

# Algebra SS16

Prof Wedhorn, Mitschrift von Daniel Kallendorf

18. Januar 2017

## Inhaltsverzeichnis

<b>1</b>	<b>Erinnerung: Ringe und Ideale</b>	<b>2</b>
1A	Ideale, Primideal, maximale Ideale und Ring-Homomorphismen .	2
1B	Operationen mit Idealen . . . . .	5
1C	Radikal und Jakobson-Radikal . . . . .	7
<b>2</b>	<b>Polynomringe</b>	<b>8</b>
<b>3</b>	<b>Tensorprodukte</b>	<b>10</b>
3A	Erinnerung . . . . .	10
3B	Basiswechsel von Tensorprodukten . . . . .	14
<b>4</b>	<b>Lokalisierung</b>	<b>18</b>
4A	Lokalisierung von Ringen und Moduln . . . . .	18
4B	Lokale Ringe und Restklassenkörper . . . . .	22
4C	Spektren . . . . .	23
	4.23 Spielzeugmodell (der Funktionalanalysis) . . . . .	23
4D	Lemma von Nakagawa??? . . . . .	25
<b>5</b>	<b>Noethersche und Artinsche Ringe</b>	<b>28</b>
5A	Noethersche und Artinsche Moduln . . . . .	28
5B	Länge von Moduln . . . . .	31
5C	Noethersche Ringe . . . . .	34
5D	Artin-Ringe . . . . .	35
<b>6</b>	<b>Ganzheit</b>	<b>36</b>
6A	Ganze Ring-Homomorphismen . . . . .	36
6B	Ganzer Abschluss . . . . .	38
6C	Going-Up . . . . .	39
<b>7</b>	<b>Irreduzibilität</b>	<b>41</b>
7A	Satz von Gauß . . . . .	41
7B	Irreduzibilitätskriterien . . . . .	43

<b>8</b>	<b>Algebraische Körpererweiterungen</b>	<b>44</b>
8A	Körpererweiterungen . . . . .	44
8.18	Bestimmung von $\mu_{a,K}$ I . . . . .	45
8E	Algebraische Erweiterungen . . . . .	46
8F	Algebraischer Abschluss . . . . .	46
8G	Fortsetzung von Körperhomomorphismen . . . . .	47
<b>9</b>	<b>Normale und separable Körpererweiterungen</b>	<b>48</b>
9A	Zerfallungskörper . . . . .	48
9B	Normale Erweiterungen . . . . .	50
9C	Separabilitätsgrad . . . . .	52
9D	Separable Polynome . . . . .	54
9E	Separable Algebren . . . . .	55
9F	Satz vom primitiven Element . . . . .	57
<b>10</b>	<b>Galois-Theorie</b>	<b>58</b>
10A	Galois-Erweiterungen . . . . .	58
<b>11</b>	<b>Anwendung der Galois-Theorie</b>	<b>61</b>
11A	Endliche Körper . . . . .	61

## 1 Erinnerung: Ringe und Ideale

### 1A Ideale, Primideal, maximale Ideale und Ring-Homomorphismen

**Definition 1.-9.** Man nennt  $(A, +, \cdot)$  einen **Ring**(in dieser VL=kommutativer Ring), wenn

1.  $(A, +)$  abelsch
2. Es gibt ein neutrales Element der Multiplikation  $1 \in A : 1a = a\forall a \in A$
3. Die Multiplikation ist  $\cdot$  assoziativ und kommutativ
4. Distributivität

**Definition 1.-8.** Seien  $A, B$  Ringe. Eine Abbildung  $\varphi : A \rightarrow B$  heißt **Ringhomomorphismus**, falls

1.  $\varphi(a + a') = \varphi(a) + \varphi(a')$  für alle  $a, a' \in A$
2.  $\varphi(aa') = \varphi(a)\varphi(a')$  für alle  $a, a' \in A$
3.  $\varphi(1) = 1$

**Definition 1.-7.** Ein  $A$ -Modul mit  $A$ -bilinearer, kommutativer und assoziativer Multiplikation und neutralem Element heißt  **$A$ -Algebra**

**Korollar 1.-6.**  $B$  ist  $A$ -Algebra genau dann wenn  $\varphi : A \rightarrow B$  ein Ringhomomorphismus ist.

**Definition 1.-5.** Man nennt  $\mathfrak{a} \subseteq A$  **Ideal**, falls

1.  $\mathfrak{a} \subseteq (A, +)$  Untergruppe

2.  $a \in A, b \in \mathfrak{a} \Rightarrow ab \in \mathfrak{a}$ .

Sei  $S \subseteq A$ , dann ist

$$AS = SA = (S) := \left\{ \sum_{i=1}^n a_i S_i \mid n \in \mathbb{N}_0, a_i \in A, S_i \in S \right\}$$

das **Kleinste Ideal** von  $A$  das  $S$  enthält.

**Korollar 1.-4.** Sei  $\mathfrak{a} \subseteq A$ . Es gilt  $1 \in \mathfrak{a}$  genau dann wenn  $\mathfrak{A}$ .

**Definition 1.-3.** Sei  $A$  Ring.  $A$  heißt **nullteilerfrei**, falls  $A \neq \{0\}$  und für  $a, b \in A$  mit  $a, b \neq 0$  auch  $ab \neq 0$  gilt.

*Beispiel 1.-2.* • Körper sind Nullteilerfrei

- $\mathbb{Z}$  ist Nullteilerfrei

- $\mathbb{Z}$  ist HIR

**Definition 1.-1.** Sei  $A$  Ring.  $A$  heißt **Hauptidealring**(HIR), falls  $A$  nullteilerfrei ist und jedes Ideal  $\mathfrak{a} \subset A$  von einem Element erzeugt wird.

(d.h.  $\mathfrak{a} = As = \{as \mid a \in A\}$  für ein  $s \in A$ )

*Beispiel 1.0.*

Körper sind Hauptidealringe (Ideale in einem Körper  $K$  sind nur  $(0) = \{0\}$  und  $(1) = K$ )

$\mathbb{Z}, K[X]$  sind HIR

$\mathbb{Z}[X]$  ist nicht HIR ( $p, X$ ) ist für  $p \in \text{Prim}$  nicht von einem Ideal erzeugt.

*Erinnerung 1.1.* Sei  $\varphi : A \rightarrow B$  ein Homomorphismus von Ringen

1.  $\varphi(A) \subset B$  ist Unterring.  
 $(0, 1 \in \varphi(A), a, a' \in \varphi(A) \Rightarrow a + a', aa' \in \varphi(A))$   
 $\text{Ker}(\varphi) = \{a \in A \mid \varphi(a) = 0\} \subseteq A$  ist Ideal  
 $A/\text{Ker}(\varphi) \xrightarrow{\sim} \varphi(A), \bar{a} \mapsto \varphi(a)$  ist ein Ring Homomorphismus.
2. Sei  $\mathfrak{b} \in B$  Ideal, dann  $\varphi^{-1}(\mathfrak{b}) = \{y \in A \mid \varphi(y) \in \mathfrak{b}\} \subseteq A$  Ideal und  $\varphi$  induziert eine injektiven Ring-Homomorphismus:

$$\bar{\varphi} : A/\varphi^{-1}(\mathfrak{b}) \hookrightarrow B/\mathfrak{b}, \quad \bar{a} \mapsto \varphi(a)$$

(wende 1) an auf  $A \rightarrow B \rightarrow B/\mathfrak{b}$ )

Falls  $\varphi$  surjektiv ist, ist  $\varphi$  ein Ring-Homomorphismus.

3. Sei  $\varphi$  surjektiv. Dann sind die Abbildungen

$$\{\mathfrak{a} \subseteq A \text{ Ideal mit } \text{Ker}(\varphi) \subseteq \mathfrak{a}\} \leftrightarrow \{\mathfrak{b} \in B \text{ Ideal}\}$$

$$\varphi^{-1}(\mathfrak{a}) \leftrightarrow \mathfrak{a}$$

$$\mathfrak{a} \leftrightarrow \varphi(\mathfrak{a})$$

zueinander Inverse Bijektionen.

**Definition 1.2.** Sei  $A$  Ring

1. Das Ideal  $\mathfrak{p} \subseteq A$  heißt **Primideal** falls  $A/\mathfrak{p}$  Nullteilerfrei ist.  
(Äquivalent:  $\mathfrak{p} \subsetneq A$  und für alle  $a, b \notin \mathfrak{p}$  gilt  $ab \notin \mathfrak{p}$ )
2. Das Ideal  $m \subseteq A$  heißt **maximales Ideal**, falls  $A/m$  ein Körper ist.  
(Äquivalent: Es gibt kein Ideal  $\mathfrak{a}$ , sodass  $m \subsetneq \mathfrak{a} \subsetneq A$ ).

Jedes Maximale Ideal ist Primideal.

**Satz 1.3.** Sei  $A$  Ring,  $\mathfrak{a} \subsetneq A$  Ideal.

Dann existiert ein maximales Ideal  $m \subset A$  mit  $\mathfrak{a} \subseteq m$ .

*Beweis.* Sei  $(I, \leq) = (\{\mathfrak{b} \subsetneq A \text{ Ideal} \mid \mathfrak{a} \subseteq \mathfrak{b}\}, \leq)$

Zu zeigen:  $(I, \leq)$  besitzt maximale Elemente:

- $\mathfrak{a} \in I \Rightarrow I \neq \emptyset$  erfüllt.
- Sei  $S \subseteq I$  total geordnet und sei  $\mathfrak{a}_0 = \bigcup_{\mathfrak{b} \in S} \mathfrak{b} \subseteq A$ .  
Seien  $x, y \in \mathfrak{a}_0$ , also existieren  $\mathfrak{b}, \mathfrak{b}' \in S$ , sodass  $x \in \mathfrak{b}, y \in \mathfrak{b}'$ .  
Sei O.E.  $\mathfrak{b} \subseteq \mathfrak{b}'$ , dann gilt, da  $S$  total geordnet ist, dass  $x + y\mathfrak{b} \leq \mathfrak{a}_0$ .  
Es gilt  $\mathfrak{a}_0 \neq A$ : Angenommen  $\mathfrak{a}_0 = A$ , dann  $1 \in \mathfrak{a}_0$ , dann gibt es  $b \in S$  mit  $1 \in \mathfrak{b}$ . dann folgt  $\mathfrak{b} = A$ .  
Dann folgt mit 1.4, dass es ein maximales Element gibt, also maximale Ideal die  $\mathfrak{a}_0$  enthalten.

□

**Lemma 1.4** (Lemma von Zorn). Sei  $(I, \leq)$  eine partielle geordnete Menge.

Für jede total geordnete Teilmenge  $S \subseteq I$  eine obere Schranke (d.h.  $\exists i \in I$  mit  $s \leq i \forall s \in S$ ).

Dann besitzt  $(I, \leq)$  maximale Elemente (d.h. Elemente, sodass für Elemente  $i \in I$  gilt, dass  $i_0 \leq i, i \neq i_0$ ).

*Beispiel 1.5.* Sei  $A$  ein Hauptidealring, sei  $\mathfrak{a} \subseteq A$  Ideal mit  $\mathfrak{a} = (a)$  für  $a \in A$ .

1.  $\mathfrak{a}$  ist genau dann Primideal, wenn  $a$  irreduzibel (d.h.  $a \neq 0, a \notin A^\times$  und  $a = bc$  für  $b, c \in A$ , dann muss  $b \in A^\times$  oder  $c \in A^\times$ ) oder  $a = 0$ .
2. Sei  $\mathfrak{a}$ , dann ist  $a$  irreduzibel oder  $A$  ist Körper und  $a = 0$ .

*Beispiel 1.6.* Sei  $A$  ein Ring. Dann ist  $A$  genau dann ein Körper, wenn  $\{0\} \subseteq A$  maximal ist.

*Bemerkung 1.7.* Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus

1. Sei  $q \subseteq B$  Primideal, dann ist  $\varphi^{-1}(q) \subset A$  ein Primideal.

*Beweis 1.* Wir wissen, dass  $\varphi$  einen injektiven Ring-Homomorphismus  $A/\varphi^{-1}(q) \rightarrow B/q$  induziert.

Da  $B/q$  nullteilerfrei ist, folgt, dass  $A/\varphi^{-1}(q)$  nullteilerfrei ist. Dann folgt, dass  $\varphi^{-1}(q)$  Primideal ist. □

*Beweis 2.* Inhalt Es gilt  $1 \notin \varphi^{-1}(q)$ . Sei nun  $x, y \in A$  mit  $x, y \in \varphi^{-1}(q)$ , also  $\varphi(x), \varphi(y) \in q$ .

Dann folgt, da  $q$  Primideal ist, dass  $\varphi(xy) = \varphi(x)\varphi(y) \in q$ , also auch  $xy \in \varphi^{-1}(q)$ . □

2. Sei  $\varphi$  surjektiv, dann ist  $A/\varphi^{-1}(q) \cong B/q$ . Also ist
- (a)  $q$  genau dann Primideal, wenn  $\varphi^{-1}(q)$  Primideal ist.
  - (b)  $q$  genau dann maximales Ideal, wenn  $\varphi^{-1}(q)$  maximales Ideal ist.
  - (c) Es gibt zueinander Inverse Bijektionen:

$$\left\{ \begin{array}{l} \mathfrak{a} \subseteq A \text{ Primideal/maximales Ideal} \\ \text{mit } \text{Ker}(\varphi) = \mathfrak{a} \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{l} \text{Primideal/maximales Ideal} \\ q \subseteq B \end{array} \right\}$$

$$\mathfrak{p} \mapsto \varphi(\mathfrak{p})$$

$$q \mapsto \varphi^{-1}(q)$$

## 1B Operationen mit Idealen

Sei im folgende  $A$  ein Ring.

**Definition 1.8.** 1. Seien  $\mathfrak{a}, \mathfrak{b} \subseteq A$  Ideale.

Dann ist die **Summe von Idealen**

$$\mathfrak{a} + \mathfrak{b} := (\mathfrak{a} \cup \mathfrak{b})\{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

Allgemein für eine Familie von Idealen  $(\mathfrak{a}_i)_{i \in I}$

$$\sum_{i \in I} := \left( \bigcup_{i \in I} \mathfrak{a}_i \right)$$

Bzw. das kleinste Ideal  $\mathfrak{b}$  mit  $\mathfrak{a}_i \subseteq \mathfrak{b}$  für alle  $i \in I$ .

2. Sei  $(\mathfrak{a}_i)_{i \in I}$  eine Familie von Idealen. Dann ist der **Schnitt von Idealen**

$$\bigcap_{i \in I} \mathfrak{a}_i \subseteq A$$

auch ein Ideal.

3. Sei  $\mathfrak{a}, \mathfrak{b} \subseteq A$  Ideale.

Dann ist das **Produkt von Idealen**

$$\mathfrak{a} \cdot \mathfrak{b} := (\{a \cdot b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}) = \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

Es folgt, dass

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$$

*Beispiel 1.9.* Sei  $A$  ein Hauptidealring,  $a, b \in A$  und  $a, b \neq 0$ .

Dann ist  $a = up_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  und  $b = vp_1^{l_1} p_2^{l_2} \dots p_r^{l_r}$  für  $u, v \in A^\times$ ,  $p_i \in A$  irreduzibel,  $(p_i) \neq p_l$  für  $i \neq l$  und  $k_i, l_i \in \mathbb{N}_0$ .

1.  $(b) + (b) = (p_1^{\min(k_1, l_1)} \dots p_r^{\min(k_r, l_r)})$   
(Ähnlich dem ggT)
2.  $(a) \cap (b) = (p_1^{\max(k_1, l_1)} \dots p_r^{\max(k_r, l_r)})$   
(Ähnlich dem kgV)

3.  $(b)(b) = (ab)$  in jedem Ring.

**Theorem 1.10** (Chinesischer Restsatz). Seien  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$  Ideale, sodass  $\mathfrak{a}_i + \mathfrak{a}_j = A$  für  $i \neq j$ . Dann gilt

1.

$$\bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i$$

2.

$$A / \bigcap_{i=1}^n \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^n A / \mathfrak{a}_i$$

$$\bar{a} \mapsto (a \bmod \mathfrak{a}_1, \dots, a \bmod \mathfrak{a}_n)$$

**Proposition 1.11.** Sei  $\mathfrak{p} \subset A$  Primideal mit  $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$  für Ideale  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$ .

Dann ist  $\mathfrak{a}_j \subseteq \mathfrak{p}$  für ein  $j$ .

*Beweis.* Angenommen für alle  $j = 1, \dots, n$  existiert  $x_j \in \mathfrak{a}_j$ , sodass  $x_j \notin \mathfrak{p}$ . Dann ist  $x_1 x_2 \dots x_n \in \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$ .

Da aber  $x_1 x_2 \dots x_n \notin \mathfrak{p}$  da  $\mathfrak{p}$  Primideal. Widerspruch!  $\square$

**Proposition 1.11.** Sei  $\mathfrak{a}$  ein Ideal,  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  Primideale.

Es gelte  $\mathfrak{a} \not\subseteq \mathfrak{p}_i$  für alle  $i$ .

Dann gilt

$$\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$$

(= kein Ideal)

*Beweis.* Induktion nach  $n$ :

- $n = 1$  erfüllt.
- Sei  $n > 0$ .  
Induktionsvoraussetzung für  $n - 1$ : Für alle  $i \in \{1, \dots, n\}$  existiere  $x_i \in \mathfrak{a}_i$ , sodass  $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$
- Entweder es existiert ein  $i$ , sodass  $x_i \in \mathfrak{p}_i$ ,  
oder für  $i$  gilt  $x_i \notin \mathfrak{p}_i$ .  
Definiere  $y \in \mathfrak{a}$  mit

$$y := \sum_{i=1}^n x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$$

dann  $x \notin \mathfrak{p}_i$  für alle  $i = 1, \dots, n$ .

$\square$

## 1C Radikal und Jakobson-Radikal

Sei  $A$  weiterhin ein Ring

**Definition 1.12.** 1.  $x \in A$  heißt **nilpotent**, falls es ein  $n \in \mathbb{N}$  gibt, sodass  $x^n = 0$

2.  $A$  heißt **reduziert**, wenn er keine nilpotenten Elemente außer 0 enthält.

*Beispiel.* 1.  $\bar{2} \in \mathbb{Z}/8\mathbb{Z}$  ist nilpotent.

2. nullteilerfreie Ringe sind reduziert.

Aber:  $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  ist reduziert aber nicht nullteilerfrei

**Definition 1.13.** Sei  $\mathfrak{a} \subseteq A$  Ideal. Dann heißt das Ideal

$$\text{rad}(\mathfrak{a}) := \sqrt{\mathfrak{a}} := \{x \in A \mid \exists n \in \mathbb{N}_0 : x^n \in \mathfrak{a}\}$$

das **Radikal** von  $\mathfrak{a}$ .

*Bemerkung 1.14.* Sei  $\mathfrak{a} \subseteq A$  ein Ideal

1.  $\mathfrak{a} \subseteq \text{rad}(\mathfrak{a})$

2.  $\mathfrak{a} = \text{rad}(\mathfrak{a})$  genau dann wenn  $A/\mathfrak{a}$  reduziert ist

*Beweis.* Es gilt  $\mathfrak{a} = \text{rad} \mathfrak{a}$

genau dann wenn für alle  $a \in A$  gilt  $0^n \in \mathfrak{a}$  für ein  $n \in \mathbb{N}$ . Es folgt  $a \in \mathfrak{a}$ .

Genau dann wenn für alle  $a \in A$  gilt  $\bar{a}^n := (a \bmod \mathfrak{a})^n = 0$  für ein  $n$ . Es folgt  $\bar{a} = 0$ .

Ist also äquivalent dazu, dass  $A/\mathfrak{a}$  reduziert ist.  $\square$

**Satz 1.15.** Sei  $\mathfrak{a} \subseteq A$  Ideal. Dann gilt

$$\text{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{g} \subset A \text{ Primideal} \\ \mathfrak{a} \subseteq \mathfrak{g}}} \mathfrak{g}$$

*Beweis.* Wir zeigen durch beidseitige Inklusion

$\subseteq$  Sei  $x \in A$  nilpotent. Dann gibt es ein  $n \in \mathbb{N}$ , sodass  $x^n = 0 \in \mathfrak{g}$  für alle Primideale  $\mathfrak{g}$

Dann liegt auch  $x \in \mathfrak{g}$  für alle Primideale  $\mathfrak{g}$ .

$\supseteq$  Sei  $x \in A$  nicht nilpotent

1. Zz: Es gibt ein Primideal  $\mathfrak{g} \subset A$ , sodass  $x \notin \mathfrak{g}$ .

???...

$\square$

**Definition 1.16.**  $\text{Nil}(A) := \text{rad}(\{0\}) = \{x \in A \mid x \text{ ist nilpotent}\}$  heißt das **Nilradikal** von  $A$ .

Mit 1.15 folgt die äquivalente Definition

$$\text{Nil}(A) = \bigcap_{\substack{\mathfrak{g} \subset A \\ \mathfrak{g} \text{ Primideal}}} \mathfrak{g}$$

**Definition 1.17.** Das **Jacobson-Radikal** von  $A$  ist definiert als

$$\text{Jac}(A) := \bigcap_{\substack{m \in A \\ m \text{ maximales Ideal}}} m$$

*Beispiel.* 1.  $\text{Jac}(\mathbb{Z}) = \{0\} = \text{Nil}(\mathbb{Z})$

2.  $\text{Jac}(\mathbb{Z}/8\mathbb{Z}) = 2\mathbb{Z}/8\mathbb{Z}$

**Proposition 1.18.**  $\text{Jac}(A) = \{x \in A \mid 1 - xy \in A^\times \forall y \in A\}$

*Beweis.* Sei  $x \in A$ , sodass  $y \in A$  existiert mit  $1 - xy \notin A^\times$  und sei  $m \subset A$  maximal, sodass  $1 - xy \in m$ .

Wäre nun  $x \in \text{Jac}(A) \subseteq m$ , dann  $1 = 1 - xy + xy \in m$ . Widerspruch!

Sei also  $x \notin \text{Jac}(A)$ , d.h. es existiert  $m \subset A$  mit  $x \notin m$ .

Dann ist  $m + (x) = A$ , d.h. es gibt eine Zerlegung der Eins  $1 = z + yx$ .

Es folgt, dass es ein  $y \in A$  gibt, sodass  $1 - xy \in m$  und damit  $1 - xy \notin A^\times$ .  $\square$

## 2 Polynomringe

**Definition 2.1.** Sei  $A^{(\mathbb{N}_0)} := \{(a_n)_{n \in \mathbb{N}_0} \mid a_n \in A, \text{ fast alle } a_n = 0\}$ .

Addition und Multiplikation:

$$\begin{aligned} (a_n) + (b_n) &:= (a_n + b_n) \\ (a_n) \cdot (b_n) &:= \sum_{k=0}^n a_k b_{n-k} \end{aligned}$$

Sei nun  $X = (0, 1, 0, \dots)$ . Dann ist nur der  $n$ -te Eintrag von  $X^n = 1$ .

Dann gilt

$$(a_n)_n = \sum_{n=0}^{\infty} a_n X^n$$

Wir erhalten einen kommutativen Ring und bezeichnen  $A[X]$  als den **Polynomring** über  $A$  in der Unbestimmten  $X$ .

Mit der Abbildung  $A \rightarrow A[X], a \mapsto a + 0X + 0X^2 + \dots$  erhält man eine  $A$ -Algebra.

**Definition 2.2.** Sei  $f = a_n X^n + \dots + a_1 X + a_0 \in A[X]$

1.  $\deg(f) := \sup\{d \in \mathbb{N} \mid a_d \neq 0\}$  heißt der **Grad** von  $f$  (Es folgt  $\deg(0) = -\infty$ )
2.  $f$  heißt **normiert**, falls  $f = X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ .
3.  $a_0$  heißt **absoluter Koeffizient** von  $f$ .

*Bemerkung 2.3.* Seien  $f, g \in A[X]$

1.  $\deg(f + g) \leq \max(\deg(f), \deg(g))$
2.  $\deg(fg) \leq \deg(f) + \deg(g)$   
(Da Ringe Nullteiler haben können. Gleichheit bei nullteilerfreien Ringen)



3.  $A$  ist genau dann nullteilerfrei wenn  $A[X]$  nullteilerfrei ist.

**Satz 2.4** (Division mit Rest). Sei  $g = a_d X^d + \dots + a_0 \in A[X]$  mit  $a_d \in A^\times$ . Dann existieren für alle Polynome  $f \in A[X]$  eindeutige  $q, r \in A[X]$ , sodass  $f = qg + r$  mit  $\deg(r) < \deg(g) = d$

*Beweis.* 1. Da  $a_d \in A^\times$  ist gilt  $\deg(gs) = \deg(g) + \deg(s)$

2. Eindeutigkeit: Sei  $f = qg + r = q'g + r'$  mit  $\deg(r), \deg(r') < d$ . Dann folgt, dass  $0 = (q - q')g + (r - r')$ . Und da  $\deg(r - r') < d$  muss  $q = q'$  und  $r = r'$ .

3. Existenz: Induktion nach  $\deg(f)$ .

IA Sei  $\deg(f) < d$ , dann  $f = 0g + r$  und  $r = f$ .

IV Für Polynome  $f \in A[X]$  mit  $\deg(f) \leq n$  sind  $r, q$  eindeutig bestimmt.

IS Sei  $\deg(f) \geq d$  ...

□

**Definition 2.5.** Definiere rekursiv  $A[X_1, \dots, X_n] := (A[X_1, \dots, X_{n-1}])[X_n]$ . Also

$$A[X_1, \dots, X_n] := \left\{ \sum_{k_1, \dots, k_n} a_{k_1, \dots, k_n} X_1^{k_1} \cdot \dots \cdot X_n^{k_n} \mid a \in A \right\}$$

Elemente der Form  $X_1^{k_1} \cdot \dots \cdot X_n^{k_n}$  heißen **Monome**.

*Bemerkung 2.6.*  $A[X_1, \dots, X_n]$  ist ein freier Modul. Die Monome bilden eine Basis.

