

Algebra II - Sommersemester 2006
Prof. Dr. F. Herrlich

Die Mitarbeiter von <http://lkwiki.nomeata.de/>

9. Mai 2008

Inhaltsverzeichnis

1	Multilineare Algebra	2
1.1	Moduln	2
1.2	Tensorprodukt	7
1.3	Flache Moduln	9
1.4	Tensoralgebra	11
1.5	Symmetrische und äußere Algebra	13
1.6	Differentiale	14
1.7	Der de Rham-Komplex	17
2	Noethersche Ringe und Moduln	19
2.1	Der Hilbertsche Basissatz	19
2.2	Ganze Ringerweiterungen	22
2.3	Der Hilbert'sche Nullstellensatz	23
2.4	Graduierte Ringe und Moduln	25
2.5	Invarianten endlicher Gruppen	30
2.6	Nakayama, Krull und Artin-Rees	32
2.7	Krull-Dimension	34
2.8	Das Spektrum eines Rings	38
2.9	Diskrete Bewertungsringe	42
2.10	Dedekindringe	46
2.11	Primärzerlegung	51
	Vokabeln	53

Benannte Sätze

Satz 1	Tensorprodukt	7
Satz 2	Symmetrische und äußere Potenz	13
Satz 4	Hilbert'scher Basissatz	21
Satz 5	Hilbert'scher Nullstellensatz	23
Satz 6	Hilbert-Polynom	28
Satz 7	Endliche Erzeugbarkeit des Invariantenrings	30
Satz 8	Lemma von Nakayama	32
Satz 9	Durchschnittssatz von Krull	33
Proposition 2.23	Artin-Rees	33
Satz 12	Diskrete Bewertungsringe	44
Satz 13	Dedekindringe	47
Satz 15	Reduzierte Primärzerlegung	52

Kapitel 1

Multilineare Algebra

§1 Moduln

Sei R ein (kommutativer) Ring (mit Eins) (in der ganzen Vorlesung).

Definition 1.1

- (a) Eine abelsche Gruppe $(M, +)$ zusammen mit einer Abbildung $\cdot : R \times M \rightarrow M$ heißt **R -Modul** (genauer: R -Linksmodul), wenn gilt:

- (i) $a \cdot (x + y) = a \cdot x + a \cdot y$
- (ii) $(a + b) \cdot x = a \cdot x + b \cdot x$
- (iii) $(a \cdot b) \cdot x = a \cdot (b \cdot x)$
- (iv) $1 \cdot x = x$

für alle $a, b \in R$, $x, y \in M$.

- (b) Eine Abbildung $\varphi : M \rightarrow M'$ zwischen R -Modulen M, M' heißt **R -Modul-Homomorphismus** (kurz **R -linear**), wenn für alle $x, y \in M$, $a, b \in R$ gilt:
 $\varphi(a \cdot x + b \cdot y) = a \cdot \varphi(x) + b \cdot \varphi(y)$

Beispiele

- (1) $R = K$ Körper. Dann ist R -Modul = K -Vektorraum und R -linear = linear
- (2) R ist R -Modul. Jedes Ideal $I \subseteq R$ ist R -Modul
- (3) Jede abelsche Gruppe ist ein \mathbb{Z} -Modul.
(denn: $n \cdot x = \underbrace{x + x + \dots + x}_{n\text{-mal}}$ definiert die Abbildung $\cdot : \mathbb{Z} \times M \rightarrow M$ wie in 1.1 gefordert)

Bemerkung + Definition 1.2

- (a) Sind M, M' R -Moduln, so ist $\text{Hom}_R(M, M') = \{\varphi : M \rightarrow M' : \varphi \text{ ist } R\text{-linear}\}$ ein R -Modul durch $(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$ und $(a \cdot \varphi_1)(x) = a \cdot \varphi_1(x)$.
- (b) $M^* = \text{Hom}_R(M, R)$ heißt dualer Modul.

Beispiele

$R = \mathbb{Z}$

$\text{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}$, denn $0 = \varphi(0) = \varphi(1 + 1) = \varphi(1) + \varphi(1) \Rightarrow \varphi(1) = 0$

Bemerkung 1.3 (Ähnlichkeiten von Moduln mit Vektorräumen)

Die R -Moduln bilden eine *abelsche Kategorie $R\text{-Mod}$* .

- (a) Eine Untergruppe N eines R -Moduls M heißt R -Untermodul von M , falls $R \cdot N \subseteq N$.
- (b) Kern und Bild R -linearer Abbildungen sind R -Moduln.
- (c) Zu jedem Untermodul $N \subseteq M$ gibt es einen Faktormodul M/N .
- (d) Homomorphiesatz:
Für einen surjektiven Homomorphismus $\varphi : M \rightarrow N$ gilt: $M/\text{Kern}(\varphi) \cong N$.
- (e) *Direktes Produkt*: Sei $\{M_i\}_{i \in I}$ eine beliebige Menge von Moduln. Dann ist ihr direktes Produkt $\prod_i M_i = \times_i M_i$ gegeben durch die Menge aller Tupel $(m_i)_{i \in I}$ mit $m_i \in M_i$ und die R -Aktion $r(m_i)_{i \in I} = (rm_i)_{i \in I}$.

Direkte Summe: Das gleiche wie beim direkten Produkt, jedoch dürfen in den Tupeln nur endlich viele $m_i \neq 0$ sein.

Beweis

- (b) $\text{Kern}(\varphi)$: Sei $\varphi : M \rightarrow N$ lineare Abbildung. $m \in \text{Kern}(\varphi)$, $r \in R$:
 $\varphi(rm) = r\varphi(m) = 0 \Rightarrow R \cdot \text{Kern}(\varphi) \subseteq \text{Kern}(\varphi)$; Untergruppe klar
 $\text{Bild}(\varphi)$: $n \in \text{Bild}(\varphi)$, d. h. $\exists m : n = \varphi(m)$, $m \in M \Rightarrow r \in R : rn = r\varphi(m) = \varphi(rm) \in \text{Bild}(\varphi) \Rightarrow R \cdot \text{Bild}(\varphi) \subseteq \text{Bild}(\varphi)$

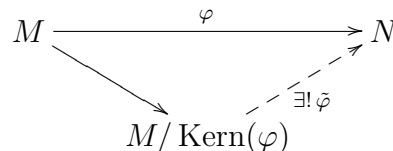
- (c) M abelsch \Rightarrow jedes N Normalteiler $\Rightarrow M/N$ ist abelsche Gruppe.

Wir definieren R -Aktion auf M/N durch $r(m+N) = rm+N$. Das ist wohldefiniert, denn
 $r((m+n)+N) = r(m+n)+N = rm + \underbrace{rn}_{\in N} + N = rm + N$

$$r((m+N) + (m'+N)) = r((m+m') + N) = r(m+m') + N = rm + N + rm' + N = r(m+N) + r(m'+N)$$

Die restlichen drei Eigenschaften gehen ähnlich.

- (d)



Wohldefiniertheit von $\tilde{\varphi}$:

Sei $k \in \text{Kern}(\varphi) : \varphi(m+k) = \varphi(m)$

surjektiv: $\forall n \in N : n = \varphi(m) = \tilde{\varphi}(m + \text{Kern}(\varphi))$

injektiv: $m, m' \in M$ mit $\varphi(m) = \varphi(m') = n \in N \Leftrightarrow \varphi(m-m') = 0 \Rightarrow m + \text{Kern}(\varphi)(m) = \text{Kern}(\varphi)(m')$

$\tilde{\varphi}$ ist R -linear: Klar, wegen φ R -linear.

Bemerkung 1.4

- (a) Zu jeder Teilmenge $X \subseteq M$ eines R -Moduls M gibt es den von X erzeugten Untermodul

$$\langle X \rangle = \bigcap_{\substack{M' \subseteq M \\ X \subseteq M'}} \text{Untermodul } M' = \left\{ \sum_{i=1}^n a_i x_i : n \in \mathbb{N}, a_i \in R, x_i \in X \right\}$$

- (b) $B \subset M$ heißt **linear unabhängig**, wenn aus $\sum_{i=1}^n \alpha_i b_i = 0$ mit $n \in \mathbb{N}, b_i \in B, \alpha_i \in R$ folgt $\alpha_i = 0$ für alle i .
- (c) Ein linear unabhängiges Erzeugendensystem heißt **Basis**.
- (d) Nicht jedes R -Modul besitzt eine Basis.
Beispiel: $\mathbb{Z}/2\mathbb{Z}$ als \mathbb{Z} -Modul: $\{\bar{1}\}$ ist nicht linear unabhängig, da $\underbrace{42}_{\neq 0 \text{ in } \mathbb{Z}} \cdot 1 = 0$
- (e) Ein R -Modul heißt **frei**, wenn er eine Basis besitzt.
- (f) Ein freier R -Modul M hat die Universelle Abbildungseigenschaft eines Vektorraums. Ist B eine Basis von $M, f : B \rightarrow M'$ eine Abbildung in einen R -Modul M' , so gibt es genau eine R -lineare Abbildung $\varphi : M \rightarrow M'$ mit $\varphi|_B = f$.
- (g) Sei M freier Modul. Dann ist M^* wieder frei und hat dieselbe Dimension wie M .

Beweis

(f) Sei $\{y_i\}_{i \in I}$ Familie von Elementen von M' .

Sei $x \in M$. Durch $x = \sum_i a_i x_i$ ist $\{a_i\}_{i \in I}$ eindeutig bestimmt.

Wir setzen: $\varphi(x) := \sum_i a_i y_i = \sum_i a_i \varphi(x_i)$

Beh. 1: Falls $\{y_i\}_{i \in I}$ ($y_i \neq y_j$ für $i \neq j$) Basis von M' ist, dann ist φ ein Isomorphismus.

Bew. 1: Wir können den Beweis des Satzes rückwärts anwenden

$\Rightarrow \exists \psi : M' \rightarrow M$ mit $\psi(y_i) = x_i \forall i \in I$

$\Rightarrow \varphi \circ \psi = id_{M'}, \psi \circ \varphi = id_M$

Beh. 2: Zwei freie Moduln mit gleicher Basis sind isomorph.

Bew. 2: klar

Proposition + Definition 1.5

Sei $0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$ kurze exakte Sequenz von R -Moduln (d.h. $M' \subseteq M$ Untermodul, $M'' = M/M'$). Dann gilt für jeden R -Modul N :

- (a) $0 \rightarrow \text{Hom}_R(N, M') \xrightarrow{\alpha^*} \text{Hom}_R(N, M) \xrightarrow{\beta_*} \text{Hom}_R(N, M'') \rightarrow 0$ ist exakt.
- (b) $0 \rightarrow \text{Hom}_R(M', N) \xrightarrow{\beta^*} \text{Hom}_R(M, N) \xrightarrow{\alpha^*} \text{Hom}_R(M'', N) \rightarrow 0$ ist exakt.
- (c) Im Allgemeinen sind β_* bzw. α^* nicht surjektiv.
- (d) Ein Modul N heißt **projektiv** (bzw. **injektiv**), wenn β_* (bzw. α^*) surjektiv ist.
- (e) Freie Moduln sind projektiv.
- (f) Jeder R -Modul M ist Faktormodul eines projektiven R -Moduls.
- (g) Jeder R -Modul M ist Untermodul eines injektiven R -Moduls.

Beweis

(a)

$$\begin{array}{ccccccc}
 & & & N & & & \\
 & & \swarrow \varphi & \downarrow \psi & \searrow & & \\
 0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' \longrightarrow 0
 \end{array}$$

α_* ist injektiv: Sei $\varphi \in \text{Hom}_R(N, M')$, ist $\alpha_*(\varphi) = \alpha \circ \varphi = 0 \stackrel{\alpha \text{ inj.}}{\Rightarrow} \varphi = 0$.

$$\text{Bild}(\alpha_*) \subseteq \text{Kern}(\beta_*): \beta_*(\alpha_*(\varphi)) = \underbrace{\beta \circ \alpha}_{=0} \circ \varphi = 0$$

$\text{Kern}(\beta_*) \subseteq \text{Bild}(\alpha_*)$:

Sei $\beta \circ \psi = 0$ ($\psi \in \text{Kern}(\beta_*)$). Für jedes $x \in N$ ist $\psi(x) \in \text{Kern}(\beta) = \text{Bild}(\alpha) \Rightarrow$ zu $x \in N \exists y \in M'$ mit $\psi(x) = \alpha(y)$; y ist eindeutig, da α injektiv.

Definiere $\varphi' : N \rightarrow M'$ durch $x \mapsto y$.

Zu zeigen: φ' ist R -linear

Seien $x, x' \in N \Rightarrow \varphi'(x + x') = z$ mit $\alpha(z) = \varphi(x + x') = \varphi(x) + \varphi(x') = \alpha(y) + \alpha(y') = \alpha(y + y')$ mit $\varphi'(x) = y, \varphi'(x') = y' \stackrel{\alpha \text{ inj.}}{\Rightarrow} z = y + y'$

Genauso: $\varphi'(a \cdot x) = a \cdot \varphi'(x)$

(b)

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\ & & & & & \searrow & \swarrow & & \\ & & & & & \beta^*(\varphi) & \varphi & & \\ & & & & & & N & & \end{array}$$

β^* injektiv, denn für $\varphi \in \text{Hom}(M'', N)$ ist $\beta^*(\varphi) = \varphi \circ \beta$

Sei $\beta^*(\varphi) = 0 \Rightarrow \varphi \circ \beta = 0 \stackrel{\beta \text{ surj.}}{\Rightarrow} \varphi = 0$.

$$\text{Bild}(\beta^*) \subseteq \text{Kern}(\alpha^*): (\alpha^* \circ \beta^*)(\varphi) = \alpha^*(\varphi \circ \beta) = \varphi \circ \underbrace{\beta \circ \alpha}_{=0} = 0$$

$\text{Kern}(\alpha^*) \subseteq \text{Bild}(\beta^*)$: Sei $\psi \in \text{Kern}(\alpha^*)$. Aber $\psi \in \text{Hom}_R(M, N)$ mit $\psi \circ \alpha = 0$
Weil ψ auf $\text{Bild}(\alpha)$ verschwindet, kommutiert

$$\begin{array}{ccc} & M'' & \\ \beta \nearrow & & \nwarrow \cong \\ M & \longrightarrow & M/\text{Bild}(\alpha) \\ \psi \searrow & & \swarrow \sigma \\ & N & \end{array}$$

$\Rightarrow \beta^*(\sigma) = \psi \implies \text{Beh.}$

(c) Im Allgemeinen sind β_* und α^* nicht surjektiv
z.B.:

$$1. \quad 0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/2\mathbb{Z} \rightarrow 0 \text{ mit } N := \mathbb{Z}/2\mathbb{Z}$$

Es gilt: $\text{Hom}(N, \mathbb{Z}) = \{0\}$
 $\text{Hom}(N, \mathbb{Z}/2\mathbb{Z}) = \{0, id\} \Rightarrow \beta_*$ nicht surjektiv $\Rightarrow N$ nicht projektiv!

$$2. \quad 0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 4} \mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/4\mathbb{Z} \rightarrow 0 \text{ mit } N := 2 \cdot \mathbb{Z}/4\mathbb{Z}$$

$\text{Hom}(\mathbb{Z}, N) = \{0, \psi\}$, wobei $\psi(1) = 2$.
 Dann: $\alpha^*(\psi) = \psi \circ \alpha = 0 \Rightarrow \alpha^*$ nicht surjektiv $\Rightarrow N$ nicht injektiv!

- (e) Sei N frei mit Basis $\{e_i, i \in I\}$. Sei $\beta : M \rightarrow M''$ surjektive R -lineare Abbildung und $\varphi : N \rightarrow M''$ R -linear. Für jedes $i \in I$ sei $x_i \in M$ mit $\beta(x_i) = \varphi(e_i)$ (so ein x_i gibt es, da β surjektiv). Dann gibt es genau eine R -lineare Abbildung $\psi : N \rightarrow M$ mit $\psi(e_i) = x_i$. Damit $\beta(\psi(e_i)) = \beta(x_i) = \varphi(e_i)$ für alle $i \in I \Rightarrow \beta \circ \psi = \varphi$
- (f) Sei M ein R -Modul. Sei X ein Erzeugendensystem von M als R -Modul (notfalls $X = M$). Sei F der freie R -Modul mit Basis X , $\varphi : F \rightarrow M$ die R -lineare Abbildung, die durch $x \mapsto x$ für alle $x \in X$ bestimmt ist. φ ist surjektiv, da $X \subseteq \text{Bild}(\varphi)$ und $\langle X \rangle = M$. Nach Homomorphiesatz ist $M \cong F / \text{Kern}(\varphi)$.

Proposition 1.6

Ein R -Modul N ist genau dann projektiv, wenn es einen R -Modul N' gibt, so dass $F := N \oplus N'$ freier Modul ist.

Beweis

„ \Rightarrow “:

Sei F freier R -Modul und $\beta : F \rightarrow N$ surjektiv (wie in [Beweis von 1.5 \(f\)](#)). Dann gibt es $\tilde{\varphi} : N \rightarrow F$ mit $\beta \circ \tilde{\varphi} = id_N$ (weil N projektiv ist).

Behauptung:

- 1.) $F = \text{Kern}(\beta) \oplus \text{Bild}(\tilde{\varphi}) \cong N' \oplus N$
- 2.) $\tilde{\varphi}$ injektiv

Beweis:

- 1.) $\text{Kern}(\beta) \cap \text{Bild}(\tilde{\varphi}) = (0)$, denn: $\beta(\tilde{\varphi}(x)) = 0 \Rightarrow x = 0 \Rightarrow \tilde{\varphi}(x) = 0$.

Sei $x \in F$, $y := \tilde{\varphi}(\beta(x)) \in \text{Bild}(\tilde{\varphi})$. Für $z = x - y$ ist $\beta(z) = \beta(x) - \underbrace{\beta(\tilde{\varphi}(\beta(x)))}_{id} = 0 \Rightarrow$

$$x = \underbrace{z}_{\in \text{Kern}(\beta)} + \underbrace{y}_{\in \text{Bild}(\tilde{\varphi})}$$

- 2.) $\tilde{\varphi}(x) = 0 \Rightarrow \underbrace{\beta(\tilde{\varphi}(x))}_{=x} = 0$

„ \Leftarrow “:

Sei $F = N \oplus N'$ frei, $\beta : M \rightarrow M''$ surjektiv, $\varphi : N \rightarrow M''$ R -linear.

Gesucht: $\psi : N \rightarrow M$ mit $\beta \circ \psi = \varphi$.

Definiere $\tilde{\varphi} : F \rightarrow M''$ durch $\tilde{\varphi}(x + y) = \varphi(x)$ wobei jedes $z \in F$ eindeutig als $z = x + y$ mit $x \in N$, $y \in N'$ geschrieben werden kann.

F ist frei also projektiv $\Rightarrow \exists \tilde{\psi} : F \rightarrow M$ mit $\beta \circ \tilde{\psi} = \tilde{\varphi}$. Sei $\psi := \tilde{\psi}|_N$. Dann ist $\beta \circ \psi = \beta \circ \tilde{\psi}|_N = \tilde{\varphi}|_N = \varphi$

§2 Tensorprodukt

Definition 1.7

Seien M, N, P R -Moduln.

- (a) Eine Abbildung $\Phi : M \times N \rightarrow P$ heißt **R -bilinear**, wenn für jedes $x_0 \in M$ und jedes $y_0 \in N$ die Abbildungen

$$\Phi_{x_0} : N \rightarrow P, y \mapsto \Phi(x_0, y)$$

$$\Phi_{y_0} : M \rightarrow P, x \mapsto \Phi(x, y_0)$$

R -linear sind.

- (b) Ein **Tensorprodukt** von M und N (über R) ist ein R -Modul T zusammen mit einer bilinearen Abbildung $\tau : M \times N \rightarrow T$, sodass
(UAE) Für jede bilineare Abbildung $\Phi : M \times N \rightarrow P$ gibt es genau eine lineare Abbildung $\varphi : T \rightarrow P$ mit $\Phi = \varphi \circ \tau$

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau} & T \\ & \searrow \Phi & \swarrow \exists! \varphi \\ & & P \end{array}$$

(τ ist die „universelle“ bilineare Abbildung)

Beispiele

- 1.) M, N freie R -Moduln mit Basis $\{e_i, i \in I\}$ bzw. $\{f_j, j \in J\}$. Dann ist $M \otimes N$ freier R -Modul mit Basis $\{e_i f_j, i \in I, j \in J\}$ ein Tensorprodukt mit $\tau(e_i, f_j) = e_i f_j$.

Denn: Sei $\Phi : M \times N \rightarrow P$ bilinear. Setze $\varphi(e_i \cdot f_j) := \Phi(e_i, f_j)$, das bestimmt eindeutig $\varphi : M \otimes N \rightarrow P$ (R -linear) mit $\Phi(e_i, f_j) = \varphi(\tau(e_i, f_j))$ für alle i, j .

Sind I, J endlich, so ist $\text{rg}(M \otimes N) = \text{rg}(M) \cdot \text{rg}(N)$, dagegen ist $\text{rg}(M \times N) = \text{rg}(M) + \text{rg}(N)$. τ ist also höchstens in Trivialfällen surjektiv. τ ist nicht injektiv: $\tau(x, 0) = \tau(x, 0 \cdot y) = 0 \cdot \tau(x, y) = 0$ (da linear im 2. Argument), genauso $\tau(0, y) = 0$. $\text{Bild}(\tau)$ ist kein Untermodul, aber $\langle \text{Bild}(\tau) \rangle = M \otimes N$.

- 2.) 0 ist ein Tensorprodukt der \mathbb{Z} -Moduln $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$.

Denn: jede bilineare Abbildung $\Phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \rightarrow P$ ist die Nullabbildung. $\Phi(\bar{1}, \bar{1}) = \Phi(3 \cdot \bar{1}, \bar{1}) = 3 \cdot \Phi(\bar{1}, \bar{1}) = \Phi(\bar{1}, 3 \cdot \bar{1}) = \Phi(\bar{1}, \bar{0}) = 0$, genauso $\Phi(\bar{1}, -\bar{1}) = 0$.

Satz 1 (Tensorprodukt)

Zu je zwei R -Moduln M, N gibt es ein Tensorprodukt. Dieses ist eindeutig bestimmt bis auf eindeutigen Isomorphismus.

Beweis 1.8

Sei F der freie R -Modul mit Basis $M \times N$. Sei Q Untermodul, der erzeugt wird von den

$$(x + x', y) - (x, y) - (x', y), (\alpha x, y) - \alpha(x, y)$$

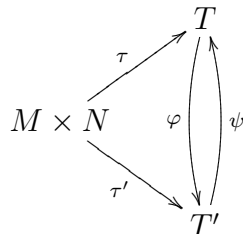
$$(x, y + y') - (x, y) - (x, y'), (x, \alpha y) - \alpha(x, y)$$

für alle $x, x' \in M, y, y' \in N, \alpha \in R$

Setze $T := F/Q$, $\tau : M \times N \rightarrow T$, $(x, y) \mapsto [(x, y)] \bmod Q$. τ ist bilinear nach Konstruktion. Ist $\Phi : M \times N \rightarrow P$ bilinear, so setze $\tilde{\varphi}((x, y)) := \Phi(x, y)$, $\tilde{\varphi} : F \rightarrow P$ ist linear. $Q \subseteq \text{Kern}(\tilde{\varphi})$, weil Φ bilinear $\xrightarrow{\text{Hom.-Satz}} \tilde{\varphi}$ induziert $\varphi : T \rightarrow P$ mit $\Phi = \varphi \circ \tau$.

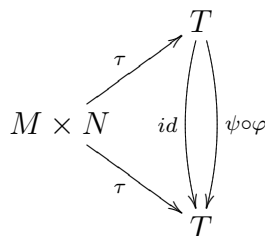
Noch zu zeigen: Eindeutigkeit

Seien (T, τ) , (T', τ') Tensorprodukte von M und N . Dann gibt es eine R -lineare Abbildung $\varphi : T \rightarrow T'$ mit $\tau' = \varphi \circ \tau$



und $\psi : T' \rightarrow T$ mit $\tau = \psi \circ \tau'$

Behauptung: $\psi \circ \varphi = id_T$ und $\varphi \circ \psi = id_{T'}$. Dazu:



ist kommutativ, d. h.

$(\psi \circ \varphi) \circ \tau = \psi \circ (\varphi \circ \tau) = \psi \circ \tau' = \tau$ mit $id : T \rightarrow T$ ist das Diagramm auch kommutativ. Wegen der Eindeutigkeit in der Definition des Tensorprodukts muss gelten: $\psi \circ \varphi = id_T$ ($\varphi \circ \psi = id_{T'}$ analog)

Bemerkung 1.9

Für alle R -Moduln M, N, M_1, M_2, M_3 gilt:

- (a) $M \otimes_R R \cong M$
- (b) $M \otimes_R N \cong N \otimes_R M$
- (c) $(M_1 \otimes_R M_2) \otimes_R M_3 \cong M_1 \otimes_R (M_2 \otimes_R M_3)$

Beweis

a) Zeige: M ist Tensorprodukt der R -Moduln M und R .

$\tau : M \times R \rightarrow M$, $(x, a) \rightarrow a \cdot x$ ist bilinear (wegen Moduleigenschaften). Sei $\Phi : M \times R \rightarrow P$ bilinear

Gesucht: $\varphi : M \rightarrow P$ linear mit $\Phi = \varphi \circ \tau$, d. h. $\Phi(x, a) = \varphi(a \cdot x)$

Setze $\varphi(x) := \Phi(x, 1)$. φ ist R -linear, da $\Phi(\cdot, 1)$ linear ist, $\Phi(x, a) = a\Phi(x, 1) = a\varphi(x) = \varphi(a \cdot x) = \varphi(\tau(x, a))$

φ ist eindeutig: es muss gelten: $\varphi(\tau(x, 1)) = \Phi(x, 1) =: \varphi(x)$, damit ist φ eindeutig bestimmt (wegen $\varphi \circ \tau = \Phi$).

b) $M \times N \cong N \times M$

c) Finde lineare Abbildung: $(M_1 \otimes_R M_2) \otimes_R M_3 \rightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$

1. Für festes $z \in M_3$ sei $\Phi_z : M_1 \times M_2 \rightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$,
 $(x, y) \rightarrow x \otimes (y \otimes z) := \tau(y, z)$
 Φ_z bilinear: klar
 Φ_z induziert eine lineare Abbildung: $\varphi_z : M_1 \otimes_R M_2 \rightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$
Weiter ist $\Psi : (M_1 \otimes_R M_2) \times M_3 \rightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$, $(w, z) \rightarrow \varphi_z(w)$
bilinear: linear in w , weil φ_z linear; linear in z weil Φ_z bilinear.
Induziert also lineare Abbildung $\psi : (M_1 \otimes_R M_2) \otimes_R M_3 \rightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$
2. Umkehrabbildung genauso!

