Inhalt

I Primideale, Jacobsonradikal,Nakayamalemma , lokale Ringe ... 3

II Nöthersche Ringe und Moduln. Hilberts Basissatz 7

III Der Hilbertsche Nullstellensatz 9

IV Ganze Ringerweiterungen. Die Sätze von Cohen Seidenberg 12

V Der nöthersche Normalisierungssatz 16

VI Lokalisierung 19

VII Primärzerlegung 23

VIII Moduln endlicher Länge 31

IX Graduierte Moduln. Das Hilbertpolynom 33

X Filtrierungen. Der Satz von Artin-Rees. Das Hilber-Samuel Polynom 38

XI Die Dimension von Moduln und Ringen 43

XII Cohen-Macaulay Moduln 49

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

XIII Die homologische Dimension 53

XIV Gorenstein Ringe 59

XV Reguläre Ringe 64

XVI Moduln endlicher homologischer Dimension 70

XVII Eindeutige Primfaktorzerlegung in regulären lokalen Ringen nach Kaplanski 72

Anhang: Gröbnerbasen 78

I Ringe, Primideale, das Jacobsonradikal. Lokale Ringe.

Alle betrachteten Ringe sind kommutativ und *unitär* , d.h. besitzen ein Einselement. Alle betrachteten Moduln über einem solchen Ring sind *unitär* , d.h. das Einselement operiert wie die Identität auf einem solchen Modul. Ein Ring A kann immer auch als Modul über sich selbst aufgefaßt werden. Genau dann sind Nullelement und Einselement eines Ringes gleich, wenn der Ring der Nullring ist, also nur das Nullelement enthält.

Definition. Ein Ring A heißt Integritätsbereich, wenn Null- und Einselement verschieden sind und wenn A nullteilerfrei ist, d.h.

$$\forall a, b \in A \text{ mit } a \neq 0, b \neq 0 \Longrightarrow ab \neq 0$$

Ein Ideal $\mathfrak{a}$ eines Ringes A ist ein A-Untermodul von A aufgefaßt als A-Modul.

Definition. Ein Ideal $\mathfrak{p}$ eines Ringes A heißt Primideal, wenn eine der folgenden Eigenschaften erfüllt sind.

(1) Der Resklassenring $A/\mathfrak{p}$ ist ein Integritätsbereich.
(2) $\mathfrak{p} \neq A$. Es gilt
$$\forall a, b \notin \mathfrak{p} \Longrightarrow ab \notin \mathfrak{p}$$

Ein Ideal $\mathfrak{m}$ von A heißt maximales Ideal, wenn eine der folgenden äquivalenten Eigenschaften erfüllt ist

(1) Der Restklassenring $A/\mathfrak{m}$ ist ein Körper.
(2) $\mathfrak{m} \neq A$. Ein Ideal, das $\mathfrak{m}$ enthält ist entweder $\mathfrak{m}$ oder der ganze Ring.

Offenbar ist jedes maximale Ideal auch ein Primideal.

Bemerkung. Die Gesamtheit $Spec(A)$ aller Primideale des Ringes A heißt das *Spectrum* von A. Es wird mit einer Topologie, der *Zariskitopologie* versehen: Abgeschlossene Mengen sind die "Nullstellenmengen"

$$W(\mathfrak{a}) = \{\mathfrak{p} \in Spec(A) | \mathfrak{a} \subseteq \mathfrak{p}\}$$

von Idealen $\mathfrak{a} \subseteq A$. Für einen endlichen Modul M über einem nötherschen Ring A ist dann der Träger bzw. die Varietät von M

$$V(M) = \{\mathfrak{p} \in Spec(A) | M_{\mathfrak{p}} \neq 0\}$$

eine abgeschlossene Menge. Dabei ist $M_{\mathfrak{p}}$ die Lokalisierung nach dem Primideal $\mathfrak{p}$ (VI Lokalisierung). Siehe den Abschnitt VII Primärzerlegung.

Existenz von Primidealen

Sei $S \subseteq A$ eine nichtleere multiplikative Teilmenge des Ringes A:

$$s, t \in S \Longrightarrow st \in S$$

Lemma. *Sei die Familie der Ideale $\mathfrak{b}$, die kein Element von S enthalten, nicht leer und sei $\mathfrak{p}$ ein maximales Element dieser Familie bezüglich der Enthaltenseinsrelation. Dann ist $\mathfrak{p}$ ein Primideal.*

Beweis. Seien a, b zwei Elemente von A, die nicht in $\mathfrak{p}$ enthalten sind mit $ab \in \mathfrak{p}$. Wegen der Maximalität von $\mathfrak{p}$ gibt es Elemente $x, y \in A$, Elemente $\alpha, \beta \in \mathfrak{p}$ und Elemente $s, t \in S$ mit $xa + \alpha = s$, $yb + \beta = t$. Es folgt

$$st = (xa + \alpha)(yb + \beta) = xyab + xa\beta + yb\alpha + \alpha\beta \in \mathfrak{p}$$

Also ist $S \cap \mathfrak{p} \neq \emptyset$. Das ist ein Widerspruch $\square$

Sei $\mathfrak{a}$ ein Ideal mit $S \cap \mathfrak{a} = \emptyset$. Aus dem Zornschen Lemma folgt dann, daß es in der Menge aller Ideale, die $\mathfrak{a}$ umfassen und die mit S einen leeren Durchschnitt haben maximale Elemente bezüglich der Enthaltenseinsrelation gibt. Ist A ein nötherscher Ring (siehe *Nöthersche Ringe*), so folgt die Existenz bereits aus der Kettenbedingung für Ideale nötherscher Ringe; es ist dann nicht notwendig, Zorns Lemma, oder äquivalent dazu das Auswahlaxiom zu benutzen. Wir können das Resultat auf die Menge $S = \{1\}$ anwenden und erhalten

Satz. *Sei $\mathfrak{a} \neq A$ ein Ideal des Ringes A. Dann gibt es ein maximales Ideal, das $\mathfrak{a}$ umfaßt. Ist A ein vom Nullring verschiedener Ring, so enthält A immer ein maximales Ideal. Insbesondere besitzt jeder solche Ring ein Primideal.*

Eigenschaften von Primidealen.

Unmittelbar aus der Definition eines Primideals folgt:

Seien $\mathfrak{a}, \mathfrak{b}$ Ideale und $\mathfrak{p}$ ein Primideal

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Longrightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ oder } \mathfrak{b} \subseteq \mathfrak{p}$$

Lemma. *Gegeben seien Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ und ein weiteres Ideal $\mathfrak{a}$.*

(1) *Sei $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$ Dann gibt es einen Index ν_0 mit $\mathfrak{a} \subseteq \mathfrak{p}_{\nu_0}$*

(2)

$$\mathfrak{a} = \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r \Longrightarrow \mathfrak{a} = \mathfrak{p}_{\nu_0}$$

Beweis von (1). Wähle r minimal mit $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$ Angenommen, es sei $r \geq 2$. Dann gibt es zu jeder natürlichen Zahl $1 \leq k \leq r$ ein Element $a_k \in \mathfrak{a}$ mit $a_k \notin \bigcup_{j \neq k} \mathfrak{p}_j$. Dann gilt $a_k \in \mathfrak{p}_k$. Sei $b_k = \prod_{j \neq k} a_j$. Dann gilt

$$b_k \begin{cases} \in \mathfrak{p}_j & j \neq k \\ \notin \mathfrak{p}_j & j = k \end{cases}$$

Es folgt $\sum_k b_k \notin \bigcup_j \mathfrak{p}_j$. Aber: $\sum_k b_k \in \mathfrak{a}$. Das ist ein Widerspruch $\square$

Auf ähnliche Weise beweist man eine Variante dieses Lemmas

Lemma. *Sei* $\mathfrak{p}$ *ein Primideal und seien* $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_s$ *beliebige Ideale mit*

$$\begin{aligned} \mathfrak{a} &\subseteq \mathfrak{p} \cup \mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_s \\ \mathfrak{a}_1, \ldots, \mathfrak{a}_s &\not\subseteq \mathfrak{p} \\ \mathfrak{a} &\not\subseteq \mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_s \end{aligned}$$

Dann gilt

$$\mathfrak{a} \subseteq \mathfrak{p}$$

Beweis. Sei $\mathfrak{a} \not\subseteq \mathfrak{p}$ und sei s minimal gewählt. $s \geq 1$. Es gibt dann ein Element p mit

$$p \in \mathfrak{a}\ ,\ p \in \mathfrak{p}\ ,\ p \notin \mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_s$$

Weil die Ideale $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_s$ nicht in $\mathfrak{p}$ enthalten sind und weil $\mathfrak{p}$ ein Primideal ist, gilt

$$\mathfrak{a}\mathfrak{a}_1 \ldots \mathfrak{a}_s \subseteq \mathfrak{a} \cap \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_s \not\subseteq \mathfrak{p}$$

Wähle ein Element $\alpha \in \mathfrak{a} \cap \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_s \setminus \mathfrak{p}$. Dann ist $p + \alpha$ in $\mathfrak{a}$, aber nicht in $\mathfrak{p} \cup \mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_s$ enthalten! $\square$

Lokale Ringe, das Jacobsonradikal.

Der Ring A sei nicht der Nullring. Ein Element von A ist genau dann invertierbar, wenn es in keinem maximalen Ideal enthalten ist. Sei a ein Element des Ringes A, das in allen maximalen Idealen enthalten ist. Dann ist $1 + a$ in keinem maximalen Ideal enthalten, also invertierbar. Sei a ein Ringelement, das in einem maximalen Ideal $\mathfrak{m}$ nicht enthalten ist. Dann ist $Aa + \mathfrak{m} = A$; es gibt also ein Element $x \in A$ und ein Element $m \in \mathfrak{m}$ mit $1 = m - xa$, und $1 + xa = m$ nicht invertierbar.

Definition. Das Jacobsonradikal $\mathfrak{r}$ des Ringes A ist das Ideal, das durch eine der folgenden äquivalenten Eigenschaften gekennzeichnet ist

$$\begin{aligned} \mathfrak{r} &= \bigcap_{\mathfrak{m}\ \text{maximal}} \mathfrak{m} \\ \mathfrak{r} &= \{a \in A | 1 + xa \text{ invertierbar } \forall x \in A\} \end{aligned}$$

Bemerkung. Ein Element a heißt nilpotent, wenn es eine natürliche Zahl $n \geq 1$ gibt mit $a^n = 0$. Im Jakobsonradikal sind alle nilpotenten Elemente enthalten. Die Gesamtheit aller nilpotenten Elemente bilden ein Ideal, das Nilradikal des Ringes A. Mit Hilfe der Existenzsätze für Primideale zeigt man, daß das Nilradikal der Durchschnitt aller Primideale ist.

Lemma von Nakayama. *Sei* $\mathfrak{a}$ *ein Ideal, das im Jakobsonradikal des Ringes* A *enthalten ist und sei* M *ein endlicher* A*-Modul mit*

$$\mathfrak{a}M = M$$

Dann verschwindet M.

Folgerung. *Sei N ein Untermodul des endlichen A-Moduls M und $\mathfrak{a}$ ein im Jakobsonradikal enthaltenes Ideal mit $\mathfrak{a}M + N = M$. Dann gilt $M = N$.*

Beweis des Lemmas. Sei $M = Ax_1 + \cdots + Ax_m$. Sei $M \neq 0$. Wir wählen m minimal. Es gibt dann Elemente $a, a_1, \ldots, a_m \in \mathfrak{a}$ mit $x_m = a_1x_1 + \ldots a_{m-1}x_{m-1} + ax_m$. Dann ist $1 - a$ eine Einheit und es gilt

$$x_m = \frac{1}{1-a}(a_1x_1 + \cdots + a_{m-1}x_{m-1}) \in Ax_1 + \cdots + Ax_{m-1}$$

Es folgt $M = Ax_1 + \cdots + Ax_{m-1}$. Das ist ein Widerspruch zur Minimalität von m.

Definition. Ein Ring A heißt lokal, wenn eine der folgenden äquivalenten Eigenschaften erfüllt ist

(1) A enthält enthält genau ein maximales Ideal.
(2) Die Nichteinheiten bilden ein Ideal.

Bemerkung. In einem lokalen Ring A ist das Jakobsonradikal das einzige maximale Ideal $\mathfrak{m}$ von A. Es ist auch die Menge der Nichteinheiten von A. Der Resklassenring $A/\mathfrak{m}$ ist dann ein Körper, der Restklassenkörper von A. Ein Ring A heißt semilokal, wenn er nur endlich viele maximale Ideale besitzt. Das Jakobsonradikal ist dann der Durchschnitt dieser endlich vielen maximalen Ideale.

II Nöthersche Moduln und Ringe.

Der Hilbertsche Basissatz.

Lemma. *Sei M ein A-Modul. Folgende Aussagen sind äquivalent:*

(1) *Jeder Untermodul N von M ist endlich erzeugt; d.h. es gibt endlich viele Elemente $n_1, \ldots, n_r \in N$ mit $N = An_1 + \cdots + An_r$.*

(2) *Jede aufsteigende Kette*

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$$

von Untermoduln N_ν von M ist stationär; d.h. es gibt einen Index n, so daß gilt $N_n = N_{n+1} = \ldots$.

(3) *jede nicht leere Familie $\mathcal{F}$ von Untermoduln von M enthält mindestens ein maximales Element N; d.h. Jeder Modul $P \in \mathcal{F}$, der N enthält stimmt mit N überein.*

Bemerkung. In abgekürzter Sprechweise nennen wir einen endlich erzeugten A-Modul auch einen endlichen A-Modul.

Definition.

(1) Ein A-Modul M heißt nöthersch, wenn er eine der äquivalenten Bedingungen des vorhergehenden Lemmas erfüllt.

(2) Der Ring A heißt nötherscher Ring, wenn A als A-Modul nöthersch ist. Das bedeutet also, daß jedes Ideal von A endlich erzeugt ist.

Beispiele für nöthersche Ringe. Ein Körper ist nöthersch. Alle Hauptidealringe sind nöthersch. Insbesondere ist der Ring $\mathbb{Z}$ der ganzen Zahlen nöthersch.

Lemma. *Gegeben sei eine kurze exakte Folge*

$$0 \longrightarrow N \xrightarrow{\ i\ } M \xrightarrow{\ q\ } P \longrightarrow 0$$

von A-Moduln. Der Modul M ist genau dann nöthersch, wenn die beiden Moduln N, P nöthersch sind.

Beweis. Seien der Untermodul N von M und der Faktormodul $P \cong M/N$ nöthersch. Sei U ein Untermodul von M. Es gibt dann endlich viele Elemente $x_1, \ldots, x_r \in i^{-1}(U) = V \subseteq N$, die V erzeugen, und es gibt endlich viele Elemente $y_1, \ldots, y_s \in U$ deren Bilder $q(y_\nu) \in P$ den Untermodul $q(U) \subseteq P$ von P erzeugen. Es folgt:

$$U = Ai(x_1) + \cdots + Ai(x_r) + Ay_1 + \cdots + Ay_s$$

Insbesondere ist ein Faktorring eines nötherschen Ringes nöthersch. Aus dem Lemma folgt, daß die direkte Summe von zwei nötherschen Moduln, allgemeiner von endlich vielen nötherschen Moduln nöthersch ist.

Folgerung. *Ein Ring A ist genau dann nöthersch, wenn alle endlich erzeugten A-Moduln nöthersch sind.*

Beweis. Sei A nötherscher Ring. Dann ist A nötherscher A-Modul; damit sind alle endlichen freien Moduln, damit auch alle Faktormoduln endlicher freier A-Moduln, also alle endlich erzeugten A-Moduln nöthersch.

Theorem. Der Hilbertsche Basissatz. *Sei A ein nötherscher Ring. Dann ist der Polynomring $B = A[T]$ einer Variablen über A nöthersch.*

Durch vollständige Induktion erhält man daraus:

Folgerung. *Der Polynomring $A[T_1, \ldots, T_n]$ in endlich vielen Variablen über einem nötherschen Ring A, allgemeiner jeder endlich erzeugte Ring über einem nötherschen Ring A ist nöthersch.*

Beweis des Hilbertschen Basissatzes. Sei $P \in A[T]$ ein nicht verschwindendes Polynom.

$$P = a_0 + a_1 T + \cdots + a_n T^n \ , \ a_n \neq 0$$

Dann ist $deg(P) = n$ der Grad von P und a_n der führende Koeffizient von P. Sei $U \subseteq A[T]$ ein von Null verschiedenes Ideal des Polynomringes B. Sei

$$\mathfrak{a} = \{0\} \cup \{a \in A | \exists P = a_0 + \cdots + a_{n-1} T^{n-1} + a T^n \in U\}$$

die Menge der führenden Koeffizienten von Polynomen aus U. Dann ist $\mathfrak{a}$ ein nicht verschwindendes Ideal von A. Weil A nöthersch ist gibt es endlich viele Polynome

$$P_\nu = \cdots + \alpha_\nu T^{n_\nu} \in U \quad 1 \leq \nu \leq m$$

mit führenden Koeffizienten α_ν so daß gilt

$$\mathfrak{a} = A\alpha_1 + \cdots + A\alpha_m$$

Sei n das Maximum der Grade $n_1, \ldots, n_m$. Sei P ein Polynom aus U mit einem Grad $deg(P) \geq n$. Man sieht leicht, daß es dann Polynome $q_1, \ldots, q_m \in B$ gibt, mit $deg(P - \sum_{\nu=1}^{m} q_\nu P_\nu) < deg(P)$ Durch Induktion folgert man

Lemma. *Zu jedem Polynom $P \in U$ gibt es ein Polynom $Q = q_1 P_1 + \cdots + q_m P_m \in U$ mit $deg(P - Q) \leq n - 1$.*

$B = A[T]$ kann als A-Modul aufgefaßt werden. Die Menge $B_n = A + AT + \cdots + AT^{n-1}$ der Polynome vom Grad höchstens $n-1$ ist ein endlicher freier Untermodul des A-Moduls B. $V = U \cap B_m$ ist ein A-Untermodul von B_m. Da A nöthersch ist, gibt es endlich viele Elemente $f_1, \ldots, f_r \in V \subseteq U$, die den A-modul V erzeugen: $V = Af_1 + \cdots + Af_r$. Wegen des vorhergehenden Lemmas gilt

$$\begin{aligned} U = BP_1 + \cdots + BP_m + V &= BP_1 + \cdots + BP_m + Af_1 + \cdots + Af_r \\ &= BP_1 + \cdots + BP_m + Bf_1 + \cdots + Bf_r \end{aligned}$$

U ist also ein endlicher B-Modul $\square$

III Der Hilbertsche Nullstellensatz.

Theorem. Algebraische Fassung des Hilbertschen Nullstelensatzes. *Gegeben sei eine Körpererweiterung $k \subseteq L$. L sei ringendlich erzeugt über k :*

$$L = k[t_1, \ldots, t_n]$$

Dann ist L eine endliche Körpererweiterung von k.

Zum Beweis dieses Satzes benötigen wir einige Hilfssätze.