**Satz 2.7** (Universaleigenschaft des Polynomrings). Sei  $\phi : A \rightarrow B$  eine  $A$ -Algebra und seine  $b_1, \dots, b_n \in B$  Elemente. Dann existiert genau ein  $A$ -Algebra-Homomorphismus  $\psi : A[X_1, \dots, X_n] \rightarrow B$ , so dass  $\psi(x_i) = b_i$  für alle  $i = 1, \dots, n$ , nämlich

$$\psi \left( \underbrace{\sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} X_1^{i_1} \cdot \dots \cdot X_n^{i_n}}_{=: f} \right) = \underbrace{\sum_{i_1, \dots, i_n \geq 0} \phi(a_{i_1, \dots, i_n}) b_1^{i_1} \cdot \dots \cdot b_n^{i_n}}_{=: f(b_1, \dots, b_n)}$$

*Bemerkung 2.8.*

$$\begin{aligned} \text{Im}(\psi) &= \text{kleinste } A\text{-Unteralgebra die } b_1, \dots, b_n \text{ enthält} \\ &= A[b_1, \dots, b_n] \subset B \end{aligned}$$

*Beispiel 2.9.* Sei  $\phi : A \rightarrow B$  eine  $A$ -Algebra,  $b \in B$ . Es existiere ein  $g \in A[X]$  mit  $g(b) = 0$ . Sei  $g$  normiert. Dann gilt

$$A[b] = \{f(b) \mid f \in A[X], \deg(f) < \deg(g)\}$$

*Beispiel 2.10.* Sei  $A = \mathbb{Q} \hookrightarrow \mathbb{C}, i \in \mathbb{C}$ .  
Dann gilt  $g(i) = 0$  wobei  $g = X^3 + X = X(X^2 + 1)$ . Es folgt:

$$\mathbb{Q}[i] = \{a_0 + q_1 i + a_2 i^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$$

$$\mathbb{Q}[i] = \text{Im}(\mathbb{Q}[X] \xrightarrow[X \mapsto i, f \mapsto f(i)]{\psi} \mathbb{C})$$

Dann  $\tilde{g} \in \mathbb{Q}[X] : \psi(\tilde{g}) = 0 \Leftrightarrow \tilde{g}(i) = 0$ .  
Also  $g \in \text{Ker}(\psi) \Rightarrow (g) \subseteq \text{Ker}(\psi)$ .  
In diesem Fall  $\text{Ker } \psi = (X^2 + 1)$ .

Begründung von 2.8:

$$(g) \subseteq \text{Ker} \left( A[X] \xrightarrow[f \mapsto f(b)]{\psi} B \right)$$

Also  $\psi$  faktorisiert:

$$A[X]/(g) \xrightarrow{\bar{\psi}} A[b] \subseteq B$$

mit  $\bar{\psi}$  surjektiv.

**Proposition 2.11.** Sei  $g \in A[X]$  normiert. Dann ist

$$\{f \in A[X], \deg(f) < \deg(g)\} \hookrightarrow A[X] \rightarrow A[X]/(g)$$

bijektiv.

*Beweis.* Gilt, da für alle  $f \in A[X]$  genau ein  $r \in A[X]$  existiert mit  $\deg(r) < \deg(g)$  mit  $f \in r + (g)$   $\square$

## 3 Tensorprodukte

- (A) Tensorprodukte von Moduln
- (B) Tensorprodukte von Algebren und Basiswechsel
- (C) Exaktheitseigenschaften des Tensorprodukts

### 3A Erinnerung

**Definition 3.1.** Ein  $A$ -Modul ist ein Tripel  $(M, +, \cdot)$  wobei  $(M, +)$  abelsche Gruppe und  $\cdot : A \times M \rightarrow M$  eine skalare Multiplikation ist.

*Bemerkung.* Ein  $\mathbb{Z}$ -Modul entspricht einer abelschen Gruppe.

*Beispiel.* Sei  $I$  eine Menge

$$A^{(I)} = \{(a_i)_{i \in I} \mid a_i \in A, a_i = 0 \text{ für fast alle } i \in I\}$$

$A$ -Modul mit Addition und Skalarprodukt.  
Für  $i \in I : e_i \in A^{(I)}$  mit

$$e_i = \begin{cases} 1 & \text{an der } i\text{-ten Stelle} \\ 0 & \text{sonst} \end{cases}$$

**Definition 3.2.** Ein  $A$ -Modul heißt **frei**, falls  $M \cong A^{(I)}$  für eine Menge  $I$

**Definition 3.3.** Sei  $M, N$   $A$ -Modul. Dann heißt  $u : M \rightarrow N$   **$A$ -linear** oder **Homomorphismus von  $A$ -Moduln**, falls

$$u(am + m') = au(m) + u(m') \forall a \in A, m, m' \in M$$

*Bemerkung.* Sei  $I$  eine Menge,  $M$  ein  $A$ -Modul  $\underline{m} = (m_i)_{i \in I}$  ein Tupel von Elementen  $m_i \in M$ . Dann Existiert genau eine Abbildung:

$$A^{(I)} \xrightarrow{u_{\underline{m}}} M$$

mit  $u_{\underline{m}}(e_i) = m_i$ .

$(m_i)_i = \underline{m}$  heißt linear Unabhängig/ Erzeugende-System/ Basis, falls  $u_{\underline{m}}$  injektiv/ surjektiv / bijektiv ist.

*Bemerkung.* Der  $A$ -Modul  $M$  ist endlich erzeugt, genau dann wenn ein  $n \in \mathbb{N}$  und eine  $A$ -lineare Surjektion  $A^n \rightarrow M$  existieren.

**Definition 3.4.** Sei  $r \in \mathbb{N}_0$ ,  $M_1, \dots, M_r, P$   $A$ -Moduln.

Eine Abbildung  $\alpha : M_1 \times \dots \times M_r \rightarrow P$  heißt  **$r$ -multilinear**, falls sie in jeder Komponente linear ist, d.h. Für alle  $i = 1, \dots, r$  gilt:

$$\alpha(m_1, \dots, am_i + m'_i, m_{i+1}, \dots, m_r) = a\alpha(m_1, \dots, m_i, \dots, m_r) + \alpha(m_1, \dots, m'_i, \dots, m_r)$$

Für alle  $m_j \in M_j, m_i \in M_i, a \in A$ .

(Insbesondere heißen  $r = 1$ : linear,  $r = 2$ : bilinear)

Wir definieren

$$L_a(M_1, \dots, M_r, P) := \{\alpha : M_1 \times \dots \times M_r \rightarrow P \mid \alpha \text{ ist } r\text{-multilinear}\}$$

**Satz 3.3.** Sei  $r \geq 2$ ,  $M_1, \dots, M_r$   $A$ -Moduln.

Dann existiert ein  $A$ -Modul  $M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_r$  und eine  $r$ -multilineare Abbildung  $\tau : M_1 \times \dots \times M_r \rightarrow M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_r$ , sodass für jede  $r$ -multilineare Abbildung:

$$\alpha : M_1 \times \dots \times M_r \rightarrow P$$

wobei  $P$  ein  $A$ -Modul, genau ein  $A$ -lineare Abbildung

$$\bar{\alpha} : M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_r \rightarrow P$$

existiert.

$$\begin{array}{ccc} M_1 \times \dots \times M_r & \xrightarrow{\forall \alpha: r\text{-multilinear}} & P \\ \downarrow \tau & \searrow \exists! \bar{\alpha} & \\ M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_r & & \end{array}$$

**Definition 3.3.** Der  $A$ -Modul  $M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_r$  heißt das **Tensorprodukt** von  $M_1, \dots, M_r$ .

*Beweis.* • Eindeutigkeit des Tensorprodukts

Seien  $(T, \tau : M_1 \times \dots \times M_r \rightarrow T)$  und  $(T', \tau')$  Tensorprodukte:

$$\begin{array}{ccc} & M_1 \times \dots \times M_r & \\ \swarrow \tau & & \searrow \tau' \\ T & \xleftrightarrow[\exists! u]{\exists! v} & T' \end{array}$$

$u$  existiert aufgrund der universellen Eigenschaft von  $(T, \tau)$ .  
 $v$  existiert aufgrund der universellen Eigenschaft von  $(T', \tau')$ .

Die Universelle Eigenschaft von  $(T, \tau)$  zeigt, dass  $v \circ u = \text{id}_T$ , genauso  
 $u \circ v = \text{id}_T$ .

- Existenz des Tensorprodukts

1. Suche einen  $A$ -Modul  $N$  und eine Abbildung  $c : M_1 \times \dots \times M_r \rightarrow R$ ,  
sodass

$$\text{Hom}_A(N, P) \xrightarrow{u \mapsto u \circ \tau} \text{Abb}(M_1 \times \dots \times M_r, P)$$

Für alle  $A$ -Moduln  $P$ . Wähle also  $N := A^{(M_1 \times \dots \times M_r)}$  und  
 $l : M_1 \times \dots \times M_r \rightarrow N, i \mapsto e_i$ .

2. Wir wollen, dass  $(am_1 + m'_1, m_2, \dots, m_r)$  und  $a(m_1, \dots, m_r) + (m'_1, \dots, m_r)$   
auf das gleiche Element abgebildet werden.  
Sei  $Q \subseteq N$  der von

$$e_{(m_1, \dots, m_{i-1}, am_i + m'_i, m_{i+1}, \dots, m_r)} - (ae_{(m_1, \dots, m_i, \dots, m_r)} + e_{(m_1, \dots, m'_i, \dots, m_r)})$$

für alle  $i = 1, \dots, r$  und  $m_i, m'_i \in M_i$  und  $a \in A$  erzeugt Untermodul.  
Dann setze  $T := N/Q$ . Dann gilt

$$\begin{aligned} \text{Hom}_A(T, P) &= \{u \in \text{Hom}(N, P) \mid u(Q) = 0\} \\ &= L_A(M_1, \dots, M_r, P) \end{aligned}$$

mit  $\tau : M_1 \times \dots \times M_r \rightarrow N \rightarrow N/Q$ .

□

*Bemerkung 3.4.*  $e_{(m_1, \dots, m_r)} \in A^{(M_1 \times \dots \times M_r)}$  bilden ein Erzeugendensystem.  
Also bilden auch die  $\tau(m_1, \dots, m_r) =: m_1 \otimes \dots \otimes m_r$  eine Erzeugenden-System  
des  $A$ -Moduls  $M_1 \otimes \dots \otimes M_r$ .

**Aber:** Nicht jedes Element von  $M_1 \otimes \dots \otimes M_r$  ist in dieser Form.

Also genügt es eine lineare Abbildung  $u : M_1 \otimes \dots \otimes M_r \rightarrow P$  auf den er-  
zeugenden  $m_1 \otimes \dots \otimes m_r$  mit  $(m_i \in M_i)$  anzugeben.

Umgekehrt sei  $P$  ein  $A$ -Modul und es seien Elemente  $u(m_1 \otimes \dots \otimes m_r) \in P$   
gegeben für alle  $m_i \in M_i$ .

Genau dann existiert eine  $A$ -lineare Abbildung  $u : M_1 \otimes \dots \otimes M_r \rightarrow P$  mit  
 $m_1 \otimes \dots \otimes m_r \mapsto u(m_1 \otimes \dots \otimes m_r)$ , wenn für alle  $i = 1, \dots, r$ ,  $a \in A$ ,  $m_j \in M_j$   
und  $m'_i \in M_i$  gilt:

$$u(m_1 \otimes \dots \otimes am_i + m'_i \otimes \dots \otimes m_r) = au(m_1 \otimes \dots \otimes m_i \otimes \dots \otimes m_r) + u(m_1 \otimes \dots \otimes am'_i \otimes \dots \otimes m_r)$$

**Satz 3.5** (Tensorprodukt linearer Abbildungen). *Seien  $M, M', N, N'$   $A$ -Moduln,  
 $u : M \rightarrow M', v : N \rightarrow N'$   $A$ -lineare Abbildungen.*

*Dann definiert*

$$\begin{aligned} M \otimes_A N &\rightarrow M' \otimes N' \\ m \otimes n &\mapsto u(m) \otimes v(n) \end{aligned}$$

*eine  $A$ -lineare Abbildung bezüglich  $u \otimes v : M \otimes N \rightarrow M' \otimes N$ .*

*Beweis.* Zu zeigen:  $u(am + m') \otimes v(n) = a(u(m) \otimes v(n)) + u(m') \otimes v(n)$   
 Es gilt da das Tensorprodukt  $r$ -linear ist.

$$\begin{aligned} u(am + m') \otimes v(n) &= (au(m) + u(m')) \otimes v(n) \\ &= (au(m) \otimes v(n)) + u(m') \otimes v(n) \end{aligned}$$

Außerdem zu zeigen:  $u(m) \otimes v(an + n') = a(u(m) \otimes v(n)) + u(m) \otimes v(n')$   
 ( $\rightarrow$  Genauso.)  $\square$

*Bemerkung 3.6.* 1.  $A \otimes_A M \cong M$

2.  $M \otimes_A N \xrightarrow{\sim} N \otimes_A M, m \otimes n \mapsto n \otimes m$  ist ... von  $A$ -Moduln.

3.

$$\begin{aligned} M \otimes_A N \otimes_A P &\xrightarrow{\sim} (M \otimes_A N) \otimes_A P && \xrightarrow{\sim} M \otimes_A (N \otimes_A P) \\ m \otimes n \otimes p &\mapsto (m \otimes n) \otimes p && (m \otimes (n \otimes p)) \end{aligned}$$

*Beweis.* 1. Sei  $u : a \otimes m \mapsto am, v : 1 \otimes m \mapsto m$

- Z.z.  $u$  wohldefiniert, d.h.  $(a, m) \rightarrow am$  ist bilinear:  
 Dann  $(ba + a') = bam + a'm$  für alle  $a, a', b \in A$  und  $m \in M$ .  
 Analog gilt Linearität in  $m$ .  
 Daraus folgt, dass  $u$   $A$ -linear ist.
- Z.z.  $v$  ist wohldefiniert:  
 analog zu  $u$ .
- Z.z.:  $v \circ u = \text{id}_{A \otimes_A M}$ :

$$(v \circ u)(a \otimes m) = v(am) = 1 \otimes am = a(1 \otimes m) = a \otimes m$$

- Z.z.:  $u \circ v = \text{id}_M$ :

2. Es gilt zu zeigen

- Z.z. Wohldefiniertheit, also  $(m, n) \mapsto n \otimes m$  ist bilinear
  - Existenz der Umkehrabbildung  $n \otimes m \mapsto m \otimes n$
- $\square$

**Proposition 3.7.** 3.7 Sei  $(M_i)_{i \in I}$  eine Familie von  $A$ -Moduln,  $N$  ein  $A$ -Modul:

$$\begin{aligned} \left( \bigotimes_{i \in I} M_i \right) \otimes_A N &\xrightarrow{\sim} \bigotimes_{i \in I} (M_i \otimes_A N) \\ (m_i)_{i \in I} \otimes n &\mapsto (m_i \otimes n)_{i \in I} \end{aligned}$$

*Beweis.* Umkehrabbildung gegeben durch:

$$\text{Inhalt..} m_i \otimes n \mapsto (m_j)_{j \in I} \otimes n$$

$$\text{mit } m_j := \begin{cases} m_i, & j = i \\ 0 & j \neq i \end{cases}$$
 $\square$

### 3B Basiswechsel von Tensorprodukten

**Satz 3.8.** 1. Sei  $M$  ein  $A$ -Modul. Dann wird

$$\varphi^*(M) := B \otimes_A M$$

zu einem  $B$ -Modul mit dem Skalarprodukt

$$\begin{aligned} B \times (B \otimes_A M) &\rightarrow B \otimes_A M \\ (b, b' \otimes m) &\mapsto bb' \otimes m \end{aligned}$$

2. Sei  $U : M \rightarrow M'$  ein Homomorphismus von  $A$ -Moduln. Dann ist

$$\begin{aligned} id_B \otimes u : B \otimes M &\rightarrow B \otimes_A M' \\ b \otimes m &\mapsto b \otimes u(m) \end{aligned}$$

eine  $B$ -lineare Abbildung.

**Proposition 3.9.** Sei  $\varphi : A \rightarrow B$  eine  $A$ -Algebra.

Sei  $M$  ein freier  $A$ -Modul. Dann ist  $B \otimes_A M$  ein freier  $B$ -Modul und

$$\vartheta_A(M) = \vartheta_B(B \otimes_A M)$$

*Beweis.* Sei  $M$  ein freier  $A$ -Modul. Dazu ist äquivalent, dass  $M \simeq A^{(I)}$ . Daraus folgt, dass

$$\begin{aligned} B \otimes_A M &\simeq B \otimes_A A^{(I)} \\ &\simeq B \otimes_A \left( \bigoplus_{i \in I} A \right) \\ &\simeq \left( \bigoplus_{i \in I} B \otimes_A A \right) \\ &\simeq \bigoplus_{i \in I} B \\ &= B^{(I)} \end{aligned}$$

Also ist  $B \otimes_A M$  frei. □

**Proposition 3.10.** Sei  $\mathfrak{a} \subseteq A$  ein Ideal,  $M$  ein  $A$ -Modul. Setze

$$\begin{aligned} \mathfrak{a} \cdot M &= \langle \{am \mid a \in \mathfrak{a}, m \in M\} \rangle \\ &= \left\{ \sum_{i=1}^m a_i m_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{a}, m_i \in M \right\} \\ &\subseteq M \quad \text{Untermodul} \end{aligned}$$

Dann ist

$$\begin{aligned} A/\mathfrak{a} \otimes_A M &\xrightarrow{\sim} M/\mathfrak{a}M \\ \bar{a} \otimes m &\mapsto \overline{am} \end{aligned}$$

ein Homomorphismus von  $A/\mathfrak{a}$ -Moduln.

*Beweis.*  $\bar{a} \oplus m \mapsto \overline{am}$  ist wohldefiniert: Zu zeigen:

1. Sei  $a' \in A$  mit  $\bar{a'} = \bar{a} \in A/\mathfrak{a}$ .

Dann ist  $\overline{am} = \overline{a'm} \in M/\mathfrak{a}M$ . Es gilt  $\bar{a'} = \bar{a}$  genau dann wenn es ein  $x \in \mathfrak{a}$  gibt sodass  $a' = a + x$ .

Daraus folgt, dass  $a'm = am + xm$ , und da  $xm \in \mathfrak{a}M$  folgt  $\overline{a'm} = \overline{am}$ .

2.  $\overline{am}$  ist linear in  $a$ , d.h.

$$\overline{(ba + a')m} = b\overline{am} + \overline{a'm} \quad \text{für } a, a' \in A, b \in A$$

3.  $\overline{am}$  ist linear in  $m$ , d.h.

$$\overline{a(bm + m')} = b\overline{am} + \overline{am'} \quad \text{für } m, m' \in M, b \in A$$

□

**Proposition 3.11.** Eine Umkehrabbildung ist gegeben durch

$$\begin{aligned} v : M &\rightarrow A/\mathfrak{a} \otimes_A M \\ m &\mapsto 1 \otimes m \end{aligned}$$

*Beweis.* Zu zeigen:  $\mathfrak{a}M \subseteq \text{Ker}(v)$ , also für alle  $x \in \mathfrak{a}, m \in M$  gilt  $v(xm) = 0$ .

$$v(xm) = 1 \otimes xm = \bar{x} \otimes m = 0$$

da  $\bar{x} = \bar{0} \in A/\mathfrak{a}$ .

Noch zu zeigen::  $v$  ist Umkehrabbildung zu  $\bar{a} \otimes m \mapsto \overline{am}$ .

□

**Definition 3.11** (Tensorprodukte von Algebren). Sei  $A \rightarrow B_1, A \rightarrow B_2$   $A$ -Algebren.

Dann definieren wir auf dem  $A$ -Modul  $B_1 \otimes_A B_2$  eine Multiplikation:

$$\begin{aligned} (B_1 \otimes B_2) \times (B_1 \otimes B_2) &\rightarrow B_1 \otimes B_1 \otimes B_2 \\ (a_1 \otimes b_2, b'_1 \otimes b'_2) &\mapsto b_1 b'_1 \otimes b_2 b'_2 \end{aligned}$$

und erhalten die  $A$ -Algebra  $B_1 \otimes_A B_2$ .

*Beispiel 3.12.* Sei  $\varphi : A \rightarrow B$  eine  $A$ -Algebra und sei  $C = A[X_1, \dots, X_n]/(f_1, \dots, f_r)$  und  $f_i \in A[X - 1, \dots, X_n]$ . Dann ist

$$B \otimes_A A[X - 1, \dots, X_n]/(f_1, \dots, f_r) = B[X_1, \dots, X_n]/(\tilde{f}_1, \dots, \tilde{d}_r)$$

wobei

$$f_i = \sum_{\underline{j} \in \mathbb{N}_0^n} a_{\underline{j}} X^{\underline{j}} \mapsto \tilde{f}_i = \sum_j \varphi(a_j)$$

*Beispiel 3.13.* 1. Sei  $A = \mathbb{Q}, C = \mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\} = \mathbb{Q}[X]/(X^2 + 1)$

2.  $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}[i] = \mathbb{R}[X]/(X^2 + 1) = \mathbb{C}$

3.  $C \otimes_{\mathbb{Q}} \mathbb{Q}[i] = C[X]/(X^2 + 1) = \mathbb{C}[X]/(X + i) \times \mathbb{C}[X]/(X - i) \simeq \mathbb{C} \times \mathbb{C}$

*Beispiel 3.14.*  $A[X] \otimes_A A[Y] = (A[X])[Y] = A[X, Y]$  mit  $f \otimes g \mapsto fg$ .

Dann ist die Umkehrabbildung

$$\sum a_{ij} X^i Y^j \mapsto \sum_{i,j} (a_{ij} X^i \otimes Y^j)$$

### C) Exaktheitseigenschaften

**Definition 3.11** (Homomorphismen-Funktor). Seien  $M, P$   $A$ -Moduln. Wir Definieren auf  $\text{Hom}_A(M, P) := \{u : M \rightarrow P \mid u \text{ ist } A\text{-linear}\}$  die Struktur eines  $A$ -Moduls.

$$\begin{aligned}(u + v)(m) &:= u(m) + v(m) & u, v &\in \text{Hom}_A(M, P) \\ (au)(m) &:= au(m) & a &\in A, m \in M\end{aligned}$$

Sei  $u : M \rightarrow M'$  eine  $A$ -lineare Abbildung. Wir erhalten die  $A$ -lineare Abbildung

$$\begin{aligned}\text{Hom}_A(u, P) : \text{Hom}_A(M', P) &\rightarrow \text{Hom}_A(M, P) \\ w' &\mapsto w' \cdot u\end{aligned}$$

Sei  $v : P \rightarrow P'$  eine  $A$ -lineare Abbildung. Wir erhalten die  $A$ -lineare Abbildung

$$\begin{aligned}\text{Hom}_A(M, v) : \text{Hom}_A(M, P) &\rightarrow \text{Hom}_A(M, P') \\ w &\mapsto v \cdot w\end{aligned}$$

*Erinnerung 3.12.* Eine Sequenz von  $A$ -linearen Abbildungen

$$\dots \rightarrow M_{i-1} \xrightarrow{u_{i-1}} M_i \xrightarrow{u_i} M_{i+1} \rightarrow \dots$$

heißt exakt, falls  $\text{Ker}(u_i) = \text{Im}(u_{i-1})$

*Beispiel.*  $0 \rightarrow M \xrightarrow{u} M$  ist exakt genau dann wenn  $u$  injektiv ist.  
 $M \xrightarrow{v} M'' \rightarrow 0$  ist exakt genau dann wenn  $v$  surjektiv ist

**Satz 3.12.** 1. Sei  $0 \rightarrow M' \xrightarrow{u} M \xrightarrow{v} M''(*)$  eine Sequenz von  $A$ -Moduln. Dann ist  $(*)$  genau dann exakt, wenn für jeden  $A$ -Modul  $P$  die Sequenz

$$\begin{aligned}\text{Hom}_A(P, (*)) : 0 \rightarrow \text{Hom}_A(P, M') &\rightarrow \text{Hom}_A(P, M) \rightarrow \text{Hom}_A(P, M'') \\ w' &\mapsto u \circ w' \quad w \mapsto v \circ w\end{aligned}$$

exakt ist.

2. Sei  $M' \rightarrow M \rightarrow M'' \rightarrow 0(**)$  eine Sequenz von  $A$ -Moduln. Dann ist  $(**)$  genau dann exakt, wenn für jeden  $A$ -Modul  $P$  die Sequenz

$$\begin{aligned}0 \rightarrow \text{Hom}_A(M'', P) \rightarrow \text{Hom}_A(M, P) &\rightarrow \text{Hom}_A(M', P) \\ w'' &\mapsto w'' \otimes v \quad w \mapsto w \otimes u\end{aligned}$$

*Beweis.* Wir beweisen Schrittweise:

1. “ $(*)$  ist exakt  $\Rightarrow \text{Hom}_A(P, (*))$  ist exakt“

(a)  $w' \mapsto u \circ w'$  injektiv:

Sei  $w \in \text{Hom}_A(P, M')$  mit  $u \circ w' = 0$ .

Dann ist (da  $u$  injektiv)  $w' = 0$ . Also ist  $\text{Ker}(w' \mapsto u \circ w') = 0$ .

(b)  $\text{Im}(w' \mapsto u \circ w') \subseteq \text{Ker}(w \mapsto v \circ w)$ :

Komposition:  $w' \mapsto u \circ w' \mapsto \underbrace{(v \circ u)}_{=0} \circ w'$  ist Null.



- (c)  $\text{Im}(w \mapsto v \circ w) \subseteq \text{Ker}(w' \mapsto u \circ w')$ :  
 Sei  $w \in \text{Hom}_A(P, M)$  mit  $v \circ w = 0$ , sodass  $\text{Im}(w) \subseteq \text{Ker}(v) = \text{Im}(u)$ .

$$\begin{array}{ccccccc}
 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' \\
 & & \nwarrow w' & & \uparrow w & \nearrow 0 & \\
 & & & & P & & 
 \end{array}$$

“ $\Leftarrow$ “

- (a)  $u$  injektiv: Sei  $m' \in M$  mit  $u(m') = 0$ ,  $P := \langle m' \rangle = Am' \subseteq M'$ ,  $w' : P \rightarrow M'$  Inklusion.  
 Dann folgt aus  $u \circ w' = 0$ , da  $w' \mapsto u \circ w'$  injektiv ist, dass  $w' = 0$  und damit  $P = 0$  sodass  $m' = 0$ .
- (b)  $\text{Im}(u) \subseteq \text{Ker}(v)$ . Z.z.  $v \circ u = 0$ .  
 Wir wissen bereits, dass für alle  $A$ -Moduln  $P$  die Abbildung  $\text{Hom}_A(P, M') \rightarrow \text{Hom}_A(P, M'')$ ,  $w' \mapsto v \circ u \circ w$  die Nullabbildung ist.  
 Wähle  $P = M'$  und  $w' = \text{id}_{M'}$ , dann ist  $v \circ u = 0$ .
- (c)  $\text{Ker}(v) \subseteq \text{Im}(u)$ :  
 Sei  $m \in \text{Ker}(v)$ ,  $P : Am \subseteq M$  und sei  $w : P \rightarrow M$  eine Inklusion.  
 Dann ist  $v \circ u = 0$ , d.h.  $w \in \text{Ker}(w \mapsto v \circ w) = \text{Im}(w' \mapsto u \circ w')$ .  
 Also existiert  $w' : P \rightarrow M'$  mit  $u \circ w' = w$ .  
 Da  $u(w'(m)) = w(m) = m$  gilt  $m \in \text{Im}(u)$ .