Proposition 1.10

Sei M ein R -Modul, $I \subseteq R$ ein Ideal. Dann ist $I \cdot M = \{a \cdot x \in M : x \in M, a \in I\}$ Untermodul von M und es gilt:

$$M/I \cdot M \cong M \otimes_R R/I$$

Beweis

Sei $\tilde{\varphi} : M \rightarrow M \otimes_R R/I, x \rightarrow x \otimes \bar{1}$

$\tilde{\varphi}$ ist R -linear.

$$I \cdot M \subseteq \text{Kern}(\tilde{\varphi}) : \forall a \in I, x \in M \text{ ist } \tilde{\varphi}(ax) = ax \otimes \bar{1} = x \otimes \underbrace{a \cdot \bar{1}}_{\bar{a}} = 0$$

$\tilde{\varphi}$ induziert also lineare Abbildung

$$\varphi : M/(I \cdot M) \rightarrow M \otimes_R R/I$$

Umgekehrt: $\Psi : M \times R/I \rightarrow M/(I \cdot M), (x, \bar{a}) \rightarrow \overline{ax}$

$$\Psi \text{ ist wohldefiniert: ist } \bar{b} = \bar{a}, \text{ so ist } \overline{bx - ax} = \overline{(b-a) \cdot x} = 0$$

$\underbrace{\hspace{10em}}_{\substack{\in I \\ \in I \cdot M}}$

Ψ ist bilinear, induziert also $\psi : M \otimes_R R/I \rightarrow M/(I \cdot M)$ (linear). Es ist $(\psi \circ \varphi)(\bar{x}) = \psi(x \otimes \bar{1}) = \overline{1x} = \bar{x}$ und $(\varphi \circ \psi)(x \otimes \bar{a}) = \varphi(\overline{ax}) = ax \otimes \bar{1} = x \otimes a \cdot \bar{1} = x \otimes \bar{a}$

§3 Flache Moduln

Bemerkung 1.11

Für jeden R -Modul M ist die Zuordnung $M \mapsto M \otimes_R N$ ein Funktor

$$\otimes_R N : \underline{R\text{-Mod}} \rightarrow \underline{R\text{-Mod}}$$

Beweis

Ist $\varphi : M \rightarrow M'$ R -linear, so setze $\varphi_N : M \otimes_R N \rightarrow M' \otimes_R N, x \otimes y \mapsto \varphi(x) \otimes y$ und linear

$$\text{fortgesetzt: } \sum_{i=0}^n a_i(x_i \otimes y_i) \mapsto \sum_{i=0}^n a_i(\varphi(x_i) \otimes y_i)$$

Proposition 1.12

Der Funktor $\otimes_R N$ ist rechtsexakt, d.h. ist $0 \rightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \rightarrow 0$ exakt,

so ist $M' \otimes_R N \xrightarrow{\varphi_N} M \otimes_R N \xrightarrow{\psi_N} M'' \otimes_R N \rightarrow 0$ exakt.

Beispiele

$$R = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z}$$

$$0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

$\varphi_N : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} (\cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \text{ nach 1.9a}) \Rightarrow \varphi_N$ ist nicht surjektiv

Beweis

1. Schritt: $\text{Bild}(\varphi_N) \subseteq \text{Kern}(\psi_N)$, denn: $\psi_N(\varphi_N(x \otimes y)) = \psi_N(\varphi(x) \otimes y) = \underbrace{\psi(\varphi(x))}_{=0} \otimes y = 0$.

Homomorphiesatz liefert ein $\Psi : M \otimes_R N / \text{Bild}(\varphi_N) \rightarrow M'' \otimes_R N$

2. Schritt: Ψ ist Isomorphismus.

Dann ist Ψ und damit ψ_N surjektiv und $\text{Kern}(\psi_N) = \text{Bild}(\varphi_N)$.

Konstruiere Umkehrabbildung $\sigma : M'' \otimes_R N \rightarrow \bar{M} := M \otimes_R N / \text{Bild}(\varphi_N)$.

Wähle zu jedem $x'' \in M''$ ein Urbild $\chi(x'') \in \psi^{-1}(x'') \subset M$.

Definiere $\tilde{\sigma} : M'' \times N \rightarrow \bar{M}$ durch $(x'', y) \mapsto \chi(x'') \otimes y$

$\tilde{\sigma}$ wohldefiniert: Sind $x_1, x_2 \in M$ mit $\psi(x_1) = \psi(x_2) = x''$, so ist $\underbrace{x_1 - x_2}_{=\varphi(x')} \in \text{Bild}(\varphi) \Rightarrow \overline{x_1 \otimes y} - \overline{x_2 \otimes y} = \overline{\varphi(x') \otimes y} = 0$

$$\overline{x_2 \otimes y} = \overline{\varphi(x') \otimes y} = 0$$

Rest klar!!

Definition + Proposition 1.13

Sei N ein R -Modul.

- N heißt **flach**, wenn, wenn der Funktor $\otimes_R N$ exakt ist, d.h. für jede kurze exakte Sequenz von R -Moduln $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ auch $0 \rightarrow M' \otimes_R N \rightarrow M \otimes_R N \rightarrow M'' \otimes_R N \rightarrow 0$ exakt ist.
- N ist genau dann flach, wenn für jeden R -Modul M und jeden Untermodul M' von M die Abbildung $i : M' \otimes_R N \rightarrow M \otimes_R N$ injektiv ist.
- Jeder projektive R -Modul ist flach.
- Ist $R = K$ ein Körper, so ist jeder R -Modul flach.
- Für jedes multiplikative Monoid S ist R_S flacher R -Modul.

Beweis

(b) folgt aus [Prop 1.12](#)

(e) Sei M ein R -Modul, $M' \subseteq M$, R -Untermodul. Nach [Ü2A4](#) ist $M \otimes_R R_S \cong M_S$.

Zu zeigen: Die Abbildung $M'_S \rightarrow M_S, \frac{a}{s} \mapsto \frac{a}{s}$ ist injektiv.

Sei also $a \in M'$ und $\frac{a}{s} = 0$ in M_S , d.h. in M gilt: $t \cdot a = 0$ für ein $t \in S$. $\Rightarrow t \cdot a = 0$ in $M' \Rightarrow \frac{a}{s} = 0$ in M'_S .

(d) folgt aus (c), weil jeder K -Modul frei ist, also projektiv.

(c) Sei N projektiv. Nach [Prop. 1.6](#) gibt es einen R -Modul N' , sodass $N \oplus N' =: F$ frei ist.

Beh. 1: F ist flach.

Dann sei M R -Modul, $M' \subseteq M$ Untermodul; dann ist $F \otimes_R M' \rightarrow F \otimes_R M$ injektiv.

Beh. 2: Tensorprodukt vertauscht mit direkter Summe.

$$\begin{array}{ccc} M' \otimes_R F & \cong & M' \otimes_R (N \oplus N') \cong (M' \otimes_R N) \oplus (M' \otimes_R N') \\ \downarrow & & \downarrow \qquad \qquad \downarrow \\ \text{und } M \otimes_R R & & \cong (M \otimes_R N) \oplus (M \otimes_R N') \end{array}$$

Die Abbildung $M' \otimes_R F \rightarrow M \otimes_R F$ bildet $M' \otimes_R N$ auf $M \otimes_R N$ ab, $M' \otimes_R N \rightarrow M \otimes_R N$ ist also als Einschränkung einer injektiven Abbildung selbst injektiv.

Bew. 1: Sei $\{e_i : i \in I\}$ Basis von F , also $F = \bigoplus_{i \in I} Re_i \cong \bigoplus_{i \in I} R$. Wegen Beh. 2 ist

$$M \otimes_R F \cong M \otimes_R \bigoplus_{i \in I} R \cong \bigoplus_{i \in I} (M \otimes_R R) = \bigoplus_{i \in I} M$$

Genauso: $M' \otimes_R F \cong \bigoplus_{i \in I} M'$.

Die Abbildung $M' \otimes_R F \rightarrow M \otimes_R F$ ist in jeder Komponente die Einbettung $M' \hookrightarrow M$, also injektiv.

Bew. 2: Sei $M = \bigoplus_{i \in I} M_i$, zu zeigen: $M \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N)$.

Die Abbildung $M \times N \rightarrow \bigoplus_{i \in I} (M_i \otimes_R N)$, $((x_i)_{i \in I}, y) \mapsto (x_i \otimes y)_{i \in I}$ ist bilinear, induziert also eine R -lineare Abbildung $\varphi : M \otimes_R N \rightarrow \bigoplus_{i \in I} (M_i \otimes_R N)$.

Umgekehrt: Für jedes $i \in I$ induziert $M_i \hookrightarrow M$ $\psi_i : M_i \otimes_R N \rightarrow M \otimes_R N$; die ψ_i induzieren $\psi : \bigoplus_{i \in I} (M_i \otimes_R N) \rightarrow M \otimes_R N$ (UAE der direkten Summe). „Nachrechnen“: φ und ψ sind zueinander invers.

§4 Tensoralgebra

Definition 1.14

Eine R -**Algebra** ist ein (kommutativer) Ring (mit Eins) R' zusammen mit einem Ringhomomorphismus $\alpha : R \rightarrow R'$. Ist α injektiv, so heißt R'/R auch **Ringerweiterung**.

Bemerkung 1.15

Sei R' eine R -Algebra.

- (a) Die Zuordnung $M \rightarrow M \otimes_R R'$ ist ein kovarianter rechtsexakter Funktor $\otimes_R R' : \underline{R}\text{-Mod} \rightarrow \underline{R}'\text{-Mod}$; dabei wird $M \otimes_R R'$ zum R' -Modul durch $b \cdot (x \otimes a) := x \otimes b \cdot a$.
- (b) Sei $V : \underline{R}'\text{-Mod} \rightarrow \underline{R}\text{-Mod}$ der „Vergiss-Funktor“, der jeden R' -Modul als R -Modul fasst, mit der Skalarmultiplikation $a \cdot x := \alpha(a) \cdot x$ für $a \in R, x \in M$.

Dann ist $\otimes_R R'$ „links adjungiert“ zu V , d.h. für alle R -Moduln M und R' -Moduln M' sind $\text{Hom}_R(M, V(M'))$ und $\text{Hom}_{R'}(M \otimes_R R', M')$ isomorph (als R -Moduln).

Beweis

- (b) Die Zuordnungen

$$\begin{aligned} \text{Hom}_R(M, V(M')) &\rightarrow \text{Hom}_{R'}(M \otimes_R R', M') \\ \varphi &\mapsto (x \otimes a \mapsto a \cdot \varphi(x)) \\ (x \mapsto \psi(x \otimes 1)) &\leftarrow \psi \end{aligned}$$

sind zueinander invers.

Beispiele

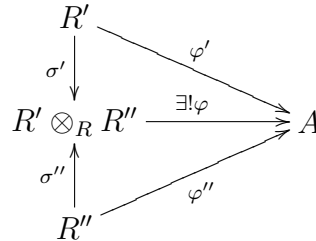
Sei R' eine R -Algebra, F freier Modul mit Basis $\{e_i : i \in I\}$. Dann ist $F \otimes_R R'$ ein freier R' -Modul mit Basis $\{e_i \otimes 1 : i \in I\}$.

denn: Sei $f : \{e_i \otimes 1 : i \in I\} \rightarrow M$ Abbildung (M beliebiger R' -Modul). Dann gibt es genau eine R -lineare Abbildung $\varphi : F \rightarrow V(M)$ mit $\varphi(e_i) = f(e_i \otimes 1)$ (UAE für F). Mit 1.15 (b) folgt: dazu gehört eine eindeutige R' -lineare Abbildung $\tilde{\varphi} : F \otimes_R R' \rightarrow M$ mit $\tilde{\varphi}(e_i \otimes 1) = \varphi(e_i)$.

Proposition 1.16

Seien R', R'' R -Algebren.

- (a) $R' \otimes_R R''$ wird zur R -Algebra durch $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) := a_1 a_2 \otimes b_1 b_2$
- (b) $\sigma' : R' \rightarrow R' \otimes_R R'', a \mapsto a \otimes 1$ und $\sigma'' : R'' \rightarrow R' \otimes_R R'', b \mapsto 1 \otimes b$ sind R -Algebrenhomomorphismen.
- (c) UAE: in der Kategorie der R -Algebren gilt:



Beweis

Setze $\varphi(a \otimes b) = \varphi'(a) \cdot \varphi''(b)$.

φ ist die lineare Abbildung, die von der bilinearen Abbildung $\tilde{\Phi} : R' \times R'' \rightarrow A, (a, b) \mapsto \varphi'(a) \cdot \varphi''(b)$ induziert wird.

Nachrechnen: φ ist Ringhomomorphismus und eindeutig bestimmt.

Beobachte: $a \otimes b = (a \otimes 1)(1 \otimes b)$

also muss: $\varphi(a \otimes b) = \underbrace{(\varphi \circ \sigma')(a)}_{\varphi'(a)} \cdot \underbrace{(\varphi \circ \sigma'')(b)}_{\varphi''(b)}$.

Beispiele

R' sei eine R -Algebra. Dann ist $R'[X] \cong R[X] \otimes_R R'$ (als R' -Algebren), denn:

Zeige, dass $R[X] \otimes_R R'$ die UAE des Polynomrings $R'[X]$ erfüllt.

Sei A eine R' -Algebra und $a \in A$. Zu zeigen: $\exists!$ R' -Algebrahomomorphismus $\varphi : R[X] \otimes_R R' \rightarrow A$ mit $\varphi(X \otimes 1) = a$. Ein solcher wird als R -Algebra-Homomorphismus induziert von $\varphi' : R[X] \rightarrow A, X \mapsto a$ und $\varphi'' : R' \rightarrow A$ (der Strukturhomomorphismus α aus der Definition)

Noch zu zeigen: φ ist R' -linear (richtig, weil φ'' Ringhomomorphismus)

Definition + Bemerkung 1.17

Sei M ein R -Modul

- a) $T^0(M) := R, T^n(M) = M \otimes_R T^{n-1}(M), n \geq 1$
- b) $T(M) := \bigoplus_{n=0}^{\infty} T^n(M)$ wird zur R -Algebra durch $(x_1 \otimes \dots \otimes x_n) \cdot (y_1 \otimes \dots \otimes y_m) := x_1 \otimes \dots \otimes x_n \otimes y_1 \otimes \dots \otimes y_m \in T^{n+m}(M)$
- c) $T(M)$ ist nicht kommutativ (außer im Trivialfall), denn $x \otimes y \neq y \otimes x$
- d) $T(M)$ erfüllt UAE: Ist R' R -Algebra (nicht notwendig kommutativ) $\varphi : M \rightarrow R'$ R -linear, so $\exists!$ R -Algebra-Homomorphismus $\tilde{\varphi} : T(M) \rightarrow R'$ mit $\underbrace{\tilde{\varphi}|_{T^1(M)}}_{=M} = \varphi$

§5 Symmetrische und äußere Algebra

Definition 1.18

Seien M, N R -Moduln, $n \geq 1$, $\Phi : M^n \rightarrow N$ R -multilinear.

- Φ heißt **symmetrisch**, wenn für alle $(x_1, \dots, x_n) \in M^n$ und alle $\sigma \in S_n$ gilt:
 $\Phi(x_1, \dots, x_n) = \Phi(x_{\sigma(1)}, \dots, x_{\sigma(n)})$
- Φ heißt **alternierend**, wenn für alle $(x_1, \dots, x_n) \in M^n$ gilt:
 Ist $x_i = x_j$ für ein Paar (x_i, x_j) mit $i \neq j$, so ist $\Phi(x_1, \dots, x_n) = 0$
 Ausser in char = 2 ist das äquivalent zu $\Phi(x_1, \dots, x_n) = -\Phi(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$
- $\text{Sym}_M^n(N) := \{\Phi : M^n \rightarrow N : \Phi \text{ multilinear, symmetrisch}\}$
 $\text{Alt}_M^n(N) := \{\Phi : M^n \rightarrow N : \Phi \text{ multilinear, alternierend}\}$
 $\text{Sym}_M^n(N)$ und $\text{Alt}_M^n(N)$ sind R -Moduln.

Satz 2 (Symmetrische und äußere Potenz)

Zu jedem R -Modul M und jedem $n \geq 1$ gibt es R -Moduln $S^n(M)$ und $\Lambda^n(M)$ (genannt die n -te **symmetrische** bzw. **äußere Potenz** von M) und eine symmetrische bzw. alternierende multilineare Abbildung $M^n \rightarrow S^n(M)$ bzw. $M^n \rightarrow \Lambda^n(M)$ mit folgender UAE:

$$\begin{array}{ccc}
 M^n & \longrightarrow & S^n(M) \\
 \searrow \Phi \in \text{Sym}_M^n(N) & & \swarrow \exists! \varphi \text{ linear} \\
 & & N
 \end{array}
 \quad \text{bzw.} \quad
 \begin{array}{ccc}
 M^n & \longrightarrow & \Lambda^n(M) \\
 \searrow \Psi \in \text{Alt}_M^n(N) & & \swarrow \exists! \psi \text{ linear} \\
 & & N
 \end{array}$$

Mit $S^0(M) := R =: \Lambda^0(M)$ heißt $S(M) := \bigoplus_{n \geq 0} S^n(M)$ die **symmetrische Algebra** über M
 $\Lambda(M) := \bigoplus_{n \geq 0} \Lambda^n(M)$ die **äußere Algebra** über M (oder **Graßmann-Algebra**)

Beweis

Sei $\mathbb{J}^n(M)$ der Untermodul von $T^n(M)$, der erzeugt wird von allen

$x_1 \otimes \dots \otimes x_n - x_{\sigma(1)} \otimes \dots \otimes x_{\sigma(n)}$, $x_i \in M$, $\sigma \in S_n$ und

$\mathbb{I}^n(M)$ der Untermodul von $T^n(M)$, der erzeugt wird von allen

$x_1 \otimes \dots \otimes x_n$ für die $x_i = x_j$ für ein Paar (i, j) mit $i \neq j$.

Setze $S^n(M) := T^n(M) / \mathbb{J}^n(M)$ und $\Lambda^n(M) := T^n(M) / \mathbb{I}^n(M)$

Sei $\Phi : M^n \rightarrow N$ multilinear und symmetrisch. Φ induziert $\tilde{\varphi} : T^n(M) \rightarrow N$ R -linear (weil Φ multilinear), da Φ symmetrisch ist, ist $\mathbb{J}^n(M) \subseteq \text{Kern}(\tilde{\varphi})$. $\tilde{\varphi}$ induziert also $\varphi : S^n(M) \rightarrow N$ R -linear; genauso falls $\Psi : M^n \rightarrow N$ alternierend.

Proposition 1.19

Sei M freier R -Modul mit Basis e_1, \dots, e_r . Dann gilt für jedes $n \geq 1$:

- $S^n(M)$ ist freier Modul mit Basis $\{e_1^{\nu_1} \cdot \dots \cdot e_r^{\nu_r} : \sum_{i=1}^r \nu_i = n\}$
- $S(M) \cong R[X_1, \dots, X_r]$
- $\Lambda^n(M)$ ist freier R -Modul mit Basis
 $\{e_{i_1} \wedge \dots \wedge e_{i_n} : 1 \leq i_1 < i_2 < \dots < i_n \leq r\}$
- $\Lambda^n(M) = 0$ für $n > r$

Beweis

b) folgt aus a)

d) folgt aus c)

c) $\Lambda^r(M)$ wird erzeugt von $e_1 \wedge \dots \wedge e_r$: klar.

$\Lambda^r(M)$ ist frei (vom Rang 1), denn aus $a \cdot e_1 \wedge \dots \wedge e_r = 0$ folgt $a = 0$.

Für $n < r$ bilden $\{e_{i_1} \wedge \dots \wedge e_{i_n} : 1 \leq i_1 < i_2 < \dots < i_n \leq r\}$ ein Erzeugendensystem.

Zu zeigen: $\{e_{i_1} \wedge \dots \wedge e_{i_n} : 1 \leq i_1 < i_2 < \dots < i_n \leq r\}$ ist linear unabhängig.

Sei dazu $\sum_{1 \leq i_1 < \dots < i_n \leq r} a_i e_{i_1} \wedge \dots \wedge e_{i_n} = 0$

Für $\underline{j} = (j_1, \dots, j_n)$ mit $1 \leq j_1 < \dots < j_n \leq r$ sei $\sigma_j \in S_n$ mit $\sigma_j(\nu) = j_\nu$ für $\nu = 1, \dots, n$

Dann ist $0 = (\sum a_i e_{i_1} \wedge \dots \wedge e_{i_n}) \wedge e_{\sigma_j(n+1)} \wedge \dots \wedge e_{\sigma_j(r)} = a_j e_1 \wedge \dots \wedge e_r \Rightarrow a_j = 0 \Rightarrow$ l.u.

§6 Differentiale

Definition + Bemerkung 1.20

Sei A eine kommutative R -Algebra, M ein A -Modul.

(a) Eine R -lineare Abbildung $\delta : A \rightarrow M$ heißt **Derivation**, wenn für alle $f, g \in A$ gilt:

$$\delta(f \cdot g) = f \cdot \delta(g) + g \cdot \delta(f)$$

(b) $\text{Der}_R(A, M) := \{\delta : A \rightarrow M : \delta \text{ } R\text{-lineare Derivation}\}$ ist ein A -Modul.

(c) $M \mapsto \text{Der}_R(A, M)$ ist ein Funktor (Unterfunktor von $\text{Hom}_R(A, \cdot)$).

Beispiele

1.) $A = R[X], d = \frac{d}{dX}$ ist eine R -Derivation $d : A \rightarrow A$, definiert durch $d(\sum_{i=0}^n a_i X^i) := \sum_{i=1}^n a_i i X^{i-1}$

2.) $A = R[[X]], d = \frac{d}{dX}$ wie in 1.) mit ∞ statt n .

Beh.: $\text{Der}_R(A, A) = A \cdot d$

Bew.: Sei $\delta : A \rightarrow A$ eine R -lineare Derivation, $f := \delta(X)$.

Dann ist $\delta(1) = \delta(1 \cdot 1) = 1 \cdot \delta(1) + 1 \cdot \delta(1) \Rightarrow \delta(1) = 0 \Rightarrow \forall r \in R : \delta(r) = 0$

$\delta(X^2) = 2 \cdot X \cdot \delta(X)$ und (Induktion) $\delta(X^n) = X \cdot \delta(X^{n-1}) + X^{n-1} \cdot \delta(X) = n \cdot X^{n-1} \cdot f \stackrel{\delta \text{ } R\text{-linear}}{\Rightarrow}$

$\delta(\sum a_i X^i) = \sum a_i i X^{i-1} \cdot f \Rightarrow \delta = f \cdot d$

3.) $A = R[X_1, \dots, X_n], \partial_i = \frac{\partial}{\partial X_i}$ ist Derivation genauso wie für 1.)

$\text{Der}_R(A, A)$ ist freier A -Modul mit Basis $\partial_1, \dots, \partial_n$.

Proposition + Definition 1.21

Der Funktor $M \mapsto \text{Der}_R(A, M)$ ist „darstellbar“, d.h. es gibt einen A -Modul $\Omega_{A/R}$ und eine Derivation $d : A \rightarrow \Omega_{A/R}$ mit folgender UAE:

Zu jedem A -Modul M und jeder R -linearen Derivation $\delta : A \rightarrow M$ existiert genau eine A -lineare Abbildung $\varphi : \Omega_{A/R} \rightarrow M$ mit $\delta = \varphi \circ d$.

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega_{A/R} \\ & \searrow \delta & \swarrow \exists! \varphi \\ & & M \end{array}$$

Beweis

Sei F der freie Modul mit Basis A , dabei sei X_f das zu $f \in A$ gehörige Basiselement von F . Sei U der Untermodul von F , der erzeugt wird von allen

$$\left. \begin{array}{l} X_{f+g} - X_f - X_g \\ X_{\lambda f} - \lambda X_f \\ X_{f \cdot g} - f \cdot X_g - g \cdot X_f \end{array} \right\} \text{für alle } f, g \in A, \lambda \in R$$

Sei $\Omega_{A/R} := F/U$, $d : A \rightarrow \Omega_{A/R}$, $f \mapsto [X_f] =: df$. d ist Derivation nach Konstruktion („universelle Derivation“).

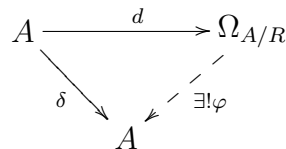
UAE: Sei M A -Modul, $\delta : A \rightarrow M$ Derivation. Sei $\Phi : F \rightarrow M$ die A -lineare Abbildung mit $\Phi(X_f) = \delta(f)$. $U \subseteq \text{Kern}(\Phi)$, weil δ Derivation, d.h. Φ induziert $\varphi : F/U \rightarrow M$.

Beispiele

$A = R[X_1, \dots, X_n]$, $\Omega_{A/R}$ ist freier Modul mit Basis dX_1, \dots, dX_n ,

denn für $f = \sum_{\nu=(\nu_1, \dots, \nu_n)} a_\nu X_1^{\nu_1} \cdots X_n^{\nu_n} \in A$ ($a_\nu \in R$) ist $df = \sum_{i=1}^n \frac{\partial f}{\partial X_i} dX_i$
 \Rightarrow die dX_i erzeugen $\Omega_{A/R}$.

Nach Prop. 1.21 ist $\boxed{\text{Der}_R(A, A) = \text{Hom}_A(\Omega_{A/R}, A)}$.



Zu zeigen: die dX_i sind linear unabhängig.

Sei also $\sum_{i=1}^n a_i dX_i = 0 \Rightarrow 0 = \frac{\partial}{\partial X_j} (\sum a_i X_i) = a_j$

Beispiele

Sei $X \subseteq \mathbb{R}^n$ offen (für ein $n > 1$), $A := \mathcal{C}^\infty(X)$ die \mathbb{R} -Algebra der beliebig oft differenzierbaren Funktionen auf X .

Beh.: $\text{Der}_{\mathbb{R}}(A, A)$ ist ein freier A -Modul mit Basis $\partial_1, \dots, \partial_n$ (mit $\partial_i := \frac{\partial}{\partial X_i}$ partielle Ableitung nach X_i).

Dann ist auch $\Omega_{A/\mathbb{R}}$ freier A -Modul mit Basis dX_1, \dots, dX_n .