Definition. Gegeben sei ein Ring A und eine A-Algebra– d.h. ein Ringhomomorphismus–

$$A \longrightarrow B$$

Dann ist B auf natürliche Weise ein A-Modul. Ein Element $b \in B$ heißt ganz über A, wenn es ein Polynom $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in A[x]$ mit führendem Koeffizienten 1 gibt, mit

$$P(b) = b^n + a_1 b^{n-1} + \cdots + a_n = 0$$

Lemma. *Gegeben sei eine A-Algebra $A \longrightarrow B = A[t_1, \ldots, t_n]$. Die Elemente t_ν seien ganz über A. Dann ist B ein endlicher A-Modul.*

Beweis. Es gibt n Polynome

$$P_1(x) = x^{m_1} + \ldots, \ldots, P_n(x) = x^{m_n} + \cdots \in A[x]$$

mit

$$P_1(t_1) = \cdots = P_n(t_n) = 0$$

Deshalb lassen sich die Potenzen $t_\nu^{m_\nu}$ von t_ν, damit auch alle höheren Potenzen, als Linearkombination der Potenzen $1, t_\nu, \ldots, t_\nu^{m_\nu - 1}$ mit Koeffizienten in A darstellen. Sei r das Maximum der Grade dieser Polynome. Dann wird B als A-Modul durch die endlich vielen Monome

$$t_1^{\nu_1} t_2^{\nu_2} \ldots t_n^{\nu_n} \quad , \quad \nu_i \leq r - 1$$

erzeugt.

.

Lemma. *Gegeben sei ein injektiver Homomorphismus $A \hookrightarrow L$ eines nötherschen Ringes A in einen Körper L. L sei ein endlicher A-Modul. Dann ist auch A ein Körper.*

Beweis. Der Einfachheit halber sei $A \subseteq L$. Sei $a \neq 0$ ein Element von A. Dann gibt es ein Element $b = \frac{1}{a}$ in L. Man betrachte die aufsteigende Kette der A-Moduln Ab^ν. Da L ein nötherscher A-Modul ist, ist diese Kette stationär; es gibt also eine natürliche Zahl n mit

$$A\frac{1}{a^n} = A\frac{1}{a^{n+1}}$$

Es gibt deshalb ein Element $c \in A$ mit $\frac{1}{a^{n+1}} = \frac{c}{a^n}$. Es folgt

$$\frac{1}{a} = c \in A$$

Lemma. *Der Polynomring $k[t]$ über dem Grundkörper k in der Variablen t enthält unendlich viele wesentlich verschiedene Primelemente. Wesenlich verschieden heißen zwei Polynome, wenn sie sich nicht nur um einen konstanten Faktor unterscheiden.*

Beweis. Ist k ein endlicher Körper, so gibt es Körperweiterungen von k mit beliebig großem Grad über k. Diese sind alle separabel. Nach dem Satz vom primitiven Element gibt es also irreduzible Polynome in $k[t]$ mit beliebig großem Grad. Sei k unendlich. Die unendlich vielen irreduziblen Polynome $t - c \quad c \in k$ sind dann wesentlich verschieden. Man kann auch nach Euklid schließen: Wenn es nur endlich viele wesentlich verschiedene Primelemente gibt, sei Q das Produkt dieser Primelemente. Dann muß aber $1 + Q$ einen von diesen verschiedenen weiteren Primteiler besitzen. Widerspruch!

Beweis des Hilbertschen Nullstellensatzes. Ist L algebraisch über k, so ist L eine endliche Körpererweiterung von k. Sei der Transzendenzgrad von L über k größer als 0. Wir wollen einen Widerspruch herleiten. Nachdem wir k gegebenenfalls durch einen geeigneten Zwischenkörper ersetzt haben, können wir annehmen, daß der Transzendenzgrad 1 ist. Wir wählen ein über k transzendentes Element $x \in L$. Die Elemente $t_1, \ldots, t_n$ sind dann algebraisch über $k(x)$, genügen also geeigneten algebraischen Gleichungen über dem Körper $k(x)$. Wir wählen einen geeigneten Hauptnener $q(x)$ und können dann annehmen, daß die Elemente t_ν sogar Gleichungen mit Koeffizienten in $A = k[x, \frac{1}{q(x)}]$ und führenden Koeffizienten 1 genügen, also ganz über A sind. Dann ist $L = k[t_1, \ldots, t_n] = A[t_1, \ldots, t_n]$ endlicher Modul über dem nötherschen Ring A. Also ist $A = k[x, \frac{1}{q(x)}]$ ein Körper. Sei $p(x) \in k[x]$ ein Primpolynom. Dann ist $\frac{1}{p(x)}$ in $A = k[x, \frac{1}{q(x)}]$ enthalten. Es folgt, daß $p(x)$ eine Potenz von $q(x)$ teilt. Da der Polynomring $k[x]$ ein Ring mit eindeutiger Primfaktorzerlegung ist, teilt $p(x)$ das Polynom $q(x)$, ist also bis auf einen konstanten Faktor einer der endlich vielen Primfaktoren von $q(x)$. Wir haben damit einen Widerspruch erhalten, weil $k[x]$ unendlich viele wesentlich verschiedene Primpolynome enthält. $\square$

Sei k ein Körper und K ein algebraisch abgeschlossener Oberkörper. Sei $\mathfrak{a} \subseteq A = k[x_1, \ldots, x_n]$ ein von A verschiedenes Ideal im Polynomring A über dem Grundkörper k. Dann gibt es ein maximales Ideal $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq A$. $L = A/\mathfrak{m}$ ist ein ringendlich erzeugter Oberkörper von k. Wie wir bwiesen haben ist $[L : k] \lneq \infty$. Weil K algebraisch abgeschlossen ist, gibt es eine Injektion $L \hookrightarrow K$, die die Identität auf k ist. Deshalb gibt es einen Homomorphismus über k, d.h. einen Homomorphismus, der die Identität ist auf k

$$\phi : A \underset{k}{\longrightarrow} K$$

mit dem Kern $\mathfrak{m}$. Insbesondere ist $\phi(\mathfrak{a}) = 0$. Oder äquivalent dazu besitzt das Ideal $\mathfrak{a}$ die gemeinsame Nullstelle $(\phi(x_1), \ldots, \phi(x_n)) \in K^n$.

Folgerung. *Ein Ideal $\mathfrak{a}$ aus dem Polynomring $k[x_1, \ldots, x_n]$ hat genau dann eine Nullstelle im algebraisch abgeschlossenen Oberkörper K von k, wenn das Ideal nicht das Einselement enthält.*

Sei $\mathfrak{a} \subseteq A$ ein Ideal und

$$\mathfrak{r}(\mathfrak{a}) = \{f \in A | \exists s \text{ mit } f^s \in \mathfrak{a}\}$$

das *Radikalideal* von $\mathfrak{a}$. Man sieht leicht, daß $\mathfrak{r}(\mathfrak{a})$ ein Ideal ist. Sei $a = (a_1, \ldots, a_n) \in K^n$ eine Nullstelle von $\mathfrak{a}$. Dann ist a auch eine Nullstelle von $\mathfrak{r}(\mathfrak{a})$.

Satz. *Sei $\mathfrak{a} \subseteq A = k[x_1, \ldots, x_n]$ ein Ideal im Polynomring A. Sei $M \subseteq K^n$ die Gesamtheit aller Nullstellen von $\mathfrak{a}$ in K^n. Genau dann verschwindet ein Polynom $q(x) \in A$ auf allen Punkten von M, wenn $q(x)$ im Radikalideal von $\mathfrak{a}$ enthalten ist.*

Beweis. Sei S eine weitere Variable und B der Polynomring $A[S] = k[x_1, \ldots, x_n, S]$. Wir betrachten in B das von $\mathfrak{a}$ und dem Element $q(x)S - 1$ erzeugte Ideal $\mathfrak{b}$. Sei $b = (a_1, \ldots, a_n, u) \in K^{n+1}$ eine Nullstelle von $\mathfrak{b}$. Dann ist $a = (a_1, \ldots, a_n) \in K^n$ eine Nullstelle von $\mathfrak{a}$ und es gilt $0 = q(a)u - 1 = -1$. Das ist ein Widerspruch. $\mathfrak{b}$ besitzt also keine Nullstelle. Damit ist ± 1 in $\mathfrak{b}$ enthalten. Es gilt also für geeignete Polynome $a_\nu(x) \in \mathfrak{a}$, $b_\nu(x) \in A$

$$\sum_{\nu=0}^{m} a_\nu(x) S^\nu + \sum_{\nu=0}^{m} b_\nu(x)(q(x)S - 1)S^\nu = -1$$

Durch Vergleich der Koeffizienten der Potenzen von S erhält man

$$\begin{aligned} a_0(x) - b_0(x) &= -1 \\ a_1(x) - b_1(x) + b_0(x)q(x) &= 0 \\ &\vdots \\ a_m(x) - b_m(x) + b_{m-1}(x)q(x) &= 0 \\ b_m(x)q(x) &= 0 \end{aligned}$$

Modulo $\mathfrak{a}$ gilt also

$$\begin{aligned} b_0(x) &\equiv 1 \quad (\mathfrak{a}) \\ b_1(x) &\equiv b_0(x)q(x) \quad (\mathfrak{a}) \\ &\vdots \\ b_m(x) &\equiv b_{m-1}(x)q(x) \quad (\mathfrak{a}) \\ b_m(x)q(x) &\equiv 0 \quad (\mathfrak{a}) \end{aligned}$$

Daraus erhält man

$$b_m(x) \equiv q(x)^m \quad (\mathfrak{a})$$

und

$$q(x)^{m+1} \equiv 0 \quad (\mathfrak{a})$$

Also ist $q(x)$ im Radikal des Ideals $\mathfrak{a}$ enthalten. $\square$

Folgerung. *Sei $B = k[t_1, \ldots, t_n]$ ein endlich erzeugter Ring über dem Grundkörper k. Dann ist das Nilradikal*

$$\{f \in B | \exists s \text{ mit } f^s = 0\}$$

von A das Jakobsonradikal von A, also der Durchschnitt der maximalen Ideale von A.

IV Ganze Ringerweiterungen. Die Sätze von Cohen-Seidenberg.

Gegeben sei eine Ringerweiterung $A \subseteq B$, allgemeiner ein Ringhomomorphismus $A \xrightarrow{j} B$. Wir fassen auch im allgemeineren Fall B als A-Modul auf:

$$ab = j(a)b \ \ \forall a \in A, b \in B.$$

Wir sagen auch, daß B eine A-Algebra ist.

Definition. Ein Element $b \in B$ heißt ganz über A, wenn es ein "ganzes " Polynom

$$P(T) = a_0 + a_1 T + \ldots a_{n-1} T^{n-1} + T^n \in A[T]$$

vom Grad $n \geq 1$ gibt mit

$$P(b) = a_0 + a_1 b + \ldots a_{n-1} b^{n-1} + b^n = 0.$$

Äquivalent dazu ist: Die A-Algebra $A[b]$ ist ein endlicher A-Modul. Der Ring B heißt ganz über A oder ganze Erweiterung von A, wenn alle Elemente von B ganz über A sind. Offenbar ist b ganz über A genau dann, wenn b ganz über dem Bild von A in B ist.

Offensichtlich ist

Lemma. *Seien $b_1, \ldots, b_n \in B$ Elemente von B, die ganz sind über A. Dann ist der von diesen Elementen über A erzeugte Unterring $A[b_1, \ldots, b_n] \subseteq B$ ein endlicher A-Modul .*

.

Bemerkung. Es gilt auch die Umkehrung dises Lemmas. Das ist offensichtlich, wenn A ein nötherscher Ring ist. Der allgemeine Fall wird mit weiter unten angegebenen Techniken auf den Fall eines endlich erzeugten Ringes A über $\mathbb{Z}$ also eines nötherschen Ringes zurückgeführt.

Sei A ein nötherscher Ring. Es gilt dann sogar

Lemma. *Das Element $b \in B$ ist genau dann ganz über A, wenn $A[b]$ in einem endlichen A-Untermodul von B enthalten ist.*

Folgerung. *Seien $b, c \in B$ über A ganze Elemente. Dann sind auch die Elemente $b + c, bc$ ganz über A. Gegeben sei außerdem eine B-Algebra $B \longrightarrow C$. B sei ganz über A und $c \in C$ ein über B ganzes Element. Dann ist c auch ganz über A.*

Zum Beweis des zweiten Teils der Folgerung. c ist Nullstelle eines ganzen Polynoms aus $B[T]$. Seien $b_1, \ldots, b_n \in B$ die Koeffizienten dieses Polynoms. Dann ist $D = A[b_1, \ldots, b_n] \subseteq B$ ein endlicher A-Modul und c ganz über D, deshalb $D[c]$ ein endlicher D-Modul, damit auch ein endlicher A-Modul und $A[c]$ in diesem endlichen A-Modul enthalten.

Bemerkung. Diese Folgerung gilt auch, wenn A nicht nöthersch ist.
Technik: Reduktion auf den nötherschen Fall mit Hilfe folgender Überlegung: Betrachte

$$\mathbb{Z} \longrightarrow A \longrightarrow B$$

Ein Element $b \in B$ ist genau dann ganz über A, wenn es endlich viele Elemente $a_1, \ldots, a_n \in A$ gibt, so daß b ganz über dem nötherschen Ring $\mathbb{Z}[a_1, \ldots, a_n]$ ist!

Die Sätze von Cohen-Seidenberg.

Gegeben sei eine ganze Ringerweiterung

$$A \subseteq B \text{ ganz über } A$$

Satz "Going up ". *Sei $\mathfrak{p}$ ein Primideal von A. Dann gibt es ein Primideal $\mathfrak{P}$ von B mit $\mathfrak{P} \cap A = \mathfrak{p}$. Sei $\tilde{\mathfrak{P}} \subseteq \mathfrak{P}$ ein weiteres Primideal mit $\tilde{\mathfrak{P}} \cap A = \mathfrak{p}$. Dann ist $\tilde{\mathfrak{P}} = \mathfrak{P}$.*

Bemerkung. Genau dann ist $\mathfrak{p}$ maximales Ideal , wenn $\mathfrak{P}$ maximal ist.

Zur Bemerkung. Sei $\mathfrak{p}$ maximal. Dann ist $k = A/\mathfrak{p}$ ein Körper und $K = B/\mathfrak{P}$ ein Integritätsbereich, der ganz über k ist. Sei α ein von Null verschiedenes Element von K. $V = k[\alpha]$ ist ein endlichdimensionaler Vektorraum über k und die Multiplikation mit α

$$V \longrightarrow V$$

eine injektive lineare Abbildung, damit auch surjektiv also ein Isomorphismus. Also besitzt α ein inverses Element α^{-1} in K. K ist ein Körper und $\mathfrak{P}$ maximales Ideal.

Durch Induktion nach der Anzahl der Primideale einer Kette von Primidealen folgert man leicht aus dem Satz

Folgerung. *Sei*

$$\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subseteq A$$

eine Kette von Primidealen von A. Dann gibt es eine Kette von Primidealen von B

$$\mathfrak{P}_1 \subsetneq \cdots \subseteq \mathfrak{P}_n \subsetneq A$$

mit

$$\mathfrak{P}_\nu \cap A = \mathfrak{p}_\nu.$$

Beweis des Satzes. Sei S das Komplement des Primideals $\mathfrak{p}$ in A. Dann ist S eine multiplikative Menge von B, die 1 enthält. Wähle ein maximales Element $\mathfrak{P}$ in der nicht leeren Menge der Ideale von B, die mit S einen leeren Durchschnitt haben. Nach allgemeinen Sätzen ist $\mathfrak{P}$ ein Primideal von B mit

$$\mathfrak{P} \cap A \subseteq \mathfrak{p}.$$

Angenommen, es sei

$$\mathfrak{P} \cap A \neq \mathfrak{p}.$$

Wir wollen einen Widerspruch herleiten. Wir ersetzen $A \subseteq B$ durch $A/(\mathfrak{P} \cap A) \subseteq B/\mathfrak{P}$ und $\mathfrak{p}$ durch $\mathfrak{p}/(\mathfrak{P} \cap A)$. Wir können dann annehmen, das A, B Integritätsbereiche sind und daß $\mathfrak{p} \neq 0$. Für ein Ideal $\mathfrak{a} \neq 0$ von B ist dann $\mathfrak{a} \cap A \not\subseteq \mathfrak{p}$. Sei K der Quotientenkörper von B. Sei α ein von Null verschiedenes Element von $\mathfrak{p}$. Dann gibt es nach Voraussetzung ein Element $s \in A \setminus \mathfrak{p}$ mit $s \in B\alpha \cap A$. Es gibt dann ein Element $\beta \in B$ mit $\beta\alpha = s$. $\beta = \frac{s}{\alpha} \in K$ ist ganz über A. Es gibt dann Elemente $a_\nu \in A$ und eine natürliche Zahl $n \geq 1$ mit

$$(\frac{s}{\alpha})^n = a_0 + \cdots + a_{n-1}(\frac{s}{\alpha})^{n-1}.$$

Man multipliziert diese Gleichung mit α^n und erhält

$$s^n = a_0\alpha^n + a_1 s\alpha^{n-1} + \cdots + a_{n-1}s^{n-1}\alpha \in A\alpha \subseteq \mathfrak{p}.$$

Da $\mathfrak{p}$ ein Primideal ist, folgt $s \in \mathfrak{p}$. Das ist ein Widerspruch.

Die zweite Behauptung: Nach Ausdivision von $\tilde{\mathfrak{P}}$ kann man annehmen, daß A, B Integritätsbereiche sind und daß $\mathfrak{p} = 0$, $\tilde{\mathfrak{P}} = 0$. Sei $0 \neq \alpha \in \mathfrak{P}$. α genügt einer ganzen Gleichung aus $A[T]$. Wähle eine solche Gleichung niedrigsten Grades:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0 \ , \ a_\nu \in A.$$

Da B ein Integritätsbereich ist, gilt wegen der Minimalität des Grades n: $a_0 \neq 0$. a_0 ist aber ein Element aus $\mathfrak{P} \cap A$. Widerspruch. □

Definition. Ein Integritätsbereich A heißt ganz abgeschlossen, wenn jedes über A ganze Element des Quotientenkörpers von A in A enthalten ist.

Bemerkung. Sei A ein Integritätsbereich und B die Gesamtheit der über A ganzen Elemente eines Erweiterungskörpers des Quotientenkörpers L von A. Dann ist B ein ganz abgeschlossener Integritätsbereich, der ganze Abschluß von A in L. Ist L algebraisch über dem Quotientenkörper von A, so ist L der Quotientenkörper von B.

Satz "Going down". *Sei A ein ganz abgeschlossener Integritätsbereich, B ein Integritätsbereich und*

$$B \supseteq A$$

eine ganze Ringerweiterung. Sei $\mathfrak{p}$ ein Primideal von A und $\mathfrak{P}$ ein Primideal von B mit $\mathfrak{p} \subseteq \mathfrak{P} \cap A$. Dann gibt es ein Primideal $\tilde{\mathfrak{P}} \subseteq \mathfrak{P}$ von B mit

$$\tilde{\mathfrak{P}} \cap A = \mathfrak{p}.$$

Beweis. Wir wollen der Einfachheit annehmen, daß der Quotientenkörper von B endlichen Grad über dem Quotientenkörper K von A besitzt. Wir können B durch den ganzen Abschluß von B in der normalen Hülle L des Quotientenkörpers von B über K ersetzen. Sei p die Charakteristik von K, wenn diese positiv ist, bzw. $p = 1$, wenn diese Charakteristik Null ist. Sei G die Galoisgruppe von L über K.