## 2. Übung

□

*Bemerkung 3.13.* Seien  $M, N, P$   $A$ -Moduln. Dann ist

$$\begin{aligned}
 \text{Hom}_A(M \otimes_A N, P) &= L_A(M, N; P) \\
 &= \text{Hom}_A(M, \text{Hom}_A(N, P)) \\
 (\alpha : M \times N \rightarrow P) &\mapsto (n \mapsto \alpha(m, n))
 \end{aligned}
 \tag{*}$$

Sei  $T_N : (A\text{-Modul}) \rightarrow (A\text{-Modul})$

$$M \mapsto M \otimes_A N$$

$$(u : M \rightarrow M') \mapsto u \otimes \text{id}_N$$

$N_N : (A\text{-Modul}) \rightarrow (A\text{-Modul})$

$$P \mapsto \text{Hom}_A(N, P)$$

Dann besagt (\*):

$$\text{Hom}(T_N(M), P) = \text{Hom}(M, H_N(P))$$

d.h.  $T_N$  ist linksadjungiert zu  $H_N$ .

Dann ist  $T_N$  rechtsexakt und  $H_N$  ist linksexakt.

**Proposition 3.14.** Sei  $M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0$  eine exakte Sequenz von  $A$ -Moduln. Dann ist für jeden  $A$ -Modul  $N$  die Sequenz

$$M' \otimes N \xrightarrow{u \otimes \text{id}_N} M \otimes N \xrightarrow{v \otimes \text{id}_N} M'' \otimes N \rightarrow 0$$

exakt.

*Beweis.* Formal mit 3.13.

Sei  $M' \rightarrow M \rightarrow M'' \rightarrow 0$  exakt.

Dann gilt mit ??, dass für alle  $A$ -Moduln  $P$ :

$$0 \rightarrow \operatorname{Hom}_A(M'', H_N(P)) \rightarrow \operatorname{Hom}_A(M, H_N(P)) \rightarrow \operatorname{Hom}_A(M', H_N(P))$$

Ist jeweils gleich (3.13)

$$0 \rightarrow \operatorname{Hom}_A(T_N(M''), P) \rightarrow \operatorname{Hom}_A(T_N(M), P) \rightarrow \operatorname{Hom}_A(T_N(M'), P)$$

exakt, sodass mit ??

$$T_N(M') \rightarrow \underbrace{T_N(M)}_{=M \otimes_A N} \rightarrow T_N(M'') \rightarrow 0$$

exakt ist. □

*Beispiel 3.15.* Sei  $A = \mathbb{Z}$ ,  $u : \mathbb{Z} \xrightarrow{x \mapsto 2x} \mathbb{Z}$ .

Dann ist  $0 \rightarrow \mathbb{Z} \xrightarrow{u} \mathbb{Z}$  exakte und  $A \otimes_A M = M$ .

Aber

$$0 \rightarrow \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{u \otimes \operatorname{id}_{\mathbb{Z}/2\mathbb{Z}}} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z}$$

ist nicht injektiv.

## 4 Lokalisierung

### 4A Lokalisierung von Ringen und Moduln

**Definition 4.1.** Eine Teilmenge  $S \subseteq A$  heißt multiplikativ, falls  $1 \in S$  und  $s, t \in S \Rightarrow st \in S$ .

*Beispiel 4.2.* 1.  $S = \mathbb{Z} \setminus \{0\} \subseteq A = \mathbb{Z}$

2. Sei  $f \in A$ , dann ist  $S_f = \{1, f, f^2, \dots\}$  eine multiplikative Teilmenge.

3. Sei  $y \in A$  Primideal. Dann ist  $A \setminus y \subseteq A$  eine multiplikative Teilmenge.

**Definition 4.3.** Sei  $A$  ein Ring,  $S \subseteq A$  eine multiplikative Teilmenge.

Definiere auf  $A \times S$  eine Äquivalenzrelation durch

$$(a, s) \sim (b, t) :\Leftrightarrow at = bs$$

Definiere  $S^{-1}A := (A \times S) / \sim$ . Die Äquivalenzklasse von  $(a, s)$  wird mit  $\frac{a}{s}$  bezeichnet.

*Beweis.* Dies ist eine Äquivalenzrelation:

- Reflexivität
- Symmetrie

- Transitiv: Sei  $(a, s) \sim (b, t)$  und  $(b, t) \sim (c, u)$

$$\begin{array}{ccc} (tvw)au & \stackrel{(!)}{=} & (tvw)cs \\ \parallel & & \parallel \\ vbswu & = & wbuvs \end{array}$$

Also  $\frac{a}{s} = \frac{b}{t}$  genau dann esnn es  $v \in S$  gibt sodass  $vat = vbs$ .

□

*Bemerkung.*  $S^{-1}A$  ist Ring mit

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

Dies ist Wohldefiniert und macht  $A^{-1}A$  zu einem kommutativen Ring mit Eins =  $\frac{1}{1}$  und Null =  $\frac{0}{1}$ .

Die Abbildung  $\iota : A \rightarrow S^{-1}A, a \mapsto \frac{a}{1}$  ist ein Ringhomomorphismus und heißt **kanonisch**.

*Beispiel.* Sei  $S = \mathbb{Z} \setminus \{0\} \subseteq A = \mathbb{Z}$ . Dann ist  $S^{-1}A = \mathbb{Q}$ .

**Satz 4.4** (Universelle Eigenschaft). *Sei  $S \subseteq A$  eine multiplikative Teilmenge und sei  $1 : A \rightarrow S^{-1}A$  kanonisch. Sei  $B$  ein Ring,  $\varphi : A \rightarrow B$  ein Ringhomomorphismus mit  $\varphi(s) \in B^\times = \{b \in B \mid \exists c \in B : bc = 1\}$  für alle  $s \in S$ . Dann existiert ein eindeutiger Ringhomomorphismus  $\tilde{\varphi} : S^{-1}A \rightarrow B$  mit  $\tilde{\varphi} \circ 1 = \varphi$ .*

$$\begin{array}{ccc} A & \xrightarrow{\forall \varphi: \varphi(s) \in B^\times} & B \\ \downarrow 1 & \nearrow \exists! \tilde{\varphi} & \\ S^{-1}A & & \end{array}$$

*Beweis.* Eindeutigkeit Für  $\frac{a}{s} \in S^{-1}A$  muss für  $\tilde{\varphi}$  gilt:

$$\begin{aligned} \tilde{\varphi}\left(\frac{a}{s}\right) &= \tilde{\varphi}\left(\frac{a}{1} \left(\frac{s}{1}\right)^{-1}\right) = \tilde{\varphi}\left(\frac{a}{1}\right) \tilde{\varphi}\left(\frac{s}{1}\right)^{-1} \\ &= \varphi(a) \varphi(s)^{-1} \end{aligned} \quad (*)$$

Eindeutigkeit Definiere  $\tilde{\varphi}$  durch (\*)

Z.z:  $\tilde{\varphi}$  ist wohldefiniert.

□

*Bemerkung 4.5.* Sei  $S \subseteq A$  eine multilineare Teilmenge.

Dann gilt:  $1 : A \rightarrow S^{-1}A$  ist injektiv  $\Leftrightarrow S$  enthält keinen Nullteiler.

*Beweis.*

$1$  ist injektiv

$$\Leftrightarrow \text{Ker}(1) = 0$$

$$\Leftrightarrow (\forall a \in A : \frac{a}{1} = 1 \Rightarrow a = 0) \Leftrightarrow (\forall a \in A : \exists s \in S : as = 0 \Rightarrow a = 0) \Leftrightarrow S \text{ enthält einen Nullteiler}$$

□

**Satz 4.6** (Lokalisierung von Moduln). Sei  $S \subseteq A$  eine multiplikative Teilmenge,  $M$  ein  $A$ -Modul. Definiere auf  $M \times S$  eine Äquivalenz Relation:

$$(m, s) \sim (n, t) \Leftrightarrow \exists v \in S : vtm = vsm$$

Man erhält den  $S^{-1}A$ -Modul  $S^{-1}M = (M \times S) / \sim$ :

- Mit Addition:  $\frac{m}{s} + \frac{n}{t} := \frac{tm+sn}{st}$
- Mit Skalarmultiplikation:  $\frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$

**Satz 4.7** (Lokalisierung als Funktor). Sei  $u : M \rightarrow N$  eine  $A$ -lineare Abbildung,  $S \subseteq A$  eine multiplikative Teilgruppe. Dann ist

$$S^{-1}u : S^{-1}M \rightarrow S^{-1}N$$

$$\frac{m}{s} \mapsto \frac{u(m)}{s}$$

eine  $S^{-1}A$  lineare Abbildung.

**Satz 4.8** (Lokalisierung ist exakt). Inhalt Sei  $M' \xrightarrow{u} M \xrightarrow{v} M''$  eine exakte Sequenz von  $A$ -Moduln,  $S \subseteq A$  eine multiplikative Teilmenge. Dann ist

$$S^{-1}M' \xrightarrow{S^{-1}u} S^{-1}M \xrightarrow{S^{-1}v} S^{-1}M''$$

eine exakte Sequenz von  $S^{-1}A$  Moduln.

*Beweis.*  $v \circ u = 0$ . Also ist  $S^{-1}v \circ S^{-1}u = 0$ .

Noch zu zeigen:  $\text{Ker}(S^{-1}v) \subseteq \text{Im}(S^{-1}u)$ .

Sei  $\frac{m}{s} \in S^{-1}M$  mit  $S^{-1}v \frac{m}{s} = \frac{v(m)}{s} = 0$ .

Also gibt es  $t \in S : tv(m) = v(tm) = 0$ .

Damit liegt  $tm \in \text{Ker}(v) = \text{Im}(u)$ .

Also existiert  $m' \in M : u(m' = tm)$ . Dann ist  $S^{-1}u \left( \frac{m'}{st} \right) = \frac{u(m')}{st} = \frac{m}{s}$  und damit  $\frac{m}{s} \in \text{Im}(S^{-1}u)$   $\square$

**Proposition 4.9.** Sei  $M$  ein  $A$ -Modul,  $S \subseteq A$  eine multiplikative Teilmenge, dann ist

$$u : S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$$

$$\frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

ist Homomorphismus von  $S^{-1}A$ -Moduln.

*Beweis.* 1.  $u$  ist wohldefiniert:

- (a) Z.z.  $\frac{a}{s} = \frac{b}{t} \Rightarrow \frac{am}{s} = \frac{bm}{t}$ :

Sei  $\frac{a}{s} = \frac{b}{t}$ . Ist äquivalent dazu, dass es  $v \in S$  gibt mit  $vat = vbs$ .

Dann erfüllt  $v$  auch  $vatm = vbsm$  für alle  $m \in M$ , also auch  $\frac{am}{s} = \frac{bm}{t}$ .

- (b) Z.z.  $\frac{am}{s}$  ist linear in  $\frac{a}{s}$  und in  $m$ :

2. Existenz einer Umkehrabbildung:

Sei  $v : S^{-1}M \rightarrow S^{-1}A \otimes_A M$ ,  $\frac{m}{s} \mapsto \frac{1}{s} \otimes m$ .

Aus  $\frac{m}{s} = \frac{n}{t}$  folgt, dass auch  $\frac{1}{s} \otimes m = \frac{1}{t} \otimes n$ . Also ist die Abbildung wohldefiniert.

Zusätzlich gilt  $v \circ u = \text{id}_{S^{-1}A \otimes_A M}$  und  $u \circ v = \text{id}_{S^{-1}M}$ .

□

**Satz 4.10** (Ideal in  $S^{-1}A$ ). Sei  $S \subseteq A$  eine multilineare Teilmenge.

$$\{\text{Ideale in } A\} \begin{array}{c} \xrightarrow{\mathfrak{a} \mapsto S^{-1}\mathfrak{a}} \\ \xleftarrow{b \mapsto \iota^{-1}(b)} \end{array} \{\text{Ideale in } S^{-1}A\}$$

$$1 : A \rightarrow S^{-1}A, a \mapsto \frac{a}{1}$$

Nicht zu einander invers.

1. Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Dann ist  $S^{-1}\mathfrak{a} = S^{-1}A$  genau dann wenn  $\mathfrak{a} \cap S \neq \emptyset$ .  
Dann folgt auch, dass  $\mapsto S^{-1}\mathfrak{a}$  ist nur invertierbar, falls  $S \subseteq A^\times$ .
2. Für  $b \subseteq S^{-1}A$  Ideal gilt:

$$S^{-1}(\iota^{-1}(b)) = b$$

Dann folgt  $b \mapsto \iota^{-1}(b)$  ist injektiv und jedes Ideal von  $S^{-1}A$  ist von der Form  $S^{-1}\mathfrak{a}$  für ein Ideal  $\mathfrak{a} \subseteq A$ .

3. Sei  $\mathfrak{a} \subseteq A$  ein Ideal. Dann gilt: Es gibt ein Ideal  $b \subseteq S^{-1}A$  mit  $\mathfrak{a} = \iota^{-1}(b)$ .  
Dies ist Äquivalent dazu, dass kein  $s \in S$  in  $A/\mathfrak{a}$  Nullteiler ist.
4. Man hat zueinander inverse Bijektionen:

$$\begin{array}{c} \{q \subset S^{-1}A \mid \text{Primideal}\} \xrightarrow{q \mapsto \iota^{-1}(q)} \\ \xleftarrow{\mathfrak{p} \mapsto S^{-1}\mathfrak{p}} \{\text{Primideale } \mathfrak{p} \subset A \text{ mit } \mathfrak{p} \cap S = \emptyset\} \end{array}$$

*Beweis.* 1.  $\frac{1}{1} = \text{in } S^{-1}A$  ist genau dann wenn es ein  $a \in \mathfrak{a}, s \in S$  gibt, sodass  $\frac{a}{s} = \frac{1}{1}$ .

$$\Leftrightarrow \exists a \in \mathfrak{a}, s, t \in S : ta = ts$$

$$\Leftrightarrow \mathfrak{a} \cap S \neq \emptyset$$

2. Sei  $\frac{a}{s} \in S^{-1}(\iota^{-1}(b))$ .

Ist äquivalent zu  $\exists t \in S$  und  $b \in A$  mit  $\frac{b}{1} \in b$ , so dass

$$\frac{a}{s} = \frac{b}{t} = \frac{b}{1} \frac{1}{t}$$

$$\Leftrightarrow \frac{a}{s} \in b$$

3. Sei  $\mathfrak{a} = \iota^{-1}(b)$  für ein Ideal  $b \subseteq S^{-1}A$ .

$$\Leftrightarrow \mathfrak{a} = \iota^{-1}(S^{-1}\mathfrak{a})$$

$$\Leftrightarrow A/\mathfrak{a} \xrightarrow{\bar{a} \mapsto \overline{(\frac{a}{1})}} S^{-1}A/S^{-1}\mathfrak{a} \stackrel{??}{=} S^{-1}A/\mathfrak{a} \quad \text{injektiv}$$

(Wende ?? an auf die exakte Sequenz

$$0 \rightarrow \mathfrak{a} \rightarrow A \rightarrow A/\mathfrak{a} \rightarrow 0$$

Dann ist auch

$$0 \rightarrow S^{-1}\mathfrak{a} \rightarrow S^{-1}A \rightarrow S^{-1}(A/\mathfrak{a}) \rightarrow 0$$

exakt.) Mit ?? gilt Äquivalenz dazu, dass kein  $s \in S$  ist Nullteiler in  $A/\mathfrak{a}$ .

4.

□

**Satz 4.11** (Universelle Eigenschaft des Quotientenkörpers). Sei  $\iota : A \rightarrow \text{Quot}(A)$  kanonisch und sei  $\varphi : A \rightarrow K$  ein injektiver Ring-Homomorphismus wobei  $K$  ein Körper.

Dann existiert genau ein Homomorphismus von Körpern  $\tilde{\varphi} : \text{Quot}(A) \rightarrow K$ .

## 4B Lokale Ringe und Restklassenkörper

**Definition 4.12.** Ein Ring  $A$  heißt lokal wenn er genau ein Maximales Ideal besitzt.

Dann bezeichnet  $\mathfrak{m}_A$  dieses Maximales Ideal.

Der Körper  $\kappa(A) := A/\mathfrak{m}_A$  heißt Restklassenkörper von  $A$ .

*Beispiel 4.13.* • Jeder Körper ist ein lokaler Ring.

- Ein Hauptidealring  $A$  ist genau dann lokal, wenn bis auf Multiplikation mit Einheiten genau ein irreduzibles Element existiert.  
Oder wenn  $A$  Körper ist

**Definition 4.14.** Ein lokaler Hauptideal Ring der kein Körper ist, heißt diskreter Bewertungsring.

*Beispiel 4.15.* Sei  $\mathfrak{p} \subset A$  Primideal,  $S := A \setminus \mathfrak{p}$  multiplikative Teilmenge,  $A_{\mathfrak{p}} := S^{-1}A$ .

$$\{\text{Primideale in } A - \mathfrak{p}\} \leftrightarrow \{\text{Primideale } q \subset A \text{ mit } q \subseteq \mathfrak{p}\}$$

(mit 4).

Also ist  $A_{\mathfrak{p}}$  ein lokaler Ring mit maximalem Ideal  $S^{-1}\mathfrak{p}$ .

Der Körper  $\kappa(\mathfrak{p}) := A/S^{-1}\mathfrak{p}$  heißt Restklassenkörper in  $\mathfrak{p}$ .

*Bemerkung 4.16.* Seien  $q \subseteq \mathfrak{p} \subset A$  Primideale.

1.

$$\{\text{Primideale in } A_{\mathfrak{p}}\} = \{\text{Primideale in } A, \text{ die in } \mathfrak{p} \text{ enthalten sind}\}$$

$$\{\text{Primideal in } A/q\} = \{\text{Primideal in } A, \text{ die } q \text{ enthalten.}\}$$

2. Sei  $S := S \smile \mathfrak{p}$ . Dann ist  $S^{-1}(A/q) = S^{-1}A/S^{-1}q$  und

$$\{\text{Primideal in } S^{-1}(A/q)\} = \{\text{Primideals in } A \text{ die zwischen } q \text{ und } \mathfrak{p} \text{ liegen}\}$$

3. Speziell für  $q = \mathfrak{p}$ :

$$\begin{aligned} S^{-1}(A/\mathfrak{p}) &= \kappa(\mathfrak{p}) \\ &= \text{Quot}(A/\mathfrak{p}) \end{aligned}$$

## 4C Spektren

*Erinnerung 4.17.* Ein Topologischer Raum ist ein Paar  $(X; \mathfrak{T})$  wobei  $X$  eine Menge,  $\mathfrak{T} \subseteq \mathcal{P}(X)$ , sodass gilt:

1.  $\emptyset \in \mathfrak{T}, X \in \mathfrak{T}$
2. Sei  $(U_i)_{i \in I}$  eine Familie von Mengen  $U_i \in \mathfrak{T}$  dann gilt  $\forall i \in I : \bigcup_{i \in I} U_i \in \mathfrak{T}$
3.  $U, V \in \mathfrak{T}$ , dann  $U \cap V \in \mathfrak{T}$

Die Mengen in  $\mathfrak{T}$  heißen offen.

*Erinnerung 4.18.* Seien  $X, Y$  topologische Räume. Eine Abbildung  $f : X \rightarrow Y$  heißt stetig, falls  $f^{-1}(V) \subseteq X$  ist offen für alle offenen  $V \subseteq Y$ .

*Erinnerung 4.19.* Sei  $(X, \mathfrak{T})$  ein topologischer Raum  $B \subseteq \mathfrak{T}$  heißt Basis der Topologie, falls jeder offenen Teilmenge Vereinigung von Menge aus  $B$  ist.

*Beispiel 4.20.* Sei  $(X, d)$  ein metrischer Raum, dann heißt  $U \subseteq X$  offen, falls

$$\forall x \in U \exists \epsilon > 0 : B_\epsilon(x) \setminus \{y \in X \mid d(x, y) < \epsilon\} \subseteq U$$

Basis der Topologie:  $\{B_\epsilon(x) \mid \epsilon \in \mathbb{R}^{>0}, x \in X\}$

**Definition 4.21.** Ein topologischer Raum  $X$  heißt Hausdorffsch, falls  $\forall x, y \in X$  mit  $x \neq y$  existieren  $U \subseteq X, V \subseteq X$  offen, sodass  $U \cap V = \emptyset$ . Metrische Räume sind Hausdorffsch.

**Definition 4.22.** Ein topologischer Raum  $X$  heißt quasikompakt, falls jede offene Überdeckung  $(U_i)_{i \in I}$  von  $X$  (d.h.  $U_i \subseteq X$  offen für alle  $i \in I$  mit  $\bigcup_{i \in I} U_i = X$ ) eine endliche Teilüberdeckung besitzt. (d.h.  $\exists J \subseteq I$  endliche Teilmenge, sodass  $\bigcup_{i \in J} U_i = X$ .)

### 4.23 Spielzeugmodell (der Funktionalanalysis)

Sei  $X$  ein kompakter topologischer Raum,

$$A := A_X := \xi(X, \mathbb{C}) := \{f : X \rightarrow \mathbb{C} \text{ stetig}\}$$

Sei  $x \in X$ , dann betrachte

$$\mathfrak{M}_x := \{f \in A \mid f(x) = 0\} \subseteq A$$

Dies ist ein Minimales Ideal, denn

$$A/\mathfrak{M}_x \xrightarrow{\sim} \mathbb{C}, \bar{f} \mapsto f(x)$$

**Satz 4.24.** *Die Abbildung*

$$\begin{aligned} X &\rightarrow \text{Max}(A) := \{\mathfrak{M} \subset A \mid \text{maximales Ideal}\} \\ x &\mapsto \mathfrak{M}_x \end{aligned}$$

*ist bijektiv.*

**Korollar 4.25.** *Sei  $f \in A$  und für  $\mathfrak{M}_x \in \text{Max}(A)$  sie  $f(x) = \text{Bild von } f \text{ in } A/\mathfrak{M}_x = \mathbb{C}$ .*

$$\begin{aligned} D(f) &= \{\mathfrak{M} \in \text{Max}(A) \mid \bar{f} \text{ in } A/\mathfrak{M} \text{ ist } \neq 0\} \\ &= \{\mathfrak{M} \in \text{Max}(A) \mid f \notin \mathfrak{M}\} \\ &= \sigma(\{x \in X \mid f(x) \neq 0\}) \end{aligned}$$

**Definition 4.26.**  $U \subseteq \text{Max}(A)$  heißt **offen**, falls  $\exists F \subseteq \text{Max}(A)$  mit

$$U = \bigcup_{f \in F} D(f)$$

Dies ist die Topologie auf  $\text{Max}(A)$ .  
(Bemerkung:  $D(f) \cap D(g) = D(fg)$ )

**Satz 4.27.**  $\sigma$  ist Homomorphismus

Seien  $X, Y$  kompakte topologische Räume,  $F : X \rightarrow Y$  stetig.  
Mann erhält den  $\mathbb{C}$ -Algebra-Homomorphismus:

$$\begin{aligned} \varphi : A_Y &\rightarrow A_x \\ f &\mapsto f \circ F \end{aligned}$$

Habe Kommutierendes Diagramm

$$\begin{array}{ccc} X & & Y \\ \sigma \downarrow \mathcal{P} & & \sigma \downarrow \sim \\ \text{Max}(A_x) & \xrightarrow{\mathfrak{M} \mapsto \varphi^{-1}(\mathfrak{M})} & \text{Max}(A_Y) \end{array}$$

Es folgt  $\forall \mathfrak{M} \subset A_x$  maximal, sodass  $\varphi^{-1}(\mathfrak{M}) \subset A$  maximal ist.  
Sei  $A$  ein Ring. Setze  $X = \text{Spec}(A) := \{y \subset A \mid \text{Primideal con } A\}$  als das **Spektrum von  $A$** .  
Für  $x \in X$  bezeichne  $y_x \subset A$  das korrespondierende Primideal. Sei  $f \in A$ ,  $x \in X$ .  
Dann definiere

$$f(x) := \text{Bild von } f \text{ unter } A \rightarrow A/y_x \hookrightarrow \text{Quot}(A/y_x) = \kappa(x)$$

*Bemerkung 4.28.*  $f$  ist keine Funktion  $X \rightarrow ?$ .  
Setze

$$\begin{aligned} D(f) &:= \{x \in X \mid f(x) \neq 0\} \\ &= \{x \in X \mid f \notin y_x\} \end{aligned}$$



**Definition 4.29.** Eine Teilmenge  $U \subseteq X = \text{Spec}(A)$  heißt **offen**, falls  $F \subseteq A$  Teilmenge existiert, sodass  $U = \bigcup_{f \in F} D(f)$ .

Wir erhalten die sogenannte **Zanski-Topologie**. Dabie

$$\begin{aligned} D(f) \cap D(g) &= D(fg) \\ \emptyset &= D(0) \\ x &= D(x) \end{aligned}$$

**Korollar 4.30** ( $D(f)$  als Spektrum). Sei  $f \in A$  und sei  $S_f := \{1, f, f^2, \dots\}$ . Dann ist

$$\begin{aligned} \text{Spec}(S_f^{-1}A) &= \{y \in \text{Spec}(A) \mid y \cap S_f = \emptyset\} \\ &= \{y \in \text{Spec}(A) \mid f \notin y\} \\ &= D(f) \end{aligned}$$

**Satz 4.31** (Abgeschlossenen Teilmengen). Sei  $X = \text{Spec}(A)$ ,  $Y \subseteq X$  Teilmenge. Dann

$$Y \subseteq X \text{ abgeschlossen} \Leftrightarrow X \setminus Y \subseteq X \text{ offen} \Leftrightarrow \exists F \subseteq A : X \setminus Y = \bigcup_{f \in F} D(f)$$

Genau dann wenn

$$\begin{aligned} \exists F \subseteq A \quad Y &= \bigcap_{f \in F} (X \setminus D(f)) \\ &= \bigcap_{f \in F} \{y \in A \mid f \in y\} \\ &= \{y \in A \text{ Primideal} \mid (F) \subseteq y\} \\ \Leftrightarrow \exists \mathfrak{a} \subseteq A \text{ Ideal} \quad Y &= \{y \in A \text{ Primideal} \mid \mathfrak{a} \subseteq y\} \\ &= \text{Spec}(A/\mathfrak{a}) \end{aligned}$$

**Satz 4.32** (Funktorialität). Sei  $\varphi A \rightarrow B$  ein Homomorphismus on Ringen. Dann ist  $\varphi \text{Spec } B \rightarrow \text{Spec}(A)$ ,  $q \mapsto \varphi^{-1}(q)$  stetig.