Beh.1: Für jedes $x \in X$ wird das Ideal $I_x = \{f \in A : f(x) = 0\}$ erzeugt von $X_i - x_i$ ($x = (x_1, \dots, x_n)$), $i = 1, \dots, n$ (Taylor-Entwicklung).

Sei nun $\partial : A \rightarrow A$ Derivation. Zu zeigen: $\partial = \sum_{i=1}^n \partial(X_i) \partial_i$.

Setze $\partial' := \partial - \sum_{i=1}^n \partial(X_i) \partial_i$

Beh.2: Für jedes $x \in X$ ist $\partial'(I_x) \subseteq I_x$

Bew.2: Sei $f \in I_x$, $f = \sum_{i=1}^n g_i (X_i - x_i)$ (siehe Beh. 1) mit $g_i \in A$. Also ist $\partial'(f) =$

$$\underbrace{\sum_{i=1}^n \partial'(g_i)(X_i - x_i)}_{\in I_x} + \sum_{i=1}^n g_i \underbrace{\partial'(X_i - x_i)}_{=0, \text{ da } \partial_j(X_i - x_i) = \delta_{ij}}.$$

Sei nun $g \in A$, $x \in X$. Schreibe $g = \underbrace{g - g(x)}_{\in I_x} + g(x) \Rightarrow \partial'(g) = \partial'(g \cdot g(x)) \in I_x$

d.h. $\partial'(y)(x) = 0 \Rightarrow \partial'(y) = 0 \Rightarrow \partial' = 0$

Proposition 1.22

a) $\Omega_{./R}$ ist ein Funktor. $\underline{\mathbb{R}\text{-Alg}} \rightarrow \underline{\mathbb{R}\text{-Mod}}$.

Beweis

Sei $\varphi : A \rightarrow B$, R -Algebra-Homomorphismus

$$\begin{array}{ccc} A & \xrightarrow{d_A} & \Omega_{A/R} \\ \varphi \downarrow & & \downarrow \exists! d\varphi \text{ } A\text{-linear} \\ B & \xrightarrow{d_B} & \Omega_{B/R} \end{array}$$

So ist $d_B \circ \varphi : A \rightarrow \Omega_{B/R}$

$$d_B \circ \varphi(\lambda \cdot a) = d_B(\lambda \varphi(a)) = \lambda d_B(\varphi(a)) \quad \forall \lambda \in R, a \in A.$$

$$d_B \circ \varphi(a_1 \cdot a_2) = d_B(\varphi(a_1) \cdot \varphi(a_2)) = \varphi(a_1) \cdot d_B(\varphi(a_2)) + \varphi(a_2) \cdot d_B(\varphi(a_1))$$

\Rightarrow Derivation, wenn $\Omega_{B/R}$ vermöge φ als A -Modul aufgefasst wird.

[Man kann $\Omega_{A/R}$ aufwerten zum B -Modul durch $\otimes_A B$:]

$$\begin{array}{ccc} A & \xrightarrow{d_A} & \Omega_{A/R} \otimes_A B \\ \varphi \downarrow & & \downarrow \exists! d\alpha \text{ } B\text{-linear} \\ B & \xrightarrow{d_B} & \Omega_{B/R} \end{array}$$

Etwas durch $\alpha(\omega \otimes b) = b \cdot d\varphi(\omega)$

b)

$$\Omega_{A/R} \otimes_A B \xrightarrow{\alpha} \Omega_{B/R} \xrightarrow{\beta} \Omega_{B/A} \rightarrow 0$$

ist exakte Sequenz von B -Moduln für jeden R -Algebra-Homomorphismus $\varphi : A \rightarrow B$

Beweis

β surjektiv: \checkmark (Konstruktion von $\Omega_{./}$)

„ $\beta \circ \alpha = 0$ “ (d.h. $\text{Bild}(\alpha) \subseteq \text{Kern}(\beta)$)

$d_{B/A}\varphi(a) = 0$ für jedes $a \in A$.

(In $\Omega_{B/A}$ werden alle „konstanten A -Funktionen“ durch die Derivation zu 0).

„ $\text{Kern}(\beta) \subseteq \text{Bild}(\alpha)$ “,

Sei $\omega = \sum_{i=1}^n b_i d_{B/R}(c_i) \in \text{Kern}(\beta)$ mit $b_i, c_i \in B$

Dann ist $\beta(\omega) = \sum_{i=1}^n b_i d_{B/A}(c_i) = 0$

$\Rightarrow \sum_{i=1}^n b_i c_i \in U_{B/A}$ (im freien B -Modul mit Basis $\{x_b : b \in B\}$ vgl Beweis zu 1.21)

$$\Rightarrow \sum_i b_i c_i = \sum_j b_j \underbrace{(x_{f_j+g_j} - x_{f_j} - x_{g_j})}_{\in U_{B/R}} + \sum_k b'_k (x_{\varphi(\lambda_k)g_k} - \varphi(\lambda_k)x_{g_k}) + \sum_l b''_l \underbrace{(x_{f_l g_l} - f_l x_{g_l} - g_l x_{f_l})}_{\in U_{B/R}}$$

für gewisse $b_j, b'_k, b''_l \in B$, $f_j, f_k, f_l, g_k, g_j, g_l \in B$, $\lambda_k \in A$

$$\Rightarrow w = \sum_k b'_k (d_{B/R}(\varphi(\lambda_k)g_k) - \varphi(\lambda_k)d_{B/R}(g_k))$$

$$= \sum_k b'_k (\varphi(\lambda_k)d_{B/R}(g_k) + g_k d_{B/R}(\varphi(\lambda_k)) - \varphi(\lambda_k)d_{B/R}(g_k))$$

$$= \sum_k b'_k g_k d_{B/R}(\varphi(\lambda_k)) = \alpha(\sum_k d\lambda_k \otimes b'_k g_k)$$

§7 Der de Rham-Komplex

A (kommutative) R -Algebra.

$\Omega_A := \Omega_{A/R}$, $\Omega_A^i := \Lambda^i \Omega_A$ für $i \geq 0$.

Satz + Definition 3

a) Für jedes $i \geq 0$ gibt es eine eindeutig bestimmte R -lineare Abbildung $d_i : \Omega_A^i \rightarrow \Omega_A^{i+1}$ mit

$$(i) \quad d_i(f \cdot \omega) = df \wedge \omega + f d_i(\omega) \text{ für alle } f \in A, \omega \in \Omega_A^i$$

$$(ii) \quad d_{i+1} \circ d_i = 0$$

b) Die Sequenz Ω_A^\bullet :

$$A \xrightarrow{d_0} \Omega_A \xrightarrow{d_1} \Omega_A^2 \xrightarrow{d_2} \dots \xrightarrow{d_{n-1}} \Omega_A^n \xrightarrow{d_n} \dots$$

heißt **de Rham-Komplex** zu A .

c) Für jedes $i \geq 0$ heißt $H_{dR}^i(A) := \text{Kern}(d_i) / \text{Bild}(d_{i-1})$ (R -Modul) der i -te de Rham-Kohomologie-Modul von A . Dabei sei $d_{-1} = 0$, d.h. $H_{dR}^0(A) = \text{Kern}(d) = R$.

Beweis

1. Fall $A = R[X_1, \dots, X_n]$

Dann ist Ω_A^k freier A -Modul mit Basis $dX_{i_1} \wedge \dots \wedge dX_{i_k}$, $1 \leq i_1 < \dots < i_k \leq n$

für $f \in A$ ist $df = d_A f = d_0 f = \sum_{i=1}^n \partial_i f dX_i$

Setze: $d_1(\sum_{i=1}^n f_i dX_i) = \sum_{i=1}^n df_i \wedge dX_i \in \Omega_A^2$

konkretes Beispiel: $d_1(f_1 dX_1 + f_2 dX_2)$

$$= \left(\frac{\partial f_1}{\partial x_1} dX_1 + \frac{\partial f_1}{\partial x_2} dX_2 \right) \wedge dX_1 + \left(\frac{\partial f_2}{\partial x_1} dX_1 + \frac{\partial f_2}{\partial x_2} dX_2 \right) \wedge dX_2 = \left(\frac{\partial f_2}{\partial x_1} - \frac{\partial f_1}{\partial x_2} \right) dX_1 \wedge dX_2$$

Erklärung: $dX_1 \wedge dX_1 = 0$, $dX_2 \wedge dX_1 = -dX_1 \wedge dX_2$

allgemein setze d_k :

$$d_k \left(\sum_{1 \leq i_1 < \dots < i_k \leq n} f_{i_1 \dots i_k} dX_{i_1} \wedge \dots \wedge dX_{i_k} \right) = \sum_{1 \leq i_1 < \dots < i_k \leq n} d(f_{i_1 \dots i_k}) \wedge dX_{i_1} \wedge \dots \wedge dX_{i_k}$$

Diese d_k erfüllen (i):

Sei $\omega = \sum_i f_i dX_{i_1} \wedge \dots \wedge dX_{i_k} \in \Omega_A^k$, $f \in A$.

$$\Rightarrow d_k(f\omega) = \sum_i d(f f_i) \wedge dX_{i_1} \wedge \dots \wedge dX_{i_k}$$

$$= \underbrace{\sum_i f df_i \wedge dX_{i_1} \wedge \dots \wedge dX_{i_k}}_{=f \cdot d_k(\omega)} + \underbrace{\sum_i f_i df \wedge dX_{i_1} \wedge \dots \wedge dX_{i_k}}_{df \wedge \omega}$$

(ii) folgt zwingend aus: $d_k(dX_{i_1} \wedge \dots \wedge dX_{i_k}) = 0$ (Induktion über k)

Eindeutigkeit der d_k : $d_0 = d$ ist vorgegeben.

d_1 : wegen (ii) ist $d_1(dX_i) = 0$ für alle $i = 1, \dots, n$

wegen (i) ist $d_1(f dX_i) = df \wedge dX_i + f \underbrace{d_1(dX_i)}_{=0}$

d_2 : zeige: $d_2(dX_{i_1} \wedge dX_{i_2}) = 0$ folgt aus (ii),

da $dX_1 \wedge dX_2 = d_1(X_1 dX_2) = d_1(-X_2 dX_1)$

wegen (i) ist $d_2(f dX_1 \wedge dX_2) = df \wedge dX_1 + dX_2$

(Induktion)

Zu zeigen: $d_{k+1} \circ d_k(f \underbrace{dX_{i_1} \wedge \dots \wedge dX_{i_k}}_{=: \omega}) = 0$ für alle $f \in A, 1 \leq i_1 < \dots < i_k \leq n$

$d_{k+1} \circ d_k(f\omega) \stackrel{(ii)}{=} d_k(d_{k+1}(df \wedge \omega + fd_k\omega) \stackrel{\text{Eind.}}{=} d_{k+1}(df \wedge \omega) = d_{k+1}((\sum_{i=1}^n \partial f_i dX_i) \wedge \omega) \stackrel{(*)}{=} \sum_{i=1}^n d(\partial_i f \wedge dX_i \wedge \omega) = \sum_{i=1}^n \sum_{j=1}^n \partial_j(\partial_i f) dX_j \wedge dX_i \wedge \omega = 0$, denn es ist $\partial_j(\partial_i f) = \partial_i(\partial_j f)$ für alle i und j und $dX_i \wedge dX_j = -dX_j \wedge dX_i$ für alle i und j .

2. Fall A beliebige R -Algebra.

Schreibe A als Faktoralgebra eines Polynomrings P (in eventuell unendlich vielen Variablen).

vornehm: Es gibt einen surjektiven R -Algebren-Homomorphismus $\varphi : P \rightarrow A$.

Ω ist Funktor, Λ^i auch, φ induziert also einen Homomorphismus $\varphi_i : \Omega_P^i \rightarrow \Omega_A^i$.

$$\begin{array}{ccc} \Omega_P^i & \xrightarrow{d_{i,P}} & \Omega_P^{i+1} \\ \downarrow \varphi_i & & \downarrow \varphi_{i+1} \\ \Omega_A^i & \xrightarrow{d_{i,A}} & \Omega_A^{i+1} \end{array}$$

Es gilt:

- $\text{Kern}(\varphi_i) \subseteq \text{Kern}(\varphi_{i+1} \circ d_{i,P})$
- φ_i surjektiv (Ü4A3a für $i = 1$)

Dann induziert $d_{i,P}$ eine Abbildung $d_{i,A} : \Omega_A^i \rightarrow \Omega_A^{i+1}$.

Die Eigenschaften (i) und (ii) werden „vererbt“.

Beispiele

$A = K[X_1, \dots, X_n], \text{char}(K) = 0$.

Beh.: $H_{dR}^i(A) = 0$ für alle $i > 0$.

Bew.: $i = n$: Ü4A2

$i > n$: $\Omega_A^i = 0$

$i = 1$: Sei $\omega = \sum_{\nu=1}^n f dX_\nu \in \text{Kern}(d_1)$, also: $0 = \sum_{\nu=1}^n df_\nu \wedge dX_\nu = \sum_{\nu=1}^n \sum_{\mu=1}^n \frac{\partial f_\nu}{\partial X_\mu} dX_\mu \wedge dX_\nu$

Für alle $\nu \neq \mu$ ist also $\frac{\partial f_\nu}{\partial X_\mu} = \frac{\partial f_\mu}{\partial X_\nu}$ (da $dX_\mu \wedge dX_\nu = -dX_\nu \wedge dX_\mu$).

Zu zeigen: $\omega = df$ für ein $f \in A$, d.h. $f_\nu = \frac{\partial f}{\partial X_\nu}, \nu = 1, \dots, n$.

Schreibe $f_\nu = \sum_{\underline{i}} a_{\underline{i}}^{(\nu)} X_1^{i_1} \dots X_n^{i_n}$.

Ansatz: $f = \sum_{\underline{i}} a_{\underline{i}} X_1^{i_1} \dots X_n^{i_n} \Rightarrow \frac{\partial f}{\partial X_\nu} = \sum_{\underline{i}=(i_1, \dots, i_n), i_\nu \geq 1} a_{\underline{i}} X_1^{i_1} \dots X_n^{i_n}$

Wähle also $a_{\underline{i}}$ so, dass $i_\nu \cdot a_{\underline{i}} = a_{\underline{i}-e_\nu}^{(\nu)}, e_\nu = (0, \dots, 0, \underbrace{1}_\nu, 0, \dots, 0)$

Es bleibt zu zeigen: $\frac{1}{i_\nu} a_{\underline{i}-e_\nu}^{(\nu)} = \frac{1}{i_\mu} a_{\underline{i}-e_\mu}^{(\mu)}$ für alle $\nu \neq \mu$.

Äquivalent: (*) $i_\mu \cdot a_{\underline{i}-e_\nu}^{(\nu)} = i_\nu \cdot a_{\underline{i}-e_\mu}^{(\mu)}$

Beweis von (*): $\sum_{\underline{i}} i_\mu a_{\underline{i}-e_\nu} X^{i-e_\nu-e_\mu} = \sum_{\underline{i}, i_\mu \geq 1} i_\mu a_{\underline{i}}^{(\nu)} X^{i-e_\mu} = \sum_{\underline{i}, i_\nu \geq 1} i_\nu a_{\underline{i}}^{(\mu)} X^{i-e_\nu}$

$= \sum_{\underline{i}} i_\nu a_{\underline{i}-e_\nu}^{(\mu)} X^{i-e_\nu-e_\mu}$, da $\frac{\partial f_\nu}{\partial X_\mu} = \frac{\partial f_\mu}{\partial X_\nu}$.

Beispiele

$A = K[X, X^{-1}] = K[X, Y]/(XY - 1) = \{f = \sum_{\nu=-n_0}^{n_1} a_\nu X^\nu : a_\nu \in K, n_0, n_1 \in \mathbb{N}\}$

$\Omega_A = AdX, df = (\sum_{\nu \neq 0} \nu a_\nu X^{\nu-1})dX \Rightarrow \Omega^2 = 0 \Rightarrow \text{Bild}(d) = \{fdx : f \in A, a_{-1} = 0\}$, d.h.

$H_{dR}^1(A) = K \frac{dx}{x}$

Kapitel 2

Noethersche Ringe und Moduln

§1 Der Hilbertsche Basissatz

Definition 2.1

Sie R ein (kommutativer) Ring (mit Eins), M ein R -Modul.

- (a) M erfüllt die **aufsteigende Kettenbedingung** (ACC), wenn jede aufsteigende Kette von Untermoduln stationär wird. D.h. sind $(M_i)_{i \in \mathbb{N}}$ Untermoduln von M mit $M_i \subseteq M_{i+1}$ für alle i , so gibt es ein $n \in \mathbb{N}$ mit $M_i = M_n$ für alle $i > n$.
- (b) M heißt **noethersch**, wenn M (ACC) erfüllt.
- (c) R heißt **noethersch**, wenn er als R -Modul noethersch ist.

Beispiele

- 1.) k Körper, ein k -Vektorraum ist noethersch $\Leftrightarrow \dim_k(V) < \infty$
[k hat nur die Ideale $\{0\}, k$.]
- 2.) $R = \mathbb{Z}$
[alle Untermodule: $n\mathbb{Z}$, mit $\text{ggT}(n, m)$ zusammenbauen]
- 3.) $R = k[X]$
[Ideale von einem Polynom erzeugt, um größer zu machen: ggT der Polynome nehmen.]

Bemerkung 2.2

Sei $0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$ kurze exakte Sequenz von R -Moduln. Dann gilt:

$$M \text{ noethersch} \Leftrightarrow M' \text{ und } M'' \text{ noethersch}$$

Beweis

“ \Rightarrow “:

- (i) $M'_0 \subseteq M'_1 \subseteq \dots \subseteq M'_i \subseteq \dots$ Kette von Untermoduln von M' $\Rightarrow \alpha(M'_0) \subseteq \alpha(M'_1) \subseteq \dots$
wird stationär $\xrightarrow{\alpha \text{ injektiv}} M'_0 \subseteq M'_1 \subseteq \dots$ wird stationär.
- (ii) Sei $M''_0 \subseteq M''_1 \subseteq \dots \subseteq M''_i \subseteq \dots$ Kette von Untermoduln von M'' $\Rightarrow \beta^{-1}(M''_0) \subseteq \beta^{-1}(M''_1) \subseteq \dots \subseteq \beta^{-1}(M''_i) \subseteq \dots$ wird stationär $\Rightarrow \underbrace{\beta(\beta^{-1}(M''_0))}_{=M''_0} \subseteq \dots \subseteq \underbrace{\beta(\beta^{-1}(M''_i))}_{=M''_i} \subseteq \dots$
... wird stationär, da β surjektiv ist.

“ \Leftarrow “:

Sei $M_0 \subseteq M_1 \subseteq \dots \subseteq M_i \subseteq \dots$ Kette von Untermoduln von M . Sei $M'_i := \alpha^{-1}(M_i)$, $M''_i := \beta(M_i)$.

Nach Voraussetzung gibt es $n \in \mathbb{N}$, so dass für $i \geq n$ gilt: $M'_i \cong M'_n$, $M''_i \cong M''_n$. Weiter gilt:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'_n & \xrightarrow{\alpha} & M_n & \xrightarrow{\beta} & M''_n \longrightarrow 0 & \text{ist exakt} \\ & & \parallel & & \downarrow \gamma & & \parallel & \\ \text{für ein } i \geq n & & 0 & \longrightarrow & M'_i & \xrightarrow{\alpha} & M_i & \xrightarrow{\beta} & M''_i \longrightarrow 0 & \text{ist exakt} \end{array}$$

γ injektiv (Einbettung).

Zu zeigen: γ surjektiv.

Sei $x \in M_i$, dazu gibt es ein $y \in M_n$ mit $\beta(y) = \beta(x) \Rightarrow z := y - x \in \text{Kern}(\beta) = \text{Bild}(\alpha) = \alpha(M'_i) = \alpha(M'_n) \Rightarrow x = \gamma(y - z)$ und $y - z \in M_n$.

Folgerung 2.3

Jeder endlich erzeugbare Modul über einem noetherschen Ring ist noethersch.

Beweis

1. Fall: F freier Modul vom Rang n .

Induktion über n .

$n = 1$: Dann ist $F \cong R$ als R -Modul, also noethersch nach Voraussetzung.

$n \geq 1$: Sei e_1, \dots, e_n Basis von F . Dann ist $F \cong \bigoplus_{i=1}^n R \cdot e_i$. Dann ist $0 \rightarrow \bigoplus_{i=1}^{n-1} R \cdot e_i \rightarrow F \rightarrow R \cdot e_n \rightarrow 0$ exakt. Nach Induktionsvoraussetzung ist $\bigoplus_{i=1}^{n-1} R \cdot e_i$ noethersch, $R \cdot e_n$ ist nach Voraussetzung noethersch $\xrightarrow{2.2}$ F noethersch.

2. Fall: M werde erzeugt von x_1, \dots, x_n . Dann gibt es (genau) einen surjektiven R -Modulhomomorphismus $\beta : \bigoplus_{i=1}^n R \cdot e_i \rightarrow M$ mit $\beta(e_i) = x_i \xrightarrow{2.2}$ M noethersch.

Proposition 2.4

Sei R ein Ring.

(a) Für einen R -Modul M sind äquivalent:

- (i) M ist noethersch
- (ii) jede nichtleere Teilmenge von Untermoduln von M hat ein (bzgl. \subseteq) maximales Element.
- (iii) jeder Untermodul von M ist endlich erzeugt.

(b) R ist genau dann noethersch, wenn jedes Ideal in R endlich erzeugbar ist.

Beweis

(a) **(i) \Rightarrow (ii):** Sei $\emptyset \neq \mathcal{M}$ eine Familie von Untermoduln von M . Sei $M_0 \in \mathcal{M}$. Ist M_0 nicht maximal, so gibt es ein $M_1 \in \mathcal{M}$ mit $M_0 \subsetneq M_1$. Ist M_1 nicht maximal, so gibt es ein $M_2 \in \mathcal{M}$ mit $M_1 \subsetneq M_2$

Die Kette $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots$ muss stationär werden, d.h. $\exists n$ mit M_n ist maximal in \mathcal{M} .

(ii) \Rightarrow (iii): Sei $N \subseteq M$ ein Untermodul, \mathcal{M} Familie der endlich erzeugbaren Untermoduln von N . $\mathcal{M} \neq \emptyset$, da $\{0\} \in \mathcal{M}$. Nach Voraussetzung enthält \mathcal{M} ein maximales Element

N_0 . Wäre $N_0 \neq N$ so gäbe es ein $x \in N \setminus N_0$. Dann wäre der von N_0 und x erzeugte Untermodul $N_1 \subset N$ endlich erzeugt und $N_0 \subsetneq N_1$. Widerspruch zu N_0 maximal.

(iii) \Rightarrow (i): Seien $M_0 \subseteq M_1 \subseteq \dots \subseteq M_i \subseteq \dots$ Untermoduln von M . Sei $N := \bigcup_{i \geq 0} M_i$. N ist Untermodul \checkmark .

N ist nach Voraussetzung endlich erzeugt, z.B. von x_1, \dots, x_n . Jedes x_k liegt in einem $M_{i(k)}$, also liegen alle in M_m mit $m = \max\{i(k) : k = 1, \dots, n\} \Rightarrow N = M_m \Rightarrow M_i = M_m$ für $i \geq m$.

(b) ist Spezialfall von (a) für $R = M$.

Satz 4 (Hilbert'scher Basissatz)

Ist R noetherscher Ring, so ist auch $R[X]$ noethersch.

Beweis

Sei \mathcal{J} ein nicht endlich erzeugbares Ideal in $R[X]$.

Sei $(f_\nu)_{\nu \in \mathbb{N}}$ Folge in \mathcal{J} wie folgt: f_1 sei maximales Element in $\mathcal{J} \setminus \{0\}$ von minimalen Grad. Für $\nu \geq 2$ sei f_ν ein Element in $\mathcal{J} \setminus \underbrace{(f_1, \dots, f_{\nu-1})}_{=: \mathcal{J}_\nu}$ von minimalen Grad.

Nach Voraussetzung ist $\mathcal{J}_\nu \neq \mathcal{J}$ für alle ν . Für $d_\nu := \deg(f_\nu)$ gilt $d_\nu \leq d_{\nu+1}$.

Sei $a_\nu \in R$ der Leitkoeffizient von f_ν (d.h. $f_\nu = a_\nu X^{d_\nu} + \dots$). Sei I_ν das von $a_1, \dots, a_{\nu-1}$ in R erzeugte Ideal $\Rightarrow I_\nu \subseteq I_{\nu+1} \Rightarrow \exists n$ mit $I_{n+1} = I_n \Rightarrow \exists \lambda_1, \dots, \lambda_{n-1} \in R$ mit $a_n = \sum_{i=1}^{n-1} \lambda_i a_i$.

Setze $g := f_n - \sum_{i=1}^{n-1} \lambda_i f_i X^{d_n - d_i} \Rightarrow g \notin \mathcal{J}_n$ (sonst wäre $f_n \in \mathcal{J}_n$) aber $\deg(g) < d_n = \deg(f_n)$ Widerspruch.

Folgerung 2.5

Sie R noetherscher Ring. Dann gilt:

- (a) $R[X_1, \dots, X_n]$ ist noethersch für jedes $n \in \mathbb{N}$
- (b) Jede endlich erzeugte R -Algebra A ist noethersch (als Ring)

Beweis

(a) $n = 1$: Satz 4

$n > 1$: $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$

(b) Es gibt surjektiven R -Algebra-Homomorphismus $\varphi : R[X_1, \dots, X_n] \rightarrow A \xrightarrow{(a), 2.3} A$ ist noethersch als $R[X_1, \dots, X_n]$ -Modul. Sei $I_0 \subseteq I_1 \subseteq \dots \subseteq I_k \subseteq \dots$ Kette von Idealen in A . Jedes I_k ist $R[X_1, \dots, X_n]$ -Modul \Rightarrow Die Kette wird stationär

§2 Ganze Ringerweiterungen

Definition 2.6

Sei S/R eine Ringerweiterung (d.h. $R \subseteq S$).

- (a) $b \in S$ heißt **ganz** über R , wenn es ein **normiertes** Polynom $f \in R[X]$ gibt mit $f(b) = 0$.
- (b) S heißt **ganz** über R , wenn jedes $b \in S$ ganz über R ist.

Beispiele

$\sqrt{2} \in \mathbb{R}$ ist ganz über \mathbb{Z} .

$\frac{1}{2} \in \mathbb{Q}$ ist nicht ganz über \mathbb{Z} (Nullstelle von $2X - 1$).

Proposition 2.7

Sei S/R Ringerweiterung. Für $b \in S$ sind äquivalent:

- (i) b ist ganz über R .
- (ii) $R[b]$ ist endlich erzeugbarer R -Modul.
- (iii) $R[b]$ ist enthalten in einem Unterring $S' \subseteq S$, der als R -Modul endlich erzeugt ist.