Da $[L:K] < \infty$ ist diese Gruppe endlich. Wähle nach "Going up" ein Primideal $\mathfrak{Q}$ von B mit $\mathfrak{Q} \cap A = \mathfrak{p}$. Dann gilt für alle Elemente $\sigma \in G$

$$\sigma(B) = B$$
$$\sigma(\mathfrak{Q}) \cap A = \mathfrak{p}$$

Für ein Element $a \in \mathfrak{Q}$ und eine genügend große natürliche Zahl r gilt dann

$$\Big(\prod_{\sigma \in G} \sigma(a)\Big)^{p^r} \in K \cap \mathfrak{Q}$$

Weil A ganz abgeschlossen ist, liegt $(\prod_{\sigma\in G}\sigma(a))^{p^r}$ bereits in A, damit in $\mathfrak{p} = \mathfrak{Q} \cap A \subseteq \mathfrak{P}$. Da $\mathfrak{P}$ ein Primideal ist, gibt es ein Element $\sigma \in G$ mit $\sigma(a) \in \mathfrak{P}$. Es folgt

$$\mathfrak{Q} \subseteq \bigcup_{\sigma \in G} \sigma(\mathfrak{P}).$$

Dann ist aber $\mathfrak{Q}$ bereits in einem Ideal $\sigma_0(\mathfrak{P})$ dieser Vereinigung enthalten. Es folgt

$$\sigma_0^{-1}(\mathfrak{Q}) \subseteq \mathfrak{P}$$
$$\sigma_0^{-1}(\mathfrak{Q}) \cap A = \mathfrak{p}$$

$\tilde{\mathfrak{P}} = \sigma_0^{-1}(\mathfrak{Q})$ ist das gesuchte Ideal.

Betrachte im Ring A Ketten von Primidealen

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m.$$

Das Supremum der Längen m aller dieser Ketten heißt die *Krulldimension* des Ringes A. Sei $\mathfrak{p}$ ein Primideal von A. Das Supremum der Längen m aller Ketten von Primidealen

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m \subseteq \mathfrak{p}$$

die in $\mathfrak{p}$ enthalten sind heißt die *Höhe* des Primideals $\mathfrak{p}$.

Folgerung. *Sei eine ganze Ringerweiterung $A \subseteq B$ gegeben. Dann stimmen die Krulldimensionen von A und B überein. Seien zusätzlich A, B Integritätsbereiche, sei A ganz abgeschlossen und sei $\mathfrak{P}$ ein Primideal von B. Dann sind die Höhen von $\mathfrak{P}$ und $\mathfrak{P} \cap A$ gleich.*

V Der noethersche Normalisierungssatz.

Im folgenden sei

$$A = k[T_1, \ldots, T_n]$$

ein Polynomring über dem Körper k in den Variablen $T_1, \ldots, T_n$. Wir betrachten lineare Variablentransformationen

$$T_i' = \sum_{j=1}^{n} c_{ij} T_j \ , \ i = 1, \ldots, n \ , \quad \det((c_{ij})) \neq 0 \ , \ c_{ij} \in k$$

Dann ist

$$A = k[T_1', \ldots, T_n']$$

Polynomring über k in den Variablen $T_1', \ldots, T_n'$.

Lemma. *Sei $P(T) = P(T_1, \ldots, T_n) \in A$ ein nicht konstantes Polynom. Enthält k unendlich viele Elemente, so gibt es eine lineare Variablensubstitution*

$$\begin{aligned} T_n' &= T_n \\ T_{n-1}' &= T_{n-1} - \alpha_{n-1} T_n \\ &\vdots \\ T_1' &= T_1 - \alpha_1 T_n \\ \alpha_\nu &\in k \end{aligned}$$

eine ganze Zahl $m > 0$ und ein Element $c \neq 0$, so daß gilt

$$P(T) = Q(T') = c {T_n'}^m + \sum_{\nu=0}^{m-1} q_\nu(T_1', \ldots, T_{n-1}') {T_n'}^\nu$$

Dann ist $c^{-1}Q(T')$ ein ganzes Polynom in der Variablen T_n' über dem Polynomring

$$k[T_1', \ldots, T_{n-1}']$$

Bemerkung. Ist der Körper k endlich mit der positiven Charakteristik p, so gilt das Lemma noch, wenn man die linearen Transformationen durch geeignete nichtlineare vom Typ

$$\begin{aligned} T_n' &= T_n \\ T_\nu' &= T_\nu - T_n^{p^{r_\nu}} \ , \ 1 \leq \nu \leq n-1 \end{aligned}$$

ersetzt.

Beweis des Lemmas. Der Totalgrad eines Monoms $aT^\nu = aT_1^{\nu_1} \ldots T_n^{\nu_n}$ ist $\nu_1 + \cdots + \nu_n$. Ein von Null verschiedenes Polynom heißt homogen vom Grad d, wenn alle in

diesem Polynom auftretenden Monome den Totalgrad d haben. Ein von Null verschiedenes Polynom läßt sich eindeutig darstellen als Summe homogener Polynome verschiedenen Grades, der homogenen Komponenten. Ein homogenes Polynom vom Grad d wird durch eine lineare Transformation wieder in ein homogenes Polynom vom Grad d überführt. Wir können das gegebene Polynom durch seine homogene Komponente höchsten Grades ersetzen und deshalb ohne Beschränkung der Allgemeinheit annehmen, daß das Polynom P homogen vom Grad m ist. Es gilt

$$\begin{aligned} T_n &= T'_n \\ T_{n-1} &= T'_{n-1} + \alpha_{n-1} T'_n \\ &\vdots \\ T_1 &= T'_1 + \alpha_1 T'_n \\ P(T) = Q(T') &= P(\alpha_1, \ldots, \alpha_{n-1}, 1) {T'_n}^m + \text{ Monome vom Grad } < m \text{ in } T'_n \end{aligned}$$

Weil $P \neq 0$ homogen ist, ist das Polynom $P(T_1, \ldots, T_{n-1}, 1)$ nicht identisch Null. Weil k unendlich ist gibt es deshalb Elemente $\alpha_1, \ldots, \alpha_{n-1} \in k$, so daß $c = P(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$. $\square$

Sei $\mathfrak{a} \neq A$ ein Ideal des Polynomringes $A = k[T_1, \ldots, T_n]$. Wenn $\mathfrak{a}$ nicht verschwindet, wähle ein Polynom $P \neq 0$ aus $\mathfrak{a}$; es ist dann nicht konstant. Nach einer Vatriablentransformation und Multiplikation mit einer Konstanten kann man annehmen, daß P ein ganzes Polynom über dem Polynomring $k[T_1, \ldots, T_{n-1}]$ ist. Dann ist $A/\mathfrak{a}$ ein endlicher $k[T_1, \ldots, T_{n-1}]$-Modul. Die gleiche Konstruktion kann mit $\mathfrak{a} \cap k[T_1, \ldots, T_{n-1}]$ durchgeführt werden. Durch vollständige Induktion erhält man

Satz Nötherscher Normalisierungssatz. *Sei $\mathfrak{a} \neq A$ ein Ideal des Polynomringes $A = k[T_1, \ldots, T_n]$. Nach einer– im Falle eines unendlichen Körpers k linearen, sonst nichtlinearen– Variablentransformation gibt es eine natürliche Zahl $m \leq n$ so daß*

$$k[T_1, \ldots, T_m] \cap \mathfrak{a} = 0$$

ist und so daß $A/\mathfrak{a}$ eine ganze Erweiterung von $k[T_1, \ldots, T_m]$ ist. Dann ist $A/\mathfrak{a}$ sogar ein endlicher $k[T_1, \ldots, T_m]$-Modul.

Anmerkung. Dieser Satz kann mit Hilfe des "Going up"-Satzes von Cohen-Seidenberg geometrisch interpretiert werden. Sei der Grundkörper k der Einfachheit halber algebraisch abgeschlossen. Nach einer Variablensubstitution ist die Nullstellenmenge $X \subseteq k^n$ des Ideals $\mathfrak{a}$ eine endliche verzweigte Überlagerung des m-dimensionalen affinen Raumes k^m. Insbesondere ist die Projektion $X \longrightarrow k^m$ surjektiv; alle Fasern sind endlich. Ist $\mathfrak{a}$ ein Primideal, so ist m der Transzendenzgrad des Quotientenkörpers von $A/\mathfrak{a}$.

Aus dem Lemma kann auch eine andere Form des Nötherscher Normalisierungssatzes mit Hilfe von Induktion gefolgert werden

Satz. *Gegeben sei eine endliche Kette von Idealen in einem über dem Körper k endlich erzeugten Ring $A = k[t_1, \ldots, t_n]$.*

$$\mathfrak{a}_0 \subseteq \cdots \subseteq \mathfrak{a}_r \subsetneq A$$

Dann enthält A einen Polynomring $B = k[T_1, \ldots, T_m]$ über dem A endlicher Modul ist und so daß für natürliche Zahlen $0 \leq \nu_0 \leq \nu_1 \leq \cdots \leq \nu_r \leq m$ gilt

$$\mathfrak{a}_i \cap B = BT_1 + \cdots + BT_{\nu_i} \ , \ 0 \leq i \leq r$$

Sei A ein Integritätsbereich und seien die Ideale $\mathfrak{a}_\nu$ der Kette untereinander verschiedene Primideale. Die Anzahl m der Variablen des Polynomrings B ist in diesem Fall der Transzendenzgrad des Quotientenkörpers von A über dem Grundkörper k. Die Durchschnitte $\mathfrak{a}_\nu \cap B$ sind dann auch paarweise verschieden(siehe "Going up" im Paragraphen *Ganze Ringerweiterungen*) Ein Polynomring über einem Körper hat eindeutige Primfaktorzerlegung und ist deshalb ganz abgeschlossen. Aus dem "Going down" Satz von Cohen-Seidenberg folgt, daß sich die gegebene Primidealkette verfeinern läßt zu einer Primidealkette von A, deren Durchschnitt mit dem Ring B die Kette der Primideale

$$0 \subsetneq BT_1 \subsetneq BT_1 + BT_2 \subsetneq \cdots \subsetneq BT_1 + BT_2 + \cdots + BT_m$$

ist.

Folgerung. *Sei $A = k[t_1, \ldots, t_n]$ ein über dem Grundkörper k ringendlich erzeugter Integritätsbereich Sei m der Transzendenzgrad des Quotientenkörpers von A über k. Dann gilt für die Länge einer Primidealkette von A*

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

die Ungleichung

$$r \leq m$$

Eine solche Kette läßt sich zu einer Kette von Primidealen der Länge m verfeinern. Insbesondere hat jedes maximale Ideal die Höhe m; die Krulldimension von A ist m.

VI Lokalisierung

Nenneraufnahme

Es soll die bekannte Konstruktion des Quotientenkörpers auf Ringe und Moduln sinngemäß übertragen werden.

Vorgegeben sei ein Ring A und eine multiplikative Menge $S \subseteq A$:

$$1 \in S; 0 \notin S; s,t \in S \Rightarrow st \in S$$

Sei M ein A-Modul. Betrachte die Menge aller symbolische Ausdrücke bzw Paare

$$M_S = \{\frac{m}{s}; m \in M, s \in S\}$$

mit folgender Definition der Gleichheit (d.i. eigentlich eine Äquvivalenzrelation)

$$\frac{m}{s} = \frac{n}{t} \Longleftrightarrow \exists r \in S \text{ mit } r(tm - sn) = 0$$

Auf M_S erklärt man auf folgende Weise die Struktur eines A-Moduls:

$$a\frac{m}{s} = \frac{am}{s} \qquad a \in A\ , \frac{m}{s} \in M_S$$
$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st} \qquad \frac{m}{s}, \frac{n}{t} \in M_S$$

Die Definition dieser Operationen ist verträglich mit der Gleichheit, d.h. ist unabhängig von der Wahl der Repräsentanten bei der Äquivalenzrelation. Man rechnet leicht nach, daß M_S mit diesen Operationen ein A-Modul wird. Es gibt einen natürlichen A-Homomorphismus

$$j : M \underset{m \longmapsto \frac{m}{1}}{\longrightarrow} M_S$$

Diese Konstruktion ist durch folgende universelle Abbildungseigenschaft bis auf einen eindeutig bestimmten Isomorphismus eindeutig gekennzeichnet.

Universelle Abbildungseigenschaft. *Sei*

$$f : M \longrightarrow X$$

ein A-Homomorphismus in einen A-Modul X für den für jedes Element $s \in S$ die Multiplikationsabbildung

$$X \xrightarrow{s} X \quad (x \mapsto sx)$$

ein Isomorphismus ist; d.h. daß es zu jedem Element $x \in X$ genau ein Element $y \in X$ gibt mit $sy = x$. Dann gibt es genau einen Homomorphismus

$$M_S \to X$$

so daß folgendes Diagramm kommutativ wird

$$\begin{array}{ccc} M & \to & M_S \\ & \searrow & \downarrow \\ & & X \end{array}$$

Man ordnet nämlich dem Element $\frac{m}{s} \in M_S$ das eindeutig bestimmte Element $y \in X$ zu mit $sy = f(m)$.
Man zeigt, daß A_S sogar eine natürliche Ringstruktur besitzt:

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \quad \frac{a}{s}, \frac{b}{t} \in A_S$$

Offenbar werden die Bilder von Elementen $s \in S$ in A_S zu Einheiten in A_S. Diese Eigenschaft ist wieder in naheliegender Weise *universell* und kennzechnet den Ring A_S. Der Modul M_S ist dann sogar ein A_S-Modul:

$$\frac{a}{s}\frac{m}{t} = \frac{am}{st} \quad \frac{a}{s} \in A_S, \frac{m}{t} \in M_S$$

Mit Hilfe der universellen Abbildungseigenschaft oder auch durch direkte Konstruktion konstruiert man auf natürliche Weise zu jedem Homomorphismus $\phi : M \to N$ von A-Moduln einen eindeutig bestimmten Homomorphismus

$$\phi_S : M_S \longrightarrow N_S$$

von A_S-Moduln, der das Diagramm

$$\begin{array}{ccc} M & \longrightarrow & N \\ \downarrow & & \downarrow \\ M_S & \longrightarrow & N_S \end{array}$$

kommutativ macht. Explizit: $\phi_S(\frac{m}{s}) = \frac{\phi(m)}{s}$.

Bemerkung. *Die Zuordnung*

$$M \mapsto M_S \quad , \quad \phi \mapsto \phi_S$$

ist ein additiver Funktor von der Kategorie der A-Moduln in die Kategorie der A_S-Moduln.

Eigenschaften dieses Funktors

(1)
$$\text{Kern}(M \longrightarrow M_S) = \{m \in M; \exists s \in S \text{ mit } sm = 0\}$$

(2) Der Lokalisierungsfunktor ist exakt:
Sei die Folge
$$N \longrightarrow M \longrightarrow P$$

an der Stelle M exakt. Dann ist die Folge

$$N_S \longrightarrow M_S \longrightarrow P_S$$

an der Stelle M_S exakt. Insbesondere gilt (und ist äquivalent zur Exaktheit):

Ist N ein Untermodul von M, so ist auch N_S ein Untermodul von M_S, d.h. wird auf natürliche Weise als Untermodul identifiziert, und es ist $(M/N)_S = M_S/N_S$.

(3) Betrachte den Homomorphismus

$$j : M \longrightarrow M_S$$

und die folgenden Zuordnungen:
Einem A-Untermodul N von M wird der A_S-Untermodul N_S von M_S zugeordnet. Einem A_S-Untermodul P von M_S wird das Urbild $j^{-1}(P) \subseteq M$ zugeordnet. Das Urbild $j^{-1}(P)$ ist dann S-saturiert,d.h.

$$sx \in j^{-1}(P) \text{ für ein Element } s \in S \text{ und } x \in M \Longrightarrow x \in j^{-1}(P)$$

Diese beiden Zuordnungen stiften eine Bijektion zwischen der Menge aller S-saturierten A-Untermoduln von M und der Menge aller A_S-Untermoduln von M_S. Dazu zeigt man:

$$j^{-1}(N_S) = \{x \in M; \exists s \in S \text{ mit } sx \in N\}$$

(4)
$$M = Am_1 + \cdots + Am_r \Longrightarrow M_S = A_S\frac{m_1}{1} + \cdots + A_S\frac{m_r}{1}$$

Mit Hilfe der dritten Eigenschaft und der aufsteigenden Kettenbedingung zeigt man

Lemma.

(1) *Wenn M noetherscher A-Modul ist, so ist M_S ein noetherscher A_S-Modul.*
(2) *Ist A ein noetherscher Ring ist, so ist auch A_S ein noetherscher Ring.*

Wir untersuchen den Spezialfall $M = A$. Für ein Ideal $\mathfrak{a} \subseteq A$ ist $\mathfrak{a}_S = j(\mathfrak{a})A_S = \mathfrak{a}A_S$

Lemma. *Sei $\mathfrak{p}$ ein Primideal von A. Dann gilt*

$$\mathfrak{p}_S = \begin{cases} \text{Primideal von } A_S & \text{falls } S \cap \mathfrak{p} = \emptyset \\ A_S & \text{sonst} \end{cases}$$

Die Zuordnungen

$$\mathfrak{p} \mapsto \mathfrak{p}_S$$
$$\mathfrak{P} \mapsto j^{-1}(\mathfrak{P})$$

stiften eine eineindeutige Korrespondenz zwischen allen Primidealen $\mathfrak{p}$ *von* A *mit* $S \cap \mathfrak{p} = \emptyset$ *und allen Primidealen* $\mathfrak{P}$ *von* A_S.

Ein Beispiel:
Sei $\mathfrak{p}$ ein Primideal von A und $S = A \setminus \mathfrak{p}$ das Komplement von $\mathfrak{p}$ in A. Wir schreiben dann unvernünftigerweise auch $A_\mathfrak{p}$ statt A_S und für einen A-Modul $M_\mathfrak{p}$ statt M_S. Dann ist $A_\mathfrak{p}$ ein lokaler Ring mit dem maximalen Ideal $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$; d.h., daß $\mathfrak{m}$ das einzige maximale Ideal von $A_\mathfrak{p}$ ist. Der Restklassenkörper $A_\mathfrak{p}/\mathfrak{m}$ ist dann der Quotientenkörper von $A/\mathfrak{p}$. Die Primideale von $A_\mathfrak{p}$ entsprechen eineindeutig den Primidealen von A, die in $\mathfrak{p}$ enthalten sind.

Bemerkung. Man kann leicht zeigen, daß gilt

$$M_S = A_S \otimes_A M$$

Insbesondere ist der Funktor

$$M \longmapsto A_S \otimes_A M$$

exakt, also A_S ein *flacher* A-Modul.

Übungsaufgabe
Sei A ein noetherscher Ring. Die Zuordnung

$$f : M \to N \longmapsto f_S : M_S \to N_S$$

ist ein A-Homomorphismus von A-Moduln

$$Hom_A(M, N) \longrightarrow Hom_{A_S}(M_S, N_S)$$

in den A_S-Modul $Hom_{A_S}(M_S, N_S)$. Dieser Homomorphismus induziert wegen der universellen Eigenschaft der Lokalisierung einen A_S-Homomorphismus

$$Hom_A(M, N)_S \longrightarrow Hom_{A_S}(M_S, N_S)$$

Zeige: Dieser Homomorphismus ist ein Isomorphsmus, falls M ein endlicher A-Modul ist.

