6. Anwendungen der Galois-Theorie

Vorbemerkungen

Inzwischen sind wir in der Gruppen- und Körpertheorie zu einem gewissen Abschluß gelangt und wollen nun zeigen, wie die Galois-Theorie zur Lösung einiger berühmter klassischer Fragestellungen eingesetzt werden kann. Wir beginnen in 6.1 mit dem Problem der Auflösbarkeit algebraischer Gleichungen durch Radikale, also mit demjenigen Problem, das E. Galois zur Entwicklung seiner "Galois"-Theorie motiviert hat, und beweisen, daß für ein normiertes separables Polynom f mit Koeffizienten aus einem Körper K die algebraische Gleichung $f(x) = 0$ genau dann durch Radikale auflösbar ist, wenn die zugehörige Galois-Gruppe im gruppentheoretischen Sinne auflösbar ist.

Die grundsätzliche Beweisidee hierzu ist einfach zu erklären. Man reduziert das Problem auf der Körperseite auf den Fall, daß K genügend viele Einheitswurzeln enthält und betrachtet Erweiterungen von K, die durch Adjunktion eines *Radikals* entstehen, also einer Nullstelle eines Polynoms des Typs $X^n - c \in K[X]$ für $\operatorname{char} K \nmid n$ oder im Falle $p = \operatorname{char} K > 0$ auch des Typs $X^p - X - c \in K[X]$. Dies sind im wesentlichen die zyklischen Galois-Erweiterungen von K; vgl. 4.8/3 und 4.8/5. Entsprechend benutzt man auf der Seite der Galois-Gruppen, daß die zyklischen Gruppen sozusagen die "Bausteine" der auflösbaren endlichen Gruppen darstellen; vgl. 5.4/6. Dabei ist es für $p = \operatorname{char} K > 0$ üblich, auch die Nullstellen von Polynomen des Typs $X^p - X - c \in K[X]$ als "Radikale" zu interpretieren, da nur so die Charakterisierung auflösbarer (separabler) algebraischer Gleichungen mittels auflösbarer Galois-Gruppen auch für Körper positiver Charakteristik gültig ist. Man bedenke hierbei, daß für $p = \operatorname{char} K > 0$ Polynome des Typs $X^p - c$ nicht separabel sind, ihre Nullstellen also nicht mit Galois-theoretischen Methoden behandelt werden können. Weiter gehen wir in 6.1/10 noch auf eine notwendige Bedingung für die Auflösbarkeit irreduzibler algebraischer Gleichungen von Primzahlgrad ein, welche man insbesondere zur Konstruktion nicht-auflösbarer algebraischer Gleichungen verwenden kann. Auch dieses Kriterium geht auf E. Galois zurück.

Als zweite Anwendung bringen wir in 6.2 einen Galois-theoretischen Beweis des Fundamentalsatzes der Algebra. Dieser Satz bietet aus algebraischer Sicht einige Tücken, wie auch die Beweise der ersten Stunde zeigen. Dies hängt damit zusammen, daß der Körper $\mathbb{C}$ der komplexen Zahlen zwar aus den reellen Zahlen $\mathbb{R}$ in algebraischer Weise durch Adjunktion einer Quadratwurzel zu -1 gewonnen werden kann, daß aber zur Konstruktion von $\mathbb{R}$ Methoden benutzt werden, die im Grunde genommen der Analysis zuzurechnen sind. Daher hat man für Polynome $f \in \mathbb{C}[X]$ nur geringe Chancen, deren Nullstellen in algebraischer Weise als Elemente von $\mathbb{C}$ zu konstruieren. Stattdessen gehen wir indirekt vor. Wenn $\mathbb{C}$ nicht algebraisch abgeschlossen ist, so gibt es nach dem Satz von Kronecker eine nicht-triviale Erweiterung $L/\mathbb{C}$, die man als Galois-Erweiterung annehmen kann. Wir zeigen dann mittels Galois-Theorie und unter Benutzung der Tatsache, daß reelle Polynome ungeraden Grades stets eine reelle Nullstelle haben, daß man $L/\mathbb{C}$ vom Grad 2 annehmen darf. Eine solche Erweiterung kann aber nicht existieren; dies erkennt man unmittelbar, wenn man ausnutzt, daß positive reelle Zahlen eine Quadratwurzel in $\mathbb{R}$ und folglich alle komplexen Zahlen eine Quadratwurzel in $\mathbb{C}$ besitzen. Wie man sieht, stützt man sich auch bei dieser Schlußweise auf gewisse "analytische" Gegebenheiten der reellen Zahlen.