Beweis

(i) \Rightarrow (ii): Nach Voraussetzung gibt es $a_0, \dots, a_{n-1} \in R$, sodass $b^n = a_{n-1}b^{n-1} + \dots + a_0$
 $\Rightarrow b^n$ ist in dem von $1, b, \dots, b^{n-1}$ erzeugtem R -Untermodul von S enthalten.

$\Rightarrow b^{n+1} = a_{n-1}b^n + \dots + a_0b = a_{n-1}(\sum_{i=0}^{n-1} a_i b^i) + \dots + a_0b \in M$

Induktion $\Rightarrow b^k \in M$ für alle $k \geq 0 \Rightarrow M = R[b]$

(iii) \Rightarrow (i): S' werde als R -Modul von s_1, \dots, s_n erzeugt $\Rightarrow b \cdot s_i \in S'$, d.h. $b \cdot s_i = \sum_{k=1}^n a_{ik} s_k$
 für $i = 1, \dots, n \Rightarrow \sum_{k=1}^n (a_{ik} - \delta_{ik} \cdot b) \cdot s_k = 0$ für $i = 1, \dots, n$.

Für die Matrix $A = (a_{ik} - \delta_{ik} \cdot b)_{i,k=1,\dots,n} \in S^{n \times n}$ gilt also $A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0$. $\det(A)$ ist normiertes

Polynom in b vom Grad n mit Koeffizienten in R

Beh.: $\det(A) = 0$.

Bew.: Cramersche Regel:

$A^\# := (b_{ij})$ mit $b_{ij} = (-1)^{i+j} \det(A'_{ji})$, $i, j = 1, \dots, n$ wobei A'_{ji} durch Streichen der j -ten Zeile und der i -ten Spalte aus A hervor geht.

$A \cdot A^\# = (c_{ik})$ mit $c_{ik} = \sum_{j=1}^n a_{ij} b_{jk} = \sum_{j=1}^n a_{ij} (-1)^{j+k} \det(A'_{kj}) = \begin{cases} i = k : \det(A) \text{ (Laplace)} \\ i \neq k : \det(A'_k) = 0 \end{cases}$

$\det(A'_k) = 0$: in der k -ten Zeile steht $a_{i1}, \dots, a_{in} \Rightarrow i$ -te und k -te Zeile sind gleich.

$\Rightarrow A \cdot A^\# = \det(A) \cdot E_n = A^\# \cdot A \Rightarrow 0 = A^\# \cdot A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \det(A) \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \Rightarrow \det(A) \cdot s_i = 0$ für

$i = 1, \dots, n$. Da $1 \in S'$, gibt es $\lambda_i \in R$ mit $1 = \sum_{i=1}^n \lambda_i s_i \Rightarrow \det(A) \cdot 1 = \sum_{i=1}^n \lambda_i \cdot \det(A) \cdot s_i = 0 \Rightarrow \det(A) = 0$.

Proposition 2.8

Ist S/R Ringerweiterung, so ist $\bar{R} := \{b \in S : b \text{ ganz über } R\}$ ein Unterring von S .

Beweis

Seien $b_1, b_2 \in \bar{R}$.

Zu zeigen: $b_1 \pm b_2, b_1 \cdot b_2 \in \bar{R}$

Nach 2.7 genügt es zu zeigen: $R[b_1, b_2]$ ist endlich erzeugt als R -Modul.

Dazu: $R[b_1]$ ist endlich erzeugt als R -Modul (von x_1, \dots, x_n) nach 2.7. $R[b_1, b_2] = (R[b_1])[b_2]$ ist endlich erzeugt als $R[b_1]$ -Modul (von y_1, \dots, y_m). Dann erzeugen die $x_i y_j$ $R[b_1, b_2]$ als R -Modul.

Definition 2.9

Sei S/R Ringerweiterung.

- (a) \bar{R} (wie in 2.8) heißt der **ganze Abschluss** von R in S .
- (b) Ist $R = \bar{R}$, so heißt R **ganz abgeschlossen** in S .
- (c) Ein nullteilerfreier Ring R heißt **normal**, wenn er ganz abgeschlossen in $\text{Quot}(R)$ ist.
- (d) Ist R nullteilerfrei, so heißt der ganze Abschluss \bar{R} von R in $\text{Quot}(R)$ die **Normalisierung** von R .

Bemerkung 2.10

Jeder faktorielle Ring ist normal.

Beweis

Sei $K = \text{Quot}(R), x = \frac{a}{b} \in K^\times, a, b \in R$ teilerfremd. Sei x ganz über R . Dann gibt es $\alpha_0, \dots, \alpha_{n-1} \in R$ mit $x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_0 = 0 \stackrel{!}{\Rightarrow} a^n + \alpha_{n-1}ba^{n-1} + \dots + \alpha_1b^{n-1}a + \alpha_0b^n = 0 \Rightarrow b \mid a^n$ Widerspruch zu teilerfremd. $\Rightarrow x \in R \Rightarrow R$ normal.

§3 Der Hilbert'sche Nullstellensatz

Satz 5 (Hilbert'scher Nullstellensatz)

Sei K ein Körper und \mathfrak{m} ein maximales Ideal in $K[X_1, \dots, X_n]$.

Dann ist $L := K[X_1, \dots, X_n]_{\mathfrak{m}}$ eine algebraische Körpererweiterung von K .

Beweis

Für $n = 1$ ist das aus Algebra I bekannt. Nimm das als Induktionsanfang einer vollständigen Induktion nach n .

L wird als K -Algebra erzeugt von den Restklassen x_1, \dots, x_n der X_1, \dots, X_n . Wenn x_1, \dots, x_n algebraisch über K sind, so auch L . Wir nehmen an, dass sei nicht der Fall, sei also ohne Einschränkung x_1 transzendent über K .

Da L Körper, liegt $K' := K(x_1)$ in L , so dass $L \subset K'[X_1, \dots, X_n]$ ein Faktoring von $K'[X_1, \dots, X_n]$ nach einem maximalen Ideal ist.

$\stackrel{!}{\Rightarrow} x_2, \dots, x_n$ sind algebraisch über $K' \Rightarrow \exists a_{i\nu} \in K' = K(x_1)$ mit $x_i^{n_i} + \sum_{\nu=0}^{n_i-1} a_{i\nu}x_i^\nu = 0$ für $i = 2, \dots, n$. Nennen wir den Hauptnenner der $a_{i\nu}$ von nun $b \in K[X_1] \Rightarrow x_2, \dots, x_n$ sind ganz über $K[x_1, b^{-1}] =: R$.

Beh.: R ist Körper.

denn: Sei $a \in R \setminus \{0\}$ und a^{-1} das Inverse von a in L . Da L ganz über R ist, gibt es $\alpha_0, \dots, \alpha_{m-1} \in R$ mit $(a^{-1})^m + \sum_{i=0}^{m-1} \alpha_i(a^{-1})^i = 0 \stackrel{!}{\Rightarrow} 1 = -\sum_{i=0}^{m-1} \alpha_i a^{m-i} = a(-\sum_{i=0}^{m-1} \alpha_i a^{m-i-1}) \Rightarrow R$ ist Körper \Rightarrow Widerspruch! R kann niemals Körper sein.

Definition 2.11

Sei $I \trianglelefteq K[X_1, \dots, X_n]$ ein Ideal. Dann heißt die Teilmenge $V(I) \subseteq K^n$, die durch

$$V(I) := \{(x_1, \dots, x_n) \in K^n : f(x_1, \dots, x_n) = 0 \forall f \in I\}$$

bestimmt ist, die **Nullstellenmenge** von I in K^n .

Beispiele

- 1.) aus der LA bekannt: affine Unterräume des K^n sind Nullstellenmenge von linearen Polynomen.
- 2.) Anschaulicher Spezialfall von 1.):
Punkte in $K^n : (x_1, \dots, x_n) : V(X_1 - x_1, X_2 - x_2, \dots, X_n - x_n)$.

Bemerkung + Definition 2.12

(a) Für 2 Ideale $I_1 \subseteq I_2$ gilt $V(I_1) \supseteq V(I_2)$.

(b) Definiert man für eine beliebige Teilmenge $V \subseteq K^n$ das **Verschwundungsideal** von V durch

$$I(V) := \{f \in K[X_1, \dots, X_n] : f(x_1, \dots, x_n) = 0 \forall (x_1, \dots, x_n) \in V\},$$

so gilt $V \subseteq V(I(V))$;

ist V bereits Nullstellenmenge $V(I)$ eines Ideals I von $K[X_1, \dots, X_n]$,

so gilt sogar $V = V(I(V))$.

Beweis

(a) Sei $x \in V(I_2) \Rightarrow f(x) = 0 \forall f \in I_2 \supseteq I_1 \Rightarrow x \in V(I_1)$

(b) " \subseteq ": Definition von V und I

" \supseteq ": Sei $V = V(I)$ für $I \trianglelefteq K[X_1, \dots, X_n]$. Nach Definition $I \subseteq I(V) \stackrel{(a)}{\Rightarrow} V(I(V)) \subseteq V(I) = V$

Satz (Schwacher Nullstellensatz)

Ist K algebraisch abgeschlossen, so ist für jedes echte Ideal $I \trianglelefteq K[X_1, \dots, X_n] : V(I) \neq \emptyset$.

Beweis

Sei $I \trianglelefteq K[X_1, \dots, X_n]$ echtes Ideal. Nach Algebra I gibt es dann maximales Ideal $\mathfrak{m} \supseteq I$. Weiter gilt: $V(\mathfrak{m}) \subseteq V(I)$, so können wir ohne Einschränkung annehmen, dass $I = \mathfrak{m}$ maximal ist.

Nach Satz 5 ist $K[X_1, \dots, X_n]/\mathfrak{m}$ eine algebraische Körpererweiterung von K .

Da K algebraisch abgeschlossen $\Rightarrow K[X_1, \dots, X_n]/\mathfrak{m} \cong K$.

Seien nun x_i die Restklasse von X_i in $K[X_1, \dots, X_n]/\mathfrak{m}$ und $x = (x_1, \dots, x_n)$.

Für $f \in K[X_1, \dots, X_n]$ ist $f(x) = f(\bar{X}_1, \dots, \bar{X}_n) = \bar{f} \pmod{\mathfrak{m}} \Rightarrow f(x) = 0 \forall f \in I \Rightarrow x \in V(I)$.

Satz (Starker Nullstellensatz)

Ist K algebraisch abgeschlossen, so gilt für jedes Ideal $I \trianglelefteq K[X_1, \dots, X_n]$:

$$I(V(I)) = \{f \in K[X_1, \dots, X_n] : \exists d \geq 1 : f^d \in I\} =: \sqrt{I}$$

Beweis (Rabinovitsch-Trick)

Sei $g \in I(V(I))$ und f_1, \dots, f_m Idealerzeuger von $I \trianglelefteq K[X_1, \dots, X_n]$.

Zu zeigen: $\exists d \geq 1$ mit $g^d = \sum_{i=1}^m a_i f_i$ für irgendwelche a_i .

Sei $J \subseteq K[X_1, \dots, X_n, X_{n+1}]$ das von $f_1, \dots, f_m, gX_{n+1} - 1$ erzeugte Ideal.

Beh.: $V(J) = \emptyset$

Bew.: Sei $x = (x_1, \dots, x_n, x_{n+1}) \in V(J)$. Dann ist $f_i(x') = 0$ für $x' = (x_1, \dots, x_n)$ und $i = 1, \dots, m \Rightarrow x' \in V(I)$.

Nach Wahl von $g \in I(V(I))$ ist also $g(x') = 0$

$\Rightarrow (gX_{n+1} - 1)(x) = g(x')x_{n+1} - 1 = -1 \neq 0. \Rightarrow V(J) = \emptyset.$

Nach schwachen Nullstellensatz ist $J = K[X_1, \dots, X_{n+1}]$

$\Rightarrow \exists b_1, \dots, b_m$ und $b \in K[X_1, \dots, X_{n+1}]$ mit $\sum_{i=1}^m b_i f_i + b(gX_{n+1} - 1) = 1.$

Sei $R := K[X_1, \dots, X_{n+1}]/(gX_{n+1} - 1) \cong K[X_1, \dots, X_n][\frac{1}{g}]$. Unter dem Isomorphismus werden die f_i auf sich selbst, die b_i auf $\tilde{b}_i \in R$ abgebildet $\Rightarrow \sum_{i=1}^m \tilde{b}_i f_i = 1$ in R . Multipliziere mit dem Hauptnenner g^d der $\tilde{b}_i \Rightarrow \sum_{i=1}^m \underbrace{(g^d \tilde{b}_i)}_{\in K[X_1, \dots, X_n]} f_i = g^d \Rightarrow I(V(I)) \subseteq \sqrt[d]{I}.$

" \supseteq ": klar.

§4 Graduierte Ringe und Moduln

Definition + Bemerkung 2.13

- (a) Ein Ring S zusammen mit einer Zerlegung $S = \bigoplus_{i \geq 0} S_i$ in abelsche Gruppen S_i heißt **graduierter Ring**, wenn für alle $i, j \in \mathbb{N}$:

$$S_i \cdot S_j \subseteq S_{i+j}$$

- (b) Ist $S = \bigoplus_{i \geq 0} S_i$ graduierter Ring, so heißen die Elemente von S_i **homogen** vom Grad i .
Für $f = \sum_{i=0}^{\infty} f_i$ heißen die f_i die homogenen Komponenten von f .
- (c) Ist $S = \bigoplus_{i \geq 0} S_i$ graduierter Ring, so ist S_0 Unterring mit $1 \in S_0$.

Beweis

- (c) $S_0 \cdot S_0 \subseteq S_{0+0} = S_0$

Sei $1 = \sum_{i \geq 0} e_i$ mit $e_i \in S_i$. Sei $f \in S_n$ mit $n \geq 1, f \neq 0. \Rightarrow f = f \cdot 1 = \sum_{i \geq 0} f e_i$ mit $f \cdot e_i \in S_{n+i}$. Da f nur auf eine Weise als Summe von homogenen Elementen geschrieben werden kann, ist $e_i = 0$ für $i \geq 0$ und $e_0 = 1$.

Definition + Bemerkung 2.14

Sei $S = \bigoplus_{i \geq 0} S_i$ graduierter Ring.

- (a) Ein Ideal $I \subseteq S$ heißt **homogen**, wenn es von homogenen Elementen erzeugt wird.
- (b) Ein Ideal $I \subseteq S$ ist genau dann homogen, wenn für jedes $f \in I, f = \sum_{i \geq 0} f_i$ ($f_i \in S_i$) gilt: $f_i \in I$.
- (c) Sei $I \subseteq S$ homogenes Ideal, erzeugt von homogenen Elementen $(h_\nu)_{\nu \in J}$. Dann hat jedes homogene $f \in I$ eine Darstellung $f = \sum_{\nu} g_\nu h_\nu$ mit g_ν homogen.
- (d) Ist I homogenes Ideal in S , so ist S/I graduierter Ring mit $(S/I)_i = S_i / (I \cap S_i)$

Beweis

(b) “ \Leftarrow ”: \checkmark

“ \Rightarrow ”: Sei $(h_\nu)_{\nu \in J}$ homogenes Erzeugendensystem von I , $f \in I$. Dann gibt es $g_\nu \in S$ mit $f = \sum_\nu g_\nu h_\nu$. Sei $g_\nu = \sum_{i \geq 0} g_{\nu,i}$ Zerlegung in homogene Komponenten.

$\Rightarrow f = \sum_{\nu,i} g_{\nu,i} h_\nu \Rightarrow f_i = \sum_\nu g_{\nu,i - \deg f_\nu} h_\nu$ (mit $g_{\nu,j} = 0$ für $j < 0$) $\Rightarrow f_i \in I$

(d) $\varphi : S = \bigoplus_{i \geq 0} S_i \rightarrow \bigoplus_{i \geq 0} S_i / (I \cap S_i)$ ist surjektiver Ringhomomorphismus. Kern(φ) wird erzeugt von $I \cap S_i$, $i \geq 0$. Da I homogen, ist Kern(φ) = I . Aus dem Homomorphiesatz folgt dann: $S/I \cong \bigoplus_{i \geq 0} S_i / (I \cap S_i)$

Beispiele

(1) $S = k[X, Y]$, $I = (Y - X^2)$ ist *nicht* homogen. $S/I \cong k[X]$, $\bigoplus_i S_i / (I \cap S_i) = \bigoplus_i S_i = S$, da I keine homogenen Elemente enthält.

(2) $S_+ := \bigoplus_{i > 0} S_i$ ist homogenes Ideal.

Ist S_0 Körper, so ist S_+ das einzige maximale homogene Ideal.

(3) $S = k[X, Y]$, $\deg(X) = 1$, $\deg(Y) = 2$. Dann ist $I = (Y - X^2)$ homogenes Ideal!

Definition + Bemerkung 2.15

Für einen graduierten Ring $S = \bigoplus_{i \geq 0} S_i$ sind äquivalent:

(i) S noethersch.

(ii) S_0 ist noethersch und S_+ endlich erzeugbares Ideal.

(iii) S_0 ist noethersch und S ist endlich erzeugbare S_0 -Algebra.

Beweis

„(i) \Rightarrow (ii)“: $S_0 \cong S/S_+$; S_+ endlich erzeugbar, da S noethersch. S_0 also noethersch.

„(iii) \Rightarrow (i)“: $S \cong \underbrace{S_0[X_1, \dots, X_n]}_{\text{noethersch nach Satz 4}} / I$ für ein $n \geq 0$ und ein Ideal $I \subset S_0[X_1, \dots, X_n]$. S ist

also noethersch.

„(ii) \Rightarrow (iii)“: Sei f_1, \dots, f_r homogenes Erzeugersystem von S_+ , $S' := S_0[f_1, \dots, f_r] \subset S$ die von den f_i erzeugte S_0 -Unteralgebra von S .

Beh.: $S' = S$

Zeige dazu: $S_i \subset S'$ für alle i .

Beweis der Behauptung durch Induktion über i :

$i = 0$: \checkmark

$i > 0$: $g \in S_i \stackrel{2.14(c)}{\Rightarrow} g = \sum_{\nu=1}^r g_\nu f_\nu$ mit $g_\nu \in S_{i - \deg(f_\nu)}$

$f_\nu \in S_+ \Rightarrow \deg(f_\nu) > 0 \Rightarrow i - \deg f_\nu < i \stackrel{\text{I.V.}}{\Rightarrow} g_\nu \in S'$, also ist $g \in S'$

Definition + Bemerkung 2.16

Sei $S = \bigoplus_{i \geq 0} S_i$ graduiertes Ring.

(a) Ein **graduierter** S -Modul ist ein S -Modul M zusammen mit einer Zerlegung $M = \bigoplus_{i \in \mathbb{Z}} M_i$ in abelsche Gruppen M_i , sodass für alle $i \in \mathbb{N}, j \in \mathbb{Z}$ gilt:

$$S_i \cdot M_j \subseteq M_{i+j}$$

- (b) Eine S -lineare Abbildung $\varphi : M \rightarrow M'$ zwischen graduierten S -Moduln heißt **graderhaltend**, wenn $\varphi(M_i) \subseteq M'_i$ für alle $i \in \mathbb{Z}$
- (c) Ein Ideal $I \subseteq S$ ist homogen $\Leftrightarrow I$ ist als S -Modul graduiert (mit der geerbten Graduierung)
- (d) $\varphi : M \rightarrow M'$ vom Grad $d \Leftrightarrow \varphi(M_i) \subseteq M'_{i+d}$ für alle i .
 Kern(φ) ein graduierter Untermodul.
- (e) Ist $I \subseteq S$ homogenes Ideal, so ist $\varphi : S \rightarrow S/I = \bigoplus_{i \geq 0} S_i / (I \cap S_i)$ graderhaltend.
 Kern(φ) ein graduierter Untermodul.

Beispiele

Sei M graduiertes S -Modul (z.B.: $M = S$). Für $l \in \mathbb{Z}$ sei $M(l)$ der S -Modul M mit der Graduierung $(M(l))_i := M_{l+i}$ (insbes.: $(M(l))_0 = M_l$)

$$S_j(M(l))_i = S_j \cdot M_{l+i} \subseteq M_{j+l+i} = (M(l))_{i+j}$$

$M(l)$ heißt (l -facher) **Twist** von M .

Beweis

- (e) Sei $\varphi : M \rightarrow M'$ lineare Abbildung von S -Moduln vom Grad d . Sei $x \in \text{Kern}(\varphi)$, $x = \sum_{i \in \mathbb{Z}} x_i \Rightarrow 0 = \varphi(x) = \sum_{i \in \mathbb{Z}} \underbrace{\varphi(x_i)}_{\in M'_{i+d}}$ ist Zerlegung in homogene Komponenten $\Rightarrow \varphi(x_i) = 0 \forall i \Rightarrow x_i \in \text{Kern}(\varphi) \forall i \Rightarrow \text{Kern}(\varphi)$ ist graduiert

Beobachtung

Ist $\varphi : M \rightarrow M'$ vom Grad d , so ist $\varphi : M \rightarrow M'(d)$ graderhaltend. Dabei ist $M'(d) = M'$ als S -Modul, aber $(M'(d))_i = M'_{d+i}$. Genauso ist $\varphi : M(-d) \rightarrow M'$ graderhaltend.

Beispiele

$M = S (= k[X_1, \dots, X_n])$, $f \in S$ homogen vom Grad $d \Rightarrow \varphi_f : S \rightarrow S, g \mapsto f \cdot g$ ist linear vom Grad d .

Proposition 2.17

Sei $S = k[X_1, \dots, X_n]$, k ein Körper, $S = \bigoplus_{d=0}^{\infty} S_d$.

$$\dim S_d^{(n)} = \binom{n+d-1}{d} = \frac{1}{(n-1)!} \cdot (n+d-1) \cdots (d+1)$$

Das ist ein Polynom vom Grad $n-1$ in d (mit Leitkoeffizient $\frac{1}{(n-1)!}$).

Beweis

Induktion über n :

$$n = 1: S = k[X], \dim S_d^{(1)} = \binom{d}{d} = 1. \checkmark$$

$$n = 2: S = k[X_1, X_2], \dim S_d^{(2)} = \binom{d+1}{d} = d+1. \checkmark$$

$n > 2$: Induktion über d :

$$d = 0: \dim S_0^{(n)} = \binom{n-1}{0} = 1. \checkmark$$

$$d = 1: \dim S_1^{(n)} = \binom{n}{1} = n. \checkmark$$

$d > 1$: $\dim S_d^{(n)}$ ist die Anzahl der Monome vom Grad d in X_1, \dots, X_n .

In $S_d^{(n)}$ gibt es $\dim S_d^{(n-1)}$ Monome in denen X_n nicht vorkommt und $\dim S_{d-1}^{(n)}$ Monome in denen X_n vorkommt

$$\begin{aligned} \stackrel{\text{I.V.}}{\implies} \dim S_d^{(n)} &= \binom{n+d-2}{d} + \binom{n+d-2}{d-1} = \frac{(n+d-2)!}{(d-1)!(n-2)!} \left(\frac{1}{d} + \frac{1}{n-1} \right) = \frac{(n+d-2)!}{(d-1)!(n-2)!} \frac{n+d-1}{d(n-1)} = \\ &= \frac{(n+d-1)!}{d!(n-1)!} = \binom{n+d-1}{d} \end{aligned}$$

Satz 6 (Hilbert-Polynom)

Sei k ein Körper, $S = k[X_1, \dots, X_n]$, M ein endlich erzeugbarer graduerter S -Modul.

Dann gibt es ein Polynom $P_M \in \mathbb{Q}[T]$ vom Grad $\leq n-1$ und ein $d_0 \in \mathbb{N}$, sodass $P_M(d) = \dim_k M_d$ für alle $d \geq d_0$.

P_M heißt das **Hilbert-Polynom** von M .

Beweis

Induktion über n :

$n = 0$: M ist endlich dimensionaler k -Vektorraum, also $M_d = 0$ für alle $d \gg 0$, $P_M = 0$ tut's.

$n \geq 1$: Sei $\varphi : M \rightarrow M$ die S -lineare Abbildung $x \mapsto X_n x$, φ ist vom Grad 1, $\text{Kern}(\varphi)$ ist also graduerter Untermodul, ebenso ist $\text{Bild}(\varphi)$ graduerter Untermodul, also auch $M/X_n M$.

Dann ist

$$0 \rightarrow \underbrace{K}_{=\text{Kern}(\varphi)} \rightarrow M(-1) \xrightarrow{\varphi} M \rightarrow M/X_n M \rightarrow 0$$

exakte Sequenz von graderhaltenden Homomorphismen zwischen graduierten endlich erzeugbaren S -Moduln.

Beachte: M ist noetherscher Modul, da S noethersch und M endlich erzeugbar, also ist K auch endlich erzeugbar.

Alle $M_d, K_d, (M/X_n M)_d$ sind endlich dimensionale k -Vektorräume \Rightarrow für jedes $d \in \mathbb{Z}$ gilt: $\dim_k K_d - \dim_k M(-1)_d + \dim_k M_d - \dim_k (M/X_n M)_d = 0$ bzw.

$$\dim_k M_d - \dim_k M_{d-1} = \dim_k (M/X_n M)_d - \dim_k K_d$$

Beh.: $M/X_n M$ und K sind (in natürlicher Weise) $k[X_1, \dots, X_{n-1}]$ -Moduln.

Bew.: klar für $M/X_n M$.

für K : Seien y_1, \dots, y_r Erzeuger von K als S -Modul. Sei $y = \sum_{i=1}^r f_i y_i \in K, f_i \in S$. Dann ist ohne Einschränkung $f_i \in k[X_1, \dots, X_{n-1}]$, da $X_n \cdot y = 0$ für alle i .

Nach I.V. gibt es $\tilde{P} \in \mathbb{Q}[T]$ mit $\deg(\tilde{P}) \leq n-2$ und $\tilde{P} = \dim_k (M/X_n M)_d - \dim_k K_d = \dim_k M_d - \dim_k M_{d-1} =: H(d) - H(d-1)$.

Sei $\binom{T}{k} := \frac{1}{k!} T(T-1) \dots (T-k+1) \in \mathbb{Q}[T], \deg \binom{T}{k} = k$.

Schreibe $\tilde{P} = \sum_{k=0}^{n-1} c_k \binom{T}{k}$. Es gilt $\binom{T}{k} - \binom{T-1}{k-1} = \binom{T}{k+1}$. Setze $P_1(T) := \sum_{k=0}^{n-2} c_k \binom{T}{k+1}, \deg(P_1) \leq n-1$ und $P_1(d) - P_1(d-1) = \tilde{P}(d)$. $P_M := P_1 + c$, sodass $P_M(d_0) = \dim_k M_{d_0}$.

