0 Wiederholungen

Der affine Fall

(1) Sei K ein Körper, $\mathfrak{a} \subseteq R := K[x_1,\dots,x_n]$. Die Nullstellenmenge

$$V(\mathfrak{a}) := \left\{P \in \mathbb{A}^n \mid \forall f \in \mathfrak{a} : f(P) = 0\right\} \subseteq \mathbb{A}^n$$

heißt eine *affine Varietät*, die durch $\mathfrak{a}$ definiert wird.

(2) Sei $W \subseteq \mathbb{A}^n$. $I(W) := \left\{f \in R \mid \forall P \in W : f(P) = 0\right\}$ heißt das *Ideal von* W.

(3) Es gelten:

(i) Ist $W \subseteq \mathbb{A}^n$ eine affine Varietät, so ist $V(I(W)) = W$.

(ii) $\mathfrak{a} \subseteq I(V(\mathfrak{a}))$.

(iii) $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow V(\mathfrak{b}) \subseteq V(\mathfrak{a})$, $W_1 \subseteq W_2 \Rightarrow I(W_2) \subseteq I(W_1)$.

(iv) Sind $W_1, W_2 \subseteq \mathbb{A}^n$ affine Varietäten, so ist $W_1 \cap W_2 = V(I(W_1) + I(W_2))$, $W_1 \cup W_2 = V(I(W_1) \cap I(W_2))$.

(v) *Hilbertscher Nullstellensatz*: Ist $K = \overline{K}$, so gilt für jede affine Varietät $W \subseteq \mathbb{A}^n$, die durch $\mathfrak{a}$ definiert wird:

$$I(W) = I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Damit erhält man die Beziehung

$$\begin{array}{ccccc}
\{\text{Untervarietäten des } \mathbb{A}^n\} & \overset{1:1}{\longleftrightarrow} & \{\text{Radikalideale von } R\} & \overset{1:1}{\longleftrightarrow} & \{\text{Faktorringe von } R \text{ ohne nilpotente Elemente}\} \\
W \longmapsto I(W) & & \mathfrak{a} \longmapsto R/\mathfrak{a} & & \\
V(\mathfrak{a}) \longleftarrow \mathfrak{a} & & \mathrm{Kern}(R \to A) \longleftarrow A & &
\end{array}$$

Ist $P = (a_1,\dots,a_n) \in \mathbb{A}^n$ ein Punkt, so ist $I(P) = (x_1 - a_1,\dots,x_n - a_n)$ ein maximales Ideal in R. Es gelten $\dim P = 0$ und $\dim R/I(P) = 0$.

Der projektive Fall

Sei $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$, $f \in R := K[x_0,\dots,x_n]$. Sagen wir, f habe eine Nullstelle in P, so meinen wir

$$\forall \lambda \in K : f(\lambda a_0,\dots,\lambda a_n) = 0.$$

Ist K unendlich, so folgt schon, daß für jede homogene Komponente f_p gelten muß $f_p(P) = 0$. Daraus folgt für $\varnothing \neq W \subset \mathbb{P}^n$, daß $I(W) := \left\{f \in R \mid \forall P \in W : f(P) = 0\right\}$ homogen ist. Ist $K = \overline{K}$, so haben wir die Beziehung

$$\{\text{Untervarietäten des } \mathbb{P}^n\} \overset{1:1}{\longleftrightarrow} \{\text{homogene Ideale } \mathfrak{a} \subseteq (x_0,\dots,x_n) \text{ mit } \sqrt{\mathfrak{a}} = \mathfrak{a}.\} \overset{1:1}{\longleftrightarrow} \{\text{Graduierte Faktorringe von } R \text{ ohne nilpotente Elemente}\}$$

Sei $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ ein Punkt. Wir nehmen $a_i \neq 0$ an. Wir haben die Beziehung

$$P \longleftrightarrow I(P) = (a_i x_j - a_j x_i),\ j \in \{0,\dots,n\} \setminus \{i\},$$

$I(P)$ hat n Erzeugende. Es gelten $\dim P = 0$, $\dim R/I(P) = 1$.

Sei $Q = (1 : 0 : \ldots : 0)$, $I(Q) = (x_1,\dots,x_n)$, also ist $R/I(Q) \cong K[x]$.

$\varnothing \longleftrightarrow \mathfrak{m} = (x_0,\dots,x_n)$.

Graduierte Algebren

Eine K-Algebra heißt *graduiert*, wenn A eine Zerlegung $A = \bigoplus_{j \in \mathbb{N}_0} [A]_j$ besitzt, wobei $[A]_j$ K-Vektorräume sind, $K \subseteq [A]_0$ und $[A]_i \cdot [A]_j \subseteq [A]_{i+j}$. Die Elemente in $A_j := [A]_j$ heißen die *homogenen Elemente in A* von Grad j. $[A]_j$ wird die *Komponente von Grad j in A* genannt.

Beispiele:

(1) $A = R = K[x_0, \ldots, x_n]$. $[R]_j$ ist die Menge der homogenen Polynome von Grad j.

(2) Ist $\mathfrak{a} \subseteq R$ ein homogenes Ideal, so ist $A = R/\mathfrak{a}$ eine graduierte K-Algebra mit der Graduierung

(1) $$[A]_j := \left\{ f \bmod \mathfrak{a} \,\middle|\, f \in [R]_j \right\}.$$

(3) Umgekehrt: Ist $\mathfrak{a}$ irgendein Ideal von R, so liefert (1) eine Graduierung von $R/\mathfrak{a}$ genau dann wenn $\mathfrak{a}$ homogen ist.

1 Schemata

Wir wollen nun den Begriff einer Varietät verallgemeinern:

1.1 Beispiel. Betrachte

$$J_1 = (x(x-y)),\ J_2 = (y)\ \subseteq R = K[x,y]$$

und $W_1 = V(J_1),\ W_2 = V(J_2)\ \in \mathbb{A}^2$. W_2 ist die y-Achse, W_1 ist die x-Achse vereinigt mit der Winkelhalbierenden des ersten bzw. dritten Quadranten. $W_1 \cap W_2$ ist als Varietät gerade $(0,0)$, denn

$$I(W_1 \cap W_2) = \sqrt{J_1 + J_2} = \sqrt{x^2 - xy, y} = \sqrt{x^2, y} = (x,y).$$

Intuitiv sollte der Schnittpunkt doppelt gezählt werden, was in dem Ideal $(x^2, y) = J_1 + J_2$ besser beschrieben wird.

1.2 Definition. Ein *affines Unterschema* $X \subseteq \mathbb{A}^n$ ist gegeben durch einen Faktorring A von $R = K[x_1, \ldots, x_n]$. Dieser Ring A heißt der *Koordinatenring* von X. Ist $A = R/\mathfrak{a}$, so heißt $\mathfrak{a}$ das *definierende Ideal* von X und man schreibt affine Unterschemata Koordinatenring definierendes Ideal I_X

$$I_X = \mathfrak{a}.$$

Sind $X, Y \subseteq \mathbb{A}^n$ affine Unterschemata, so heißt X ein *Unterschema von* Y, falls $I_Y \subseteq I_X$ (Inklusionsumkehrend)

X und Y heißen *isomorph*, falls R/I_X und R/I_Y als K-Algebren isomorph sind. Isomorphie

Das *reduzierte Schema* X_{red} ist das durch $\sqrt{I_X}$ definierte Schema. (Ist K algebraisch abgeschlossen, so ist X_{red} also die Varietät $V(\sqrt{I_X})$.) reduziertes Schema X_{red}

1.3 Bemerkung. (i) Statt Unterschema sagen wir oft nur *Schema*, obwohl obige Definition nur ein Spezialfall des allgemeinen Begriffes eines Schemas ist. Schema

(ii) Intuition: Die Punkte des Schemas X sind die Punkte der Varietät X_{red}. Deren "Vielfachheit" wird im Ideal I_X widergespiegelt.

1.4 Beispiel. (i) $\mathfrak{a}_j = (x^j, y) \subseteq K[x,y]$ definert ein Unterschema $X_j \subseteq \mathbb{A}^2$. Es ist $(X_j)_{\text{red}} = P$, wobei $P = (0,0)$. (X_j ist ein "*dicker* Punkt.")

(ii) X_{j-1} ist ein Unterschema von X_j, denn $(x^j, y) \subseteq (x^{j-1}, y)$.

(iii) Ist $Y \subseteq \mathbb{A}^2$ der Punkt $(1,1)$, so sind Y und X_1 isomorph als Schemata.

1.5 Definition. (i) Sind $X, Y \subseteq \mathbb{A}^n$ affine Schemata, so ist der Durchschnitt $X \cap Y$ das durch $I_X + I_Y$ definierte Schema, und die Vereinigung $X \cup Y$ das durch $I_X \cap I_Y$ definierte Schema.

(ii) Das Schema $X \subseteq \mathbb{A}^n$ heißt *irreduzibel*, wenn gilt: Ist $X = X_1 \cup X_2$ für affine Unterschemata $X_1, X_2 \subseteq X$, so folgt $X = X_1$ oder $X = X_2$ oder $X_{\text{red}} = (X_1)_{\text{red}} = (X_2)_{\text{red}}$. Irreduzibilität

X heißt *reduziert*, falls $X = X_{\text{red}}$. reduzierte Schemata

1.6 Lemma. *Es sei $X \in \mathbb{A}^n$ ein Schema mit definierendem Ideal I_X. Dann gilt*

(a) X ist irreduzibel genau dann, wenn I_X ein Primärideal ist,

(b) X ist irreduzibel und reduziert genau dann, wenn I_X ein Primideal ist.

Beweis. (a) "$\Rightarrow$" Es sei $\operatorname{Ass}(R/I_X) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, und es sei $I_X = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ eine Primärzerlegung mit $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$.

Antithese: Es sei $s > 1$. Dann seien X_1, X_2 die durch $\mathfrak{q}_1$ bzw. $\mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_s$ definierten Schemata. Es folgt $X = X_1 \cup X_2$, aber $X \neq X_1, X \neq X_2$. Angenommen, es wäre $X_{\text{red}} = (X_1)_{\text{red}} = (X_2)_{\text{red}}$. Dann folgte, daß $\sqrt{I_X} = \sqrt{I_{X_1}} = \mathfrak{p}_1 = \sqrt{I_{X_2}} = \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_2$, also $\mathfrak{p}_1 = \mathfrak{p}_j$ für ein $j \in \{2, \ldots, s\}$, im Widerspruch zur Wahl der $\mathfrak{p}_i$.

Folglich ist X nicht irreduzibel, Widerspruch zur Voraussetzung.

"$\Leftarrow$" Sei $X = X_1 \cup X_2$. Nach Voraussetzung ist dann $\mathfrak{p} := \sqrt{I_X} = \sqrt{I_{X_1}} \cap \sqrt{I_{X_2}}$ ein Primideal. Daraus folgt O.E. $\mathfrak{p} = \sqrt{I_{X_1}}$. Fall 1: $\mathfrak{p} = \sqrt{I_{X_2}}$, d.h. $X_{\text{red}} = (X_1)_{\text{red}} = (X_2)_{\text{red}}$. Fall 2: $\mathfrak{p} \neq \sqrt{I_{X_2}} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$, also $\mathfrak{p} \subsetneq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$, es folgt $\mathfrak{p} \subsetneq \mathfrak{p}_i$ für alle $i \in \{1, \ldots, s\}$.

Wegen $\mathfrak{p} = \sqrt{I_X}$ hat $I_{X_1} = \mathfrak{q} \cap \tilde{\mathfrak{q}}_1 \cap \ldots \cap \tilde{\mathfrak{q}}_t$ eine Primärzerlegung, in der $\mathfrak{q}$ die einzige isolierte Komponente ist. Folglich ist $\mathfrak{q}$ auch die einzige isolierte Komponente von $I_{X_1} \cap I_{X_2} = I_X$. Da I_X ein Primärideal ist, folgt $\mathfrak{q} = I_X$ aus der Eindeutigkeit isolierter Komponenten. Es ergibt sich $\mathfrak{q} = I_{X_1} \cap I_{X_2} \subseteq I_{X_1} \subseteq \mathfrak{q}$, also $\mathfrak{q} = I_{X_1}$, d.h. $X = X_1$.

Aus der Fallunterscheidung folgt die Irreduzibilität von X.

(b) Folgt aus (a). □

1.7 Folgerung. Jedes affine Schema ist Vereinigung endlich vieler irreduzibler Schemata.

Beweis. Folgt aus der Existenz der Primärzerlegung im Polynomring. □

Wir wollen nun die analogen Begriffe im projektiven Raum einführen. Ist $\mathfrak{m} = (x_0, \ldots, x_n) \subseteq R = K[x_0, \ldots, x_n]$, so gilt für jedes $\mathfrak{m}$-primäre Ideal $\mathfrak{q}$: $V(\mathfrak{q}) = V(\mathfrak{m}) = \varnothing$.

saturierte Schemata

1.8 Definition. Es sei $\mathfrak{a} \subseteq \mathfrak{m}$ ein homogenes Ideal von R. Dann heißt $\mathfrak{a}$ *saturiert*, falls $\mathfrak{m} \notin \operatorname{Ass}(\mathfrak{a})$ gilt.

Saturierung $\mathfrak{a}_{\text{sat}}$

Das Ideal $\mathfrak{a}_{\text{sat}} := \bigcup_{j \geq 1} (\mathfrak{a} : \mathfrak{m}^j)$ heißt die *Saturierung* von $\mathfrak{a}$. $\mathfrak{a}_{\text{sat}}$ ist ein saturiertes homogenes Ideal. (Folgt aus Übungsaufgabe 2 und Lemma I.7.19.)

1.9 Beispiel. Betrachte $\mathfrak{a} = (x_0^2, x_1^2, x_0 x_1) \subseteq K[x_0, x_1, x_2]$. Es ist $\mathfrak{a} = (x_0, x_1^2) \cap (x_0^2, x_1, x_2)$ nicht saturiert, denn $\operatorname{Ass}(\mathfrak{a}) = \{(x_0, x_1), (x_0, x_1, x_2)\}$. Es ist $\mathfrak{a}_{\text{sat}} = (x_0, x_1^2)$.

Bemerkung: Ist $\mathfrak{a}$ nicht saturiert, so hat $\mathfrak{a}$ eine Primärzerlegung $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s \cap \mathfrak{q}_T$ mit $\sqrt{\mathfrak{q}_i} \subsetneq \sqrt{\mathfrak{q}_T} = \mathfrak{m}$. Dann ist $\mathfrak{a}_{\text{sat}} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$.

projektive Schemata

1.10 Definition. (i) Ein *projektives Unterschema* $X \subseteq \mathbb{P}^n$ ist gegeben durch einen graduierten Faktorring von $R := K[x_0, \ldots, x_n]$, der einen homogenen Nichtnullteiler positiven Grades besitzt.

homogenes Ideal I_X

homogener Koordinatenring

Ist $A = R/\mathfrak{a}$, so nennt man $\mathfrak{a}$ das *homogene Ideal* von X. Schreibweise $I_X = \mathfrak{a}$. Ferner wird A als *homogener Koordinatenring* von X bezeichnet.

(ii) Ist $\mathfrak{a} \subseteq \mathfrak{m} = (x_0, \ldots, x_n)$ ein homogenes Ideal, so *definiert* $\mathfrak{a}$ *das Schema* $R/\mathfrak{a}_{\text{sat}}$.

Dies ist sinnvoll nach folgendem Lemma:

1.11 Lemma. *Ist $\mathfrak{a} \subseteq \mathfrak{m}$ ein homogenes Ideal, das nicht $\mathfrak{m}$-primär ist, so besitzt $R/\mathfrak{a}$ einen homogenen Nichtnullteiler positiven Grades genau dann, wenn $\mathfrak{a}$ saturiert ist.*

Beweis. "$\Rightarrow$" Es sei $f \in R$ ein Repräsentant des Nichtnullteiler von $R/\mathfrak{a}$. Dann gilt $\mathfrak{a} : f = \mathfrak{a}$, denn die Abbildung

$$\begin{aligned} \nu : \quad R/\mathfrak{a} &\longrightarrow R/\mathfrak{a} \\ r \bmod \mathfrak{a} &\longmapsto (f \cdot r) \bmod \mathfrak{a} \end{aligned}$$

ist injektiv. Es ist $\nu(r \bmod \mathfrak{a}) = 0$ genau dann, wenn $fr \in \mathfrak{a}$. Aus der Injektivität folgt aber $r \bmod \mathfrak{a} = 0$, also $r \in \mathfrak{a}$. Dies bedeutet $\mathfrak{a} : f \subseteq \mathfrak{a}$, also $\mathfrak{a} : f = \mathfrak{a}$. Wäre $\mathfrak{m} \in \mathrm{Ass}(\mathfrak{a})$, so folgte wegen $f \bmod \mathfrak{a} \in \mathfrak{m} \bmod \mathfrak{a}$, daß $f \bmod \mathfrak{a}$ ein Nullteiler von $R/\mathfrak{a}$ wäre (nach Folgerung I.7.28), Widerspruch.

"$\Leftarrow$" Es sei $\mathfrak{a} = \mathfrak{q}_i \cap \ldots \cap \mathfrak{q}_s$ eine Primärzerlegung von $\mathfrak{a}$ mit $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Nach Voraussetzung gilt $\mathfrak{m} \subsetneq \mathfrak{p}_i$ für $i = 1 \ldots s$. Nach dem Primvermeidungslemma (IV.3.2) folgt die Existenz eines homogenen $f \in \mathfrak{m} \setminus \bigcup \mathfrak{p}_i$. Nach (I.7.28) ist $f \bmod \mathfrak{a}$ ein Nichtnullteiler von $R/\mathfrak{a}$ mit positivem Grad. □

1.12 Bemerkung. (i) Für ein homogenes Ideal $\mathfrak{a} \subseteq \mathfrak{m}$ gilt: $\mathfrak{a}$ ist $\mathfrak{m}$-primär genau dann, wenn $\sqrt{\mathfrak{a}} = \mathfrak{m}$.

(ii) Aus Lemma (1.11) und Definition (1.10) folgt

{projektive Unterschemata von $\mathbb{P}^n$} $\overset{1:1}{\longleftrightarrow}$ {graduierte Fakorrringe von $K[x_0, \ldots, x_n]$ mit einem homogenen Nichtnullteiler positiven Grades} $\overset{1:1}{\longleftrightarrow}$ {$K[x_0, \ldots, x_n]/\mathfrak{a}$, wobei $\mathfrak{a} \subseteq \mathfrak{m}$ ein homogenes saturiertes Ideal}

(iii) Ist $\mathfrak{a}$ ein homogenes, $\mathfrak{m}$-primäres Ideal, so sagen wir, daß $R/\mathfrak{a}$ die leere Menge (als Schema) definiert.

1.13 Definition. Seien $X, Y \subseteq \mathbb{P}^n$ Unterschemata. Dann ist der *Durchschnitt* definiert durch $I_X + I_Y$, also $I_{X \cap Y} = (I_X + I_Y)_{\mathrm{sat}}$.

Die *Vereinigung, Irreduzibilität, Reduziertheit und Unterschemata* von X sind wie für affine Schemata definiert.

X und Y heißen *isomorph*, wenn R/I_X und R/I_Y als graduierte K-Algebren isomorph sind.

Durchschnitt
Vereinigung
Irreduzibilität
Reduziertheit
Unterschemata
Isomorphie

1.14 Beispiel. $X, Y \subseteq \mathbb{P}^3$ mit $I_X = (x_0, x_1) \cap (x_2, x_3) = (x_0x_2, x_0x_3, x_1x_2, x_1x_3)$ (Paar windschiefer Geraden) und $I_Y = (x_1 + x_2)$ (Ebene). Erwartung: $X \cap Y$ besteht aus zwei Punkten.

$$I_X + I_Y = (x_0x_2, x_0x_3, x_1x_2, x_1x_3, x_1 + x_2) = (x_1, x_2, x_3) \cap (x_0, x_1, x_2) \cap \underbrace{(x_0, x_1x_2, x_1 + x_2, x_3)}_{\mathfrak{m}-\text{primär}},$$

also $(I_X + I_Y)_{\mathrm{sat}} = (x_0, x_1, x_2) \cap (x_1, x_2, x_3)$.

1.15 Erinnerung. Es sei A eine graduierte K-Algebra, dann ist die *Hilbertfunktion* gegeben durch

Hilbertfunktion h_A

$$h_A : \mathbb{Z} \to \mathbb{N}_0, \quad h_A(j) = \dim_K [A]_j.$$

Das *Hilbertpolynom* von A ist dasjenige Polynom $p_A \in \mathbb{Q}[T]$, so daß gilt $h_A(j) = p_A(j)$ für alle $j \gg 0$.

Hilbertpolynom p_A

Ist $d = \deg p_A$, so kann man das Hilbertpolynom schreiben als

$$p_A(j) = h_0(A)\binom{j}{d} + h_1(A)\binom{j}{d-1} + \ldots + h_d(A)$$

mit $h_0(A), \ldots, h_d(A) \in \mathbb{Z}$, wobei $h_j(A) > 0$ falls $p_A \neq 0$. (Dies folgt per Induktion über d $[p_{A/lA}(j) = p_A(j) - p_A(j-1)$ für hinreichend allgemeine $l \in [A]_1]$).

1.16 Definition. Sei $X \in \mathbb{P}^n$ ein projektives Schema mit homogenem Koordinatenring $A = R/I_X$. Dann nennt man $h_X := h_A$, $p_X := p_A$ die *Hilbertfunktion* bzw. das *Hilbertpolynom* von X und $\dim X := \dim A - 1$ die *Dimension* von X.

Hilbertfunktion h_X
Hilbertpolynom p_X

Ferner setzen wir

Dimension $\dim X$

$$\deg X := \begin{cases} h_0(A) & \text{falls } p_A \neq 0, \\ \sum_{j \geq 0} h_A(j) & \text{falls } p_A = 0, \end{cases}$$

und nennen dies den *Grad* von X bzw. A bzw. I_X.