Als weitere Anwendung diskutieren wir in 6.3 Konstruktionen mit Zirkel und Lineal in der komplexen Zahlenebene. Eine genaue Analyse der Konstruktionsschritte, die man mit solchen Mitteln ausführen kann, zeigt, daß man beginnend mit den Punkten $0, 1 \in \mathbb{C}$ lediglich Punkte $z \in \mathbb{C}$ konstruieren kann, zu denen es eine Galois-Erweiterung $L/\mathbb{Q}$ mit $z \in L$ gibt, wobei der Grad $[L : \mathbb{Q}]$ eine Potenz von 2 ist. Insbesondere ist dann z algebraisch über $\mathbb{Q}$, mit einem Grad, der ebenfalls eine Potenz von 2 ist. So kann etwa die Konstruierbarkeit der Kubikwurzel $\sqrt[3]{2}$ ausgeschlossen werden, und es folgt als Beispiel, daß das antike Problem der Würfelverdoppelung mit Zirkel und Lineal nicht lösbar ist. Im übrigen werden wir auf die Untersuchungen von C. F. Gauß zur Konstruierbarkeit regelmäßiger n-Ecke eingehen.

6.1 Auflösbarkeit algebraischer Gleichungen

Um die Kompliziertheit des Problems der Auflösbarkeit algebraischer Gleichungen durch Radikale zu illustrieren, geben wir zunächst ohne Beweis die expliziten Auflösungen für Polynome vom Grad ≤ 4 an; Details hierzu findet man etwa bei B. L. van der Waerden [14], §59.

Sei also im folgenden K ein Körper und $f \in K[X]$ ein normiertes Polynom. Wir beginnen mit dem Fall $\operatorname{grad} f = 2$ und betrachten das Polynom

$$f = X^2 + aX + b \in K[X],$$

wobei $\operatorname{char} K \neq 2$ gelte. Die Nullstellen von f lassen sich mittels quadratischer Ergänzung bekanntlich in der Form

$$-\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$$

darstellen.

Im Falle $\operatorname{grad} f = 3$ gehen wir von dem Polynom

$$f = X^3 + aX^2 + bX + c \in K[X]$$

aus, wobei wir $\operatorname{char} K \neq 2,3$ voraussetzen. Mittels kubischer Ergänzung, man ersetze X durch $X - \frac{1}{3}a$, können wir annehmen, daß f von der etwas einfacheren Gestalt

$$f = X^3 + 3pX + 2q$$

ist. Die Nullstellen von f werden dann durch die sogenannten *Cardanoschen Formeln* beschrieben, und zwar berechnen sie sich zu

$$\begin{aligned} x_1 &= u + v, \\ x_2 &= \zeta u + \zeta^2 v, \\ x_3 &= \zeta^2 u + \zeta v, \end{aligned}$$

wobei ζ eine primitive dritte Einheitswurzel ist sowie die Wurzeln

$$u = \sqrt[3]{-q + \sqrt{q^2 + p^3}}, \qquad v = \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$

mit der Bedingung $uv = -p$ gewählt sind.

