# § 0. Wiederholung: Körpererweiterungen und polynomiale Gleichungen

Erstes Hauptziel der Algebra II - Vorlesung ist der Hauptsatz der Galoistheorie, der Körpererweiterungen und endliche Gruppen miteinander verbindet. Dieser Satz wird dann auf die (Un-) Lösbarkeit polynomialer Gleichungen angewandt.
Zur Vorbereitung: Wiederholung aus Algebra.

Ausgangsfrage: Wie konstruiert man Lösungen algebraischer Gleichungen?
Beispiel: $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, ein Polynom mit rationalen Koeffizienten
$f(x)$ hat in $\mathbb{Q}$ keine Nullstellen — warum sind $\pm\sqrt{2} \notin \mathbb{Q}$?
Wie findet / konstruiert man $\pm\sqrt{2}$, wenn $\mathbb{Q}$ und $f(x) \in \mathbb{Q}[x]$ gegeben sind? — warum kann es keine anderen Nullstellen geben?

Satz von Kronecker (Algebra, Theorem 4.7): Sei $f(x) \in K[x]$, $K$ ein Körper, $f(x)$ irreduzibel (Definition?). Dann existiert eine einfache und endliche Körpererweiterung $L = K(a) \supset K$, so daß $f(x)$ in $L$ mindestens die Nullstelle $a$ hat. Ist $-a$ auch immer eine Nullstelle?

Es gilt $\underset{\dim_K L}{\underset{\shortparallel}{[L:K]}} = \underset{\text{Grad von } f}{\underset{\shortparallel}{\deg f}}$

Induktiv findet man alle Nullstellen von $f$.
Also ist jede polynomiale Gleichung mit Koeffizienten in einem Körper lösbar (in einem endlichen Erweiterungskörper).

Konstruktion von $L$ und explizite Bestimmung von $a$:
$f(x)$ erzeugt ein Ideal $\langle f(x)\rangle \subset K[x]$, das maximal ist.
Denn: $\langle f(x)\rangle \subset \langle g(x)\rangle \Rightarrow f(x) = g(x)h(x)$ für ein $h(x)$ — Details?
$f(x)$ irreduzibel $\Rightarrow \langle g(x)\rangle = \langle f(x)\rangle$ oder $\langle g(x)\rangle = K[x]$
Warum ist $K[x]$ ein Hauptidealring?

$\Rightarrow K[x]/\langle f(x)\rangle$ ist ein Körper warum? Sei $L := K[x]/\langle f(x)\rangle$.

$$\begin{tikzcd} K[x] \arrow[r, two heads, "\text{surj}"] & K[x]/\langle f(x)\rangle = L \\ K \arrow[u, hook, "\text{inj}"] \arrow[ur, "\text{inj warum?}"'] & \end{tikzcd}$$

Sei $a := \bar{x} = x + \langle f(x)\rangle \in L$

$\Rightarrow f(a) = f(\bar{x}) = \overline{f(x)} = 0$ in $L$

$\Rightarrow$ die gesuchte Lösung von $f(x) = 0$ ist $\bar{x} = a$.

Im Beispiel: $f(x) = x^2 - 2$ ist irreduzibel über $\mathbb{Q}$ mindestens drei Gründe dafür

$$\begin{tikzcd} \mathbb{Q}[x] \arrow[r, two heads] & \mathbb{Q}[x]/\langle x^2-2\rangle = L \ni a := \bar{x} \\ \mathbb{Q} \arrow[u, phantom, "\cup"] \arrow[ur] & \end{tikzcd}$$

definiere $a := \sqrt{2}$ oder $a := -\sqrt{2}$ macht das einen Unterschied?

$L = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ was bedeutet das?

Für $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$, $f(x)$ irreduzibel, gilt:

$\underbrace{K[x]/\langle f(x)\rangle}_{\substack{\shortparallel \\ L}}$ hat $K$-Basis $1, x, x^2, \ldots, x^{n-1}$ warum?

$\Rightarrow [L:K] = \deg f = n$

z.B. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$

Um Körpererweiterungen $K \subset L$ besser zu verstehen, betrachtet man $K$-Automorphismen von $L$: $\mathrm{Aut}_K(L) = \{\varphi : L \to L : \varphi \text{ Körperisom}, \varphi|_K = \mathrm{id}_K\}$

Falls $[L:K] < \infty$: $\mathrm{Aut}_K(L) = \{\varphi : L \to L \text{ Körperhom}, \varphi|_K = \mathrm{id}_K\}$ warum?

$f(x) = \sum a_i x^i$, $\varphi^*(f(x)) := \sum \varphi(a_i) x^i = \sum a_i x^i = f(x)$, falls $\varphi$ $K$-Homom

$\Rightarrow \varphi$ bildet Nullstellen von $f(x)$ wieder auf Nullstellen ab nachprüfen

Im Beispiel: $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ bildet $\sqrt{2}$ auf $\pm\sqrt{2}$ ab

$\varphi_1 : \sqrt{2} \to \sqrt{2} \Rightarrow \varphi_1 = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$

$\varphi_2 : \sqrt{2} \to -\sqrt{2}$, anderer $K$-Hom ist $\varphi_2$ ein Körperisom?

In diesem Fall ist $2 = |\mathrm{Aut}_K(L)| = [L:K]$

Das gilt nicht immer, sondern ist eine Eigenschaft der Körpererweiterung $L/K$.

$L/K$ ist separabel $:\Leftrightarrow [L:K]_s = [L:K]$ ($\leq$ gilt immer)
warum?
$[L:K]_s = |\{K\text{-Homom } L \to \bar{K}\}|$
$\bar{K}$ = algebraischer Abschluß von $K$
was ist das?

Sei $L/K$ endlich. Dann sind äquivalent
(Algebra, Theorem 6.12): • $L/K$ ist separabel
• alle $a \in L$ sind separabel über $K$, d.h. jedes Minimalpolynom $m_{a,K}$ hat nur einfache Nullstellen
was ist das?
• $L = K(a_1, \ldots, a_n)$ mit separablen Elementen $a_1, \ldots, a_n$ über $K$
Falls $\operatorname{char} K = 0$: $L/K$ ist separabel
Falls $L$ endlich: $L/K$ ist separabel

Zweite wichtige Eigenschaft von Körpererweiterungen:
$L/K$ ist normal $:\Leftrightarrow$ $L$ ist der Zerfällungskörper einer Menge von Polynomen $\Lambda \subset K[x]$
Das heißt: $L = K(S)$, wobei $S = \{$Nullstellen in $\bar{K}$ von $f \in \Lambda \subset K[x]\}$
Für $L/K$ sind äquivalent (Algebra, Theorem 6.7):
- $L/K$ ist normal
- Jeder $K$-Homomorphismus $\varphi: L \to \bar{K}$ erfüllt $\varphi(L) = L$
- $\forall f \in K[x]$ irreduzibel über $K$ gilt: wenn $f$ in $L$ eine Nullstelle hat, dann zerfällt $f$ über $L$ in ein Produkt von Linearfaktoren

Prüfen Sie die folgenden Beispiele im Detail nach und bestimmen Sie $\operatorname{Aut}_K(L)$

$K = \mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2})$ ist normal und separabel
$K = \mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2})$ ist separabel, aber nicht normal
$x^3 - 2$ ist irreduzibel über $\mathbb{Q}$
zwei Nullstellen, $e^{2\pi i/3}$ und $e^{4\pi i/3}$ liegen nicht in $\mathbb{R}$
nur ein $\varphi: L \to \bar{K} = \bar{\mathbb{Q}}$ erfüllt $\varphi(L) = L$