Anleitung
Die Behauptung ist "trivial" wenn $M = A$; denn es gilt auf natürliche Weise $Hom_A(A, M) = M$. Wegen der Verträglichkeit additiver Funktoren mit endlichen direkten Summen gilt sie auch für endliche freie A-Moduln. Der allgemeine Fall wird darauf zurückgeführt. Zu dem endlichen Modul M gibt es nämlich eine eakte Folge

$$F \longrightarrow G \longrightarrow M \longrightarrow 0,$$

mit zwei endlichen freien A-Moduln F, G, eine endliche Präsentation von M. Man nutze die Linksexaktheit des Funktors Hom, die Exaktheit des Lokalisierungsfunktors $X \mapsto X_S$ und wende das (eigentlich "triviale") *Fünfer-Lemma* der homologischen Algebra an, veranstalte also eine Diagrammjagd.

VII Primärzerlegung in noetherschen Ringen und Moduln

In diesem Abschnitt soll der Satz von der eindeutigen Primfaktorzerlegung auf beliebige noethersche Ringe übertragen werden. In einem Haupidealring formuliert man diesen Satz auch in der Sprache der Ideale: Jedes von Null verschiedene Ideal kann eindeutig bis auf die Reihenfolge dargestellt werden als Produkt von Potenzen von verschiedenen Primidealen. Dieser Idealzerlegungssatz gilt auch noch in den allgemeineren, in der algebraischen Zahlentheorie bedeutsamen Dedekindringen, in denen im allgemeinen der Satz von der eindeutigen Primfaktorzerlegung von Elementen falsch ist. In diesen Ringen ist das Produkt von Potenzen verschiedener Primideale auch gleich ihrem Durchschnitt. Im allgemeinen Fall eines noetherschen Ringes treten an die Stelle von Primidealpotenzen die sogenannten Primärideale zu Primidealen. Ein Ideal ist dann nur noch Durchschnitt von Primäridealen zu verschiedenen Primidealen; eindeutig bestimmt ist nur noch die Anzahl dieser Primärideale und die Menge der zugehörigen Primideale. Es ist zweckmäßig diese Theorie gleich für Moduln zu entwickeln.

Wir betrachten im folgenden nur noethersche Ringe A und noethersche Moduln M über A.

Zuerst einige Bezeicnungen.

Das *Spektrum* eines Ringes A ist die Menge aller Primideale von A; Schreibweise:

$$Spec(A)$$

Darin enthalten ist das *maximale Spektrum*

$$Specmax(A),$$

die Menge aller maximalen Ideale von A. Für ein Ideal $\mathfrak{a}$ und einen A-Modul M erklärt man die "Nullstellenmenge" des Ideals $\mathfrak{a}$ und den Träger bzw. die Varietät des Moduls M

$$W(\mathfrak{a}) = \{\mathfrak{p} \in Spec(A) | \mathfrak{a} \subseteq \mathfrak{p}\}$$
$$V(M) = \{\mathfrak{p} \in Spec(A) | M_{\mathfrak{p}} \neq 0\}$$

Bemerkung. Man zeigt, daß die Mengen $W(\mathfrak{a})$ die abgeschlossenen Mengen einer Topologie auf $Spec(A)$ sind, der *Zariskitopologie,* die zwar quasikompakt, aber im allgemeinen nicht separiert ist.

Lemma. *Sei*

$$Ann(M) = \{a \in A; aM = 0\}$$

der Annulator des Moduls M und $\mathfrak{q}$ ein weiteres Ideal von A. Es gilt

(1)
$$V(M) = W(Ann(M))$$

Insbesondere ist $V(M)$ in $Spec(A)$ (Zariski-)abgeschlossen.

(2)
$$V(M/\mathfrak{q}M) = V(M) \cap W(\mathfrak{q}M)$$

(3) *Für eine kurze exakte Folge*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

gilt

$$V(M) = V(N) \cup V(P)$$

Beweis. Sei $S \subseteq A$ eine multipliplikative Menge dann gilt für den A_S-Modul M_S

$$Ann(M_S) = Ann(M)_S$$

Also ist $M_S = 0$ genau dann, wenn $Ann(M)_S = A_S$. Also gilt

$$M_S \neq 0 \Leftrightarrow S \cap Ann(M) = \emptyset$$

Sei $S = A \setminus \mathfrak{p}$ für ein Primideal $\mathfrak{p}$ von A.

(1) : $M_{\mathfrak{p}} \neq 0 \Leftrightarrow Ann(M) \subseteq \mathfrak{p}$

(2) : $(M/\mathfrak{q}M)_S \neq 0 \Leftrightarrow M_S \neq 0$, $\mathfrak{q}_S \neq A_S \Leftrightarrow \mathfrak{p} \in V(M) \cap W(\mathfrak{q})$

□

Bemerkung. Sei $A = k[T_1, \ldots, T_n]$ der Polynomring in den Variablen $T_1, \ldots, T_n$ über dem algebraisch abgeschlossenen Körper k. Einem Punkt $(c_1, \ldots, c_n) \in k^n$ ordnet man das von $T_1 - c_1, \ldots, T_n - c_n$ erzeugte maximale Ideal zu und erhält eine Bijektion

$$k^n = Specmax(A).$$

Bei dieser Identifizierung gilt für ein Ideal $\mathfrak{a} \subseteq A$

$$\text{Nullstellenmenge von } \mathfrak{a} = W(\mathfrak{a})$$

Die nichtmaximalen Primideale aus $W(\mathfrak{a})$ entsprechen in einem gewissen (nicht eineindeutigen)Sinne Nullstellen in einem (transzendenten) Erweiterungskörper K von k. Sei $c = (c_1, \ldots, c_n) \in K^n$ eine Nullstelle von $\mathfrak{a}$ in einem solchen Erweiterungskörper K von k und

$$\phi : \underset{P(T) \longmapsto P(c)}{A \longrightarrow K}$$

der Einsetzungshomomorphismus. Dann ist $Kern(\phi)$ das zugeornete Primideal aus $W(\mathfrak{a})$.

Primärzerlegung

Definition und Satz. *Sei M ein (endlicher) von 0 verschiedener Modul über dem (noetherschen) Ring A und N ein Untermodul von M.*

(1) *M heißt koprimär, wenn für ein Element $a \in A$ die Multiplikationsabbildung*

$$M \xrightarrow{a} M$$

entweder injektiv oder nilpotent ist. Das bedeutet: Entweder gilt für jedes $x \in M$: $ax = 0 \Rightarrow x = 0$, oder es gibt zu a eine natürliche Zahl k mit $a^k M = 0$.

(2) *Ist M koprimär, so bildet die Menge der Elemente $a \in A$, für die die Multiplikationsabbildung $M \xrightarrow{a} M$ nilpotent ist, ein Primideal $\mathfrak{p}$. Man nennt dann M auch $\mathfrak{p}$-koprimär.*
(3) *N heißt $\mathfrak{p}$-primär, wenn M/N $\mathfrak{p}$-koprimär ist.*
(4) *ein Ideal $\mathfrak{a} \neq A$ heißt Prmärideal bzw. $\mathfrak{p}$-primäres Ideal, wenn $\mathfrak{a}$ als Untermodul von A $\mathfrak{p}$-primär ist.*

.

Zum Beweis von (2). Die Summe zweier vertauschbarer nilpotenter Abbildungen ist nilpotent. Das Produkt einer nilpotenten Abbildung mit einer damit vertauschbaren Abbildung ist nilpotent. Das Produkt zweier injektiven Abbildungen ist injektiv. □

Lemma.

(1) *Sei M ein $\mathfrak{p}$-koprimärer Modul. Dann ist auch jeder von 0 verschiedene Untermodul $\mathfrak{p}$-koprimär*
(2) *Gegeben sei eine kurze exakte Folge*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

Seien N, P $\mathfrak{p}$-koprimär–zum gleichen Primideal!–, insbesondere nicht Null. Dann ist M $\mathfrak{p}$-koprimär. Insbesondere ist die direkte Summe endlich vieler $\mathfrak{p}$-koprimärer Moduln $\mathfrak{p}$-koprimär.

Folgerung. *Der Durchschnitt zweier zum gleichen Primideal $\mathfrak{p}$- primären Untermoduln ist $\mathfrak{p}$- primär.*

Beweis der Folgerung. Man hat eine natürliche Injektion

$$M/(N_1 \cap N_2) \hookrightarrow M/N_1 \oplus M/N_2$$

□

Fundamentales Lemma. *Der Modul $M \neq 0$ sei nicht koprimär. Dann gibt es zwei von M verschiedene Untermoduln $N \neq 0, P \neq 0$ mit*

$$0 = N \cap P.$$

Unmittelbar daraus ergibt sich

Folgerung. *Sei $N \subsetneq M$ ein nicht primärer Untermodul von M. Dann ist N Durchschnitt zweier von N verschiedenen Untermoduln.*

Beweis des Lemmas. Es gibt nach Voraussetzung ein Ringelement $s \in A$, so daß die Multiplikation mit s

$$\psi : \underset{m \longmapsto sm}{M \longrightarrow M}$$

weder nilpotent noch injektiv ist. Sei

$$K_n = Kern(\psi^n), B_n = Bild(\psi^n)$$

Es gilt

$$0 \neq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq M \quad , \quad K_n \neq M \ \forall n$$
$$M \supseteq B_1 \supseteq B_2 \supseteq B_3 \supseteq \ldots \quad , \quad B_n \neq 0 \ \forall n$$

Da M noethersch ist gibt es eine naturliche Zahl $r \geq 1$ mit

$$K_r = K_{r+1} = K_{r+2} = \ldots$$

Behauptung: $K_r \cap B_r = 0$.
Wähle ein Element $x \in K_r \cap B_r$. Dann ist $s^r x = 0$, und es gibt ein $y \in M$ mit $s^r y = x$. Es folgt, daß $s^{2r} y = 0$. Also ist $y \in K_{2r} = K_r$ und damit $x = s^r y = 0$. Es ist

$$0 \neq K_r \neq M, B_r \neq 0$$

Wäre $B_r = M$, so wäre $K_r \cap B_r = K_r \neq 0$. Also ist auch $B_r \neq M$. $\square$

Sei nun M ein von Null verschiedener A-Modul. Ist der Nulluntermodul nicht primär, so gibt es eine Zerlegung

$$0 = P_1 \cap Q_1, P_1 \subsetneq M, Q_1 \subsetneq M$$

Ist z.B. Q_1 nicht primär, so gibt es eine Zerlegung

$$Q_1 = P_2 \cap Q_2, P_2 \subsetneq M, Q_2 \subsetneq M.$$

$$\vdots$$

Das Verfahren muß wegen der aufsteigenden Kettenbedingung abbrechen! Es gibt also primäre Untermoduln $P_1, \ldots, P_m$ von M so daß gilt

$$0 = P_1 \cap \cdots \cap P_m.$$

In dieser Durchschnitsdarstellung der 0 kann man noch überflüssige Untermoduln P_ν weglassen. Da der Durchschnitt von Primärmoduln zum gleichen Primideal wieder ein Primärmodul ist, kann man alle Primärmoduln zum gleichen Primideal durch ihren Durchschnitt ersetzen und erhält so eine *unverkürzbare* Darstellung des Nulluntermoduls

Satz. *Sei M ein von Null verschiedener endlicher A- Modul. Dann gibt es eine unverkürzbare Darstellung*

$$0 = P_1 \cap \cdots \cap P_m$$

durch Primärmoduln P_ν. Unverkürzbar heißt, daß die Primideale $\mathfrak{p}_\nu$ zu den Primärmoduln P_ν paarweise verschieden sind und daß kein Modul $P\nu$ in der Nulldarstellung weggelassen werden kann. Die Primideale $\mathfrak{p}_\nu$ heißen assoziert zu dieser Darstellung.

Eindeutigkeitssatz. *Gegeben sei eine unverkürzbare Primärzerlegung der* 0 *des Moduls* M *wie im vorhergehenden Existenzsatz; sei* $\mathfrak{M}$ *die Menge der zu dieser Darstellung assozierten Primideale. Dann ist die Primidealmenge* $\mathfrak{M}$ *durch die folgende Charakterisierung unabhängig von der Darstellung gekennzeichnet; auch die Anzahl* m *der auftretenden Primärmoduln ist unabhängig von der Darstellung:* $m = \#(\mathfrak{M})$.

(1)
$$\mathfrak{p} \in \mathfrak{M} \Longrightarrow \exists\, 0 \neq x \in M \text{mit } \mathfrak{p} = \{a \in A, ax = 0\}$$

(2) *Sei* $x \in M$ *ein von* 0 *verschiedenes Element aus* M *für das der Annulator* $\mathfrak{p} = \{a \in A; ax = 0\}$ *ein Primideal ist. Dann gilt*
$$\mathfrak{p} \in \mathfrak{M}$$

Definition. Die durch den Eindeutigkeissatz von der Primärzerlegung unabhängig gekennzeichnete Menge $\mathfrak{M}$ von Primmidealen heißt die Menge der assozierten Ideale des Moduls $M \neq 0$; Schreibweise:
$$\mathfrak{M} = Ass(M)$$

Beweis des Eindeutigkeitssatzes. Sei zuerst M $\mathfrak{p}$-koprimär. Weil $\mathfrak{p}$ und M endlich erzeugt sind, gibt es eine Potenz $\mathfrak{p}^r$ mit $\mathfrak{p}^r M = 0$, $\mathfrak{p}^{r-1} M \neq 0$. Wähle ein von Null verschiedenes Element $x \in \mathfrak{p}^{r-1} M$. Dann ist $\mathfrak{p}x = 0$. Sei $a \in A$ ein Element mit $ax = 0$. Dann ist die Multiplikationsabbildung $M \xrightarrow{a} M$ nicht injektiv, also nilpotent; a ist in $\mathfrak{p}$ enthalten. $\mathfrak{p}$ ist der genaue Annulator von x.
Sei $x \neq 0$ ein Element von M, dessen Annulator $\mathfrak{q} \subseteq A$ ein Primideal ist. Dann ist für jedes $a \in \mathfrak{q}$ die Multiplikation mit a $M \xrightarrow{a} M$ nicht injektiv, also nilpotent; a ist deshalb in $\mathfrak{p}$ enthalten. Es gilt $\mathfrak{q} \subseteq \mathfrak{p}$. Andererseits ist $\mathfrak{p}^r M = 0$ damit $\mathfrak{p}^r x = 0$. Damit ist: $\mathfrak{p}^r \subseteq \mathfrak{q}$. Es folgt: $\mathfrak{p} \subseteq \mathfrak{q}$. Die beiden Primideale sind gleich!

Wir betrachten nun den allgemeinen Fall und eine unverkürzbare Primärzerlegung der 0 in M wie im Existenzsatz. Man faßt die Restklasseabbildungen von M auf die Faktormoduln $M/P\nu$ zusammen und erhält eine natürliche Injektion
$$M \hookrightarrow M/P_1 \times \cdots \times M/P_m = N_1 \times \cdots \times N_m = N.$$

N_ν ist $\mathfrak{p}_\nu$-koprimär. Sei $x \neq 0$ ein Element aus M, allgemeiner aus N. Bei geeigneter Reihenfolge ist $x = (x_1, \ldots, x_s, 0 \ldots, 0)$, $x_\nu \neq 0$. Sei $\mathfrak{q}_\nu$ der Annulator von x_ν. Dann ist der Annulator von x
$$\mathfrak{p} = \bigcap_{\nu=1}^{s} \mathfrak{q}_\nu.$$

Sei $\mathfrak{p}$ ein Primideal. Dann gibt es einen Index $1 \leq \nu_0 \leq s$ mit $\mathfrak{q}_{\nu_0} \subseteq \mathfrak{p}$. Da andererseits $\mathfrak{p} \subseteq \mathfrak{q}_{\nu_0}$, gilt sogar $\mathfrak{p} = \mathfrak{q}_{\nu_0}$. Also ist der Annulator $\mathfrak{q}_{\nu_0}$ des Elementes x_{ν_0} aus dem $\mathfrak{p}_{\nu_0}$-koprimären Modul N_{ν_0}ein Primideal; damit ist, wie bereis bewiesen
$$\mathfrak{p} = \mathfrak{q}_{\nu_0} = \mathfrak{p}_{\nu_0}.$$

Sei nun ein Index k zwischen 1 und m gegeben. Wegen der Unverkürzbarkeit der Primärzerlegung gilt $P = \bigcap_{\nu \neq k} P_\nu \neq 0$, und man hat eine natürliche Injektion $P \hookrightarrow N_k$. Deshalb ist auch P $\mathfrak{p}_k$-koprimär und es gibt, wie bereits bewiesen ein Element $0 \neq x \in P \subseteq M$, dessen Annulator das Primideal $\mathfrak{p}_k$ ist. $\square$

Folgerung. *Zu einem A-Modul M gibt es eine Kette von Untermoduln und Primideale*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{m-1} \subseteq M_m = M$$
$$\mathfrak{p}_1, \ldots, \mathfrak{p}_m \subseteq A$$

so daß gilt

$$M_\nu / M_{\nu-1} \cong A/\mathfrak{p}_\nu \ , \ 1 \leq \nu \leq m$$

Beweis. Wenn $M \neq 0$ ist, gibt es ein Element $x \in M$, dessen Annulator ein Primideal $\mathfrak{p} \in Ass(M)$ ist. Sei $M_1 = Ax \cong A/\mathfrak{p}$. Die gleiche Schlußweise kann auf M/M_1 angewendet werden .... Das Verfahren muß wegen der aufsteigenden Kettenbedingung abbrechen. $\square$

Eine weitere Eigenschaft von $Ass(M)$.
Ein Element a des Ringes A heißt **Nullteiler** des Moduls M, wenn es ein von Null verschiedenes Element $x \in M$ gibt mit $ax = 0$.

Satz. *Die Menge der Nullteiler des Moduls M ist*

$$\bigcup_{\mathfrak{p} \in Ass(M)} \mathfrak{p}$$

Bemerkung. Diese Eigenschaft kann nur zur Charakterisierung der in $Ass(M)$ maximalen Elemente benutzt werden. Es ist aber möglich, daß eine unverkürzbare Primärzerlegung auch *eingebettete Komponenten* enthält, d.h., daß es in $Ass(M)$ zwei Primideale $\mathfrak{p}, \mathfrak{P}$ gibt mit

$$\mathfrak{p} \subseteq \mathfrak{P} \ , \ \mathfrak{p} \neq \mathfrak{P};$$

Beweis. Wir betrachten wie vorher eine Einbettung

$$M \hookrightarrow N_1 \times \cdots \times N_m.$$

Dabei ist N_ν ein $\mathfrak{p}_\nu$ koprimärer Modul und $\mathfrak{p}_\nu \in Ass(M)$. Im vorhergehenden Eindeutigkeitssatz wurde gezeigt, daß alle Primideale aus $Ass(M)$ in der Nullteilermenge von M enthalten sind. Sei umgekehrt $a \neq 0$ ein Nullteiler von M. Dann gibt es ein Element $0 \neq x \in M$ mit $ax = 0$.

$$x = (x_1, \ldots, x_m) \in N_1 \times \cdots \times N_m$$

Sei $x_{\nu_0} \neq 0$. Dann ist auch $ax_{\nu_0} = 0$. Die Multiplikationsabbildung $N_{\nu_0} \xrightarrow{a} N_{\nu_0}$ ist dann nicht injektiv, also nilpotent; also ist $a \in \mathfrak{p}_{\nu_0}$. $\square$

Sei $\mathfrak{a} \subsetneq A$ ein Ideal. Man wendet die bisherigen Resltate auf den Modul $A/\mathfrak{a}$ an und erhält

Proposition. *Das Ideal* $\mathfrak{a}$ *besitzt eine unverkürzbare Darstellung*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

als Durchschnitt von Primäridealen. Die Anzahl m *und die Menge* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *der zugehörigen Primideale hängen nicht von der Wahl dieser Darstellung ab. Es gilt*

$$W(\mathfrak{a}) = \bigcap_{\nu} W(\mathfrak{p}_\nu)$$

Folgerung. *Sei* $\mathfrak{r} = \{a \in A | \exists s \ , \text{ mit } a^s \in \mathfrak{a}\}$ *das Radikal von* $\mathfrak{a}$ *und seien etwa* $\{\mathfrak{p}_\nu \ , \ 1 \leq \nu \leq r\}$ *die Primideale, die in der Menge* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *minimal sind. Dann ist*

$$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$$

die Primärzerlegung von $\mathfrak{r}$.