*Beweis.* Für  $f \in A$  gilt

$$\begin{aligned} \varphi^{-1}(D(f)) &= \{y \in \text{Spec}(B) \mid \varphi(y) \in D(f)\} \\ &= \{q \subset B \text{ Primideal} \mid \varphi^{-1}(q) \in D(f)\} \\ &= \{q \subset B \text{ Primideal} \mid f \in \varphi^{-1}(q)\} \\ &= \{q \subset B \text{ Primideal} \mid \varphi(f) \notin q\} \\ &= D(\varphi(f)) \subseteq \text{Spec}(B) \text{ offen.} \end{aligned}$$

□

#### 4D Lemma von Nakagama???

**Definition 4.33.** Sei  $u : M \rightarrow N$  ein Homomorphismus von  $A$ -Moduln und sei  $(m_1, \dots, m_r)$  ein Erzeugendensystem von  $M$  und  $(n_1, \dots, n_s)$  von  $N$ . Dann existiert

$$T = (t_{ij})_{\substack{1 \leq i \leq s \\ 1 \leq j \leq r}} \in M_{s \times r}(A)$$

sodass

$$n(m_j) = \sum_{i=1}^s t_{ij} n_i$$

Dann heißt  $T$  eine **Matrix von  $U$  bezüglich  $(m_1, \dots, m_r)$  und  $(n_1, \dots, n_s)$** .

*Bemerkung 4.34.* 1.  $T$  ist nicht eindeutig durch  $u$  bestimmt  
(es sei denn  $(n_1, \dots, n_s)$  ist Basis)

2. Nicht jede Matrix in  $M_{s \times r}(A)$  ist eine Matrix von  $u$  bezüglich  $(m_1, \dots, m_r)$  und  $(n_1, \dots, n_s)$ .  
(Es sei denn  $m_1, \dots, m_r$  ist Basis von  $M$ )

*Erinnerung 4.35.* Sei  $T \in M_n(A) = A^{n \times n}$ ,  $n \in \mathbb{N}$ .

Dann existiert  $S \in M_n(A)$ , sodass  $TS = ST = \det T I_n$ . Dann ist  $S = (s_{ij})$

$$s_{ij} = (-1)^{i+j} \det(T_{ji})$$

( $T$  mit  $j$ -ter Spalte und  $i$ -ter Spalte gestrichen.)

$S$  heißt die Adjunkte von  $T$ .

**Satz 4.36** (Cayley-Hamilton). *Sei  $M$  ein  $A$ -Modul,  $(m_1, \dots, m_n)$  ein Erzeugendensystem und sei  $u : m \rightarrow M$  eine  $A$ -Lineare Abbildung. Sei  $T \in M_r(A)$  eine Matrix von  $u$  bezüglich  $(m_1, \dots, m_r)$ .*

Setze

$$\chi_T := \det \underbrace{(XI_r - A)}_{\in M_r(A[x])} = X^r + a_1 X^{r-1} + \dots + a_{r-1} X + a_r$$

Dann gilt

$$\chi_T(u) = u^r + a_1 u^{r-1} + \dots + a_{r-1} u + a_r \text{Id}_M = 0 \in \text{End}_A(M)$$

1. Sei  $\mathfrak{a} \subseteq A$  Ideal, sodass  $u(M) \subseteq \mathfrak{a}M$ . Dann  $a_i \in \mathfrak{a} \forall i = 1, \dots, r$ .

*Beweis.*  $u(M) \subseteq \mathfrak{a}M$ . Es folgt, dass die Koeffizienten von  $T$  in  $\mathfrak{a}$  liegen.

$a_i$  ist Summe von  $i$ -fachen Produkten von Koeffizienten von  $T$ .

Also  $a_i \in \mathfrak{a} \forall i = 1, \dots, r$ .

Sei nun  $T^T = (t_{ji})_{i \leq i, j \leq r}$  aber  $u(m_j) = \sum_i t_{ji} m_i$ .

Dann gilt

$$\sum_i (u \delta_{ji} - t_{ji} m_i) = 0$$

Sei nun

$$C := (X \delta_{ji} - t_{ji})_{ji} \in M_r(A[X])$$

wobei  $\chi_T = \det(C)$ .

Sei

$$D := (d_{jk})_{jk}$$

Die Adjunkte von  $C$ , also

$$CD = \chi_T I_r \in M_r(A[X]) \quad (**)$$

Betrachte den Homomorphismus  $u \in \text{End}_A(A)$

$$A[X] \xrightarrow{f \mapsto f(u)} A[u] = \{f(u) \mid f \in A[x]\}$$

$A[u]$  ist nun eine kommutative  $A$ -Algebra. Erhalte

$$\begin{aligned} C(u) &= (u\delta_{ij} - t_{ji})_{i,j} \in M_r(A[u]) \\ C(u) &= (\delta_{kj}(u))_{k,j} \end{aligned}$$

Multipliziere  $(\star)$  mit  $\delta_{kj}(u)$ .

$$0 = \sum_{i=1}^r \underbrace{\sum_{j=1}^r \delta_{kj}(u)(u\delta_{ji} - t_{ji})}_{\text{k-te Koeffizienten von } DC(u)=\chi_T(u)\delta_{ki}} m_i$$

Also ... □

**Lemma 4.37** (Lemma von Nakogama (1. Version)). *Sei  $M$  eine endlich erzeugter  $A$ -Modul,  $\mathfrak{a} \subseteq A$  ein Ideal, sodass  $M = \mathfrak{a}M$ .*

*Dann existiert  $f \in 1 + \mathfrak{a} = \{1 + x \mid x \in \mathfrak{a}\}$ , sodass  $fM = 0$*

*Beweis.* Wende 4.36 auf  $u = \text{id}_M$  : Mit 4.36.1 Gilt

$$u^r + a_1 u^{r-1} + \dots + a_{r-1} u + a_r \text{id} = 0$$

mit  $a_i \in \mathfrak{a}^i = \mathfrak{a}$ .

Also ist  $f \text{id}_M = 0$ , wobei

$$f = 1 + a_1 + a_2 + \dots + a_r \in 1 + \mathfrak{a}$$

sodass  $fM = 0$  □

*Bemerkung 4.38.* (Einschränkung von  $A$  auf  $\text{Spec}(A/\mathfrak{a})$ )

$$\dots = A/\mathfrak{a} \otimes_A M = M/\mathfrak{a}M = 0$$

Da  $f \in 1 + \mathfrak{a}$  folgt

$$\text{Spec}(A/\mathfrak{a}) \subseteq^{(\star)} D(f) = \text{Spec}(S_f^{-1}A)$$

wobei  $S_f = \{1, f, f^2, \dots\}$ , sodass

$$(\text{Einschränkung von } M \text{ aus } D_f) = S_f^{-1}A \otimes_A M = S_f^{-1}M \stackrel{(\star\star)}{=} 0$$

Zu  $(\star)$ : Sei  $x \in \text{Spec}(A)$ .

$$x \in \text{Spec}(A/\mathfrak{a}) \Leftrightarrow g(x) = 0 \forall g \in \mathfrak{a}$$

Also gilt für  $f = 1 + g, g \in \mathfrak{a}$  und  $x \in \text{Spec}(A/\mathfrak{a})$ :

$$f(x) = 1 + g(x) = 1 \neq 0$$

$$\Rightarrow \text{Spec}(A/\mathfrak{a}) \subseteq \{x \mid f(x) \neq 0\} = D(f)$$

Zu  $(\star\star)$ : Sei  $M$  endlich erzeugt.

Dann  $S_f^{-1}M = 0$  genau dann wenn  $\exists g \in S_f : gM = 0$ .

$$\Leftrightarrow \exists n \in \mathbb{N} : f^n M = 0 \Leftrightarrow fM = 0$$

**Lemma 4.39** (Lemma von Nakagana (2.Version)). Sei  $M$  ein endlich erzeugter  $A$ -Modul,  $\mathfrak{a} \subseteq \text{Jac}(A)$  ein Ideal mit  $M = \mathfrak{a}M$ . Dann  $M = 0$ .

*Beweis.* Sei  $\mathfrak{a} \subseteq \text{Jac}(A) \xrightarrow{??} 1\mathfrak{a} \subseteq A^\times \xrightarrow{4.37} \dots$  □

...

*Beispiel 4.40.* Sei  $A = \mathbb{Z}$ ,  $M = \mathbb{Z}$ . Dann ist die  $\mathbb{Z}$ -lineare Abbildung  $M \xrightarrow{\cdot 2} \mathbb{Z}$  injektiv aber nicht bijektiv.

**Satz 4.41.** Sei  $M$  ein endlich erzeugter  $A$ -Modul und sein  $U : M \rightarrow M$  eine surjektive  $A$ -lineare Abbildung.

Dann ist  $u$  ein Isomorphismus.

*Beweis.* Fass  $(M, u)$  als  $A[X]$  Modul auf durch  $X \cdot m := u(m)$  für  $m \in M$ .

Dann ist  $u$  genau dann surjektiv, wenn  $X \cdot M = M$  ist.

Es folgt durch 4.37 mit  $\mathfrak{a} = (X)$ , dass es ein  $g \in A[X]$  gibt, sodass  $(a+gX)(M) = 0$ .

Sei  $m \in \text{Ker}(u)$ , dann

$$u = (1 + gX)(m) = m + \underbrace{g(u)(m)u(m)}_{=0} = m$$

Also ist  $u$  injektiv. □

## 5 Noethersche und Artinsche Ringe

### 5A Noethersche und Artinsche Moduln

**Lemma 5.1.** ...

*Beweis.* ... □

**Definition 5.2.** Ein  $A$ -Modul heißt **noethersch**, falls die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jede Aufsteigende Kette von Untermoduln von  $M$

$$N_2 \subseteq N_2 \subseteq \dots \subseteq M$$

wird stationär

2. Jede Nichtleere Menge von Untermoduln von  $M$  besitzt ein Maximales Element

Ein  $A$ -Modul heißt **artinsch**, falls die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jede absteigende Kette von Untermoduln von  $M$

$$N_2 \supseteq N_2 \supseteq \dots$$

wird stationär.

2. Jede Nichtleere Menge von Untermoduln von  $M$  besitzt ein minimales Element.

**Definition 5.2.** Der Ring  $A$  heißt **noethersch**, wenn er als  $A$ -Modul noethersch ist. Äquivalent dazu sind:

1. Jede aufsteigende Kette von Idealen in  $A$  wird stationär.
2. Jede nichtleere Menge von Idealen in  $A$  besitzt ein maximales Element.

Der Ring  $A$  heißt **artinsch**, wenn er als  $A$ -Modul artinsch ist. Äquivalent dazu sind:

1. Jede absteigende Kette von Idealen in  $A$  wird stationär
2. Jede nichtleere Menge von Idealen in  $A$  besitzt ein minimales Element.

*Beispiel 5.3.* -1.  $0$  ist noethersch und artinsch.

0. Jeder Körper ist noethersch und artinsch.

1.  $\mathbb{Z}$  ist noethersch:

Sei  $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$   $(\star)$  eine aufsteigende Kette.

Dann  $\mathfrak{a}_1 = (x_1)$ ,  $x_1 = p_1^{l_1} \cdot \dots \cdot p_r^{l_r}$ .

$$\{\text{Ideale die } \mathfrak{a}_1 \text{ enthalten}\} \xleftrightarrow{1:1} \{\text{Teiler von } x_1\} / \{\text{Einheiten}\}$$

Diese Mengen sind endlich also wird  $(\star)$  stationär.

$\mathbb{Z}$  ist nicht artinsch:

Sei  $x \in \mathbb{Z}$   $x \neq 0, 1, -1$ . Dann

$$(x) \supsetneq (x^2) \supsetneq (xs) \supsetneq \dots$$

ist absteigende Kette die nicht stationär wird.

2. Sei  $p \in \mathbb{Z}$  eine Primzahl. Dann ist der  $\mathbb{Z}$ -Modul

$$\{x \in \mathbb{Q}/\mathbb{Z} \mid \exists n \in \mathbb{N} : p^n x = 0\}$$

artinsch aber nicht noethersch. (Wir werden zeigen:  $A$  artinscher Ring  $\Rightarrow$  noethersch)

3. Sei  $\kappa$  Körper, dann ist  $\kappa[T_1, T_2, \dots]$  nicht noethersch:

$$(T_1) \subsetneq (T_1, T_2) \subsetneq (T_1, T_2, T_3) \subsetneq \dots$$

**Satz 5.4.** Sei  $M$  ein  $A$ -Modul.

Dann ist  $M$  genau dann noethersch, wenn jeder  $A$ -Untermodul von  $M$  endlich erzeugt ist. (Dann ist auch  $M$  endlich erzeugt).

Insbesondere ist  $M$  genau dann noethersch, wenn jedes Ideal von  $A$  endlich erzeugt ist.

**Korollar 5.5.** Jeder Hauptidealring ist noethersch.

**Proposition 5.6.** Sei  $0 \rightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0$  eine Exakte Sequenz von  $A$ -Moduln.

Dann gilt

1.  $M$  ist genau dann noethersch, wenn  $M', M''$  noethersch.

2.  $M$  ist genau dann artinsch, wenn  $M', M''$  artinsch.

*Beweis.* 1. " $\Rightarrow$ ": Es gilt  $M' \cong u(M') \subseteq M$ . Es folgt  $M'$  ist noethersch.

Sei  $N_1 \subseteq N_2 \subseteq \dots \subseteq M''$  eine aufsteigende Kette von Untermoduln von  $M''$ . Da  $M$  noethersch ist, gibt es ein  $r \in \mathbb{N}$ , sodass  $v^{-1}(N_r) = v^{-1}(N_{r+1}) = \dots$

Da  $v$  surjektiv ist gilt dann

$$n_r = v(v^{-1}(N_r)) = v(v^{-1}(N_{r+1})) = N_{r+1}$$

Also wird  $N_1 \subseteq N_2 \subseteq \dots$  stationär.

" $\Leftarrow$ ": Sei  $M_1 \subseteq M_2 \subseteq \dots \subseteq M$  eine aufsteigende Kette von Untermoduln in  $M$ .

Dann sind auch  $u^{-1}(M_1) \subseteq u^{-1}(M_2) \subseteq \dots \subseteq M'$  und  $v(M_1) \subseteq v(M_2) \subseteq \dots \subseteq M''$  aufsteigende Ketten.

Da  $M, M''$  gibt es  $r \in \mathbb{N}$ , sodass  $u^{-1}(M_r) = u^{-1}(M_{r+1}) = \dots$  und  $v(M_r) = v(M_{r+1}) = \dots$

Dies ist äquivalent  $(\star)$  dazu, dass  $M_r = M_{r+1} = \dots$ . Also ist  $M$  noethersch.

Beweis von  $(\star)$ :

Seien  $P \subseteq Q \subseteq M$  Untermoduln mit  $u^{-1}(P) = u^{-1}(Q)$  und  $v(P) = v(Q)$ , sei  $q \in Q$ .

Dann existiert ein  $p \in P$  mit  $v(p) = v(q)$ . Dann gilt  $v(p - q) = 0$ , also  $p - q \in \text{Im}(u)$ .

Dann existiert auch  $m' \in u^{-1}(Q) = u^{-1}(P)$  mit  $u(m') = p - q$  und es gilt  $u(m') \in P$ , also  $q \in P$ , also  $q \in P$ , also  $q = P - u(m')$ .

Es folgt, dass  $P = Q$ .

2. analoge

□

**Korollar 5.7.** Seien  $M_1, \dots, M_r$   $A$ -Moduln und sei  $r \in \mathbb{N}$ . Dann gilt

1.  $\bigoplus_{i=1}^r M_i$  ist genau dann noethersch, wenn  $M_i$  noethersch für alle  $i = 1, \dots, r$ .

2.  $\bigoplus_{i=1}^r M_i$  ist genau dann artinsch, wenn  $M_i$  artinsch für alle  $i = 1, \dots, r$ .

*Beweis.* Induktion nach  $r$ :

Der Fall  $r = 1$  ist klar. Für  $r > 1$  betrachte die Sequenz

$$\begin{array}{rcl} 0 \rightarrow M_r & \rightarrow & \bigoplus_{i=1}^r M_i \rightarrow 0 \\ m_r & \mapsto & (0, \dots, 0, m_r) \\ & & (m_1, \dots, m_r) \mapsto (m_1, \dots, m_{r-1}) \end{array}$$

Mit Proposition 5.6 folgt die Behauptung.

□

**Korollar 5.8.** Ein Ring  $A$  ist genau dann noethersch bzw. artinsch, wenn jeder erzeugte  $A$ -Modul noethersch bzw. artinsch ist.

*Beweis.* Sei  $A$  noethersch bzw. artinsch und sei  $M$  ein endlich erzeugter  $A$ -Modul. Dann gilt  $M \cong A^n/N$  für  $n \in \mathbb{N}$  und  $N \subseteq A^n$  Untermodul. Dann ist die Sequenz  $0 \rightarrow N \rightarrow A^n \rightarrow M \rightarrow 0$  exakt.

Mit 5.7 folgt daraus dass  $A$  noethersch ist auch dass  $A^n$  noethersch ist.

Mit 5.6 folgt dann dass auch  $M$  noethersch ist.  $\square$

**Korollar 5.9.** Sei  $A$  noethersch bzw artinsch und  $\mathfrak{a} \subseteq A$  ein Ideal, dann ist  $A/\mathfrak{a}$  noethersch bzw artinsch.

*Bemerkung 5.10.* Sei  $A$  noethersch bzw artinsch und  $S$  eine  $A$  multiplikative Teilmenge.

Dann ist  $S^{-1}A$  noethersch bzw artinsch.

*Beweis.* Beweis in Übung.  $\square$

## 5B Länge von Moduln

**Definition 5.11.** Sei  $G$  eine Gruppe und sei  $R$  ein (nicht notwendig kommutativer) Ring, sei  $M$  ein  $R$ -(links-)Modul.

1. Eine **Kompositionsreihe von  $G$**  (bzw **von  $M$** ) ist eine Folge  $G = G_0 \supsetneq G_1 \supsetneq \dots \supsetneq G_r = 1$  von Untergruppen, sodass für alle  $i = 1, \dots, r$  die Gruppe  $G$  ein Normalteiler von  $G_{i-1}$  ist.  
(Analog für die Folge  $m = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_r = 0$  von  $R$ -Untermoduln)  
Dann heißt  $r \in \mathbb{N}_0$  die **Länge der Kompositionsreihe**.
2.  $G$  heißt **einfach** falls  $G \neq \{0\}$  und falls  $\{0\}$  und  $G$  die einzigen Normalteiler sind.  
 $M$  heißt **einfach**, falls  $M \neq 0$  und falls  $0$  und  $M$  die einzigen Untermoduln sind.
3. Eine Kompositionsreihe heißt **maximal** oder **Jordan-Hölder Reihe** falls keine echten Normalteiler (bzw. Untermoduln) eingefügt werden können.  
(Äquivalent:  $G_{i+1}/G_1$  bzw.  $m_{i+1}/M_i$  sind einfach für alle  $i = 1, \dots, r$ )

*Bemerkung 5.12.* 1. Normalerweise existiert keine Jordan-Hölder-Reihe

2. Sei  $R = K$  Körper und sei  $V$  ein  $K$ -Vektorraum. Dann ist  $V$  genau dann einfach, wenn  $\dim_K(V) = 0$ .  
Sei  $(v_1, \dots, v_r)$  eine Basis von  $V$ , dann ist  $V = \langle v_1, \dots, v_r \rangle \supsetneq \langle v_1, \dots, v_{r-1} \rangle \supsetneq \dots \supsetneq \langle v_1 \rangle \supsetneq 0$  eine JH-Reihe.
3. Jede Endliche Gruppe besitzt eine JH-Reihe.

*Beispiel 5.12.* Sei  $R = \mathbb{Z} = M$  dann kann man in jede Folge  $\mathbb{Z} = n_0\mathbb{Z} \supsetneq n_1\mathbb{Z} \supsetneq \dots \supsetneq n_r\mathbb{Z} = 0$  mit  $n_0 = 1, n_1 > 1, n_r = 0$  zwischen  $n_{r-1}\mathbb{Z}$  und  $n_r\mathbb{Z}$  die Untergruppe  $2n_{r-1}\mathbb{Z}$  einfügen.

**Proposition 5.13.** Sei  $A$  kein kommutativer Ring,  $M$  ein  $A$ -Modul, dann gilt  $M$  ist genau dann ein einfacher  $A$ -Modul wenn  $M \cong A/\mathfrak{m}$  für maximales Ideal  $\mathfrak{m} \subset A$ .

*Beweis.* " $\Leftarrow$ ": gilt, da  $A/m$  Körper.

" $\Rightarrow$ ": Sei  $M$  einfach,  $x \in M$ ,  $x \neq 0$ . Dann ist  $Ax = M$  also ist  $u : A \rightarrow M, x \mapsto ax$  surjektiv. Damit ist für  $\mathfrak{a} = \text{Ker}(u)$ , dass  $M \cong A/\mathfrak{a}$ . Da

$$\{\text{Untermoduln von } A/\mathfrak{a}\} \xleftrightarrow{1:1} \{\text{Ideale } b \subseteq A \text{ mit } b \supseteq \mathfrak{a}\}$$

muss  $\mathfrak{a}$  maximal sein.  $\square$

**Satz 5.14** (Satz von Jordan-Hölder (simple Variante)). *Sei  $G$  eine Gruppe (bzw.  $R$  ein nicht notwendig kommutativer Ring und  $M$  ein  $R$ -Modul). Dann besitzen je zwei JH-Reihen von  $G$  bzw.  $M$  dieselbe Länge.*

*In diesem Fall kann jede Kompositionsreihe zu einer JH-Reihe ergänzt werden.*

*Bemerkung* (Satz von Hölder (genaue Variante)). Seien  $G = G_0 \supsetneq G_1 \supsetneq \dots \supsetneq G_r = 1$  und  $G = G'_0 \supsetneq G'_1 \supsetneq \dots \supsetneq G'_s = 1$  JH-Reihen.

Dann ist  $r = s$  und es existieren Permutationen  $\sigma \in S_r$ , sodass  $G_{i-1}/G_i \cong G'_{\sigma(i)-1}/G'_{\sigma(i)}$ .

**Definition 5.15.** Sei  $G$  eine Gruppe. Dann heißt

$$l(G) := \begin{cases} \infty & G \text{ besitzt keine JH-Reihe} \\ r & G \text{ besitzt eine JH-Reihe der Länge } r \end{cases}$$

die **Länge von  $G$** .

Sei  $M$  eine  $R$ -Modul. Dann heißt

$$l(M) := \begin{cases} \infty & M \text{ besitzt keine JH-Reihe} \\ r & M \text{ besitzt eine JH-Reihe der Länge } r \end{cases}$$

die **Länge von  $M$** .

*Bemerkung.* Dabei ist  $l(M) = 1$  genau dann wenn  $M$  einfach und  $l(M) = 0$  genau dann wenn  $M = 0$ .

*Beweis.* (für Moduln, für Gruppen analog)

Sei  $M$  ein  $R$ -Modul.

Setze  $l(M) := \inf\{\text{Längen von JH-Reihene von } M\} \in \mathbb{N}_0 \cup \{\infty\}$

1.  $N \subseteq M$  Untermodul  $\Rightarrow l(N) \leq l(M)$ .

Falls  $l(M) = \infty$ .

Man kann also annehmen, dass  $M$  eine JH-Reihe  $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_r = 0$  besitzt mit  $r = l(M)$ .

Sei  $N_i := N \cap M_i$ ,  $\forall i = 0, \dots, r$ .

Die Einbettung  $N_{i-1}/N_i \hookrightarrow M_{i-1}/M_i$  ist injektiv, da  $M_i \cap N_{i-1} = N_i$ .

Daraus folgt (da  $M_{i-1}/M_i$  einfach ist), dass  $N_{i-1}/N_i$  entweder einfach oder  $= 0$  ist.

Dann kann die Reihe  $N = N_0 \supseteq N_1 \supseteq \dots \supseteq N_r = 0$  durch Weglassen einiger Terme zu einer JH-Reihe werden.

Dann gilt  $l(N) \leq l(M)$ .

2. Aus  $N \subseteq M$  Untermodul mit  $l(N) = l(M) < \infty$  folgt  $N = M$ :

Wie in 1) gilt  $M_{i-1}/M_i \cong N_{i-1}/N_i$ , da  $l(N) = l(M)$ .

Aus  $M_r = N_r = 0$  folgt  $M_{r-1} = N_{r-1}$  und da  $N_{r-2}/N_{r-1} = M_{r-2}/M_{r-1}$  folgt auch  $N_{r-2} = M_{r-2}$ .

Induktiv gilt damit  $N_0 = N = M_0 = M$



3. Jede Kompositions Reihe von  $M$  besitzt Länge  $\leq l(M)$ :  
 $(\Rightarrow$  Alle JH-Reihen haben die selbe Länge)  
 Sei  $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_r = 0$  eine Kompositions-Reihe.  
 Aus 1), 2) folgt  $l(M_i) \leq l(M_{i-1})$  für alle  $i = 1, \dots, r$ . Daraus folgt  $s \leq l(M)$ .
4. Sei  $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_s = 0$  eine Kompositions-Reihe,  $l(M) < \infty$ :  
 Wenn  $s = l(M)$ , dann ist  $(M_i)$  JH-Reihe. Wenn  $s < l(M)$ , dann ist  $(M_i)$  keine JH-Reihe und die Kompositions-Reihe kann ergänzt werden.

□

**Satz 5.16.** Sei  $0 \rightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0$  eine exakte Sequenz von  $R$ -Moduln. (Dabei ist  $R$  nicht notwendigerweise kommutativ) Dann ist  $l(M) = l(M') + l(M'')$ .