Definition 2.18

Sei S endlich erzeugte graduierte k -Algebra, $S_0 = k$, M endlich erzeugbarer graduerter S -Modul. Dann heißt die formale Potenzreihe

$$H_M(t) := \sum_{i=0}^{\infty} (\dim_k M_i) t^i$$

Hilbert-Reihe zu M .

Beispiele

1.) $M = S = k[X] \Rightarrow \dim M_i = 1$ für alle $i \Rightarrow H_M(t) = \sum_{i=0}^{\infty} t^i = \frac{1}{1-t}$.

2.) $M = S = k[X_1, \dots, X_n]$

Beh.: $H_M(t) = \frac{1}{(1-t)^n}$

Bew.: $\frac{1}{(1-t)^n} = \left(\sum_{i=0}^{\infty} t^i\right)^n = \sum_{i=0}^{\infty} c_i t^i$ mit $c_i = \#\text{Partitionen von } i \text{ durch höchstens } n \text{ Summanden} = \text{Anzahl der Monome vom Grad } i \text{ in } X_1, \dots, X_n$.

3.) $M = S = k[Y](\cong k[X^d]), \deg Y = d > 0 \Rightarrow H_M(t) = \sum_{i=0}^{\infty} t^{d \cdot i} = \frac{1}{1-t^d}$

$$\dim M_i = \begin{cases} 1 : & d \mid i \\ 0 : & \text{sonst} \end{cases}$$

Satz (6')

Wie in [Definition 2.18](#) seien S endlich erzeugbare graduierte k -Algebra, M endlich erzeugbarer graduiertes S -Modul.

f_1, \dots, f_r homogene Erzeuger von S als k -Algebra, $d_i := \deg f_i$.

Dann gibt es ein Polynom $F(t) \in \mathbb{Z}[t]$, sodass gilt:

$$H_M(t) = \frac{F(t)}{(1-t^{d_1}) \cdot (1-t^{d_2}) \cdot \dots \cdot (1-t^{d_r})}$$

Beweis

Induktion über r :

$r = 0$: $S = S_0 = k \Rightarrow \dim_k M_i = 0$ für $i \gg 0 \Rightarrow F(t) := H_M(t)$ ist Polynom in $\mathbb{Z}[t]$.

$r > 0$: Multiplikation mit f_r gibt exakte Sequenz von graderhaltenden S -Modul-Homomorphismen:

$$0 \rightarrow K \rightarrow M \xrightarrow{f_r} M(d_r) \rightarrow (M/f_r M)(d_r) \rightarrow 0$$

Wie in Beweis von [Satz 6](#) sind K und $Q := (M/f_r M)$ Moduln über $S' := k[f_1, \dots, f_{r-1}] \subset S \Rightarrow$ für jedes $i \geq 0$ ist

$$\begin{aligned} & -\dim M_i + \dim M_{i+d_r} = \dim Q_{i+d_r} - \dim K_i \\ \Rightarrow & \sum_{i=0}^{\infty} \dim M_{i+d_r} t^{i+d_r} - t^{d_r} \sum_{i=0}^{\infty} \dim M_i t^i = \sum_{i=0}^{\infty} \dim Q_{i+d_r} t^{i+d_r} - t^{d_r} \sum_{i=0}^{\infty} \dim K_i t^i \\ \Rightarrow & H_M(t) - \sum_{i=0}^{d_r-1} \dim M_i t^i - t^{d_r} H_M(t) = H_Q(t) - \sum_{i=0}^{d_r-1} \dim Q_i t^i - t^{d_r} H_K(t) \\ & (1-t^{d_r})H_M(t) = H_Q(t) - t^{d_r} H_K(t) + \sum_{i=0}^{d_r-1} \dim M_i t^i - \sum_{i=0}^{d_r-1} \dim Q_i t^i \end{aligned}$$

Nach Induktionsvoraussetzung gibt es $F_1(t), F_2(t) \in \mathbb{Z}[t]$ mit

$$(1-t^{d_r})H_M(t) = \frac{F_1(t)}{\prod_{i=1}^{r-1} (1-t^{d_i})} - \frac{t^{d_r} F_2(t)}{\prod_{i=1}^{r-1} (1-t^{d_i})} + \underbrace{\sum_{i=0}^{d_r-1} \dim M_i t^i - \sum_{i=0}^{d_r-1} \dim Q_i t^i}_{=: G(t)}$$

\Rightarrow Behauptung mit $F(t) = F_1(t) - t^{d_r} F_2(t) + G(t) \cdot \prod_{i=1}^{r-1} (1-t^{d_i})$

§5 Invarianten endlicher Gruppen

Definition + Bemerkung 2.19

Sei k ein Körper, $n \geq 1$, $k[\mathfrak{X}] := k[X_1, \dots, X_n]$.

Sei $G \subseteq \text{Aut}(k[\mathfrak{X}])$ eine Untergruppe der k -Algebra-Automorphismen.

- (a) $k[\mathfrak{X}]^G := \{f \in k[\mathfrak{X}] : \sigma(f) = f \text{ für alle } \sigma \in G\}$ heißt **Invariantenring** von $k[\mathfrak{X}]$ bezüglich G .
- (b) $k[\mathfrak{X}]^G$ ist k -Algebra.
- (c) G heißt **linear**, wenn jedes $\sigma \in G$ graderhaltend ist. Dann ist $\sigma|_{k[\mathfrak{X}]_1}$ ein k -Vektorraum-Automorphismus und $\sigma \mapsto \sigma|_{k[\mathfrak{X}]_1}$ ist ein Gruppenhomomorphismus $G \rightarrow \text{GL}_n(k)$.

Beispiele

- 1.) $n = 2$, $G = \{id, \sigma\}$ mit $\sigma(X) = Y$, $\sigma(Y) = X \Rightarrow k[X, Y]^G$ wird erzeugt von $X + Y$ und $X \cdot Y$.
 $X^k + Y^k - (X + Y)^k = -X^{k-1}Y - \dots - XY^{k-1} = -XY(X^{k-2} + Y^{k-2}) - \dots$
- 2.) $n = 2$, $G = \{id, \varphi\}$ mit $\varphi(X) = -X$, $\varphi(Y) = -Y$ ($\text{char } k \neq 2$).
 $k[X, Y]^G$ wird erzeugt von X^2, Y^2, XY .

Satz 7 (Endliche Erzeugbarkeit des Invariantenrings)

Seien k , G , $k[\mathfrak{X}]$ wie in Def. 2.19, G linear und endlich.

- (a) (Hilbert) $k[\mathfrak{X}]^G$ ist endlich erzeugbare k -Algebra
- (b) (E. Noether) Ist $m = |G|$, so wird $k[\mathfrak{X}]^G$ von Elementen vom Grad $\leq m$ erzeugt.

Beweis

- (a) Sei $S := k[\mathfrak{X}]^G$ (graduierte Unter algebra von $k[\mathfrak{X}]$).
 $S_+ = \bigoplus_{i>0} S_i$, $I := S_+ k[\mathfrak{X}]$ (Ideal in $k[\mathfrak{X}]$) $\Rightarrow I$ ist endlich erzeugt.
 Seien $f_1, \dots, f_r \in S_+$ homogene Erzeuger von I , $S' := k[f_1, \dots, f_r] \subseteq S$

Beh.: $S = S'$

Bew.: Sei also $f = \sum_{i=0}^n \tilde{f}_i \in S$, $\tilde{f}_i \in S_i$. Zeige mit Induktion: $S_d \subseteq S'$ für jedes $d \geq 0$.

$d = 0$: $S_0 = k = S'_0$

$d \geq 1$: Sei $f \in S_d \Rightarrow f \in S_+ \subseteq I \Rightarrow f = \sum_{i=1}^r g_i f_i$ mit $g_i \in k[\mathfrak{X}]_{d-d_i}$, $d_i = \deg(f_i) \Rightarrow \deg(g_i) < d$

„Mittelung“: Die Abbildung $\varphi : k[\mathfrak{X}] \rightarrow S$, $f \mapsto \frac{1}{|G|} \sum_{\sigma \in G} \sigma(f)$ ist lineare, graderhaltende Projektion.

$\Rightarrow f = \varphi(f) = \sum_{i=1}^r \varphi(g_i) f_i$ mit $\varphi(g_i) \in S$, $\deg(\varphi(g_i)) < d$

Also nach Induktionsvoraussetzung $\varphi(g_i) \in S' \Rightarrow f \in S'$

$\Rightarrow k[f_1, \dots, f_r] \cong k[\mathfrak{X}]^G$

Beispiele

S_n operiert auf $k[X_1, \dots, X_n]$ durch $\sigma(X_i) := X_{\sigma(i)}$. $k[X_1, \dots, X_n]^{S_n}$ sind die symmetrischen Polynome.

Beh.1:

$k[X_1, \dots, X_n]^{S_n}$ wird (als k -Algebra) erzeugt von den „elementarsymmetrischen“ Polynomen:

$$\begin{aligned}
s_1 &:= X_1 + \dots + X_n \\
s_2 &:= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n = \sum_{1 \leq i < j \leq n} X_iX_j \\
s_3 &:= \sum_{1 \leq i < j < k \leq n} X_iX_jX_k \\
&\vdots \\
s_n &:= X_1 \cdot \dots \cdot X_n
\end{aligned}$$

Beh.2: $k[X_1, \dots, X_n]^{S_n}$ wird erzeugt von den Potenzsummen

$$\begin{aligned}
f_1 &= s_1 = \sum X_i \\
f_k &= \sum_{i=1}^n X_i^k, \quad k = 1, \dots, n
\end{aligned}$$

Bemerkung

$\varphi : k[\mathfrak{X}] \rightarrow k[\mathfrak{X}]^G, f \mapsto \frac{1}{|G|} \sum_{\sigma \in G} \sigma(f)$ ist k -lineare graderhaltende Projektion.

Beweis

(b) Sei \tilde{S} die von den $\varphi(X^\nu), |\nu| \leq |G|$ erzeugte Unteralgebra von $k[\mathfrak{X}]^G$. Dabei sei für $\nu = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n : X^\nu := X_1^{\nu_1} \cdot \dots \cdot X_n^{\nu_n}$ und $|\nu| := \sum \nu_i$.

Zu zeigen: $\varphi(X^\nu) \in \tilde{S}$ für alle $\nu \in \mathbb{N}^n$.

Hilfsgröße: Für $d > 0$ sei $F_d := \sum_{\sigma \in G} \underbrace{\left(\sum_{i=1}^n \sigma(X_i) Y_i \right)^d}_{=: Z_\sigma} \in k[X_1, \dots, X_n, Y_1, \dots, Y_n]$

$$F_d = \sum_{\sigma \in G} Z_\sigma \stackrel{G = \{\sigma_1, \dots, \sigma_n\}, |G|=m}{=} \sum_{i=1}^m Z_j \text{ mit } Z_j := Z_{\sigma_j}.$$

Umformungen:

$$(1) F_d = \sum_{\sigma \in G} \sum_{|\nu|=d} \gamma_\nu \sigma(X^\nu) Y^\nu \quad (\text{mit } \gamma_\nu = \frac{d!}{\nu_1! \cdot \dots \cdot \nu_n!}) = \sum_{|\nu|=d} \gamma_\nu (\sum_{\sigma \in G} \sigma(X^\nu) Y^\nu) = \sum_{|\nu|=d} \gamma_\nu m \varphi(X^\nu) Y^\nu.$$

Nach Beh.2 gibt es $a_\mu \in k, \mu \in \mathbb{N}^n$ mit $\sum_{i=1}^m i \mu_i = d$

$$(2) F_d = \sum_{\mu \in \mathbb{N}^m} a_\mu F_1^{\mu_1} \cdot \dots \cdot F_m^{\mu_m} \stackrel{(1)}{=} \sum_{\mu \in \mathbb{N}^m} a_\mu \prod_{j=1}^m (\sum_{|\nu|=j} \gamma_\nu m \varphi(X^\nu) Y^\nu)^{\mu_j} \stackrel{\text{sortieren nach Potenzen von } Y}{=} \sum_{\lambda \in \mathbb{N}^m} P_\lambda(X) Y^\lambda \text{ mit } P_\lambda \in \tilde{S}.$$

Koeffizientenvergleich zwischen (1) und (2) ergibt:

$$P_\lambda = \begin{cases} 0 & , |\lambda| \neq d \\ \gamma_\lambda m \varphi(X^\lambda) & , |\lambda| = d \end{cases}$$

$\Rightarrow \varphi(X^\lambda) \in \tilde{S}$ für alle $\lambda \in \mathbb{N}^m$

Beispiele

$n = 2, G = \langle \sigma \rangle, \sigma(X) = Y, \sigma(Y) = -X \Rightarrow G \cong \mathbb{Z}/4\mathbb{Z}$

Durchrechnen aller Monome mit Grad $\leq |G|$:

$f = id(f)$	$\sigma(f)$	$\sigma^2(f)$	$\sigma^3(f)$	$\sum_{\sigma \in G} \sigma(f) = 4\varphi(f)$
X	Y	$-X$	$-Y$	0
Y	$-X$	$-Y$	X	0
X^2	Y^2	X^2	Y^2	$2(X^2 + Y^2)$
Y^2	X^2	Y^2	X^2	$2(X^2 + Y^2)$
XY	$-YX$	XY	$-YX$	0
X^3	Y^3	$-X^3$	$-Y^3$	0
Y^3	$-X^3$	$-Y^3$	X^3	0
X^2Y	$-XY^2$	$-X^2Y$	XY^2	0
XY^2	X^2Y	$-XY^2$	$-X^2Y$	0
X^4	Y^4	X^4	Y^4	$2(X^4 + Y^4)$
XY^3	$-X^3Y$	XY^3	$-X^3Y$	$2XY(Y^2 - X^2)$
X^2Y^2	X^2Y^2	X^2Y^2	X^2Y^2	$4(X^2Y^2)$

$\Rightarrow k[X, Y]^G$ wird erzeugt von $I_1 = X^2 + Y^2$, $I_2 = X^2Y^2$, $I_3 = XY(X^2 - Y^2)$ (und $I_4 = X^4 + Y^4 = I_1^2 - 2I_2$). Zwischen I_1, I_2, I_3 besteht die Gleichung $I_3^2 = I_2(X^4 + Y^4 - 2X^2Y^2) = I_1(I_1^2 - 4I_2)$

§6 Nakayama, Krull und Artin-Rees

Definition + Bemerkung 2.20

Sei R ein Ring.

(a)

$$\mathcal{J}(R) := \bigcap_{\mathfrak{m} \text{ maximales Ideal in } R} \mathfrak{m}$$

heißt **Jacobson-Radikal** von R .

(b) $\mathcal{J}(R)$ ist Radikalideal.

(c) Für jedes $a \in \mathcal{J}(R)$ ist $1 - a$ eine Einheit in R .

Beweis

(b) Sei $x \in R$, $x^n \in \mathcal{J}(R)$; zu zeigen: $x \in \mathcal{J}(R)$.

Sei \mathfrak{m} maximales Ideal von R , dann ist $x^n \in \mathfrak{m} \xrightarrow{\mathfrak{m} \text{ prim}} x \in \mathfrak{m} \Rightarrow x \in \mathcal{J}(R)$

(c) Ist $1 - a \notin R^\times$, so gibt es ein maximales Ideal \mathfrak{m} mit $1 - a \in \mathfrak{m}$,
aber: a ist auch $\in \mathfrak{m}$, also auch $1 = 1 - a + a \in \mathfrak{m} \Rightarrow$ Widerspruch.

Beispiele

$$\mathcal{J}(\mathbb{Z}) = 0, \quad \mathcal{J}(k[X]) = 0$$

R lokaler Ring $\Rightarrow \mathcal{J}(R) = \mathfrak{m}$ (es gibt nur ein maximales Ideal in R)

Satz 8 (Lemma von Nakayama)

Sei R ein Ring, $I \subseteq \mathcal{J}(R)$ ein Ideal, M ein endlich erzeugbarer R -Modul, $N \subseteq M$ ein Untermodul.

Dann gilt:

$$\text{Ist } M = I \cdot M + N, \text{ so ist } N = M$$

Speziell: Ist $M = I \cdot M \Rightarrow M = 0$.

Beweis

Sei $M = I \cdot M + N \Rightarrow M/N = (I \cdot M)/N = I \cdot M/N$, also ohne Einschränkung $N = 0$.

Annahme: $M \neq 0$

Dann sei x_1, \dots, x_n ein minimales Erzeugendensystem von M , also $M' := \langle x_2, \dots, x_n \rangle \subsetneq M$.

Nach Voraussetzung ist $M = I \cdot M$, also $x_1 \in I \cdot M \Rightarrow \exists a_1, \dots, a_n \in I$ mit $x_1 = \sum_{i=1}^n a_i x_i = a_1 x_1 + \underbrace{a_2 x_2 + \dots + a_n x_n}_{\in M'} \Rightarrow x_1 \underbrace{(1 - a_1)}_{\in R^\times \text{ 2.20 (c)}} \in M' \Rightarrow x_1 \in M'$. Widerspruch.

Folgerung 2.21

R, I, M wie in Satz 8.

Dann gilt für $x_1, \dots, x_n \in M$:

$$x_1, \dots, x_n \text{ erzeugt } M \Leftrightarrow \bar{x}_1, \dots, \bar{x}_n \text{ erzeugen } \bar{M} = M/IM$$

Beweis

„ \Rightarrow “: klar.

„ \Leftarrow “: Sei N der von x_1, \dots, x_n erzeugte Untermodul von M . Dann ist $M = N + I \cdot M \stackrel{\text{Satz 8}}{\Rightarrow} M = N$.

Beispiele

R lokaler Ring mit maximalem Ideal \mathfrak{m} . $M = \mathfrak{m}$, $I = \mathfrak{m}$.

Falls \mathfrak{m} endlich erzeugt, d.h. falls R noethersch: $\mathfrak{m}^2 = \mathfrak{m} \Rightarrow \mathfrak{m} = 0$, also R Körper.

Satz 9 (Durchschnittssatz von Krull)

Sei R noethersch, M endlich erzeugbarer R -Modul, $I \subseteq R$ Ideal.

Dann gilt für

$$N := \bigcap_{n \geq 0} I^n M \quad : \quad I \cdot N = N$$

Folgerung 2.22

(a) Ist in Satz 9 $I \subseteq \mathcal{J}(R)$, so ist $N = 0$.

(b) Ist R nullteilerfrei, so ist $\bigcap_{n \geq 0} I^n = 0$, falls $I \neq R$.

Beweis

(a) klar.

(b) Sei \mathfrak{m} ein maximales Ideal mit $I \subseteq \mathfrak{m}$. $R_{\mathfrak{m}}$ die Lokalisierung von R nach \mathfrak{m} .

$R_{\mathfrak{m}}$ ist noethersch, lokal, also $\mathcal{J}(R_{\mathfrak{m}}) = \mathfrak{m}R_{\mathfrak{m}}$.

$i : R \rightarrow R_{\mathfrak{m}}$, $a \mapsto \frac{a}{1}$ ist injektiv, da R nullteilerfrei.

Dann ist $i(\bigcap_{n \geq 0} I^n) \subseteq \bigcap_{n \geq 0} i(I^n) \subseteq \bigcap_{n \geq 0} (\mathfrak{m}R_{\mathfrak{m}})^n \stackrel{(a)}{=} 0$.

Da i injektiv ist, folgt $\bigcap_{n \geq 0} I^n = 0$.

Proposition 2.23 (Artin-Rees)

Sei R noethersch, $I \subseteq R$ Ideal, M endlich erzeugbarer R -Modul, $N \subseteq M$ Untermodul.

Dann gibt es ein $n_0 \in \mathbb{N}$, sodass für alle $n \geq n_0$ gilt:

$$I^n M \cap N = I^{n-n_0} (I^{n_0} M \cap N)$$

Beweis (Satz 9)

Setze in Prop. 2.23 (Artin-Rees) $N = \bigcap_{n > 0} I^n M$.

$$\begin{aligned} \text{Dann ist } N &= \bigcap_{n \geq 0} I^n M = I^{n_0+1} M \cap \bigcap_{n \geq 0} I^n M = I^{n_0+1} M \cap N \\ &\stackrel{\text{Artin-Rees}}{=} I(I^{n_0} M \cap N) = I(I^{n_0} M \cap \bigcap_{n \geq 0} I^n M) = I \cdot \bigcap_{n \geq 0} I^n M = I \cdot N \end{aligned}$$

Beweis (Prop. 2.23)

Führe Hilfsgrößen ein:

$R' := \bigoplus_{n \geq 0} I^n$ ist graduerter Ring, $R'_0 = R$ ist noethersch, I ist endlich erzeugt,

$\Rightarrow R'$ ist noethersch (als endlich erzeugte R -Algebra),

$M' := \bigoplus_{n \geq 0} I^n M$ ist graduerter, endlich erzeugter R' -Modul,

$N' := \bigoplus_{n \geq 0} \underbrace{I^n M \cap N}_{=: N'_n}$ ist graduirter R' -Modul, Untermodul von M' , also auch endlich erzeug-

bar. N' werde erzeugt von den homogenen Elementen x_1, \dots, x_r mit $x_i \in N'_{n_i}$.

Für $n \geq n_0 := \max\{n_1, \dots, n_r\}$ ist dann $N'_{n+1} = \{\sum_{i=1}^r a_i x_i : a_i \in R'_{n+1-n_i} = I^{n+1-n_i}\}$.

$I \cdot N'_n = I \cdot \{\sum_{i=1}^r a_i x_i : a_i \in R'_{n-n_i} = I^{n-n_i}\} = \{\sum_{i=1}^r \tilde{a}_i x_i : \tilde{a}_i \in I \cdot I^{n-n_i} = I^{n+1-n_i}\} = N'_{n+1}$.

Mit Induktion folgt die Behauptung.

Beispiele

1) $R = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ ist noethersch, aber nicht nullteilerfrei.

Sei I das von $e_1 = (1, 0)$ erzeugte Ideal, $I^2 = (e_1^2) = (e_1) = I$ (e_1 ist „idempotent“)

$e \in R$ heißt idempotent, wenn $e^2 = e$ ist. Dann ist $(e - 1)e = 0$.

Frage: was ist \mathbb{Z}^2 lokalisiert nach I ?

Antwort: $(\mathbb{Z} \oplus \mathbb{Z})_I = \mathbb{Q}$.

2) $R = C^\infty(-1, 1)$, $I = \{f \in R : f(0) = 0\}$. $R/I = \mathbb{C}$ (oder \mathbb{R}).

I ist Hauptideal, erzeugt von $f(x) = x$.

$\bigcap I^n = ?$ z.B. $f(x) = e^{-\frac{1}{x^2}} \in \bigcap I^n$.

R ist nicht noethersch!

3) $R = k[X, Y]$, $I = (X, Y)$, k algebraisch abgeschlossen.

$R' = R \oplus I \oplus I^2 \oplus \dots = \bigoplus_{n \geq 0} I^n = R[u, v]/(Xv - Yu)$.

Was sind die maximalen homogenen Ideale in R' , die nicht ganz R'_+ enthalten?

Typ 1: maximale Ideale in R , $\neq (X, Y) : (X - a, Y - b)$ mit $(a, b) \neq (0, 0)$

Typ 2: $(X, Y, \alpha u + \beta v)$, $(\alpha, \beta) \neq (0, 0)$

§7 Krull-Dimension

Definition 2.24

Sei R ein Ring.

(a) Eine Folge $\mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_n$ von Primidealen in R heißt **Primidealkette** zu $\mathfrak{p} = \mathfrak{p}_n$ der Länge n , wenn $\mathfrak{p}_{i-1} \subsetneq \mathfrak{p}_i$ für $i = 1, \dots, n$.

(b) Für ein Primideal $\mathfrak{p} \subset R$ heißt

$$h(\mathfrak{p}) := \sup\{n \in \mathbb{N} : \text{es gibt Primidealkette der Länge } n \text{ zu } \mathfrak{p}\}$$

die **Höhe** von \mathfrak{p} .

(c) $\dim R := \sup\{h(\mathfrak{p}) : \mathfrak{p} \text{ Primideal in } R\}$ heißt **Krull-Dimension** von R .

Beispiele

(a) $R = k$ Körper: $\dim k = 0$

(b) $R = \mathbb{Z}$: $\dim \mathbb{Z} = 1$

(c) $R = k[X]$: $\dim k[X] = 1$

(d) $R = k[X, Y]$: $\dim k[X, Y] = 2$

≥ 2 ist klar, da $(0) \subsetneq (X) \subsetneq (X, Y)$. Aber warum = 2?

Bemerkung 2.25

Sei R ein nullteilerfreier Ring. Dann gilt:

- (a) Sind p, q Primelemente, $p \neq 0 \neq q$ mit $(p) \subseteq (q)$, so ist $(p) = (q)$.
- (b) Ist R Hauptidealring, so ist R Körper oder $\dim(R) = 1$

Beweis

- (a) $(p) \subseteq (q) \Rightarrow p \in (q)$, d.h. $p = q \cdot r$ für ein $r \in R$.
Da R nullteilerfrei, ist p irreduzibel, also $r \in R^\times \Rightarrow (p) = (q)$
- (b) $\dim R \leq 1$ nach (a). Sei R kein Körper, also gibt es ein $p \in R$ ($p \neq 0$) mit $p \notin R^\times$.
Da R nullteilerfrei, ist (0) Primideal; p ist in einem maximalen Ideal \mathfrak{m} enthalten ($\mathfrak{m} = (q)$)
 $\Rightarrow (0) \subsetneq \mathfrak{m}$ ist Kette der Länge 1 $\Rightarrow \dim(R) \geq 1 \Rightarrow \dim(R) = 1$

Satz 10

Sei S/R eine ganze Ringerweiterung. Dann gilt:

- (a) Zu jedem Primideal \mathfrak{p} in R gibt es ein Primideal \mathfrak{P} in S mit $\mathfrak{P} \cap R = \mathfrak{p}$
- (b) Zu jeder Primidealkette $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$ in R gibt es eine Primidealkette $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \dots \subsetneq \mathfrak{P}_n$ in S mit $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ ($i = 0, \dots, n$)
- (c) $\dim R = \dim S$

Beweis

- (a) **Beh. 1:** $\mathfrak{p} \cdot S \cap R = \mathfrak{p}$

Dann sei $N := R \setminus \mathfrak{p}$ und $\mathcal{P} := \{I \subseteq S \text{ Ideal} : I \cap N = \emptyset, \mathfrak{p} \cdot S \subseteq I\}$

Nach Beh. 1 ist $\mathcal{P} \neq \emptyset$. Nach Zorn gibt es ein maximales Element \mathfrak{P} in \mathcal{P} . Die Aussage folgt also aus Beh 2.:

Beh. 2: \mathfrak{P} ist Primideal.