Zum Beweis. Angenommen diese Darstellung sei verkürzbar. Dann gilt etwa

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{r-1}$$

und damit $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{r-1} \subseteq \mathfrak{p}_r$. Daraus folgt für ein Primideal auf der linken Seite, etwa das erste $\mathfrak{p}_1 \subseteq \mathfrak{p}_r$. Da die Primideale $\mathfrak{p}_\nu \ , \ 1 \leq \nu \leq m$ paarweise verschieden sind gilt $\mathfrak{p}_1 \neq \mathfrak{p}_r$. $\mathfrak{p}_r$ wäre nicht minimal!

Primärzerlegung und Lokalisierung.

Im folgenden sei $S \subseteq A$ eine multiplikative Menge. Sei M ein $\mathfrak{p}$-koprimärer Modul. Dann gilt für eine natürliche Zahl r $\mathfrak{p}^r M = 0$. Damit gilt auch $\mathfrak{p}_S^r M_S = 0$.
Sei $S \cap \mathfrak{p} \neq \emptyset$. Dann ist $\mathfrak{p}_S = A_S$ und damit $M_S = 0$.
Sei $S \cap \mathfrak{p} = \emptyset$. Dann ist $Kern(M \to M_S) = \{x \in M | \exists s \in S \ , \ sx = 0\} = 0$, also $(M \to M_S)$ injektiv. Sei $\frac{a}{s} \in A_S \setminus \mathfrak{p}_S$. Dann ist $a \notin \mathfrak{p}$ und $M \xrightarrow{a} M$ injektiv, damit auch $M_S \xrightarrow{\frac{a}{1}} M_S$ injektiv, also auch die Multiplikationsabbildung $M_S \xrightarrow{\frac{a}{s}} M_S$. Die Multiplikation mit einem Element aus $\mathfrak{p}_S$ ist eine nilpotente Abbildung von M_S. M_S ist $\mathfrak{p}_S$-koprimär! Man kann aus diesem Ergebnis folgenden Satz ableiten

Satz. *Gegeben sei ein von Null verschiedener A-Modul* M. *Dann ist*

$$Ass(M_S) = \{\mathfrak{p}_S | \mathfrak{p} \in Ass(M) \ , \ \mathfrak{p} \cap S = \emptyset\}$$

Insbesondere heißt daß : $M_S \neq 0 \Leftrightarrow \exists \mathfrak{p} \in Ass(M)$ mit $\mathfrak{p} \cap S = \emptyset$. *Sei* $0 = P_1 \cap \cdots \cap P_m$ *eine unverkürzbare Primärzerlegung von* 0 *in* M *und seien* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *die zugehörigen Primideale, so ist*

$$0 = \bigcap_{\nu \ , \ \mathfrak{p}_\nu \cap S = \emptyset} P_\nu$$

eine unverkürzbare Primärzerlegung von 0 *in* M_S.

Zum Beweis. Nach dem Vorhergehenden gilt für einen Primärmodul P_ν

$$P_{\nu\, S} \text{ ist } \begin{cases} \mathfrak{p}_{\nu\, S} - \text{primär} & \text{falls } \mathfrak{p}_\nu \cap S = \emptyset \\ M_S & \text{sonst} \end{cases}$$

Für einen Untermodul $N \subsetneq M$ wurde im Abschnitt *Lokalisierung* die S-saturierte Hülle definiert

$$S(N) = \{x \in M | \exists s \in S \text{ mit } sx \in N.\}$$

Man zeigt: P_ν ist S-saturiert für $\mathfrak{p}_\nu \cap S = \emptyset$. Der Durchschnitt dieser S-saturierten P_ν ist die S-saturierte Hülle des Nullmoduls in M. Alle Behauptungen folgen wegen der eineindeutigen Beziehung zwischen A_S-Untermoduln von M_S und S-saturierten Untermoduln von M.

Wir wiederholen: $V(M) = \{\mathfrak{p} \in Spec(A) | M_\mathfrak{p} \neq 0\}$ ist der Träger des Moduls M in $Spec(A)$. $W(\mathfrak{a})$ ist die Menge der Primideale, die das Ideal $\mathfrak{a}$ umfassen.

Folgerung. *Es gilt*

$$V(M) = \{\mathfrak{q} \in Spec(A) | M_\mathfrak{q} \neq 0\} = \bigcap_{\mathfrak{p} \in Ass(M)} W(\mathfrak{p})$$

Aufgaben

Für ein Primideal $\mathfrak{p}$ des Ringes A sei $S_\mathfrak{p}$ das Komplement von $\mathfrak{p}$ in A. Sei M ein A-Modul.

1) Zeige folgende von der Darstelung des Nullmoduls unabhängige Charakterisierung von $Ass(M)$ Äquivalent ist

(1) $\mathfrak{p} \in Ass(M)$

(2) $\mathfrak{p}$ ist ein Primideal. Für jedes Primideal $\mathfrak{q} \subseteq \mathfrak{p}$, $\mathfrak{q} \neq \mathfrak{p}$ ist $S_\mathfrak{q}(N) \neq S_\mathfrak{p}(N)$

2) Sei N ein von Null verschiedener Untermodul von M. Dann gilt $Ass(N) \subseteq Ass(M)$.

VIII Ringe und Moduln endlicher Länge

Aus der Gruppentheorie; zur Erinnerung:

Ein A-Modul heißt ein Modul von endlicher Länge, wenn es eine Kompositionsreihe gibt, d.h. eine Reihe von Untermoduln

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

die sich nicht verfeinern läßt. n ist die Länge dieser Reihe. Äquivalent zur Nichtverfeinerbarkeit: Alle Faktormoduln $M_\nu/M_{\nu-1}$ sind einfach, enthalten also keine nichtrivialen ($\neq 0, \neq M_\nu/M_{\nu-1}$) Untermoduln. Ist dann

$$0 = X_0 \subsetneq X_1 \subsetneq X_2 \subsetneq \cdots \subsetneq X_m = M$$

eine weitere Reihe von Untermoduln, so läßt diese sich verfeinern zu einer Kompositionsreihe; diese Kompositionsreihe hat die gleiche Länge n, wie die Ausgangsreihe. Die Faktormoduln einer Kompositionsreihe sind bis auf die Reihenfolge eindeutig bestimmt. Äquvalent zur Existenz einer Kompositionsreihe ist:

Jede aufsteigende Kette von Untermoduln bricht ab, und jede absteigende Kette von Untermoduln bricht ab.

Definition. Sei M ein Modul endlicher Länge. Die gemeinsame Länge aller Kompositionsreihen heißt die Länge $\ell(M)$ von M; die Länge des Nullmoduls ist 0. Hat M keine endliche Länge, so ist $\ell(M) = \infty$.
Hat der Ring A als A-Modul endliche Länge, so heißt er ein artinscher Ring.

Unmittelbar aus der Definition folgt:

Satz. *Die Längenfunktion ist additif. Für eine kurze exakte Folge von Moduln*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

gilt: M hat genau dann endliche Länge, wenn N und P endliche Länge haben; es gilt

$$\ell(M) = \ell(N) + \ell(P)$$

Sei allgemeiner eine endliche Kette von Untermoduln gegeben:

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

Dann hat M genau dann endliche Länge, wenn alle auftretenden Faktormoduln $M_\nu/M_{\nu-1}$ endliche Länge haben; es gilt:

$$\ell(M) = \sum_\nu \ell(M_\nu/M_{\nu-1})$$

Beispiele. Ist $\mathfrak{m}$ ein maximales Ideal von A, so ist $A/\mathfrak{m}$ ein einfacher Modul, hat also die Länge 1. Umgekehrt sieht man leicht, daß jeder einfache Modul $M \neq 0$ von dieser Form ist. Werde allgemeiner der endliche Modul M von der Potenz $\mathfrak{m}^n$ eines endlich erzeugten maximalen Ideals $\mathfrak{m}$ annuliert. Dann gibt es die Reihe von Untermoduln

$$0 = \mathfrak{m}^n M \subseteq \mathfrak{m}^{n-1} M \subseteq \cdots \subseteq \mathfrak{m} M \subseteq M.$$

Alle auftretenden Faktormoduln $\mathfrak{m}^\nu M/\mathfrak{m}^{\nu+1} M$ werden von $\mathfrak{m}$ annuliert, sind also endliche Vektorräume über dem Restklassenkörper $A/\mathfrak{m}$, haben damit endliche Länge. Also hat auch M endliche Länge.

Im folgenden ist A immer ein noetherscher Ring, und jeder Modul über A noethersch.

Satz.

(1) *Sei A ein artinscher Ring. Dann hat jeder endliche A-Modul endliche Länge.*
(2) *Sei M ein A-Modul mit endlicher Länge. Wenn M ein treuer A-Modul ist, d.h. wenn der Annulator von M verschwindet, so ist A ein artinscher Ring.*
(3) *Ist M ein Modul endlicher Länge und $\mathfrak{a}$ der Annulator von M, so ist $A/\mathfrak{a}$ ein artinscher Ring.*

Beweis. (1): Jeder endliche freie Modul hat dann endliche Länge. Da jeder endliche Modul Faktormodul eines endlichen freien Moduls ist, hat also jeder solche Modul endliche Länge.

(2) : M ist ein endlicher A-Modul; also ist $M = \sum_{\nu=1}^{r} A x_\nu$. Da M ein treuer Modul ist, gibt es eine injektive Abbildung

$$A \underset{a \mapsto (ax_1, \ldots, ax_r)}{\hookrightarrow} M \times \cdots \times M = Q.$$

Mit M hat auch die direkte Summe Q und damit der Untermodul A endliche Länge. □

Satz. *Genau dann hat M endliche Länge, wenn der Träger von M $V(M)$ nur maximale Ideale enthält; die Anzahl dieser Ideale ist dann endlich. Äquivalent dazu ist auch (Primärzerlegung ....): $Ass(M)$ enthält nur maximale Ideale.*

Beweis. **a)** $M \neq 0$ habe endliche Länge. Sei $\mathfrak{p} \in Ass(M)$. Dann hat auch $P = A/\mathfrak{p} \subseteq M$ endliche Länge. Dann enthält aber P einen einfachen Untermodul $N \neq 0$. N ist isomorph zu einem Modul $A/\mathfrak{m}$ mit einem maximalen Ideal m. Daraus folgt aber $\mathfrak{m} \in Ass(P) = \{\mathfrak{p}\}$.

b) $Ass(M)$ enthalte nur maximale Ideale. $Ass(M) = \{\mathfrak{m}_1 \ldots, \mathfrak{m}_r\}$. Ist $r = 1$, so ist M koprimär zum maximalen Ideal $\mathfrak{m}_1$, und damit annuliert eine Potenz dieses maximalen Ideals diesen Modul. M hat also endliche Länge. Ist $r > 1$ und $0 = N_1 \cap \cdots \cap N_r$ die zugehörige Primärzerlegung des Nullmoduls in M, so ist M isomorph zu einem Untermodul des Moduls $M/N_1 \oplus \cdots \oplus M/N_r = Q$. M/N_ν ist koprimär zum maximalen Ideal $\mathfrak{m}_\nu$, hat also, wie schon bewiesen, endliche Länge. Damit hat auch die direkte Summe Q endliche Länge, damit auch M. □

Folgerung. *Sei A lokal. Ein endlicher A-Modul hat genau dann endliche Länge, wenn er durch eine Potenz des maximalen Ideals von A annuliert wird.*

IX Graduierte Ringe und Moduln
Das Hilbert-Polynom

Definition. Ein graduierter Ring A ist ein Ring A zusammen mit einer Familie $(A_\nu)_{\nu\in\mathbb{Z},\nu\geq 0}$ von Untergruppen–bei der Addition– A_ν von A, die folgende Eigenschaften besitzt

(1) $A = \bigoplus_\nu A_\nu$
(2) $A_\nu A_\mu \subseteq A_{\nu+\mu}$

Ein Element $a \in A_\nu$ heißt homogen vom Grad ν. Die erste Eigenschaft bedeutet, daß sich jedes Element $a \in A$ eindeutig als endliche Summe $a = a_{\nu_1} + \cdots + a_{\nu_n}$ homogener Elemente $a_{\nu_i} \in A_{\nu_i}$ verschiedenen Grades, den homogenen Komponenten von a, darstellen läßt.

Offenbar ist dann A_0 ein Unterring von A, der die 0 enthält und A_ν ist ein A_0-Modul.

Beispiel. Der Poynomring $B = R[T_1, \ldots, T_n]$ über dem Ring R ist auf natürliche Weise ein graduierter Ring mit $B_0 = R$;

$$B_d = \sum_{\nu_1+\cdots+\nu_n=d\ \nu_i\geq 0} RT_1^{\nu_1}\ldots T_n^{\nu_n}$$

ist der R-Modul der homogenen Polynome vom (totalen) Grad d.

Definition. Sei A ein graduierter Ring. Ein graduierter A-Modul ist ein A-Modul M zusammen mit einer Familie $(M_\nu)_{\nu\in\mathbb{Z}}$ von A_0-Moduln $M_\nu \subseteq M$ mit folgenden Eigenschaften

(1) $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$
(2) $A_\nu M_\mu \subseteq M_{\nu+\mu}$

Ein Element von M_d heißt homogen vom Grad d. Die erste Eigenschaft bedeutet, daß sich jedes Element x von M eindeutig als endliche Summe homogener Elemente verschiedenen Grades, den homogenen Komponeten von x, darstellen läßt.

Beispiele. Der graduierte Ring A ist als A-Modul ein graduierter Modul. Die direkte Summe graduierter A-Moduln ist auf natürliche Weise graduiert. Ein Untermodul N eines graduierten Moduls M enthalte mit einem Element auch alle seine homogenen Elemente. Dann ist N auf natürliche Weise ein graduierter Modul, ein graduierter Untermodul von M :

$$N_\nu = N \cap M_\nu$$

Dann ist auch der Faktormodul M/N auf natürliche Weise ein graduierter Modul:

$$(M/N)_\nu = M_\nu/N_\nu$$

Definition. Gegeben seien zwei graduierte Moduln M, N über dem graduierten Ring A. Ein Homomorphismus $f : M \to N$ heißt homogen vom Grad Null, oder einfach ein Homomorphismus graduierter Moduln oder graduierter Homomorphismus wenn gilt $f(M_\nu) \subseteq N_\nu \quad \forall \nu$. f induziert dann für alle ν einen A_0 Homomorphismus $f_\nu = f|M_\nu : M_\nu \to N_\nu$ Für ein Element $a \in A_\nu$ und $x \in M_\mu$ gilt $af_\mu(x) = f_{\nu+\mu}(ax)$ Eine Familie $(f_\nu)_{\nu\in\mathbb{Z}}$ von A_0-Homomorphismen $M_\nu \to N_\nu$ mit der vorher angegebenen Eigenschaft definiert umgekehrt einen eindeutig definierten Homomorphismus $f : M \to N$ graduierter Moduln. Allgemeiner heißt ein Homomorphismus $f : M \to N$ homogen vom Grad d, wenn $f(M_\nu) \subseteq N_{\nu+d} \quad \forall \nu$.

Definition. Gegeben sei ein graduierter Modul M. Für jede natürliche Zahl n erklärt man auf M eine verschobene Graduierung und nennt M mit dieser Graduierung $M[n]$:

$$M[n]_\nu = M_{\nu+n}$$

Ein Homomorphismus $f : M \to N$ graduierter Moduln ist dann auch graduierter Homomorphismus der verschobenen Moduln; Bezeichnung

$$f[n] : M[n] \longrightarrow N[n]$$

Sei $f : M \to N$ ein homogener Homomorphismus vom Grad d. Dann kann f auch aufgefaß t werden als homogener Homomorphismus vom Grad 0 :

$$M \longrightarrow N[d]$$

oder

$$M[-d] \longrightarrow N$$

Beispiel. Sei M ein graduierter A-Modul und $a \in A_d$. Dann ist die Multiplikation mit dem Element a ein graduierter Homomorphismus $M[-d] \stackrel{a}{\to} M$ oder $M \stackrel{a}{\to} M[d]$.

Exaktheit. Kern und Bild eines graduierten Homomorphismus sind graduierte Untermoduln. Sei

$$M \xrightarrow{f} N \xrightarrow{g} P$$

eine Folge graduierter Homomorphismen von A-Moduln. Diese Folge ist genau dann exakt, wenn die induzierten Folgen von A_0-Homomorphismen der homogenen Bestandteile

$$M_\nu \xrightarrow{f_\nu} N_\nu \xrightarrow{g_\nu} P_\nu$$

exakt sind.

Sei nun der graduierte Ring A noethersch. Dann ist auch A_0 noethersch und man sieht leicht, daß die A_0-Moduln A_ν noethersch sind. Sei $A_1 = A_0t_1 + \cdots + A_0t_n$. Wir wollen im folgenden zusätzlich voraussetzen, daß A über A_0 durch A_1 erzeugt wird:

$$A = A_0[A_1] = A_0[t_1, \ldots, t_n]$$

Dann ist der Einsetzungshomomorphismus des Polynomringes $A_0[T_1 \ldots T_n]$, versehen mit seiner natürlichen Graduierung durch den Totalgrad, in A

$$A_0[T_1 \ldots T_n] \underset{P(T_1,\ldots,T_n)\longmapsto P(t_1,\ldots,t_n)}{\longrightarrow} A$$

surjektiv und mit den Graduierungen verträglich. Das Kernideal ist homogen, d.h. ein graduierter Untermodul des Polynomringes.

Sei M ein noetherscher graduierter Modul über A. Dann wird M durch endlich viele homogene Elemente erzeugt. Alle A_0-Moduln M_ν sind endliche A_0-Moduln. Es gilt

$$M_\nu = 0 \ \ \forall \nu \leq \nu_0.$$

Sei A ein graduierter Ring. Wir wollen im folgenden annehmen, daß A_0 ein artinscher Ring ist, also endliche Länge hat. Sei dann M ein endlicher graduierter A-Modul. Dann haben auch alle A_0-Moduln M_ν endliche Länge.

Definition. Sei M ein endlicher graduierter Modul über dem graduierten Ring A. Wir definieren eine Funktion

$$F_M : \mathbb{Z} \longrightarrow \mathbb{Z}$$

durch $F_M(n) = \ell(M_n)$. Dabei ist $\ell(M_n)$ die Länge von M_n. Da $M_n = 0$ für $n \leq n_0$ gilt $F_M(n) = 0$ für $n \leq n_0$. Es ist $F_M(n) \geq 0$.

