

# Tutorium 12

## 1 Der algebraische Abschluss

**1 Aufgabe.** Sei  $K$  Körper und  $I \triangleleft K[X_1, \dots, X_n]$  echtes Ideal. Zeige:

- (a)  $K$  ist Teilkörper von  $K[X_1, \dots, X_n]/I$
- (b) Ist  $I$  maximales Ideal, dann ist  $(K[X_1, \dots, X_n]/I)/K$  Körpererweiterung
- (c) Gilt zusätzlich  $n = 1$ , so ist die Körpererweiterung sogar endlich.

*Beweis.* (a) Die Abbildung

$$\phi : K \rightarrow K[X_1, \dots, X_n]/I, \quad x \mapsto \bar{x}$$

ist Homomorphismus (Komposition von Inklusion und kanonischer Projektion), und injektiv wegen

$$\phi(x) = 0 \Rightarrow x \in K \cap I \Rightarrow x = 0$$

(sonst wäre  $x$  Einheit in  $I$  und  $I$  kein echtes Ideal!)

(b) Klar, dann ist nämlich  $K[X_1, \dots, X_n]/I$  auch Körper.

(c)  $K[X_1]$  ist euklidisch. Folglich gilt  $I = (m)$  für ein irreduzibles  $m \in K[X_1]$ , und Division mit Rest durch  $m$  zeigt, dass  $\{1, X_1, \dots, X_1^{\deg(m)-1}\}$  Erzeugendensystem ist.  $\square$

**2 Lemma** (Kronecker). Sei  $K$  ein Körper und  $f \in K[X] \setminus K$ . Dann gibt es

- (a) eine endliche Körpererweiterung  $L/K$ , so dass  $f$  in  $L$  eine Nullstelle hat,
- (b) eine endliche Körpererweiterung  $L/K$ , so dass  $f$  über  $L$  in Linearfaktoren zerfällt.

*Beweis.* (a) O.E. sei  $f$  irreduzibel (sonst irreduziblen Faktor betrachten). Nach Aufgabe 1 tut es  $L := K[X]/(f)$ , denn  $(f)$  ist maximales Ideal. Eine Nullstelle ist  $\alpha := \bar{X}$ .

(b) Induktion.  $\square$

(Wie hängen  $L$  und  $K[\alpha]$  zusammen?)

**3 Definition.**  $L/K$  heißt *Zerfällungskörper* von  $f \in K[X] \setminus K$  über  $K$ , falls

- (i)  $f$  zerfällt über  $L$  in Linearfaktoren
- (ii)  $L$  wird über  $K$  von den Nullstellen von  $f$  erzeugt

(Ein Zerfällungskörper ist also "gerade groß genug" dass  $f$  in Linearfaktoren zerfällt.)

**4 Korollar.** Sei  $f \in K[X] \setminus K$ . Dann existiert ein Zerfällungskörper  $Z(f)$  und es gilt  $[Z(f) : K] \leq \deg(f)!$ .

**5 Aufgabe** (ohne Kronecker). Bestimme den Zerfällungskörper von

$$f := X^3 + X^2 + X + 1$$

über  $\mathbb{Q}$  sowie dessen Grad.

*Lösung.* Man sieht sofort, dass  $-1 \in \mathbb{Q}$  Nullstelle ist und also

$$f = (X + 1)(X^2 + 1)$$

Bekanntlich ist  $g := X^2 + 1$  Minimalpolynom von  $i$  über  $\mathbb{Q}$ , d.h.  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ .

$\mathbb{Q}(i)$  ist damit auch Zerfällungskörper, denn es gilt

$$f = (X + 1)(X + i)(X - i)$$

$\square$

**6 Aufgabe** (mit Kronecker). Bestimme den Zerfällungskörper von

$$f := X^3 + X^2 + 1$$

über  $\mathcal{F}_2$  sowie dessen Grad.

*Lösung.* Man sieht zunächst durch ausprobieren, dass  $f$  keine Nullstelle in  $\mathcal{F}_2$  hat; also ist  $f$  irreduzibel.