(Insbesondere ist  $l(M) < \infty$  genau dann wenn  $l(M'), l(M'') < \infty$ )

Für Gruppen ergibt sich ein anderes Resultat.

*Beweis.* Sei  $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_r = 0$  eine Kompositions-Reihe von  $M'$ . Dann ist  $M \supsetneq u(M') = u(M'_0) \supsetneq \dots \supsetneq u(M'_r) = 0$  eine Kompositions-Reihe und  $(M''_i)$  ist eine Kompositionsreihe von  $M''$ . Dann folgt durch  $v^{-1}$ , dass es auch eine Kompositionsreihe von  $M$ .

Insbesondere folgt aus  $l(M') = \infty$  oder  $l(M'') = 0$ , dass  $l(M) = \infty$ .

Sei  $l(M'), l(M'') < \infty$  und sei  $M' = M'_0 \supsetneq M'_1 \supsetneq \dots \supsetneq M'_r = 0$  die JH-Reihe von  $M'$  und  $M'' = M''_0 \supsetneq M''_1 \supsetneq \dots \supsetneq M''_s = 0$  von  $M''$ .

Dann ist

$$M = v^{-1}(M''_0) \supsetneq \dots \supsetneq v^{-1}(M''_s) = \text{Ker}(v) = u(M') \supsetneq u(M'_1) \supsetneq \dots \supsetneq u(M'_r) = 0$$

eine Kompositions-Reihe mit einfachen Subquotienten, also eine JH-Reihe.

Diese hat Länge  $r + s = l(M') + l(M'')$ . □

**Satz 5.17.** Sei  $M$  ein  $A$ -Modul ( $A$  ist kommutativer Ring). Dann ist äquivalent:

1.  $l(M) < \infty$
2.  $M$  ist artinsch und noethersch.

*Beweis.*  $1 \Rightarrow 2$ :

$\text{Ausl}(M) < \infty$  folgt, dass jede nicht stationäre Kette endlich ist und damit 2.

$2 \Rightarrow 1$ :

Sei o.E.  $M \neq 0$ ,  $M$  noethersch.

Dann folgt, dass  $\{N \subseteq M \mid N \text{ Untermodul}\}$  besitzt maximale Elemente, etwas  $M_1$ .

Induktiv gilt  $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$ , wobei  $M_{i-1}/M_i$  einfach.

Da  $M$  artinsch ist folgt, dass es ein  $r \in \mathbb{N}_0$  gibt, sodass  $M_r = 0$ . □

**Beispiel 5.18.** Sei  $K$  Körper,  $V$  ein  $K$ -Vektorraum. Dann sind äquivalent:

1.  $\dim_K(V) < \infty$
2.  $l_k(V) < \infty$
3.  $V$  ist noethersch
4.  $V$  ist artinsch

Es folgt auch, dass  $\dim V = l(V)$ .

## 5C Noethersche Ringe

Wenn  $A$  noethersch, so ist auch  $A/\mathfrak{a}$  noethersch für alle  $\mathfrak{a} \subseteq A$  Ideal und es auch  $S^{-1}A$  noethersch für alle  $S \subseteq A$  multiplikativ.

**Definition 5.19.** Sei  $\varphi : A \rightarrow B$  eine  $A$ -Algebra.

1. Die  $A$ -Algebra  $B$  heißt **endlich erzeugt** oder **von endlichem Typ** (v.e.T.), wenn  $b_1, \dots, b_n \in B$  existieren, die  $B$  erzeugen.  
(Äquivalent:  $B \cong A[X_1, \dots, X_n]/\mathfrak{a}$  für  $\mathfrak{a} \subseteq A[X_1, \dots, X_n]$  Ideal.)
2. Die  $A$ -Algebra  $B$  heißt **endlich**, falls  $B$  als  $A$ -Modul endlich erzeugt ist.

*Bemerkung 5.20.* Sei  $\varphi : A \rightarrow B$  eine  $A$ -Algebra

1.  $B$  endliche  $A$ -Algebra, so folgt, dass  $B$  eine  $A$ -Algebra v.e.T.
2. Sei  $A = K$  Körper, dann ist  $K[X]$  eine  $K$ -Algebra v.e.T., aber  $K[X]$  ist nicht endliche  $K$ -Algebra, da  $\dim_K(K[X]) = \infty$ .

**Satz 5.21** (Hilbertscher Basissatz). Sei  $\varphi : A \rightarrow B$  eine  $A$ -Algebra v.e.T. und sei  $A$  noethersch.

Dann ist  $B$  noethersch.

*Beweis.* 1. Es gilt  $B$  ist genau dann v.e.T. wenn  $B \cong A[X_1, \dots, X_n]/\mathfrak{a}$ .  
Also ist o.E.  $B = A[X_1, \dots, X_n] = (A[X_1, \dots, X_{n-1}])[X_n]$ .  
Induktiv folgt o.E.  $B = A[X]$ .

2. Sei  $\mathfrak{a} \subseteq A[X]$  Ideal und sei  
 $I = \{a \in A \mid \exists f \in \mathfrak{a} \text{ mit } f = aX^d + (\text{Terme niederen Grades})\}$ .  
Da  $\mathfrak{a}$  Ideal folgt, dass  $I$  Ideal und da  $A$  noethersch auch, dass  $I$  endlich erzeugt (etwa von  $a_1, \dots, a_n$ ).  
Wähle nun  $f_1, \dots, f_n \in \mathfrak{a}$ , sodass  $f_i = a_i X^{r_i} + (\text{Terme niedere Ordnung})$ .  
Sei nun  $\mathfrak{a}' := (f_1, \dots, f_n) \subseteq \mathfrak{a}$  und  $r := \max\{r_i \mid i = 1, \dots, n\}$
3. Für alle  $f \in \mathfrak{a}$  existiert  $g \in \mathfrak{a}'$ , so dass  $\deg(f - g) < r$ :  
Sei  $f = aX^m + (\text{Terme niedere Ordnung})$ ,  $s \in I$ .  
Im Fall  $m < r$  folgt die Behauptung.  
Falls  $m \geq r$  Setze  $a = b_1 a_1 + \dots + b_n a_n$  mit  $b_i \in A$ . Dann hat

$$f - \underbrace{\sum_{i=1}^n b_i f_i}_{\in \mathfrak{a}} X^{m-r}$$

Grad  $< m$ .

Induktiv folgt die Behauptung.

4. Sei  $M = A + AX + \dots + AX^{n-1}$  ein endlich erzeugter  $A$ -Modul.  
3 bedeutet, dass  $\mathfrak{a} = \mathfrak{a}' + (\mathfrak{a} \cap M)$ , sodass (da  $A$  noethersch)  $\mathfrak{a} \cap M$  als  $A$ -Modul endlich erzeugt von  $g_1, \dots, g_r$ .  
Dann ist  $\mathfrak{a} = (f_1, \dots, f_n, g_1, \dots, g_r)$ . □

**Korollar 5.22.** Sei  $K$  Körper. Dann ist  $K[X_1, \dots, X_n]$  noethersch.

## 5D Artin-Ringe

**Lemma 5.23.** *In einem Artinring  $A$  ist jedes Primideal ein maximales Ideal.*

*Beweis.* Sei  $\mathfrak{p} \subset A$  Primideal, dann ist  $B := A/\mathfrak{p}$  ein nullteilerfreier Artinring. Behauptung:  $B$  ist Körper ( $\mathfrak{p}$  ist maximal).

Sei  $x \in B, 0 \neq x$ . Betrachte die Kette  $(x) \supseteq (x^2) \supseteq \dots$

Da  $B$  Artinring ist gibt es ein  $n \in \mathbb{N}$ , sodass  $(x^n) = (x^{n+1})$ , also  $x^n = yx^{n+1}$  für ein  $y \in B$ .

Daraus folgt (da  $x$  kein Nullteiler) dass  $1 = xy$ , also  $y \in B^\times$ .  $\square$

**Satz 5.24.** *Jeder Artinring besitzt nur endlich viele Primideale.*

*Beweis.* Sei  $\Sigma := \{m_1 \cap \dots \cap m_r \mid r \geq 0, m_i \subset A \text{ maximale Ideale}\}$ . Dann folgt aus  $A \in \Sigma$ , dass  $\sigma \neq \emptyset$ .

Da  $A$  artinsch folgt, dass  $\Sigma$  ein minimales Element besitzt (etwa  $m_1 \cap \dots \cap m_n$ ).

Sei  $m \subset A$  ein maximales Ideal. Dann ist  $m \cap m_1 \cap \dots \cap m_n = m_1 \cap \dots \cap m_n$ .

Dann ist  $m \supset m_1 \cap \dots \cap m_n = m_1 \cdot \dots \cdot m_n$ . Dann gibt es mit ?? ein  $i$ , sodass  $m \supseteq m_i$ . Da  $m_i$  minimal folgt, dass es sogar ein  $i$  gibt mit  $m = m_i$ .

Also gilt  $\{m \subset A \text{ maximales Ideal}\} = \{m_1, \dots, m_n\}$ .

Dann folgt, mit 5.23 die Behauptung.  $\square$

**Lemma 5.25.** *Sei  $A$  Artinring, dann existiert  $k \in \mathbb{N}$ , sodass  $(\text{Nil}(A))^k = 0$ .*

*Beweis.* Da  $A$  artinsch, wird  $\text{Nil}(A) \supseteq \text{Nil}(A)^2 \supseteq \dots$  stationär.

Also existiert ein  $k \in \mathbb{N}$ , sodass  $\text{Nil}(A)^k = \text{Nil}(A)^{k+1} = \dots =: \mathfrak{a}$ .

Annahme:  $\mathfrak{a} \neq 0$ .

Sei  $\Sigma = \{b \supseteq A \text{ Ideal} \mid b\mathfrak{a} \neq 0\}$ . Dann gilt  $A \in \Sigma$ . Da  $A$  artinsch gibt es ein maximales element  $b_0 \in \Sigma$ .

Sei nun  $x \in b_0$  mit  $x\mathfrak{a} \neq 0$ . Dann ist  $(x)\mathfrak{a} \neq 0$  und es folgt (da  $(x) \subseteq b_0$ ), dass  $(x) = b_0$ .

Da auch  $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$  gilt (da  $x\mathfrak{a} \subseteq (x)$ ), dass  $x\mathfrak{a} = (x)$ .

Also ist  $x = xy$  für ein  $y \in \mathfrak{a} = \text{Nil}(A)^k \subseteq \text{Nil}(A)$ .

Aber mit  $x = xy = xy^2 = \dots$  da  $y$  nilpotent folgt  $x = 0$ .  $\square$

**Theorem 5.26.** *Sei  $A$  ein Ring dann sind äquivalent*

1.  $A$  ist artinsch
2.  $A$  ist noethersch und jedes Primideal ist maximal
3.  $l_A(A) < \infty$ .

*Beweis.* 3)  $\Rightarrow$  1): gilt mit 5.17

3)  $\Rightarrow$  2): ???

1)  $\Rightarrow$  3): Aus 5.24 folgt, dass es endlich viele maximale Ideale gibt, etwa  $m_1 \cap \dots \cap m_n = m_1 \cdot \dots \cdot m_n$ .

Mit 5.25 folgt, dass es ein  $k \in \mathbb{N}$  gibt, sodass  $m_1^k m_2^k \cdot \dots \cdot m_n^k = \text{Nil}(A)^k = (0)$ .

Schreibe  $(0) = M_1 M_2 \dots M_s$  mit  $M_i \subset A$  maximal.

Behauptung: Für  $j = 0, \dots, s$  gilt  $l_A(M_1 M_1, \dots, M_j) < \infty$ :

Für  $j = s$  gilt die Behauptung.

Für  $j \leq s$  ist

$$0 \rightarrow \underbrace{M_1 \dots M_j M_{j+1}}_{\text{Länge} < \infty} \rightarrow M_1 \dots M_j \rightarrow \underbrace{(M_1 \dots M_j / M_1 \dots M_{j+1})}_{\substack{A/M_{j+1}-VR \\ \text{ist artinsch} \\ (?? \text{ hat endliche Länge})}} \rightarrow 0$$

Es folgt, dass  $l_A(M_1 \dots M_j) < \infty$ .

2)  $\Rightarrow$  3): Sei  $l_A(A) = \infty$  und Sei  $\Sigma := \{\mathfrak{a} \subseteq A \mid l_A(A/\mathfrak{a}) = \infty\}$  mit  $(0) \in \Sigma$ .

Dann folgt, da  $A$  noethersch, dass  $\Sigma$  maximales Element  $\mathfrak{a}_0$  besitzt.

Behauptung:  $\mathfrak{a}_0$  ist Primideal.

Sei  $a, b \in A : ab \in \mathfrak{a}_0, a \notin \mathfrak{a}_0$ .

Betrachte nun die exakte Sequenz

$$0 \rightarrow A / \underbrace{\{x \in A \mid xa \in \mathfrak{a}_0\}}_{=: \mathfrak{a}'} \xrightarrow{\cdot a} A/\mathfrak{a}_0 \rightarrow \underbrace{A/(\mathfrak{a}_0 + (a))}_{l_A(\cdot) < \infty}$$

Dann folgt  $l_A(A/\mathfrak{a}') = \infty$ .

Wähle  $b \neq \mathfrak{a}_0$ .  $\mathfrak{a}' \supseteq \mathfrak{a}_0 + (b) \supsetneq \mathfrak{a}_0$ .

Dann folgt  $l(A/\mathfrak{a}') < l(A/\mathfrak{a}_0 + (b)) < \infty$ , da  $\mathfrak{a}_0$  maximal mit  $l(A/\mathfrak{a}_0) = \infty$ .

Aus dem Widerspruch folgt, dass  $\mathfrak{a}_0$  ein maximales Ideal ist,

sodass  $l(A/\mathfrak{a}_0) = 1 \neq \infty$ . Widerspruch!  $\square$

**Korollar 5.27.** Sei  $A$  ein lokaler Artinring.

Dann  $\text{Spec}(A) = \{m\}$  mit  $m = \text{Nil}(A)$  und es gibt ein  $k$ , sodass  $m^k = 0$ ,  $A \setminus m = A^\times$ .

*Beispiel.* Sei  $A$  ein lokaler noetherscher Ring und  $m \subset A$  maximal.

Dann gilt für alle  $n \geq 1$ , dass  $A/m^n$  ein lokaler Artinring ist.

Man kann zeigen, dass  $\bigcap_{n \geq 1} m^n = \{0\}$ .

Definiere eine Metrik auf  $A$ :  $0 < \rho, \rho \in \mathbb{R}$  mit  $d(x, y) := \rho^n$ , falls  $x - y \in m^n \setminus m^{n+1}$ .

Approximation von

$$\hat{A} := \text{Vervollständigung von } A \text{ bezüglich } d \text{ durch } A/m^n$$

*Beispiel.* Sei  $\mathbb{Z}(p) := \{\frac{a}{b} \in \mathbb{Q} \mid p \text{ teilt nicht } b\}$  für  $p$  Primzahl.

**Satz 5.28** (Struktursatz für Artinringe). Jeder Artinring  $A$  ist Produkt von endlichen lokalen Artinringen.

*Beweis.* Seien  $m_1, \dots, m_n \subset A$  die maximalen Ideale.

Dann existiert ein  $k \in \mathbb{N}$ , sodass  $0 = m_1^k \dots m_n^k = m_1^k \cap \dots \cap m_n^k$ . Mit dem Chinesischen Restsatz folgt, dass

$$A \xrightarrow{\sim} \prod_{i=1}^n \underbrace{A/m_i^k}_{\text{lokale Artin-Ringe}}$$

ist ein Isomorphismus.  $\square$

## 6 Ganzheit

### 6A Ganze Ring-Homomorphismen

**Definition 6.1.** Sei  $\varphi : A \rightarrow B$  ein Ring Homomorphismus:

1. Ein Element  $b \in B$  heißt **ganz über**  $A$  (bezüglich  $\varphi$ ) falls ein normiertes Polynom  $f \in A[X]$  existiert, sodass  $f(b) = b^n + \varphi(a_{n-1})b^{n-1} + \dots + \varphi(a_0) = 0$ .

2.  $\varphi$  heißt **ganz**, falls jedes Element  $b \in B$  ganz über  $A$  ist.

*Bemerkung 6.2.* 1. Sei  $\varphi : A \rightarrow B$  ein surjektiver Ring Homomorphismus.

Dann ist  $\varphi$  ganz:

Sei  $b \in B$ . Wähle  $a \in A$  mit  $\varphi(a) = b$ .

Dann  $f(b) = 0$ , wobei  $f = X - a$ .

2. Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus,  $b \in B$ .

Dann ist  $b$  ganz über  $A$  genau dann wenn  $b$  ganz über  $\varphi(A)$ .

*Beispiel 6.3.* Sei  $A$  ein faktorieller Ring,  $K = \text{Quot}(A)$ . Dann ist  $x \in K$  ganz über  $A$  genau dann wenn  $x \in A$ .

*Beweis.*  $\Rightarrow$  Sei  $x = \frac{1}{b}$  mit  $a, b \in A, b \neq 0$ , sodass kein Primielement  $a$  und  $b$  teilt.

Da  $x$  ganz ist folgt

$$\left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \dots + a_1 \frac{a}{b} + a_0 = 0$$

für  $a_0, \dots, a_{n-1} \in A$ : Multiplikation mit  $b^n$  ergibt:

$$a^n + ba_{n-1}a^{n-1} + \dots + b^{n-1}a_1a + b^na_0 = 0$$

Sei  $p$  ein Primteiler von  $b$ , also  $p$  teilt  $a^n$ . Dann teilt  $p$  auch  $a$ . Widerspruch!

Also  $b \in A^\times$ , also  $x \in A$ .  $\square$

*Beispiel.* Sei  $A = \mathbb{Z}$ ,  $x = \frac{1}{2}$ ,  $f(x) = 0$  mit  $f = 2X - 1$

*Bemerkung (Anwendung).* Sei  $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ .

Falls  $f(x) = 0$  für  $x \in \mathbb{Q}$ , dann  $x \in \mathbb{Z}$  und  $x$  Teiler von  $a_0$ .

**Satz 6.4.** Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus und  $b \in B$ . Dann ist äquivalent:

1.  $b$  ist ganz über  $A$ .
2.  $A[b] = \{f(b) \mid f \in A[T]\} = \{\sum_{i=1}^n \varphi(a_i)b^i \mid a_i \in A, n \in \mathbb{N}\}$  ist eine endliche  $A$ -Algebra (d.h.  $A[b]$  ist als  $A$ -Modul endlich erzeugt)
3.  $A[b]$  ist in einem Unterring  $C \subseteq B$  enthalten, sodass  $C$  eine endliche  $A$ -Algebra ist.

*Beweis.* •  $1) \Rightarrow 2)$ :  $b$  ist ganz über  $A$ , also gibt es  $a_i \in A$ , sodass  $b^n = -(\varphi(a_{n-1})b^{n-1} + \dots + \varphi(a_0))$ . Dann auch

$$b^{n+r} = -(\varphi(a_{n-1})b^{n-1+r} + \dots + \varphi(a_0)b^r)$$

für alle  $r \geq 0$ . Dann ist  $A[b]$  der  $A$ -Modul, der von  $1, b, \dots, b^{r-1}$  erzeugt wird.

- $2) \Rightarrow 3)$ :  $C = A[b]$ .

- $3) \Rightarrow 1)$ : Sei  $U : C \rightarrow C, c \mapsto bc$ . Mit 4.36 folgt, dass es  $a_i \in A$  gibt, sodass  $u^n + a_{n-1}u^{n-1} + \dots + a_0 = 0 \in \text{End}_A(C)$ . Dann ist aber (mit  $b = u(1)$ )

$$b^n + \varphi(a_{n-1})b^{n-1} + \dots + \varphi(a_0) = 0$$

$\square$

**Satz 6.5.** Sei  $\varphi : A \rightarrow B$  ein Ring Homomorphismus. Dann sind äquivalent:

1.  $\varphi$  endlich
2.  $\varphi$  ist von endlichem Typ und ganz
3. Es gibt  $b_1, \dots, b_n \in B$ , sodass  $b_i$  ganz über  $A$  ist und  $B = A[b_1, \dots, b_n]$

*Beweis.* durch Ringschluss:

- 1)  $\Rightarrow$  2): nach 6.4
- 2)  $\Rightarrow$  3): Betrachte die Abbildung  $A[T_1, \dots, T_n] \xrightarrow{\sim} B$ , wobei  $b_i := \psi(T_i)$ .
- 3)  $\Rightarrow$  1): Sei  $B = A[b_1, \dots, b_n]$  mit  $b_i$  ganz über  $A$ .  
Wir wissen, dass  $A[b_1]$  eine endliche  $A$ -Algebra ist.  
Sei nun  $A_k := A[b_1, \dots, b_k]$  für  $k \leq n$ .  
Dann ist  $A_k = A_{k-1}[b_k]$

□

**Satz 6.6.** Seien die Ring-Homomorphismen  $\varphi : A \rightarrow B$ ,  $\psi : B \rightarrow C$  ganz.  
Dann ist auch  $\psi \circ \varphi$  ganz.

*Beweis.* OE (referenz auf bem)  $A \subseteq B \subseteq C$ . Sei  $x \in C$ , also existieren  $b_0, \dots, b_{n-1} \in B$  sodass  $x^n + b_{n-1}x^{n-1} + \dots + b_0 = 0$ .

Betrachte nun  $B' = A[b_0, \dots, b_{n-1}]$ . Dann ist  $B'$  ein endlich erzeugter  $A$ -Modul und  $B'[x]$  ist ein endlich erzeugter  $B'$ -Modul.

(d.h. es gibt surjektive Abbildungen  $A^r \rightarrow B'$ ,  $(B')^k \rightarrow B'[x]$ , also auch surjektives  $B'^{rk} \rightarrow B'[x]$ )

Also ist  $B'[x]$  ein endlich erzeugter  $A$ -Modul und damit ist nach 6.4  $x$  ganz über  $A$ . □

## 6B Ganzer Abschluss

**Korollar 6.7.** Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus. Dann ist

$$C := \{b \in B \mid b \text{ ist ganz über } A\} \quad (6.7.1)$$

ein Unterring von  $B$ .

*Beweis.* Sei  $x, y \in C$ . Betrachte  $A[x, y]$  (ist nach 6.5 endliche  $A$ -Algebra).

Dann ist mit 6.5 die Abbildung  $A \rightarrow A[x, y]$  ganz.

Insbesondere sind  $x \cdot y, x \pm y \in A[x, y]$  ganz über  $A$ . □

**Definition 6.8.** 1. Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus. Der Unterring  $C$  (aus 6.7.1) wird der **ganze Abschluss von  $A$  in  $B$**  genannt.

2.  $A$  heißt **ganz abgeschlossen**, falls  $C = \varphi(A)$ .

**Korollar 6.9.** Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus und sei  $C$  der ganze Abschluss von  $A$  in  $B$ , dann ist  $C$  ganz abgeschlossen.

*Beweis.* Sei  $b \in B$  und  $b$  ganz über  $C$  (bezüglich der Inklusion  $C \subseteq B$ ). Da  $C$  ganz über  $A$  ist, ist auch  $b$  ganz über  $A$  (vgl 6.6). Also ist  $b \in C$ . □

**Bemerkung 6.10.** Sei  $\varphi : A \rightarrow B$  ein ganzer Ring-Homomorphismus,  $\mathfrak{b} \subseteq B$  ein ideal. Dann ist

$$A/\varphi^{-1}(\mathfrak{b}) \rightarrow B/\mathfrak{b}$$

auch ganz.

**Satz 6.11.** Sei  $\varphi : A \rightarrow B$  ein Ring-Homomorphismus,  $C \subseteq B$  der Ganze Abschluss von  $A$  in  $B$  und sei  $S \subseteq A$  eine multiplikative Teilmenge. Dann ist  $\varphi(S)^{-1}C$  der ganze Abschluss von  $S^{-1}A$  in  $\varphi(S)^{-1}B$ . Insbesondere ist  $\varphi(S)^{-1}B$  ganz über  $S^{-1}A$ , falls  $\varphi$  ganz ist.

*Beweis.* OE  $A \subseteq B \subseteq C$ . Wir zeigen zuerst, dass  $S^{-1}C$  ganz über  $S^{-1}A$ . Sei dazu  $\frac{c}{s} \in S^{-1}C$ . Es existieren  $a_i$ , sodass  $c^n a_{n-1} c^{n-1} + \dots + a_0 = 0$ . Dann ist

$$\left(\frac{c}{s}\right)^n + \underbrace{\left(\frac{c}{s}\right)^{n-1} \left(\frac{a_{n-1}}{s}\right)}_{\in S^{-1}A} + \dots + \frac{a_0}{s^n}$$

ist Ganzheitsgleichung für  $\frac{c}{s}$  über  $S^{-1}A$ , also ist  $\frac{c}{s}$  ganz über  $S^{-1}A$ .

Sei nun  $\frac{b}{s} \in S^{-1}B$  ganz über  $S^{-1}A$ , d.h. es gibt  $a_i \in A, s_i \in S$ , sodass

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}} \left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_0}{s_0} = 0 \quad (\star)$$

Sei  $t = s_0 \cdot \dots \cdot s_{n-1}$ . Multipliziere  $(\star)$  mit  $(ts)^n$ , dann ist

$$(tb)^n + a_{n-1}x_1(tb)^{n-1} + \dots + x_n = 0$$

(wobei  $x_1, \dots, x_n \in A$ ) Ganzheitsgleichung von  $t \cdot B$  über  $A$ .  $\square$

**Definition 6.12.** Ein Nullteiler freier Ring heißt **ganz Abgeschlossen** (ohne Spezifizierung worin) oder **normal**, falls  $A$  ganz abgeschlossen in  $\text{Quot}(A)$ .

**Satz 6.13.** Jeder faktorielle Ring ist normal

*Beweis.* in Beispiel 6.3.  $\square$

## 6C Going-Up

**Satz 6.14.** Sei  $B$  ein nullteiler freier Ring und  $A \subseteq B$  ein Unterring und sei  $B$  ganz über  $A$ .

Dann ist  $A$  genau dann ein Körper wenn  $B$  ein Körper ist.

*Beweis.* • Sei  $A$  Körper und  $y \in B$  mit  $y \neq 0$ . Nehme Ganzheitsgleichung von  $y$  über  $A$  mit minimalem Grad:

$$y^n + a_{n-1}y^{n-1} + \dots + a_0 = 0$$

Da  $B$  nullteilerfrei ist, gilt  $a_0 \neq 0$ .

