26 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zwei weitere Anwendungen der Galoistheorie präsentieren. In der Folgevorlesung Algebra 2 werden wir die Galoistheorie und ihre Anwendungen fortsetzen und vertiefen, insbesondere auf endliche Körper, Radizierbare Körpererweiterungen, und Kreisteilungskörper.

Fundamentaler Satz der Algebra.

Bemerkung 26.1. Wir werden die folgenden (aus der Analysis bekannte) Eigenschaften von $\mathbb{R}$ und $\mathbb{C}$ benötigen. [1]

(i) Es ist $[\mathbb{C} : \mathbb{R}] = 2$, da $\mathbb{C} = \mathbb{R}(\sqrt{-1})$.

(ii) $a \in \mathbb{R}$ mit $a \geq 0$ hat eine Quadratwurzel in $\mathbb{R}$.

(iii) Jedes $f \in \mathbb{R}[x]$ ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.

Daraus folgt:

Lemma 26.2. (i) Jedes Polynom zweiten Grades aus $\mathbb{C}[x]$ hat eine Nullstelle in $\mathbb{C}$.

(ii) Insbesondere hat $\mathbb{C}$ keine quadratische Erweiterungen, d.h. keine Körpererweiterung L von $\mathbb{C}$ mit $[L : \mathbb{C}] = 2$.

Beweis: Dafür genügt es zu zeigen, dass $z \in \mathbb{C}$ eine Quadratwurzel in $\mathbb{C}$ hat.
Sei also $z = x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$. Wir wollen $a, b \in \mathbb{R}$ finden so dass:
$z = x + iy = (a + ib)^2 = (a^2 - b^2) + i2ab$, also so dass $x = a^2 - b^2$ und $y = 2ab$ $\quad(*)$
Betrachte

$$a^2 = \frac{1}{2}\,(x + \sqrt{x^2 + y^2})$$
$$b^2 = \frac{1}{2}\,(-x + \sqrt{x^2 + y^2}).$$

Bemerke dass $(x+\sqrt{x^2 + y^2}) \geq 0$ und $(-x+\sqrt{x^2 + y^2}) \geq 0$ (weil $\sqrt{x^2 + y^2} \geq \sqrt{x^2} = |x|$). Bemerkung 26.1(i) impliziert: es gibt eine Lösung $a, b \in \mathbb{R}$. Man prüft: $x = a^2 - b^2$ und $y^2 = 4a^2b^2$ (die Gleichungen $(*)$ sind abgesehen von der Wahl des Vorzeichens von a und b, dazu äquivalent). $\square$

---

[1] Diese Eigenschaften werden allgemeiner für reell abgeschlossene Körper und ihre algebraische Abschlüsse in der Vorlesung "Reelle algebraische Geometrie I " gezeigt.

Satz 26.3.
$\mathbb{C}$ ist algebraich abgeschlossen.

Beweis:

Es genügt zu zeigen das $\mathbb{C}$ keine echte endliche Körpererweiterung hat.
Sei also $L/\mathbb{C}$ endlich und betrachte $\mathbb{R} \subseteq \mathbb{C} \subseteq L$, ist. Zu zeigen: $L = \mathbb{C}$.

Setze $[L : \mathbb{R}] = 2^k m$ mit $k \in \mathbb{N}$ und $2 \nmid m$ (s. Bemerkung 26.1(i)).

Ohne Einschränkung ist $L/\mathbb{R}$ Galois (ggfs. L durch ist die Normalhülle von $L/\mathbb{R}$ ersetzen, siehe Bemerkung 25.8). Setze $G \coloneqq \text{Gal } (L/\mathbb{R})$. Dann ist $|G| = 2^k m$ (Satz 24.5).

Nun enthält G eine 2-Sylow $H \leq G$ (Sylow 1; Skript 20). Satz 24.5 impliziert dass $[L : \text{Inv } H] = |H| = 2^k$ beziehungsweise $[\text{Inv } H : \mathbb{R}] = m$.

Da aber jedes reelle Polynom ungeraden Grades eine Nullstelle in $\mathbb{R}$ hat (Bemerkung 26.1 (ii)), ergibt sich notwendig $m = 1$ (benutze Satz 25.9). Also $[L : \mathbb{R}] = 2^k$ und somit ist $[L : \mathbb{C}] = 2^{k-1}$. Wir müssen nun zeigen dass $k = 1$.

