z}/n\mathbb{Z}$. Insbesondere sind Galoisgruppen von Erweiterungen endlicher Körper also immer zyklisch.

(5) Kreisteilungskörper

- Sei $\zeta_n = e^{2\pi i/n}$ (primitive n-te Einheitswurzel in $\mathbb{C}$). Dann gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Dabei wird jedem Element $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $a \in \mathbb{Z}$ und $\mathrm{ggT}(a, n) = 1$ der eindeutig bestimmte Automorphismus $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ mit $\sigma_a(\zeta_n) = \zeta_n^a$ zugeordnet.

(An dieser Stelle empfiehlt es sich, noch einmal zu wiederholen, was aus der Zahlentheorie-Vorlesung über die Struktur der primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ bekannt ist.)

(6) Polynome der Form $x^p - a$

- Sei p eine Primzahl und $a \in \mathbb{Q}$ eine Zahl mit der Eigenschaft, dass $f = x^p - a \in \mathbb{Q}[x]$ irreduzibel ist. Dann ist $L = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$ mit $\zeta_p = e^{2\pi i/p}$ ein Zerfällungskörper von f über $\mathbb{Q}$. Für die Gruppe $G = \mathrm{Gal}(f|\mathbb{Q})$ gilt $G = \mathrm{Gal}(L|\mathbb{Q}) = \langle\sigma, \tau\rangle$ mit $\sigma, \tau \in G$ gegeben durch

$$\sigma(\sqrt[p]{a}) = \zeta_p \sqrt[p]{a}\ ,\ \sigma(\zeta_p) = \zeta_p \qquad \text{und} \qquad \sigma(\sqrt[p]{a}) = \sqrt[p]{a}\ ,\ \tau(\zeta_p) = \zeta_p^m \quad ,$$

  wobei $m \in \mathbb{N}$ eine Primitivwurzel modulo p bezeichnet. Es ist $U = \mathrm{Gal}(L|\mathbb{Q}(\sqrt[p]{a})) = \langle\tau\rangle$ eine Untergruppe von $G = \mathrm{Gal}(L|\mathbb{Q})$, und $N = \mathrm{Gal}(L|\mathbb{Q}(\zeta_p)) = \langle\sigma\rangle$ ist ein Normalteiler von G. Darüber hinaus gilt für die Gruppenordnung $|G| = [L : \mathbb{Q}] = p(p-1)$, und G ist inneres semidirektes Produkt von N und U.

(Dieses Beispiel wird selten in dieser Form als Satz formuliert, aber Galois-Erweiterungen dieser Form kommen in den Aufgaben immer wieder mal vor. Es ist empfehlenswert und nicht sehr schwierig, diese Aussagen zur Übung noch einmal selbstständig zu verifizieren.)

(7) Konstruktion mit Zirkel und Lineal

- Eine Zahl $z \in \mathbb{C}$ (aufgefasst als Punkt in der Gaußschen Zahlenebene) ist genau dann mit Zirkel und Lineal konstruierbar, wenn der Grad des Minimalpolynoms von z über $\mathbb{Q}$ eine Zweierpotenz ist. Dies ist wiederum genau dann erfüllt, wenn eine Kette $\mathbb{Q} = K_0 \subsetneq ... \subsetneq K_r$ von Zwischenkörpern von $\mathbb{C}|\mathbb{Q}$ mit $z \in K_r$ und $[K_j : K_{j-1}] = 2$ für $1 \leq j \leq r$ existiert.

- Daraus folgt: Ist z konstruierbar, dann ist z algebraisch über $\mathbb{Q}$ und $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Zweierpotenz. (Achtung: Hier ist die Umkehrung im Allgemeinen falsch. Es gibt Elemente $z \in \mathbb{C}$ mit $[\mathbb{Q}(z) : \mathbb{Q}] = 4$, die nicht konstruierbar sind.)

- Ein Winkel $\alpha \in [0, 2\pi[$ ist genau dann konstruierbar, wenn die Zahl $e^{i\alpha}$ konstruierbar ist.

- Allgemeiner gilt: Eine Zahl $w \in \mathbb{C}$ ist *aus* einer gegebenen Punktmenge $S \subseteq \mathbb{C}$ konstruierbar, wenn das oben angegebene Kriterium statt für $\mathbb{Q}$ für den Grundkörper $\mathbb{Q}(S)$ erfüllt ist. Der Grad des Minimalpolynoms von w über $\mathbb{Q}(S)$ muss also eine Zweierpotenz sein, oder es existiert ein Körperturm wie angegeben, der bei $K_0 = \mathbb{Q}(S)$ statt bei $\mathbb{Q}$ startet.

Hierzu noch die zwei wichtigsten Standard-Beispiele:

- Die Quadratur des Kreises, also die Konstruktion eines Quadrats mit demselben Flächeninhalt wie der Einheitskreis, ist nicht möglich. Denn die Kantenlänge eines solchen Quadrats wäre $\sqrt{\pi}$, und aus der Konstruierbarkeit des Quadrats würde die Konstruierbarkeit von $\sqrt{\pi}$ folgen. Aber bekanntlich ist π eine transzendente Zahl, und daraus folgt, dass auch $\sqrt{\pi}$ transzendent ist (weil das Quadrat einer algebraischen Zahl wiederum algebraisch ist). Somit ist $\sqrt{\pi}$ nicht konstruierbar.

- Die Dreiteilung des Winkels ist nicht möglich. Denn wäre dies der Fall, dann könnte aus dem $60°$-Winkel $\frac{\pi}{3}$ der $20°$-Winkel $\frac{\pi}{9}$ konstruiert werden. Wegen $e^{\frac{1}{3}\pi i} = \frac{1}{2} + \frac{1}{2}i\sqrt{3}$ gilt $[\mathbb{Q}(e^{\frac{1}{3}\pi i}) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$ ist das Minimalpolynom von $e^{1/3\pi i}$ über $\mathbb{Q}$ vom Grad 2, und auch der Zerfällungskörper ist vom Grad 2. Also ist ist der Winkel $\frac{\pi}{3}$ auch ohne vorgegebene Punkte (oder Winkel) konstruierbar. Damit müsste auch der Winkel $\frac{\pi}{9}$ und die Zahl $e^{\frac{1}{9}\pi i}$ konstruierbar sein. Aber $e^{\frac{1}{9}\pi i}$ ist die 18-te Einheitswurzel, es gilt also $[\mathbb{Q}(e^{\frac{1}{9}\pi i}) : \mathbb{Q}] = \varphi(18) = 6$, und dies ist keine Zweierpotenz. Also ist der Winkel $\frac{\pi}{9}$ nicht konstruierbar.