Aus elementaren Eigenschaften der Länge, z.B. der Additivität bei kurzen exakten Folgen erhält man

Lemma.

(1) *Sei*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

eine kurze exakte Folge graduierter A-Moduln, d.h insbesondere daß die auftretenden Abbildungen graduiert sind. Dann gilt

$$F_M = F_N + F_P$$

(2) *Sei eine endliche aufsteigende Folge graduierter Untermoduln von M gegeben:*

$$0 = M^{(0)} \subseteq M^{(1)} \subseteq \cdots \subseteq M^{(r)} = M$$

Dann gilt

$$F_M = \sum_{\nu=1}^{r} F_{M^{(\nu)}/M^{(\nu-1)}}$$

(3)

$$F_{M[d]}(n) = F_M(n+d)$$

Theorem Hilbert. *Sei $A = A_0[t_1, \ldots, t_r]$ $t_\nu \in A_1$ ein graduierter Ring und M ein graduierter Modul über A. Dann gibt es ein eindeutig bestimmtes Polynom $P_M(x) \in \mathbb{Q}[x]$, das Hilbertpolynom des graduierten Moduls M, mit*

$$P_M(n) = F_M(n) \ \ \forall n \geq n_0$$

Es gilt für den Grad dieses Polynoms die Abschätzung $deg(P_M) \leq r-1$. *Offenbar hat dannn der höchste Term dieses Polynoms–falls es nicht identisch verschwindet– einen positiven Koeffizienten.*

Beweis. Weil ein Polynom durch seine Werte an unendlich vielen Stellen eindeutig festgelegt ist, folgt die behauptete Eindeutigkeit. Wir betrachten den Einsetzungshomomorphismus

$$A_0[T_1, \ldots, T_r] \xrightarrow{T_\nu \mapsto t_\nu} A$$

des Polynomringes $A_0[T_1, \ldots, T_r]$ auf A. M kann dann als graduierter Modul über dem natürlich graduierten Polynomring aufgefaßt werden, und es genügt, den Satz für den Modul als Modul über diesem Polynomring zu beweisen. O.B.d.A : $A = A_0[T_1, \ldots, T_r]$. Wir führen einen Induktionsbeweis nach der Anzahl r der Variablen. Sei $r = 0$, also $A = A_0$. Dann ist der ganze Modul M ein endlicher Modul über A_0 und M_n verschwindet für genügend große n. $F_M(n) = 0 \ \forall n \geq n_0$.

Sei $r > 0$. Angenommen, die Variable T_r annuliert M. Dann genügt es, M als Modul über $A_0[T_1, \ldots, T_{r-1}]$ aufzufassen und die Behauptung des Satzes für diesen Modul über $A_0[T_1, \ldots, T_{r-1}]$ zu beweisen. Nach Induktionsvoraussetzung gilt aber die Behauptung des Satzes für alle $A_0[T_1, \ldots, T_{r-1}]$-Moduln. Wir wollen den allgemeinen Fall auf diese speziellen schon bewiesenen zurückführen.

Erster Fall: T_r sei Nichtnullteiler von M. Dann gibt es eine kurze exakte Folge graduierter Moduln

$$0 \longrightarrow M[-1] \xrightarrow{T_r} M \longrightarrow N \longrightarrow 0$$

Dabei ist N der Faktormodul von M nach dem graduierten Untermodul $T_r M$. Der Modul N wird durch T_r annuliert; nach Induktionsvoraussetzung gibt es also ein Polynom $P_N(x)$ mit $deg(P_N) \leq r-2$ mit $F_N(n) = P_N(n)$ für große n. Ferner gilt

$$F_{M[-1]} + F_N = F_M$$

Wegen $F_{M[-1]}(n) = F_M(n-1)$ gilt damit für große ganze Zahlen n

$$F_M(n) - F_M(n-1) = P_N(n) \ \forall n \geq n_0$$

Sei $c = F_M(n_0 - 1)$. Es folgt für $n \geq n_0$

$$F_M(n) = c + \sum_{\nu=n_0}^{n} P_\nu(n)$$

Die gesuchte Aussage für den Modul M erhält man nun aus dem Lemma

Lemma Existenz von Summenformeln. *Sei* $P(x) \in \mathbb{Q}[x]$ *ein Polynom vom Grad* s. *Dann gibt es ein Polynom* $Q(x) \in \mathbb{Q}[x]$ *vom Grad* $s+1$ *mit*

$$Q(x) - Q(x-1) = P(x)$$

Beweis des Lemmas. Sei $U_\nu \subseteq \mathbb{Q}[x]$ der endliche Vektorraum über $\mathbb{Q}$ der Polynome vom Grad kleiner oder gleich ν. Wir betrachten die lineare Abbildung

$$U_{s+1} \to U_s,$$

die einem Polynom $G(x)$ das Polynom $G(x) - G(x-1)$ zuordnet. Der Kern ist der Vektorraum der konstanten Polynome, hat also die Dimension 1. Wegen $dim(U_{s+1}) = 1 + dim(U_s)$ ist diese lineare Abbildung surjektiv.

Wir fahren mit dem Beweis des Theorems fort. Der allgemeine Fall. T_r annuliere M nicht. Sei $N^{(\nu)} = \{x \in M | T_r^\nu x = 0\}$. Dann ist $N^{(\nu)}$ ein graduierter Untermodul von M.

$$0 = N^{(0)} \subseteq N^{(1)} \subseteq N^{(2)} \subseteq \cdots \subseteq M$$

Weil M noethersch ist, bricht diese aufsteigende Kette von Untermoduln ab. Es gibt also eine natürliche Zahl m, so daß gilt $N = N^{(m)} = N^{(m+1)} = \ldots$. Dann ist T_r Nichtnullteiler von M/N. Die Faktormoduln $N^{(\nu)}/N^{(\nu-1)}$ werden durch T_r annuliert. Wie bereits bewiesen, gibt es also Polynome P_ν vom Grad $deg(P_\nu) \leq r-2$ und ein Polynom P vom Grad $deg(P) \leq r-1$, so daß für große n gilt $F_{N_\nu/N_{\nu-1}}(n) = P_\nu(n)$, $F_{M/N}(n) = P(n)$. Für große n gilt dann

$$F_M(n) = \sum_{\nu=1}^{m} F_{N_\nu/N_{\nu-1}}(n) + F_{M/N}(n) = \sum_{\nu=1}^{m} P_\nu(n) + P(n) = Q(n)$$

$Q(x)$ ist ein Polynom vom Grad $deg(Q) \leq r-1$! $\square$

X Filtrierte Ringe und Moduln Das Lemma von Artin-Rees Das Hilbert-Samuel-Polynom

Wir betrachten noethersche Ringe A und noethersche Moduln M über A.

Definition. Eine Familie $\mathcal{F} = (\mathfrak{a}_\nu)_{\nu \geq 0}$ von Idealen des Ringes A heißt eine Filtrierung von A, wenn gilt

(1) $\mathfrak{a}_0 = A\ ,\ \mathfrak{a}_n \supseteq \mathfrak{a}_{n+1} \quad \forall n \geq 0$
(2) $\mathfrak{a}_\nu \mathfrak{a}_\mu \subseteq \mathfrak{a}_{\nu+\mu} \forall \nu, \mu \geq 0$

A zusammen mit der Filtrierung heißt ein filtrierter Ring. Sei M ein Modul über dem filtrierten Ring A. Eine Familie $\mathcal{G} = (M_\nu)_{\nu \geq 0}$ von Untermoduln von M heißt eine Filtrierung von M wenn gilt

(1) $M_0 = M\ ,\ M_n \supseteq M_{n+1}\ \ \forall n \geq 0$
(2) $\mathfrak{a}_\nu M_\mu \subseteq M_{\nu+\mu}\ \ \forall \nu, \mu \geq 0$

M zusammen mit der Filtrierung heißt ein filtrierter Modul über dem filtrierten Ring A. Sei N ein zweiter mit der Familie $(N_\nu)_{\nu \geq 0}$ filtrierter Modul. Ein Homomorphismus

$$f : M \longrightarrow N$$

ist mit den Filtrierungen verträglich und heißt Homomorphismus filtrierter Moduln, wenn gilt

$$f(M_\nu) \subseteq N_\nu\ \ \forall \nu \geq 0$$

Beispiele. *Ein filtrierter Ring A ist auch ein filtrierter A Modul. Sei M ein Modul über dem Ring A und $\mathfrak{q}$ ein Ideal von A. Dann bilden die Potenzen $\mathfrak{q}^\nu\ ,\ \nu \geq 0$ eine Filtrierung von A, die $\mathfrak{q}$-adische Filtrierung von A. Die $\mathfrak{q}$-adische Filtierung von M ist die Familie $(\mathfrak{q}^\nu M)_{\nu \geq 0}$. Mit dieser Filtrierung ist M ein filtrierter Modul über dem $\mathfrak{q}$-adisch filtrierten Ring. Sei $\mathcal{G} = (M_\nu)_{\nu \geq 0}$ eine Filtrierung von M, N ein Untermodul von M und P ein Faktormodul. Dann ist $(M_\nu \cap N)_{\nu \geq 0}$ eine Filtrirung von N, die in N induzierte Filtrierung. Die Bilder der M_ν in P bilden eine Filtrierung von P, die in P induzierte Filtrierung. Sei $\mathcal{G}$ die $\mathfrak{q}$-adische Filtrierung von M. Dann ist die in P induzierte Filtrierung die $\mathfrak{q}$-adische Filtrierung, die in N induzierte im allgemeinen nicht.*

Im folgenden sei A ein $\mathfrak{q}$- adisch filtrierter Ring. Sei

$$\overline{A} = A \oplus \mathfrak{q} \oplus \mathfrak{q}^2 \oplus \mathfrak{q}^3 \oplus \ldots$$

Dann wird auf naheliegende Weise auf $\overline{A}$ eine Multiplikation erklärt und man erhält so einen auf natürliche Weise graduierten Ring, graduiert durch $\overline{A}_\nu = \mathfrak{q}^\nu$. Sei $\mathfrak{q} = At_1 + \cdots + At_r$. Wir fassen die Elemente $t_1, \ldots, t_r$ als Elemente $t_\nu \in \overline{A}_1$, also als Elemente vom Grad 1 von $\overline{A}$ auf und erhalten

$$\overline{A} = A[t_1, \ldots, t_r]$$

In dieser Formel ist $A = \overline{A}_0$. Insbesondere ist dieser Ring $\overline{A}$ noethersch.

Sei M ein filtrierter Modul über dem –$\mathfrak{q}$-adisch–filtrierten Ring A mit der Filtrierung $(M_\nu)_{\nu\geq 0}$, die aber nicht notwendig $\mathfrak{q}$-adisch sein muß . Dann ist

$$\overline{M} = \bigoplus_{\nu\geq 0} M_\nu$$

in naheliegender Weise ein graduierter Modul über $\overline{A}$.

Lemma. *Folgende Aussagen sind äquvivalent:*

(1) $M_{n+1} = \mathfrak{q}M_n \ \ \forall n \geq n_0$
(2) $M_{n_0+k} = \mathfrak{q}^k M_{n_0} \ \ \forall k \geq n_0$
(3) $\overline{M}$ *ist ein endlicher* $\overline{A}$*-Modul.*

Beweis. Es ist klar, daß die beiden erste Aussagen äquivalent sind.
(2) $\Rightarrow$ (3): Aus der Voraussetzung (2) folgt, daß $\overline{M}$ als $\overline{A}$-Modul durch

$$\bigoplus_{0\leq\nu\leq n_0} M_\nu$$

also durch eine endlichen ($\overline{A}_0 = A$)-Modul erzeugt wird.
(2) $\Rightarrow$ (3) Sei $\overline{M}$ endlicher $\overline{A}$-Modul. Dann gibt es eine natürliche Zahl n_0, so daß der $\overline{A}$-Modul $\overline{M}$ durch $\bigoplus_{0\leq\nu\leq n_0} M_\nu$ erzeugt wird. Daraus folgt aber

$$M_{n_0+k} = \mathfrak{q}^k M_{n_0} \ \ \forall k \geq n_0$$

□

Definition. Sei M ein filtrierter Modul über dem $\mathfrak{q}$-adisch filtrierten Ring A. Die Filtrierung von M heißt $\mathfrak{q}$-gut und M $\mathfrak{q}$-gut filtriert, wenn eine der drei äquvalenten Bedingungen des vorhergehenden Lemmas erfüllt ist. Insbesondere ist die $\mathfrak{q}$-adische Filtrierung $\mathfrak{q}$-gut.

Satz von Artin-Rees. *N sein filtrierter Untermodul des $\mathfrak{q}$-gut filtrierten Moduls M. Dann ist die Filtrierung von N auch $\mathfrak{q}$-gut. Insbesondere ist die durch die Filtrierung von M in N induzierte Filtrierung $\mathfrak{q}$-gut.*

Beweis. Wir verwenden die dritte Bedingung des vorigen Lemmas. $\overline{A}$ ist ein noetherscher Ring und $\overline{N}$ ein $\overline{A}$-Untermodul von $\overline{M}$. Weil $\overline{M}$ ein endlicher $\overline{A}$-Modul ist, ist auch $\overline{N}$ endlicher $\overline{A}$-Modul. □

Folgerung. *Sei A ein lokaler Ring und das Ideal $\mathfrak{q}$ im maximalen Ideal enthalten. Dann ist die $\mathfrak{q}$-adische Filtrierung, allgemeiner jede $\mathfrak{q}$-gute Filtrierung des Moduls M separiert. D.h der Durchchnitt der filtrierenden Untermoduln ist der Nullmodul.*

$$\bigcap_\nu \mathfrak{q}^\nu M = 0$$

Bemerkung. Es genügt, daß $\mathfrak{q}$ im Durchschnitt aller maximalen Ideale, dem sogenannten Jakobsonradikal enthalten ist. Dann gilt nämlich für das Ideal $\mathfrak{q}$ das Lemma von Nakayama.

Beweis. sei $N = \bigcap_\nu \mathfrak{q}^\nu M$. Dann gilt für die induzirte Filtrierung (N_ν) auf N

$$N_\nu = N \cap \mathfrak{q}^n M = N$$

Da diese Filtrierung aber $\mathfrak{q}$-gut ist folgt: $\mathfrak{q}N = N$. Nach dem Lemma von Nakayama folgt $N = 0$. Für eine beliebige $\mathfrak{q}$-gute Filtrierung (M_ν) von M gilt $M_{n+n_0} = \mathfrak{q}^n M_{n_0} \subseteq \mathfrak{q}^n M \ \ \forall n \geq 0$. Es folgt $\bigcap_n M_n = 0 \quad \square$

Im folgenden sei $\mathfrak{q}$ ein Ideal des Ringes A und (M_ν) eine $\mathfrak{q}$-gute Filtrierung des Moduls M.

Definition. *Der assozierte graduierte Ring zur $\mathfrak{q}$- adischen Filtrierung bzw. der assozierte graduierte Modul zu einem filtrierten Modul.* Sei $\mathcal{F} = (M_\nu)$ die Filtrierung von M.

Sei

$$gr_\mathfrak{q}(A) = A/\mathfrak{q} \oplus \mathfrak{q}/\mathfrak{q}^2 \oplus \mathfrak{q}^2/\mathfrak{q}^3 \oplus \dots$$
$$gr_\mathcal{F}(M) = M_0/M_1 \oplus M_1/M_2 \oplus M_2/M_3 \oplus \dots$$

Dann ist $gr_\mathfrak{q}(A)$ auf natürliche Weise ein graduierter Ring und $gr_\mathcal{F}(M)$ auf natürliche Weise ein graduierter $gr_\mathfrak{q}(A)$-Modul. Ist $\mathcal{F}$ die $\mathfrak{q}$-adische Filtrierung, so schreiben wir auch $gr_\mathcal{F}(M) = gr_\mathfrak{q}(M)$

Bemerkung. Sei $q = A\tilde{t_1} + \dots + A\tilde{t_r}$ und seien die Elemente t_ν die Bilder in $\mathfrak{q}/\mathfrak{q}^2 \subseteq gr_\mathfrak{q}(A)$. Dann gilt $gr_\mathfrak{q}(A) = A/\mathfrak{q}[t_1, \dots, t_r]$. $gr_\mathfrak{q}(A)$ ist Faktorring des anfangs eingeführten graduierten Ringes $\overline{A}$ und $gr_\mathcal{F}(M)$ Faktormodul von $\overline{M}$. Ist die Filtrierung $\mathcal{F}$ $\mathfrak{q}$-gut, so ist $\overline{M}$ endlicher $\overline{A}$-Modul, also $gr_\mathcal{F}(M)$ endlicher $gr_\mathfrak{q}(A)$-Modul.

Sei nun zunächst $A/\mathfrak{q}$ ein artinscher Ring. Dann gibt es nach Hilbert ein Polynom $Q(x) \in \mathbb{Q}[x]$ mit $\ell(M_n/M_{n+1}) = Q(n) \ \ \forall n \geq n_0$. Der Grad von Q ist kleiner oder gleich $r-1$. Dann hat auch M/M_n endliche Länge und es gilt

$$\begin{aligned}\ell(M/M_n) &= \ell(M/M_1) + \ell(M_1/M_2) + \dots + \ell(M_{n_0-1}/M_{n_0}) \\ &\quad + Q(n_0) + Q(n_0+1) + \dots + Q(n-1) + Q(n) \\ &= P(n) \ \ \forall n \geq n_0\end{aligned}$$

Dabei ist P ein Polynom mit rationalen Koeffizienten vom Grad kleiner oder gleich r.

Dieses Resultat wollen wir verallgemeinern. Der Einfacheit halber sei A ein lokaler Ring mit dem maximalen Ideal $\mathfrak{m}$. Nur der Faktormodul $M/\mathfrak{q}M$ habe endliche Länge. Sei $\mathfrak{a}$ der Annulator von M. Man kann A durch $A/\mathfrak{a}$ ersetzen bzw. $\mathfrak{q}$ durch das Bild in $A/\mathfrak{a}$. Es gilt dann

$$\begin{aligned}\{\mathfrak{m}\} &= V(M/\mathfrak{q}M) = V(M) \cap W(\mathfrak{q}) = W(Ann(M)) \cap W(\mathfrak{q}) = W(0) \cap W(\mathfrak{q}) \\ &= V(A/\mathfrak{q})\end{aligned}$$

Dann hat also auch $A/\mathfrak{q}$ endliche Länge und es gelten die vorhergehenden Resultate.

Satz Das Hilbert-Samuel-Polynom. *Sei $\mathcal{F} = (M_\nu)$ eine $\mathfrak{q}$-gute Filtrierung des A-Moduls. Der Modul $M/\mathfrak{q}M$ habe endliche Länge; äquivalent dazu $V(M/\mathfrak{q}M)$ enthalte nur maximale Ideale und deren Anzahl sei endlich. Dann haben alle Moduln M/M_n endliche Länge und es gibt ein eindeutig bestimmtes Polynom $P_{\mathcal{F}}(M,x) \in \mathbb{Q}[x]$ und eine natürliche Zahl n_0 mit*

$$\ell(M/M_n) = P_{\mathcal{F}}(M,n) \ \ \forall n \geq n_0$$

Wird das Ideal $\mathfrak{q}$ durch r Elemente erzeugt, so gilt für den Grad $deg(P_{\mathcal{F}}(M,x))$ die Abschätzung

$$deg(P_{\mathcal{F}}(M,x)) \leq r$$

Ist die Filtierung die $\mathfrak{q}$-adische so schreiben wir auch

$$P_{\mathcal{F}}(M,x) = P_{\mathfrak{q}}(M,x)$$

Das Polynom $P_{\mathcal{F}}(M,x)$ heißt auch das Hilbert-Samuel-Polynom von M zur Filtrierung $\mathcal{F}$ von M. Falls dieses Polynom nicht identisch verschwindet, ist der Koeffizient des höchsten Terms von $P_{\mathcal{F}}(M,x)$ eine positive rationale Zahl.