Grad $\deg X$

1.17 Beispiel. (i) Für $R = K[x_0, \dots, x_n]$ gilt für $j \geq 0$

$$h_R(j) = \binom{n+j}{n} = \frac{(j+n)(j+n-1)\cdots(j+1)}{n!}$$
$$= \frac{j^n}{n!} + \text{kleinere Potenzen von } j,$$

also ist $\dim R = \deg p_R + 1 = n+1$ und $\deg R = 1$.

(ii) Ist $P \in \mathbb{P}^n$ ein Punkt, so ist $A := R/I(P) \cong R/(x_1, \dots, x_n) \cong K[x_0]$. Also folgt aus (i) $\dim A = 1$, $\dim P = 0$ und $\deg P = 1$. (Wie erwartet.)

(iii) Sei $0 \neq f \in R$ ein homogenes Polynom vom Grad d. Dann ergibt sich für $A := R/fR$: $[A]_j = [R]_j / f \cdot [R]_{j-d}$, also für $j \geq d$

$$h_A(j) = h_R(j) - \dim_K f \cdot [R]_{j-d} = h_R(j) - h_R(j-d)$$
$$= \binom{j+n}{n} - \binom{j-d+n}{n}$$
$$= \frac{(j+n)\cdots(j+1) - (j-d+n)\cdots(j-d+1)}{n!}$$
$$= \frac{1}{n!}\Big[j^n(1-1) + j^{n-1}\big(n + (n-1) + \ldots + 1 + (d-n) + (d-n+1) + \ldots$$
$$\ldots + (d-1)\big) + \text{kleinere Potenzen von } j \Big],$$

denn $\varphi : [R]_{j-d} \to f \cdot [R]_{j-d}$, $r \mapsto f \cdot r$ ist ein Isomorphismus und damit ist $\dim_K f \cdot [R]_{j-d} = \dim_K [R]_{j-d}$.

Hyperfläche

Also $h_A(j) = \frac{1}{n!} j^{n-1} \cdot n \cdot d + \ldots = d \frac{j^{n-1}}{(n-1)!} + \ldots$. Folglich ist $\dim A = n$ (d.h. die Dimension von $\dim R/fR = \dim R - 1$) und $\deg A = d$. Ist $n \geq 1$, so definiert $(f) = fR$ eine *Hyperfläche* in $\mathbb{P}^n$ der Dimension $n-1$ und des Grades d. Der Grad der Hyperfläche ist also gleich dem Grad des definierenden Polynoms (wie erwartet).

(iv) $\deg(x^a, y^b, z^c) = a \cdot b \cdot c$. (Übungsaufgabe 8).

2 Moduln

Der Begriff des *Moduls* verallgemeinert den Begriff des Vektorraumes, häufig werden Ringe durch Betrachtung von Moduln über ihnen studiert. Ringe sind weiterhin immer kommutativ mit Einselement.

2.1 Definition. Es sei R ein Ring. Ein *R-Modul* $M = (M,+,\cdot)$ oder *Modul über dem Ring R* ist eine Menge M mit Abbildungen $+: M \times M \to M$, $(m_1, m_2) \mapsto m_1 + m_2$, genannt *Addition*, und $\cdot : R \times M \to M$, $(a,m) \mapsto a \cdot m$, genannt *skalare Multiplikation*, so daß $(M,+)$ eine abelsche Gruppe ist und für alle $a,b \in R$, $m_1, m_2, m \in M$ gilt: Modul M

(i) $a(m_1 + m_2) = am_1 + am_2$

(ii) $(a+b)m = am + bm$

(iii) $(ab)m = a(bm)$

(iv) $1_R \cdot m = m$

2.2 Beispiel. (i) Ist R ein Ring, so ist R auch ein R-Modul mit den Operationen von R.

(ii) Ist $R = K$ ein Körper, so ist eine Menge M ein K-Modul genau dann, wenn M ein K-Vektorraum ist.

(iii) Eine Teilmenge M des Ringes R ist ein R-Modul genau dann, wenn M ein Ideal von R ist.

(iv) Es sei $G = (G,+)$ eine abelsche Gruppe. Definiert man für $g \in G$, $n \in \mathbb{Z}$:

$$n \cdot g := \begin{cases} \underbrace{g + \ldots + g}_{n \text{ mal}} & \text{falls } n > 0, \\ 0 & \text{falls } n = 0 \text{ und} \\ \underbrace{(-g) + \ldots + (-g)}_{-n \text{ mal}} & \text{falls } n < 0, \end{cases}$$

so wird G zu einem $\mathbb{Z}$-Modul.

(v) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $R/\mathfrak{a}$ ein R-Modul vermöge der skalaren Multiplikation $r \cdot (a \bmod \mathfrak{a}) := (r \cdot a \bmod \mathfrak{a})$ für $r, a \in R$.

2.3 Definition. Es sei M ein R-Modul. Eine Teilmenge $M' \subseteq M$ heißt *Untermodul* von M, wenn M' eine Untergruppe von M ist, die abgeschlossen bezüglich skalarer Multiplikation von M ist, d.h. für $r \in R$, $m' \in M'$ gilt $r \cdot m' \in M'$. (Ein Untermodul ist wieder ein R-Modul.) Untermoduln

2.4 Lemma (Untermodulkriterium). *Es sei M ein R-Modul, dann ist eine Teilmenge M' von M ein Untermodul genau dann, wenn für alle $m_1, m_2 \in M'$, $r \in R$ gilt:*

(i) $m_1 - m_2 \in M'$

(ii) $r \cdot m_1 \in M'$

Beweis. Analog zu Unterraumkriterium der linearen Algebra. $\square$

2.5 Definition (& Lemma). Es sei M ein R-Modul, und es sei $M_\lambda, \lambda \in \Lambda$, eine Familie von Untermoduln von M.

Summe von Moduln $\sum_{\lambda\in\Lambda} M_\lambda$

(i) Die *Summe* $\sum_{\lambda\in\Lambda} M_\lambda$ ist die Menge aller *endlichen* Summen $\sum_{\lambda\in\Lambda'} m_\lambda$, wobei $\Lambda' \subseteq \Lambda$ endlich ist, und $m_\lambda \in M_\lambda$ für alle $\lambda \in \Lambda'$.

Die Summe ist der kleinste Untermodul von M, der alle M_λ enthält.

Durchschnitt von Moduln $\bigcap_{\lambda\in\Lambda} M_\lambda$

(ii) Der *Durchschnitt* $\bigcap_{\lambda\in\Lambda} M_\lambda$ ist ein Untermodul.

Beweis. Siehe Übung. □

Die Vereinigung zweier Untermoduln ist nicht notwendigerweise ein Untermodul. (Siehe Übung 9)

2.6 Definition. Es sei R ein Ring und M und N R-Moduln. Eine Abbildung $\varphi : M \to N$ heißt ein *R-Modul-Homomorphismus* oder *R-linear*, wenn für alle $m_1, m_2 \in M, r \in R$ gilt:

Modulhomomorphismus R-linear

(i) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$,

(ii) $\varphi(r \cdot m_1) = r \cdot \varphi(m_1)$.

$\mathrm{Hom}_R(M,N)$

Die Menge der R-linearen Abbildungen $M \to N$ wird mit $\mathrm{Hom}_R(M,N)$. Ein R-Modulisomorphismus ist ein bijektiver R-Modulhomomorphismus.

2.7 Bemerkung. (i) Ist $R = K$ ein Körper, so ist ein R-Modulhomomorphismus dasselbe wie eine K-lineare Abbildung von K-Vektorräumen.

(ii) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist der kanonische Epimorphismus $\pi : R \to R/\mathfrak{a}$ R-linear.

(iii) Sind M, N, P R-Moduln, und sind $\varphi : M \to N$, $\psi : N \to P$ R-Modulhomomorphismen, so ist auch $\psi \circ \varphi : M \to P$ ein R-Modulhomomorphismus.

(iv) Es seien M, N R-Moduln. Für $\varphi, \psi \in \mathrm{Hom}_R(M,N)$ und $r \in R, m \in M$ setzen wir $(\varphi + \psi)(m) := \varphi(m) + \psi(m)$ und $(r \cdot \varphi)(m) := r \cdot \varphi(m)$. Damit ist eine Addition und skalare Multiplikation auf der Menge $\mathrm{Hom}_R(M,N)$ erklärt, die $\mathrm{Hom}_R(M,N)$ zu einem R-Modul macht.

(v) Ist M ein R-Modul, so heißen die Elemente von $\mathrm{Hom}_R(M,M)$ *Endomorphismen* von M. Durch die Festlegung $\varphi \cdot \psi := \varphi \circ \psi$ für $\varphi, \psi \in \mathrm{Hom}_R(M,M)$ wird eine Multiplikation erklärt, die $\mathrm{Hom}_R(M,M)$ zu einem Ring macht. Er wird *Endomorphismenring* von M genannt. Er hat als Einselement die identische Abbildung $\mathrm{id}_M : m \mapsto m$, ist aber im Allgemeinen nicht kommutativ.

Endomorphismenring $\mathrm{Hom}_R(M,M)$

(vi) Jeder R-Modulhomomorphismus $\varphi : R \to M$ ist eindeutig bestimmt durch $\varphi(1_R)$, denn $\varphi(r) = \varphi(1_R \cdot r) = r \cdot \varphi(1_R)$. Dies liefert einen R-Modulhomomorphismus $M \xrightarrow{\sim} \mathrm{Hom}_R(R,M)$.

2.8 Lemma (& Definition). *Es sei $\varphi : M \to N$ ein R-Modulhomomorphismus. Dann heißt* $\mathrm{Kern}\,\varphi := \{m \in M \mid \varphi(m) = 0\}$ *der* Kern *von φ und* $\mathrm{Im}\,\varphi := \{\varphi(m) \mid m \in M\}$ *das* Bild *von φ.*

Kern $\mathrm{Kern}\,\varphi$

Bild $\mathrm{Im}\,\varphi$

Es ist $\mathrm{Kern}\,\varphi$ *ein Untermodul von M,* $\mathrm{Im}\,\varphi$ *ein Untermodul von N. φ ist injektiv genau dann, wenn* $\mathrm{Kern}\,\varphi = \{0\}$.

Beweis. Folgt aus den Definitionen wie in der linearen Algebra. □

2.9 Satz (& Definition). *Es sei M' ein Untermodul des R-Moduls M. Definiere für $m \in M$: $m + M' := m \bmod M' := \{n \in M \mid m - n \in M'\}$ die* Restklasse *von m modulo M',*

Restklasse
$m \bmod M' = m + M'$

$\overline{M} := \{m + M' \mid m \in M\}$ die Menge der Restklassen, $\pi : M \to \overline{M}$, $m \mapsto m + M'$. Dann wird für $m, n \in M$, $r \in R$ durch $(m + M') + (n + M') := (m + n) + M'$ und $r \cdot (m + M') := (r \cdot m) + M'$ auf $\overline{M}$ eine Addition und skalare Multiplikation erklärt, die $\overline{M}$ zu einem R-Modul und $\pi : M \to \overline{M}$ zu einem surjektiven R-Modulhomomorphismus machen mit $\operatorname{Kern} \pi = M'$.

$\overline{M}$ heißt der Restklassenmodul *von M modulo M' oder* Faktormodul *von M nach M'. Schreibweise ist dann $M/M' := \overline{M}$. Die Abbildung π heißt* Restklassenhomomorphismus *oder* kanonischer Epimorphismus *von M auf M/M'.*

Restklassenmodul
Restklassenhomomorphismus π

Beweis. (1) Auf M wird durch $m \sim n :\Leftrightarrow m - n \in M'$ eine Äquivalenzrelation erklärt. Die Äquivalenzklasse, die m enthält ist gerade $m + M'$. Deshalb ist die Abbildung π wohldefiniert.

(2) Die festgelegte Addition und skalare Multiplikation sind wohldefiniert und machen $\overline{M}$ zu einem R-Modul; das Inverse von $m + M'$ bezüglich der Addition ist $(-m) + M'$, das Nullelement ist $0_M + M' = M'$.

Dies ist die einzige R-Modulstruktur von $\overline{M}$, die π zu einem R-Modulhomomorphismus macht.

(3) Für $m \in M$ ist $\pi(m) = 0_{\overline{M}} = 0_M + M' = M'$ genau dann, wenn $m + M' = 0_M + M'$, d.h. $m \in M'$. Folglich ist $\operatorname{Kern} \pi = M'$.

□

2.10 Bemerkung. Untermoduln von M sind genau die Kerne von R-Modulhomomorphismen $M \to N$.

2.11 Lemma (& Definition). *Es sei $\varphi : M \to N$ ein R-Modulhomomorphismus, und es sei M' ein Untermodul von M mit $M' \subseteq \operatorname{Kern} \varphi$. Dann wird durch $\overline{m} := m + M' \mapsto \varphi(m)$ ein R-Modulhomomorphismus $\overline{\varphi} : M/M' \to N$ definiert. Dieser heißt* durch φ induziert. *Es gilt* $\operatorname{Kern} \overline{\varphi} = \operatorname{Kern} \varphi / M'$.

induzierter Modulhomomorphismus

Beweis. $\overline{\varphi}$ ist wohldefiniert, denn aus $\overline{n} = \overline{m}$ folgt $m - n =: x \in M'$, also $\varphi(m) = \varphi(n + x) = \varphi(n) + \varphi(x) = \varphi(n)$, denn $x \in \operatorname{Kern} \varphi$.

$\overline{\varphi}$ ist offenbar ein R-Modulhomomorphismus und $\overline{\varphi}(\overline{m}) = 0$ genau dann, wenn $\varphi(m) = 0$, also $\operatorname{Kern} \overline{\varphi} = \operatorname{Kern} \varphi / M'$. □

2.12 Satz (Homomorphiesatz). *Es seien $\varphi : M \to N$ ein R-Modulhomomorphismus, M' ein Untermodul von M und $\pi : M \to M/M'$ der kanonische Epimorphismus. Dann gilt:*

(a) *φ faktorisiert durch π, d.h., es gibt einen R-Modulhomomorphismus $\psi : M/M' \to N$ mit $\varphi = \psi \circ \pi$.*

$$\begin{tikzcd} M \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & N \\ & M/M' \arrow[ur, "\psi"'] & \end{tikzcd}$$

genau dann, wenn $M' \subseteq$ $\operatorname{Kern} \varphi$. *In diesem Fall ist ψ durch φ induziert und insbesondere eindeutig bestimmt.*

(b) $\operatorname{Im} \varphi \cong M / \operatorname{Kern} \varphi$.

Beweis. (a) "$\Rightarrow$" Angenommen, $\psi : M/M' \to N$ existiert. Dann gilt für $\overline{m} = m + M' \in M/M'$: $\varphi(m) = \psi(\pi(m)) = \psi(\overline{m})$, d.h. ψ ist durch φ induziert. Weiterhin gilt $\psi(\overline{m}) = 0 \Leftrightarrow \varphi(m) = 0$. Für $m \in M'$ gilt aber $\varphi(m) = \psi(\pi(m)) = \psi(0) = 0$, also $M' \subseteq \operatorname{Kern}\varphi$.

"$\Leftarrow$" Ist $M' \subseteq \operatorname{Kern}\varphi$, so folgt die Existenz von ψ aus (2.11).

(b) Im Fall $M' = \operatorname{Kern}\varphi$, $N = \operatorname{Im}\varphi$ folgt die Existenz von $\psi : M/\operatorname{Kern}\varphi \to \operatorname{Im}\varphi$. Offenbar ist ψ surjektiv und $\operatorname{Kern}\psi \overset{(2.11)}{=} \operatorname{Kern}\varphi/\operatorname{Kern}\varphi = \{\overline{0}\}$, d.h. ψ ist ein Isomorphismus.

□

2.13 Folgerung. Sind $P \subseteq N$ Untermoduln von M, so induziert der kanonische Epimorphismus $\pi : M \to M/N$ einen Isomorphismus $(M/P)/(N/P) \cong M/N$.

Beweis. Wegen $P \subseteq N = \operatorname{Kern}\pi$ haben wir nach dem Homomorphiesatz ein kommutatives Diagramm

$$\begin{tikzcd} M \arrow[rr, "\pi"] \arrow[dr] & & M/N \\ & M/P \arrow[ur, "\psi"'] & \end{tikzcd}$$

mit $\operatorname{Kern}\psi = \operatorname{Kern}\pi/P = N/P$. Mit π ist auch ψ surjektiv. Also folgt nach dem Homomorphiesatz $M/N = \operatorname{Im}\psi \cong (M/P)/\operatorname{Kern}\psi = (M/P)/(N/P)$. □

2.14 Satz (Isomorphiesatz). *Sind M_1, M_2 Untermoduln von M, so gilt*

$$(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2).$$

Beweis. Es sei φ die Komposition von $M_1 \overset{\varepsilon}{\hookrightarrow} M_1 + M_2 \overset{\pi}{\twoheadrightarrow} (M_1 + M_2)/M_2$, d.h. $\varphi : M_1 \longrightarrow M_1 + M_2/M_2, m_1 \longmapsto m_1 + M_2$.

φ ist surjektiv, denn die Elemente von $(M_1 + M_2)/M_2$ sind der Form $m_1 + m_2 + M_2 = m_1 + M_2$, $m_1 \in M_1,\ m_2 \in M_2$.

Es ist $\varphi(m_1) = 0$ genau dann, wenn $m_1 \in M_2$, also folgt $\operatorname{Kern}\varphi = M_1 \cap M_2$. Somit ergibt sich die Behauptung aus dem Homomorphisatz. □

2.15 Beispiel. (i) Es seien $f, g \in R = K[X]$ teilerfremd. Dann gilt $(f)/(f) \cap (g) \cong R/g$, denn $(f) + (g) = (\operatorname{ggT}(f,g)) = (1) = R$.

(ii) In $\mathbb{Z}$ gilt z.B. $(3)/(15) \cong \mathbb{Z}/5\mathbb{Z}$.

$(m) = R \cdot m$

2.16 Definition. Es sei M ein R-Modul. Ist $m \in M$, so ist $(m) := R \cdot m = \{rm \mid r \in R\}$ ein Untermodul von M. Ist $(m_\lambda)_{\lambda \in \Lambda}$ eine Familie von Elementen $m_\lambda \in M$ mit $M = \sum_{\lambda \in \Lambda} R \cdot m_\lambda$, so heißt $(m_\lambda)_{\lambda \in \Lambda}$ ein *Erzeugendensystem* von M. Ist Λ endlich, dann heißt M *endlich erzeugt*. Man schreibt dann $(m_1, \ldots, m_s) := \sum_{i=1}^{s} R \cdot m_i$.

Erzeugendensystem
endlich erzeugt

unverkürzbar Erzeugendensystem

Ein *unverkürzbares Erzeugendensystem* ist ein Erzeugendensystem derart, daß keine echte Teilmenge ein Erzeugendensystem ist.

Basis, linear unabhängig

Ein Erzeugendensystem M heißt *Basis* von M, wenn es *linear unabhängig* über R ist, d.h. für je endlich viele paarweise verschiedene Elemente $m_1, \ldots, m_s \in B$ gilt: Ist $0 = \sum_{i=1}^{s} r_i m_i$ mit $r_1, \ldots, r_s \in R$, so folgt $r_1 = \ldots = r_s = 0$.

2.17 Bemerkung. (i) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $R/\mathfrak{a}$ ein R-Modul mit unverkürzbarem Erzeugendensystem $\{1 \bmod \mathfrak{a}\}$.

(ii) Ist $R = K$ ein Körper, so ist jedes unverkürzbare Erzeugendensystem eine Basis. Ist R kein Körper, so sind minimale Erzeugendensysteme i.a. *keine* Basis.

Beispiel: $R = K[X]$, $\mathfrak{a} = (X^3)$, dann ist $X^3 \neq 0$ in R, aber $X^3(1 \bmod \mathfrak{a}) = 0$ in $R/\mathfrak{a}$. $R/\mathfrak{a}$ hat keine Basis als R-Modul, denn für alle $m \in R/\mathfrak{a}$ ist $X^3 \cdot m = 0$.

Als $R/\mathfrak{a}$-Modul hat $R/\mathfrak{a}$ die Basis $\{1_R \bmod \mathfrak{a}\}$, denn aus $(r \bmod \mathfrak{a}) \cdot (1 \bmod \mathfrak{a}) = 0$ in $R/\mathfrak{a}$ für $r \in R$ folgt $r \in \mathfrak{a}$, d.h. $r \bmod \mathfrak{a} = 0$ in A.

Allgemein: Jeder Ring A hat als A-Modul die Basis $\{1_A\}$.

(iii) Die Elementanzahl eines unverkürzbarer Erzeugendensysteme ist im allgemeinen nicht eindeutig bestimmt.

2.18 Definition. Es sei $(M_\lambda)_{\lambda\in\Lambda}$ eine Familie von R-Moduln. Dann ist

direkte Summe $\bigoplus_{\lambda\in\Lambda} M_\lambda$

$$\bigoplus_{\lambda\in\Lambda} M_\lambda := \left\{ (m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda \text{ für alle } \lambda \in \Lambda \text{ und } m_\lambda = 0 \text{ für fast alle } \lambda \right\}$$

mit der durch

$$(m_\lambda)_{\lambda\in\Lambda} + (n_\lambda)_{\lambda\in\Lambda} := (m_\lambda + n_\lambda)_{\lambda\in\Lambda}$$

definierten Addition und der durch

$$r(m_\lambda)_{\lambda\in\Lambda} := (r \cdot m_\lambda)_{\lambda\in\Lambda}$$

definierten Skalarmultiplikation ein R-Modul, der die *direkte Summe* von $(M_\lambda)_{\lambda\in\Lambda}$ genannt wird.

Ist $M_\lambda = R$ für alle $\lambda \in \Lambda$, so schreibt man $R^{(\Lambda)} := \bigoplus_{\lambda\in\Lambda} M_\lambda$. Hat Λ $n < \infty$ viele Elemente, so schreibt man R^n statt $R^{(\Lambda)}$. Man setzt $R^0 := \{0_R\}$. $R^{(\Lambda)}$, R^n

Ein R-Modul heißt *frei*, wenn er isomorph zu einem R-Modul der Form $R^{(\Lambda)}$ ist. freie Moduln

2.19 Bemerkung. (i) Die Elemente von R^n sind n-Tupel $(r_1, \ldots, r_n)$ mit $r_i \in R$.

(ii) Jeder freie R-Modul $R^{(\Lambda)}$ besitzt die *kanonische Basis* $(e_\lambda)_{\lambda\in\Lambda}$ mit $e_\lambda = (\delta_{\mu\lambda})_{\mu\in\Lambda}$.