Schließlich betrachten wir noch ein Polynom vierten Grades, etwa

$$f = X^4 + aX^3 + bX^2 + cX + d \in K[X].$$

Es sei wieder $\operatorname{char} K \neq 2,3$. Ähnlich wie vorhin ersetze man X durch $X - \frac{1}{4}a$. Es genügt dann, den Spezialfall

$$f = X^4 + pX^2 + qX + r$$

zu betrachten. Zu f bildet man die sogenannte *kubische Resolvente*, nämlich das Polynom dritten Grades

$$X^3 - 2pX^2 + (p^2 - 4r)X + q^2.$$

Seine Nullstellen z_1, z_2, z_3 sind gemäß den Cardanoschen Formeln durch Wurzelausdrücke in den Koeffizienten darstellbar. Wählt man dann Quadratwurzeln zu $-z_1, -z_2, -z_3$ mit der Nebenbedingung

$$\sqrt{-z_1} \cdot \sqrt{-z_2} \cdot \sqrt{-z_3} = -q,$$

so sind

$$\begin{aligned} x_1 &= \tfrac{1}{2}(\sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}), \\ x_2 &= \tfrac{1}{2}(\sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}), \\ x_3 &= \tfrac{1}{2}(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}), \\ x_4 &= \tfrac{1}{2}(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}) \end{aligned}$$

die Nullstellen von f.

Algebraische Gleichungen vom Grad ≥ 5 lassen sich im allgemeinen nicht mehr durch Radikale auflösen. Bevor wir jedoch auf weitere Einzelheiten hierzu eingehen, soll zunächst der Begriff der Auflösbarkeit präzisiert werden.

Definition 1. *Eine endliche Körpererweiterung L/K heißt* durch Radikale auflösbar, *wenn es zu L einen Erweiterungskörper E sowie eine Körperkette*

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

gibt, so daß E_{i+1} jeweils aus E_i durch Adjunktion eines Elements des folgenden Typs entsteht, nämlich einer

(1) *Einheitswurzel oder*
(2) *Nullstelle eines Polynoms $X^n - a \in E_i[X]$ mit $\operatorname{char} K \nmid n$ oder*
(3) *Nullstelle eines Polynoms $X^p - X - a \in E_i[X]$ mit $p = \operatorname{char} K > 0$.*

Es ist L/K dann notwendig separabel.

Hauptziel dieses Abschnitts ist es, die Auflösbarkeit durch Radikale mit Hilfe der Auflösbarkeit von Galois-Gruppen (vgl. 5.4/3) zu charakterisieren.

Definition 2. *Eine endliche Körpererweiterung L/K heißt* auflösbar, *wenn es einen Oberkörper $E \supset L$ gibt, so daß E/K eine endliche Galois-Erweiterung mit (im Sinne von 5.4/3) auflösbarer Galois-Gruppe* $\operatorname{Gal}(E/K)$ *ist.*

Man beachte bei dieser Definition, daß eine Galois-Erweiterung L/K genau dann auflösbar ist, wenn die Galois-Gruppe $\operatorname{Gal}(L/K)$ auflösbar ist. Können wir nämlich L/K zu einer endlichen Galois-Erweiterung E/K mit auflösbarer Galois-Gruppe vergrößern, so ist $\operatorname{Gal}(L/K)$ nach 4.1/2 ein Quotient von $\operatorname{Gal}(E/K)$ und somit nach 5.4/7 ebenfalls auflösbar.

Die beiden Auflösbarkeitsbegriffe lassen sich in naheliegender Weise auf algebraische Gleichungen übertragen. Ist f ein nicht-konstantes (separables) Polynom mit Koeffizienten aus einem Körper K, so wähle man einen Zerfällungskörper L von f über K. Wir sagen dann, daß die algebraische Gleichung $f(x) = 0$ *über K auflösbar* bzw. *durch Radikale auflösbar* ist, wenn die Erweiterung L/K die entsprechende Eigenschaft besitzt.

Als nächstes wollen wir einige mehr oder weniger elementare Eigenschaften der beiden Auflösbarkeitsbegriffe behandeln.

Lemma 3. *Es sei L/K eine endliche Körpererweiterung sowie F ein beliebiger Erweiterungskörper von K. Man bette L mittels eines K-Homomorphismus in einen algebraischen Abschluß $\overline{F}$ von F ein, vgl. 3.4/9, und bilde das Kompositum FL in $\overline{F}$. Ist dann L/K auflösbar (bzw. galoissch mit auflösbarer Galois-Gruppe, bzw. durch Radikale auflösbar, bzw. ausschöpfbar durch eine Körperkette des in Definition 1 genannten Typs), so gilt dasselbe auch für die Erweiterung FL/F.*