

Algebra SS16

Prof Wedhorn, Mitschrift von Daniel Kallendorf

7. Dezember 2016

Inhaltsverzeichnis

1	Erinnerung: Ringe und Ideale	1
1A	Ideale, Primideal, maximale Ideale und Ring-Homomorphismen .	1
3	Tensorprodukte	5
3A	Erinnerung	5
3B	Multilineare Abbildungen	5
3C	6
3D	Basiswechsel von Tensorprodukten	8
4	Lokalisierung	12
4A	Lokalisierung von Ringen und Moduln	12
4B	Lokale Ringe und Restklassenkörper	15
4C	Spektren	16
	4.23 Spielzeugmodell (der Funktionalanalysis)	17
4D	Lemma von Nakagawa???	19
5	Noethersche und Artinsche Ringe	21
5A	Noethersche und Artinsche Moduln	21
5B	Länge von Moduln	24
5C	Noethersche Ringe	27
5D	Artin-Ringe	28
6	Ganzheit	30
6A	Ganze Ring-Homomorphismen	30
6B	Ganzer Abschluss	32
6C	Going-Up	33
7	Irreduzibilität	34
7A	Satz von Gauß	34
7B	Irreduzibilitätskriterien	36

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 φ 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 φ surjektiv ist, ist φ ein Ring-Homomorphismus.

3. Sei φ surjektiv. Dann sind die Abbildungen

$$\begin{aligned} \{\mathfrak{a} \subseteq A \text{ Ideal mit } \text{Ker}(\varphi) \subseteq \mathfrak{a}\} &\leftrightarrow \{\mathfrak{b} \in B \text{ Ideal}\} \\ \varphi^{-1}(\mathfrak{a}) &\leftrightarrow \mathfrak{b} \\ \mathfrak{a} &\leftrightarrow \varphi(\mathfrak{a}) \end{aligned}$$

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 $\mathfrak{m} \subseteq A$ heißt **maximales Ideal**, falls A/\mathfrak{m} ein Körper ist.
(Äquivalent: Es gibt kein Ideal \mathfrak{a} , sodass $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq A$).

Jedes Maximale Ideal ist Primideal.

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

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

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

□

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. ????

Bemerkung 2.8. $A[X_1, \dots, X_n]$ ist ein freier A -Modul, wobei die Monome eine Basis bilden.

Satz 2.9 (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 2.10.

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

Beispiel 2.11. Sei $\phi : A \rightarrow B$ ein A -Algebra, $b \in B$. Es existiere ein $g \in A[X]$ mit $g(b) = 0$. Sei g normiert. Dann gilt

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

Beispiel 2.12. 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:

$$\begin{aligned} \mathbb{Q}[i] &= \{a_0 + q_1 i + a_2 i^2 | a_0, a_1, a_2 \in \mathbb{Q}\} \\ \mathbb{Q}[i] &= \text{Im}(\mathbb{Q}[X] \xrightarrow[X \mapsto i, f \mapsto f(i)]{\psi} \mathbb{C}) \end{aligned}$$

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 ψ faktorisiert:

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

mit $\bar{\psi}$ surjektiv.

Proposition 2.13. 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. A -Modul: $(M, +, \cdot)$ wobei $(M, +)$ abelsche Gruppe und $\cdot : A \times M \rightarrow M$ ein Skalarprodukt.

Bemerkung 3.2. \mathbb{Z} -Modul = abelsche Gruppe

Beispiel 3.3. 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 3.4. Ein A -Modul heißt frei, falls $M \cong A^{(I)}$ für eine Menge I

Definition 3.5. 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 3.6. 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 3.7. 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.

3B Multilineare Abbildungen

Definition 3.8. 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 $m_j \in M_j, m_i \in M_i, a \in A$. ($r = 1$: linear, $r = 2$: bilinear)

3C ..

Definition 3.9. 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

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

existiert. $M_1 \times \dots \times M_r \xrightarrow{\forall \alpha, r\text{-multilinear}} P$

$$M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_r$$

Satz 3.10 (Eindeutigkeit des Tensorprodukts). Seien $(T, \tau : M_1 \times \dots \times M_r \rightarrow T)$ und (T', τ') Tensorprodukte:

$$\begin{array}{ccc} M_1 \times \dots \times M_r & & \\ \downarrow \tau & \searrow \tau' & \\ T & \xrightarrow{\exists! v} & T' \end{array}$$

u existiert aufgrund der universellen Eigenschaft von (T, τ) .

v existiert aufgrund der universellen Eigenschaft von (T', τ') .

Ferner kommutiert

Die Universelle Eigenschaft von (T, τ) zeigt, dass $v \circ u = id_T$, genauso $u \circ v = id_{T'}$.