2.20 Satz. *Es sei M ein R-Modul. Dann gilt*

(a) M ist endlich erzeugt genau dann, wenn M isomorph zu einem Faktormodul eines endlich erzeugten freien Moduls ist.

(b) M ist frei genau dann, wenn M eine Basis hat. frei $\leftrightarrow$ Basis

Beweis. (a) "$\Rightarrow$" Es sei $M = (m_1, \ldots, m_s)$. Dann ist die Abbildung $\varphi : R^s \to M, (r_1, \ldots, r_s) \mapsto r_1 m_1 + \ldots + r_s m_s$ ein surjektiver Homomorphismus, also $M = \operatorname{Im}\varphi \cong R^s / \operatorname{Kern}\varphi$ nach Homomorphiesatz.

"$\Leftarrow$" Nach Voraussetzung haben wir R-Modulhomomorphismen $R^s \xrightarrow{\pi} R^s/N \xrightarrow[\sim]{\psi} M$, wobei ψ ein Isomorphismus ist. Da π surjektiv ist, ist auch $\varphi := \psi \circ \pi$ surjektiv. Ist $\{e_1, \ldots, e_s\}$ eine Basis von R^s, so ist $\{\varphi(e_1), \ldots, \varphi(e_s)\}$ ein Erzeugendensystem von M. (Denn $m = \varphi(\sum r_i e_i) = \sum r_i \varphi(e_i)$).

(b) Die Abbildung φ im ersten Teil des Beweises von (a) ist injektiv (also ein Isomorphismus) genau dann, wenn $\{m_1, \ldots, m_s\}$ linear unabhängig ist.

□

2.21 Beispiel. Es sei $R = K[x,y,z]$. Dann ist $M = ((x,y),(y,z)) \subseteq R^2$ ein Untermodul des R^2. Folglich ist R^2/M ein R-Modul, der durch die Restklassen $\bar{e}_1, \bar{e}_2$ von $(1,0)$ bzw. $(0,1)$ erzeugt wird.

Die Elemente von R^2/M sind von der Form

$$(r_1, r_2) + M = r_1(1,0) + r_2(0,1) + M = r_1[(1,0) + M] + r_2[(0,1) + M] = r_1\bar{e}_1 + r_2\bar{e}_2.$$

Rang

2.22 Definition. Es sei F ein endlich erzeugter freier R-Modul. Dann heißt die Anzahl der Elemente einer (jeder) Basis von F der *Rang* von F. Er ist wohldefiniert nach Übung 15.

[Tip: Zurückführen auf Situation bei Vektorräumen.]

Ist $R = K$ ein Körper, so ist der Rang von F gerade die Vektorraumdimension.

2.23 Definition. Sei M ein R-Modul.

$\mathfrak{a} \cdot M$

(i) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist das Produkt
$$\mathfrak{a} \cdot M := \left\{ \sum_{i=1}^{s} a_i m_i \,\middle|\, s \in \mathbb{N}, a_i \in \mathfrak{a}, m_i \in M \right\}$$
ein Untermodul von M.

(ii) Ist N ein Untermodul von M, so ist
$$N : M := N :_R M := \{ r \in R \mid r \cdot M \subseteq N \}$$
ein Ideal von R, genannt *Quotientenideal*.

Quotientenideal $N : M$

Annulator $\operatorname{Ann}_R M$

(iii) Das Ideal $0 :_R M = \{ r \in R \mid r \cdot M = 0 \}$ heißt der *Annulator* von M. Bezeichnung $\operatorname{Ann}_R M$.

2.24 Beispiel. (i) $\operatorname{Ann}_R(R) = (0_R)$, denn $r 1_R = 0_R$ genau dann, wenn $r = 0_R$. Ist F ein freier R-Modul, so ist $\operatorname{Ann}_R(F) = (0_R)$.

(ii) $\operatorname{Ann}_R(R/\mathfrak{a}) = \mathfrak{a}$.

(iii) Der Modul R^2/M aus Beispiel (2.21) ist nicht frei, denn:
$$(xz - y^2)(1,0) = z(x,y) + (-y)(y,z) \in M$$
und
$$(xz - y^2)(0,1) = (-y)(x,y) + x(y,z) \in M,$$
also $0 \neq xz - y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \in \operatorname{Ann}_R(R^2/M)$.

2.25 Lemma. *Es sei M ein R-Modul, und es sei $\mathfrak{a} \subseteq \operatorname{Ann}_R(M)$ ein Ideal. Dann besitzt M auch eine $(R/\mathfrak{a})$-Modulstruktur.*

Beweis. Wir übernehmen die Addition von M als R-Modul, aber wir definieren eine neue skalare Multiplikation durch
$$\bar{r} \cdot m := (r + \mathfrak{a}) \cdot m := rm \qquad \text{für } r \in R,\ m \in M.$$
Dies ist unabhängig von der Auswahl des Repräsentanten r der Restklasse $r + \mathfrak{a}$, da $a \cdot M = 0$, also wohldefiniert und leistet das Gewünschte. $\square$

2.26 Beispiel. (i) Ist $\mathfrak{a}$ ein Ideal von R, so ist $R/\mathfrak{a}$ auch ein $R/\mathfrak{b}$-Modul für jedes Ideal $\mathfrak{b}$ mit $\mathfrak{b} \subseteq \operatorname{Ann}_R(R/\mathfrak{a}) = \mathfrak{a}$.

(ii) Ist M ein R-Modul und ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $M/\mathfrak{a}M$ ein $R/\mathfrak{a}$-Modul, denn $\mathfrak{a} \subseteq \operatorname{Ann}_R(M/\mathfrak{a}M)$.

$\mu_R(M)$

2.27 Definition. Es sei M ein endlich erzeugter R-Modul. Dann bezeichnen wir mit $\mu(M) := \mu_R(M)$ die minimale Anzahl der Elemente eines Erzeugendensystems von M als R-Modul.

minimale Erzeugendensysteme

Ein Erzeugendensystem mit $\mu(M)$ Elementen heißt ein *minimales Erzeugendensystem*.

Ist $R = K$ ein Körper, also M ein endlich erzeugter K-Vektorraum, so ist ein Erzeugendensystem von M unverkürzbar genau dann, wenn es minimal ist, genau dann, wenn es eine Basis ist. Dann ist $\mu(M) = \dim_K(M)$.

Ist R kein Körper, so müssen unverkürzbare Erzeugendensysteme, nicht minimal sein. Betrachte $(1-x,x) = (1) = K[x]$.

Wir wollen nun sehen, daß die Situation über lokalen Ringen besser ist.

2.28 Definition. Ist R ein Ring, so nennt man den Durchschnitt $\mathrm{Rad}(R)$ aller maximalen Ideale von R das *Jacobson-Radikal* von R. $\mathrm{Rad}(R)$ ist ein Ideal von R. Jacobson-Radikal $\mathrm{Rad}(R)$

2.29 Beispiel. (i) $\mathrm{Rad}(K[x_1,\dots,x_n]) = (0)$.

(ii) Ist $(R,\mathfrak{m})$ ein lokaler Ring mit dem (einzigen) maximalen Ideal $\mathfrak{m}$, so ist $\mathrm{Rad}(R) = \mathfrak{m}$.

2.30 Lemma. *Für ein Element a eines Ringes R sind äquivalent:*

(a) $a \in \mathrm{Rad}(R)$,

(b) $1-ab \in R^\times$ *für alle* $b \in R$.

Beweis. (a)⇒(b): Ist $1-ab \notin R^\times$, also $(1-ab)R \neq R$, so gibt es ein maximales Ideal $\mathfrak{m}$ vom R mit $1-ab \in \mathfrak{m}$. Wegen $a \in \mathrm{Rad}(R) \subseteq \mathfrak{m}$ ist auch $ab \in \mathfrak{m}$, folglich $1 = (1-ab)+(ab) \in \mathfrak{m} \neq R$, Widerspruch. (b)⇒(a): Antithese: Es sei $\mathfrak{m}$ ein maximales Ideal von R mit $a \notin \mathfrak{m}$. Dann ist $aR+\mathfrak{m} = R$, also $ab+r = 1$ für geeignete $b \in R$, $r \in \mathfrak{m}$. Daher ist $1-ab = r \in \mathfrak{m}$ keine Einheit, Widerspruch. □

2.31 Bemerkung. Ist $(R,\mathfrak{m})$ ein lokaler Ring, so ist $R^\times = R \setminus \mathfrak{m}$.

Beweis. Es ist klar, daß $\mathfrak{m} \not\subseteq R^\times$, also $R^\times \subseteq R \setminus \mathfrak{m}$.

Ist umgekehrt $a \in R \setminus \mathfrak{m}$, aber $a \notin R^\times$, also $aR \neq R$, so muß a im einzigen maximalen Ideal enthalten sein, also $a \in \mathfrak{m}$, Widerspruch. □

2.32 Lemma (Lemma von Nakayama (1912-1964)). *Ist M ein endlich erzeugter R-Modul und $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a} \subseteq \mathrm{Rad}(R)$, so folgt aus $\mathfrak{a}M = M$ schon $M = 0$.*

Beweis. Nach Voraussetzung besitzt M ein minimales Erzeugendensystem $\{m_1,\dots,m_s\}$. Antithese: $s > 0$. Wegen $\mathfrak{a}M = M$ gibt es dann eine Gleichung $m_s = \sum_{i=1}^s a_i m_i$ mit $a_i \in \mathfrak{a}$, also $(1-a_s)m_s = \sum_{i=1}^{s-1} a_i m_i$. Wegen $a_s \in \mathfrak{a} \subseteq \mathrm{Rad}(R)$ ist $1-a_s$ eine Einheit (nach 2.30), also $m_s \in Rm_1+\ldots+Rm_{s-1}$ im Widerspruch zur vorausgesetzten Minimalität von $\{m_1,\dots,m_s\}$. □

2.33 Folgerung. Ist $(R,\mathfrak{m})$ ein lokaler Ring, $K := R/\mathfrak{m}$ und M ein endlich erzeugter R-Modul, so sind für Elemente $m_1,\dots,m_s$ äquivalent:

(a) $M = Rm_1+\ldots+Rm_s$,

(b) die Restklassen $\overline{m}_1,\dots,\overline{m}_s \in M/\mathfrak{m}M$ der $m_i \in M$ bilden ein Erzeugendensystem des K-Vektorraumes $M/\mathfrak{m}$.

Beweis. (a)⇒(b) klar.

(b)⇒(a) Aus $M/\mathfrak{m}M = Km_1+\ldots+Km_s$ folgt für $N := Rm_1+\ldots+Rm_s$ aber $M = N+\mathfrak{m}M$, also $M/N = \mathfrak{m}\cdot(M/N)$. [da $(M/N)/\mathfrak{m}(M/N) = (M/N)/((N+\mathfrak{m}M)/N) \cong M/(N+\mathfrak{m}M) = 0$] Aus dem Nakayama-Lemma folgt nun $M/N = 0$, also $M = N$. □

2.34 Folgerung. Unter den Voraussetzungen von (2.33) gelten:

(a) $\mu(M) = \dim_K(M/\mathfrak{m}M)$,

(b) $\{m_1, \ldots, m_s\} \subseteq M$ ist ein minimales Erzeugendensystem von M genau dann, wenn $\{\overline{m}_1, \ldots, \overline{m}_s\}$ eine K-Basis von $M/\mathfrak{m}M$ ist.

(c) (Auswahlsatz) Jedes Erzeugendensystem von M enthält ein minimales Erzeugendensystem. Jedes unverkürzbare Erzeugendensystem ist minimal.

(d) (Ergänzungssatz) Elemente $m_1, \ldots, m_s \in M$ lassen sich zu einem minimalen Erzeugendensystem ergänzen genau dann, wenn ihre Restklassen $\overline{m}_1, \ldots, \overline{m}_s \in M/\mathfrak{m}M$ linear unabhängig über K sind.

3 Noethersche Moduln

Diese Strukturen wurden 1921 von Emmy Noether eingeführt und untersucht. Sie gestatten Endlichkeitsaussagen.

3.1 Definition. Ein R-Modul M heißt *noethersch*, wenn jeder Untermodul von M, also insbesondere M selbst, endlich erzeugt ist.

3.2 Beispiel. Es sei R ein noetherscher Ring. Dann ist R ein noetherscher R-Modul, denn die Untermoduln von R sind Ideale von R, also endlich erzeugt.

3.3 Satz. *Für einen R-Modul M sind äquivalent:*

(a) M ist noethersch,

(b) Jede aufsteigende Kette von Untermoduln $M_1 \subseteq M_2 \subseteq \ldots$ von M wird stationär,

(c) Jede nichtleere Menge von Untermoduln von M enthält ein "$\subseteq$"-maximales Element

Beweis. Analog zu Satz (I.6.1). □

Wir wollen nun weitere noethersche Moduln konstruieren. In diesem Zusammenhang führen wir einige Begriffe ein, die eine Formalisierung von Standardschlußweisen gestatten ("Diagramm-Kalkül").

3.4 Definition. (i) Eine Folge/Sequenz von R-Moduln und R-Modulhomomorphismen

$$\ldots M_{k-1} \xrightarrow{\varphi_{k-1}} M_k \xrightarrow{\varphi_k} M_{k+1} \longrightarrow \ldots$$

keißt ein *Komplex*, wenn für alle $k \in \mathbb{Z}$ gilt $\varphi_k \circ \varphi_{k-1} = 0$. Komplexe

Die Sequenz heißt *exakt* in M_k, wenn $\operatorname{Im}\varphi_{k-1} = \operatorname{Kern}\varphi_k$. Sie heißt *exakte Sequenz*, wenn sie in allen M_k, $k \in \mathbb{Z}$, exakt ist. exakte Sequenzen

Eine exakte Sequenz der Form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

heißt *kurze exakte Sequenz* kurze exakte Sequenzen

(ii) Ist $\varphi : M \to N$ ein Homomorphismus von R-Moduln, so heißt $N/\operatorname{Im}\varphi$ der *Kokern* von N. Symbol $\operatorname{Cokern}\varphi$. Kokern $\operatorname{Cokern}\varphi$

3.5 Bemerkung. (i) Es gilt $0 \longrightarrow M' \xrightarrow{\varphi} M$ ist exakt genau dann, wenn φ injektiv ist. $M \xrightarrow{\psi} M'' \longrightarrow 0$ ist exakt genau dann, wenn ψ surjektiv ist.

(ii) Ein Homomorphismus $\varphi : M \to N$ von R-Moduln ist surjektiv genau dann, wenn $\operatorname{Cokern}\varphi = 0$.

(iii) Ist M' ein Untermodul von M, so ist die Sequenz

$$0 \longrightarrow M' \xrightarrow{\varepsilon} M \xrightarrow{\pi} M/M' \longrightarrow 0$$

exakt, wobei ε die Einbettung und π der kanonische Epimorphismus ist. Es ist $\operatorname{Cokern}\varepsilon = M/M'$. Dies ist das "Muster" *jeder* kurzen exakten Sequenz.

3.6 Lemma. *Eine Sequenz von R-Moduln (und R-Modulhomomorphismen)*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

ist exakt genau dann, wenn φ ist injektiv, ψ ist surjektiv und ψ induziert einen Isomorphismus $\operatorname{Cokern}\varphi \cong M''$.

Beweis. "⇒" Die ersten beiden Aussagen sind klar nach (3.5). Wegen $\mathrm{Kern}\,\psi = \mathrm{Im}\,\varphi$ gibt es nach dem Homomorphiesatz ein komm. Diagramm

$$\begin{tikzcd} M \arrow[rr, "\psi"] \arrow[dr, "\pi"'] & & M'' \\ & M/\mathrm{Im}\,\varphi \arrow[ur, "\alpha"'] & \end{tikzcd}$$

wobei α durch ψ induziert ist und $\mathrm{Kern}\,\alpha = \mathrm{Kern}\,\psi/\mathrm{Im}\,\varphi = 0$. Da mit ψ auch α surjektiv ist, ist α ein Isomorphismus.

"⇐" Da ψ einen Isomorphismus $\alpha : M/\mathrm{Im}\,\varphi \longrightarrow M''$ induziert folgt nach dem Homomorphiesatz $\mathrm{Im}\,\varphi \subseteq \mathrm{Kern}\,\psi$ und $0 = \mathrm{Kern}\,\alpha = \mathrm{Kern}\,\psi/\mathrm{Im}\,\varphi$, also $\mathrm{Kern}\,\psi = \mathrm{Im}\,\varphi$. Der Rest ist klar. □

3.7 Satz. *Es sei*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

eine kurze exakte Sequenz von R-Moduln. Dann ist M noethersch genau dann, wenn M' und M" noethersch sind.

Beweis. "⇒" Ist $M_1'' \subset M_2'' \subset \dots$ eine aufsteigende Kette von Untermoduln von M'', so ist $\psi^{-1}(M_1'') \subset \psi^{-1}(M_2'') \subset \dots$ (als Urbild) eine aufsteigende Kette von Untermoduln von M. Diese wird stationär, also auch die ursprüngliche Kette, denn $\psi(\psi^{-1}(M_i'')) = M_i''$, da ψ surjektiv ist. Also ist M'' noethersch.

Analog induziert jede aufsteigende Kette von Untermoduln von M' eine aufsteigende Kette von Untermoduln von M, wird also stationär. Also ist M' noethersch.

"⇐" Es sei $M_1 \subset M_2 \subset \dots$ eine aufsteigende Kette von Untermoduln von M. Dann sind $\varphi^{-1}(M_1) \subset \varphi^{-1}(M_2) \subset \dots$ und $\psi(M_1) \subset \psi(M_2) \subset \dots$ aufsteigende Ketten in M' bzw. M''. Diese werden stationär. Daher wird auch die ursprüngliche Kette stationär, denn aus $\varphi^{-1}(M_i) = \varphi^{-1}(M_{i+1})$ und $\psi(M_i) = \psi(M_{i+1})$ folgt $M_i = M_{i+1}$. Sei dazu $m \in M_{i+1}$. Zu zeigen: $m \in M_i$.

Fall 1: Es sei $m \in \mathrm{Im}\,\varphi$, d.h. es gibt ein $m' \in M'$ mit $\varphi(m') = m$. Also $m' \in \varphi^{-1}(M_{i+1}) = \varphi^{-1}(M_i)$, daher $m = \varphi(m') \in M_i$.

Fall 2: Sei $m \in M_{i+1}$ beliebig. Es ist $\psi(m) \in \psi(M_{i+1}) = \psi(M_i)$, also gibt es ein $n \in M_i$ mit $\psi(n) = \psi(m)$, d.h. $m - n \in \mathrm{Kern}\,\psi = \mathrm{Im}\,\varphi$. Nach Fall 1 ist also $n - m \in M_i$, somit $m \in M_i$. □

3.8 Folgerung. (i) Unter- und Faktormoduln eines noetherschen Moduls sind noethersch.

(ii) Ist M noethersch und N ein zu M isomorpher Modul, so ist auch N noethersch.

3.9 Folgerung. Sind $M_1, \dots, M_s$, $s \in \mathbb{N}$, noethersche R-Moduln, so ist auch ihre direkte Summe $\bigoplus_{i=1}^{s} M_s$ noethersch.

Beweis. Betrachte die Sequenz

$$0 \longrightarrow M_s \xrightarrow{m_s \mapsto (0,\dots,0,m_s)} \bigoplus_{i=1}^{s} M_i \xrightarrow{(m_1,\dots,m_s) \mapsto (m_1,\dots,m_{s-1})} \bigoplus_{i=1}^{s-1} M_i \longrightarrow 0.$$

Diese ist offenbar exakt, so daß die Behauptung aus (3.7) per Induktion über s folgt. □

3.10 Satz. *Endlich erzeugte Moduln über noetherschen Ringen sind noethersch.*

Beweis. Es sei R ein noetherscher Ring, und es sei M ein R-Modul mit Erzeugendensystem $\{m_1, \dots, m_s\}$. Nach (2.20) ist M isomorph zu einem Faktormodul eines endlich erzeugten freien Moduls F. Hat F den Rang r, so ist $F \cong R^r$. Nach (3.9) ist F noethersch, somit auch M (nach 3.8). □

3.11 Notation. Ein Diagramm kommutative Diagramme

$$\begin{tikzcd} M \arrow[rr, "\alpha"] \arrow[dr, "\beta"'] & & N \\ & P \arrow[ur, "\gamma"'] & \end{tikzcd}$$

von R-Modulhomomorphismen heißt *kommutativ*, wenn $\alpha = \gamma \circ \beta$, was gelegentlich durch einen Kringel bezeichnet wird.

3.12 Bemerkung (& Notation). (i) Es sei $A \in R^{p \times q}$ eine Matrix über dem Ring R. Dann ist die Abbildung

$$\varphi_A : R^q \longrightarrow R^p \quad (r_1, \dots, r_q)^t \mapsto A(r_1, \dots, r_q)^t$$

ein R-Modulhomomorphismus. Wir setzen Kern A, Im A, Cokern A

$$\operatorname{Kern} A := \operatorname{Kern} \varphi_A, \quad \operatorname{Im} A := \operatorname{Im} \varphi_A, \quad \operatorname{Cokern} A := \operatorname{Cokern} \varphi_A.$$

(ii) Es sei $\varphi : F \longrightarrow G$ ein R-Modulhomomorphismus zwischen freien Moduln vom Rang q bzw. p. Es seien $\{f_1, \dots, f_q\}, \{g_1, \dots, g_p\}$ Basen von F bzw. G. Dann gibt es $a_{ij} \in R$ derart, daß gilt

$$\varphi(f_j) = \sum_{i=1}^{p} a_{ij} g_i, \quad i = 1, \dots, q.$$

Dann heißt die Matrix $A = (a_{ij}) \in R^{p \times q}$ die *Koordinatenmatrix* von φ bezüglich der gewählten Basen. Das folgende Diagramm ist kommutativ: Koordinatenmatrix

$$\begin{tikzcd} s_1 f_1 + \ldots + s_q f_q & F \arrow[r, "\varphi"] & G & r_1 g_1 + \ldots + r_p g_p \\ (s_1, \dots, s_q)^t \arrow[u] & R^q \arrow[u, "\cong"'] \arrow[r, "A"] & R^p \arrow[u, "\cong"'] & (r_1, \dots, r_p)^t \arrow[u] \end{tikzcd}$$

3.13 Satz. *Es sei M ein endlich erzeugter Modul über dem noetherschen Ring R. dann hat M eine* Präsentationsmatrix, *d.h. es existiert eine Matrix $A \in R^{p \times q}$ derart, daß* $\operatorname{Cokern} A \cong M$. Präsentationsmatrix

Mit anderen Worten: Es gibt eine exakte Sequenz

$$R^q \xrightarrow{A} R^p \longrightarrow M \longrightarrow 0.$$

Je zwei Präsentationsmatrizen von M gleichen Formats sind äquivalent.