Sei $G' \coloneqq \text{Gal } (L/\mathbb{C})$. Wenn $L \neq \mathbb{C}$, also wenn $k \geq 2$, liefert Satz Sylow 1 eine Teilgruppe $H' \leq G'$ mit $|H'| = 2^{k-2}$. Also ist $[L : \text{Inv } H'] = 2^{k-2}$, und somit $[\text{Inv } H' : \mathbb{C}] = 2$.
Widerspruch (s. Lemma 26.2(ii)). □

Auflösbare Erweiterungen.

Satz 26.4. [Galoisgruppe als Untergruppen von S_n]
Sei K ein Körper, und $f \in K[x]$ separabel, mit $\deg f = n \in \mathbb{N}$. Sei L/K der Zerfällungskörper von f über K, und $a_1, \ldots, a_n \in L$ die Nullstellen von f. Die Abbildung

$$\begin{array}{rccl} \varphi : & \text{Gal } (L/K) & \longrightarrow & Sym\{a_1, \ldots, a_n\} \\ & \delta & \longmapsto & \delta \,|\, \{a_1, \ldots, a_n\} \end{array}$$

definiert einen injektiven Gruppenhomomorphismus.

Beweis:
$\delta \in \text{Gal } (L/K), f(a_i) = 0 \Rightarrow 0 = \delta(f(a_i)) = f(\delta(a_i))$, da δ die Koeffizienten von f fest lässt. Also ist $\delta(a_i)$ eine Nullstelle von f. Da δ injektiv ist, und $\delta : \{a_1, \ldots, a_n\} \to \{a_1, \ldots, a_n\}$, ist δ bijektiv. Damit ist φ wohldefiniert. Außerdem ist φ ein Gruppenhomomorphismus (ÜA).

Da $L = K(a_1, \ldots, a_n)$ und $\delta \in \text{Gal } (L/K)$ bereits eindeutig durch seine Werte auf $\{a_1, \ldots, a_n\}$ bestimmt ist (ÜA), ist φ injektiv.

□

Korollar 26.5.
Sei L/K eine endliche Galois Erweiterung vom Grad n, so lässt sich Gal (L/K) als Untergruppe von S_n auffassen.

Definition 26.6.
Eine endliche Körpererweiterung L/K ist *auflösbar*, wenn es einen Oberkörper $E \supset L$ gibt, so dass E/K eine endlische Galois Erweiterung mit auflösbarer Gal (E/K) ist.

Korollar 26.7.
Sei L/K eine separable Erweiterung vom Grad ≤ 4, dann ist L/K auflösbar.

Beweis:

Satz 25.9 impliziert dass $L = K(a)$ eine einfache Erweiterung ist. Sei $f \in K[x]$ das $Min.Pol._K a$. Sei L' ein Zerfällungskörper von f über K. Die Galoisgruppe Gal (L'/K) lässt sich als Untergruppe von S_4 auffassen (s. Korollar 26.5). Da S_4 und alle ihre Untergruppen auflösbar sind (s. Beispiel 18.9), so sind L'/K und L/K auflösbar. $\square$

Korollar 26.8.
Es gibt endlich separable Körpererweiterungen, die nicht auflösbar sind.

Beweis:
Sei F ein Körper und setze $L := F(T_1, \ldots, T_n) = \text{Quot }(F[T_1, \ldots, T_n])$
(der Körper der rationalen Funktionen in endlich vielen Variablen $T_1, \ldots, T_n$).

Jede $\pi \in S_n$ definiert einen Automorphismus von L, in dem man π auf die Variablen $T_1, \ldots, T_n$ anwendet:

$$\begin{array}{ccc} F(T_1, \ldots, T_n) & \longrightarrow & F(T_1, \ldots, T_n) \\ \frac{g(T_1, \ldots, T_n)}{h(T_1, \ldots, T_n)} & \longmapsto & \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})} \end{array}$$

Sei $K := \text{Inv } S_n \subseteq L$. Es ist (s. Satz 24.3) L/K Galois und Gal $(L/K) = S_n$. Wähle nun $n \geq 5$, dann ist Gal (L/K) nicht auflösbar (s. Korollar 20.4). $\square$