Satz 3.11 (Existenz des Tensorprodukts). 1. Suche einen A -Modul N und eine Abbildung $c : M_1 \times \dots \times M_r \rightarrow N$, 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 .

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 3.12. 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 erzeugendnesn $m_1 \otimes \dots \otimes m_r$ 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:

$$u(m_1 \otimes \dots \otimes a m_i + m'_i \otimes \dots \otimes m_r) = a u(m_1 \otimes \dots \otimes m_i \otimes \dots \otimes m_r) + u(m_1 \otimes \dots \otimes a m'_i \otimes \dots \otimes m_r)$$

Satz 3.13 (Tensorprodukt linearer Abbildungen). *Seien M, M', N, n' A -Moduln, $u : M \rightarrow M', v : N \rightarrow N'$ A -lineare Abbildungen.*

Dann definiert

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

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.) □

Bemerkung 3.14. 3.6

1. $A \otimes_A M \cong M$

$$u : a \otimes m \mapsto am$$

$v : 1 \otimes m \mapsto m$ Dabei ist u wohldefiniert, d.h. $(a, m) \rightarrow am$ ist bilinear.

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

Zu zeigen: Wohldefineirtheit

3. $M \otimes_A N \otimes_A P \simeq (M \otimes_A N) \otimes_A P$

$$m \otimes n \otimes p \mapsto (m \otimes n) \otimes p$$

$$m \otimes n \otimes p \mapsto m \otimes (n \otimes p)$$

Proposition 3.15. 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:

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

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

□

3D Basiswechsel von Tensorprodukten

Satz 3.16. 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 3.17. 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 3.18. Sei $\mathfrak{a} \subseteq A$ ein Ideal, M ein A -Modul. Setze

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

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. $\bar{a} \otimes m \mapsto \overline{am}$ 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.

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

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 3.19. 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 3.20 (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 3.21. Sei $A \xrightarrow{\varphi} B$ 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

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

wobei

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

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

Beispiel 3.22. $A[X] \otimes_A A[Y] = (A[X])[Y] = A[X, Y]$ mit $f \otimes g \mapsto fg$.

Dann ist die Umkehrabbildung

C) Exaktheitseigenschaften

Definition 3.23 (Homomorphismen-Funktor). Seien M, P A -Moduln. Wir Definieren auf $\text{Hom}_A(M, P) := \{u : M \rightarrow P \mid u \text{ A-linear}\}$ 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 3.24. Eine Sequenz von A -lineare 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 3.25. $0 \rightarrow M \xrightarrow{u} M'$ ist exakt genau dann wenn u injektiv ist.
 $M \xrightarrow{v} M'' \rightarrow 0$ ist exakt genau dann wenn v surjektiv ist

Satz 3.26. 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

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

exakt ist.

2.

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

□

Bemerkung 3.27. Seien M, N, P A -Moduln. Dann ist

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

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

$$M \mapsto M \otimes_A N$$

$$(u : M \rightarrow M') \mapsto u \otimes id_N$$

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

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

Dann besagt (*):

$$\operatorname{Hom}(T_M(M), P) = \operatorname{Hom}(M, H_N(P))$$

d.h. T_N ist linksadjungiert zu H_N .

Dann ist T_N rechtsexakt und H_N linksexakt.

Proposition 3.28. 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

$$M' \otimes N \xrightarrow{u \otimes id_N} M \otimes N \xrightarrow{v \otimes id_N} M'' \otimes N \rightarrow 0$$

exakt.

Beweis. Formal mit 3.27.

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 (3.27)

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

exakt, sodass mit ??

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

exakt ist.

□

Beispiel 3.29. 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

$$\begin{array}{ccc} 0 \rightarrow \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} & \xrightarrow{u \otimes \text{id}_{\mathbb{Z}/2\mathbb{Z}}} & \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \\ & & \downarrow \cdot 2 \\ & & \mathbb{Z}/2\mathbb{Z} \end{array}$$

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 $s, t \in S \Rightarrow st \in A$.

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

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

Beweis. Dies ist eine Äquivalenzrelation:

- Reflexivität
- Symmetrie
- Transitiv: $(a, s) \sim (b, t), (b, t) \sim (c, u)$

$$\exists v, w \in S : \quad vat = bvs \quad , \quad wba = wtc$$

Dann ist $vbsw =!$

□

Satz 4.4 (Universelle Eigenschaft). Sei $S \subseteq A$ eine multiplikative Teilmenge und sei $1 : A \rightarrow S^{-1}$ kanonisch. Sei B ein Ring, $\varphi : A \rightarrow B$ ein Ring-Homomorphismus 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 Ring-Homomorphismus $\tilde{\varphi} : S^{-1}A \rightarrow B$ 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 injektive $\Leftrightarrow S$ 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

$$\begin{aligned}S^{-1}u : S^{-1}M &\rightarrow S^{-1}N \\ \frac{m}{s} &\mapsto \frac{u(m)}{s}\end{aligned}$$

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

Satz 4.8 (Lokalisierung ist exakt). 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 $tm \in \text{Ker}(v) = \mathfrak{Z}(u)$.