Beweis. Es sei $\{m_1, \dots, m_p\}$ ein Erzeugendensystem von M. Dann ist die Abbildung

$$\varphi : R^p \longrightarrow M, \quad (r_1, \dots, r_p)^t \longmapsto r_1 m_1 + \ldots + r_p m_p$$

surjektiv. Als Untermodul von R^p ist $\operatorname{Kern} \varphi$ endlich erzeugt. Folglich gibt es einen Epimorphismus $\psi : R^q \longrightarrow \operatorname{Kern} \varphi$.

Betrachte das Diagramm mit der Einbettung ε und $\alpha := \varepsilon \circ \psi$:

$$\begin{tikzcd} R^q \arrow[rr, "\alpha"] \arrow[dr, "\psi"'] & & R^p \arrow[r, "\varphi"] & M \arrow[r] & 0 \\ & \operatorname{Kern} \varphi \arrow[ur, "\varepsilon"'] & & & \\ 0 \arrow[ur] & & & & \end{tikzcd}$$

Dann gilt $\operatorname{Cokern} \alpha = R^p / \operatorname{Im} \alpha = R^p / \operatorname{Kern} \varphi = \operatorname{Cokern} \varepsilon \cong M$ (3.6). Die Behauptung folgt dann also, wenn wir A als eine Koordinatenmatrix von α wählen.

Die zweite Behauptung ist Übungsaufgabe 16. $\square$

3.14 Definition. Eine exakte Sequenz von R-Moduln

$$\ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

in der $F_0, F_1, \ldots$ endlich erzeugte freie R-Moduln sind, heißt *freie Auflösung* des R-Moduls M. Sie heißt *endliche freie Auflösung*, falls es ein $v \in \mathbb{N}$ gibt mit $F_i = 0$ für $i > v$. In diesem Fall heißt v die *Länge* der Auflösung.

3.15 Satz. *Jeder endlich erzeugte Modul M über einem Noetherschen Ring R besitzt eine freie Auflösung.*

Beweis. Wir iterieren das Argument aus (3.13): Es sei $F_l \longrightarrow F_{l-1} \longrightarrow \ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$ eine schon gefundene exakte Sequenz, in der $F_0, \ldots, F_l$ freie R-Moduln sind. (Existenz für $l = 0, 1$ klar nach (3.13)) Als Untermodul des Noetherschen Moduls F_l ist $\operatorname{Kern}\varphi_l$ endlich erzeugt, also gibt es (2.20) einen Epimorphismus $\alpha : F_{l+1} \twoheadrightarrow \operatorname{Kern}\varphi_l$, in der F_{l+1} ein freier R-Modul ist. Setze $\varphi_{l+1} := \varepsilon \circ \alpha$. Dann ist die Sequenz

$$\begin{tikzcd}
F_{l+1} \arrow[rr, "\varphi_{l+1}"] \arrow[dr, "\alpha"'] & & F_l \arrow[r, "\varphi_l"] & F_{l-1} \arrow[r] & \cdots \arrow[r] & F_0 \arrow[r] & M \arrow[r] & 0 \\
& \operatorname{Kern}\varphi_l \arrow[ur, "\varepsilon"'] \arrow[dr] & & & & & & \\
0 \arrow[ur] & & 0 & & & & &
\end{tikzcd}$$

exakt nach Konstruktion. $\square$

3.16 Beispiel. (i) Sei $R = K[x,y]$ und $M = R/(x,y)$.

$$\begin{tikzcd}
\operatorname{Kern}\varphi_2 = 0 \arrow[r] & R \arrow[r, "{\varphi_2,\ (-y,x)^t}"] \arrow[d] & R^2 \arrow[r, "{\varphi_1, (x,y)}"] \arrow[d] & R \arrow[r] & R/(x,y) \arrow[r] & 0 \\
& \operatorname{Kern}\varphi_1 = R(-y,x)^t \arrow[ur] & (x,y) \arrow[ur] \arrow[dr] & & & \\
& 0 \arrow[u] & 0 \arrow[u] & 0 & &
\end{tikzcd}$$

Es ist $(r_1, r_2)^t \in \operatorname{Kern}\varphi_1$ genau dann, wenn $0 = (x,y) \cdot (r_1, r_2)^t = r_1 x + r_2 y = 0$, also $r_1 x = -r_2 y$. Folglich gibt es ein $r \in R$ mit $r_1 = r(-y)$ und nach Kürzen $r_2 = rx$, d.h. $(r_1, r_2)^t \in \operatorname{Kern}\varphi_1$ genau dann, wenn $(r_1, r_2)^t = (r(-y), rx)^t = r(-y,x)^t$.

(ii) Betrachte $M = R/(x,y)^2$

$$\begin{tikzcd}
\operatorname{Kern}\varphi_2 = 0 \arrow[r] & R^2 \arrow[r, "{\varphi_2,\ \begin{pmatrix}-y & 0\\ x & -y\\ 0 & x\end{pmatrix}}"] \arrow[d] & R^3 \arrow[r, "{\varphi_1,(x^2,xy,y^2)}"] \arrow[d] & R \arrow[r] & R/(x,y)^2 \longrightarrow 0 \\
& \operatorname{Kern}\varphi_1 = R\begin{pmatrix}-y\\ x\\ 0\end{pmatrix} + R\begin{pmatrix}0\\ -y\\ x\end{pmatrix} \arrow[ur] & (x^2,xy,y^2) \arrow[ur] \arrow[dr] & & \\
& 0 \arrow[u] & 0 \arrow[u] & 0 &
\end{tikzcd}$$

Ist $(r_1,r_2)^t \in \operatorname{Kern}\varphi_2$, so folgt $0 = r_1(-y) + r_2 \cdot 0 = -r_1 y$, also $r_1 = 0$ und $0 = r_1 0 + r_2 x = r_2 x$, also $r_2 = 0$, d.h. $\operatorname{Kern}\varphi_2 = \{(0,0)^t\}$.

Im allgemeinen sind freie Auflösungen nicht endlich. Über Polynomringen gilt aber folgender

3.17 Satz (Hilbertscher Syzygiensatz). *Ist M ein endlich erzeugter Modul über einem Polynomring R, so besitzt M eine freie Auflösung der Länge $\leq \dim R$.*

Ohne Beweis.

Für die Betrachtung kommutativer Diagramme ist oft nützlich:

3.18 Lemma (Schlangenlemma). *Es sei*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\alpha"] \arrow[d, "\varphi'"] & M \arrow[r, "\beta"] \arrow[d, "\varphi"] & M'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\gamma"] & N \arrow[r, "\delta"] & N'' \arrow[r] & 0
\end{tikzcd}$$

ein kommutatives Diagramm. Dies induziert eine exakte Sequenz

$$0 \longrightarrow \operatorname{Kern}\varphi' \longrightarrow \operatorname{Kern}\varphi \longrightarrow \operatorname{Kern}\varphi'' \xrightarrow{\sigma} \operatorname{Cokern}\varphi' \longrightarrow \operatorname{Cokern}\varphi \longrightarrow \operatorname{Cokern}\varphi'' \longrightarrow 0$$

wobei σ durch $\gamma^{-1} \circ \varphi \circ \beta^{-1}$ "induziert" wird (β^{-1} ist keine Abbildung). Die Abbildung σ heißt Verbindungshomomorphismus.

Beweis. (i) Konstruktion von σ: Es sei $m'' \in \operatorname{Kern}\varphi''$. Da β surjektiv ist, gibt es ein $m \in M$ mit $\beta(m) = m''$. Die Kommutativität liefert $\delta(\varphi(m)) = \varphi''(\beta(m)) = \varphi''(m'') = 0$, also $\varphi(m) \in \operatorname{Kern}\delta = \operatorname{Im}\gamma$. Setze $\sigma(m'') := \gamma^{-1}(\varphi(m)) + \operatorname{Im}\varphi' \in \operatorname{Cokern}\varphi'$.

(ii) Wohldefiniertheit von σ: Dazu sei $\tilde{m} \in M$ mit $\beta(\tilde{m}) = m''$. Zu zeigen: $\gamma^{-1}(\varphi(\tilde{m})) - \gamma^{-1}(\varphi(m)) \in \operatorname{Im}\varphi'$. Es ist $0 = \beta(\tilde{m}) - \beta(m) = \beta(\tilde{m} - m)$, also ist $\tilde{m} - m \in \operatorname{Kern}\beta = \operatorname{Im}\alpha$, daher $\tilde{m} - m = \alpha(m')$ für ein $m' \in M'$. Es folgt $\gamma^{-1}(\varphi(\tilde{m})) - \gamma^{-1}(\varphi(m)) = \gamma^{-1}(\varphi(\tilde{m} - m) = \gamma^{-1}(\varphi(\alpha(m'))) \overset{komm.}{=} \gamma^{-1}(\gamma(\varphi'(m'))) = \varphi'(m') \in \operatorname{Im}\varphi'$.

(iii) Die anderen Abbildungen in der Sequenz sind durch α, β, γ bzw. δ induziert. Die Exaktheit rechnet man nach.

$\square$

4 Assoziierte Primideale, Primärzerlegungen

Assoziierte Primideale eines Moduls tragen wichtige Informationen über den Modul.

4.1 Definition. Es sei M ein R-Modul.

Spektrum $\operatorname{Spec}(R)$

(i) Die Menge $\operatorname{Spec}(R)$ der Primideale $\neq R$ von R heißt das *Spektrum* von R.

assoziierte Primideale $\operatorname{Ass}_R(M)$

(ii) Ein Primideal $\mathfrak{p} \in \operatorname{Spec}(R)$ heißt *assoziiertes Primideal* von M, wenn es ein $m \in M$ gibt, so daß $\mathfrak{p} = \operatorname{Ann} m := \operatorname{Ann}_R(Rm)$.

Die Menge der assoziierten Primideale von M wird mit $\operatorname{Ass}_R M$ bzw. $\operatorname{Ass} M$ bezeichnet.

Primteiler

(iii) Ist $\mathfrak{a} \subseteq R$ ein Ideal, so heißen die assoziierten Primideale in $\operatorname{Ass}_R(R/\mathfrak{a})$ die *Primteiler* von $\mathfrak{a}$.

(Nicht-)Nullteiler

(iv) Ein Element $r \in R$ heißt *Nullteiler* von M, wenn es ein $m \in M \setminus \{0_M\}$ gibt mit $rm = 0$, andernfalls *Nichtnullteiler* bzw. *M-regulär*.

(0_R ist ein Nullteiler, falls $M \neq 0$.)

4.2 Beispiel. Es sei $R = K[x,y,z]$ der Polynomring in drei Variablen, $\mathfrak{a} = (x^2y)$ und $\overline{R} = R/\mathfrak{a} = R/(x^2y)R$.

(i) Dann ist xy ein Nullteiler von $\overline{R}$, denn $\overline{x} := x + \mathfrak{a} \neq 0_{\overline{R}} = \overline{0}$, aber $xy \cdot \overline{x} = \overline{x^2y} = 0$.

(ii) Für $\overline{xy} = xy + \mathfrak{a}$ gilt $\operatorname{Ann}_R(\overline{xy}) = x \cdot R$, denn aus $f \in \operatorname{Ann}_R(\overline{xy})$ folgt $\overline{0} = f(\overline{xy}) = \overline{fxy}$, also $fxy \in \mathfrak{a} = x^2yR$. Da R faktorieller Ring und x,y Primelemente von R sind, folgt $x \,\big|\, f$, also $f \in x \cdot R$. Dies zeigt $\operatorname{Ann}_R(\overline{xy}) \subseteq xR$, aber die umgekehrte Inklusion ist klar.

(iii) Da x ein Primelement ist, ist xR ein Primideal von R, also ist $(x) = xR \in \operatorname{Ass}_R(\overline{R})$.

(iv) Analog ergibt sich $\operatorname{Ann}_R(\overline{x^2}) = yR = (y) \in \operatorname{Ass}_R(R/\mathfrak{a})$. Somit sind (x) und (y) Primteiler von $\mathfrak{a} = (x^2y) = (x^2) \cap (y)$.

(v) z ist $\overline{R}$-regulär, denn für $\overline{f} := f + \mathfrak{a} \in \overline{R}$ folgt aus $\overline{0} = z\overline{f} = \overline{zf}$, also $zf \in \mathfrak{a} = (x^2y)$, somit $x^2y \,\big|\, f$, daher $\overline{f} = 0$.

4.3 Satz. *Es sei R ein noetherscher Ring, und es sei $M \neq 0$ ein R-Modul. Dann gilt:*

(a) Jedes maximale Element der Familie von Idealen

$$\mathcal{F} := \{\operatorname{Ann}_R(m) \mid m \in M \setminus \{0\}\}$$

ist ein assoziiertes Primideal von M. Insbesondere ist $\operatorname{Ass}_R(M) \neq 0$.

(b) Die Menge aller Nullteiler von M ist die Vereinigung aller assoziierter Primideale von M.

Beweis. (a) Es sei $\operatorname{Ann}_R(m) \in \mathcal{F}$ ein maximales Element von $\mathcal{F}$. Zu zeigen: $\operatorname{Ann}_R(m)$ ist ein Primideal.

Dazu seien $a,b \in R$ mit $a \cdot b \in \operatorname{Ann}_R(m)$ und $b \notin \operatorname{Ann}_R(m)$. D.h. $abm = 0$, aber $bm \neq 0$. Wegen $\operatorname{Ann}_R(m) \subseteq \operatorname{Ann}_R(bm)$ folgt aus der Maximalität die Gleichheit, also insbesondere $a \in \operatorname{Ann}_R(bm) = \operatorname{Ann}_R(m)$.

Da R noethersch ist, enthält $\mathcal{F}$ maximale Elemente, somit ist $\operatorname{Ass}_R(M) \neq 0$.

(b) Ist $am = 0$ für $a \in R$ und $m \in M \setminus \{0\}$, so ist $a \in \operatorname{Ann}_R(m) \in \mathcal{F}$. Nach (a) existiert ein $\mathfrak{p} \in \operatorname{Ass}_R(M)$ mit $\operatorname{Ann}_R(m) \subseteq \mathfrak{p}$.

□

4.4 Lemma. *Ist M ein R-Modul und $m \in M$, so gilt für den Untermodul Rm von M:*

$$Rm \cong R/\operatorname{Ann}_R(m)$$

als Untermoduln.

Beweis. Durch $a \longmapsto am$ wird ein Epimorphismus $\varphi : R \longrightarrow Rm$ definiert. Offenbar ist $\operatorname{Kern}\varphi = \operatorname{Ann}_R(m)$. Somit liefert der Homomorphiesatz die Behauptung. □

4.5 Lemma. *Es sei $N \neq 0$ ein Untermodul des R-Moduls M. Gibt es ein Primideal $\mathfrak{p}$ von R mit $N \cong R/\mathfrak{p}$ (als R-Modul), so gilt $\operatorname{Ann}_R(n) = \mathfrak{p}$ für alle $n \in N \setminus \{0\}$ und insbesondere $\mathfrak{p} \in \operatorname{Ass}_R(M)$.*

Beweis. Nach Voraussetzung gibt es einen Isomorphismus $\varphi : R/\mathfrak{p} \longrightarrow N$. Es sei $m := \varphi(1_{R/\mathfrak{p}})$. Dann folgt $N = Rm$ und $\operatorname{Ann}_R(m) = \mathfrak{p}$. Zu jedem $n \in N \setminus \{0\}$ gibt es ein $a \in R$ mit $n = a \cdot m$. Somit ist $\mathfrak{p} = \operatorname{Ann}_R(m) \subseteq \operatorname{Ann}_R(n)$. Gäbe es ein $b \in \operatorname{Ann}_R(n) \setminus \mathfrak{p}$, so folgte $abm = 0$, aber $bm \neq 0$, somit wegen $ab \in \mathfrak{p}$ und $b \notin \mathfrak{p}$ aber $a \in \mathfrak{p}$, d.h. $n = am = 0$, im Widerspruch zu $n \neq 0$. □

4.6 Satz. *Es sei*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

eine kurze exakte Sequenz. Dann gilt

$$\operatorname{Ass} M' \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} M' \cup \operatorname{Ass} M''.$$

Beweis. Die erste Inklusion ist klar wegen Lemma (4.5). Wir zeigen nun die zweite: Es sei $\mathfrak{p} \in \operatorname{Ass} M$. Somit gibt es ein $m \in M$ mit $\mathfrak{p} = \operatorname{Ann}_R(m)$ und für $N = Rm$ gilt $N \cong R/\mathfrak{p}$ (nach (4.4)). Ist $\varphi(M') \cap N \neq 0$, so gibt es ein $m' \in M'$ mit $n := \varphi(m') \in N \setminus \{0\}$. Nach (4.5) folgt $\mathfrak{p} = \operatorname{Ann}_R(n) = \operatorname{Ann}_R(m')$, also $\mathfrak{p} \in \operatorname{Ass} M'$

Ist $\varphi(M') \cap N = 0$, d.h. $\operatorname{Kern}\psi \cap N = 0$, so folgt aus dem Homomorphiesatz $\psi(N) \cong N/\operatorname{Kern}\psi \cap N = N \cong R/\mathfrak{p}$. Wegen (4.5) ergibt sich also $\mathfrak{p} \in \operatorname{Ass} M''$. □

4.7 Lemma. *Es sei M ein endlich erzeugter Modul über dem noetherschen Ring R mit $M \neq 0$. Dann gibt es eine Kette von Untermoduln $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_n = M$ derart, daß für $i = 1, \ldots, n$ gilt $M_i/M_{i-1} \cong R/\mathfrak{p}$ für ein $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Beweis. Wir wählen ein $\mathfrak{p}_1 \in \operatorname{Ass}_R(M)$. Dann gibt es einen Untermodul M_1 von M mit $M_1 \cong R/\mathfrak{p}_1$, denn $\mathfrak{p}_1 = \operatorname{Ann}_R(m)$, also ist $Rm \cong R/\mathfrak{p}_1$. Ist $M \neq M_1$, so wählen wir ein $\mathfrak{p}_2 \in \operatorname{Ass}_R(M/M_1)$. Dann existiert ein Untermodul M_2 von M mit $M_2/M_1 \cong R/\mathfrak{p}_2$. Auf diese Weise kann man jede Kette $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_k$ mit $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ durch einen Modul M_{k+1} “verlängern”, falls $M_k \neq M$. Da M noethersch ist, wird jede aufsteigende Kette stationär. Daraus folgt die Behauptung. □

4.8 Satz. *Ist M ein endlich erzeugter Modul über dem noetherschen Ring R, so ist die Menge $\operatorname{Ass}_R(M)$ endlich.*

Beweis. Sei $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_n = M$ eine Kette von Untermoduln mit $M_i/M_{i-1} \cong R/\mathfrak{p}_i$, $\mathfrak{p}_i \in \operatorname{Spec}(R), i = 1, \ldots, n$. Wegen $\operatorname{Ass}_R(R/\mathfrak{p}_i) = \{\mathfrak{p}_i\}$ (nach (4.5)) folgt durch Anwendung von (4.6) auf $0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow R/\mathfrak{p}_i \longrightarrow 0$ aber $\operatorname{Ass}_R(M_i) \subseteq \operatorname{Ass}_R(M_{i-1}) \cup \{\mathfrak{p}_i\}$, also $\operatorname{Ass}_R(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. □

4.9 Folgerung. Ist $\mathfrak{a} \subseteq R$ ein Ideal des noetherschen Ringes R, so ist die Menge der Primteiler von $\mathfrak{a}$ endlich.

Beweis. $R/\mathfrak{a}$ ist als R-Modul durch $1 + \mathfrak{a}$ erzeugt. Daher ist $\operatorname{Ass}_R(R/\mathfrak{a})$ endlich. □

primäre Untermoduln

$\mathfrak{p}$-primär

4.10 Definition. Es sei N ein Untermodul des R-Moduls M. Dann heißt N ein *primärer Untermodul* von M, wenn $N \neq M$ und M/N genau ein assoziiertes Primideal hat. Ist $\mathfrak{p}$ dieses Primideal, so heißt N auch $\mathfrak{p}$-*primär* oder zu $\mathfrak{p}$ gehörig.

4.11 Lemma. *Sei R ein noetherscher Ring. Dann ist der Durchschnitt endlich vieler $\mathfrak{p}$-primärer Untermoduln eines R-Moduls M wieder $\mathfrak{p}$-primär.*

Beweis. Es genügt, dies für zwei $\mathfrak{p}$-rimäre Untermoduln $N_1, N_2 \subseteq M$ zu beweisen. Dann ist $M/N_1 \cap N_2 \neq 0$, also $\varnothing \neq \mathrm{Ass}_R(M/N_1 \cap N_2)$ nach (4.3). Wir betrachten die exakte Sequenz

$$0 \longrightarrow N_1/N_1 \cap N_2 \longrightarrow M/N_1 \cap N_2 \longrightarrow M/N_1 \longrightarrow 0.$$

Mit (4.6) ergibt sich dann wegen $N_1/N_1 \cap N_2 \cong (N_1+N_2)/N_2$

$$\varnothing \neq \mathrm{Ass}_R(M/N_1 \cap N_2) \subseteq \mathrm{Ass}_R(N_1+N_2/N_2) \cup \mathrm{Ass}_R(M/N_1) \overset{(4.6)}{\subseteq} \mathrm{Ass}_R(M/N_2) \cup \{\mathfrak{p}\} = \{\mathfrak{p}\}.$$

Also ist $\mathrm{Ass}_R(M/N_1 \cap N_2) = \{\mathfrak{p}\}$. □

Irreduzibilität

4.12 Definition. Ein Untermodul N des R-Moduls M heißt *irreduzibel* (in M), wenn gilt: Ist $N = U_1 \cap U_2$ für Untermoduln U_1, U_2 von M, so folgt $N = U_1$ oder $N = U_2$.