Für eine genügend große Zahl n_0 gilt $\mathfrak{q}^n M \subseteq M_n \subseteq \mathfrak{q}^{n-n_0} M \ \ \forall n \geq n_0$ und daher $P_{\mathfrak{q}}(M, n-n_0) \leq P_{\mathcal{F}}(M,n) \leq P_{\mathfrak{q}}(M,n) \ \ \forall n \geq n_0$. Man erhält

Lemma. *Unter den Voraussetzungen des Satzes gilt: Der höchste Term des Hilbert-Samuel-Polynoms von M zur $\mathfrak{q}$-guten Filtrierung $\mathcal{F}$ von M und der höchste Term des Hilbert-Samuel-Polynoms von M zur $\mathfrak{q}$-adischen Filtrierung stimmen überein. Dieser höchste Term hängt also nur von $\mathfrak{q}$, nicht von der speziel gewählten $\mathfrak{q}$-guten Filtrierung ab. Insbesondere gilt*

$$deg(P_{\mathfrak{q}}(M,x)) = deg(P_{\mathcal{F}}(M,x))$$

.

Bemerkung. Ähnlich zeigt man: Gegeben sei ein zweites Ideal $\mathfrak{q}'$ mit $\mathfrak{q}^s \subseteq \mathfrak{q}' \subseteq \mathfrak{q}'$ für eine natürliche Zahl s. Dann gilt

$$deg(P_{\mathfrak{q}}(M,x)) = deg(P_{\mathfrak{q}'}(M,x))$$

Aus der Additivität der Längenfunktion und dem Lemma von Artin-Rees folgt

Lemma. *Sei*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

eine kurze exakte Folge und $\mathcal{F}$ die durch die $\mathfrak{q}$-adische Filtrierung von M im Untermodul N induzierte Folge. Dann gilt

$$P_{\mathfrak{q}}(M,x) = P_{\mathcal{F}}(N,x) + P_{\mathfrak{q}}(P,x)$$
$$deg(P_{\mathfrak{q}}(M,x)) = \sup(deg(P_{\mathfrak{q}}(N,x)), deg(P_{\mathfrak{q}}(P,x)))$$

Ergänzungen: Komplettierung von Ringen und Moduln

Sei A ein fitrierter A Ring und M ein filtrierter A-Modul mit der Filtrierung $\mathcal{F} = (M_\nu)$. Diese Filtrierrung definiert eine Topologie auf M. Eine Basis von Umgebungen eines Elements $x \in M$ ist die Familie von Teilmengen $(x+M_\nu)$. Ist die Filtrierung separiert, ist also der Durchschnitt aller Untermoduln M_ν der Nullmodul, so ist diese Topologie Hausdorffsch. Die Filtrierung des Ringes A liefert ebenso eine Topologie auf A. Alle algebraischen Operationen, also Multiplikation und Addition, sind stetig. Diese Topologien werden jeweils durch eine Metrik erzeugt: Etwa

$$d(x,y) = 2^{-(\sup\limits_{x-y\in M_n} n)} \quad \forall x, y \in M$$

Die Topologie zu einer $\mathfrak{q}$-guten Filtrierung stimmt immer mit der Topologie zur $\mathfrak{q}$-adischen Filtrierung überein. Die zugehörigen Metriken sind dann äquivalent, definieren also die gleichen Cauchyfolgen. Beschränken wir uns auf $\mathfrak{q}$-adische Filtrierungen zu einem festen Ideal $\mathfrak{q}$. Ein Modulhomomorphismus ist dann immer stetig. Mit Hilfe von Cauchyfolgen konstruiert man die Komplettierungen $\hat{A}, \hat{M}$ von A und M. Die algebraischen Operatione lassen sich stetig auf die Komplettierungen fortsetzen; $\hat{A}$ ist dann ein Ring und $\hat{M}$ ein Modul über $\hat{M}$. Ein Homomorphismus läßt sich immer stetig zu einem Homomorphismus der Komplettierungen fortsetzen. Man zeigt mit Hilfe des Lemmas von Artin-Rees:

(1) $\hat{A}$ ist wieder ein noetherscher Ring.
(2) Die Komplettierung einer kurzen exakten Folge endlicher Moduln ist wieder eine kurze exakte Folge endlicher Moduln.
(3) Die Komplettierung eines endlichen freien Moduls ist ein endlicher freier Modul.

Aus der zweiten Eigenschaft folgt, daß die Komplettierung ein exakter Funktor auf der Kategorie der endlichen Moduln ist. Man kann die Komplettierung auch rein algebraisch konstruieren, benötigt dazu aber den Begrif des projektiven Limes:

$$\hat{M} = \varprojlim M/M_n$$

Dieser projektive Limes besteht aus allen Folgen (x_n), von Elementen $x_n \in M/M_n$ mit folgender Eigenschaft: Bei der natürlichen Abbildung

$$M/M_{n+1} \longrightarrow M/M_n$$

wird x_{n+1} in x_n abgebildet.

Die Komplettierungen von Ringen haben in wichtigen Fällen viel einfachere Eigenschaften als der Ausgangsring; es gibt eine Stukturtheorie der kompletten lokalen Ringe.

Beispiele $\mathfrak{q}$-adischer Komplettierungen. Sei $A = k[x]$ ein Polynomring in der Variablen x über k und $\mathfrak{q} = Ax$. Dann ist die Komplettierung der Ring der formalen Potenzreihen über k in der Variablen x. Sei $p \in \mathbb{Z}$ eine Primzahl und $\mathfrak{q} = \mathbb{Z}p$. Die Komplettierung ist ein Integritätsbereich, der Ring der ganzen p-adichen Zahlen. Dieser Ring und sein Quotientenkörper, der Körper $\mathbb{Q}_p$ der p-adischen Zahlen spielen ein wichtige Rolle in der Zahlentheorie.

XI Die Dimension von Moduln und Ringen.

In diesem Paragraphen ist A ein noetherscherl *lokaler* Ring; man könnte allgemeiner annehmen, daß A nur semilokal ist. Sei $\mathfrak{m}$ das maximale Ideal von A. Ein *Primärideal* ist im folgenden immer ein Primärideal zum maximalen Ideal $\mathfrak{m}$; ein Primärideal $\mathfrak{q}$ ist dann gekennzeichnet durch

$$\mathfrak{m}^{n_0} \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

Wir betrachten einen von Null verschiedenen endlichen Modul M über A. Es gibt drei verschiedene Dimensionsbegriffe für den Modul M.

Die Krull-Dimension von M

Sei $\mathfrak{a}$ der Annulator des Moduls M. Dann gilt für den Träger von M

$$V(M) = W(\mathfrak{a}) = \{\mathfrak{p} \in Spec(A) | \mathfrak{a} \subseteq \mathfrak{p}\}$$

Wir betrachten Ketten von Primidealen in $V(M)$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq p_m \ , \ \mathfrak{p}_\nu \in V(M)$$

m heißt die Länge dieser Kette.

Definition. Die Krulldimension $\dim(M)$ von M ist das Supremum der Längen aller solcher Primidealketten in $V(M)$. Es gilt $\dim(M) \leq \infty$. Offenbar ist

$$\dim(M) = \dim(A/\mathfrak{a})$$

Die Hilbert-Samuel-Dimension des Moduls M.

Sei $\mathfrak{q}$ ein Primärideal von A. Dann hat $M/\mathfrak{q}M$ endliche Länge. Sei $\mathcal{F} = (M_\nu)$ eine $\mathfrak{q}$-gute Filtrierung von M. Seien $P_{\mathcal{F}}(M,n)$, $P_{\mathfrak{q}}(M,n)$, $P_{\mathfrak{m}}(M,n)$ die Hilber-Samuel-Polynome von M zur Filtrierung $\mathcal{F}$ bzw. zur $\mathfrak{q}$-adischen bzw. zur $\mathfrak{m}$-adischen Filtrierung von M. Es gilt für eine genügend große natürliche Zahl n_0

$$\mathfrak{q}^n M \subseteq M_n \subseteq \mathfrak{q}^{n-n_0} M \text{ für } n \geq n_0$$
$$\mathfrak{m}^{nn_0} M \subseteq \mathfrak{q}^n M \subseteq \mathfrak{m}^n M \text{ für } n \geq 0$$

Daraus folgt

$$P_{\mathfrak{q}}(M,n) \geq P_{\mathcal{F}}(M,n) \geq P_{\mathfrak{q}}(M,n-n_0)$$
$$P_{\mathfrak{m}}(M,nn_0) \geq P_{\mathfrak{q}}(M,n) \geq P_{\mathfrak{m}}(M,n)$$

Die Grade der drei Polynome stimmen überein!

$$deg(P_{\mathcal{F}}) = deg(P_{\mathfrak{q}}) = deg(P_{\mathfrak{m}}).$$

Definition. Der gemeinsame Grad dieser drei Polynome, der insbesondere nicht von der Wahl des Primärideals $\mathfrak{q}$ abhängt, heißt die Hilbert-Dimension von M. Schreibweise

$$d_H(M).$$

Diese Dimension ist eine endliche natürliche Zahl.

Aus der Additivität der Länge und dem Lemma von Artin-Rees folgt

Lemma. *Gegeben sei eine kurze exakte Folge von Moduln ($\neq 0$)*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

Dann gilt

$$d_H(M) = \sup(d_H(N), d_H(P))$$

Wir behandeln noch einen Spezialfall:

Lemma. *Sei $t \in \mathfrak{m}$ ein Nichtnullteiler von M. Dann ist die Folge*

$$0 \longrightarrow M \xrightarrow{t} M \longrightarrow M/tM \longrightarrow 0$$

exakt und es gilt die Abschätzung

$$d_H(M) \geq d_H(M/tM) + 1$$

Zum Beweis. Bei der Injektion $M \overset{t}{\hookrightarrow} M$ induziert die $\mathfrak{m}$-adische Filtrierung von M eine $\mathfrak{m}$- gute Filtrierung $\mathcal{F}$ auf M. Aus der schon einmal benutzten Abschätzung

$$P_{\mathfrak{m}}(M, n) \geq P_{\mathcal{F}}(M, n) \geq P_{\mathfrak{m}}(M, n - n_0)$$

folgt, daß die höchsten Terme der beiden Polynome $P_{\mathfrak{m}}$, $P_{\mathcal{F}}$ übereinstimmen. Andererseits gilt wegen der Additivität der Länge

$$P_{\mathfrak{m}}(M/tM, n) + P_{\mathcal{F}}(M, n) = P_{\mathfrak{m}}(M, n)$$

Aus diesen beiden Aussagen ergibt sich die Behauptung des Lemmas.

Die Chevalleydimesion von M

Wir betrachten Systeme $x = \{x_1, \ldots, x_r\}$ von Elementen $x_\nu \in \mathfrak{m}$. Wir nennen r die Länge von x. Das von den Elementen x_ν erzeugte Ideal sei (x). Ist x leer, so ist die Länge Null und das Ideal (x) das Nullideal. Sei $\mathfrak{a} = Ann(M)$ der Annulator von M. Der Modul $M/(x)M$ hat genau dann endliche Länge, wenn $V(M/(x)M) = V(M) \cap W((x)) = W(\mathfrak{a}) \cap W((x)) = W(\mathfrak{a} + (x))$ nur endlich viele und nur maximale Ideale enthält, damit nur $\mathfrak{m}$. Das bedeutet aber, daß $\mathfrak{a} + (x)$ ein Primärideal ist.

Definition. Die Chevalleydimension $s(M)$ ist das Infimum der Längen von Elemensystemen x, für die der Modul $M/(x)M$ endliche Länge hat. Insbesondere ist $s(M)$ eine endliche natürliche Zahl.

Bemerkung. Für alle drei Dimensionen gilt

(1) $\mathfrak{a}$ sei der Annulator von M oder allgemeiner in diesem Annulator enthalten. Dann ist die Dimension von M als A-Modul die gleiche, wie die von M als $A/\mathfrak{a}$-Modul betrachtet.
(2) M habe endliche Länge. Dann sind alle drei Dimensionen Null!

Theorem. *Es gilt*

$$s(M) = d_H(M) = \dim(M)$$

Wir sprechen einfach von der Dimension $\dim(M)$ *von* M*. Sie ist endlich.*

Folgerung. *Es gilt die absteigende Kettenbedingung für Primideale in einem lokalen Ring.*

Folgerung. *Seien* $x_1, \ldots, x_r$ *Elemente aus* $\mathfrak{m}$*, so daß* $M/(x)M$ *endlche Länge hat; das gilt z.B. , wenn diese Elemete ein Primärideal (zum maximalen Ideal) erzeugen. Dann ist* $\dim(M) \leq r$*.*

Beweis. Der Beweis des Theorems erfolgt durch *noethersche Indukton* :

Induktionsvoraussetzung: A enthalte von 0 und dem ganzen Ring verschiedene Ideale. Das Theorem sei bewiesen für alle Faktorringe $A/\mathfrak{a}$ nach einem von 0 und ganz A verschiedenes Ideal $\mathfrak{a}$; oder äquvilalent: es sei bewiesen für alle A-Moduln, die durch $\mathfrak{a}$ annuliert werden.

Induktionsschluß Dann gilt das Theorem auch für alle A-Moduln.

Induktionsanfang Das Theorem ist trivialerweise für Vektorräume über einem Körper, insbesondere für Moduln über dem Restklassenkörper $A/\mathfrak{m}$ bewiesen.

Erster Reduktionsschritt :
Reduktion auf den Fall $M = A$. O.B.d.A: Der Annulator von M ist Null. Sonst wäre die Behauptung für M wegen noetherscher Induktion schon bewiesen.

(1) Wegen $V(M) = W(Ann(M)) = W(0) = Spec(A)$ gilt

$$\dim(A) = \dim(M).$$

(2) Behauptung $s(M) = s(A)$.
Sei x ein System von Elementen aus $\mathfrak{m}$. Dann ist $M/(x)M$ genau dann von endlicher Länge, wenn $Ann(M) + (x) = (x)$ ein Primärideal ist, also wenn $A/(x)$ endliche Länge hat.

(3) Behauptung $d_H(M) = d_H(A)$.
Es gibt einen surjektiven Homomorphismus eines endlichen freien Moduls F auf M

$$F \twoheadrightarrow M$$

Also gilt $d_H(A) = d_H(F) \geq d_H(M)$.
Sei $M = Ax_1 + \cdots + Ax_n$. Weil der Annulator von M verschwindet hat man eine injektive Abbildung

$$\begin{array}{ccc} A & \hookrightarrow & M \times \cdots \times M. \\ a & \longmapsto & (ax_1, \ldots, ax_n) \end{array}$$

Also gilt auch $d_H(A) \leq d_H(M \times \cdots \times M) = d_H(M)$.

O.B.d.A könen wir nun annehmen $M = A$.

Zweiter Reduktionsschritt auf den Fall, daß A keine nilpotenten Elemente enthält.
Sei

$$\mathfrak{r} = \{a \in A | \exists n \; a^n = 0\}$$

das Nilradikal von A und $B = A/\mathfrak{r}$. Sei $\mathfrak{r} \neq 0$. Das Nilradikal ist in jedem Primideal enthalten.

(1)
$$\dim(A) = \dim(B).$$

(2)
$$s(A) = s(B)$$

Denn: Sei $x = \{x_1, \ldots, x_n\}$ $x_\nu \in \mathfrak{m}$. Dann ist $V(B/(x)B) = W(\mathfrak{r} + (x)) = W((x)) = V(A/(x))$. $A/(x)$ hat genau dann endliche Länge, wenn $B/(x)B$ endliche Länge hat.

(3)
$$d_H(A) = d_H(B)$$

Wir betrachten die kurze exakte Folge

$$0 \longrightarrow \mathfrak{r} \longrightarrow A \longrightarrow B \longrightarrow 0$$

Es gilt
$$d_H(A) = \sup(d_H(\mathfrak{r}), d_H(B))$$

Es gibt eine natürliche Zahl $s \geq 1$ mit $\mathfrak{r}^s \neq 0$, $\mathfrak{r}^{s+1} = 0$. Weil der Modul $\mathfrak{r}$ durch das Ideal $\mathfrak{r}^s \neq 0$ annuliert wird, gilt nach nötherscher Induktionsvoraussetzung

$$d_H(\mathfrak{r}) = \dim(\mathfrak{r}) \leq \dim(A) = \dim(B) = d_H(B)$$

Es folgt $d_H(A) = d_H(B)$.

O.B.d.A nehmen wir im folgenden an, daß $M = A$ und der Ring A reduziert ist, also keine nilpotenten Elemente enthält. Das Nullideal ist dann Durchschnitt der minimalen Primideale
$$0 = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_n.$$
Wir können annehmen, daß diese Ideale $\mathfrak{P}_\nu$ vom maximalen $\mathfrak{m}$ verschieden sind. Wir wählen ein Primideal $\mathfrak{P} = \mathfrak{P}_{\nu_0}$ aus mit

$$\dim(A) = \dim(A/\mathfrak{P})$$

Betrachte eine beliebig lange Kette von Primidealen

$$\mathfrak{P} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m \subseteq \mathfrak{m}$$

Wäre $\mathfrak{p}_1 \subseteq \bigcup_\nu \mathfrak{P}_\nu$, so folgte $\mathfrak{P} \subsetneq \mathfrak{p}_1 \subseteq \mathfrak{P}_{\nu_1}$. Widerspruch! Es gibt also ein Element

$$t \in \mathfrak{p}_1 \ , \ t \notin \bigcup_\nu \mathfrak{P}_\nu.$$

t ist Nichtnullteiler von A. Sei $B = A/tA$. Nach Induktionsvoraussetzung gilt

$$m - 1 \leq \dim(B) = d_H(B) \leq d_H(A) - 1,$$

und es folgt $m \leq d_H(A)$. Die Länge m einer betrachteten Kette ist also beschränkt. Wir können also eine Kette mit maximaler Länge $m = \dim(A)$ auswählen; dann gilt sogar

$$\dim(A) = \dim(B) + 1$$

Ferner gilt

$$s(A) \leq s(B) + 1$$
$$d_H(A) \geq d_H(B) + 1$$

und nach Induktionsvoraussetzung $\dim(B) = s(B) = d_H(B)$. Man erhält die Ungleichungen

$$s(A) \leq \dim(A) \leq d_H(A).$$

Wähle ein System $\{x_1, \ldots, x_r\}$ minimaler Länge $r = s(A)$ von Elementen, die ein Primärideal $(x) = \mathfrak{q}$ erzeugen. Es folgt $d_H(A) = deg(P_{\mathfrak{q}}(A, n)) \leq r = s(A)$. Aus den bewiesenen Resultaten folgen die gesuchten Gleichungen:

$$s(A) = \dim(A) = d_H(A).$$

□

Definition. Ein Elementsystem $x = \{x_1, \ldots, x_r\}$, $x_\nu \in \mathfrak{m}$ heißt Parametersystem des Moduls M, wenn $M/(x)M$ endliche Länge hat und wenn es minimal ist, d.h $r = \dim(M)$. Ein Elementfolge heißt Teil eines Parametersystems des Moduls M wenn sie in einem Parametersystem von M enthalten ist.