Bew. 2: Seien $b_1, b_2 \in S \setminus \mathfrak{P}$ mit $b_1 \cdot b_2 \in \mathfrak{P}$. Dann sind $\mathfrak{P} + (b_1)$ und $\mathfrak{P} + (b_2)$ nicht in \mathcal{P} . Es gibt also $s_i \in S$ und $p_i \in \mathfrak{P}$ ($i = 1, 2$) mit $p_i + s_i \cdot b_i \in N$. $\Rightarrow (p_1 + s_1 b_1)(p_2 + s_2 b_2) \in N \cap \mathfrak{P} = \emptyset$. Widerspruch.

Bew. 1: Sei $b \in \mathfrak{p} \cdot S \cap R$, $b = p_1 t_1 + \dots + p_k t_k$ mit $p_i \in \mathfrak{p}, t_i \in S$. Da S ganz ist über R , ist $S' := R[t_1, \dots, t_k] \subseteq S$ endlich erzeugbarer R -Modul.

Seien s_1, \dots, s_n R -Modul Erzeuger von S' . Für jedes i hat $b \cdot s_i$ eine Darstellung $b \cdot s_i = \sum_{k=1}^n a_{ik} s_k$ mit $a_{ik} \in \mathfrak{p}$ (weil $b \in \mathfrak{p} \cdot S'$).

Es folgt: b ist Nullstelle eines Polynoms vom Grad n mit Koeffizienten in \mathfrak{p} :

$$b^n + \underbrace{\sum_{i=0}^{n-1} \alpha_i b^i}_{\in \mathfrak{p}} = 0, \alpha_i \in \mathfrak{p}$$

Nach Voraussetzung ist $b \in R$: $b^n \in \mathfrak{p} \Rightarrow b \in \mathfrak{p} \Rightarrow \mathfrak{p} \cdot S \cap R \subseteq \mathfrak{p}$.

- (b) Induktion über n : $n = 0$ ist (a). $n \geq 1$:

Nach Induktionsvoraussetzung gibt es eine Kette $\mathfrak{P}_0 \subsetneq \dots \subsetneq \mathfrak{P}_{n-1}$ in S mit $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ ($i = 0, \dots, n-1$).

Sei $S' := S/\mathfrak{P}_{n-1}$, $R' := R/\mathfrak{p}_{n-1}$. Dann ist S'/R' ganze Ringerweiterung.

Nach (a) gibt es in S' ein Primideal \mathfrak{P}'_n mit $\mathfrak{P}'_n \cap R' = \mathfrak{p}'_n := \mathfrak{p}_n/\mathfrak{p}_{n-1}$.

Dann gilt für $\mathfrak{P}_n := \text{pr}^{-1}(\mathfrak{P}'_n)$ ($\text{pr} : S \rightarrow S'$ kanonische Projektion):

$\mathfrak{P}_n \cap R = \mathfrak{p}_n$ und $\mathfrak{P}_n \neq \mathfrak{P}_{n-1}$.

(c) Aus (b) folgt: $\dim S \geq \dim R$. Es bleibt zu zeigen: $\dim S \leq \dim R$.

Sei $\mathfrak{P}_0 \subsetneq \dots \subsetneq \mathfrak{P}_n$ Kette in S , $\mathfrak{p}_i := \mathfrak{P}_i \cap R$, $i = 0, \dots, n$.

klar: \mathfrak{p}_i ist Primideal in R , $\mathfrak{p}_{i-1} \subseteq \mathfrak{p}_i$. Noch zu zeigen: $\mathfrak{p}_{i-1} \neq \mathfrak{p}_i$ für alle i .

Gehe über zu R/\mathfrak{p}_{i-1} und S/\mathfrak{P}_{i-1} , also ohne Einschränkung $\mathfrak{p}_{i-1} = (0)$ und $\mathfrak{P}_{i-1} = (0)$.

Annahme: $\mathfrak{p}_i = (0)$

Sei $b \in \mathfrak{P}_i \setminus \{0\}$. b ist ganz über R : $b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$.

Sei n der minimale Grad einer solchen Gleichung.

Es ist $a_0 = -b(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) \in R \cap \mathfrak{P}_i = \mathfrak{p}_i = (0)$.

$\Rightarrow 0 = -b(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1)$

Da S nullteilerfrei ist, muss gelten: $b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1 = 0$.

Widerspruch zur Wahl von n .

Folgerung 2.26

Sei S/R ganze Ringerweiterung, \mathfrak{p} bzw. \mathfrak{P} Primideale in R bzw. S . Ist $\mathfrak{p} = \mathfrak{P} \cap R$, so gilt:

$$\mathfrak{p} \text{ maximal} \iff \mathfrak{P} \text{ maximal}$$

Beweis

„ \Rightarrow “: Sei \mathfrak{P}' maximales Ideal in S mit $\mathfrak{P} \subseteq \mathfrak{P}'$. Dann ist $\mathfrak{P}' \cap R = \mathfrak{p}$ weil \mathfrak{p} maximal $\Rightarrow \mathfrak{P}' = \mathfrak{P}$.
Nach dem Beweis von Teil (c) des Satzes.

„ \Leftarrow “: Sei \mathfrak{p}' maximales Ideal mit $\mathfrak{p} \subseteq \mathfrak{p}'$. Nach (b) gibt es ein Primideal \mathfrak{P}' in S mit $\mathfrak{P}' \cap R = \mathfrak{p}'$ und $\mathfrak{P} \subseteq \mathfrak{P}' \xRightarrow{\mathfrak{P} \text{ maximal}} \mathfrak{P}' = \mathfrak{P} \Rightarrow \mathfrak{p}' = \mathfrak{p}$.

Satz 11

Sei k Körper, A endlich erzeugbare k -Algebra.

(a) In A gibt es algebraisch unabhängige Elemente x_1, \dots, x_d (für ein $d \geq 0$), sodass A ganz ist über $k[x_1, \dots, x_d]$. [isomorph zum $k[X_1, \dots, X_d]$, da algebraisch unabhängig; Als Modul endlich erzeugbar, da als Algebra endlich erzeugbar.]

(b) Ist $I \subseteq A$ ein echtes Ideal, so können in a) die x_i so gewählt werden, dass $I \cap k[x_1, \dots, x_d] = (x_{\delta+1}, \dots, x_d)$ für ein $\delta \leq d$.

(c) $\dim k[x_1, \dots, x_d] = d$ ($\Rightarrow \dim A = d$)

Beweis

(c) „ \geq “: klar.

„ \leq “: Sei $0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_m$ Primidealkette in A . Ohne Einschränkung (Satz 10) sei $A = k[x_1, \dots, x_n]$.

Nach (b) existiert eine Einbettung $B := k[y_1, \dots, y_d] \hookrightarrow A$ mit $\mathfrak{p}_1 \cap k[y_1, \dots, y_d] = (y_{\delta+1}, \dots, y_d)$.

Beh.: $\delta \leq d - 1$ (d.h. $\mathfrak{p}_1 \cap k[y_1, \dots, y_d] \neq \{0\}$)

Denn: Sonst A ganz über $B \Rightarrow \mathfrak{p}_1 = 0$ (Satz 10, Beweis Teil (c)).

Sei nun $A_1 := A/\mathfrak{p}_1$, $B_1 := B/(\mathfrak{p}_1 \cap B) \cong k[y_1, \dots, y_\delta]$. A_1 ist ganz über B_1 , also ist nach Satz 10 (c) $\dim A_1 = \dim B_1 \stackrel{\text{I.V.}}{=} \delta$

Weiter ist $0 = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1$ Primidealkette in A_1 .

$\Rightarrow m - 1 \leq \delta \leq d - 1 \Rightarrow m \leq d$

(a) Sei $A = k[a_1, \dots, a_n]$ (endliches Erzeugendensystem)

Induktion über n :

$n = 1$: $A = k[a]$; ist a transzendent, so ist $A \cong k[X]$. Sonst: $A \cong k[X]/(f)$ für ein irreduzibles $f \in k[X]$, also endliche Körpererweiterung von k .

$n > 1$: Sind a_1, \dots, a_n algebraisch unabhängig, so ist $A \cong k[X_1, \dots, X_n]$. Andernfalls gibt es $F \in k[X_1, \dots, X_n]$ mit $F(a_1, \dots, a_n) = 0$.

1. Fall: $F = X_n^m + \sum_{i=0}^{m-1} g_i X_n^i$ für ein $m \geq 1$ und $g_i \in k[X_1, \dots, X_{n-1}]$.

Aus $F(a_1, \dots, a_n) = 0$ folgt a_n ganz über $k[a_1, \dots, a_{n-1}] =: A'$. Nach Induktionsvoraussetzung existieren algebraisch unabhängige Elemente x_1, \dots, x_d in $k[a_1, \dots, a_{n-1}]$, sodass A' ganz über $k[x_1, \dots, x_d]$. A ist also ganz über $k[x_1, \dots, x_d]$, da $A = A'[a_n]$.

2. Fall: F beliebig, $F = \sum_{i=0}^m F_i$ homogen vom Grad i .

Ersetze a_i durch $b_i := a_i - \lambda_i a_n$ ($i = 1, \dots, n-1$, $\lambda_i \in k$ „geeignet“). Dann sind b_1, \dots, b_{n-1}, a_n auch k -Algebra-Erzeuger von A . Das Monom $a_1^{\nu_1} \cdots a_n^{\nu_n}$ geht über in

$$a_n^{\nu_n} \prod_{i=1}^{n-1} (b_i + \lambda_i a_n)^{\nu_i} = a_n^{\nu_n} \prod_{i=1}^m \lambda_i^{\nu_i} a_n^{\nu_i} + \text{Terme niedriger Ordnung in } a_n$$

$$\Rightarrow F_m(a_1, \dots, a_n) = F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \cdot a_n^m + \text{Terme niedriger Ordnung in } a_n$$

$$\Rightarrow F(a_1, \dots, a_n) = F(\lambda_1, \dots, \lambda_{n-1}, 1) \cdot a_n^m + \text{Terme niedriger Ordnung in } a_n$$

Ist $F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$, so weiter wie in Fall 1.

Ist k unendlich, so kann man immer $\lambda_1, \dots, \lambda_n$ finden, sodass $F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$.

Ist k endlich, so hilft es, a_i durch $b_i = a_i - a_n^{\mu_i}$ zu ersetzen.

(b) Ohne Einschränkung sei $A = k[x_1, \dots, x_d]$ (betrachte $I' = I \cap k[x_1, \dots, x_d]$).

1. Fall: $I = (f)$ Hauptideal, $f \neq 0$.

Setze $y_d := f$, $y_i = x_i - \lambda_i x_d$ für geeignete $\lambda_i \in k$.

Dann ist $f - y_d = 0$ normiertes Polynom in x_d über $k[y_1, \dots, y_d]$ (vgl. (a))

Beh.: $I \cap k[y_1, \dots, y_d] = (y_d)$

Denn: Sei $g \in I \cap k[y_1, \dots, y_d]$, d.h. $g = h \cdot f$ für ein $h \in k[x_1, \dots, x_d]$. h ist ganz über $k[y_2, \dots, y_d] \Rightarrow h^m + b_{m-1}h^{m-1} + \dots + b_1h + b_0 = 0$ ($m \geq 1$, $b_i \in k[y_1, \dots, y_d]$) \Rightarrow
 $g^m + \underbrace{b_{m-1}fg^{m-1} + \dots + b_1f^{m-1}g + b_0f^m}_{=y_d \cdots} = 0$

y_d teilt also g^m , d.h. $g^m \in (y_d) \stackrel{\text{prim}}{\Rightarrow} g \in (y_d)$

2. Fall: Sei I beliebig. Induktion über d :

$d = 1$: $A = k[X] \Rightarrow$ jedes Ideal ist Hauptideal.

$d > 1$: Sei $f \in I$, $f \neq 0$.

Dann gibt es nach Fall 1 eine Einbettung $k[y_1, \dots, y_d] \hookrightarrow A$ mit $f = y_d$.

$I' := I \cap k[y_1, \dots, y_{d-1}]$

Nach Induktionsvoraussetzung gibt es Einbettung $k[z_1, \dots, z_{d-1}] \hookrightarrow k[y_1, \dots, y_{d-1}]$ mit $I' \cap k[z_1, \dots, z_{d-1}] \subset (z_{\delta+1}, \dots, z_{d-1})$ für ein $\delta \leq d-1$.

$\Rightarrow I \cap k[z_1, \dots, z_{d-1}, z_d] = (z_{\delta+1}, \dots, z_{d-1}, y_d)$

Folgerung: Für jede endlich erzeugte nullteilerfreie k -Algebra A über einem Körper k gilt:

$$\text{trdeg}(\text{Quot}(A)) = \dim A$$

Dabei ist $\text{trdeg}(A)$ (der **Transzendenzgrad** von K über k) die Maximalzahl über k algebraisch unabhängiger Elemente in K .

§8 Das Spektrum eines Rings

Definition + Bemerkung 2.27

Sei R ein Ring.

- a) $\text{Spec}(R) := \{\mathfrak{p} \subset R : \mathfrak{p} \text{ Primideal}\}$ heißt **Spektrum** von R .
- b) Eine Teilmenge $V \subset \text{Spec}(R)$ heißt **abgeschlossen**, wenn es ein Ideal $I \subseteq R$ gibt mit

$$V = V(I) := \{\mathfrak{p} \in \text{Spec}(R) : I \subseteq \mathfrak{p}\}$$

- c) Die abgeschlossenen Teilmengen von $\text{Spec}(R)$ definieren eine Topologie auf $\text{Spec}(R)$, sie heißt die **Zariski-Topologie**.

Beispiele

$$R = \mathbb{Z}: \text{Spec}(\mathbb{Z}) = \{(0)\} \cup \{(p) : p \text{ Primzahl}\}$$

$$V((p)) = (p) \Rightarrow (p) \text{ ist abgeschlossen in } \text{Spec}(R) \text{ für jede Primzahl } p.$$

$$V((0)) = \text{Spec}(\mathbb{Z}).$$

$$I = n\mathbb{Z} \Rightarrow V(I) = \{(p_1), \dots, (p_k)\}, \text{ wenn } n = p_1^{\nu_1} \cdots p_k^{\nu_k} \text{ die Primfaktorzerlegung von } n \text{ ist.}$$

$$\overline{\{(0)\}} = \text{Spec}(\mathbb{Z})$$

$$R = k[X]: \overline{\{(0)\}} = \text{Spec}(R).$$

$$f \in k[X] \text{ irreduzibel} \Rightarrow (f) \text{ ist abgeschlossener Punkt.}$$

$$k := \mathbb{C}: f \text{ irreduzibel} \Leftrightarrow f(X) = X - c \text{ für ein } c \in \mathbb{C}. \Rightarrow \text{Spec}(\mathbb{C}[X]) = \mathbb{C} \cup \{(0)\}$$

Beweis

c) Sei $U \subseteq \text{Spec}(R)$ offen $:\Leftrightarrow \text{Spec}(R) \setminus U$ abgeschlossen.

Zu zeigen:

- (i) \emptyset ist abgeschlossen: $\emptyset = V(R)$.
 $\text{Spec}(R)$ ist abgeschlossen: $\text{Spec}(R) = V((0))$.
- (ii) endliche Vereinigung von abgeschlossenen Mengen ist abgeschlossen.

$$\text{Zeige dazu: } V(I_1) \cup \dots \cup V(I_n) = V(I_1 \cap \dots \cap I_n) = V(I_1 \cdots I_n)$$

denn: Ohne Einschränkung sei $n = 2$:

$$\text{„}\subseteq\text{“ Sei } \mathfrak{p} \in V(I_1) \Rightarrow I_1 \subseteq \mathfrak{p} \Rightarrow I_1 \cap I_2 \subseteq \mathfrak{p} \Rightarrow \mathfrak{p} \in V(I_1 \cap I_2).$$

$$\text{„}\supseteq\text{“ Sei } \mathfrak{p} \in V(I_1 \cap I_2), \mathfrak{p} \notin V(I_1).$$

Dann gibt es ein $a \in I_1 \setminus \mathfrak{p}$. Sei $b \in I_2$.

$$\text{Dann ist } a \cdot b \in I_1 \cap I_2 \underset{\text{Vor.}}{\overset{\mathfrak{p} \text{ prim}}{\subsetneq}} \mathfrak{p}. \xrightarrow{a \notin \mathfrak{p}} b \in \mathfrak{p} \Rightarrow I_2 \subseteq \mathfrak{p}, \text{ d.h. } \mathfrak{p} \in V(I_2).$$

(iii) beliebiger Durchschnitt von abgeschlossenen Mengen ist abgeschlossen. Zeige dazu:

$$\bigcap_{\nu} V(I_{\nu}) = V\left(\sum_{\nu} I_{\nu}\right)$$

denn: $\mathfrak{p} \in \bigcap_{\nu} V(I_{\nu}) \Leftrightarrow I_{\nu} \subseteq \mathfrak{p} \forall \nu \Leftrightarrow \sum_{\nu} I_{\nu} \subseteq \mathfrak{p}$.

Bemerkung 2.28

a) Für Ideale $I_1 \subseteq I_2$ ist $V(I_1) \supseteq V(I_2)$.

b) Für jedes Ideal $I \subseteq R$ ist $V(I) = V(\sqrt{I}) = V(\text{Rad}(I))$

Beweis

Sei \mathfrak{p} Primideal mit $I \subseteq \mathfrak{p}$, $f \in \sqrt{I}$, dann ist $f^n \in I$ für ein $n \geq 1$. $\Rightarrow f^n \in \mathfrak{p} \underset{\mathfrak{p} \text{ prim}}{\Rightarrow} f \in \mathfrak{p} \Rightarrow \sqrt{I} \subseteq \mathfrak{p}$.

c) Die $U(f) := \text{Spec}(R) - V((f))$, $f \in R \setminus \sqrt{(0)}$ bilden eine Basis der Zariski-Topologie.

Beweis

$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p} \quad (\text{Ü7A2b})$$

Also ist $V(f) = \text{Spec}(R) \Leftrightarrow f \in \sqrt{(0)}$. Für $f \in R \setminus \sqrt{(0)}$ ist also $U(f) \neq \emptyset$.

Zu zeigen: Ist $U \subseteq \text{Spec}(R)$ offen, $U \neq \emptyset$, so gibt es ein $f \in R \setminus \sqrt{(0)}$ mit $U(f) \subseteq U$.

Sei also $U = \text{Spec}(R) - V(I)$ mit $I \not\subseteq \sqrt{(0)}$. Für $f \in I \setminus \sqrt{(0)}$ ist $(f) \subseteq I$, also $V(f) \supseteq V(I) \Rightarrow U(f) \subseteq U$.

Zusatz: $U(f) = \{\mathfrak{p} \in \text{Spec}(R) : f \notin \mathfrak{p}\}$.

Definition + Proposition 2.29

a) Ein topologischer Raum X heißt *irreduzibel*, wenn er nicht Vereinigung zweier echter abgeschlossener Teilmengen ist.

Beispiele

$$R = \mathbb{C}[X, Y],$$

$$V((X)) = \{(X)\} \cup \{(X, Y - c), c \in \mathbb{C}\}$$

$$V((Y)) = \{(Y)\} \cup \{(X - a, Y), a \in \mathbb{C}\}.$$

$$V(X \cdot Y) = V((X)) \cup V((Y)) = \text{Achsenkreuz und } (X), (Y).$$

b) Eine abgeschlossene Teilmenge $V(I) \subseteq \text{Spec}(R)$ ist genau dann irreduzibel, wenn I ein Primideal ist.

Beweis

„ \Rightarrow “ Seien $f_1, f_2 \in R$, $f_1 \cdot f_2 \in I$ und $f_1 \notin I$. Dann ist $V(f_1) \not\subseteq V := V(I)$.

$$\text{Andererseits: } V \subseteq V(f_1 \cdot f_2) = V(f_1) \cup V(f_2)$$

$$\Rightarrow V = (V \cap V(f_1)) \cup (V \cap V(f_2))$$

$$\underset{V \text{ irreduz.}}{\Rightarrow} V \subseteq V(f_2) \Rightarrow f_2 \in I.$$

„ \Leftarrow “ Sei $V(I) = V = V(I_1) \cup V(I_2)$ und $V(I_1) \neq V$

d.h. $I_1 \not\subseteq I$. Sei $f_1 \in I_1 \setminus I$

$$\text{Andererseits ist } V(I_1 \cdot I_2) = V(I_1) \cup V(I_2) = V \Rightarrow I_1 \cdot I_2 \subseteq \sqrt{I} = I$$

Für jedes $f \in I_2$ ist also $f_1 \cdot f \in I \underset{f_1 \notin I}{\Rightarrow} f \in I \Rightarrow I_2 \subseteq I \Rightarrow V(I) \subseteq V(I_2)$.

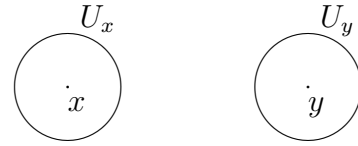
Folgerung 2.30

Ist $\text{Spec}(R)$ hausdorffsch, so ist $\dim R = 0$

Beweis

$\text{Spec}(R)$ hausdorffsch, \Rightarrow jede irreduzible Teilmenge von $\text{Spec}(R)$ ist einelementig.

- \Rightarrow Für jedes Primideal \mathfrak{p} von R ist $V(\mathfrak{p}) = \{\mathfrak{p}\}$
- \Rightarrow jedes Primideal in R ist maximales Ideal.
- $\Rightarrow \dim R = 0$



$X = (X - U_x) \cup (X - U_y)$
 $\Rightarrow X$ nicht irreduzibel.

Definition + Bemerkung 2.31

a) Für eine beliebige Teilmenge V von $\text{Spec}(R)$ heißt

$$I(V) = \bigcap_{\mathfrak{p} \in V} \mathfrak{p}$$

das **Verschwundungsideal** von V .

b) Für jedes Ideal I von R gilt:

$$I(V(I)) = \sqrt{I}$$

Beweis

Nach Ü7A2d ist $\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \supseteq I \\ \mathfrak{p} \text{ Primideal}}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$

Folgerung

Ist $V(I_1) = V(I_2)$, so ist $\sqrt{I_1} = \sqrt{I_2}$.

Definition + Proposition 2.32

- a) Sei X ein topologischer Raum. Eine irreduzible Teilmenge $V \subseteq X$ heißt **irreduzible Komponente**, wenn V maximale irreduzible Teilmenge ist bzgl. \subseteq .
- b) Jeder topologischer Raum ist Vereinigung seiner irreduziblen Komponenten.
- c) Ist R noethersch, so ist jede abgeschlossene Teilmenge von V von $\text{Spec}(R)$ endliche Vereinigung von irreduziblen Komponenten von V ; diese sind eindeutig bestimmt.

Beweis

b) Zu zeigen: jedes $x \in X$ ist in einer irreduziblen Teilmenge von X enthalten.

Sei $\mathcal{C}_x := \{U \subseteq X : x \in U, U \text{ irreduzibel}\}$.

$\mathcal{C}_x \neq \emptyset$, da $\{x\} \in \mathcal{C}_x$.

Seien $(U_i)_{i \in \mathbb{N}}$ in \mathcal{C}_x mit $U_i \subseteq U_{i+1}$ für alle i .

Sei $U := \bigcup_{i \in \mathbb{N}} U_i$, zu zeigen: $U \in \mathcal{C}_x$, d.h. U irreduzibel.

denn: Sei $U = V \cup W$, V, W abgeschlossene Teilmengen von U . Dann ist $U_i = (U_i \cap V) \cup (U_i \cap W)$ für jedes $i \in \mathbb{N}$

Da U_i irreduzibel, ist (ohne Einschränkung) $U_i \cap V = U_i$ für unendliche viele i .

$\Rightarrow U_i \subseteq V \Rightarrow U = \bigcap_{\text{diese } i} U_i \subseteq V \Rightarrow U \subseteq V$.

$\Rightarrow U$ irreduzibel.

Mit dem Zornschen Lemma folgt: \mathcal{C}_x enthält ein maximales Element.

c) Ohne Einschränkung sei $V = \text{Spec}(R)$: Sei $V = V(I)$ für ein Ideal I .

$$V(I) = \{\mathfrak{p} \in \text{Spec}(R) : I \subseteq \mathfrak{p}\} \xrightarrow{\text{bijektiv}} \{\mathfrak{p}' \in \text{Spec}(R/I)\}$$

Aus 2.34b wird folgen: Die Abbildung ist ein Homöomorphismus.

Sei \mathfrak{V} die Menge der abgeschlossenen Teilmengen von $\text{Spec}(R)$, die nicht Vereinigung von endlich vielen irreduziblen Teilmengen sind. Weiter sei $J := \{I(V) : V \in \mathfrak{V}\}$

Zu zeigen: $\mathfrak{V} = \emptyset$

Anderenfalls ist auch $J \neq \emptyset$. Da R noethersch ist, enthält J ein maximales Element $I(V_0)$ für ein $V_0 \in \mathfrak{V}$.

V_0 ist nicht irreduzibel.

Also gibt es abgeschlossene Teilmengen V_1, V_2 von V_0 mit $V_0 = V_1 \cup V_2$, $V_1 \neq V_0 \neq V_2$.

$V_i \notin \mathfrak{V}$ für $i = 1, 2$, da $I(V_0) \subsetneq I(V_1)$

Also lassen sich V_1 und V_2 als endliche Vereinigung von irreduziblen Teilmengen schreiben.

$\Rightarrow V_0$ lässt sich auch als endliche Vereinigung von irreduziblen Teilmengen schreiben.

Widerspruch zur Wahl von V_0 .

$\Rightarrow \mathfrak{V} = \emptyset$.

Sei also $V = V_0 \cup \dots \cup V_r$ mit irreduziblen Teilmengen V_i .

Noch zu zeigen:

- die V_i sind (ohne Einschränkung) irreduzible Komponenten.
- Eindeutigkeit

denn:

Aus b) folgt: jedes V_i ist in einer irreduziblen Komponente \tilde{V}_i von V enthalten, also $V = \bigcup_{i=0}^r \tilde{V}_i$; ohne Einschränkung alle \tilde{V}_i verschieden.