4.13 Lemma. *Ist R noethersch und ist $N \neq M$ ein irreduzibler Untermodul von M, so ist N primär.*

Beweis. (i) N ist irreduzibel in M genau dann, wenn der Nullmodul in M/N irreduzibel ist.

(ii) Wegen $M/N \neq 0$ ist $\mathrm{Ass}_R(M/N) \neq \varnothing$.

(iii) Antithese: Es seien $\mathfrak{p}_1, \mathfrak{p}_2$ verschiedene Primideale in $\mathrm{Ass}_R(M/N)$. Dann gibt es in M/N Untermoduln U_1, U_2 mit $U_1 \cong R/\mathfrak{p}_1$ und $U_2 \cong R/\mathfrak{p}_2$ nach (4.4). Für $x \in U_1 \cap U_2$ mit $x \neq 0$ folgte $\mathrm{Ann}_R(x) = \mathfrak{p}_1$ und $\mathrm{Ann}_R(x) = \mathfrak{p}_2$; Widerspruch. Somit ist $U_1 \cap U_2 = 0$. Da (0) in M/N irreduzibel ist (nach (i)) folgt $U_1 = 0$ oder $U_2 = 0$; Widerspruch.

Also hat $\mathrm{Ass}_R(M/N)$ genau ein Element.

□

Primärzerlegung

4.14 Definition. Eine *Primärzerlegung* eines Untermoduls $N \subsetneq M$ ist eine Darstellung $N = Q_1 \cap \ldots \cap Q_s$, wobei $s \in \mathbb{N}$ und $Q_1, \ldots, Q_s$ primäre Untermoduln von M sind.

reduzierte Primärzerlegung

Sie heißt *reduzierte* Primärzerlegung, wenn gilt

(i) $\bigcap_{i \neq j} Q_j \not\subset Q_i$ für $i = 1, \ldots, s$,

(ii) ist Q_i $\mathfrak{p}_i$-primär, so ist $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i \neq j$.

Primärkomponenten

Die dann auftretenden Moduln $Q_1, \ldots, Q_s$ heißen *Primärkomponenten* dieser Zerlegung von N.

4.15 Satz (Existenz einer reduzierten Primärzerlegung). *Es sei R ein noetherscher Ring und es sei M ein endlich erzeugter R-Modul. Dann besitzt jeder Untermodul $N \subsetneq M$ eine reduzierte Primärzerlegung.*

Beweis. Analog zu (I.7.17). □

4.16 Beispiel. Es sei R ein faktorieller Ring und $1 \neq a \in R$. Ist $a = \varepsilon p_1^{k_1} \cdots p_s^{k_s}$ eine Primfaktorzerlegung von a in paarweise nicht assoziierte irreduzible Elemente $p_1, \ldots, p_s$ mit $\varepsilon \in R^\times$, $k_i \in \mathbb{N}$, so ist $(a) = (p_1^{k_1}) \cap \ldots \cap (p_s^{k_s})$ eine Primärzerlegung des Hauptideals (a).

4.17 Satz (1. Eindeutigkeitssatz). *Ist R noethersch, und ist $N \subsetneq M$ ein Untermodul mit einer reduzierten Primärzerlegung $N = Q_1 \cap \ldots \cap Q_s$, wobei Q_i $\mathfrak{p}_i$-primär sei, so ist $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Die in einer reduzierten Primärzerlegung von N auftretenden Primideale sind durch M und N eindeutig bestimmt.*

Beweis. Es sei $U_i := \bigcap_{j \neq i} Q_j$, also $N = U_i \cap Q_i$ und $U_i \neq N$.
"$\supseteq$" Es folgt aus dem Isomorphiesatz $(0) \neq U_i/N = U_i/U_i \cap Q_i \cong (U_i + Q_i)/Q_i \subseteq M/Q_i$, also $\varnothing \neq \mathrm{Ass}_R(U_i/N) \subseteq \mathrm{Ass}_R(M/Q_i) = \{\mathfrak{p}_i\}$ und somit $\{\mathfrak{p}_i\} = \mathrm{Ass}_R(U_i/N) \overset{(4.6)}{\subseteq} \mathrm{Ass}_R(M/N)$, also $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} \subseteq \mathrm{Ass}_R(M/N)$
"$\subseteq$" Durch Induktion nach s: $s = 1$, klar. $s > 1$, dann $U_i = \bigcap_{j \neq i} Q_j$ ist eine reduzierte Primärzerlegung von U_i, also nach Induktionsvoraussetzung $\mathrm{Ass}_R(M/U_i) = \{\, \mathfrak{p}_j \mid j \neq i \}$. Wegen $M/U_i \cong (M/N)/(U_i/M)$ ergibt sich nach (4.6) aus $0 \longrightarrow U_i/N \longrightarrow M/N \longrightarrow M/U_i \longrightarrow 0$, daß $\mathrm{Ass}_R(M/N) \subseteq \mathrm{Ass}_R(U_i/N) \cup \mathrm{Ass}_R(M/U_i) = \{\mathfrak{p}_i\} \cup \{\, \mathfrak{p}_i \mid i \neq j\}$. □

4.18 Lemma. *Es sei M ein endlich erzeugter Modul über dem noetherschen Ring R. Dann gilt*
$$\sqrt{\mathrm{Ann}\, M} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}\, M} \mathfrak{p}.$$

Beweis. "$\subseteq$" Es sei $a \in \sqrt{\mathrm{Ann}\, M}$, d.h. $a^k M = 0$ für ein $k \in \mathbb{N}$. Dann folgt für alle $\mathfrak{p} = \mathrm{Ann}\, m \in \mathrm{Ass}\, M$ mit $m \in M$ wegen $a^k M = 0$ aber $a^k \in \mathfrak{p}$, also $a \in \mathfrak{p}$.
"$\supseteq$" Sei $a \notin \sqrt{\mathrm{Ann}\, M}$ und es sei $M = Rm_1 + \ldots + Rm_s$. Gäbe es $k_i \in \mathbb{N}$ mit $a^{k_i} m_i = 0$, so wäre für $k := \max\{k_1, \ldots, k_s\}$ aber $a^k M = 0$; Widerspruch. Also gibt es ein $m \in M$ derart, daß $a^k m \neq 0$ für alle $k \in \mathbb{N}$. Unter allen solchen Elementen m wähle eines, etwa x, mit maximalem Annulator $\mathfrak{p} := \mathrm{Ann}\, x$.

(i) Per Definition von x gilt dann $a^k \notin \mathfrak{p}$ für alle $k \in \mathbb{N}$

(ii) $\mathfrak{p}$ ist ein Primideal, denn gilt $bc \in \mathfrak{p}$ für $b, c \in R$, so folgt $bcx = 0$, also $c \in \mathrm{Ann}(bx)$ ($\supseteq \mathrm{Ann}\, x = \mathfrak{p}$).

Fall 1: Ist $a^k bx \neq 0$ für alle $k \in \mathbb{N}$, so folgt aus der Maximalität von $\mathfrak{p} = \mathrm{Ann}\, x$ schon $\mathrm{Ann}(bx) = \mathrm{Ann}\, x$, also $c \in \mathfrak{p}$.

Fall 2: Es sei $a^k bx = 0$ für ein $k \in \mathbb{N}$. Dann ist $b \in \mathrm{Ann}(a^k x)$. Wegen $a^j \notin \mathrm{Ann}\, x = \mathfrak{p}$ für alle $j \in \mathbb{N}$ folgt $a^j \notin \mathrm{Ann}(a^k x)$, daher aus der Maximalität von $\mathfrak{p} = \mathrm{Ann}\, x$ aber $b \in \mathrm{Ann}(a^k x) = \mathrm{Ann}\, x = \mathfrak{p}$.

Aus (i) und (ii) folgt $mfp \in \mathrm{Ass}\, M$ und $a \notin \mathfrak{p}$. □

4.19 Folgerung (Kriterium für Primärmoduln). Es sei M ein endlich erzeugter Modul über dem noetherschen Ring R. Dann gilt

(a) Ein Untermodul $N \subseteq M$ ist primär genau dann, wenn für alle $a \in R, m \in M$ gilt
(2) $\quad am \in N \wedge m \notin N \Longrightarrow \exists k \in \mathbb{N} :\ a^k M \subseteq N.$

(b) Ist N ein $\mathfrak{p}$-rimärer Untermodul von M, so ist $I := \mathrm{Ann}(M/N)$ ein $\mathfrak{p}$-primäres Ideal.

(c) Ein Ideal $\mathfrak{q} \subseteq R$ ist ein primärer Untermodul von R genau dann, wenn $\mathfrak{q}$ ein Primärideal ist.

Beweis. (a) "$\Leftarrow$" Ist $\mathfrak{p} \in \mathrm{Ass}(M/N)$, so sind alle $a \in \mathfrak{p}$ Nullteiler von M/N (4.3), also gibt es zu $a \in \mathfrak{p}$ ein $m \in M \setminus N$ mit $a(m + N) = 0$, d.h. $am \in N$. Mit (2) ergibt sich $a \in \sqrt{I} := \sqrt{\mathrm{Ann}(M/N)}$, somit $\mathfrak{p} \subseteq \sqrt{I}$. Nach (4.18) gilt $\sqrt{I} = \bigcap_{\mathfrak{p}' \in \mathrm{Ass}(M/N)} \mathfrak{p}' \subseteq \mathfrak{p}$. Also folgt $\mathfrak{p} = \sqrt{I}$ und somit $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$. Daher ist N ein primärer Untermodul.

"$\Rightarrow$" Ist $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$, so folgt für jeden Nullteiler $a \in R$ von M/N nach (4.3) $a \in \mathfrak{p}$, also wegen (4.18) $a^k \in I = \mathrm{Ann}(M/N)$ für ein $k \in \mathbb{N}$. Somit ist (2) erfüllt.

(b) Es seien $a, b \in R$ mit $ab \in I$, aber $b \notin I$, d.h. $ab(M/N) = 0$, aber $b(M/N) \neq 0$. Somit ist a ein Nullteiler von M/N, also $a \in \mathfrak{p}$ (nach (4.3)). Aber $\mathfrak{p} = \sqrt{I}$ (4.18), d.h., I ist ein $\mathfrak{p}$-primäres Ideal.

(c) Folgt durch Vergleich von (2) mit Definition (I.7.5).

□

4.20 Bemerkung. Für ein Ideal $\mathfrak{a} \subseteq R$ stimmen die Definitionen der Primärzerlegung in (I.7.16) und (4.11) überein. Insbesondere sind die Primteiler von $\mathfrak{a}$ genau die im Sinne von Definition (I.7.21) assoziierten Primideale von $\mathfrak{a}$. Diese Definition werden wir künftig nicht mehr verwenden.

Beispiel: $R = K[X]$, $\mathfrak{q} = (X^2)$. $\mathrm{Ass}_R(R/\mathfrak{q}) = \{(x)\}$, aber $\mathrm{Ass}_R(\mathfrak{q}) = \{0\}$, da R Integritätsring.

4.21 Bemerkung. Ist M ein endlich erzeugter Modul über dem noetherschen Ring R, und ist $0_M = Q_1 \cap \ldots \cap Q_s$, wobei $\{\mathfrak{p}_i\} = \mathrm{Ass}(M/Q_i)$ die Primärzerlegung des Nullmoduls, so ist $\mathrm{Ass}_R(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.

Beweis. Dies folgt aus dem ersten Eindeutigkeitssatz (4.17). □

isolierte Primideale
isolierte Primärkomponenten
eingebettete Primärkomponenten

4.22 Definition. Es sei N ein Untermodul von M mit reduzierter Primärzerlegung $N = Q_1 \cap \ldots \cap Q_s$, $\mathrm{Ass}(M/Q_i) = \{\mathfrak{p}_i\}$. Dann heißen die minimalen Elemente in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ *isolierte Primideale* von M/N und die entsprechenden Q_i *isolierte Primärkomponenten* von N. Die verbleibenden Primideale bzw. Primärkomponenten heißen *eingebettet*.

4.23 Beispiel. Im Polynomring $K[x,y]$ gilt $(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, x+y)$. Dabei ist (x) ein isoliertes Primideal und (x^2, y) bzw. $(x^2, x+y)$ sind eingebettete Primärideale, die zum Primideal (x,y) gehören. Der Name "eingebettet" erklärt sich geometrisch: Es ist $V(x^2, y) \subseteq V(x)$ und $V(x^2, x+y) \subseteq V(x)$.

4.24 Satz (2. Eindeutigkeitssatz). *Es sei N ein Untermodul von M mit reduzierter Primärzerlegung $N = Q_1 \cap \ldots \cap Q_s$. Dann sind die isolierten Primärkomponeneten von N eindeutig durch M und N bestimmt (d.h. unabhängig von der gewählten Primärzerlegung von N.)*

Obacht: *Die analoge Aussage ist falsch für eingebettete Primärkomponenten.*

Beweis. Dies beweist man mit Hilfe der Lokalisierung von Moduln und soll hier nicht gezeigt werden. □

Krull-Dimension $\dim R$

4.25 Definition. Die *Krull-Dimension* $\dim R$ eines Ringes R ist das Supremum der Längen n der Primidealketten

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

in $\mathrm{Spec}(R)$.

Die *Höhe* $h(\mathfrak{p})$ eines Primideals $\mathfrak{p} \in \mathrm{Spec}(R)$ ist das Supremum der Längen aller Ketten mit $\mathfrak{p}_n = \mathfrak{p}$.

Höhe $h(\mathfrak{a})$

Die *Höhe* eines beliebigen Ideals $\mathfrak{a} \subsetneq R$ ist $h(\mathfrak{a}) := \inf\{\, h(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec} R,\ \mathfrak{a} \subseteq \mathfrak{p}\}$

4.26 Beispiel. (i) Im Polynomring $R = K[x_0, \ldots, x_n]$ hat man die Primidealkette

$$(0) \subsetneq (x_0) \subsetneq (x_0, x_1) \subsetneq \ldots \subsetneq (x_0, \ldots, x_n).$$

Daraus folgt $\dim R \geq n+1$. Es ist $\dim R = n+1$ und $h(x_0, \ldots, x_i) = i+1$. (Ohne Beweis)

(ii) Es ist $\dim \mathbb{Z} = 1$ und $h(0) = 0$, und für jede Primzahl $p \in \mathbb{Z}$ gilt $h(p) = 1$.

(iii) Ist R ein Integritätsring, so ist $\dim R = 0$ genau dann, wenn R ein Körper ist.

Beweis. Im Integritätsring ist (0) ein Primideal. $\square$

4.27 Lemma. *Es sei $\mathfrak{a} \subseteq R$ ein Ideal. Dann gilt*

(a) Ist R noethersch, so gelten

$$h(\mathfrak{a}) = \min\{\, h(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Ass}_R(R/\mathfrak{a})\} \text{ und } \dim(R/\mathfrak{a}) = \max\{\, \dim R/\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}_R(R/\mathfrak{a})\}\,.$$

Insbesondere ist $\dim R/\mathfrak{a} = \dim R/\sqrt{\mathfrak{a}}$.

(b) $\dim R/\mathfrak{a} + h(\mathfrak{a}) \leq \dim R$

Beweis. (a) Es sei $P \in \operatorname{Spec} R$ ein Primideal mit $\mathfrak{a} \subseteq P$. Wegen $\bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})} \mathfrak{p} = \sqrt{\mathfrak{a}} \subseteq \sqrt{P} = P$ gibt es ein $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})$ mit $\mathfrak{p} \subseteq P$. Damit folgt $h(\mathfrak{a}) = \min\{\, h(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Ass}_R(R/\mathfrak{a})\}$.

Ist $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_h$ eine Primidealkette in $R/\mathfrak{a}$, so erhalten wir vermöge des kanonischen Epimorphismus $\pi : R \longrightarrow R/\mathfrak{a}$ eine Primidealkette $\mathfrak{a} \subsetneq \pi^{-1}(\mathfrak{p}_0) \subsetneq \pi^{-1}(\mathfrak{p}_1) \subsetneq \ldots \subsetneq \pi^{-1}(\mathfrak{p}_h)$ und ein $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})$ mit $\mathfrak{p} \subseteq \pi^{-1}(\mathfrak{p}_0)$. Dann ist $\pi^{-1}(\mathfrak{p}_0)/\mathfrak{p} \subsetneq \pi^{-1}(\mathfrak{p}_1)/\mathfrak{p} \subsetneq \ldots \subsetneq \pi^{-1}(\mathfrak{p}_n)/\mathfrak{p}$ eine Primidealkette in $R/\mathfrak{p}$. Dies zeigt $\dim R/\mathfrak{a} \leq \dim R/\mathfrak{p}$.

Umgekehrt liefert jede Primidealkette in $R/\mathfrak{p}$, wobei $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})$, eine Primidealkette in $R/\mathfrak{a}$ gleicher Länge.

Dies zeigt $\dim R/\mathfrak{p} \leq \dim R/\mathfrak{a}$.

(b) Ist mit obigen Bezeichnungen $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_s = \mathfrak{p} := \pi^{-1}(\mathfrak{p}_0)$ eine Primidealkette in R, so erhalten wir daraus eine Primidealkette $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_s = \pi^{-1}(\mathfrak{p}_0) \subsetneq \ldots \subsetneq \pi^{-1}(\mathfrak{p}_n)$ der Länge $s+n$. Daraus folgt $\dim R \geq n + h(\mathfrak{a})$, also schließlich $\dim R \geq \dim R/\mathfrak{a} + h(\mathfrak{a})$.

$\square$

4.28 Definition. Eine Primidealkette $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_s \subsetneq R$ heißt *maximal*, wenn sie nicht durch ein $\mathfrak{p} \in \operatorname{Spec} R$ verlängert werden kann, d.h., wenn für jedes $\mathfrak{p} \in \operatorname{Spec}(R)$ die Bedingungen $\mathfrak{p} \subsetneq \mathfrak{p}_0$, $\mathfrak{p}_s \subsetneq \mathfrak{p}$ und $\mathfrak{p}_i \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_{i+1}$ verletzt sind. maximale Primidealketten

Noethersche Ringe müssen nicht endliche Krull-Dimension haben. Ferner kann es in noetherschen Integritätsringen maximale Primidealketten verschiedener Länge geben. Im geometrischen Kontext ist die Situation besser.

4.29 Satz. *Es sei $A = K[x_1, \ldots, x_n]/\mathfrak{a}$. Sind $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} A$ Primideale mit $\mathfrak{p} \subseteq \mathfrak{q}$, so haben alle maximalen Primidealketten $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l = \mathfrak{q}$ die gleiche Länge l, nämlich* $\dim A/\mathfrak{p} - \dim A/\mathfrak{q}$.

Zusatz: *Ist A ein Integritätsring, so gilt für jedes Ideal I von A:* $\dim A = h(I) + \dim(A/I)$.

Beweis. Es sei $0 = \mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_t$ eine Primidealkette in $A/\mathfrak{q}$ maximaler Länge $t = \dim A/\mathfrak{q} \leq n = \dim K[x_1, \ldots, x_n]$. Es sei $\pi : A \longrightarrow A/\mathfrak{q}$ der kanonische Epimorphismus. Dann ist $0 = \mathfrak{p}_0/\mathfrak{p} \subseteq \mathfrak{p}_1/\mathfrak{p} \subseteq \ldots \subseteq \mathfrak{p}_l/\mathfrak{p} = \mathfrak{q}/\mathfrak{p} = \pi^{-1}(\mathfrak{q}_0)/\mathfrak{p} \subseteq \pi^{-1}(\mathfrak{q}_1)/\mathfrak{p} \subseteq \ldots \subseteq \pi^{-1}(\mathfrak{q}_t)/\mathfrak{p}$ eine Primidealkette in $A/\mathfrak{p}$ der Länge $l + t = l + \dim A/\mathfrak{q}$, also $\dim A/\mathfrak{p} \geq l + \dim A/\mathfrak{q}$.

Die Umkehrung $l \geq \dim A/\mathfrak{p} - \dim A/\mathfrak{q}$ verlangt stärkere Hilfsmittel (Siehe etwa Kunz: "Einführung in die kommutative Algebra und algebraische Geometrie")

Zusatz: Mit $\mathfrak{p} = (0)$ folgt für alle $\mathfrak{q} \in \operatorname{Spec} A$, daß $h(\mathfrak{q}) = \dim A - \dim A/\mathfrak{q}$. Die Behauptung ergibt sich daher aus Lemma (4.27). $\square$

4.30 Bemerkung. Es ist $A/I \cong K[x_1, \ldots, x_n]/J$ für ein Ideal $J \subseteq K[x_1, \ldots, x_n] =: R$

Beweis. $J := \pi^{-1}(I)$, dann ist $I = J/\mathfrak{a}$ und somit $A/I \cong (R/\mathfrak{a})/J/\mathfrak{a} \cong R/J$ $\square$

Krull-Dimension $\dim_R M$

4.31 Definition. Es sei M ein R-Modul. Dann nennt man $\dim M := \dim_R M := \dim R/\operatorname{Ann}_R(M)$ die *(Krull-)Dimension* von M.

Ist F ein freier R-Modul, so ist $\dim F = \dim R$, denn $\operatorname{Ann}_R(R) = 0$ wegen $1 \in R$.