(Nehme an, dass  $a_0 = 0$ , dann  $y(y^{n-1} + a_{n-1}y^{n-2} + \dots + a_1) = 0$  also Grad nicht minimal)

Sei  $\delta := -a_0^{-1}(y^{n-1} + a_{n-1}y^{n-2} + \dots + a_1) \in B$  mit  $\delta y = 1$ . Also ist  $B$  Körper.

- Sei nun  $B$  Körper,  $x \in A \setminus \{0\}$ . Es gilt  $x^{-1} \in B$ , also ganz über  $A$ . Also finden wir zur Gleichung  $x^{-m} + a_{m-1}x^{-m+1} + \dots + a_0 = 0$  durch Multiplikation mit  $x^{m-1}$

$$x^{-1} + \underbrace{a_{m-1} + a_{m-2} + \dots + a_0 x^{m-1}}_{\in A} = 0$$

Also liegt  $x^{-1} \in A$ .

□

**Korollar 6.15.** Sei  $\varphi : A \rightarrow B$  ein ganzer Ring-Homomorphismus. Sei  $q \subseteq B$  Primideal,  $p := \varphi^{-1}(q)$ . Damit ist  $q$  maximal gdw  $p$  maximal.

*Beweis.* Es gilt  $A/p \rightarrow B/q$  ist ganz. Satz 6.14 gibt uns, dass  $A/p$  genau dann Körper ist, wenn  $B/q$  Körper ist. Es folgt die Behauptung □

**Korollar 6.16.** Sei  $\varphi : A \rightarrow B$  ein ganzer Ring-Homomorphismus, seien  $q \subseteq q' \subseteq B$  Primideale, so dass  $p := \varphi^{-1}(q) = \varphi^{-1}(q')$ . Dann gilt  $q = q'$

*Beweis.* In  $A_p = S^{-1}A$ ,  $S = A \setminus p$  ist  $pA_p$  maximal. Betrachte

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ a \mapsto \frac{a}{1} \downarrow & & \downarrow b \mapsto \frac{b}{1} \\ A_p & \xrightarrow{\psi = S^{-1}\varphi} & B_p \end{array}$$

Wobei  $pA_p \subset A_p$  und  $qB_p \subseteq B_p = \varphi^{-1}SB$  und auch  $qB_p \subseteq pB_p$  Primideal.

Mit 6.11 folgt  $\psi$  ist ganz.

Also gilt OE  $p \subset A$  ist maximal, sodass mit 6.15 folgt, dass  $q, q'$  maximal sind und da  $q \subseteq q'$  gilt  $q = q'$ . □

**Satz 6.17.** Sei  $\varphi : A \rightarrow B$  ein injektiver ganzer Ring Homomorphismus. Dann existiert für jedes Primideal  $p \subset A$  ein Primideal  $q \in B$  mit  $\varphi^{-1}(q) = p$ . (D.h.  $\text{Spec}(B) \rightarrow \text{Spec}(A), q \mapsto \varphi^{-1}(q)$  ist surjektiv.)

*Beweis.* Ersetze  $A$  durch  $A_p$ , dann gilt OE, dass  $p \subset A$  maximal und  $A$  lokal ist.

Da  $\varphi$  injektiv ist folgt  $B \neq 0$ .

Also existiert ein maximales Ideal  $q \subseteq B$  und mit 6.15 ist  $\varphi^{-1}(q)$  maximal, also  $\varphi^{-1}(q) = p$ . □

**Theorem 6.18** (Going Up). Sei  $\varphi : A \rightarrow B$  ein ganzer injektiver Ring-Homomorphismus und seien  $n \geq m \geq 0$  ganze Zahlen. Sei  $p_i \subsetneq \dots \subsetneq p_m \subsetneq \dots \subsetneq p_n \subset A$  eine Kette von Primidealen und sei  $q_1 \subseteq \dots \subseteq q_n \subset B$  eine Kette von Primidealen mit  $\varphi(q_i) = p_i$  für  $i = 1, \dots, m$ .

Dann gilt  $q_1 \subsetneq \dots \subsetneq q_m$  und es existiert eine Kette von Primidealen  $q_1 \subsetneq \dots \subsetneq q_m \subsetneq q_{m+1} \subsetneq \dots \subsetneq q_n \subset B$  mit  $\varphi^{-1}(q) = p_i$  für alle  $i = 1, \dots, n$ .

*Beweis.* Sei OE  $n > m$ ,  $n_1 = 1, m = 0$ . Dann folgt mit 6.17, dass  $q_1 \subsetneq \dots \subsetneq q_m$ : Vollständige Induktion: Sei OE  $m = 1, n = 2$ . Betrachte

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & & \downarrow \\ A/p_1 & \xrightarrow{\bar{\varphi}} & B/q \end{array}$$



Wobei  $\bar{\varphi}$  ganz und injektiv ist, da  $\varphi^{-1}(q_i) = p_1$  und  $p_2/p_1 \subseteq A/p_1$ .  
Dann folgt mit 6.17, dass es das Primideal  $\bar{q}_2 \subset B/q_i$  gibt mit  $\bar{\varphi}^{-1}(\bar{q}_2) = p_2/p_1$ .  
Dass ist  $\bar{q}_2 \hat{=} q_2 \subset B$ , wobei  $q_2$  Primideal mit  $q_2 \supseteq q_1$  und  $\varphi^{-1}(q_2)p_2$ .  $\square$

## 7 Irreduzibilität

### 7A Satz von Gauß

*Erinnerung 7.1.* 1. Sei  $A$  ein nullteilerfreier Ring. Ein Element  $p \in A$  heißt

- (a) **irrefuzibel**, falls  $0 \neq p \notin A^\times$  und falls  $p = ab$  mit  $a, b \in A$ , so gilt  $a \in A^\times$  oder  $b \in A^\times$ .
- (b) **Primelement**, falls  $p \neq 0$  und  $(p)$  ist Primideal.

Es gilt, wenn  $p$  Primelement ist, so ist  $p$  irreduzibel.

2.  $A$  heißt **faktoriell**, falls er die folgenden äquivalenten Bedingung erfüllt:

- (a) Jedes  $0 \neq a \notin A^\times$  ist Produkt von irreduziblen Elementen und diese Zerlegung ist eindeutig bis auf Reihenfolge und Multiplikation mit Einheiten.
- (b) Jedes Element  $0 \neq a \notin A^\times$  ist Produkt von Primelementen.
- (c) Jedes Irreduzible Element ist ein Primelement und jede aufsteigende Kette von Hauptidealen wird stationär.

*Beweis.* • b)  $\Rightarrow$  a): Einführung in die Algebra (Beweis HIR sind faktoriell)

• a)  $\Rightarrow$  c):

- 1. Sei  $p \in A$  irreduzibel. Seien  $a, b \in A$  mit  $ab \in (p)$ .  
Setze  $ab = dp$  mit  $d \in A$ . Seien  $a = p_1 \dots p_r$ ,  $b = q_1 \dots q_s$  und  $d = l_1 \dots l_t$   
irreduzible Zerlegungen. Dann

$$p_1 \dots p_r q_1 \dots q_s = p l_1 \dots l_t$$

Aus der Eindeutigkeit folgt, dass es ein  $i$  gibt sodass  $(p) = (p_i)$  oder ein  $j$ , sodass  $(p) = (q_j)$ .

Daraus folgt,  $p$  teilt  $a$  oder  $b$ .

- 2. gibt, dass jedes Element  $\neq 0$  hat nur endlich viele Teiler. (Bis auf Multiplikation mit Einheiten).

Mit Anderen Worten: Für jedes Hauptideal  $\mathfrak{a} \neq 0$  existieren nur endlich viele Hauptideale, die  $\mathfrak{a}$  enthalten.

$\Rightarrow$  Jede aufsteigende Kette von Hauptidealen wird stationär.

- c)  $\Rightarrow$  b): Sei  $\Sigma := \{(a) \mid 0 \neq a \in A^\times \text{ und } a \text{ ist nicht Produkt von irreduziblen Elementen}\}$ .  
Angenommen  $\Sigma \neq \emptyset$ :  
Dann folgt mit 5.1

$\square$

*Beispiel 7.2.* Jeder Hauptidealring ist faktoriell. Insbesondere auch  $\mathbb{Z}, K[X]$

**Definition 7.3.** Sei  $A$  ein Ring,  $f = a_m X^m + \dots + a_1 X + a_0 \in A[X]$  heißt **primitiv**, falls  $(a_1, \dots, a_n) = A$ .

*Beispiel.* 1. Sei  $A$  faktoriell. Dann ist  $f$  genau dann Primitiv, wenn kein Primelement alle  $a_i$  teilt.

2. Seien  $f, g \in A[X]$ . Dann sind  $f, g$  genau dann primitiv, falls  $fg$  primitiv.

**Definition 7.3.** Sei  $A$  faktoriell. Ein  $c(f) \in A$  heißt **Inhalt von  $f$** , falls  $c(f)$  ein größter gemeinsamer Teiler von  $a_1, \dots, a_0$  ist.

*Bemerkung.* Also ist  $g$  genau dann primitiv, falls  $c(f) \in A^\times$ .

Für  $f \in A[X]$  gilt, dass  $f = c(f)\tilde{f}$  mit  $\tilde{f}$  primitiv.

*Bemerkung.* Sei  $f = 3X^{1000} + 30X^7 + 21X + 27$ , dann  $c(f) = 3$  oder  $-3$ .  
Dann  $f = 3\tilde{f}$ , also  $\tilde{f} = X^{1000} + 10X^7 + 7X + 9$ .

**Theorem 7.4** (Satz von Gauß). *Sei  $A$  ein faktorieller Ring. Dann ist auch  $A[X]$  faktoriell.*

*Die irreduziblen Elemente von  $A[X]$  sind:*

1.  $p \in A$  irreduzibel und
2.  $f \in A[X]$  primitiv, sodass  $f \in \text{Quot}(A)[X]$  irreduzibel ist.

*Beispiel.* Sei  $A = \mathbb{Z}$ ,

- $2X + 4 \in \mathbb{Z}[X]$  ist reduzibel, da  $2X + 4 = 2(X + 2)$
- $X^3 - 5 \in \mathbb{Z}[X]$  ist primitiv und irreduzibel in  $\mathbb{Q}[X]$

*Beweis.* 1. Seien  $f, g \in K[X] \setminus \{0\}$ . Schreibe  $f = c(f)\tilde{f}$ ,  $g = c(g)\tilde{g}$  mit  $\tilde{f}, \tilde{g}$  primitiv. Dann  $fg = c(f)c(g)\tilde{f}\tilde{g}$ , sodass  $c(fg) = c(f)c(g)$  gilt.

2. Behauptung:  $p \in A$  ist irreduzibel, dann ist  $p \in A[X]$  Primelement:

$$A[X]/pA[X] = (A/p)[X]$$

ist nullteilerfrei (da  $A/p$  nullteilerfrei ist). Dann ist  $p \in A$  prim.

3. Sei  $q \in A[X]$  primitiv,  $q \in K[X]$  irreduzibel.

Behauptung:  $qK[X] \cap A[X] = qA[X]$ :

- " $\supseteq$ " ist klar
- " $\subseteq$ ": Sei  $f \in K[X]$  mit  $qf \in A[X]$ , sei  $f = c(f)\tilde{f}$  mit  $\tilde{f}$  primitiv. Dann gilt  $c(qf) \in A$  und  $c(qf) = c(q)c(f)$  wobei  $c(q) \in A^\times$ . Dann folgt, dass  $c(q)c(f) = c(f)$  und damit  $f \in A[X]$ .

Die Behauptung gilt also genau dann wenn  $A[X]/qA[X] \rightarrow K[X]/qK[X]$  injektiv ist.

Also ist  $q \in A[X]$  Primelement.

4. Jedes  $f \in A[X]$  mit  $0 \neq f \notin A^\times$  ist Produkt der Primelemente von (a) und (b).  
 Schreibe  $f = c(f)\tilde{f}$ ,  $c(f)$  ist Produkt von Primelementen in (a) und  $\tilde{f}$  ist primitiv.  
 Sei  $\tilde{f} = g_1 \dots g_r$  mit  $g_i \in K[X]$  irreduzibel,  $g_i = c_i \tilde{g}_i$ ,  $c_i \in K^\times$ ,  $\tilde{g}_i$  primitiv.  
 Es folgt, dass  $\tilde{f} = c_1 \dots c_r \tilde{g}_1 \dots \tilde{g}_r$ .  
 Da  $c(f) \in A^\times$  und  $c(\tilde{g}_1 \dots \tilde{g}_r) \in A^\times$  ist auch  $c_1 \dots c_r \in A^\times$ .  
 Mit 7.1 folgt die Aussage. □

**Korollar 7.5.** *Sei  $A$  ein faktorieller Ring. Dann ist  $A[X_1, \dots, X_n]$  faktoriell. Insbesondere folgt dies wenn  $A$  Körper.*

## 7B Irreduzibilitätskriterien

Sei  $K$  Körper,  $f \in K[X]$ ,  $f \neq 0$ .

0. Sei  $\deg(f) = 0$ , dann  $f$  nicht irreduzibel in  $K[X]$ , da  $f \in K[X]^\times = K^\times$ .
1. Sei  $\deg(f) = 1$ , dann ist  $f$  immer irreduzibel in  $K[X]$ .
2. Sei  $\deg(f) = 2$  oder  $\deg(f) = 3$ , dann ist  $f$  genau dann reduzibel, wenn  $f$  eine Nullstelle hat.
3. Sei  $\deg(f) > 1$  und  $f$  habe eine Nullstelle, dann ist  $f$  reduzibel

**Satz 7.6** (Reduzibilitätskriterium). *Sei  $A$  ein faktorieller Ring,  $K = \text{Quot}(A)$ ,  $f = a_n X^n + \dots + a_1 X + a_0 \in A[X]$ , zu  $p \in A$  Primelement mit  $p$  teilt nicht  $a_n$ . Sei  $\bar{f} \in A/p[X]$  das Bild von  $f$ . Dann folgt aus  $\bar{f}$  irreduzibel in  $A/p[X]$ , dass  $f$  in  $K[X]$  irreduzibel ist.*

*Beweis.* Betrachte zuerst  $f$  primitiv:

Sei  $f \in K[X]$  reduzibel, dann folgt mit 7.4, dass  $f$  in  $A[X]$  reduzibel ist.  
 Also gibt es  $g, h \in A[X]$ , mit  $\deg(g), \deg(h) \geq 1$ , sodass  $f = gh$ .  
 Da der Führende Koeffizient von  $f$  nach Voraussetzung nicht durch  $p$  teilbar ist, sind auch die Führenden Koeffizienten von  $g, h$  nicht durch  $p$  teilbar.  
 Da  $\deg(\bar{g}) = \deg(g) \geq 1$  und  $\deg(\bar{h}) = \deg(h) \geq 1$  folgt, dass  $\bar{f} = \bar{g}\bar{h}$  reduzibel ist.

Allgemeiner Fall: Schreibe  $f = c(f)\tilde{f}$  mit  $c(f) \in A \setminus \{0\}$  und  $\tilde{f}$  primitiv.  
 $f$  ist genau dann in  $K[X]$  reduzibel, wenn  $\tilde{f}$  in  $K[X]$  reduzibel ist.

Im gezeigten Spezialfall folgt aus  $\tilde{f}$  ist reduzibel in  $A/p[X]$ , dass  $\bar{f} = \overline{c(f)}\bar{\tilde{f}}$  reduzibel ist. □

*Beispiel.* 1. Sei  $f = 3X^4 + 2X^2 + 7X^2 + X - 5 \in \mathbb{Z}[X]$ . Dann gilt mod 2:

$$f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$$

Betrachte nun die Reduziblen Polynome mit  $\deg = 2$ :  $\{X^2 + X + 1, X^2 + 1, X^2\}$ , wobei deren Quadrate keinen Teiler von  $f$  sind.  
 Also ist  $f$  irreduzibel.

2. Sei  $f = X + Y^2 + YX - 2Y + 3 \in \mathbb{Q}[X, Y]$  ist gleich  $XY^2 + (X - 2)Y + 3 \in (\mathbb{Q}[X])[Y]$  modulo  $X - 2$  gilt:  
 $2Y^2 + 3 \in \mathbb{Q}[Y] = \mathbb{Q}[X, Y]/(X - 2)$  ist irreduzibel, also ist  $f$  irreduzibel.

**Satz 7.7** (Eisensteinkriterium). *Sei  $A$  faktoriell,  $f = a_n X^n + \dots + a_1 X + a_0 \in A[X]$  primitiv und es existiert ein Primelement  $p \in A$ , sodass*

1.  $p$  teilt nicht  $a_n$
2.  $p$  teilt  $a_i$  für alle  $i = 0, \dots, n - 1$
3.  $p^2$  teilt nicht  $a_0$

Dann ist  $f$  irreduzibel in  $\text{Quot}(A)[X]$ .

*Beweis.* Sei  $f$  reduzibel in  $A[X]$ ,  $f = gh$  für  $g, h \in A[X]$  mit  $\deg(g), \deg(h) \geq 1$  (und  $< n$ ).

Modulo  $p$  gilt:  $\bar{a}_n X^n = \bar{f} = \bar{g}\bar{h} \in A/p[X]$  und  $a_n \neq 0$ .

Da die irreduzible Zerlegung Eindeutig in  $\text{Quot}(A/p)[X]$  ist:

$\bar{g} = uX^m, \bar{h} = vX^r$ , mit  $u, v \neq 0$  und  $m, r > 0$ .

Dann sind die Absoluten Koeffizienten von  $g, h$  durch  $p$  Teilbar, was einen Widerspruch zu 3) darstellt.  $\square$

*Beispiel 7.8.* Sei  $A$  faktorielle  $p \in A$  prim,  $n \geq 1$ .

Dann ist  $X^n - p$  irreduzibel.

## 8 Algebraische Körpererweiterungen

### 8A Körpererweiterungen

**Definition 8.1.** Eine  $K$ -Algebra  $\iota : K \hookrightarrow L$  heißt **Körpererweiterung**, falls  $L$  Körper ist. (Also  $K \rightarrow L$  injektiv).

Eine **Teilerweiterung** ist ein Unterkörper  $M$  von  $L$ , sodass  $\iota(K) \subset M$ .

**Definition 8.17.** Sei  $A$  eine  $K$ -Algebra,  $a \in A$  algebraisch. Betrachte den  $K$ -Algebra Homomorphismus  $\varphi : K[X] \rightarrow A, f \mapsto f(a)$ . Dann ist  $\mu_{a,K} \in K[X]$  das **Minimalpolynom von  $a$  über  $K$** , wenn  $\text{Ker}(\varphi) = (\mu_{a,K})$ .

*Bemerkung.* Sei  $A$  eine  $K$ -Algebra,  $a \in A$ . Betrachte den  $K$ -Algebra Homomorphismus  $\varphi : K[X] \rightarrow A, f \mapsto f(a)$ . Dann ist

$$\text{Im } \varphi = \{f(a) \in A \mid f \in K[X]\} = K[a]$$

und es sind äquivalent:

1.  $a$  ist algebraisch
2.  $\varphi$  ist nicht injektiv
3.  $\text{Ker}(\varphi) = (\mu_{a,K})$  für ein eindeutiges, normiertes Polynom  $\mu_{a,K} \in K[X]$ .
4.  $[K[a] : K] < \infty$ .  
 In diesem Fall gilt  $[K[a] : K] = \deg(\mu_{a,K})$

*Beweis.* •  $1) \Leftrightarrow 2) \Leftrightarrow 3)$  ist klar.

- 3) $\Rightarrow$ 4): Es gilt, 3) ist äquivalent dazu, dass  $K[a] = K[X]/(\mu_{a,K})$  für normierte Polynome  $\mu_{a,K}$ .  
Es folgt, dass  $K[a]$  eine endliche  $K$ -Algebra ist mit  $[K[a] : K] = \deg(\mu_{a,K})$ .
- 4) $\Rightarrow$ 2): gilt, da sonst  $K[a] \cong K[X]$ .

□

### 8.18 Bestimmung von $\mu_{a,K}$ I

Sei  $A$  eine  $K$ -Algebra,  $a \in A$  algebraisch. Sei  $f \in K[X]$  mit  $f(a) = 0$ , dann ist  $\mu_{a,K}$  ein Teiler von  $f$ . Also gilt für  $f \in K[X]$ :

$\mu_{a,K}$  ist genau dann gleich  $f$ , wenn  $f$  normiert  $f(a) = 0$  und  $\deg(f) \leq [K[a] : K]$ .

*Beispiel.* Sei  $A = K \times K$ , (mit  $x \mapsto (x, x)$ ), sei  $a = (1, 0)$ . Dann ist  $\mu_{a,K} = X^2 - X = X(X - 1)$ .

**Proposition 8.19.** Sei  $K \hookrightarrow L$  eine Körpererweiterung,  $a \in L$ .

Dann ist  $a$  genau dann algebraisch über  $K$ , wenn  $K[a] = K(a) \Leftrightarrow K[a]$  Körper).

### Bestimmung von $\mu_{a,K}$ II

Für  $f \in K[X]$ :

$f = \mu_{a,K}$  genau dann wenn  $f$  normiert,  $f(a) = 0$  und  $f$  irreduzibel ist.

*Beweis.* " $\Rightarrow$ ": Sei  $a$  algebraisch, dann ist  $K[a] \subseteq L$  nullteilerfrei und ganz über  $K$ .

Dann folgt mit ??, dass  $K[a]$  ein Körper ist, sodass  $K(a) = K[a]$ .

Ferner gilt  $K[a] = K[X]/(\mu_{a,K})$  ist genau dann Körper wenn  $\mu_{a,K}$  ein maximales Ideal, was äquivalent dazu ist, dass  $\mu_{a,K}$  irreduzibel ist. " $\Leftarrow$ ": Sei  $a$  transzendent, dann folgt mit ??, dass  $K[X] \xrightarrow{\sim} K[a]$ , dann ist  $K[a]$  kein Körper. □

*Beispiel 8.20.* Sei  $K = \mathbb{Q}$ .

1. Sei  $a = \sqrt{2} \in \mathbb{R}$ , dann ist  $\mu_{a,\mathbb{Q}} = X^2 - 2$  (da  $X^2 - 2$  irreduzibel, normiert und  $(\sqrt{2})^2 - 2 = 0$  ist.)  
Allgemein: Sei  $p$  Primzahl,  $a = \sqrt[p]{p} \in \mathbb{C}$ . Dann ist  $\mu_{a,\mathbb{Q}} = X^p - p$  (da  $X^p - p$  mit 7.7 irreduzibel ist.)

2. Sei  $a = \sqrt[4]{2}$ , dann ist  $\mu_{a,\mathbb{Q}[\sqrt{2}]} = X^2 - \sqrt{2} \in \mathbb{Q}[\sqrt{2}][X]$ .

3. Sei  $p$  Primzahl,  $\zeta \in \mathbb{C}$ ,  $\zeta \neq 1$  mit  $\zeta^p = 1$ .  
(Dann  $\zeta = e^{\frac{2\pi i k}{p}}$  für  $k = 1, \dots, p-1$ ) Sei  $f = X^p - 1$ , dann  $f(\zeta) = 0$  und

$$f = (X - 1)(X^{p-1} + \dots + X + 1)$$

ist irreduzible Zerlegung.

Da  $\zeta \neq 1$ , gilt  $\mu_{a,K} = X^{p-1} + \dots + X + 1$ .

Also  $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$ .

## 8E Algebraische Erweiterungen

**Definition 8.21.** Eine  $K$ -Algebra  $A$  heißt **algebraisch über  $K$** , falls  $A$  eine ganze  $K$ -Algebra ist. (d.h. jedes  $a \in A$  ist algebraisch über  $K$ ).

**Proposition 8.22.** Sei  $A$  eine  $K$ -Algebra. Dann sind äquivalent:

1.  $[A : K] < \infty$  (d.h.  $A$  ist endliche  $K$ -Algebra)
2.  $A$  ist algebraisch und endlich erzeugt  $K$ -Algebra.
3. Es gibt algebraische Elemente  $a_1, \dots, a_n \in A$ , sodass  $A = K[a_1, \dots, a_n]$

*Beweis.* Siehe 6.4 □

**Proposition 8.23.** Sei  $K \hookrightarrow L$  eine Körpererweiterung und  $L \hookrightarrow A$  ist  $L$ -Algebra, dann gilt:

$A$  ist algebraisch über  $K$  genau dann, wenn  $L$  algebraische Erweiterung von  $K$  und  $A$  algebraisch über  $L$ .

*Beweis.* Siehe 6.6 □

## 8F Algebraischer Abschluss

**Definition 8.24.** Ein Körper  $K$  heißt **algebraisch abgeschlossen**, falls die folgenden äquivalenten Bedingungen erfüllt sind:

1. Jedes Polynom  $f \in K[X]$  mit  $\deg(f) \geq 1$  besitzt eine Nullstelle in  $K$ .
2. Jedes Polynom  $f \in K[X]$  mit  $\deg(f) \geq 1$  ist Produkt von Polynomen vom Grad 1.
3. Jedes irreduzible Polynom in  $K[X]$  hat Grad 1.
4. Jede algebraische Körpererweiterung von  $K$  hat Grad 1.

*Beweis.* •  $1) \Leftrightarrow 2) \Leftrightarrow 3)$ .

- $3) \Rightarrow 4)$ : Sei  $K \hookrightarrow L$  algebraische Körpererweiterung,  $a \in L$ . Dann folgt aus 3), dass  $\mu_{a,K}$  Grad 1 hat, also  $\mu_{a,K} = X - a \in K[X]$ . Also  $a \in K$ .

- $4) \Rightarrow 3)$ : Sei  $f \in K[x]$  irreduzibel. Dann ist  $K[X]/(f)$  eine endliche Körpererweiterung mit  $[K[X]/(f) : K] = \deg(f)$ . Es folgt mit 4), dass  $\deg(f) = 1$ . □

*Beispiel 8.25.*  $\mathbb{C}$  ist Algebraisch abgeschlossen.

**Definition 8.26.** Sei  $K$  Körper. Eine Algebraische Erweiterung  $K \hookrightarrow \bar{K}$  heißt **algebraischer Abschluss von  $K$** , wenn  $\bar{K}$  abgeschlossen ist.

*Beispiel.* 1.  $\mathbb{R} \hookrightarrow \mathbb{C}$  ist algebraischer Abschluss.

2.  $\mathbb{Q} \hookrightarrow \mathbb{C}$  ist kein algebraischer Abschluss.