Kronecker: Setze  $K := \mathcal{F}_2[X]/(f)$ . Diese Körpererweiterung hat Grad 3, denn  $f$  ist irreduzibel. Ferner ist  $\alpha := \bar{X}$  nach Konstruktion eine Nullstelle von  $f$ , und es gilt sogar

$$f = (X - \alpha)(X^2 + (\alpha + 1)X + \alpha(\alpha + 1)) =: gh$$

$K$  ist als Vektorraum isomorph zu  $\mathcal{F}_2^3$ , hat also 8 Elemente. Wir suchen eine weitere Nullstelle:

$$\begin{aligned} h(\alpha^2) &= \alpha^4 + (\alpha + 1)\alpha^2 + \alpha(\alpha + 1) \\ &= \alpha \left( \underbrace{\alpha^3 + \alpha^2 + 1}_{=0} + \underbrace{\alpha + \alpha}_{=0} \right) = 0 \end{aligned}$$

Damit ist  $\alpha^2$  eine weitere Nullstelle, und  $f$  zerfällt über  $K$  in Linearfaktoren.

$K$  ist also Zerfällungskörper von  $f$  vom Grad 3. □

**7 Definition.** Ein Körper  $K$  heißt *algebraisch abgeschlossen* wenn jedes  $f \in K[X] \setminus K$  eine Nullstelle in  $K$  hat.

**8 Proposition.** Die folgenden Aussagen sind äquivalent.

- (i)  $K$  ist algebraisch abgeschlossen
- (ii) jedes  $f \in K[X] \setminus K$  zerfällt über  $K$  in Linearfaktoren
- (iii)  $K$  besitzt keine echte algebraische Körpererweiterung

**9 Aufgabe.** (iv) für jedes  $f \in K[X] \setminus K$  ist  $\phi : K \rightarrow K, x \mapsto f(x)$  surjektiv

*Beweis.* (i) $\Rightarrow$ (iv): Für jedes  $a \in K$  hat  $f - a \in K[X] \setminus K$  eine Nullstelle  $x$ , damit  $\phi(x) = a$ .

(iv) $\Rightarrow$ (i): Insbesondere liegt 0 im Bild, d.h. jedes  $f \in K[X] \setminus K$  hat eine Nullstelle. □

**10 Satz.** Zu jedem Körper  $K$  existiert eine algebraische Körpererweiterung  $\bar{K}/K$ , die algebraisch abgeschlossen ist.

$\bar{K}$  heißt algebraischer Abschluss von  $K$ .

**11 Aufgabe.** Endliche Körper sind nicht algebraisch abgeschlossen.

*Beweis.* Sei  $K = \{a_1, \dots, a_n\}$  endlicher Körper. Dann hat das Polynom

$$f := 1 + \prod_{k=1}^n (X - a_k)$$

vom Grad  $n \geq 2$  keine Nullstelle in  $K$ . □

## 2 Körperhomomorphismen

**12 Aufgabe.** Sei  $K$  ein Körper.

- (a)  $\text{char}(K) = 0 \Rightarrow K$  enthält einen zu  $\mathbb{Q}$  isomorphen Teilkörper
- (b)  $\text{char}(K) = p \neq 0 \Rightarrow K$  enthält einen zu  $\mathcal{F}_p$  isomorphen Teilkörper

Diese Teilkörper heißen *Primkörper*.

*Beweis.* Betrachte den Homomorphismus

$$i : \mathbb{Z} \rightarrow K, \quad n \mapsto n \cdot 1$$

(a) Der Homomorphismus  $i$  ist injektiv, erfüllt damit insbesondere  $i(\mathbb{Z} \setminus \{0\}) \leq K^\times$ . Nach der UAE des Quotientenkörpers folgt die Existenz eines Homomorphismus  $\tilde{i} : \mathbb{Q} \rightarrow K$ . Dieser ist notwendigerweise injektiv (siehe letztes Tutorium), also  $\mathbb{Q} \cong \tilde{i}(\mathbb{Q}) \leq K$ .