4.32 Lemma. *Hat der R-Modul M die Präsentationsmatrix $A \in R^{p\times q}$, so ist $\dim M = \dim R/I_p(A)$.*

Beweis. Es gilt (ohne Beweis) $\sqrt{I_p(A)} = \sqrt{\operatorname{Ann} M}$. Also folgt die Behauptung aus $\dim M = \dim R/\operatorname{Ann} M \overset{4.27}{=} \dim R/\sqrt{\operatorname{Ann} M}$. □

4.33 Beispiel. Es sei $R = K[x,y,z]$. Dann gilt für $A = (x,y)^t$, $B = \begin{pmatrix} x & z \\ y & x \end{pmatrix}$ aber $\dim(\operatorname{Cokern} A) = \dim R = 3$, da $I_2(A) = 0$, und $\dim(\operatorname{Cokern} B) = \dim R/I_2(B) = \dim R/(x^2 - yz) = 2$, da $x^2 - yz$ ein homogener Nichtnullteiler von R ist.

4.34 Lemma. *Ist M ein endlich erzeugter Modul über dem noetherschen Ring R, so gilt* $\dim M = \max\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R(M)\}$.

Beweis. Wegen $\operatorname{Ann}_R(M) = \bigcap_{\mathfrak{p}\in\operatorname{Ass}_R(M)} \mathfrak{p}$ folgt die Behauptung aus (4.27). □

4.35 Lemma. *Es sei* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *eine exakte Sequenz von R-Moduln. Dann gilt*

(a) $\dim M \geq \max\{\dim M', \dim M''\}$.

(b) Ist R noethersch, und sind M, M', M'' endlich erzeugt, so gilt $\dim M = \max\{\dim M', \dim M''\}$.

Beweis. (a) Nach Übungsaufgabe 13 ist $\operatorname{Ann} M' \supseteq \operatorname{Ann} M$, also $\dim M' \leq \dim M$, und auch $\operatorname{Ann} M \subseteq \operatorname{Ann} M''$, also $\dim M'' \leq \dim M$.

(b) Wegen $\operatorname{Ass} M \subseteq \operatorname{Ass} M' \cup \operatorname{Ass} M''$ folgt nach (4.34) $\dim M \leq \max\{\dim M', \dim M''\}$, also folgt die Behauptung mit (a).

□

4.36 Satz (Krullscher Hauptidealsatz). *Ist R ein noetherscher Ring und ist $\mathfrak{a} \subsetneq R$ ein Ideal, so gilt für jeden* minimalen *Primteiler $\mathfrak{p}$ von $\mathfrak{a}$*

$$h(\mathfrak{p}) \leq \mu(\mathfrak{a}),$$

also insbesondere $h(\mathfrak{a}) \leq \mu(\mathfrak{a})$.

Beweis. Für die erste Behauptung sei wieder auf Kunz, Theorem V.3.4 verwiesen. Die zweite Behauptung folgt aus der ersten wegen Lemma (4.27). □

4.37 Folgerung. Ist $a \in R \setminus R^\times$ ein Nichtnullteiler des noetherschen Ringes R, so hat jeder minimale Primteiler von $(a) = aR$ die Höhe 1.

Beweis. Nach Definition (4.36) gilt $h(\mathfrak{p}) \leq 1$. Als Nichtnullteiler ist a aber in keinem assoziierten Primideal von R enthalten. □

4.38 Bemerkung. Ist R ein noetherscher Ring, so sind für $\mathfrak{p} \in \operatorname{Spec} R$ äquivalent:

(i) $\mathfrak{p}$ ist ein Primideal der Höhe null,

(ii) $\mathfrak{p}$ ist ein isoliertes Primideal von (0_R),

(iii) $\mathfrak{p}$ ist ein minimales Primideal von R.

4.39 Definition. Ein Ideal $\mathfrak{a} \subsetneq R$ des noetherschen Ringes R heißt *vollständiger Durchschnitt*, wenn $h(\mathfrak{a}) = \mu(\mathfrak{a})$. vollständige Durchschnitte

Ein Schema $S \subseteq \mathbb{A}^n$ bzw. $S \subseteq \mathbb{P}^n$ heißt *vollständiger Durchschnitt*, wenn sein Ideal I_S ein vollständiger Durchschnitt ist.

4.40 Beispiel. (i) Jeder Punkt, jede Gerade im $\mathbb{P}^n$ ist ein vollständiger Durchschnitt, denn für $\mathfrak{a} = (x_0, x_1, \dots, x_k)$ gilt $\mu(\mathfrak{a}) = k+1$ und $(0) \subsetneq (x_0) \subsetneq (x_0, x_1) \subsetneq \dots \subsetneq (x_0, \dots, x_k) = \mathfrak{a}$, also $k+1 \le h(\mathfrak{a}) \overset{4.36}{\le} \mu(\mathfrak{a}) \le k+1$. Somit gilt Gleichheit.

(Alternativ: $R = K[x_0, \dots, x_n]$, $h(\mathfrak{a}) = \dim R - \dim R/\mathfrak{a} = n+1-\dim K[x_{k+1}, \dots, x_n] = k+1$)

(ii) $\mathfrak{a} = (x_0^3, x_1^2)$ ist ein vollständiger Durchschnitt der Höhe 2, denn $\mu(\mathfrak{a}) \le 2$ und $\dim R/\mathfrak{a} = \dim R/\sqrt{\mathfrak{a}} = \dim R/(x_0, x_1) = n-1$, also $h(\mathfrak{a}) = \dim R - \dim R/\mathfrak{a} = 2$.

Eine partielle Umkehrung zum Krullschen Satz liefert

4.41 Folgerung. Ist R noethersch und ist $\mathfrak{p} \in \operatorname{Spec} R$ ein Primideal der Höhe c, so ist $\mathfrak{p}$ minimaler Primteiler eines vollständigen Durchschnitts der Höhe c.

Beweis. Per Induktion über $0 \le s \le c$ konstruieren wir Ideale $(a_1, \dots, a_s) \subseteq \mathfrak{p}$ der Höhe s.

$s = 0$ ist klar. Ist $s > 0$, und hat $(a_1, \dots, a_{s-1}) \subseteq \mathfrak{p}$ die Höhe $s-1$, so ist $\mathfrak{p}$ nach (4.36) in keinem minimalen Primteiler von $(a_1, \dots, a_{s-1})$ enthalten. Nach dem "Primidealvermeidungslemma" gibt es also ein $a_s \in \mathfrak{p}$, das in keinem minimalen Primteiler von $(a_1, \dots, a_{s-1})$ enthalten ist. Es folgt $h(a_1, \dots, a_{s-1}, a_s) \ge s$, also Gleichheit nach (4.36) □

4.42 Folgerung. Ist $(R, \mathfrak{m})$ ein noetherscher lokaler Ring endlicher Dimension, und ist $a \in \mathfrak{m}$ in keinem minimalen Primideal von R enthalten, so gilt $\dim R/aR = \dim R - 1$.

Beweis. Es sei $d = \dim R$. Nach Voraussetzung ist $h(aR) \ge 1$. Wegen Krull folgt $h(aR) = 1$. Aus $d = \dim R \ge h(aR) + \dim R/aR$ folgt $\dim R/aR \le d-1$. Da $\mathfrak{m}$ das einzige maximale Ideal ist, ist $h(\mathfrak{m}) = \dim R = d$. Wegen $a \in \mathfrak{m}$ und $h(aR) = 1$ gibt es wie im Beweis von (4.41) Elemente $a_1 := a, a_2, \dots, a_d \in \mathfrak{m}$ mit $h(a_1, \dots, a_i) = i$ für $i = 1, \dots, d$. Folglich gibt es minimale Primteiler $\mathfrak{p}_i$ von $(a_1, \dots, a_i)$, so daß wir eine Kette $aR \subset \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_d = \mathfrak{m}$, haben. Also ist $\mathfrak{p}_1/aR \subsetneq \mathfrak{p}_2/aR \subsetneq \dots \subsetneq \mathfrak{p}_d/aR$ eine Primidealkette in $\operatorname{Spec}(R/aR)$, somit $\dim R/aR \ge d-1$. □

4.43 Folgerung. (i) Ohne die Voraussetzung *lokal* kann $\dim R/aR < \dim R - 1$ gelten.

(ii) Die Folgerung präzisiert die Vorstellung, daß die Hinzunahme einer Gleichung die Dimension um eins verringert.

Beispiel: Es sei $S \subseteq \mathbb{P}^3$ definiert durch $I_S = (x_0, x_1) \cap (x_1, x_2, x_3)$ (Gerade $\cup$ Punkt) und F die durch $f = x_0^2 + x_1^2 + x_2^2$ definierte Hyperfläche. Dann hat $S \cap F$ die Dimension null, denn mit $R = K[x_0, x_1, x_2, x_3]$ folgt mit

$$\dim\left[(R/I_S)/f \cdot (R/I_S)\right] = \dim R/I_S + f \cdot R = \dim R/I_S - 1 = 2 - 1 = 1,$$

daß $\dim S \cap F = \dim R/(I_S + f \cdot R)_{\mathrm{sat}} - 1 = \dim\left[R/I_S + f \cdot R\right] - 1 = 0$.

$S \cap F$ nennt man den *Hyperflächenschnitt* von S mit F. Hyperflächenschnitt

Es gilt auch $\dim\left[S \cap V(x_1^2 + x_2^2)\right] = 0$, denn $\sqrt{I_S + gR} = \sqrt{(x_0, x_1, g)} \cap \sqrt{(x_1, x_2, x_3, g)} = (x_0, x_1, x_2) \cap (x_1, x_2, x_3)$ und $\dim R/I_S + gR = \dim R/\sqrt{I_S + gR} = 1$.

4.44 Folgerung. Es sei $\mathfrak{a} \neq R$ ein homogenes Ideal von $R = K[x_0, \dots, x_n]$. Ferner sei $f \in \mathfrak{m} = (x_0, \dots, x_n)$ ein homogenes Ideal, das in keinem minimalen Primteiler von $\mathfrak{a}$ enthalten ist. Dann gilt

$$\dim R/\mathfrak{a} + fR = \dim R/\mathfrak{a} + 1.$$

Beweis. Setze $A := R/\mathfrak{a}$. Da A graduiert ist, gibt es eine Kette *homogener* Primideale $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_d = \mathfrak{m}$ in $R/\mathfrak{a}$, wobei $d = \dim R/\mathfrak{a}$ (ohne Beweis). Es folgt $h(\mathfrak{m}) = d$. Daher ergibt sich die Behauptung wie in (4.42). $\square$

5 Graduierte Moduln

Für das Studium projektiver Schemata ist die Betrachtung graduierter Moduln wesentlich.

5.1 Definition. Ein *graduierter Ring A* ist ein Ring (wie immer kommutativ mit 1) und eine Familie $(A_k)_{k\in\mathbb{Z}}$ von Untergruppen von $(A,+)$, so daß gilt graduierte Ringe

(i) $A=\bigoplus_{k\in\mathbb{Z}} A_k$

(ii) $A_i\cdot A_j\subseteq A_{i+j}$ für alle $i,j\in\mathbb{Z}$.

Ein *graduierter A-Modul* ist ein Modul über dem graduierten Ring A, der (als $\mathbb{Z}$-Modul) eine Zerlegung $M=\bigoplus_{k\in\mathbb{Z}} M_k$ besitzt derart, daß $A_i\cdot M_j\subseteq M_{i+j}$. graduierte Moduln

Elemente in M_k heißen *homogene Elemente* vom Grad k, die Elemente in A_k auch *k-Formen*. Für $m\in M_k$ schreibt man $\deg m=k$. Jedes Element $m\in M$ läst sich (in eindeutiger Weise) schreiben als $m=\sum_{k\in\mathbb{Z}} m_k$ mit $m_k\in M_k$. Dann nennt man m_k die *homogene Komponente k-ten Grades von m*. homogene Elemente, k-Formen homogene Komponenten

5.2 Beispiel. (i) Der Polynomring $A=R[x_0,\dots,x_n]$ über einem Ring R ist graduiert: Die homogenen Elemente vom Grad k sind die homogenen Polynome k-ten Grades $\sum_{\nu_0+\dots+\nu_n=k} r_\nu x_0^{\nu_0}\cdots x_n^{\nu_n}$, mit $r_\nu\in R$. Es gilt also $\deg r=0$ für alle $r\in R$ und $\deg x_i=1$. Diese Graduierung nennt man die *Standardgraduierung* von $R[x_0,\dots,x_n]$. Standardgraduierung

(ii) Ist A ein graduierter Ring, so ist A^k ein graduierter A-Modul mit

$$(A^k)_i:=\left\{(a_1,\dots,a_k)^t\in A^k\;\middle|\;\deg a_1=\ldots=\deg a_k=i\right\}.$$

5.3 Bemerkung. (i) $0_A,0_M$ sind homogen von jedem Grad.

(ii) A_0 ist ein Unterring von A, da $A_0\cdot A_0\subseteq A_0$ und $1_A\in A_0$, denn ist $1=\sum_{k\in\mathbb{Z}} a_k, a_k\in A_k$, so folgt für alle homogenen Elemente $b\in A$ aus $b=b\cdot 1_A=\sum_{k\in\mathbb{Z}} ba_k$ durch Gradvergleich $b=ba_0$ und analog $b=a_0b$, also muß $a_0=1_A\in A_0$ gelten.

(iii) A_k und M_k sind A_0-Moduln. Insbesondere ist jeder graduierte Ring A eine A_0-Algebra. Die Zerlegung $M=\bigoplus_{k\in\mathbb{Z}} M_k$ ist eine direkte Summe von A_0-Moduln.

5.4 Definition. Ein Untermodul N des graduierten A-Moduls M heißt *graduierter Untermodul*, falls $N=\bigoplus_{k\in\mathbb{Z}} N_k$ ein graduierter A-Modul ist mit $N_k\subseteq M_k$ für alle $k\in\mathbb{Z}$.

5.5 Lemma. *Für einen Untermodul N des graduierten A-Moduls M sind äquivalent:*

(a) N ist ein graduierter Untermodul,

(b) N besitzt ein Erzeugendensystem, das nur aus homogenen Elementen besteht,

(c) Für alle $m\in M$ gilt: Ist $m=\sum_{k\in\mathbb{Z}} m_k\in N$ die Zerlegung in homogene Komponenten, so gehören alle homogenen Komponenten $m_k\in M_k$ zu N.

(d) M/N ist ein graduierter A-Modul mit der Graduierung $[M/N]_k:=(M_k+N)/N$

Beweis. “(a)⇔(c)” folgt aus der Definition (5.4). $(N=\bigoplus_{k\in\mathbb{Z}}\underbrace{(N\cap M_k)}_{N_k})$

“(b)⇒(c)” Es sei $\{m_\lambda\}_{\lambda\in\Lambda}$ ein Erzeugendensystem von N mit $m_\lambda\in A_{d_\lambda}, d_\lambda\in\mathbb{Z}$. Es sei $m\in N$. Dann gibt es $a_{\lambda_i}\in A$ mit $m=\sum_{i=1}^s a_{\lambda_i}m_{\lambda_i}$ und Zerlegungen in homogene Komponenten $a_{\lambda_i}=\sum_{k\in\mathbb{Z}}(a_{\lambda_i})_k$. Es folgt

$$m=\sum_{k\in\mathbb{Z}} m_k \;\text{ mit }\; m_k=\sum_{i=1}^s (a_{\lambda_i})_{k-d_{\lambda_i}}\cdot m_{\lambda_i}\in M_k\cap N.$$

"(c)⇒(b)" Ist E ein Erzeugendensystem von N, so ist auch die Menge aller homogenen Komponenten von Elementen aus E ein Erzeugendensystem von N.

"(d)⇒(c)" Ist $n = \sum_{k\in\mathbb{Z}} n_k \in N, n_k \in N_k$, so gilt in M/N für die Restklassen: $0 = \overline{n} = \sum_{k\in\mathbb{Z}} \overline{n}_k$ mit $\overline{n}_k := (n_k + N)/N$, also $\overline{n}_k = 0$, d.h. $n_k \in N$

"(c)⇒(d)" Aus der Definition folgt $A_j \cdot (M/N)_k \subseteq (M/N)_{j+k}$ und $M/N = \sum_{k\in\mathbb{Z}} (M/N)_k$. Zu zeigen bleibt, daß aus $0_{M/N} = \sum_{k\in\mathbb{Z}} \overline{m}_k, \overline{m}_k = (m_k + N)/N \in (M/N)_k$ folgt, daß $\overline{m}_k = 0_{M/N}$, d.h. $m_k \in N$.

Wegen $0_{M/N} = \overline{\sum_{k\in\mathbb{Z}} m_k}$ folgt aber $\sum_{k\in\mathbb{Z}} m_k \in N$, also wegen (c) $m_k \in N$. □

5.6 Bemerkung. Es sei M ein graduierter A-Modul.

(i) Die graduierten Untermoduln von A sind gerade die homogenen Ideale von A.

(ii) Ist N ein graduierter Untermodul von M, so wird M/N stets als graduierter Modul mit der in (5.5 (d)) definierten Graduierung betrachtet. Analoges gilt für die Graduierung von $A/\mathfrak{a}$ für homogene Ideale $\mathfrak{a} \subseteq A$. Insbesondere ist dann $A/\mathfrak{a}$ ein graduierter A-Modul.

(iii) Summe und Durchschnitt graduierter Untermoduln von M sind wieder graduiert. (Vgl. Übung 31)

5.7 Satz. *Ist M ein graduierter A-Modul, so ist jedes assoziierte Primideal $\mathfrak{p}$ von M homogen. Ferner gibt es ein homogenes Element $m \in M$ mit $\mathfrak{p} = \operatorname{Ann} m$.*

Beweis. Wegen $\mathfrak{p} \in \operatorname{Ass} M$ gibt es ein $m \in M$ mit $\operatorname{Ann} m = \mathfrak{p}$. Es sei $m = m_k + \ldots + m_l$ die Zerlegung in homogene Komponenten. Es sei $a \in \mathfrak{p}$ mit der Zerlegung $a = a_p + \ldots + a_q$ in homogene Komponenten. Aus $am = 0$ folgt

$$\begin{aligned} a_p \cdot m_k &= 0 \\ a_{p+1} \cdot m_k + a_p \cdot m_{k+1} &= 0 \\ &\vdots \\ a_p \cdot m_l + \ldots + a_{p+l-k} \cdot m_k &= 0 \\ &\vdots \\ a_q \cdot m_l &= 0. \end{aligned}$$

Induktiv ergibt sich $a_p m_k = 0, a_p^2 m_{k+1} = 0, \ldots, a_p^{l-k+1} m_l = 0$, also $a_p^{l-k+1} \cdot m = 0$, d.h. $a_p^{l-k+1} \in \mathfrak{p}$, folglich $a_p \in \mathfrak{p}$. Iteration dieses Schlusses liefert wegen $(a - a_p) \cdot m = 0$ schrittweise $a_{p+1}, \ldots, a_q \in \mathfrak{p}$. Gemäß (5.5 (c)) ist daher $\mathfrak{p}$ homogen.

Ferner ergibt sich $\mathfrak{p} \cdot m_i = 0$, d.h. $\mathfrak{p} \subseteq \mathfrak{a}_i := \operatorname{Ann} m_i$. Andererseits ist $\mathfrak{a}_k \cap \ldots \cap \mathfrak{a}_l \subseteq \operatorname{Ann} m = \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, gibt es ein j mit $\mathfrak{a}_j \subseteq \mathfrak{p}$. es folgt $\mathfrak{p} = \mathfrak{a}_i = \operatorname{Ann} m_j$ □

5.8 Satz. *Es sei M ein endlich erzeugter, graduierter Modul über dem noetherschen graduierten Ring A. Dann besitzt jeder graduierte Untermodul N von M eine reduzierte Primärzerlegung, $N = Q_1 \cap \ldots \cap Q_S$, in der alle Q_i graduierte Primärmoduln sind.*

Beweis. (Idee) Dies folgt wie die Existenz der Primärzerlegung, wenn man statt beliebiger Untermoduln immer nur graduierte Untermoduln betrachtet. □

Standard-K-Algebren

5.9 Definition. Ein graduierter Ring A heißt *Standard-K-Algebra*, K ein Körper, wenn A noethersch ist und $A_k = 0$ für $k < 0$, $A_0 = K$ und wenn $A_1 \cdots A_1$ (k Faktoren???) ein Erzeugendensystem von A_k als $K = A_0$-Vektorraum ist für alle $k > 0$.

5.10 Lemma. *Es ist $A \neq 0$ eine graduierte Standard-K-Algebra genau dann, wenn $A = K[x_0, \dots, x_n]/\mathfrak{a}$, wobei $\mathfrak{a} \subsetneq K[x_0, \dots, x_n]$ ein homogenes Ideal des Polynomringes mit der Standard-Graduierung (vgl. (5.2)) ist.*

Beweis. “$\Rightarrow$” Für R ist die Behauptung klar: Die hier relevanten Eigenschaften von R übertragen sich auf $R/\mathfrak{a}$.

“$\Leftarrow$” Es sei $\{a_0, \dots, a_n\}$ ein Erzeugendensystem des K-Vektorraumes A_1. Betrachte die K-lineare Abbildung

$$\varphi : R := K[x_0, \dots, x_n] \longrightarrow A, \qquad \lambda x_0^{k_0} \cdots x_n^{k_n} \longmapsto \lambda a_0^{k_0} \cdots n_n^{k_n}$$

für alle $\lambda \in K$, $k_0, \dots, k_n \in \mathbb{N}$. φ ist ein Ringhomomorphismus, der sogenannte *Einsetzungshomomorphismus*. Sein Kern $\mathfrak{a} := \operatorname{Kern} \varphi$ ist ein homogenes Ideal von R. Demnach ist $A \cong R/\mathfrak{a}$ nach dem Homomorphiesatz. □ Einsetzungs-homomorphismus

5.11 Bemerkung. Ist A eine graduierte Standard-K-Algebra, so ist $\mathfrak{m} = \mathfrak{m}_A = \bigoplus_{k>0} A_k$ das eindeutig bestimmte maximale homogene Ideal von A.

Wir werden sehen, daß A ähnliche Eigenschaften wie ein lokaler Ring hat.