**Theorem 8.27.** Sei  $K$  Körper.

Dann existiert ein algebraischer Abschluss von  $K$ .

## 8G Fortsetzung von Körperhomomorphismen

*Bemerkung 8.28.* Seien  $K \hookrightarrow A_1, K \hookrightarrow A_2$   $K$ -Algebren und sei

$$\text{Hom}_{K\text{-Alg}}(A_1 A_2) = \{\varphi : A_1 \rightarrow A_2 \mid \varphi \text{ ist } K\text{-Algebra-Homomorphismus}\}$$

Jedes  $\varphi \in \text{Hom}_{K\text{-Algebra}}$  ist  $K$ -linear.

Falls  $A - 1 = L$  ein Körper,  $A_2 \neq 0$ , dann ist  $\varphi$  injektiv und es gilt

1.  $[L : K] \leq [A_2 : K]$
2. Falls  $[L : K] = [A_2 : K] \leq \infty$ , dann ist  $\varphi$  ein Homomorphismus von  $K$ -Algebren.

**Satz 8.29.** Sei  $K \hookrightarrow L$  und  $K \hookrightarrow L'$  Körpererweiterungen. Sei  $a \in L$  algebraisch über  $K$ .

1. Sei  $\varphi : K[a] \rightarrow L'$  ein  $K$ -Algebra-Homomorphismus.  
Dann ist  $\varphi(a) \in L'$  algebraisch und  $\mu_{\varphi(a), K} = \mu_{a, K}$ .
2. Es gibt die Bijektion

$$\begin{aligned} \text{Inhalt } \text{Hom}_{K\text{-Algebra}}(K[a], L') &\rightarrow \{a' \in L' \mid \mu_{a', K} = 0\} \\ \varphi &\mapsto \varphi(a) \end{aligned}$$

Insbesondere gilt

$$\deg(\mu_{a, K}) = [K[a] : K] \geq \# \text{Hom}_{K\text{-Algebra}}(K[a], L')$$

mit Gleichheit genau dann wenn  $\mu_{1, K}$  in  $L'$  vollständig in Linearfaktoren zerfällt und alle Nullstellen von  $\mu_{a, K}$  in  $L'$  paarweise verschieden sind.

*Beweis.* Sei  $\varphi : K[a] \rightarrow L'$  ein  $K$ -Algebra-Homomorphismus.

Dann ist  $\mu_{a, K} = 0$ , denn:

Sei  $\mu_{a, K} = X^{n-1} \lambda_{n-1} X^{n-1} + \dots + \lambda_0 \in K[X]$ .

$$\begin{aligned} \mu_{a, K}(\varphi(a)) &= \varphi(a)^n + \lambda_{n-1} \varphi(a)^{n-1} + \dots + \lambda_0 \\ &= \varphi(a^n) + \varphi(\lambda_{n-1} a^{n-1}) + \dots + \lambda_0 \\ &= \varphi(a^n + \lambda_{n-1} a^{n-1} + \dots + \lambda_0) \\ &= \varphi(0) = 0 \end{aligned}$$

Also ist  $\varphi(a)$  algebraisch und  $\mu_{\varphi(a), K}$  teilt  $\mu_{a, K}$ .

Da  $\mu_{a, K}$  irreduzibel ist folgt, dass  $\mu_{\varphi(a), K} = \mu_{a, K}$ .

Dies zeugt (1) und dass die Abbildung  $\varphi \mapsto \varphi(a)$  in (2) wohldefiniert ist.

Sei  $a' \in L'$  mit  $\mu_{a', K}(a) = 0$ , dann teilt  $\mu_{a', K}$  das Polynom  $\mu_{a, K}$ , also  $\mu_{a', K} \mu_{a, K}$ .

$$K[a] = \text{Ker}[X]/(\mu_{a, K}) = K[X]/(\mu_{a', K}) = K[a'] \subseteq L$$

stellen  $K$ -Algebra Homomorphismen  $\varphi : K[a] \rightarrow L'$  mit  $\varphi(a) = a'$  dar.

$\varphi$  ist eindeutig, da die  $K$ -Algebra  $K[a]$  durch  $a$  erzeugt wird.  $\square$

**Satz 8.30.** Sei  $K \hookrightarrow L$  eine algebraische Erweiterung und sie  $L'$  eine algebraische abgeschlossene Erweiterung von  $K$ .

1. Dass existiert ein  $K$ -Algebra-Homomorphismus  $\varphi : L \hookrightarrow L'$ .
2. Falls  $L$  und  $L'$  algebraisch Abschlüssen von  $K$  sind, ist  $\varphi$  ein Homomorphismus.

**Korollar 8.31.** Sei  $\overline{K}$  und  $\overline{K}'$  algebraische Abschlüsse von  $K$ . Dann existiert ein  $K$ -Algebra-Homomorphismus  $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$ .

*Beweis.* Sei  $\mathfrak{F} := \{(Z, \tau) \mid K \hookrightarrow Z \subseteq L \text{ Teilkörper und } \tau : Z \hookrightarrow L' \text{ K-Algebra-Homomorphismen}\}$ . Für  $(Z, \tau), (Z', \tau')$  schreibe

$$(Z, \tau) \leq (Z', \tau') :\Leftrightarrow Z \subset Z', \tau = \tau'|_Z$$

Also ist  $\leq$  eine partielle Ordnung auf  $\mathfrak{F}$ .

Und da  $(K, K \hookrightarrow L') \in \mathfrak{F}$  gilt  $\mathfrak{F} \neq \emptyset$ .

Sei nun  $\xi \subseteq \mathfrak{F}$  eine total geordnete Teilmenge, dass ist

$$\left( \bigcup_{(Z, \tau_Z) \in \xi} Z, \tau \right)$$

mit  $\tau|_Z = \tau_Z$  für alle  $(Z, \tau_Z) \in \xi$  eine obere Schranke in  $\mathfrak{F}$ .

Mit 1.4 folgt, dass es ein maximales Element  $(Z_0, \tau_0) \in \mathfrak{F}$  gibt.

Behauptung:  $Z_0 = L$  (setze dann  $\varphi := \tau_0$ )

Angenommenes existiert ein  $a \in L \setminus Z_0$ . Dann ist  $a$  algebraisch über  $Z_0$  und

$$\text{Hom}_{Z_0}(Z_0[a], L') \xrightarrow{\neq} \{a' \in L' \mid \mu_{a, Z_0}(a') = 0\} \neq \emptyset$$

Also existiert ...

□

## 9 Normale und separable Körpererweiterungen

### 9A Zerfällungskörper

**Definition 9.1.** Sei  $\mathfrak{F} \subseteq K[x]$  eine Menge nicht konstanter Polynome. Eine Körpererweiterung  $K \hookrightarrow L$  heißt **Zerfällungskörper** von  $\mathfrak{F}$ , falls gilt

1. Jedes  $f \in \mathfrak{F}$  zerfällt über  $L$  vollständig in Linearfaktoren
2. Für  $f \in \mathfrak{F}$  sei  $R_f := \{a \in L \mid f(a) = 0\}$ . Dann ist

$$L = K \left( \bigcup_{f \in \mathfrak{F}} R_f \right)$$

*Bemerkung.* Dann ist  $L = K \left[ \bigcup_{f \in \mathfrak{F}} R_f \right]$  eine algebraische Erweiterung von  $K$ .

*Beispiel 9.2.* Sei  $f \in K[X]$ ,  $\deg(f) \geq 1$  und Sei  $\overline{K}$  ein algebraischer Abschluss von  $K$ .

Seien  $a_1, \dots, a_n \in \overline{K}$  die Nullstellen von  $F$ .

Dann ist  $K[a_1, \dots, a_n] \subseteq \overline{K}$  ein Zerfällungskörper von  $f$ .



**Proposition 9.3.** Sei  $\mathfrak{F} \subseteq K[X]$  eine Menge nicht konstanter Polynome.

1. Dann existiert ein Zerfällungskörper von  $\mathfrak{F}$ .
2. Seien  $L_1$  und  $L_2$  Zerfällungskörper von  $\mathfrak{F}$ , seien  $\bar{L}_1$  und  $\bar{L}_2$  algebraische Abschlüsse von  $L_1$  bzw  $L_2$  und sei  $\varphi : \text{ol} L_1 \rightarrow \bar{L}_2$  ein  $K$ -Algebra-Homomorphismus. Dann ist  $\varphi(L_1) = L_2$ .

*Beweis.* 1. Sei  $\bar{K}$  ein algebraischer Abschluss und sei  $S := \{a \in \bar{K} \mid \exists f \in \mathfrak{F} : f(a) = 0\}$ .

Dann ist  $K(S)$  Zerfällungskörper von  $\mathfrak{F}$ .

2. Seien  $\bar{L}_1$  und  $\bar{L}_2$  bereits algebraische Abschlüsse von  $K$ .

Dann folgt 8.30, dass  $\varphi$  Homomorphismus ist.

Sei  $S_1 := \{a \in L_1 \mid \exists f \in \mathfrak{F} : f(a) = 0\}$ .

Es folgt, dass  $L_1 = K(S_1)$ .

Zeige:  $\varphi(S_1) \subseteq L_2$ . Sei:  $f \in \mathfrak{F}$ ,  $a \in L_1$  Nullstelle von  $f$ .

Dann ist  $f(\varphi(a)) = \varphi(f(a)) = 0$ . Also  $\varphi(a) \in \bar{L}_2$ , also Nullstelle von  $f$  ist.

Es folgt  $\varphi(a) \in L_2$ .

Also folgt  $\varphi(S_1) \subseteq L_2$ , dann ist  $\varphi(L_1) \subseteq L_2$ .

Analog für  $\varphi^{-1} : \varphi^{-1}(L_2) \subseteq L_1$ .

Zusammen folgt, dass  $\varphi(L_1) = L_2$ .

□

**Korollar 9.4.** Sei  $\mathfrak{F} \subseteq K[X]$  eine Menge nicht konstanter Polynome, sei  $\Omega$  Körpererweiterung von  $K$  und seien  $L_1, L_2 \subseteq \Omega$  Zerfällungskörper von  $\mathfrak{F}$ . Dann ist  $L_1 = L_2$ .

*Beweis.* Übergang zu einem algebraischen Abschluss von  $\Omega$ :

Sei  $\bar{\Omega}$  ein algebraischer Abschluss.

Dann folgt aus  $L_1, L_2$  ist algebraisch über  $K$ , dass  $L_1, L_2 \subseteq \{q \in \bar{\Omega} \mid q \text{ algebraisch über } K\}$ .

Also ist  $\bar{\Omega}$  algebraischer Abschluss von  $K$ .

Dann ist  $\bar{\Omega}$  algebraischer Abschluss von  $L_1$  und von  $L_2$ .

Wende nun 9.3 an auf  $\bar{L}_1 = \bar{L}_2 \bar{\Omega}$  und  $\varphi = \text{id}_{\bar{\Omega}}$

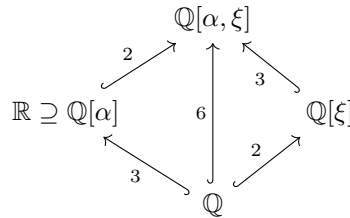
□

*Beispiel 9.5.* Sei  $p \in \mathbb{N}$  Primzahl, sei  $f = X^3 - p$ . (Es folgt  $f$  ist irreduzibel über  $K = \mathbb{Q}$ ) und sei  $\alpha = \sqrt[3]{p} \in \mathbb{R}_{>0}$ .

Sei  $\zeta := e^{\frac{2\pi i}{3}}$ . Dann sind  $\alpha, \zeta\alpha, \zeta^2\alpha \in \mathbb{C}$  die Nullstellen von  $f$ .

Der Zerfällungskörper von  $f$  ist

$$\mathbb{Q}[\alpha, \zeta\alpha\zeta^2\alpha] = \mathbb{Q}[\alpha, \zeta]$$



## 9B Normale Erweiterungen

**Definition 9.6.** Eine algebraische Körpererweiterung  $K \hookrightarrow L$  heißt **normal**, falls eine der folgenden äquivalenten Bedingungen erfüllt ist

1. Es existiert eine Menge  $\mathfrak{F} \subseteq K[X]$  mit konstanten Polynomen, sodass  $L$  der Zerfällungskörper von  $\mathfrak{F}$  in  $A$  ist.
2. Sei  $f \in K[X]$  irreduzibel mit Nullstelle in  $L$ , dann zerfällt  $f$  in  $L[X]$  vollständig in Linearfaktoren.
3. Für jede Körpererweiterung  $L'$  von  $L$  und für jeden  $K$ -Algebra-Homomorphismus  $\varphi : L \hookrightarrow L'$  gilt  $\varphi(L) = L$ .
4. Für jeden algebraischen Abschluss  $\Omega$  von  $L$  und für jeden  $K$ -Algebra-Automorphismus  $\varphi : \Omega \rightarrow \Omega$  gilt  $\varphi(L) = L$ .

*Beweis.* • 1) $\Rightarrow$ 2): Sei  $L$  Zerfällungskörper von  $\mathfrak{F}$ , dann folgt  $\varphi(L)$  ist zerfällungskörper von  $\mathfrak{F}$ . Dann folgt mit ??, dass  $\varphi(L) = L$ .

- 3) $\Rightarrow$ 4): Sei  $\varphi : \Omega \xrightarrow{\sim} \Omega$  ein  $K$ -Algebra-Automorphismus. Wende 3) auf  $\varphi|_L : L \rightarrow \Omega$  an.

- Sei OE  $L'$  algebraisch abgeschlossen. Ersetze  $L'$  durch

$$L'_{\text{alg}} := \{a \in L' \mid a \text{ ist algebraisch über } K\}$$

Da  $K \subseteq L$  algebraisch ist, folgt, dass  $\varphi(L) \subseteq L'_{\text{alg}}$ . Also ist OE  $L'$  algebraischer Abschluss von  $L$ .

Aus 8.30 folgt die Existenz einer Fortsetzung  $\varphi' : L' \rightarrow L'$  zu  $\varphi$  und  $\varphi'$  ist Automorphismus.

Also  $\varphi(L) = \varphi'(L) = L$ .

- 3) $\Rightarrow$ 2): Sei  $f \in K[X]$  irreduzibel,  $a \in L$  mit  $f(a) = 0$ . Sei  $L'$  ein algebraischer Abschluss von  $L$ ,  $b \in L'$  mit  $f(b) = 0$ . Zu Zeigen: auch  $b \in L$ . Sei OE  $f$  normiert. Dann  $f = \mu_{a,K}$ . Also existiert ein eindeutiger  $K$ -Algebra-Homomorphismus  $\bar{\varphi} : K[a] \rightarrow L'$  mit  $\bar{\varphi}(a) = b$ . Setze nun  $\bar{\varphi}$  fort mit  $\varphi : L \rightarrow L'$  (Existenz durch 8.30). Dann folgt durch 3), dass  $\varphi(L) = L$ , also  $\varphi(a) = b \in L$ .
- Sei  $S \subseteq L$  Teilmenge und  $L = K(S)$ . Sei  $\mathfrak{F} := \{\mu_{a,K} \mid a \in S\}$ . Aus 2) folgt, dass  $\mu_{a,K}$  über  $L$  für alle  $a \in S$  in Linearfaktoren zerfällt. Sei  $S' := \{b \in L \mid \exists f \in \mathfrak{F} : f(b) = 0\} \supseteq S$ . Dann ist  $K(s) = L$ ,  $K(s) \subseteq K(s') \subseteq L$ . Also  $L = K(s')$ , d.h.  $L$  ist Zerfällungskörper von  $\bar{f}$ .

□

*Beispiel.* Sei  $L = K[a]$  normal, dann ist  $L$  Zerfällungskörper von  $\mu_{a,K}$ .

**Proposition 9.7.** Sei  $K \hookrightarrow L$  eine normale Körpererweiterung. Sei  $M \subseteq L$  Teilkörpererweiterung.

1. Jeder  $K$ -Algebra-Homomorphismus  $\varphi : M \hookrightarrow L$  kann in einem  $K$ -Algebra-Automorphismus  $\bar{\varphi} : L \xrightarrow{\sim} L$  fortgesetzt werden.
2.  $K \hookrightarrow M$  ist genau dann normal, wenn für jeden  $K$ -Automorphismus  $\sigma : L \xrightarrow{\sim} L$  gilt  $\sigma(M) = M$ .

*Beweis.* 1. Betrachte  $\varphi' : M \hookrightarrow L \hookrightarrow L'$  und  $L'$  ist algebraischer Abschluss von  $L$ .

Dann gibt 8.30 die Existenz einer Fortsetzung  $\bar{\varphi}' : L' \xrightarrow{\sim} L'$ , die  $K$ -Algebra-Automorphismus ist.

Dann folgt mit 9.6.3, dass  $\bar{\varphi}' = L$ , sodass  $\bar{\varphi} = \overline{\varphi'}|_L$  ein  $K$ -Algebra-Automorphismus von  $L$  ist.

2. " $\Rightarrow$ " ist durch 9.6.3 gegeben. " $\Leftarrow$ " Sei  $L'$  algebraischer Abschluss von  $L$ ,  $\bar{\sigma} : L' \xrightarrow{\sim} L'$  Fortsetzung von  $\sigma$  und jeder Automorphismus von  $L$  ist Einschränkung eines Automorphismus von  $L'$ . Also gilt  $\bar{\sigma}(M) = M$  für alle  $\bar{\sigma} \in \text{Aut}_{K\text{-Algebra}}(L')$ . Dann folgt mit 9.6.3, dass  $K \hookrightarrow M$  normal ist. □

*Beispiel 9.8.* 1. Sei  $\varphi : K \hookrightarrow L$  Körpererweiterung mit  $[L : K] = 2$ . Dann ist  $\varphi$  normal.

*Beweis.* Sei  $f \in K[X]$  irreduzibel,  $a \in L$  mit  $f(a) = 0$ . Dann ist  $f = \mu_{a,K}$ , also  $\deg(\mu_{a,K}) = [K[a] : K] \leq 2$ . Wenn  $\deg(\mu_{a,K}) = 1$ , dann  $\mu_{a,K} = X - a$  mit  $a \in K$ .

Wenn  $\deg(\mu_{a,K}) = 2$  genau dann gilt  $a \in L \setminus K$ . Dann ist  $\mu_{a,K} = (X - a)g$  mit  $g \in L[X]$  vom Grad 1, also  $g = X - b \in L[X]$ .

Also sind die Nullstellen von  $\mu_{a,K}$  beide in  $L$ .

Dann folgt mit 9.6.3, dass  $K \hookrightarrow L$  normal ist. □

2. Sei  $K \hookrightarrow \bar{K}$  ein algebraischer Abschluss. Dann ist  $K \hookrightarrow \bar{K}$  eine normale Erweiterung.  
(z.B. ist  $\bar{K}$  Zerfällungskörper von  $\{f \in K[x] \mid f \text{ nicht konstant}\}$ ).
3.  $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{7}]$  ist nicht normal.  
Denn  $X^3 - 7$  hat Nullstelle in  $\mathbb{Q}[\sqrt[3]{7}]$ , aber nicht jede Nullstelle von  $X^3 - 7$  liegt in  $\mathbb{Q}[\sqrt[3]{7}]$ :

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{7}] \subset \mathbb{Q}[\sqrt[3]{7}, \zeta]$$

für  $\zeta = e^{\frac{2\pi i}{3}}$ .

*Bemerkung 9.9.* Seien  $K \hookrightarrow L \hookrightarrow M$  Körpererweiterungen.

1. Wenn  $K \hookrightarrow M$  normal ist, dann ist  $L \hookrightarrow M$  normal.  
( $M$  ist Zerfällungskörper von  $\mathfrak{F} \subseteq K[X] \subseteq L[X]$ ).
2. Aus  $K \hookrightarrow M$  normal folgt i.A. **nicht**, dass  $K \hookrightarrow L$  normal ist mit ??3.
3. Aus  $K \hookrightarrow L$ ,  $L \hookrightarrow M$  normal folgt i.A. **nicht**, dass  $K \hookrightarrow M$  normal.

## 9C Separabilitätsgrad

**Proposition 9.10.** Sei  $A$  ein Ring, sei  $E \neq 0$  ein freier  $A$ -Modul. Dann ist die Sequenz  $0 \rightarrow M' \rightarrow M'' \rightarrow 0$  von  $A$ -Moduln genau dann exakt, wenn

$$0 \rightarrow E \otimes_A M' \rightarrow E \otimes_A M'' \rightarrow E \otimes_A M''/E \otimes_A M' \rightarrow 0$$

exakt ist.

(Insbesondere  $E \otimes_A M = 0 \Leftrightarrow M = 0$ )

*Beweis.*  $E$  ist genau dann frei, wenn  $E \cong A^{(I)}$  mit  $I \neq \emptyset$ .

Man erhält insbesondere die Isomorphismen

$$\begin{array}{ccccccc} 0 & \longrightarrow & E \otimes_A M' & \xrightarrow{\text{id}_E \otimes u} & E \otimes_A M & \xrightarrow{\text{id}_E \otimes v} & E \otimes_A M'' \longrightarrow 0 \\ & & \downarrow \sim & & \downarrow \sim & & \downarrow \sim \\ 0 & \longrightarrow & (M')^{(I)} & \xrightarrow{(u(m'_i))_{i \in I}} & M^{(I)} & \xrightarrow{(v(m''_i))_{i \in I}} & M''^{(I)} \longrightarrow 0 \end{array}$$

Es folgt die Behauptung.  $\square$

*Bemerkung 9.11.* Sei  $A$  eine endliche  $K$ -Algebra. Dann folgt mit ??, dass  $A = \prod_{i=1}^r A/m_i e_i$ , mit  $m_1, \dots, m_r \subset A$  maximale Ideale.

Sei  $B$  eine nullteilerfreie  $K$ -Algebra, sei  $\varphi : A \rightarrow B$  ein  $K$ -Algebra-Homomorphismus.

Dann ist  $\varphi(A) \subseteq B$  nullteilerfrei, oder  $\text{Ker}(\varphi) = m_i$  für ein  $i \in \{1, \dots, r\}$ .

Also faktorisiert  $\varphi$  in  $A \rightarrow A/m_i \hookrightarrow B$ . Insbesondere:

$$\text{Hom}_{K\text{-Algebra}}(A, B) = \bigcup_{i=1}^r \text{Hom}_{K\text{-Algebra}}(A/m_i, B)$$

*Bemerkung 9.12.* Sei  $K \hookrightarrow A$  eine  $K$ -Algebra,  $K \hookrightarrow L$  eine Körpererweiterung,  $L \hookrightarrow B$  ein  $L$ -Algebra. Dann hat man zueinander inverse Bijektionen:

$$\begin{array}{ccc} \text{Hom}_{K\text{-Algebra}}(A, B) & \xleftrightarrow{1:1} & \text{Hom}_{L\text{-Algebra}}(L \otimes_K A, B) \\ \varphi & \mapsto & (l \otimes a \mapsto l\varphi(a)) \\ (a \mapsto \varphi(1 \otimes a)) & \xleftarrow{\quad} & \varphi \end{array}$$

*Bemerkung 9.15.* Sei  $A$  algebraische  $K$ -Algebra,  $K \hookrightarrow L$  Körpererweiterung. Dann

$$[A \otimes_K L : L]_S = [A : K]_S$$

*Beweis.* Sei  $\Omega$  eine algebraisch abgeschlossene Erweiterung von  $L$ . Dann gibt es die Bijektion

$$\begin{array}{ccc} \text{Hom}_{K\text{-Algebra}} & \xleftrightarrow{1:1} & \text{Hom}_L(A \otimes_K L, \Omega) \\ \sigma \mapsto (a \otimes l \mapsto l\sigma(a)) & & \\ a \mapsto \tau(a \otimes 1) \xleftarrow{\quad} \tau & & \end{array}$$

$\square$

**Lemma 9.16.** Sei  $A$  eine endliche  $K$ -Algebra. Dann ist  $(A : K)_S$  die Anzahl der maximalen Ideale von  $A \otimes_K \Omega$ . ( $\Omega$  als algebraisch abgeschlossene Erweiterung von  $K$ )

*Beweis.* Mit 9.15 folgt, dass OE  $\Omega = K$ .

Seien  $m_1, \dots, m_r \subset A$  die maximalen Ideal. Dann ist  $A/m_i$  eine endliche Körpererweiterung von  $\Omega$ , also  $A/m_i = \Omega$ .

Dann folgt mit 9.11, dass

$$\# \text{Hom}_{\Omega\text{-Algebra}}(A, \Omega) = \# \bigcup_{i=1}^r \text{Hom}_{\Omega\text{-Algebra}}(\underbrace{A/m_i}_{=\Omega}, \Omega) = r$$

□

**Proposition 9.17.** Sei  $a$  endliche  $K$ -Algebra. Dann gilt

$$[A : K]_S \leq [A : K] (= \dim_K(A))$$

*Beweis.* Sei OE  $K = \Omega$  algebraisch abgeschlossen. Sei  $A = \prod_{i=1}^r A/m_i e_i$ . Also

$$\begin{aligned} [A : K]_S &\stackrel{9.16}{=} r = \sum_{i=1}^r \dim_K(\underbrace{A/m_i}_{=K}) \\ &\leq \sum_{i=1}^r \dim_K(A/m_i e_i) = [A : K] \end{aligned}$$

□

*Bemerkung 9.18.* Der Beweis von 9.17 zeigt  $[A : K]_S = [A : K] \Leftrightarrow A \otimes_K \Omega$  ist reduziert  $\Leftrightarrow A \otimes_K \Omega \cong \Omega \times \dots \times \Omega$  ( $r = [A : K]$  mal).

**Proposition 9.19.** Sei  $K \hookrightarrow L$  algebraische Körpererweiterung,  $A$  ganze  $L$ -Algebra.

Dann ist

$$[A : K]_S = [A : L]_S \cdot [L : K]_S$$

*Beweis.* Sie  $\Omega$  ein algebraischer Abschluss in  $L$ . Betrachte

$$\rho : \text{Hom}_{K\text{-Algebra}}(A; \Omega) \rightarrow \text{Hom}_{K\text{-Alg}}(L, \omega), \quad \sigma \mapsto \sigma|_L$$

$\rho$  ist surjektiv (8.30). Sei  $\varphi : L \hookrightarrow \Omega$  ein  $K$ -Algebra-Homomorphismus. Dann ist

$$\begin{aligned} \rho^{-1}(\{\varphi\}) &= \{\sigma \in \text{Hom}_{K\text{-Algebra}}(A, \Omega) \mid \sigma|_L = \varphi\} \\ &= \text{Hom}_{L\text{-Algebra}}(A, \Omega) \end{aligned}$$

wobei  $\Omega$  von  $\varphi$  als  $L$ -Algebra aufgefasst wird.

