Ausblick: Die Cardanischen Formeln

Satz

Seien K ein Körper mit $\mathrm{char}(K) \neq 2, 3$ und $p, q \in K$, L ein algebraisch abgeschlossenener Erweiterungskörper, $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ und außerdem

$$\beta = \sqrt[3]{-\tfrac{1}{2}q + \sqrt{\tfrac{1}{4}q^2 + \tfrac{1}{27}p^3}}, \gamma = \begin{cases} \sqrt[3]{-\frac{1}{2}q - \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}} & \text{falls } \beta = 0 \\ -\frac{1}{3}p\beta^{-1} & \text{falls } \beta \neq 0. \end{cases}$$

Dann sind die drei Nullstellen des Polynoms $f = x^3 + px + q \in K[x]$, eventuell mit Vielfachheiten, geben durch

$$\alpha_1 = \beta + \gamma \quad , \quad \alpha_2 = \zeta\beta + \zeta^2\gamma \qquad \text{und} \qquad \alpha_3 = \zeta^2\beta + \zeta\gamma.$$

Wiederholung: Algebraische Körpererweiterungen

- Körpererweiterung $L|K$ = Paar (K, L), wobei L einen Körper und K einen Teilkörper von L bezeichnet
  Beispiele: (i) $\mathbb{R}|\mathbb{Q}$ (ii) $\mathbb{F}_4|\mathbb{F}_2$, wobei

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{\bar{0}, \bar{1}, \alpha, \alpha + \bar{1}\} \text{ mit } \alpha^2 + \alpha + \bar{1} = \bar{0}$$

- Erweiterungsgrad $[L : K]$ = Dim. von L als K-Vektorraum
- Möglichkeiten zur Bestimmung des Erweiterungsgrades

  (i) Gradformel: $[L : K] = [L : M] \cdot [M : K]$
  falls M ein Zwischenkörper von $L|K$ ist

  (ii) Minimalpolynom: $[K(\alpha) : K] = \operatorname{grad}(f)$
  falls α algebraisch über K und $f = \mu_{\alpha,K}$ ist

Wiederholung: Algebraische Körpererweiterungen (Forts.)

- Eine Körpererweiterung $L|K$ wird endlich genannt, wenn $[L : K]$ endlich ist.
- Jede endliche Körpererweiterung ist algebraisch.
- Es gibt unendliche algebraische Erweiterungen (zum Beispiel $\mathbb{F}_p^{\mathrm{alg}}|\mathbb{F}_p$, wobei $\mathbb{F}_p^{\mathrm{alg}}$ den algebraischen Abschluss von $\mathbb{F}_p$ bezeichnet).
- Jede endlich erzeugte algebraische Erweiterung ist endlich.
- Ist $\alpha \in L$ algebraisch über K und $n = [K(\alpha) : K]$, dann gilt

$$K(\alpha) \quad = \quad \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in K\}.$$

Wiederholung: Fortsetzung von Körperhomomorphismen

Sei $L|K$ eine endliche und $M|K$ eine beliebige Körperweiterung.

- K-Homomorphismus = Körperhomomorphismus $L \to M$, der $\mathrm{id}_K : K \to K$ fortsetzt
- Eindeutigkeit: Ist $L = K(\alpha_1, ...\alpha_r)$, dann ist jeder K-Homomorphismus $\sigma : L \to M$ durch $\sigma(\alpha_k)$ mit $1 \leq k \leq r$ eindeutig festgelegt.
- Bedingung: Ist $\sigma : L \to M$ ein K-Homomorphismus, $\alpha \in L$, und $f \in K[x]$ mit $f(\alpha) = 0$, dann folgt $f(\sigma(\alpha)) = 0$.
- Existenz: Ist $f \in K[x]$ ein irreduzibles Polynom, und $\alpha \in L$ mit $f(\alpha) = 0$, dann ist die Anzahl der K-Homomorphismen $K(\alpha) \to M$ gleich der Anzahl der Nullstellen von f in M.

Wiederholung: Normale Körpererweiterungen

- Eine normale Körpererweiterung ist eine algebraische Erweiterung $L|K$ mit der Eigenschaft, dass jedes irreduzible Polynom $f \in K[x]$, das in L eine Nullstelle besitzt, über L in Linearfaktoren zerfällt.
  - Beispiel: jede Erweiterung vom Grad 2
  - Gegenbeispiel: $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$

- Ein Zerfällungskörper eines Polynoms $f \in K[x]$ über einem Körper K ist ein minimaler Erweiterungskörper L von K, über dem f in Linearfaktoren zerfällt. (Dabei bedeutet die Minimalität, dass L über K durch die Nullstellen von f in L erzeugt wird.)

Wiederholung: Normale Körpererweiterungen (Forts.)