5.12 Lemma (Nakayama graduiert). *Es sei M ein endlich erzeugter, graduierter Modul über der graduierten Standard-K-Algebra A. Ist $M = \mathfrak{m}_A \cdot M$, so folgt $M = 0$.*

Beweis. Analog zu (2.32). □

5.13 Folgerung. Unter den Voraussetzungen von (5.12) gelten die Aussagen von (2.33) und (2.34) auch für homogene Elemente $m_1, \dots, m_s \in M$. Insbesondere besitzt M ein minimales Erzeugendensystem, das nur aus homogenen Elementen besteht.

5.14 Lemma. *Ist A ein noetherscher, graduierter Ring und ist $\mathfrak{p} \subseteq A$ ein homogenes Primideal der Höhe $h < \infty$, so gibt es eine Kette*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_h = \mathfrak{p}.$$

Beweis. Siehe etwa Bruns-Herzog, Cohen-Macaulay rings, Theorem 15.8 □

Ein Homomorphismus graduierter Moduln sollte die Graduierung respektieren. Insbesondere sollten Kern und Cokern wieder graduierte Moduln sein.

5.15 Definition. Es seien M, N graduierte A-Moduln. Wir sagen, daß ein Homomorphismus $\varphi : M \longrightarrow N$ von A-Moduln den *Grad* j hat, wenn $\varphi(M_i) \subseteq N_{i+j}$ für alle $i \in \mathbb{N}$ gilt, d.h. wenn Elemente vom Grad i auf Elemente vom Grad $i + j$ abgebildet werden. Grad von Homomorphismen

Die Abbildung φ heißt ein *Homomorphismus graduierter Moduln*, wenn φ den Grad Null hat. Homomorphismen graduierter Moduln

5.16 Beispiel. Es sei $R := K[x_0, \dots, x_n]$ der Polynomring mit der Standardgraduierung. Dann ist die Multiplikationsabbildung

$$\mu : R \xrightarrow{x_1^2 + x_2} R, \qquad r \longmapsto r(x_1^2 + x_2)$$

ein R-Modulhomomorphismus, der keinen Grad besitzt, denn $\mu(1) = x_1^2 + x_2$ ist nicht homogen.

Ist $f \in R$ homogen vom Grad d, so ist die Multiplikationsabbildung

$$\eta : R \xrightarrow{f} R, \qquad r \longmapsto r \cdot f$$

ein R-Modulhomomophismus vom Grad $d = \deg f$. Wir können diesen zu einem Homomorphismus graduierter Moduln machen vermöge der folgenden

5.17 Definition. Es sei M ein graduierter A-Modul. Für $k \in \mathbb{Z}$ sei $M(k)$ der graduierte A-Modul mit der gleichen A-Modulstruktur wie M, aber mit der Graduierung $(M(k))_i = M_{i+k}$ für alle $i \in \mathbb{Z}$. $M(k)$ heißt der *um den Grad k geshiftete Modul* von M.

geshiftete Moduln $M(k)$

5.18 Beispiel. (i) $x^5 \in (K[x])_5 = (K[x](2))_3$

(ii) Für $a \in A_d$ ist die Multiplikationsabbildung

$$\mu : M(-d) \xrightarrow{a} M, \qquad m \longmapsto a \cdot m$$

ein Homomorphismus graduierter A-Moduln, denn für $m \in (M(-d))_i = M_{i-d}$ hat $\mu(m) = an$ den Grad $i - d + d = i$.

5.19 Bemerkung (Warnung!). $A(k)$ ist ein graduierter A-Modul, aber für $k \neq 0$ *kein* graduierter Ring, denn dann müsste gelten $(A(k))_i \cdot (A(k))_j \subseteq (A(k))_{i+j}$. Es gilt aber $A_{k+i} \cdot A_{k+j} \subseteq A_{2k+i+j} \not\subseteq (A(k))_{i+j}$ falls $k \neq 0$.

5.20 Lemma. *Ist $\varphi : M \longrightarrow N$ ein Homomorphismus graduierter A-Moduln, so ist* $\operatorname{Kern}\varphi$ *ein graduierter Untermodul von M,* $\operatorname{Im}\varphi$ *ein graduierter Untermodul von N, also insbesondere* $\operatorname{Cokern}\varphi = N/\operatorname{Im}\varphi$ *ein graduierter A-Modul.*

Beweis. Es sei $m = \sum_{k\in\mathbb{Z}} m_k$, $m_k \in M_k$ im Kern von φ. Zu zeigen: Für alle $k \in \mathbb{Z}$ ist $m_k \in \operatorname{Kern}\varphi$, somit ist $\operatorname{Kern}\varphi$ ein graduierter Untermodul von M. Ist E ein Erzeugendensystem von M, das nur aus homogenen Elementen besteht, so ist $\varphi(E)$ ein Erzeugendensystem von $\operatorname{Im}\varphi$, das nur aus homogenen Komponenten besteht. Daher ist $\operatorname{Im}\varphi$ graduiert nach (5.5).

Ferner ist $\operatorname{Cokern}\varphi = N/\operatorname{Im}\varphi$ ein graduierter Modul nach (5.5). □

Der Einsetzungshomomorphismus $\varphi : R \longrightarrow A$ in (5.10) ist ein Homomorphismus graduierter R-Moduln. Daher ist $\operatorname{Kern}\varphi$ *ein homogenes Ideal von R.*

5.21 Bemerkung. Es sei M ein endlich erzeugter, graduierter Modul über der Standard-K-Algebra A. Dann ist M noethersch.

Ist $\{m_1, \dots, m_s\}$ ein Erzeugendensystem von M aus homogenen Elementen, so besitzt der K-Vektorraum M_j das Erzeugendensystem $\bigcup_{i=1}^s m_i A_{j-\deg(m_i)}$, denn ist $m \in M_j$, so ist $m = \sum_{i=1}^s a_i m_i$ für geeignete $a_i \in A_{j-\deg m_i}$. Es gilt also $\dim_K(M_j) \leq \sum_{i=1}^s \dim_K(A_{j-\deg(m_i)}) < \infty$.

5.22 Definition. Unter den Voraussetzungen von (5.21) heißt die Funktion

$$h_M : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad j \longmapsto \dim_K(M_j)$$

die *Hilbertfunktion* von M.

Hilbertfunktion eines Moduls h_M

5.23 Satz (& Definition). *Es sei $0 \neq M$ ein endlich erzeugter graduierter Modul über der Standard-K-Algebra A. Dann gibt es ein Polynom $p_M \in \mathbb{Q}[T]$ derart, daß $p_M(j) = h_M(j)$ für alle $j \gg 0$. Dieses Polynom heißt das* Hilbertpolynom *von M.*

Hilbertpolynom eines Moduls p_M

Es ist $p_M = 0$ genau dann, wenn $\dim M = 0$. Ist $p_M \neq 0$, so ist $\dim M = \deg p_M + 1$.

Ferner gibt es zu $d := \deg p_M$ ganze Zahlen $h_0(M), \dots, h_d(M) \in \mathbb{Z}$ derart, daß

$$p_M(j) = h_0(M) \cdot \binom{j}{d} + h_1(M) \cdot \binom{j}{d-1} + \ldots + h_d(M) \binom{j}{0}.$$

Der Grad *von M ist definiert durch*

Grad eines Moduls $\deg M$

$$\deg M := \begin{cases} h_0(M) & \text{falls } p_M \neq 0, \\ \sum_{j\in\mathbb{Z}} h_M(j) & \text{falls } p_M = 0. \end{cases}$$

Es ist $\deg M > 0$. Dies verallgemeinert die Aussagen für graduierte Standard-K-Algebren und wird analog bewiesen.

5.24 Definition. Eine *Sequenz graduierter A-Moduln*

$$\ldots \longrightarrow M_{i-1} \xrightarrow{\varphi_i - 1} M_i \xrightarrow{\varphi_i} M_i + 1 \longrightarrow \ldots$$

ist eine Sequenz graduierter A-Moduln, in der alle Homomorphismen φ_i Homomorphismen graduierter A-Moduln sind.

5.25 Lemma. *Es sei* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *eine exakte Sequenz endlich erzeugter graduierter Moduln über der Standard-K-Algebra A. Dann gilt* $h_M = h_{M'} + h_{M''}$ *und* $p_M = p_{M'} + p_{M''}$.

Beweis. Die zweite Behauptung folgt aus der ersten. Aus der Voraussetzung folgt, daß

$$0 \longrightarrow (M')_i \longrightarrow M_i \longrightarrow (M'')_i \longrightarrow 0$$

für alle $i \in \mathbb{Z}$ eine exakte Sequenz von endlich-dimensionalen K-Vektorräumen ist. Daher ergibt sich die erste Behauptung aus (Übungsaufgabe 18(a)). □

5.26 Satz. *Es sei M ein endlich erzeugter, graduierter Modul über der Standard-K-Algebra A. Ferner sei* $a \in A$ *ein homogenes M-reguläres Element vom Grad* $d \geq 1$. *Dann gilt*

(a) $\dim M/aM = \dim M - 1$,

(b) $p_{M/aM}(i) = p_M(i) - p_M(i-d)$, *also insbesondere ist* $\deg M/aM = d \cdot \deg M$.

Beweis. Da a M-regulär ist, ist die Sequenz

$$0 \longrightarrow M(-d) \xrightarrow{\cdot a} M \longrightarrow M/aM$$

eine exakte Sequenz graduierter A-Moduln. Es folgt $h_M(i) = h_{M/aM}(i) + h_M(i-d)$. Somit ergibt sich die Behauptung aus (5.23) wie in Übungsaufgabe 7. □

5.27 Lemma. *Es seien* $N \subseteq M$ *graduierte Moduln über der Standard-K-Algebra A. Hat N die reduzierte Primärzerlegung* $N = Q_1 \cap \ldots \cap Q_s$, *so gilt*

$$\deg N = \sum_{\dim M/Q_i = \dim M/N} \deg Q_i.$$

(Die Summe erstreckt sich nur über die Primärmoduln maximaler Dimension.)

Beweis. Analog zu Übungsaufgabe 27. □

5.28 Lemma. *Jeder endlich erzeugte, graduierte A-Modul, A noethersch, besitzt eine* (graduierte) freie Auflösung, *d.h. eine freie Auflösung, in der alle Abbildungen Homomorphismen vom Grad null sind.*

Beweis. Es sei $\{m_1, \ldots, m_s\}$ ein Erzeugendensystem von M aus homogenen Elementen m_i vom Grad d_i. Dann ist die Abbildung

$$\varphi : \bigoplus_{i=1}^{s} A(-d_i) \longrightarrow M, \qquad (a_1, \ldots, a_s)^t \longmapsto a_1 m_1 + \ldots + a_s m_s$$

surjektiv und hat den Grad null, denn

$$(a_1, \ldots, a_s) \in (\bigoplus_{i=1}^{s} A(-d_i))_j = \bigoplus_{i=1}^{s} A_{j-d_i}$$

genau dann, wenn $\deg a_k = j - d_k$ für alle k, daher $a_k m_k \in M_j$. Folglich ist $\operatorname{Kern} \varphi$ ein endlich erzeugter, graduierter Untermodul.

Iteration dieses Schlusses liefert wie in (3.15) die Behauptung. □

5.29 Folgerung. Jeder endlich erzeugte, graduierte Modul M über dem noetherschen Ring A besitzt eine Präsentationsmatrix B, deren Einträge *homogene* Elemente sind. Hat M die (graduierte) Präsentation

$$\bigoplus_{j=1}^{t} A(-e_j) \xrightarrow{B} \bigoplus_{i=1}^{s} A(-d_i) \longrightarrow M \longrightarrow ?$$

mit der Präsentationsmatrix $B = (b_{ij}) \in A^{s\times t}$, so ist $\deg b_{ij} = e_j - d_i$.

Beweis. Betrachte $v := (0,\dots,0,a,0,\dots,0)^t$, a in $p$ter Zeile, wobei $\deg a = \delta$, also $a \in A_\delta = (A(-e_p))_{\delta+e_p}$. Dann ist $w = Bv = (ab_{1p},\dots,ab_{sp})^t$. Es ist $v \in (\bigoplus_{j=1}^{t} A(-e_j))_{\delta+e_p}$ Da $\deg w = \deg v$, d.h., für $1 \le q \le s$ folgt wegen

$$(ab_{1p},\dots,ab_{sp})^t \in (\bigoplus_{i=1}^{s} A(-d_i))_{\delta+e_p},$$

daß $ab_{qp} \in A_{\delta+e_p-d_q}$. Wegen $a \in A_\delta$ muß b_{qp} homogen vom Grad $e_p - d_q$ sein. □

5.30 Beispiel. (Vgl (3.16 i)) Über $R = K[x,y]$ hat $R/(x,y)^2$ folgende graduierte freie Auflösung

$$0 \longrightarrow R(-3)\oplus R(-3) \xrightarrow{\begin{pmatrix} -y & 0 \\ x & -y \\ 0 & x \end{pmatrix}} R^3(-2) \xrightarrow{(x^2,xy,y^2)} R \longrightarrow R/(x,y)^2 \longrightarrow 0$$

5.31 Bemerkung. (i) Wir kennen die Hilbertfunktion von $R = K[x_0,\dots,x_n]$, also auch die Hilbertfunktion von jedem endlich erzeugten, graduierten freien R-Modul, denn ist $F = \bigoplus_{i=1}^{s} R(-e_i)$, so ergibt sich

$$h_F(j) = \sum_{i=1}^{s} h_{R(-e_i)}(j) = \sum_{i=1}^{s} h_R(j-e_i).$$

(ii) Hat also ein graduierter R-Modul M die graduierte, freie Auflösung $0 \longrightarrow F_t \longrightarrow \dots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$, so können wir aus ihr die Hilbertfunktion von M berechnen, denn (nach Übung 26) ist

$$h_M(j) = \sum_{i=0}^{t} (-1)^i h_{F_i}(j).$$

5.32 Lemma. *Ist* $0 \xrightarrow{\varphi} M' \xrightarrow{\psi} M \longrightarrow M'' \longrightarrow 0$ *eine exakte Sequenz von R-Moduln und ist* $\mathfrak{a} \subseteq R$ *ein Ideal, so ist auch die Sequenz von R-Moduln* $M'/\mathfrak{a}M' \xrightarrow{\overline{\varphi}} M/\mathfrak{a}M \xrightarrow{\overline{\psi}} M''/\mathfrak{a}M'' \longrightarrow 0$ *exakt.*

Beweis. Vgl. Übung 36. □

5.33 Lemma. *Es sei M ein endlich erzeugter R-Modul, R noethersch. Dann gilt für jedes Ideal* $\mathfrak{a}$ *von R:*

$$\sqrt{Ann_R(M/\mathfrak{a}M)} = \sqrt{Ann_R(M)+\mathfrak{a}}.$$

Beweis. Es sei $R^q \xrightarrow{\varphi, A=(a_{ij})} R^p \xrightarrow{\psi} M \longrightarrow 0$ eine Präsentation von M. Diese induziert die Präsentation von $M/\mathfrak{a}M$

$$(R/\mathfrak{a})^q \xrightarrow{\overline{A}=(\overline{a}_{ij})} (R/\mathfrak{a})^q \longrightarrow M/\mathfrak{a}M \longrightarrow 0$$

wobei $\overline{a}_{ij} := a_{ij} + \mathfrak{a}/\mathfrak{a}$. Dann gilt

$$\sqrt{Ann_R(M)} = \sqrt{I_p(A)} \text{ und } \sqrt{\mathrm{Ann}_{R/\mathfrak{a}R}(M/\mathfrak{a}M)} = \sqrt{I_p(\overline{A})} = \sqrt{I_p(A)+\mathfrak{a}/\mathfrak{a}} \subseteq R/\mathfrak{a},$$

also $\sqrt{\mathrm{Ann}_R(M/\mathfrak{a}M)} = \sqrt{I_p(A)+\mathfrak{a}} = \sqrt{\mathrm{Ann}_R(M)+\mathfrak{a}}$. □

5.34 Satz. *Ist M ein endlich erzeugter, graduierter Modul über der Standard-K-Algebra A, so gilt für homogene Elemente $a_1, \dots, a_s \in A$ positiven Grades $\dim M/(a_1, \dots, a_s)M \geq \dim M - s$. Die analoge Aussage gilt, wenn M ein endlich erzeugter Modul über dem noetherschen lokalen Ring $(R, \mathfrak{m})$ ist und $a_1, \dots, a_s \in \mathfrak{m}$.*

Beweis. Dies folgt aus (5.33) wie in Übungsaufgabe 30. □

5.35 Folgerung. Ist $S \in \mathbb{P}^n$ ein projektives Schema und ist $F \in \mathbb{P}^n$ eine Hyperfläche, so gilt $\dim S - 1 \leq \dim S \cap F \leq \dim S$.

6 Liieren von Schemata

Dies geht auf eine Idee aus dem 19. Jahrhundert zurück, daß man eine Kurve duch Einbettung in eine “einfache” Kurve und Vergleich mit der “Restkurve” studiert.

Als “einfach” werden hier vollständige Durchschnitte gelten.

Im Folgenden sei stets $R = K[x_0, \dots, x_n]$ aufgefasst als graduierte Standard-K-Algebra.

ungemischte Schemata

6.1 Definition. Ein Ideal $\mathfrak{a} \subseteq R$ bzw. ein Schema $S \subseteq \mathbb{P}^n$ heißt *ungemischt*, wenn alle seine Primärkomponenten die gleiche Dimension haben, d.h., wenn für alle $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})$ gilt $\dim R/\mathfrak{p} = \dim R/\mathfrak{a}$.

6.2 Lemma. *Es sei $S \subseteq \mathbb{P}^n$ ein vollständiger Durchschnitt der Höhe c. Dann gilt:*

(a) S ist ungemischt.

(b) Hat S den Typ $(d_1, \dots, d_c)$, d.h. $I_s = (f_1, \dots, d_c)$ mit $\deg f_i = d_i$*, so ist* $\deg S = d_1 \cdots d_c$.

Beweis. (a) Wird sich später aus einem allgemeineren Resultat ergeben.

(b) Übungsaufgabe 35.

□

geometrische Liaison $V_1 \underset{X}{\sim} V_2$

6.3 Definition. Zwei nichtleere, ungemischte Schemata $V_1, V_2 \subseteq \mathbb{P}^n$ gleicher Höhe heißen *geomertrisch liiert durch X*, wenn V_1 und V_2 keine gemeinsamen Primärkomponenten haben, d.h. $\mathrm{Ass}(R/I_{V_1}) \cap \mathrm{Ass}(R/I_{V_2}) = \varnothing$, und wenn $X := V_1 \cup V_2$ ein vollständiger Durchschnitt ist.

Schreibweise: $V_1 \underset{X}{\sim} V_2$.

Algebraisch: Sind $I_{V_1} = \mathfrak{q}_1 \cap \dots \cap q_s$, $I_{V_2} = \tilde{\mathfrak{q}_1} \cap \dots \cap \tilde{\mathfrak{q}_t}$, so ist $I_{V_1} \cap I_{V_2}$ ein vollständiger Durchschnitt mit der reduzierten Primärzerlegung $I_{V_1} \cap I_{V_2} = \mathfrak{q}_1 \cap \dots \cap q_s \cap \tilde{\mathfrak{q}_1} \cap \dots \cap \tilde{\mathfrak{q}_t}$.

6.4 Beispiel. Zwei Geraden in $\mathbb{P}^3$, die sich schneiden, sind geometrisch liiert. $(x_1, x_3) \cap (x_2, x_3) = (x_1x_2, x_3)$. [Bilder]

6.5 Folgerung. Sind $V_1, V_2 \subseteq \mathbb{P}^n$ geometrisch liiert durch X, so gilt $\deg V_1 + \deg V_2 = \deg X$.

Beweis. Die Behauptung folgt aus Übungsaufgabe 27. □

6.6 Beispiel. $(x_1, x_2) \cap ?? = (x_1x_2, x_1 + x_2)$. [Bilder] Der Durchschnitt ist (als reduziertes Schema) eine Gerade L. Man ist versucht, zu sagen, daß L zu sich selbst liiert ist. Formal wird das präzisiert durch die folgende

Direkte Liaison $V_1 \underset{X}{\sim} V_2$

6.7 Definition. Zwei nichtleere Schemata $V_1, V_2 \subseteq \mathbb{P}^n$ heißen *direkt liiert* (durch X), wenn es einen vollständigen Durchschnitt $X \in \mathbb{P}^n$ gibt, so daß gilt $I_X : I_{V_1} = I_{V_2}$ und $I_X : I_{V_2} = I_{V_1}$. Schreibweise wieder $V_1 \underset{X}{\sim} V_2$. Analog ist dies definiert für homogene Ideale von $R = K[x_0, \dots, x_n]$.

6.8 Beispiel. (i) (Vgl. 6.6) $(x_1x_2, x_1 + x_2)$ definiert einen vollständigen Durchschnitt $X \subseteq \mathbb{P}^3$. Für die durch $I_L = (x_1, x_2)$ definierte Gerade $L \subseteq \mathbb{P}^3$ gilt $I_X : I_L = (x_1x_2, x_1 + x_2) : (x_1, x_2) = (x_1, x_2)$, d. h., L ist zu sich selbst direkt liiert.

(ii) Die Ideale $(x_1, x_2)^2$ und (x_1, x_2) sind direkt liiert, denn $(x_1^2, x_2^2) : (x_1^2, x_1x_2, x_2^2) = (x_1, x_2)$ und $(x_1^2, x_2^2) : (x_1, x_2) = (x_1^2, x_1x_2, x_2^2)$.

6.9 Lemma. *Sind V_1, V_2 direkt durch X liiert, so gilt:*

(a) $\sqrt{I_{V_1} \cap I_{V_2}} = \sqrt{I_X}$.

(b) V_1 *und* V_2 *sind ungemischt und haben die gleiche Höhe wie* X.

(c) Haben V_1, V_2 *keine gemeinsamen Primärkomponenten, so sind* V_1, V_2 *geometrisch liiert.*

(d) $\deg X = \deg V_1 + \deg V_2$.