Also

$$\begin{aligned} [A : K]_S &= \# \text{Hom}_{K\text{-Alg}}(A, \Omega) \\ &= \sum_{\varphi \in \text{Hom}_{K\text{-Alg}}(L, \Omega)} \# \rho^{-1}(\{\varphi\}) \\ &= \sum_{\varphi} [A : L]_S \\ &= [L : K]_S [A : L]_S \end{aligned}$$

□

## 9D Separable Polynome

**Definition 9.20.** Sei  $f = a_n X^n + \dots + a_1 X + a_0 \in A[X]$ .

Definiere

$$f' := na_n X^{n-1} + (n-1)a_{n-1} X^{n-2} + \dots + 2a_2 X + a_1$$

$f'$  heißt die (formale) **Ableitung** von  $f$ .

*Bemerkung.* Seien  $f, g \in A[X]$  und  $a, b \in A$ .

- Die Ableitung ist Linear:  $(af + bg)' = af' + bg'$
- Es gilt die Leibnitz-Regel  $(fg)' = fg' + f'g$

*Beweis.* • Linearität. klar.

- Aus der Linearität können wir OE annehmen, dass  $f = X^i, g = X^j$ .  
Dann

$$(fg)' = (X^{i+j})' = (i+j)X^{i+j-1} = iX^{i-1}X^j + jX^iX^{j-1} = fg' + f'g$$

□

*Beispiel.* Sei  $\dim(K) = p > 0$ . Dann folgt aus  $f = X^p + 1$ , dass  $f' = pX^{p-1} = 0$ .

**Definition 9.21.** Sei  $f \in K[X]$ ,  $a \in K$ . Dann ist

$$\text{Ord}_a(f) := \sup\{n \geq 0 \mid (X-a)^n \text{ teilt } f\}$$

die **Ordnung der Nullstelle**  $a$  von  $f$ .

*Bemerkung 9.21.* •  $\text{Ord}_a(f) = \infty \Leftrightarrow f = 0$ .

- $\text{Ord}_a(f) = 0 \Leftrightarrow f(a) \neq 0$ .
- $\text{Ord}_a(f) = 1 \Leftrightarrow f(a) = 0$  und  $f'(a) \neq 0$ .

*Beweis.*  $\text{Ord}_a(f) = 1$  genau dann wenn  $f = (X-a)g$  mit  $g(a) \neq 0$ .  
 $\Leftrightarrow f(a) = 0$  und  $f'(a) = g(a) + g'(a)(a-a) = g(a) \neq 0$ .

□

**Definition 9.22.** Ein Polynom  $f \in K[X]$ ,  $f \neq 0$  heißt **separabel**, falls alle Nullstellen in einem Zerfällungskörper paarweise verschieden sind.

**Proposition 9.23.** Sei  $\Omega$  eine algebraisch abgeschlossen Erweiterung von  $K$ ,  $f \in K[X]$ ,  $f \neq 0$ . Dann sind äquivalent:

1.  $f$  ist separabel
2. Alle Nullstellen von  $f$  in  $\Omega$  sind verschieden
3.  $f$  und  $f'$  haben in  $\Omega$  keine gemeinsame Nullstelle.
4.  $f$  und  $f'$  sind in  $K[X]$  teilerfremd

*Beweis.* (1)  $\Leftrightarrow$  (2) Sei  $L$  ein Zerfällungskörper von  $f$ . Dann existiert (8.30) eine eindeutige Körpererweiterung  $L \hookrightarrow \Omega$ .

(ii)  $\Leftrightarrow$  (iii) aus 9.21

(iii)  $\Leftrightarrow$  (iv)  $f$  und  $f'$  zerfallen in  $\Omega[X]$  in Linearfaktoren.

Also ist (iii) äquivalent dazu, dass  $f$  und  $f'$  sind in  $\Omega[X]$  teilerfremd sind.

Ist äquivalent  $\Omega \otimes_K K[X]/(f, f') \cong \Omega[X]/(f, f') = 0$ .

?? gibt uns dann die Äquivalenz zu  $K[X]/(f, f') = 0$ , genau dann wenn  $f, f'$  auch teilerfremd in  $K[X]$  sind.

□

*Beispiel.* 1.  $(X^3 - 2)(X - 1) \in \mathbb{Q}[X]$  ist separabel

2. Sei  $K = \text{Quot}(\mathbb{F}_p[T])$  und  $f = X^p - T \in K[X]$  ist nach dem Eisensteinkriterium mit  $p = T$  irreduzibel.

Aber  $f$  ist nicht separabel:

Im Zerfällungskörper  $K[\sqrt[p]{T}]$  gilt  $f = (X - \sqrt[p]{T})^p$ .

Äquivalent:  $f$  ist nicht teilerfremd zu  $f' = pX^{p-1} = 0$ .

**Satz 9.24.** Sei  $f \in K[X]$  irreduzibel. Dann gilt

1.  $f$  ist separabel genau dann wenn  $f' \neq 0$ .

2. Sei  $\text{char}(K) = 0$ . Dann ist  $f$  separabel.

*Beweis.* 1. Sei  $f' = 0$ , dann sind  $f'$  und  $f$  zueinander teilerfremd und somit (9.23)  $f$  separabel.

2. Sei  $\text{char}(K) = 0$ , dann  $\deg(f') = \deg(f) - 1$ , also  $\deg(f') \geq 0$ .

Also ist  $f \neq 0$ , sodass (1)  $f$  separabel ist.

□

## 9E Separable Algebren

**Definition 9.25.** Eine algebraisch  $K$ -Algebra  $A$ .

Ein  $a \in A$  heißt **separabel**, falls  $\mu_{a,K}$  separabel ist.

$A$  heißt **separabel**, falls jedes  $a \in A$  separabel ist.

**Theorem 9.26.** Sei  $A$  eine endliche  $K$ -Algebra und sei  $\Omega$  eine algebraisch abgeschlossen Erweiterung von  $K$ .

Dann sind äquivalent:

1.  $A$  ist separable  $K$ -Algebra

2.  $[A : K]_S = [A : K]$

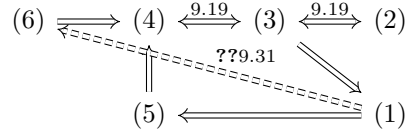
3.  $A \otimes_K \Omega$  ist reduziert.

4.  $A \otimes_K \Omega \cong \Omega^r$  also  $\Omega$ -Algebra.

5. Es existieren  $a_1, \dots, a_n \in A$  separabel, sodass  $A = K[a_1, \dots, a_n]$

6. Es existiert  $a \in A$  separabel, sodass  $A = K[a]$ .

*Beweis.* Zeige:



**(3)⇒(1)** Sei  $a \in A$ . (Zz.  $a$  ist separabel)

Dann ist  $K[a] = K[X]/\mu_{a,K} \hookrightarrow A$ .

Dass ist  $\Omega \otimes_K K[a] \hookrightarrow \Omega \otimes_K A$  injektiv.

Dann ist (mit (3))  $\Omega \otimes_K K[a] = \Omega[X]/(\mu_{a,K})$  ist reduziert.

Mit ?? folgt, dass alle Nullstellen von  $\mu_{a,K}$  in  $\Omega$  verschieden sind. Also ist  $\mu_{a,K}$  separabel, also auch  $a$ .

**(1)⇒(5)** klar

**(6)⇒(4)** Es gelte (6), dann ist  $A = K[X]/(\mu_{a,K})$ .

Dann ist

$$A \otimes_K \Omega = \Omega[X]/(\mu_{a,K}) \cong \prod \Omega[X]/(X - \alpha_i) = \prod \Omega$$

Da  $\mu_{a,K}$  in  $\Omega$  in Linearfaktoren zerfällt.

**(5)⇒(4)** Seien  $a_1, \dots, a_n \in A$ . Wir verwenden (6)⇒(4). Also gilt  $K[a_i] \otimes_{\Omega} \cong \Omega^{d_i}$  und  $\mu_{a,K} = \prod (x - a_i)$ .

Dann gilt, dass

$$\begin{aligned}
(K[a_1]) \otimes_K \dots \otimes_K K[a_n] \otimes_{\Omega} \Omega &= (K[a_1] \otimes_K \Omega) \otimes_K \dots \otimes_K (K[a_n] \otimes_K \Omega) \\
&\cong \Omega^{d_1} \otimes_{\Omega} \Omega^{d_2} \otimes_{\Omega} \dots \otimes_{\Omega} \Omega \\
&= \Omega^{d_1 \dots d_n}
\end{aligned}$$

Wähle nun

$$\begin{aligned}
\varphi : K[a_1] \otimes_K \dots \otimes_K K[a_n] &\rightarrow K[a_1, \dots, a_n] \\
x_1 \otimes \dots \otimes x_n &\mapsto x_1 \cdot \dots \cdot x_n
\end{aligned}$$

Dann ist  $\varphi$  surjektiver  $K$ -Algebra-Homomorphismus.

Es folgt, dass  $A \otimes_K \Omega$  Quotient der  $\Omega$ -Algebra  $\Omega^{d_1 \dots d_n}$  und damit  $A \otimes_K \Omega \cong \Omega^m$ ,  $m \leq d_1 \cdot \dots \cdot d_n$

□

**Definition 9.27.** Ein Körper  $K$  heißt **perfekt** wenn  $\text{char}(K) = 0$  ist oder  $\text{char}(K) = p > 0$  und  $x \mapsto x^p$  surjektiv ist.

**Satz 9.27.** Sei  $K$  perfekt. Dann ist jede endliche Körpererweiterung separabel

*Beweis.* Sei  $K \hookrightarrow L$  eine endliche Körpererweiterung,  $a \in L$ . Zz.  $\mu_{a,K}$  ist separabel.

Wir wissen  $\mu_{a,K}$  ist irreduzibel und (9.24) falls  $\text{char}(K) = 0$  auch separabel.

Sei nun  $\text{char}(K) = p > 0$ . Zz.  $\mu_{a,K} \neq 0$ .

Sei  $\mu_{a,K} = X^n + a_{n-1}X^{n-1} + \dots + a_0$ .

Angenommen  $\mu'_{a,K} = nX^n + (n-1)a_{n-1}X^{n-1} + \dots + a_1 = 0$  dann muss  $a_i = 0$  falls  $p$  nicht  $i$  teilt.



Dann ist  $\mu_{a,K} = X^{pk} + b_k X^{p(k-1)} + \dots + b_0$  mit  $b_j = a_{p \cdot j}$ .  
Wähle nun  $\beta_j^p = b_j$ .  
Dann ist

$$\mu_{a,K} = \sum_j \beta_j^p X^{pj} = \left( \sum_j \beta_j X^j \right)^p$$

Also ist  $\mu_{a,K}$  nicht irreduzibel. Widerspruch!  $\square$

*Beispiel 9.28.* Sei  $K = \text{Quot}(\mathbb{F}_1[T])$ .

Dann ist  $K(\sqrt[p]{T})$  eine nicht separable Erweiterung von  $K$ .

**Proposition 9.29.** Sei  $K \hookrightarrow L$  eine endliche Körpererweiterung,  $L \hookrightarrow A$  endliche  $L$ -Algebra,  $A \neq 0$ . Dann gilt:

$A$  ist genau dann separable  $K$ -Algebra, wenn  $A$  separabel  $L$ -Algebra und  $L$  separabel  $K$ -Algebra.

*Beweis.* Sei  $A$  separabel  $K$ -Algebra. Dies ist äquivalent (9.26) dazu, dass

$$[A : L][L : K] = [A : K] = [A : K]_S = [A : L]_S [L_K]_S$$

$\Leftrightarrow A$  ist separable  $L$ -Algebra und  $L$  ist separable  $K$ -Algebra.  $\square$

## 9F Satz vom primitiven Element

**Satz 9.30.** Sei  $G \subseteq (K^\times, \cdot)$  eine endliche Untergruppe.

Dann ist  $G$  zyklisch ( $\Leftrightarrow G \cong (\mathbb{Z}/n\mathbb{Z}, +)$ )

*Beweis.* Sei  $G$  endliche abelsche Gruppe.

Dann  $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$  mit  $1 < n_r$  und  $n_r | n_{r-1} | \dots | n_1$ .

Also gilt für jedes  $g \in G \subseteq K^\times$ , dass  $g$  Nullstelle von  $X^{n_1} - 1 \in K[X]$ , Also  $\#G \subset n_1$ , Also  $G \cong \mathbb{Z}/n_1\mathbb{Z}$ .  $\square$

**Definition 9.31.** Sei  $A$  eine endliche separable  $K$ -Algebra und sei  $a \in A$  mit  $A = K[a]$  dann heißt  $a$  **primitives Element**.

**Theorem 9.31** (Satz vom primitiven Element). Sei  $A$  eine endliche separable  $K$ -Algebra. Dann existiert ein primitives Element  $a \in A$ .

*Beweis.* Sei  $\Omega$  eine algebraisch abgeschlossen Erweiterung von  $K$  zu  $\text{Hom}_{K\text{-Algebra}}(A, \Omega) = \{\varphi_1, \dots, \varphi_m\}$ ,  $m = [A : K]_S = [A : K]$ .

1. Sei  $a \in A$ . Z.z.  $a$  ist primitives Element ist äquivalent  $\varphi_i(a) \neq \varphi_j(a)$  für alle  $i \neq j$ :

” $\Rightarrow$ ” ist klar, da  $a$  Erzeuger von  $A$  als  $K$ -Algebra ist.

” $\Leftarrow$ ” Seien  $\varphi_i(a) \neq \varphi_j(a)$  für alle  $i \neq j$ , dann sind auch  $\varphi_I|_{K[a]}$  paarweise verschieden.

Also gilt

$$m \leq [K[a] : K]_S \leq [A : K]_S = [A : K] = m$$

Daraus folgt, dass  $[K[a] : K] = [A : K]$  und damit  $A = K[a]$ .

2. Sei  $A$  endlich und separabel,  $\Leftrightarrow$  ( Übung )  $A \cong K_1 \times \dots \times K_d$  für endliche separable Erweiterungen  $K_i$  von  $K$ .  
Falls  $i = K[a_i]$ , so gilt  $A = K[a, \dots, a_d]$ .  
Als ist  $A = L$  endliche separable Körpererweiterung.
3. Sei  $K$  endlich. Dann ist  $L$  endlich, also  $L^\times = \{1 = a^0, a, a^2, \dots\}$  für  $a \in L^\times$  (9.30).  
Dann ist  $L = K[a]$ .
4. Sei nun  $K$  unendlich,  $L = [a_1, \dots, a_n]$ ,  $a_i \in L$  separabel.  
Wir beweisen durch Induktion nach  $n$ .  
 $n = 1$  Klar.  
 $n > 1$   $L = K[a_1, \dots, a_{n-1}][a_n] = K[b, a_n]$ . Also gilt  $OEL = K[b, c]$
5. Z.z. Sei  $N := \{\lambda \in K \mid \lambda b + c \text{ nicht primitiv}\}$ , dann ist  $\#N \leq \frac{m(m-1)}{2}$ .

$$\begin{aligned}
N &\stackrel{(1)}{=} \{\lambda \in K \mid \exists i < j : \varphi_i(\lambda b + c) = \varphi_j(\lambda b + c)\} \\
&= \bigcup_{1 \leq i < j \leq m} \underbrace{\{\lambda \in K \mid \lambda(\varphi_i(b) - \varphi_j(b)) + \varphi_i(c) - \varphi_j(c) = 0\}}_{\text{hat } \leq 1 \text{ Elemente, da } b, c \text{ } L \text{ erzeugen}}
\end{aligned}$$

Da  $K$  unendlich ist folgt die Behauptung

□

*Beispiel 9.31.* Sei  $L = \mathbb{Q}[\sqrt[3]{7}, \sqrt{5}]$ ,  $\varphi : L \rightarrow \mathbb{C}$ . (...)

## 10 Galois-Theorie

### 10A Galois-Erweiterungen

**Definition 10.1.** Eine algebraische Körpererweiterung  $K \hookrightarrow L$  heißt **Galois-Erweiterung** oder **galoisch**, falls sie normal und separabel ist.

**Definition 10.2.** Sei  $K \hookrightarrow L$  eine Körpererweiterung. Dann ist

$$\text{Aut}_{K\text{-Algebra}}(L) := \{\sigma : L \rightarrow L, \text{ bijektiver } K\text{-Algebra-Homomorphismen}\}$$

*Bemerkung.* Sei  $K \hookrightarrow L$  eine Körpererweiterung. Dann ist  $\text{Aut}_{K\text{-Algebra}}(L)$  eine Gruppe bezüglich der Komposition.

*Beispiel.* 1.  $\text{Aut}_{\mathbb{Q}\text{-Algebra}}(\mathbb{Q}[\sqrt{7}]) = \{\text{id}_{\mathbb{Q}[\sqrt{7}]}, a + b\sqrt{7} \mapsto a - b\sqrt{7}\}$

2.  $\text{Aut}_{\mathbb{Q}\text{-Algebra}}(\mathbb{Q}[\sqrt[3]{2}]) = \{\text{id}\}$

**Definition 10.2.** Sei  $K \hookrightarrow L$  eine Galois-Erweiterung. Dann heißt

$$\text{Gal}(L/K) := \text{Aut}_{K\text{-Algebra}}(L)$$

**Galoisgruppe** von  $K \hookrightarrow L$ .

**Definition 10.3.** Sei  $K \hookrightarrow L$  eine Körpererweiterung und sei  $H \subseteq \text{Aut}_{K\text{-Algebra}}(L)$  eine Untergruppe. Dann heißt

$$L^H := \{a \in L \mid \sigma(a) = a, \forall \sigma \in H\}$$

der **Fixkörper** von  $H$ .

Hier könnte Ihre Werbung die VL vom 16.01.2016 stehen

**Satz 10.4.** Sei  $K \hookrightarrow L$  eine endliche Galois-Erweiterung und  $M \subseteq L$  ein Zwischenkörper.

Dann ist  $K \hookrightarrow L$  normal  $\Leftrightarrow \text{Gal}(L/M) \subseteq \text{Gal}(L/K)$  ist Normalteiler.

In diesem Fall ist die Sequenz

$$1 \rightarrow \text{Gal}(L/M) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(M/K) \rightarrow 1$$

$$\sigma \mapsto \sigma|_M$$

*Beweis.* Sei  $\sigma \in \text{Gal}(L/K)$ ,  $H \subseteq \text{Gal}(L/K)$ . Dann ist

$$\begin{aligned} \sigma(L^H) &= \{\sigma(a) \mid a \in L^H\} \\ &= \{\sigma(a) \mid \forall \gamma \in H : \gamma(a) = a\} \\ &\stackrel{a'=\sigma(a)}{=} \{a' \in L \mid \forall \gamma \in H : \underbrace{\gamma(\sigma^{-1}(a')) = \sigma^{-1}(a'))}_{\Leftrightarrow \sigma(\gamma(\sigma^{-1}(a'))) = a'}\} \\ &= L^{\sigma H \sigma^{-1}} \end{aligned}$$

Sei  $M = L^H$ . Dann ist  $K \hookrightarrow L$  normal  $\stackrel{??}{\Leftrightarrow}$  für alle  $\sigma \in \text{Gal}(L/K)$  gilt  $L^{\sigma H \sigma^{-1}} \sigma(M) = M = L^H$ .

Da  $H \mapsto L^H$  injektiv ist, folgt

$$\begin{aligned} K \hookrightarrow M = L^H &\Leftrightarrow \forall \sigma \in \text{Gal}(L/K) : \sigma H \sigma^{-1} = H \\ &\Leftrightarrow H \subseteq \text{Gal}(L/K) \text{ Normalteiler} \end{aligned}$$

Dann folgt mit ??, dass  $\sigma \mapsto \sigma|_M$  ist surjektiv und  $\text{Ker}(\sigma \mapsto \sigma|_M) = \text{Gal}(L/M)$ . □

*Bemerkung 10.5.* Bestimmung von  $L^H$ : Sei  $K \hookrightarrow L$  eine endliche Galois-Erweiterung,  $H \subseteq \text{Gal}(L/K)$ .

1. Sei  $a \in L$ . Setze  $Z_a^H := \{\sigma(a) \mid \sigma \in H\} \subseteq L$ . Dann ist

$$\mu_{a, L^H} = \prod_{b \in Z_a^H} (X - b)$$

2. Sei  $a \in L$  mit  $L = K[a]$  und sei  $S \subseteq L^H$  die Menge der Koeffizienten von  $\mu_{a, L^H}$ .  
Dann ist  $L^H = K[S]$ .

*Beweis.* 1. Sei  $K \hookrightarrow L$  normal. Dann zerfällt  $\mu_{a,L^H}$  über  $L'$  vollständig in Linearfaktoren.

Die Nullstellen von  $\mu_{a,L^H}$  sind  $\{\sigma(a) \mid \sigma \in \text{Gal}(L/L^H) = H\}$ . Es folgt die Behauptung.

2. Es ist klar, dass  $K[S] \subseteq L^H$ .

Zusätzlich ist  $\mu_{a,L^H}$  irreduzibel in  $K[S][X]$ , also ist  $\mu_{a,L^H} = \mu_{a,K[S]}$ . Dann ist

$$\begin{aligned} [L : L^H] &\stackrel{L=K[a]}{=} [L^H[a] : L^H] = \deg \mu_{a,L^H} = \deg \mu_{a,K[S]} \\ &= [K[S][a] : K[S]] = [L : K[S]] \end{aligned}$$

Es folgt die Behauptung. □

*Beispiel 10.6.* Sei  $g = X^3 + a_2X^2 + a_1 + a_0 \in K[X]$  und  $\text{char}(K) \neq 3$ . Substituiere  $X \mapsto M_{\frac{1}{3}}a_2$ :

$$f = X^3 + aX + b \in K[X]$$

Beachte:  $f$  ist genau dann irreduzibel wenn  $g$  irreduzibel ist. (bzw separabel)

Sei  $L$  ein Zerfällungskörper von  $f$  (dann ist  $K \hookrightarrow L$  normal).

$f' = 3X^2 + \dots \neq 0$ , also ist  $f$  separabel, also ist  $K \hookrightarrow L$  Galois-Erweiterung.

Es gilt  $3 \leq [L : K]$  und  $[L : K]$  teil  $3! = 6$ , also

1. Entweder  $[L : K] = 3$ ,

2. oder  $[L : K] = 6$

$\text{Gal}(L/K)$  ist isomorph zu einer Untergruppe von  $S_3$ . Also im Fall

1.  $\text{Gal}(L : K) \cong A_3 := \{\sigma \in S_3 \mid \text{sgn}(\sigma) = 1\}$

2.  $\text{Gal}(L/K) \cong S_3$

Seien  $a_1, a_2, a_3 \in L$  die Nullstellen von  $f$ . Schreibe

$$\delta_f = \prod_{i < j \leq 3} (a_i - a_j) = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$$

$\Delta_f := \delta_f^2$  heißt die **Diskriminante** von  $f$ .

Jedes  $\sigma \in \text{Gal}(L/K)$  permutiert die Nullstellen und

$$\sigma(\delta_f) = \text{sgn}(\sigma)\delta_f$$

Es folgt  $\text{sgn}(\Delta_f) = \Delta_f$ .

Also  $\Delta_f \in L^{\text{Gal}(L/K)} = K$ .

Es ist  $\Delta_f = -4a^3 - 27b^2$ :

und  $\delta_f \in K$  genau dann wenn  $\text{Gal}(L/K) \cong A_3$ .

Fazit:  $[L : K] = 3 \Leftrightarrow \text{Gal}(L : K) \cong A_3 \Leftrightarrow \Delta_f$  ist Quadrat.

## 11 Anwendung der Galois-Theorie

### 11A Endliche Körper

*Bemerkung 11.1.* Sei  $K$  ein endlicher Körper.

1.  $\text{char}(K) = p > 0$  dann ist  $\#K = p^m$  mit  $m = [K : \mathbb{F}_p]$
2.  $K$  ist perfekt. Insbesondere ist jede algebraische Erweiterung  $K \hookrightarrow L$  separabel.

**Satz 11.2.** Sei  $p$  Primzahl und  $\overline{\mathbb{F}_p}$  ein algebraischer Abschluss von  $\mathbb{F}_p$ . Dann ist für alle  $m \in \mathbb{N}$ :

$$K = \{a \in \overline{\mathbb{F}_p} \mid a^{p^m} = a\}$$

ein Körper mit  $p^m$  Elementen.

Jeder Körper mit  $p^m$  Elementen ist Zerfällungskörper von  $X^p - X \in F_p[X]$ .

(Dann ist  $K, K'$  Körper mit  $p^m$  Elementen,  $K \cong K'$ .)

Es gilt:  $K$  besteht genau aus den Nullstellen von  $X^p - X$ .

*Beweis.* Sei  $f = X^{p^m} - X$ , dann ist  $f' = -1$ , also ist  $f$  separabel.

Es folgt  $\#\{a \in \overline{\mathbb{F}_p} \mid a^{p^m} = a\} = p^m$ .

Sei  $K$  ein beliebiger Körper mit  $p^m$  Elementen.

Wähle einen  $\mathbb{F}_p$ -Algebra-Homomorphismus  $K \hookrightarrow \overline{\mathbb{F}_p}$  (betrachte  $K$  als Unterkörper von  $\overline{\mathbb{F}_p}$ ).

Also  $K^\times = \{a \in \overline{\mathbb{F}_p} \mid a^{p^m-1} = 1\}$ . Es folgt  $K = \{a \in \overline{\mathbb{F}_p} \mid a^{p^m} = a\}$  □

**Satz 11.3.** Sei  $K$  ein endlicher Körper, sei  $q := \#K$ ,  $K \hookrightarrow L$  eine endliche Erweiterung und  $d := [L : K]$ .

Dann ist  $K \hookrightarrow L$  Galois-Erweiterung mit  $\text{Gal}(L/K) \cong \mathbb{Z}/d\mathbb{Z}$  erzeugt von  $\varphi : X \mapsto x^q$ .

*Beweis.* Aus 11.2 folgt, dass  $K \hookrightarrow L$ . Dann ist

$$L = \{a \in \overline{L} \mid a^{q^d} = a\}$$

$$K = \{a \in \overline{L} \mid a^q = a\}$$

Also  $\varphi \in \text{Gal}(L/K)$  hat Ordnung  $d$ , und dann  $\text{Gal}(L/K)$  ist zyklisch. □