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 $\frac{m}{s} \in \text{Im}(S^{-1}u)$ □

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: z.Z:

- (a) $\frac{a}{s} = \frac{b}{t} \Rightarrow \frac{am}{s} = \frac{bm}{t}$.
- (b) $\frac{am}{s}$ ist linear in $\frac{a}{s}$ und in m .

2.

□

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

$$\{\text{Ideale in } A\} \xrightleftharpoons[b \mapsto \iota^{-1}(b)]{a \mapsto S^{-1}a} \{\text{Ideale in } S^{-1}A\}$$

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

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 $\iota : S^{-1}\mathfrak{a} \rightarrow S^{-1}A$ 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:

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

$$\xleftarrow{\mathfrak{p} \mapsto S^{-1}\mathfrak{p}}$$

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

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

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

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.

$$\begin{aligned}\{\text{Primideale in } A_{\mathfrak{p}}\} &= \{\text{Primideale in } A, \text{ die in } \mathfrak{p} \text{ enthalten sind}\} \\ \{\text{Primideal in } A/q\} &= \{\text{Primideal in } A, \text{ die } q \text{ enthalten.}\}\end{aligned}$$

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

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

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 $\text{Max}(A)$.

(Bemerke: $D(f) \cap D(g) = D(fg)$)

Satz 4.27. σ 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

$$\begin{array}{ccc} X & \xrightarrow{F} & Y \\ \sigma \downarrow \sim & & \sigma \downarrow \sim \\ \text{Max}(A_X) & \xrightarrow[\mathfrak{M} \mapsto \varphi^{-1}(\mathfrak{M})]{} & \text{Max}(A_Y) \end{array}$$

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 von 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 $u \in \text{Hom}_A(A)$

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

$A[u]$ 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 $(*)$ mit $\delta_{kj}(u)$.

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

Also ... □

Lemma 4.37 (Lemma von Nakagama (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

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

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

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

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

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

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

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

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

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. Fasse (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

$$N_1 \supseteq N_2 \supseteq \dots$$

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

$$(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \dots$$

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 κ 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 -Untermodule 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 $q = P - u(m')$.

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. \square

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 \mathbf{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_i 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/\mathfrak{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. □

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 notwendiger weise 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 $\{N \subsetneq M \text{ Untermodul}\}$ besitzt maximale Elemente, etwas M_1 .

Induktiv gilt $M = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots$, wobei M_{i-1}/M_i ist 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 $y \in B^\times$. □

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 Σ 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. □

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 $x = 0$. □

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 $l_A(M_1 M_2, \dots, M_j) < \infty$:

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 Σ 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 $b \neq \mathfrak{a}_0$. $\mathfrak{a}' \supseteq \mathfrak{a}_0 + (b) \not\subseteq \mathfrak{a}_0$.

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

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

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 φ) 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. φ 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 φ 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 $u^n + a_{n-1}u^{n-1} + \dots + a_0 = 0 \in \text{Hom}_A(C)$. Dann ist aber (mit $b = u(1)$)

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

□

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

1. φ endlich
2. φ 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

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

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 . \square

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 $b \in C$. \square

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 φ 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 freie 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 $y \neq 0$. Nehem 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 ψ 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 φ injektiv ist folgt $B \neq 0$.

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

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 $\varphi^{-1}(q_i) = p_i$ 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 $\bar{q}_2 \subset B/q_1$ gibt mit $\bar{\varphi}^{-1}(\bar{q}_2) = p_2/p_1$. Dass ist $\bar{q}_2 \cong q_2 \subset B$, 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) **irreduzibel**, 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 $o \notin A^\times$ 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 $\Sigma := \{(a) \mid 0 \neq a \in A^\times \text{ und ist nicht Produkt von irreduziblen Elementen}\}$.
Angenommen $\Sigma \neq \emptyset$:
Dann folgt mit 5.1

□

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 $fg = c(f)c(g)\tilde{g}\tilde{f}$, 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 $\bar{f} = \overline{c(f)\tilde{f}}$ reduzibel ist. \square

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, $f = a_nX^n + \dots + a_1X + a_0 \in A[X]$ 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: $\bar{a}_nX^n = \bar{f} = \bar{g}\bar{h} \in A/p[X]$ und $\bar{a}_n \neq 0$.

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 faktoriell, $p \in A$ prim, $n \geq 1$.

Dann ist $X^n - p$ irreduzibel.