Sei W irreduzible Komponente von V .

$$\Rightarrow W = \bigcup_{i=0}^r (W \cap \tilde{V}_i) \underset{W \text{ irreduz.}}{\Rightarrow} \text{es gibt ein } i \text{ mit } W \subseteq \tilde{V}_i$$

$$\underset{W \text{ Komponente}}{\Rightarrow} W = \tilde{V}_i$$

Folgerung 2.33

Ein noetherscher Ring hat nur endlich viele minimale Primideale.

Beweis

Sei $\mathfrak{p} \in \text{Spec}(R)$ minimales Primideal. $\Leftrightarrow V(\mathfrak{p}) \subseteq \text{Spec}(R)$ irreduzible Komponente.

Proposition 2.34

Sei $\alpha : R \rightarrow S$ Ringhomomorphismus.

a) Die Abbildung $\varphi_\alpha : \text{Spec}(S) \rightarrow \text{Spec}(R)$, $\mathfrak{p} \mapsto \alpha^{-1}(\mathfrak{p})$ ist stetig.

Eleganter: $R \rightarrow \text{Spec}(R)$ ist kontravarianter Funktor Ringe \rightarrow top. Räume

b) Ist α surjektiv, so ist φ_α injektiv und $\varphi_\alpha(\text{Spec}(S)) = V(\text{Kern}(\alpha))$

Beweis

a) $\alpha^{-1}(\mathfrak{p})$ ist Primideal:

Seien $a, b \in R$ mit $a \cdot b \in \alpha^{-1}(\mathfrak{p}) \Rightarrow \alpha(a \cdot b) \in \mathfrak{p} \stackrel{\text{OE}}{\Rightarrow} \alpha(a) \in \mathfrak{p} \Rightarrow a \in \alpha^{-1}(\mathfrak{p})$

φ_α **stetig**: Zu zeigen: für jede abgeschlossene Teilmenge $V = V(I)$ von $\text{Spec}(R)$ ist $\varphi_\alpha^{-1}(V)$ abgeschlossen in $\text{Spec}(S)$.

$$\varphi_\alpha^{-1}(V(I)) = \{\mathfrak{p} \in \text{Spec}(S) : I \subseteq \alpha^{-1}(\mathfrak{p})\} = \{\mathfrak{p} \in \text{Spec}(S) : \alpha(I) \subseteq \mathfrak{p}\} = \{\mathfrak{p} \in \text{Spec}(S) : \alpha(I) \cdot S \subseteq \mathfrak{p}\} = V(\alpha(I) \cdot S)$$

b) Seien $\mathfrak{p}, \mathfrak{p}' \in \text{Spec}(S)$ mit $\varphi_\alpha(\mathfrak{p}) = \varphi_\alpha(\mathfrak{p}')$

$$\Rightarrow \alpha^{-1}(\mathfrak{p}) = \alpha^{-1}(\mathfrak{p}') \Rightarrow \alpha(\alpha^{-1}(\mathfrak{p})) = \alpha(\alpha^{-1}(\mathfrak{p}')) \stackrel{\alpha \text{ surj.}}{\Rightarrow} \mathfrak{p} = \mathfrak{p}'$$

§9 Diskrete Bewertungsringe

Definition 2.35

Sei K ein Körper.

Ein surjektiver Gruppenhomomorphismus $v : K^\times \rightarrow \mathbb{Z}$ heißt **diskrete Bewertung**, wenn für alle $x, y \in K^\times$ mit $x + y \in K^\times$ gilt:

$$v(x + y) \geq \min\{v(x), v(y)\}$$

Anmerkungen: Manchmal setzt man $v(0) = \infty$.

Da v Gruppenhomomorphismus ist, gilt: $v(x \cdot y) = v(x) + v(y)$ und $v(1) = 0$.

Beispiele

1.) $K = \mathbb{Q}$, $p \in \mathbb{Z}$ Primzahl.

Für $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, $a, b \in \mathbb{Z}$ schreibe $a = p^n \cdot a'$, $b = p^m \cdot b'$ mit $p \nmid a'$, $p \nmid b'$.

Setze $v_p(\frac{a}{b}) := n - m$. Und es gilt: $a + b \stackrel{\text{OE: } n \leq m}{=} p^n \cdot (a' + p^{m-n}b')$.

v_p heißt **p -adische Bewertung** auf \mathbb{Q} . Es gilt:

- $v_p(a) \geq 0 \forall a \in \mathbb{Z}$. $v_3(\frac{7}{2}) = 0$, $v_3(\frac{9}{2}) = 2$.
- $v_p(a + b) = \min\{v_p(a), v_p(b)\}$, falls $v_p(a) \neq v_p(b)$.

2.) $K = k(X) = \text{Quot}(k[X])$ (k Körper).

Für $f = \frac{f_1}{f_2}$ sei $v(f) = v(f_1) - v(f_2)$.

(a) $v(f_1) = \text{ord}_a(f_1)$ für festes $a \in k$ (Nullstellenordnung).

Es gilt $v_a(f_1 \cdot f_2) = v_a(f_1) + v_a(f_2)$

$$v_a(f_1 + f_2) = v_a((X - a)^{n_1} \cdot g_1 + (X - a)^{n_2} \cdot g_2)$$

$$\stackrel{\text{OE: } n_1 \leq n_2}{=} v_a((X - a)^{n_1}(g_1 + (X - a)^{n_2 - n_1} \cdot g_2))$$

(b) Für $f \in k[X]$ sei $v(f) = -\deg(f)$.

Bemerkung 2.36

Sei $v : K^\times \rightarrow \mathbb{Z}$ diskrete Bewertung. Sei $\rho \in \mathbb{R}$ mit $0 < \rho < 1$. Dann ist die Abbildung

$$|\cdot|_v : K \rightarrow \mathbb{R}, |x|_v = \begin{cases} 0 & : x = 0 \\ \rho^{v(x)} & : x \in K^\times \end{cases}$$

ein **Absolutbetrag** auf K , d.h. eine Abbildung $K \rightarrow \mathbb{R}$ mit:

- (i) $|x|_v = 0 \Leftrightarrow x = 0$
- (ii) $|x \cdot y|_v = |x|_v \cdot |y|_v$
- (iii) $|x + y|_v \leq |x|_v + |y|_v$

In unserer Situation gilt sogar:

$$|x + y|_v \leq \max\{|x|_v, |y|_v\} \leq |x|_v + |y|_v \Rightarrow \text{„nichtarchimedischer Betrag“}$$

Weiter ist $d(x, y) := |x - y|_v$ eine Metrik auf K .

Zur Geometrie

Kreis um a mit Radius r : $K_r = \{b \in K : d(a, b) \leq r\}$.

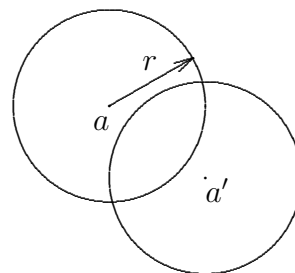
Jeder Kreis hat mehrere Mittelpunkte:

Beh.: Für jedes $a' \in K_r$ ist $K_r(a') = K_r(a)$

Bew.: Sei $b \in K_r(a)$, also $d(b, a) \leq r$.

Dreiecksungleichung:

$$d(b, a') \leq \max\{\underbrace{d(b, a)}_{\leq r}, \underbrace{d(a, a')}_{\leq r}\} \leq r \Rightarrow b \in K_r(a')$$



Es gibt kein allgemeines Dreieck:

Ist $d(a, b) < d(a, c)$, also $|a - b| < |c - a|$, so ist $|c - b| = |a - b + c - a| = \max\{|a - b|, |c - a|\} = |c - a|$
 \Rightarrow jedes Dreieck ist gleichschenkelig.

Erinnerung

\mathbb{R} entsteht aus \mathbb{Q} durch „Vervollständigung“:

$C :=$ Ring der Cauchy-Folgen von \mathbb{Q} (bzgl. $|\cdot|$)

$N :=$ Ideal der Nullfolgen in C (maximales Ideal)

$\mathbb{R} := C/N$

Analog:

$C_p :=$ Ring der Cauchy-Folgen von \mathbb{Q} (bzgl. $|\cdot|_p := |\cdot|_{v_p}$)

$N_p :=$ Ideal der Nullfolgen in C_p (maximales Ideal)

$\mathbb{Q}_p := C_p/N_p$ „**Körper der p-adischen Zahlen**“

Bemerkung 2.37

Ist v diskrete Bewertung auf K^\times , so ist $\mathcal{O}_v := \{x \in K : v(x) \geq 0\} \cup \{0\}$ ein Ring, genauer: ein lokaler Ring mit maximalem Ideal $\mathfrak{m}_v := \{x \in K : v(x) > 0\} \cup \{0\}$.

Beweis

\mathcal{O}_v ist Ring, da $v(x + y) \geq \min\{v(x), v(y)\} \geq 0$ für alle $x, y \in \mathcal{O}$.

\mathfrak{m}_v ist Ideal: Ist $x \in \mathfrak{m}_v$, $r \in \mathcal{O}_v$, so ist $v(x \cdot r) = v(x) + v(r) > 0$.

Für $x \in \mathcal{O}_v \setminus \mathfrak{m}_v = \{x \in K : v(x) = 0\}$ ist $v(\frac{1}{x}) = -v(x) = 0 \Rightarrow \frac{1}{x} \in \mathcal{O}_v \setminus \mathfrak{m}_v \Rightarrow x \in \mathcal{O}_v^\times$.

Definition + Proposition 2.38

(a) Ein nullteilerfreier Ring R heißt **diskreter Bewertungsring**, wenn es eine diskrete Bewertung von $K = \text{Quot}(R)$ gibt mit $R = \mathcal{O}_v$.

(b) Jeder diskrete Bewertungsring ist noethersch, lokal und eindimensional.

Beweis

Zeige mehr: R ist Hauptidealring.

R ist lokal \checkmark , sei \mathfrak{m} das maximale Ideal in R .

Beh.1: \mathfrak{m} ist Hauptideal.

Bew.1: Sei $t \in R$ mit $v(t) = 1 \Rightarrow t \in \mathfrak{m}$. Sei $x \in \mathfrak{m} \setminus \{0\}$, $y = \frac{x}{t^{v(x)}} \Rightarrow v(y) = v(x) - v(t^{v(x)}) = 0 \Rightarrow y \in R^\times \Rightarrow x = t^{v(x)} \cdot y \in (t)$.

Beh.2: Jedes Ideal $\neq 0$ in R ist von der Form \mathfrak{m}^n für ein $n \geq 0$.

Bew.2: Sei $I \subseteq R$ ein Ideal, $n := \min\{v(x) : x \in I \setminus \{0\}\}$. Sei $x_0 \in I$ mit $v(x_0) = n \Rightarrow v(\frac{x_0}{t^n}) = 0 \Rightarrow t^n = \frac{t^n}{x_0} \cdot x_0 \in I \Rightarrow \mathfrak{m}^n = (t^n) \subseteq I$.

Umgekehrt: $x_0 = t^n \cdot \frac{x_0}{t^n} \in (t^n)$.

Sei $x \in I \Rightarrow v(\frac{x}{t^n}) = v(x) - n \geq 0 \Rightarrow x = t^n \cdot \frac{x}{t^n} \in (t^n) \Rightarrow I \subseteq \mathfrak{m}^n$.

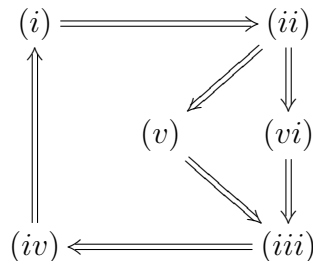
Satz 12 (Diskrete Bewertungsringe)

Sei R ein lokaler noetherscher Ring der Dimension 1 mit maximalem Ideal \mathfrak{m} und Restklassenkörper $k = R/\mathfrak{m}$.

Dann sind äquivalent:

- (i) R ist diskreter Bewertungsring
- (ii) R ist (nullteilerfreier) Hauptidealring
- (iii) R ist nullteilerfrei und \mathfrak{m} ist ein Hauptideal
- (iv) es gibt ein $t \in R$, sodass jedes $x \in R \setminus \{0\}$ eine eindeutige Darstellung $x = u \cdot t^n$ hat mit $n \in \mathbb{N}$, $u \in R^\times$
- (v) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$
- (vi) R ist normal

Beweis



(i) \Rightarrow (ii) [Proposition 2.38](#)

(iv) \Rightarrow (i)

R nullteilerfrei:

Annahme: $u \cdot t^n \cdot v \cdot t^m = 0 = u \cdot v \cdot t^{n+m} \Rightarrow t^{n+m} = t^{n+m} + 0 = t^{n+m} + u \cdot v \cdot t^{n+m} = (1 + u \cdot v)t^{n+m} \xrightarrow{\text{Eind.}} 1 + u \cdot v = 1 \Rightarrow u \cdot v = 0 \Rightarrow$ Widerspruch zu $u \cdot v \in R^\times$.

Diskrete Bewertung:

Für $a = u \cdot t^n \in R \setminus \{0\}$ setze $v(a) = n$. Für $x = \frac{a}{b} \in K = \text{Quot}(R)$, $a, b \in R \setminus \{0\}$ setze $v(x) = v(a) - v(b)$.

$v(x)$ wohldefiniert: Ist $x = \frac{a'}{b'}$ mit $a', b' \in R \setminus \{0\}$, so ist $a \cdot b' = a' \cdot b$. Aus $a = u \cdot t^n, b = v \cdot t^m, a' = u' \cdot t^{n'}, b' = v' \cdot t^{m'}$ folgt: $u' \cdot v \cdot t^{n'+m} = u \cdot v' \cdot t^{n+m'} \xrightarrow{\text{Eind.}} n' + m = n + m' \Rightarrow n' - m' = n - m$.

v ist diskrete Bewertung: $v(x \cdot y) = v(u \cdot t^n \cdot v \cdot t^m) = v(u \cdot v \cdot t^{n+m}) = n + m = v(x) + v(y)$.

$v(x + y) \stackrel{m \leq n}{=} v(t^m \cdot (v + u \cdot t^{n-m})) \geq m = \min\{v(x), v(y)\}$.

(iii) \Rightarrow (iv) Sei $\mathfrak{m} = (t)$. Sei $x \in R \setminus \{0\}$. Da R noethersch ist, ist $\bigcap_{n \geq 0} \mathfrak{m}^n = (0)$ (Folgerung 2.22). Also gibt es ein (eindeutiges) $n \geq 0$ mit $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1} \Rightarrow \exists u \in R^\times$ mit $x = u \cdot t^n$. u ist eindeutig: Wäre $u \cdot t^n = v \cdot t^n$, so wäre $(u - v) \cdot t^n = 0$, also t Nullteiler \Rightarrow Widerspruch

(ii) \Rightarrow (v) $\mathfrak{m}/\mathfrak{m}^2$ ist k -Vektorraum: $\mathfrak{m}, \mathfrak{m}^2$ und damit $\mathfrak{m}/\mathfrak{m}^2$ sind R -Moduln. Für $a \in \mathfrak{m}$ und $x \in \mathfrak{m}/\mathfrak{m}^2$ ist $a \cdot \bar{x} = \overline{a \cdot x} = 0$, da $a \cdot x \in \mathfrak{m}^2 \Rightarrow \bar{a} \cdot \bar{x}$ ist wohldefiniert für die Klasse \bar{a} von a in $R/\mathfrak{m} = k$.

Es ist $\mathfrak{m}^2 \neq \mathfrak{m}$, da $\dim R = 1$ (und R noethersch) $\Rightarrow \dim_k \mathfrak{m}/\mathfrak{m}^2 \geq 1$.

$\mathfrak{m}/\mathfrak{m}^2$ wird von \bar{t} erzeugt (als R -Modul und damit auch als R/\mathfrak{m} -Modul) $\Rightarrow \dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$
 $\Rightarrow \dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

(v) \Rightarrow (iii) Sei $t \in \mathfrak{m}$, sodass $\bar{t} \in \mathfrak{m}/\mathfrak{m}^2$ Erzeuger ist.

Mit Nakayama (Folgerung 2.21) folgt: t erzeugt \mathfrak{m} .

(ii) \Rightarrow (vi) Jeder (nullteilerfreie) Hauptidealring ist faktoriell

$\Rightarrow R$ ist normal. (Bemerkung 2.10)

(vi) \Rightarrow (iii) Sei $K = \text{Quot}(R)$.

Sei $\bar{\mathfrak{m}} := \{x \in K : x \cdot \mathfrak{m} \subseteq \mathfrak{m}\}$, $\mathfrak{m}^{-1} := \{x \in K : x \cdot \mathfrak{m} \subseteq R\}$

Offensichtlich: $R \subseteq \bar{\mathfrak{m}} \subseteq \mathfrak{m}^{-1}$

Beh. 1:

1.) $\bar{\mathfrak{m}} = R$

2.) $\mathfrak{m}^{-1} \neq R$

3.) $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$ ($\mathfrak{m} \cdot \mathfrak{m}^{-1}$ ist das von allen $a \cdot x$, $a \in \mathfrak{m}$, $x \in \mathfrak{m}^{-1}$ erzeugte Ideal in R)

Dann sei $t \in \mathfrak{m} \setminus \mathfrak{m}^2 \Rightarrow t \cdot \mathfrak{m}^{-1} \subseteq R$ ist Ideal in R . Wäre $t \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m}$, so wäre $(t) = t \cdot R \stackrel{3.)}{=} t \cdot \mathfrak{m}^{-1} \cdot \mathfrak{m} \subseteq \mathfrak{m}^2 \Rightarrow$ Widerspruch zu $t \notin \mathfrak{m}^2$. Also ist $t \cdot \mathfrak{m}^{-1} = R$ und $(t) \stackrel{3.)}{=} t \cdot \mathfrak{m}^{-1} \cdot \mathfrak{m} = \mathfrak{m}$.

Bew. 3: Aus $R \subseteq \mathfrak{m}^{-1}$ folgt $\mathfrak{m} \subseteq \mathfrak{m} \cdot \mathfrak{m}^{-1}$. Wäre $\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}^{-1}$, so wäre $\mathfrak{m}^{-1} \subseteq \bar{\mathfrak{m}} = R$ im Widerspruch zu Beh. 2.).

Bew. 1: $\bar{\mathfrak{m}}$ ist Unterring von K .

Zeige: $\bar{\mathfrak{m}}$ ist ganz über R (dann ist $\bar{\mathfrak{m}} = R$, da R normal).

Es genügt zu zeigen: $\bar{\mathfrak{m}}$ ist endlich erzeugter R -Modul.

Für $t \in \mathfrak{m} \setminus \{0\}$ ist $t \cdot \bar{\mathfrak{m}} \subseteq R$, also endlich erzeugt, da R noethersch. Als R -Modul sind $\bar{\mathfrak{m}}$ und $t \cdot \bar{\mathfrak{m}}$ isomorph.

Bew. 2: Sei $t \in \mathfrak{m} \setminus \{0\}$

Beh. 4: Es gibt ein $n \geq 1$ mit $\mathfrak{m}^n \subseteq (t)$.

Sei n in Beh.4 minimal, $y \in \mathfrak{m}^{-1} \setminus (t)$, $x := \frac{y}{t} \in K$. Dann ist $x \in \mathfrak{m}^{-1} : x \cdot \mathfrak{m} = \frac{y}{t} \cdot \mathfrak{m} \subseteq \frac{1}{t} \cdot \mathfrak{m}^n \subseteq R$, aber $x \notin R$, sonst wäre $y = x \cdot t \in (t) \Rightarrow$ Widerspruch.

Bew. 4: $\sqrt{(t)} = \bigcap_{\mathfrak{p} \subset R, t \in \mathfrak{p}} \mathfrak{p} = \mathfrak{m}$.

Seien x_1, \dots, x_r Erzeuger von \mathfrak{m} , $\nu_i \in \mathbb{N}$ ($i = 1, \dots, r$) mit $x_i^{\nu_i} \in (t)$.

Für $N = 1 + \sum_{i=1}^r (\nu_i - 1)$ ist dann $\mathfrak{m}^N \subseteq (t)$, da \mathfrak{m}^N erzeugt wird von den $x_1^{\nu_1} \cdot \dots \cdot x_r^{\nu_r}$ mit $\sum \nu_i = N \Rightarrow \exists \nu_i = 1$.

Beispiele

$R = \left(k[X, Y] / (Y^2 - X^3 - X^2) \right)_{(X, Y)}$ ist nullteilerfrei, eindimensional, lokal, noethersch aber *kein* diskreter Bewertungsring.

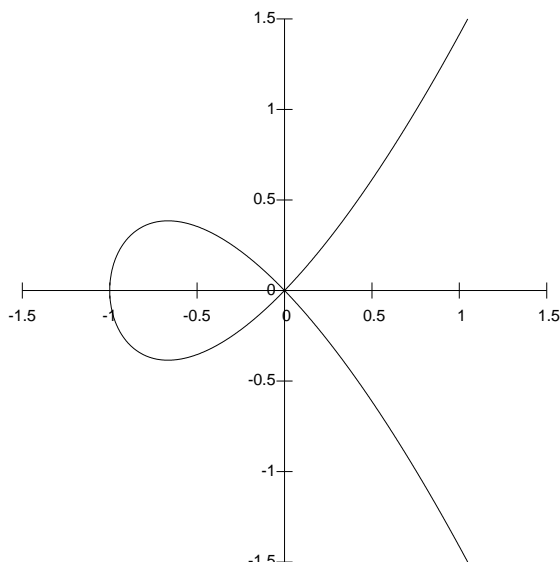
Denn: das maximale Ideal in R ist kein Hauptideal:
 $\mathfrak{m} = (X, Y)$, $f = Y^2 - X^2(X + 1) \in \mathfrak{m}^2$.

Es gilt $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 2$, da X, Y linear unabhängig in $\mathfrak{m}/\mathfrak{m}^2$. Sei \mathfrak{M} das von X und Y in $k[X, Y]$ erzeugte Ideal. $\mathfrak{m}/\mathfrak{m}^2 = (\mathfrak{M}/(f))/(\mathfrak{M}^2/(f)) \cong \mathfrak{M}/\mathfrak{M}^2$

Geometrisch:

$V(f) = \{(x, y) \in k^2 : f(x, y) = 0\} = \{(x, y) \in k^2 : y^2 = x^2(x + 1)\}$

Singularität in $(0, 0) = (X, Y) \Rightarrow$ "Newton-Knoten".



§10 Dedekindringe

Definition 2.39

Ein nullteilerfreier Ring heißt **Dedekindring**, wenn er noethersch, normal und eindimensional ist.

Beispiele

- 1) \mathbb{Z} , $k[X]$ (k Körper)
- 2) diskrete Bewertungsringe
- 3) Hauptidealringe (nullteilerfrei)
- 4) der ganze Abschluss \mathcal{O}_d von \mathbb{Z} in $\mathbb{Q}(\sqrt{d})$ wobei $d \in \mathbb{Z}$ quadratfrei.

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4} \end{cases}$$

Beobachtung: Es gibt Dedekindringe, die nicht faktoriell sind: Beispiel: $\mathbb{Z}[\sqrt{-5}]$.
 $(2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}))$.

Definition + Bemerkung 2.40

Sei R nullteilerfrei, $K = \text{Quot}(R)$

- a) Ein R -Untermodul $I \neq (0)$ von K heißt **gebrochenes Ideal** von R , wenn es ein $a \in R \setminus \{0\}$ gibt mit $a \cdot I \subseteq R$. (Beispiel: $n \cdot \left(\frac{1}{n}\right)$ mit $R = \mathbb{Z}$)
- b) Für gebrochene Ideale I, J von R sei $I \cdot J$ der von allen $a \cdot b$, $a \in I, b \in J$, erzeugte R -Untermodul von K .
- c) Die gebrochenen Ideale von R bilden mit der Multiplikation aus b) ein kommutatives Monoid mit neutralem Element R .
- d) Die Einheiten in diesem Monoid heißen **invertierbare** (gebrochene) Ideale.
d.h. I invertierbar $\Leftrightarrow \exists I'$ mit $I \cdot I' = R$.

Beispiele

0) Jedes Ideal in R .

1) Jeder endlich erzeugbare R -Untermodul von K ist gebrochenes Ideal.

denn: Seien $x_1 = \frac{a_1}{b_1}, \dots, x_n = \frac{a_n}{b_n}$ Erzeuger von M ($a_i, b_i \in R$) \Rightarrow für $b = b_1 \cdot \dots \cdot b_n$ ist $b \cdot M \subseteq R$.

2) Ist I gebrochenes Ideal, so ist $I^{-1} := \{x \in K : x \cdot I \subseteq R\}$ ebenfalls gebrochenes Ideal: für jedes $a \in I$ ist $a \cdot I^{-1} \subseteq R$.

I ist invertierbar $\Leftrightarrow I \cdot I^{-1} = R$.

3) $R = k[X, Y]$, $I = (X, Y) \Rightarrow I^{-1} = R$.

denn: für $a = \frac{f}{g} \in I^{-1}$ muss gelten: $a \cdot X \in R$, $a \cdot Y \in R$.

4) Jedes Hauptideal $\neq (0)$ ist invertierbar: $(a) \cdot (\frac{1}{a} \cdot R) = R$.

Bemerkung 2.41

Jedes invertierbare Ideal in einem Integritätsbereich ist endlich erzeugbar (als R -Modul).

Beweis

Sei I invertierbar, also $I \cdot I^{-1} = R$, dann gibt es $a_i \in I, b_i \in I^{-1}$ mit $1 = \sum_{i=1}^n a_i b_i$

Beh: a_1, \dots, a_n erzeugen I .

denn: Sei $a \in I \Rightarrow a = a \cdot 1 = a \cdot \sum_{i=1}^n a_i b_i = \sum_{i=1}^n a_i \underbrace{(a b_i)}_{\in R}$

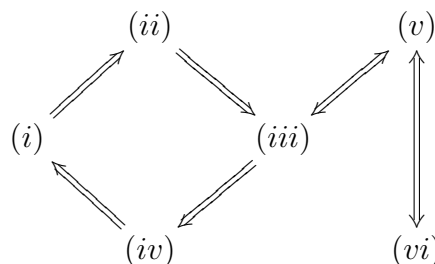
Satz 13 (Dedekindringe)

Für einen nullteilerfreien Ring R sind äquivalent:

- (i) R ist Dedekindring oder Körper.
- (ii) R ist noethersch und $R_{\mathfrak{p}}$ ist diskreter Bewertungsring für jedes Primideal $\mathfrak{p} \neq (0)$ in R .
- (iii) Jedes Ideal $I \neq (0)$ in R ist invertierbar.
- (iv) Die gebrochenen Ideal in R bilden eine Gruppe.
- (v) Jedes echte Ideal in R ist Produkt von endlich vielen Primidealen.
- (vi) Jedes echte Ideal besitzt eine eindeutige Darstellung als Produkt von endlich vielen Primidealen.