- Eine endliche Körpererweiterung $L|K$ ist genau dann normal, wenn L Zerfällungskörper eines Polynoms $f \in K[x]$ über K ist.
- Eine algebraische Körpererweiterung $L|K$ ist genau dann normal, wenn L Zerfällungskörper einer Menge $S \subseteq K[x]$ von Polynomen über K ist.
- Ist $S_K \subseteq K[x]$ die Menge aller nicht-konstanten Polynome, dann erhält man als Zerfällungskörper von S_K über K den algebraischen Abschluss von K.

wichtige Anwendung:
Existenz und Eindeutigkeit der endlichen Körper

- Ist p eine Primzahl und $n \in \mathbb{N}$, dann existiert ein Körper $\mathbb{F}_{p^n}$ mit p^n Elementen.
- Dieser ist bis auf Isomorphie eindeutig bestimmt.
- Es handelt sich um den Zerfällungskörper des Polynoms $f = x^{p^n} - x \in \mathbb{F}_p[x]$ über $\mathbb{F}_p$. (Genauer gesagt besteht $\mathbb{F}_{p^n}$ aus den p^n verschiedenen Nullstellen von f.)
- Für alle $m, n \in \mathbb{N}$ gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ genau dann, wenn m ein Teiler von n ist.
- Der algebraische Abschluss $\mathbb{F}_p^{\mathrm{alg}}$ von $\mathbb{F}_p$ hat die Form

$$\mathbb{F}_p^{\mathrm{alg}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}.$$

Moodle: kxp 8635 MAGH

Separable Körpererweiterungen

Def. $f \in K[x]$ irreduzibles Polynom (K Körper)

f separabel $\iff ggT(f, f') = 1$

(gleichbed.: f hat in keiner Erw. von K mehrfache Nullst.)

Sei $L|K$ eine Körpererw.

i) $\alpha \in L$ separabel über K $\iff$ Das Minimalpolynom $M_{\alpha,K}$ ist ein separables Pol. (Insb. ist α algebraisch über K.)

(iii) $L|K$ ist separabel $\Leftrightarrow$ Jedes $\alpha \in L$ ist separabel über K

- $\mathrm{char}(K) = 0$ (z.B. $K = \mathbb{Q}$) $\Rightarrow$ Jede algebraische Erweiterung von K ist algebraisch.
- K endl. Körper (z.B. $K = \mathbb{F}_p$, p Primzahl)
  $\Rightarrow$ Jede alg. Erw. von K ist separabel.
- Satz vom primitiven Element:
  Ist $L|K$ eine endliche separable Erweiterung, dann existiert ein $\gamma \in L$ mit $L = K(\gamma)$.

Definition der Galois-Erweiterungen und Galoisgruppen

Definition (21.1)

Eine Körpererweiterung $L|K$ wird Galois-Erweiterung oder auch galois'sche Erweiterung genannt, wenn sie normal und separabel ist. Die Gruppe $\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$ heißt dann die Galoisgruppe der Erweiterung $L|K$.

Beispiel für eine Galoisgruppe

$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$L|K$ ist eine Galois-Erweiterung,

denn:
- $\sqrt{2}, \sqrt{3}$ sind algebraisch über $\mathbb{Q}$ $\Rightarrow$ $L|K$ ist algebr.
- $\mathrm{char}(K) = 0$, $L|K$ ist algebraisch $\Rightarrow$ $L|K$ ist separabel
- Man kann überprüfen: L ist Zerfällungskörper von $f = (x^2-2)(x^2-3) \in K[x]$ über K $\Rightarrow$ $L|K$ ist normal

Ziel: Bestimmung der Elemente von

$\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(a) = a \ \forall\, a \in K\}$

- Jedes $\sigma \in \mathrm{Gal}(L|K)$ ist durch die Bilder $\sigma(\sqrt{2})$, $\sigma(\sqrt{3})$ eindeutig festgelegt.
- Da $\sqrt{2}$ Nullstelle von x^2-2 ist, muss $\sigma(\sqrt{2})$ jeweils Nullstelle von x^2-2 sein.

  $\Rightarrow \sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}$, analog $\sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}$

Zwischenergebnis: $\mathrm{Gal}(L|K)$ hat höchstens vier Elemente ($= 2 \cdot 2$ Kombinationsmögl.)

- Man kann zeigen, dass X^2-2 nicht nur über $\mathbb{Q}$, sondern auch über $\mathbb{Q}(\sqrt{3})$ irreduzibel ist. Fortsetzungssatz → Es gibt einen $\mathbb{Q}(\sqrt{3})$-Hom. $\sigma: L = \mathbb{Q}(\sqrt{3})(\sqrt{2}) \to \mathbb{C}$ mit $\sigma(\sqrt{2}) = -\sqrt{2}$.
leicht zu sehen: $\sigma \in Gal(L|K)$, $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$.
zeige analog: Es gibt ein $\tau \in Gal(L|K)$ mit $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$.
Insgesamt ist $Gal(L|K)$ also gegeben durch

id_L	σ	τ	$\sigma \circ \tau$
$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$
$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$