(b) Der Homomorphiesatz liefert direkt  $\mathcal{F}_p = \mathbb{Z}/p\mathbb{Z} \cong i(\mathbb{Z}) \leq K$ . □

**13 Korollar.** Ist  $\sigma : K \rightarrow L$  Körperhomomorphismus. Dann haben  $K, L$  die gleiche Charakteristik, wir können also die Primkörper miteinander identifizieren und von dem Primkörper  $F$  sprechen.

Es gilt sogar:  $\sigma|_F = \text{id}_F$ .

**14 Aufgabe.** Sei  $K$  ein Körper,  $\text{char}(K) = p \neq 0$ . Dann ist

$$\Phi : K \rightarrow K, \quad x \mapsto x^p$$

ein Homomorphismus, der sog. *Frobenius-Homomorphismus*.

Welche Elemente von  $K$  werden auf sich abgebildet? Wann ist  $\Phi$  ein Automorphismus?

*Beweis.* (1) Beim Überprüfen der Homomorphismus-Eigenschaften ist lediglich

$$\Phi(x + y) = (x + y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p = \Phi(x) + \Phi(y)$$

nicht direkt ersichtlich.

(2) Sei  $F$  der Primkörper in  $K$ .  $F^\times$  hat  $p - 1$  Elemente, damit gilt zumindest

$$\Phi(x) = x^p = x \quad \forall x \in F \leq K$$

Aber damit haben wir alle  $p$  Nullstellen von  $X^p - X$  gefunden — genau die Elemente des Primkörpers werden also auf sich selbst abgebildet!

(3)  $\Phi$  ist notwendigerweise injektiv (siehe letztes Tutorium), d.h.  $\Phi$  ist Automorphismus gdw.  $\Phi$  surjektiv ist.

Für endlich Körper folgt dies aber bereits aus der Injektivität! □

### 3 Fortsetzung von Körperhomomorphismen

**15 Definition.** Ein Körperhomomorphismus  $\tilde{\sigma} : M \rightarrow L$  heißt *Fortsetzung* von  $\sigma : K \rightarrow L$ , falls

- (i)  $M/K$  Körpererweiterung
- (ii)  $\tilde{\sigma}|_K = \sigma$

**16 Proposition.** Sei  $\alpha$  algebraisch über  $K$  mit Minimalpolynom  $m = \sum a_k X^k \in K[X]$ ,  $\sigma : K \rightarrow L$  Körperhomomorphismus und  $m^\sigma := \sum \sigma(a_k) X^k \in L[X]$ . Dann:

- (a) Zu jeder Nullstelle  $\beta$  von  $m^\sigma$  in  $L[X]$  gibt es genau eine Fortsetzung  $\tilde{\sigma} : K(\alpha) \rightarrow L$  von  $\sigma$  mit  $\tilde{\sigma}(\alpha) = \beta$ .
- (b) Ist  $\tilde{\sigma} : K(\alpha) \rightarrow L$  Fortsetzung von  $\sigma$ , so ist  $\tilde{\sigma}(\alpha)$  Nullstelle von  $m^\sigma$ .

Beachte: (b) sagt, dass *alle* Fortsetzungen vom Typ (a) sind!

**17 Korollar.** Zerfällungskörper sind eindeutig bestimmt (bis auf Isomorphie).

**18 Aufgabe.** Bestimme alle Körperhomomorphismen  $\sigma : \mathbb{Q}(2^{\frac{1}{4}}, i) \rightarrow \bar{\mathbb{Q}}$ .

*Lösung.*  $2^{\frac{1}{4}}$  ist Nullstelle des über  $\mathbb{Q}$  irreduziblen Polynoms  $f := X^4 - 2$  (Eisenstein). Andererseits hat  $f$  im algebraischen Abschluss  $\bar{\mathbb{Q}}$  vier paarweise verschiedene Nullstellen  $2^{\frac{1}{4}}\{\pm 1, \pm i\}$ .