Beweis

Beweisplan:



(i) \Rightarrow (ii) :

Sei $\mathfrak{p} \neq (0)$ Primideal im Dedekindring R . $\Rightarrow R_{\mathfrak{p}}$ noethersch, $\dim R_{\mathfrak{p}} = \text{lat}(\mathfrak{p}) = 1$, da $\dim R = 1$.

$R_{\mathfrak{p}}$ normal: Sei $a \in K = \text{Quot}(R) = \text{Quot}(R_{\mathfrak{p}})$ ganz über $R_{\mathfrak{p}}$.

Dann gibt es eine Gleichung: $a^n + \sum_{i=0}^{n-1} \frac{b_i}{s_i} a^i = 0$ mit $b_i \in R, s_i \in R \setminus \mathfrak{p}$

$\Rightarrow (s \cdot a)^n + \sum_{i=0}^{n-1} \tilde{b}_i (sa)^i = 0$ mit $\tilde{b}_i \in R, s := \prod_{i=0}^{n-1} s_i$

$\xRightarrow{R \text{ normal}} s \cdot a \in R \Rightarrow a = \frac{s \cdot a}{s} \in R_{\mathfrak{p}}$

(iii) \Rightarrow (iv) :

Sei $(0) \neq I \subset K$ gebrochenes Ideal, $a \in R \setminus \{0\}$ mit $a \cdot I \subseteq R$. $\xRightarrow{(iii)} a \cdot I$ invertierbar. \Rightarrow

$R = (a \cdot I) \cdot I' = I \cdot (a \cdot I') \Rightarrow I$ ist invertierbar.

(ii) \Rightarrow (iii) :

Sei $I \neq (0)$ Ideal in R . $K = \text{Quot}(R)$. $I^{-1} := \{x \in K : x \cdot I \subseteq R\}$

Zu zeigen: $I \cdot I^{-1} = R$.

Annahme: $I \cdot I^{-1} \subsetneq R$:

Dann gibt es ein maximales Ideal \mathfrak{m} von R mit $I \cdot I^{-1} \subseteq \mathfrak{m}$.

$\Rightarrow R_{\mathfrak{m}}$ ist diskreter Bewertungsring.

$\Rightarrow I \cdot R_{\mathfrak{m}}$ ist Hauptideal, d.h. $I \cdot R_{\mathfrak{m}} = \frac{a}{s} \cdot R_{\mathfrak{m}}$ für ein $a \in I, s \in R \setminus \mathfrak{m}$

Seien $b_1, \dots, b_n \in I$ Erzeuger (R ist noethersch). $\Rightarrow \frac{b_i}{1} = \frac{a}{s} \cdot \frac{r_i}{s_i}$ für gewisse $r_i \in R, s_i \in R \setminus \mathfrak{m}$

Sei $t = s \cdot \prod_{i=1}^n s_i$. Es gilt: $t \in R \setminus \mathfrak{m}$.

Für jedes $i = 1, \dots, n$ ist $\frac{t}{a} \cdot b_i = r_i \cdot s_i \cdot \dots \cdot \hat{s}_i \cdot \dots \cdot s_n \in R$.

$\Rightarrow \frac{t}{a} \in I^{-1} \Rightarrow t = a \cdot \frac{t}{a} \in I \cdot I^{-1} \subseteq \mathfrak{m}$. Widerspruch.

(iv) \Rightarrow (i) :

R noethersch: Nach [Bemerkung 2.41](#) ist jedes invertierbare Ideal endlich erzeugbar.

R normal: Sei $x \in K$ ganz über R . $\Rightarrow R[x]$ ist endlich erzeugbarer R -Modul, also gebrochenes Ideal (Beispiel 1). $\xRightarrow{(iv)} R[x]$ ist invertierbar.

Da $R[x]$ Ring ist, gilt $R[x] \cdot R[x] = R[x]$. $\xRightarrow{R[x] \text{ invertierbar}} R[x] = R$ (neutrale Element).

$\Rightarrow x \in R$.

$\dim R \leq 1$: Sei $\mathfrak{p} \neq (0)$ Primideal in R , $\mathfrak{m} \subseteq R$ maximales Ideal mit $\mathfrak{p} \subseteq \mathfrak{m}$.

$\Rightarrow \mathfrak{m}^{-1} \cdot \mathfrak{p} \subseteq \mathfrak{m}^{-1} \mathfrak{m} = R$ und $\mathfrak{m} \cdot (\mathfrak{m}^{-1} \mathfrak{p}) = \mathfrak{p}$.

$\xRightarrow{\mathfrak{p} \text{ Primideal}} \mathfrak{m} = \mathfrak{p}$ oder $\mathfrak{m}^{-1} \mathfrak{p} \subseteq \mathfrak{p}$.

Falls $\mathfrak{m}^{-1} \mathfrak{p} \subseteq \mathfrak{p} \xrightarrow{\mathfrak{p}^{-1}} \mathfrak{m}^{-1} \subseteq R$. Widerspruch (da sonst $\mathfrak{m}^{-1} \cdot \mathfrak{m} \subseteq \mathfrak{m}$)

(iii) \Rightarrow (v) :

Sei $I \neq (0), I \neq R$ Ideal in R .

Setze $I_0 := I$.

Definiere induktiv: I_n für $n \geq 1$:

Ist $I_{n-1} \neq R$, so sei \mathfrak{m}_{n-1} maximales Ideal mit $I_{n-1} \subseteq \mathfrak{m}_{n-1}$ und $I_n := I_{n-1}\mathfrak{m}_{n-1}^{-1} \subseteq R$.

Es ist $I_{n-1} \subseteq I_n$

Wäre $I_n = I_{n-1}$, so wäre $\mathfrak{m}_{n-1}^{-1} = R$. Widerspruch zu $\mathfrak{m}_{n-1}^{-1} \cdot \mathfrak{m}_{n-1} = R$.

Da nach 2.41 R noethersch ist, wird die Kette $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ stationär.

$\Rightarrow \exists n$ mit $R = I_n = I_{n-1}\mathfrak{m}_{n-1}^{-1} = I_{n-2}\mathfrak{m}_{n-2}^{-1}\mathfrak{m}_{n-1}^{-1} = \dots = I_0 \cdot \prod_{i=0}^{n-1} \mathfrak{m}_i^{-1}$

$\Rightarrow I = I_0 = \prod_{i=0}^{n-1} \mathfrak{m}_i$

(v) \Rightarrow (vi) :

Sei $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ mit Primidealen $\mathfrak{p}_i, \mathfrak{q}_i$. Zu zeigen: $n = m$ und $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ für eine Permutation $\sigma \in S_n$:

Induktion über n :

$n = 1$: $\mathfrak{p} = \mathfrak{p}_1 = \mathfrak{q}_1 \cdots \mathfrak{q}_m \underset{\mathfrak{p} \text{ prim}}{\Rightarrow} \exists i_0$ mit $\mathfrak{q}_{i_0} \subseteq \mathfrak{p}$. Umgekehrt ist $\mathfrak{p} \subseteq \mathfrak{q}_i$ für jedes i . $\Rightarrow \mathfrak{p} = \mathfrak{q}_{i_0}$

$n > 1$: Ohne Einschränkung \mathfrak{p}_1 minimal bzgl. \subseteq in $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.

Aus $\prod \mathfrak{q}_i \subseteq \prod \mathfrak{p}_j \subseteq \mathfrak{q}_{i_1} \Rightarrow \exists j_0$ mit $\mathfrak{p}_{j_0} \subseteq \mathfrak{q}_{i_0} \subseteq \mathfrak{p}_1 \underset{\mathfrak{p}_1 \text{ minimal}}{\Rightarrow} \mathfrak{p}_1 = \mathfrak{q}_{i_0} \underset{\text{(iii)}}{\Rightarrow} \mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \widehat{\mathfrak{q}_{i_0}} \cdots \mathfrak{q}_m \Rightarrow$ Behauptung aus Induktionsvoraussetzung.

(v) \Rightarrow (iii) :

Sei $I \neq (0)$, $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ mit Primidealen \mathfrak{p}_i . Ist jedes \mathfrak{p}_i invertierbar, so ist $I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$ und $I \cdot I^{-1} = R$. Also ohne Einschränkung $I = \mathfrak{p}$ Primideal.

Sei $a \in \mathfrak{p} - \{0\}$, $(a) = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ mit Primidealen $\mathfrak{q}_i \Rightarrow \mathfrak{q}_i \subseteq \mathfrak{p}$ für ein i .

\mathfrak{q}_i ist invertierbar: $\mathfrak{q}_i^{-1} = \frac{1}{a} \cdot R \cdot \mathfrak{q}_1 \cdots \widehat{\mathfrak{q}_i} \cdots \mathfrak{q}_n$

Es genügt also zu zeigen: $\mathfrak{q}_i = \mathfrak{p}$

Beh. 1: Jedes invertierbare Primideal \mathfrak{q} in R ist maximal.

Bew. 1: Ist \mathfrak{q} nicht maximal, so sei $x \in R \setminus \mathfrak{q}$ mit $\mathfrak{q} + (x) \neq R$.

Beh. 2: Dann ist $(\mathfrak{q} + (x))^2 = \mathfrak{q} + (x^2)$

Dann ist $\mathfrak{q} \subseteq \mathfrak{q} + (x^2) \underset{\text{Beh. 2}}{=} (\mathfrak{q} + (x))^2 \subseteq \mathfrak{q}^2 + (x) (*)$

Weiter ist $\mathfrak{q} \subseteq \mathfrak{q}^2 + \mathfrak{q} \cdot (x)$

denn: Sei $b \in \mathfrak{q}$, schreibe nach (*) $b = c + rx$ mit $c = \mathfrak{q}^2, r \in R$, dabei ist $r \in \mathfrak{q}$, da $r \cdot x \in \mathfrak{q}$ und $x \notin \mathfrak{q}$.

$\Rightarrow \mathfrak{q} = \mathfrak{q}^2 + \mathfrak{q} \cdot (x)$ („ \supseteq “ ist trivial)

$\Rightarrow \mathfrak{q} = \mathfrak{q}(\mathfrak{q} + (x)) \underset{\mathfrak{q} \text{ invertierbar}}{\Rightarrow} R = \mathfrak{q} + (x)$ Widerspruch.

Bew. 2: „ \subseteq “ \checkmark , „ \supseteq “

Schreibe beide Seiten als Produkt von Primidealen.

$\mathfrak{q} + (x) = \mathfrak{p}_1 \cdots \mathfrak{q}_r, \mathfrak{q} + (x^2) = \mathfrak{q}_1 \cdots \mathfrak{q}_s$.

In R/\mathfrak{q} ist dann: $(\bar{x}) = \bar{\mathfrak{p}}_1 \cdots \bar{\mathfrak{p}}_r, (\bar{x})^2 = \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_s = \bar{\mathfrak{p}}_1^2 \cdots \bar{\mathfrak{q}}_r^2$

$(\bar{x}), (\bar{x}^2)$ invertierbar. $\Rightarrow \bar{\mathfrak{p}}_i, \bar{\mathfrak{q}}_j$ invertierbar.

$\underset{\text{„(iii) + (v) = (vi)“}}{\Rightarrow} \bar{\mathfrak{q}}_i = \bar{\mathfrak{p}}_{\sigma(i)}^2 \Rightarrow$ ohne Einschränkung $\mathfrak{q}_i = \mathfrak{p}_i^2$.

Satz 14

Sie R ein Dedekindring, $K = \text{Quot}(R)$, L/K endliche separable Körpererweiterung. S der ganze Abschluß von R in L .

Dann ist S ein Dedekindring.

Beweis

$\dim S = 1$: Folgt aus Satz 10(c)

S normal:

Sei $x \in L$ ganz über S , also $x^n + \sum_{i=1}^{n-1} a_i x^i = 0$ mit $a_i \in S$. Sei S' der von R und a_1, \dots, a_{n-1} erzeugte Unterring von S . S' ist endlich erzeugbarer R -Modul, da die a_i ganz über R sind. $S[X]$ ist endlich erzeugter S' -Modul und damit endlich erzeugbarer R -Modul $\Rightarrow x$ ist ganz über $R \Rightarrow x \in S$.

S noethersch:

Beh. 1: Es gibt ein primitives Element α von L/K mit $\alpha \in S$.

Bew. 1: Sei $\tilde{\alpha} \in L$ primitives Element, also $1, \tilde{\alpha}, \tilde{\alpha}^2, \dots, \tilde{\alpha}^{n-1}$ ist K -Basis von L ($n := [L : K]$). Sei $\tilde{\alpha} = \sum_{i=0}^{n-1} c_i \tilde{\alpha}^i$ für gewisse $c_i \in K$, $i = 0, \dots, n-1$. Schreibe $c_i = \frac{a_i}{b_i}$ mit $a_i, b_i \in R$, $b := \prod_{i=0}^{n-1} b_i$. Setze $\alpha := b \cdot \tilde{\alpha} \Rightarrow \alpha^n = b^n \cdot \sum_{i=0}^{n-1} c_i \tilde{\alpha}^i = \sum_{i=0}^{n-1} \underbrace{c_i b^{n-i}}_{\in R} \alpha^i \Rightarrow \alpha \in S$

$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ linear unabhängig:

Sei $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0 \Rightarrow \sum \lambda_i b^i \tilde{\alpha}^i = 0 \Rightarrow \lambda_i b^i = 0 \forall i$

Sei nun \bar{K} ein algebraischer Abschluss von K . Seien $\sigma_1, \dots, \sigma_n$ die verschiedenen Einbettungen von L in \bar{K} , also die Elemente von $\text{Hom}(L, \bar{K})$.

$d := d(\alpha) := (\det(\sigma_i(\alpha^{j-1}))_{i,j=1,\dots,n})^2$ heißt die Diskriminante von L/K (bzgl. α).

Beh. 2:

(a) $d \neq 0$

(b) S ist in dem von $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}$ erzeugten R -Untermodul von L enthalten.

Dann ist S als Untermodul eines endlich erzeugbaren R -Modul selbst endlich erzeugbar und damit noethersch (weil R noethersch ist).

Bew. 2:

$$(a) \quad d = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \dots & \sigma_n(\alpha) \\ \sigma_1(\alpha)^2 & \sigma_2(\alpha)^2 & \dots & \sigma_n(\alpha)^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha)^{n-1} & \sigma_2(\alpha)^{n-1} & \dots & \sigma_n(\alpha)^{n-1} \end{pmatrix} \stackrel{\text{Vandermonde}}{=} \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha)) \neq 0$$

(b) Für $x \in L$ sei $\text{Spur}(x) := \sum_{i=1}^n \sigma_i(x) \in \bar{K}$

$\text{Spur}(x) \in K$: Für $\sigma \in \text{Aut}_K(\bar{K})$ ist $\sigma \circ \sigma_i \in \text{Hom}_K(L, \bar{K})$

$\sigma(\text{Spur}(x)) = \sum_{i=1}^n (\sigma \circ \sigma_i)(x) = \text{Spur}(x) \in \bar{K}^{\text{Aut}_K(\bar{K})} = K$.

Sei $x \in S$, $x = \sum_{j=1}^n c_j \alpha^j$ mit $c_j \in K$.

Beh. 3: $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ ist Lösung eines LGS $A \cdot c = b$ mit $b \in R^n$ und $A \in R^{n \times n}$ mit $\det A = d$.

Nach der Cramerschen Regel ist dann $c_i = \frac{\det A_i}{\det A}$ wobei A_i aus A dadurch entsteht, dass die i -te Zeile durch b ersetzt wird. $\Rightarrow c_i \in \frac{1}{d}R \Rightarrow x$ liegt in dem von $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}$ erzeugten R -Modul.

Bew. 3: Für $i = 1, \dots, n$ ist $\text{Spur}(\alpha^{i-1}x) = \sum_{j=1}^n \text{Spur}((\alpha^{i-1}\alpha^{j-1})c_j) \in K$ (*) ganz über R
 $\Rightarrow \text{Spur}(\alpha^{i-1}x) \in R \Rightarrow A := (\text{Spur}(\alpha^{i-1}\alpha^{j-1}))_{i,j=1,\dots,n} \in R^{n \times n}$

$$b := \begin{pmatrix} \text{Spur}(x) \\ \text{Spur}(\alpha x) \\ \vdots \\ \text{Spur}(\alpha^{n-1}x) \end{pmatrix} \in R^n \text{ (*) heißt } A \cdot c = b.$$

Noch zu zeigen: $\det A = d$.

Nach Definition ist $d = (\det B)^2$ mit $B = (\sigma_i(\alpha^{j-1}))_{i,j}$

$$\Rightarrow B^T \cdot B = (\beta_{ij}) \text{ mit } \beta_{ij} = \sum_{k=1}^n \sigma(\alpha^{i-1})\sigma_k(\alpha^{j-1}) = \text{Spur}(\alpha^{i-1}\alpha^{j-1})$$

$$\Rightarrow B^T \cdot B = A \Rightarrow \det A = (\det B)^2 = d$$

Beispiele

$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$, D quadratfrei, $R = \mathbb{Z}$.

Was ist d ? $\alpha = \sqrt{D}$, $\sigma_1 = \text{id}$, $\sigma_2(a + b\sqrt{D}) = a - b\sqrt{D}$

$$B = \begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix}$$

$$d = (\det B)^2 = (-2\sqrt{D})^2 = 4D$$

§11 Primärzerlegung

Beispiele

$R = k[X, Y]$. $I = (X^2, Y)$ hat keine Darstellung als Produkt von Primidealen.

denn: Wäre $I = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$ mit paarweise verschiedenen Primidealen \mathfrak{p}_i , so wäre $\sqrt{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = (X, Y) = \mathfrak{m}$. also $r = 1$, $\mathfrak{p}_1 = \mathfrak{m}$. Aber: $\mathfrak{m} \not\supseteq I \not\supseteq \mathfrak{m}^2$.

Definition + Bemerkung 2.42

Sei R Ring, $\mathfrak{q} \subseteq R$ echtes Ideal.

- \mathfrak{q} heißt **Primärideal**, wenn für alle $a, b \in R$ mit $a \cdot b \in \mathfrak{q}$ und $a \notin \mathfrak{q}$ gilt: es gibt ein $n \geq 1$ mit $b^n \in \mathfrak{q}$.
- Ist \mathfrak{q} Primärideal, so ist $\mathfrak{p} = \sqrt{\mathfrak{q}}$ Primideal. \mathfrak{p} heißt zu \mathfrak{q} **assoziertes** Primideal.

Beweis

Seien $a, b \in R$ mit $a \cdot b \in \sqrt{\mathfrak{q}} \Rightarrow a^n b^n \in \mathfrak{q}$ für ein $n \geq 1$.

Ist $a \notin \sqrt{\mathfrak{q}}$, so ist $a^n \notin \mathfrak{q} \xRightarrow{\text{Def.}} (b^n)^m \in \mathfrak{q} \Rightarrow b \in \sqrt{\mathfrak{q}}$

- \mathfrak{q} Primärideal \Leftrightarrow jeder Nullteiler in R/\mathfrak{q} ist nilpotent.

Beispiele

- Ist $p \in R$ ein Primelement, so ist $(p^n) = (p)^n$ Primärideal für jedes $n \geq 1$.

denn: Seien $a, b \in R$ mit $a \cdot b \in (p^n)$ und $a \notin (p^n)$. Ist $b \in (p)$, so ist $b^n \in (p^n)$.

Anderenfalls ist $a \in (p)$. Dann gibt es $1 \leq d < n$ mit $a \in (p^d) \setminus (p^{d+1}) \Rightarrow a = p^d \cdot u$ mit $u \in R \setminus (p)$. Dann ist $u \cdot b \notin (p) \Rightarrow a \cdot b = p^d \cdot u \cdot b \notin (p^{d+1})$ Widerspruch.

2) Ist R Dedekindring, so sind die Primär Ideale genau die Potenzen von Primidealen.

denn: Ist \mathfrak{q} Primärideal, $\mathfrak{q} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$ die Zerlegung von \mathfrak{q} in Primidealen.

$$\Rightarrow \sqrt{\mathfrak{q}} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \quad \sqrt{\mathfrak{q}} \text{ ist prim} \Rightarrow r = 1.$$

Sei umgekehrt $\mathfrak{q} = \mathfrak{p}^n$ für ein Primideal \mathfrak{p} , $n \geq 1$. Seien $a, b \in R$, $a \cdot b \in \mathfrak{p}^n$, $a \notin \mathfrak{p}^n$. Nach **Satz 13** ist $R_{\mathfrak{p}}$ Hauptidealring. D.h. $\mathfrak{p}R_{\mathfrak{p}}$ wird erzeugt von einem $\frac{p}{s}$, wobei $p \in \mathfrak{p}$, $s \in R \setminus \mathfrak{p}$

$$\Rightarrow \mathfrak{p}^n R_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^n \text{ ist Primideal.}$$

Ist $a \in \mathfrak{p}^n R_{\mathfrak{p}}$, so ist $a = \frac{p^n}{s^n} \cdot \frac{u}{t}$ mit $u \in R, t \in R \setminus \mathfrak{p} \Rightarrow t \cdot s^n \cdot a \in \mathfrak{p}^n \Rightarrow a \in \mathfrak{p}^n$. Widerspruch.

Anderenfalls ist $b^m \in \mathfrak{p}^n R_{\mathfrak{p}}$ für ein m und damit $b \in \mathfrak{p}$ und $b^n \in \mathfrak{p}^n$.

Bemerkung 2.43

Sind I_1, \dots, I_r \mathfrak{p} -primär (d.h. I_i primär und $\sqrt{I_i} = \mathfrak{p}$), so ist auch $I := \bigcap_{i=1}^r I_i$ \mathfrak{p} -primär.

Beweis

Seien $a, b \in R$ mit $a \cdot b \in I$, $a \notin I$. Dann gibt es i mit $a \notin I_i \Rightarrow b^{n_i} \in I_i$ für ein $n_i \geq 1 \Rightarrow b \in \sqrt{I_i} = \mathfrak{p} \Rightarrow$ Für $j = 1, \dots, r$ gibt es $n_j \geq 1$ mit $b^{n_j} \in I_j \Rightarrow b^n \in I$ für $n = \max_{j=1}^r n_j$.

Definition 2.44

Sei I Ideal in R .

- Eine Darstellung $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ heißt **Primärzerlegung** von I , wenn alle \mathfrak{q}_i primär sind.
- Eine Primärzerlegung heißt **reduziert**, wenn $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ für $i \neq j$ und kein \mathfrak{q}_i weggelassen werden kann.
- Besitzt \mathfrak{q} eine Primärzerlegung, so auch eine reduzierte.

Satz 15 (Reduzierte Primärzerlegung)

Sei R noetherscher Ring.

Dann hat jedes echte Ideal in R eine reduzierte Primärzerlegung. Die assoziierten Primideale sind eindeutig. Die Primär Ideale, deren assoziierten Primideale minimal unter den in der Zerlegung vorkommenden sind, sind ebenfalls eindeutig.

Beweis

Sei $\mathcal{B} = \{I \subset R \text{ Ideal} : I \text{ besitzt keine Primärzerlegung}\}$. Ist $\mathcal{B} \neq \emptyset$, so besitzt \mathcal{B} ein maximales Element I_0 . Da I_0 nicht primär ist, gibt es $a, b \in R$ mit $a \cdot b \in I_0$ und $a \notin I_0$ und $b^n \notin I_0$ für alle $n \geq 1$.

Ziel: Konstruiere Ideale I und J mit $I_0 = I \cap J$ und $I \neq I_0 \neq J$. Dann haben I und J Primärzerlegungen, also I_0 auch. Widerspruch!

Für $n \geq 1$ sei $I_n := \{c \in R : c \cdot b^n \in I_0\}$. I_n ist Ideal mit $I_0 \subseteq I_n \subseteq I_{n+1}$. Da R noethersch ist, gibt es $k \in \mathbb{N}$ mit $I_n = I_k$ für alle $n \geq k$. Setze $I := I_n$. Beachte $a \in I_1 \setminus I_0 \subseteq I \setminus I_0$.

Sei $J := I_0 + (b^k) \supsetneq I_0$, da $b^k \notin I_0$.

Beh: $I \cap J = I_0$

denn: „ \supseteq “ \checkmark „ \subseteq “ Sei $y \in I \cap J$, also $y = x + b^k \cdot r$ (für ein $x \in I_0, r \in R$) und $y \cdot b^k \in I_0 \Rightarrow y \cdot b^k = b^{2k} \cdot r + x \cdot b^k \Rightarrow r \cdot b^{2k} = y b^k \cdot x b^k \Rightarrow r \in I_{2k} = I_k \Rightarrow r \cdot b^k \in I_0 \Rightarrow y \in I_0$.

Vokabeln

- Abbildung
 - alternierende, 13
 - graderhaltende, 27
 - symmetrische, 13
- abgeschlossen, 38
- Abschluss
 - ganzer, 23
- Absolutbetrag, 42
- Algebra
 - symmetrische, 13
 - äußere, 13
- Basis, 4
- Bewertung
 - diskrete, 42
 - p-adische, 42
- de Rahm-Komplex, 17
- Dedekindring, 46
- Derivation, 14
- Graßmann-Algebra, 13
- Hilbert
 - Polynom, 28
 - Reihe, 28
- homogen
 - Elemente, 25
 - Ideal, 25
- Ideal
 - gebrochenes, 46
- Invariantenring, 30
- irreduzibel
 - Komponente, 40
 - topologischer Raum, 39
- Jacobson-Radikal, 32
- Kategorie
 - abelsche, 3
 - R-Mod, 3
- Krull-Dimension, 34
- linear unabhängig, 4
- Normalisierung, 23
- Nullstellenmenge, 24
- p-adischen Zahlen, 43
- Potenz
 - symmetrische, 13
 - äußere, 13
- Primideal
 - assoziertes, 51
- Primidealkette, 34
 - Höhe, 34
- Primärideal, 51
- Primärzerlegung, 52
 - reduziert, 52
- R-Algebra, 11
- R-bilinear, 7
- R-linear, 2
- R-Modul, 2
 - Homomorphismus, 2
 - dualer, 2
 - flacher, 10
 - freier, 4
 - graduierter, 26
 - injektiver, 4
 - noetherscher, 19
 - projektiver, 4
- Ring
 - diskreter Bewertungs-, 43
 - ganz abgeschlossener, 23
 - graduierter, 25
 - noetherscher, 19
 - normaler, 23
- Ringerweiterung, 11
 - ganze, 22
- Spektrum, 38
- Tensorprodukt, 7
- Transzendenzgrad, 38
- Twist, 27
- Verschwindungsideal, 24, 40
- Zariski-Topologie, 38