Beweis. (a) Es gilt $I_{V_1} \cdot I_{V_2} \subseteq I_X \subseteq I_{V_1} \cap I_{V_2}$. Daraus folgt die Behauptung, da $\sqrt{\mathfrak{a} \cdot \mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

(b) Sei $I_X = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ die reduzierte Primärzerlegung von I_X. Dann ist $I_{V_1} = I_X : I_{V_2} = \bigcap_{i=1}^s (\mathfrak{q}_i : I_{V_2})$ und

$$q_i : I_{V_2} = \begin{cases} R, & \text{falls } I_{V_2} \in \mathfrak{q}_i, \\ \text{ein zu } \sqrt{\mathfrak{q}_i}\text{assoziiertes Primärideal} & \text{sonst.} \end{cases}$$

Damit sind V_1, V_2 ungemischt der Höhe von I_X, da I_X als vollständiger Durchschnitt ungemischt ist, und $h(\mathfrak{q}_i) = h(\mathfrak{q}_i : I_{V_2})$ falls $I_{V_2} \not\subseteq \mathfrak{q}_i$. Also sind V_1, V_2 ungemischt und $h(I_{V_1}) = h(I_{V_2}) = h(X)$.

(c) Zu zeigen: $I_{V_1} \cap I_{V_2} = I_X$.

"$\supseteq$" klar.

"$\subseteq$" Sei $F \in I_{V_1} \cap I_{V_2}$. Angenommen $F \notin \mathfrak{q}_i$ für ein $\mathfrak{q}_i$ aus $I_X = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ (d.h. $F \notin I_X$). Sei o. E. $\sqrt{\mathfrak{q}_i} \in \operatorname{Ass}(R/I_{V_1})$.

Aus der Voraussetzung folgt, daß es ein $G \in I_{V_2}$ gibt mit $G \notin \mathfrak{p}$ für alle $\mathfrak{p} \in \operatorname{Ass}(R/I_{V_1})$. Wegen $F \in I_{V_1}$ und $G \in I_{V_2}$ ergibt sich aus $I_{V_1} = I_X : I_{V_2}$, daß $F \cdot G \in I_X \subseteq \mathfrak{q}_i$. Da aber $G \notin \sqrt{\mathfrak{q}_i}$, folgt $F \in \mathfrak{q}_i$. Widerspruch zur Annahme.

(d) Siehe J. Migliore: "Introduction to liaison theory and deficiency modules".

□

Sind V_1 und V_2 direkt liiert, so ist die Liaison eine symmetrische Relation. Direktes Liieren ist jedoch im Allgemeinen weder reflexiv noch transitiv. Es erzeugt aber eine Äquivalenzrelation:

6.10 Definition. Zwei nichtleere Schemata $V, W \subseteq \mathbb{P}^n$ heißen *liiert*, wenn es vollständige Durchschnitte $X_1, \ldots, X_k \subseteq \mathbb{P}^n$ gibt derart, daß gilt — Liierte Schemata

(3) $\quad V =: V_1 \underset{X_1}{\sim} V_2 \underset{X_2}{\sim} \ldots \underset{X_k}{\sim} V_{k+1} := W.$

Wir schreiben dann $V \sim W$. Diese Relation ist eine Äquivalenzrelation und heißt Liaison. Die Menge $[V] := \{W \subseteq \mathbb{P}^n \mid W \sim V\}$ heißt die *Liaisonklasse* von V. — Liaisonklasse $[V]$

Die Schemata V und W heißen *gerade liiert*, falls k in (3) als gerade Zahl gewählt werden kann. Die Menge $\mathcal{L}_V := \{W \subseteq \mathbb{P}^n \mid W \text{ ist gerade liiert zu } V\}$ heißt die *gerade Liaisonklasse* von V. — Gerade Liaison, gerade Liaisonklasse

Die analogen Definitionen gelten auch für homogene Ideale von R.

6.11 Bemerkung (Probleme). (i) Wie kann man entscheiden, ob zwei ungemischte Schemata $V, W \subseteq \mathbb{P}^n$ gleicher Höhe zur gleichen Liaisonklasse gehören?

(ii) Kann man alle Element einer Liaisonklasse beschreiben? Gibt es in ihr ausgezeichnete Elemente?

6.12 Bemerkung. (i) Nach (6.9 (b)) sind alle Schemata in $[V]$ ungemischt und haben gleiche Höhe.

(ii) Ist W direkt liiert zu V, so gilt $[V] = \mathcal{L}_V \cup \mathcal{L}_W$, d. h., jede Liaisonklasse besteht aus höchstens zwei geraden Liaisonklassen. Aber es kann auch $[V] = \mathcal{L}_V$ gelten.

Beispiel: $(x_0^2, x_1) : (x_0, x_1) = (x_0, x_1)$ also $[(x_0, x_1)] = \mathcal{L}_{(x_0,x_1)}$.

Folgende Resultate helfen manchmal zu entscheiden, ob zwei Schemata liiert sind.

6.13 Lemma. *Sind* $\mathfrak{a}, \mathfrak{b}$ *homogene ungemischte Ideale gleicher Höhe mit* $\mathfrak{a} \subseteq \mathfrak{b}$ *und* $\deg \mathfrak{a} = \deg \mathfrak{b}$*, so gilt schon* $\mathfrak{a} = \mathfrak{b}$.

Beweis. Für $\dim R/\mathfrak{a} \leq 1$.

(1) Sei $\dim R/\mathfrak{a} = \dim R/\mathfrak{b} = 0$. Aus $\mathfrak{a} \subseteq \mathfrak{b}$ folgt $\dim_k [R/\mathfrak{a}]_j \geq \dim [R/b]_j$ für alle $j \in \mathbb{Z}$. Da nun $\sum_{j\in\mathbb{Z}} \dim_k [R/\mathfrak{a}]_j = \deg R/\mathfrak{a} = \deg R/\mathfrak{b} = \sum_{j\in\mathbb{Z}} \dim_k [R/\mathfrak{b}]_j$ ergibt sich $\dim_k [R/\mathfrak{a}]_j = \dim_k [R/\mathfrak{b}]_j$ und somit $[R/\mathfrak{a}]_j = [R/\mathfrak{b}]_j$ für alle $j \in \mathbb{Z}$.

(2) Sei $\dim R/\mathfrak{a} = 1 = \dim R/\mathfrak{b}$. Da $\mathfrak{a}$ und $\mathfrak{b}$ ungemischt sind, gibt es eine Linearform $l \in [R]_1$, die in keinem Primteiler von $\mathfrak{a}$ oder $\mathfrak{b}$ enthalten ist. Damit ist l ein Nichtnullteiler sowohl von $R/\mathfrak{a}$ als auch von $R/\mathfrak{b}$. Es gilt dann

(4) $\deg R/(\mathfrak{a} + lR) = \deg R/\mathfrak{a} = \deg R/\mathfrak{b} = \deg R/(\mathfrak{b} + lR)$.

Wir betrachten die exakten Sequenzen

$$0 \longrightarrow R/\mathfrak{a}(-1) \xrightarrow{l} R/\mathfrak{a} \longrightarrow R/\mathfrak{a} + lR \longrightarrow 0,$$

$$0 \longrightarrow R/\mathfrak{b}(-1) \xrightarrow{l} R/\mathfrak{b} \longrightarrow R/\mathfrak{b} + lR \longrightarrow 0.$$

Also $h_{R/\mathfrak{a}}(j) - h_{R/\mathfrak{a}}(j-1) = A_{R/\mathfrak{a}+lR}(j)$ und $h_{R/\mathfrak{b}}(j) - h_{R/\mathfrak{b}}(j-1) = A_{R/\mathfrak{b}+lR}(j)$ für alle $j \in \mathbb{Z}$. Wegen $\dim R/\mathfrak{a} + lR = \dim R/\mathfrak{b} + lR = 0$ gilt bereits wegen (4) $h_{R/\mathfrak{a}+lR} = h_{R/\mathfrak{b}+lR}$, also $h_{R/\mathfrak{a}} = h_{R/\mathfrak{b}}$, und somit gilt $\mathfrak{a} = \mathfrak{b}$

□

6.14 Folgerung. Ist $\mathfrak{a}$ ein homogenes, ungemischtes Ideal der Höhe h, und ist $\mathfrak{c} \subseteq \mathfrak{a}$ ein vollständiger Durchschnitt der Höhe h, dann sind $\mathfrak{c} : \mathfrak{a}$ und $\mathfrak{a}$ durch $\mathfrak{c}$ direkt liiert.

Beweis. Zu zeigen bleibt: $\mathfrak{c} : (\mathfrak{c} : \mathfrak{a}) = \mathfrak{a}$. Nun gilt $\mathfrak{a} \subseteq \mathfrak{c} : (\mathfrak{c} : \mathfrak{a})$ und nach (6.9) gilt $\deg(\mathfrak{c} : (\mathfrak{c} : \mathfrak{a})) = \deg \mathfrak{c} - \deg(\mathfrak{c} : \mathfrak{a}) = \deg \mathfrak{c} - (\deg \mathfrak{c} - \deg \mathfrak{a}) = \deg \mathfrak{a}$.

Also gilt nach (6.12) $\mathfrak{c} : (\mathfrak{c} : \mathfrak{a}) = \mathfrak{a}$. □

6.15 Folgerung. Alle vollständigen Durchschnitte gleicher Höhe liegen in der selben Liaisonklasse.

Beweis. Betrachte den Spezialfall der vollständigen Durchschnitte $\mathfrak{a} = (f_1, \ldots, f_{h-1}, f)$ und $\mathfrak{b} = (f_1, \ldots, f_{h-1}, g)$. Wir setzen $\mathfrak{c} = (f_1, \ldots, f_{h-1}, f \cdot g)$. Dann gilt $\mathfrak{c} : \mathfrak{a} \supseteq \mathfrak{b}$ und $\deg(\mathfrak{c} : \mathfrak{a}) = \deg \mathfrak{b}$. Also $\mathfrak{a} \underset{\mathfrak{c}}{\sim} \mathfrak{b}$ nach (6.13).

Sind $\mathfrak{a}, \mathfrak{b}$ beliebige vollständige Durchschnitte der Höhe h, so kann man mit dieser Methode von $\mathfrak{a}$ in höchstens h Schritten $\mathfrak{b}$ erreichen, indem man in jedem Schritt ein Erzeugendes auswechselt. □

6.16 Bemerkung. (i) Jede Gerade ist ein Vollständiger Durchschnitt. Daher liegen alle Geraden in der gleichen Liaison-Klasse.

(ii) Nach Beispiel (6.4) liegt ein Paar sich schneidender Geraden in der gleichen Liaisonklasse $\mathfrak{L}$ wie jede der Geraden.

(iii) Wir werden später sehen, daß ein Paar windschiefer Geraden *nicht* in der gleichen Liaison-Klasse $\mathfrak{L}$ liegen.

Für die Beschreibung einer geraden Liaisonklasse ist folgende Konstruktion wesentlich:

6.17 Satz. *Sei $\mathfrak{a} \subseteq R$ ein homogenes ungemischtes Ideal der Höhe h. Ferner sei $\mathfrak{c} := (f_1, \dots, f_h)$ ein vollständiger Durchschnitt der Höhe h mit $(f_1, \dots, f_h) \subseteq \mathfrak{a}$. Dann gilt mit $\mathfrak{b} := (f_1, \dots, f_{h-1}) + f_h \cdot \mathfrak{a}$ und $d = \deg f_h$ für die Hilbert-Funktionen:*

$$h_{R/\mathfrak{b}}(j) = h_{R/\mathfrak{a}}(j-d) + h_{R/\mathfrak{c}}(j).$$

Insbesondere gilt $\deg \mathfrak{b} = \deg \mathfrak{a} + \deg \mathfrak{c}$.

Beweis. Sei $\tilde{\mathfrak{c}} := (f_1, \dots, f_{h-1})$. Da $\mathfrak{c} = \tilde{\mathfrak{c}} + f_h R$ ein vollständiger Durchschnitt ist, gilt $\tilde{\mathfrak{c}} : f_h = \tilde{\mathfrak{c}}$ (Vgl. Übung 35). Die Sequenz

$$0 \longrightarrow \tilde{\mathfrak{c}}(-d) \xrightarrow{\varphi} \tilde{\mathfrak{c}} \oplus \mathfrak{a}(-d) \xrightarrow{\psi} \mathfrak{c} + f_h \cdot \mathfrak{a} \longrightarrow 0$$

mit $\varphi : r \longmapsto (f_h \cdot r, r)$ und $\psi : (r,s) \longmapsto r - f_h \cdot s$ ist exakt, denn ψ ist offenbar surjektiv, $\psi \circ \varphi = 0$ und mit $\psi(r,s) = 0$ ist $r - f_h \cdot s = 0$, also $r = f_h \cdot s \in \tilde{\mathfrak{c}}$, und damit $s \in \tilde{\mathfrak{c}} : f_h = \tilde{\mathfrak{c}}$.

Folglich ergibt sich $h_{R/(\mathfrak{c}+\tilde{f}_h\mathfrak{a})(j)} = h_{R/\mathfrak{a}}(j-d) + h_{R/\tilde{\mathfrak{c}}}(j) - h_{R(\tilde{\mathfrak{c}}}(j-d)$. Da auch die Sequenz

$$0 \longrightarrow R/\tilde{\mathfrak{c}}(-d) \xrightarrow{f_h} R/\tilde{\mathfrak{c}} \longrightarrow R/\mathfrak{c} \longrightarrow 0$$

exakt ist, gilt $h_{R/\mathfrak{c}}(j) = h_{R/\tilde{\mathfrak{c}}}(j) - h_{R/\tilde{\mathfrak{c}}}(j-d)$. Einsetzten in in die obige Gleichung ergibt die Behauptung. □

6.18 Bemerkung. (i) Seien $V, W, X \subseteq \mathbb{P}^n$ die durch $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in R$ definierten Schemata (wie in (6.17)). Intuitiv würde man $W = V \cup X$ erwarten. Dies ist i. A. nur richtig, wenn W reduziert ist.

(ii) Wir werden sehen, daß $\mathfrak{b}$ in zwei Schritten zu $\mathfrak{a}$ liiert ist.

7 Berechnung von Idealquotienten und freien Auflösungen mit Hilfe von Gröbnerbasen.

Se stets $R = k[x_1,\dots,x_n]$ und $F = \bigoplus_{i=1}^{s} R\cdot e_i$ ein ein freier Modul vom Rang r mit Basis $\{e_1,\dots,e_r\}$

Monome in F

7.1 Definition. (i) Ein *Monom in F* ist ein Element der Form $m\cdot e_i$, $1\le i\le r$, wobei $m\in R$ ein Monom ist.

monomiale Ordnung $\succ$

(ii) Eine *monomiale Ordnung* $\succ$ auf F ist eine totale Ordnung auf F mit der Eigenschaft:

Für alle Monome $m_1,m_2\in F,\ n\in R$ gilt $m_1\succ m_2 \Longrightarrow n\cdot m_1\succ n\cdot m_2$.

Eine solche Ordnung ist stets eine Wohlordnung.

7.2 Beispiel. Sei $\succ$ eine monomiale Ordnung auf R. Dann definieren wir eine Ordnung $\succ$ auf F wie folgt: Sind $m_1,m_2\in F$ Monome mit $m_1 = n_1\cdot e_j$ und $m_2 = n_2\cdot e_j$ für Monome $n_1,n_2\in R$, so setzen wir $m_1\succ m_2$ falls $j>i$ oder $j=i$ und $n_1\succ n_2$. Dies ist eine monomiale Ordnung auf F.

$in_{\succ}(f)$

Leitterm, Leitform, Initialform

7.3 Definition. Für $f\in F$ bezeichne $in(f) := in_{\succ}(f) :=$ das bezüglich $\succ$ größte Monom von f. Es wird *Leitterm, Leitform* oder auch *Initialform* von f genannt.

Gröbnerbasen

7.4 Definition. Sei M ein Untermodul von F. Dann heißt $G=\{g_1,\dots,g_s\}$, $g_i\in M$ für $1\le i\le s$, eine *Gröbnerbasis* von M, falls G eine Basis von M ist und

$$im(M) := \langle\{\, in(m)\mid m\in M\}\rangle = \langle\{\, in(g)\mid g\in G\}\rangle$$

gilt.

7.5 Satz. *Jeder Untermodul $M\subseteq F$ besitzt eine Gröbnerbasis.*

Beweis. Wie bei Idealen. □

7.6 Definition. Es seien $f,g_1,\dots,g_t\in F=\bigoplus_{i=1}^{r} Re_i$. Ein Ausdruck der Form $f=\sum_{i=1}^{t} f_ig_i + h$ mit $f_i\in R, h\in F$ derart, daß kein Monom von h in $(in(g_1),\dots,in(g_t))$ liegt und $in(f)\ge in(f_ig_i)$ für alle i, heißt *Standardausdruck* von f bezüglich $\{g_1,\dots,g_t\}$ (und h der *Rest*).

Die Existenz liefert der

7.7 Algorithmus (Divisionsalgorithmus). Eingabe: $f,g_1,\dots,g_t\in F$

Ausgabe: $f_1,\dots,f_t\in R,\ h\in F$ derart daß $f=\sum_{i=1}^{t} f_ig_i+h$ ein Standardausdruck ist.

(1) $h:=f,\ j:=1$

(2) while $h\neq 0$ do: Bestimme $i_j\in\{1,\dots,.\}.t$ derart, daß $in(g_{i_j})$ das größte Monom m von h teilt, welches in $(in(g_1),\dots,in(g_t))$ liegt; bei Nichtexistenz gehe zu (3).

Setze $r_{ij} := \frac{m}{in(g_{i_j})}\in R$, $h:=h-r_{i_j}g_{i_j}$, $j:=j+1$.

(3) Sortiere r_{i_j} zu den Koeffizienten f_i von g_i.

7.8 Beispiel. $x>y,\ <=<_{lex}$

	$g_1 = xy-1$	$g_2 = y^2-1$
$f = x^2y+xy^2+y^2-(x^2y-x)$	x	
$xy^2+x+y^2-(xy^2-y)$	y	
$x+y^2+y-(y^2-1)$		1
$x+y+1=h$		

Also ist der Standardausdruck von f bezüglich $\{g_1, g_2\}$

$$(x+y)g_1 + 1g_2 + \underbrace{x+y+1}_{h}.$$

7.9 Definition (Notationen).

$$\varphi : G := \bigoplus_{j=1}^{t} R\varepsilon_j \xrightarrow{\varphi} M = (g_1, \dots, g_t) \subseteq F = \bigoplus_{i=1}^{r} Re_i, \qquad \varepsilon_j \longmapsto g_j$$

Elemente von $\operatorname{Kern}\varphi$ nennen wir *Syziygien*, genauer *erste Syzygien* von *m*.

Es sei $(i, j), 1 \leq i, j \leq t$ ein Paar von Indizes.

Fall 1: $in(g_i)$ und $in(g_j)$ sind nicht Vielfache desselben Basiselements von F. Setze $h_{ij} = 0$.

Fall 2: Anderenfalls setze $m_{ij} := \frac{in(g_i)}{\mathrm{ggT}(in(g_i), in(g_j))} \in R$ und bilde einen Standardausdruck $m_{ji}g_i - m_{ij}g_j = \sum_{k=1}^{t} f_k^{(ij)g_k + h_{ij}}$.

7.10 Satz. *(a)* **(Buchberger Kriterium)** $\{g_1, \dots, g_t\}$ *ist eine Gröbnerbasis von M genau dann, wenn alle* $h_{ij} = 0$.

(b) Ist $\{g_1, \dots, g_t\}$ *eine Gröbnerbasis von M, so ist* $\left\{ \tau_{ij} \,\middle|\, 1 \leq i, j \leq t \right\}$ *ein Erzeugendensystem von* $\operatorname{Kern}\varphi$, *wobei*

$$\tau_{ij} = m_{ji}\varepsilon_i - m_{ij}\varepsilon_j - \sum_{k=1}^{t} f_k^{(ij)}\varepsilon_k.$$

In Vektorschreibweise:

$$\tau_{ij} = \begin{pmatrix} 0 \\ vdots \\ m_{ji} \\ \vdots \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ vdots \\ m_{ij} \\ \vdots \\ 0 \end{pmatrix} - \begin{pmatrix} f_1^{(ij)} \\ \vdots \\ f_t^{(ij)} \end{pmatrix} \in R^t.$$

(c) Definiere eine monomiale Ordnung auf G wie folgt: Für Monome $m, n \in R$ *ist* $m\varepsilon_i \geq n\varepsilon_j$, *falls* $in(m\varepsilon_i) > in(n\varepsilon_j)$ *bezüglich der Ordnung auf F oder* $in(m\varepsilon_i) = in(n\varepsilon_j)$, *aber* $i < j$.

Ist $\{g_1, \dots, g_t\}$ *eine Gröbnerbasis von M, so ist* $\left\{ \tau_{ij} \,\middle|\, 1 \leq i, j \leq t \right\}$ *eine Gröbnerbasis von* $\operatorname{Kern}\varphi$ *bezüglich der obigen Ordnung auf G.*

7.11 Beispiel. $x > y$, $<=<_{lex}$, $g_1 = x^2, g_2 = xy + y^2, M = (g_1, g_2) \subseteq R = K[x,y]$. $in(g_1) = x^2$, $in(g_2) = xy$ haben ggT x.

$$\frac{in(g_2)}{x} g_1 - \frac{in(g_1)}{x} g_2 = -xy^2 = (-y)g_2 + \underbrace{y^3}_{h_{12}} \quad \text{Standardausdruck.}$$

Setze $g_3 := h_{12} = y^3$ und erhalte Syzygie von $M = (g_1, g_2, g_3)$:

$$\tau_{12} = \begin{pmatrix} y \\ -x+y \\ -1 \end{pmatrix}.$$

Es ist $h_{13} = 0$. Betrachte das Paar $(g2, g3)$. Es ist $\mathrm{ggT}(in(g_2), in(g_3)) = y$

$$\frac{in(g_3)}{y} g_2 - \frac{in(g_2)}{y} g_3 = y = yg_3,$$

also $h_{23} = 0$. Somit ist $\{g_1, g_2, g_3\}$ eine Gröbnerbasis von M und $\{\tau_{12}, \tau_{13}, \tau_{23}\}$ eine Gröbnerbasis (bezüglich der richtigen Ordnung) des Syzyienmoduls von M.