Nach (a), (b) gibt es also *genau* 4 Körperhomomorphismen  $\sigma_k : \mathbb{Q}(2^{\frac{1}{4}}) \rightarrow \bar{\mathbb{Q}}$ ,

Wegen  $i \notin \mathbb{Q}(2^{\frac{1}{4}}) \subseteq \mathbb{R}$  sind wir noch nicht fertig, und  $i$  ist Nullstelle des über  $\mathbb{Q}(2^{\frac{1}{4}})$  irreduziblen Polynoms  $g := X^2 + 1$ , welches im algebraischen Abschluss die Nullstellen  $\pm i$  hat.

Wiederum nach (a) können wir jeden der  $\sigma_k$  auf 2 verschiedene Arten zu einem Körperhomomorphismus  $\sigma_{k,l} : \mathbb{Q}(2^{\frac{1}{4}}, i) \rightarrow \bar{\mathbb{Q}}$  fortsetzen, und (b) sagt, dass wir so *alle* Körperhomomorphismen erhalten!

	$\sigma_{1,1}$	$\sigma_{2,1}$	$\sigma_{3,1}$	$\sigma_{4,1}$	$\sigma_{1,2}$	$\sigma_{2,2}$	$\sigma_{3,2}$	$\sigma_{4,2}$
$2^{\frac{1}{4}}$	$2^{\frac{1}{4}}$	$-2^{\frac{1}{4}}$	$2^{\frac{1}{4}}i$	$-2^{\frac{1}{4}}i$	$2^{\frac{1}{4}}$	$-2^{\frac{1}{4}}$	$2^{\frac{1}{4}}i$	$-2^{\frac{1}{4}}i$
$i$	$i$	$i$	$i$	$i$	$-i$	$-i$	$-i$	$-i$

□

**19 Satz.** Sei  $M/K$  algebraische Körpererweiterung,  $\bar{L}$  algebraisch abgeschlossener Körper,  $\sigma : K \rightarrow \bar{L}$  Homomorphismus. Dann existiert eine Fortsetzung  $\tilde{\sigma} : M \rightarrow \bar{L}$ .

Beachte:  $M/K$  wurde *nicht* als endlich vorausgesetzt!

**20 Korollar.** Algebraische Abschlüsse sind eindeutig bestimmt (bis auf Isomorphie).

**21 Definition.** Seien  $L/K, M/K$  Körpererweiterungen.

$$\text{Hom}_K(L, M) := \{\sigma : L \rightarrow M \mid \sigma|_K = \text{id}_K\}$$

$$\text{Aut}_K(L) := \text{Aut}(L/K) := \{\sigma \in \text{Hom}_K(L, L) \mid \sigma \text{ bijektiv}\}$$

**22 Aufgabe.** Sei  $L/K$  Körpererweiterung vom Grad  $n$ ,  $\alpha \in L$  und  $\sigma_1, \dots, \sigma_n \in \text{Aut}_K(L)$  mit  $\sigma_k(\alpha)$  paarweise verschieden.

Zeige:  $L = K(\alpha)$ .

*Beweis.* Idee:

$$\begin{aligned}\sigma_k(\alpha) &\in K(\alpha) \\ \Rightarrow \sigma_k|_{K(\alpha)} &\in \text{Hom}_K(K(\alpha), L)\end{aligned}$$

Nach Voraussetzung haben wir mindestens  $n$  verschiedene Homomorphismen  $\tau \in \text{Hom}_K(K(\alpha), L)$ , die alle schon durch  $\tau(\alpha)$  bestimmt sind.

Allerdings muss nach Proposition (b)  $\tau(\alpha)$  wiederum eine Nullstelle des Minimalpolynoms sein; dieses muss also mindestens Grad  $n$  haben, d.h.  $[K(\alpha) : K] \geq n$ .  $\square$

**23 Lemma.** Sei  $L/K$  endliche Körpererweiterung,  $\bar{K}$  algebraischer Abschluss von  $K$ . Dann gilt:

$$\#\text{Hom}_K(L, \bar{K}) \leq [L : K]$$