Offensichtlich gilt $\dim(M/(x_1, \ldots, x_\nu)M) = \dim(M) - \nu$ für $\nu \leq r$. Sei umgekehrt eine Elementfolge $y = \{y_1, \ldots, y_\nu\}$ von Elementen aus $\mathfrak{m}$ gegeben mit $\dim(M/(y)M) \leq \dim(M) - \nu$. Dann erhält man durch Hinzufügen eines Parametersystems von $M/(y)M$ ein Parametersystem von M.

Satz. *Sei $y = \{y_1, \ldots, y_\nu\}$ eine Elementfolge von Elementen aus dem maximalen Ideal von A. Genau dann ist y Teil eines Parametersystems des Moduls M, wenn gilt*

$$\dim(M/(y)M) \leq \dim(M) - \nu$$

Aus dieser Ungleichung folgt dann sogar die Gleichheit.

Satz. *Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ diejenigen in $V(M)$ minimalen Primideale mit $\dim(M) = dim A/\mathfrak{p}_\nu$. Gegeben sei ein Elemen t des maximalen Ideal von A. Genau dann ist t ein Parameter des Moduls $M \neq 0$, d.h. Teil eines Parametersystems von M, wenn gilt*

$$t \notin \bigcup_{\nu=1}^{s} \mathfrak{p}_\nu$$

Insbesondere ist t ein Parameter von M, wenn t ein Nichtnullteiler von M ist.

Folgerung. *Gegeben sei eine Folge* $\{t_1, \ldots, t_r\}$ *von Nichtnullteilern von* M*. D.h.: Die Elemente sind im maximalen Ideal enthalten und für* $1 \leq \nu \leq r$ *ist* t_ν *Nichtnullteiler von* $M/(t_1, \ldots, t_{\nu-1})M$*. Dann ist* $\dim(M/(t_1, \ldots, t_\nu)M) = \dim(M) - \nu$*. Ist insbesondere* $M/(t_1, \ldots, t_r)M$ *von endlicher Länge, so gilt*

$$\dim(M) = r$$

Definition und Satz. *Gegeben sei ein nicht unbedingt lokaler noetherscher Ring* A*, und sei* $M \neq 0$ *ein endlicher* A*-Modul. Die Dimension von* M *ist*

$$\dim(M) = \sup_{\mathfrak{m} \in V(M)\ ,\ \text{maximal}} \dim(M_{\mathfrak{m}}.)$$

Für ein Primideal $\mathfrak{p}$ *von* A *ist die Höhe* $\mathrm{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$*. Für ein beliebiges Ideal* $\mathfrak{a}$ *sind Höhe und Kohöhe definiert:*

$$\mathrm{ht}(\mathfrak{a}) = \inf_{\mathfrak{p} \in W(\mathfrak{a})} \mathrm{ht}(\mathfrak{p})$$
$$\mathrm{coht}(\mathfrak{a}) = \dim(A/\mathfrak{a})$$

Es gilt für ein Primideal $\mathfrak{p}$

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \leq \dim(A).$$

Wir schreiben auch statt der französischen Abkürzungen $\mathrm{ht}(), \mathrm{coht}()$ *einfach* $h(), coh()$*.*

Beispiele

Satz. *Sei* $A = k[T_1, \ldots, T_n]$ *ein Polynomring über dem Körper* k *und* $\mathfrak{m}$ *ein maximales Ideal. Dann ist*

$$\dim(A_{\mathfrak{m}}) = n$$

Für einen Faktorring B *dieses Polynomringes nach einem Primideal und ein maximales Ideal* $\mathfrak{m}$ *von* B *ist die Dimension* $\dim(B_{\mathfrak{m}})$ *der Transzendenzgrad des Quotientenkörpers von* B *über dem Körper* k*.*

Zum Beweis. Sei k algebraisch abgeschlossen. Dann wird das maximale Ideal durch eine Elementfolge $\{T_1 - a_1, \ldots, T_n - a_n\}$, $a_\nu \in k$ erzeugt. Diese Elementfolge ist eine Nichtnullteilerfolge von $A_{\mathfrak{m}}$. Der allgemeine Fall kann mit Hilfe von Grundkörpererweiterung und mit den Sätzen von Cohen-Seidenberg auf den speziellen zurückgeführt werden. Der zweite Teil des Satzes kann mit Hilfe des noetherschen Normalisierungssatzes und mit Hilfe der Sätze von Cohen-Seidenberg bewiesen werden. □

XII Die Homologische Kodimension

Cohen-Macaulay Moduln und Ringe

Im folgenden ist A ein nötherscher lokaler Ring mit dem maximalen Ideal $\mathfrak{m}$ und dem Restlassenkörper k. Sei $M \neq 0$ ein endlicher A-Modul. Ein Nichtnullteiler a von M ist ein Element aus dem maximalen Ideal, für das die Multiplikation mit a

$$M \xrightarrow{a} M$$

injektiv ist.

Definition. Eine Folge $x_1, \ldots, x_m$ von Elementen aus dem maximalen Ideal $\mathfrak{m}$ heißt M-Folge der Länge m, wenn für $1 \leq i \leq m$ das Element x_i Nichtnullteiler von $M_{i-1} = M/(x_1, \ldots, x_{i-1})M$ ist. Dabei ist $M_0 = M$. Die M-Folge heißt maximal, wenn sie sich nicht verlängern läßt. Das bedeutet, daß M_m keinen Nichtnullteiler besitzt.

Die Folge $x_{i+1}, \ldots, x_m$ ist dann eine M_i-Folge bzw. eine maximale M_i-Folge. Die leere Folge ist genau dann eine maximale M-Folge, wenn M keinen Nichtnullteiler besitzt, oder äquvivalent dazu, wenn das maximale Ideal $\mathfrak{m}$ assoziert zu M ist. Aus der Dimensionstheorie folgt mit Hilfe der Chevalley-Dimension, daß gilt:

$$dim(M_i) = dim(M) - i$$

Definition. Die Tiefe oder die homologische Kodimension $t(M) = codh(M)$ von M ist das Supremum aller natürlichen Zahlen r mit

$$Ext^{\nu}_A(k, M) = 0 \text{ für } \nu < r$$

Ein Modul endlicher Länge besitzt eine Kompositionsreihe, deren Faktoren isomorph zu k sind. Man folgert leicht:

Anmerkung zur Definition der Tiefe. *Sei l ein von Null verschiedener Modul endlicher Länge. Dann ist $t(M)$ das Supremum aller natürlichen Zahlen r mit*

$$Ext^{\nu}_A(l, M) = 0 \text{ für } \nu < r$$

Lemma.

(1) *Genau dann verschwindet $t(M)$, wenn $\mathfrak{m} \in Ass(M)$ oder äquivalent, wenn M keinen Nichtnullteiler besitzt.*
(2) *Sei a ein Nichtnullteiler von M. Dann gilt $t(M/aM) = t(M) - 1$.*

Beweis.

(1) $t(M) = 0$ bedeutet $Hom_A(k, M) \neq 0$. Ein nichtverschwindender Homomorphismus von k in M ist eine Injektion $k = A/\mathfrak{m} \hookrightarrow M$; die Existenz dieser Injektion bedeutet aber $\mathfrak{m} \in Ass(M)$.

(2) Es gilt $t(M) \geq 1$. Die Multiplikationsabbildung $k \xrightarrow{a} k$ ist die Nullabbildung. Diese Multiplikationsabbildung induziert aber die Multiplikationsabbildung

$$Ext^i_A(k,M) \xrightarrow{a} Ext^i_A(k,M).$$

Also folgt $aExt^i_A(k,M) = 0$. Die Multiplikationsabbildung $M \xrightarrow{a} M$ induziert ebenfalls die Multiplikationsabbildung $Ext^i_A(k,M) \xrightarrow{a} Ext^i_A(k,M)$, also die Nullabbildung. Man betrachte zu der kurzen exakten Folge

$$0 \longrightarrow M \xrightarrow{a} M \longrightarrow N = M/aM \longrightarrow 0$$

die lange exakte Kohomologiesequenz

$$\cdots \to Ext^i_A(k,M) \xrightarrow{0} Ext^i_A(k,M) \to Ext^i_A(k,N) \to Ext^{i+1}_A(k,M) \xrightarrow{0} \ldots$$

Diese zerfällt in kurze exakte Folgen

$$0 \to Ext^i_A(k,M) \to Ext^i_A(k,N) \to Ext^{i+1}_A(k,M) \to 0$$

Man erhält

$$Ext^i_A(k,N) \cong Ext^{i+1}_A(k,M) \;\; \forall i \leq t(M) - 1$$

Es folgt die Behauptung.

□

Aus diesem Lemma folgert man durch vollständige Induktion

Satz. *Sei $x_1, \ldots, x_n$ eine maximale M-Folge. Dann gilt*

$$t(M) = n$$

Insbesondere sind die Längen aller maximalen M-Folgen eines – von Null verschiedenen – Moduls M gleich. Es gilt die Abschätzung

$$t(M) \leq dim(M)$$

Lemma. *Sei $\mathfrak{p}$ ein assoziiertes Primideal von M. Dann gilt*

$$t(M) \leq dim(A/\mathfrak{p})$$

Beweis. Wir führen den Beweis durch vollständige Induktion nach der Tiefe von M. Wir können annehmen, daß $t(M) > 0$ ist. Sei a ein Nichtnullteiler von M und $N = M/aM$. Weil $\mathfrak{p}$ assoziiert zu M ist, gibt es eine Injektion $A/\mathfrak{p} \hookrightarrow M$. Das Bild von 1 sei das Element $u \neq 0$ von M. Dann ist $\mathfrak{p}$ der Annulator $Ann(u)$ von u. Wegen $\bigcap_{\nu>0} a^\nu M = 0$ gibt es ein Element $w \in M$ und eine natürliche Zahl $n \geq 0$ mit

$$u = a^n w \text{ und } w \notin aM$$

Der Annulator von w ist ebenfalls $\mathfrak{p}$. Man ersetze u gegebenenfalls durch w und kann dann o.B.d.A. annehmen, daß das Bild von $A/\mathfrak{p}$ nicht in aM enthalten ist. Dann ist das Bild B von $A/\mathfrak{p}$ in N von Null verschieden. $\mathfrak{p}$ und a annulieren B; also ist $\mathfrak{p} + Aa$ im Annulator von B, damit in jedem assoziierten Primideal von B enthalten. Wähle ein Primideal $\mathfrak{P} \in Ass(B) \subseteq Ass(N)$. Da der Nichtnullteiler a von M nicht im assoziierten Primideal $\mathfrak{p}$ von M enthalten sein kann gilt

$$\mathfrak{p} \subsetneq \mathfrak{p} + Aa \subseteq \mathfrak{P}.$$

Es gilt $dim(A/\mathfrak{P}) \leq dim(A/\mathfrak{p}) - 1$ und nach Induktionsvoraussetzung $t(M) - 1 = t(N) \leq dim(A/\mathfrak{P})$. Es folgt die Behauptung des Satzes für M und $\mathfrak{p}$.

Definition. Ein – endlicher – A-Modul M heißt Cohen-Macaulay Modul, wenn er verschwindet, oder wenn gilt: $t(M) = dim(M)$. Der Ring A heißt Cohen-Macaulay Ring, wenn A als A-Modul Cohen-Macaulay Modul ist.

Bemerkung. Wird der Modul M durch das Ideal $\mathfrak{a}$ von A annuliert, so ist M auf natürliche Weise auch Modul über dem Faktorring $B = A/\mathfrak{a}$. Die Tiefe von M als A-Modul stimmt dann mit der Tiefe von M als B-Modul überein, weil die Tiefe die Länge einer maximalen M-Folge ist. Insbesondere ist M genau dann ein Cohen-Macaulay Modul über A, wenn M ein Cohen-Macaulay Modul über dem Ring B ist.

Folgerung. *Sei M ein Cohen-Macaulay Modul und $\mathfrak{p} \in Ass(M)$. Dann ist $\mathfrak{p}$ minimal in $Ass(M)$, damit auch minimal in $V(M)$. Es gilt $dim(M) = dim(A/\mathfrak{p})$.*

Folgerung. *Sei M ein Cohen-Macaulay Modul und die Folge $a_1, \ldots, a_r$ Teil eines Parametersystems von M. Dann ist $a_1, \ldots, a_r$ eine M-Folge.*

Beweis. Sei $a \in \mathfrak{m}$ ein Parameter von M, also $dim(M/aM) = dim(M) - 1$. Wenn a ein Nullteiler von M ist, gibt es ein zu M assoziiertes Primideal $\mathfrak{p}$ mit $a \in \mathfrak{p}$. Dann ist $\mathfrak{p} \in V(M) \cap W((a)) = V(M/aM)$ und $dim(M/aM) \geq dim(A/\mathfrak{p}) = dim(M)$. Das ist ein Widerspruch; also ist jeder Parameter von M ein Nichtnullteiler von M. Der Beweis der Folgerung ergibt sich jetzt durch Induktion. $\square$

Lemma. *Sei M sei ein Cohen-Macaulay Modul und $\mathfrak{p} \in V(M)$. Dann gibt es eine M-Folge $x_1, \ldots, x_r \in \mathfrak{p}$, so daß $\mathfrak{p}$ minimal in $V(M/M/(x_1, \ldots, x_r)M)$ ist, insbesondere zu $Ass(M/(x_1, \ldots, x_r)M)$ gehört.*

Beweis. Sei $x_1, \ldots, x_r \in \mathfrak{p}$ eine M-Folge, die sich nicht durch ein Element aus $\mathfrak{p}$ zu einer M-Folge verlängern läßt. Dann ist $\mathfrak{p} \subseteq \bigcup_{\mathfrak{P} \in Ass(M/(x_1,\ldots,x_r)M)} \mathfrak{P}$. Es gibt dann ein Primideal $\mathfrak{P} \in Ass(M/(x_1, \ldots, x_r)M)$, das $\mathfrak{p}$ enthält. Es gilt $\mathfrak{p} \in V(M) \cap W((x_1, \ldots, x_r)) = V(M/(x_1, \ldots, x_r)M)$. Da $M/(x_1, \ldots, x_r)M$ Cohen-Macaulay ist, ist $\mathfrak{P}$ minimal in $V(M/(x_1, \ldots, x_r)M)$. Also ist $\mathfrak{p} = \mathfrak{P}$. $\square$

Es gilt dann offenbar $dim(M) - r = dim(M/(x_1, \ldots, x_r)M) = dim(A/\mathfrak{p})$. Außerdem ist das maximale Ideal $\mathfrak{p}A_\mathfrak{p}$ von $A_\mathfrak{p}$ ein minimales assoziiertes Ideal von

$$(M/(x_1, \ldots, x_r)M)_\mathfrak{p},$$

damit $(M/(x_1, \ldots, x_r)M)_\mathfrak{p}$ ein $A_\mathfrak{p}$-Modul endlicher Länge und $x_1, \ldots, x_r$ eine maximale $M_\mathfrak{p}$-Folge. Also ist $dim(M_\mathfrak{p}) = r$ und der $A_\mathfrak{p}$-Modul $M_\mathfrak{p}$ Cohen-Macaulay. Ist das Primideal $\mathfrak{p}$ nicht in $V(M)$ enthalten, so verschwindet $M_\mathfrak{p}$, ist also ebenfalls Cohen-Macaulay.

Folgerung. *Sei M ein Cohen-Macaulay Modul und $\mathfrak{p}$ ein Primideal von A. Dann ist der $A_\mathfrak{p}$-Modul $M_\mathfrak{p}$ ein Cohen-Macaulay Modul. Wenn $\mathfrak{p}$ in $V(M)$ enthalten ist, gilt*

$$dim(M) = dim(M_\mathfrak{p}) + dim(A/\mathfrak{p})$$

Sei $\mathfrak{p}$ ein Primideal von A. Dann bezeichnen wir mit $h(p) = dim(A_\mathfrak{p})$ die Höhe von $\mathfrak{p}$ und mit $ch(\mathfrak{p}) = dim(A/\mathfrak{p})$ die Kohöhe von $\mathfrak{p}$.

Folgerung. *Sei A ein Cohen-Macaulay Ring und $\mathfrak{p}$ ein Primideal von A. Dann gilt*

$$h(\mathfrak{p}) + ch(\mathfrak{p}) = dim(A)$$

Sei $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \cdots \subsetneq \mathfrak{p}_n$ eine maximale Kette von Primidealen von A, d.h. eine Kette von Primidealen $\mathfrak{p}_\nu$, die sich nicht verlängern läßt. Dann gilt

$$dim(A) = n$$

Sei $B = A/\mathfrak{a}$ ein Faktorring von A nach einem Ideal $\mathfrak{a} \neq A$, für das alle minimalen Ideale in $W(\mathfrak{a})$ gleiche Höhe haben. Dann gelten die beiden vorhergehenden Aussagen für A allgemeiner auch für B.

Beweis der Behauptung über maximale Ketten von Primidealen von A durch Induktion nach der Länge n der Kette. Wegen der Maximalität ist $\mathfrak{p}_n = \mathfrak{m}$ das maximale Ideal von A.

$$dim(A) = dim(A_{\mathfrak{p}_{n-1}}) + dim(A/\mathfrak{p}_{n-1}) = n - 1 + 1 = n$$

□

Beispiel. Sei $A = k[X_1, \ldots, X_n]$ ein Polynomring über dem Körper k und $\mathfrak{p}$ ein Primideal von A. Dann ist $A_\mathfrak{p}$ ein Cohen-Macaulay Ring.

Die Behauptung ist richtig für ein maximales Ideal der Form

$$\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n),$$

damit auch für ein Primideal $\mathfrak{p}$, das in einem solchen maximalen Ideal enthalten ist, weil dann $A_\mathfrak{p}$ Lokalisierung von $A_\mathfrak{m}$ ist. Im Fall eines algebraisch abgeschlossenen Grundkörpers ist dann alles gezeigt. Der allgemeine Fall kann durch Grundkörpererweiterung auf diesen zurückgeführt werden:

Sei $\mathfrak{n}$ ein maximales Ideal von A. Dann gibt es eine endliche Körpererweiterung K von k und ein maximales Ideal von $B = K[X_1, \ldots, X_n]$ der Form

$$\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n),$$

das über $\mathfrak{n}$ liegt. $B_\mathfrak{m}$ ist flach über $A_\mathfrak{n}$; der Funktor $\otimes_{A_\mathfrak{n}} B_\mathfrak{m}$ ist also exakt. Außerdem ist $B_\mathfrak{m}$ treuer $A_\mathfrak{n}$-Modul; ein $A_\mathfrak{n}$-Modul M verschwindet genau dann, wenn $M \otimes_{A_\mathfrak{n}} B_\mathfrak{m}$ veschwindet. Sei $h = A/\mathfrak{n}$ der Restklassenkörper von $A_\mathfrak{n}$. Dann ist $l = h \otimes_{A_\mathfrak{n}} B_\mathfrak{m}$ ein nichtverschwindender $B_\mathfrak{m}$-Modul endlicher Länge, und man zeigt

$$Ext^\nu_{A_\mathfrak{n}}(h, A_\mathfrak{n}) \otimes_{A_\mathfrak{n}} B_\mathfrak{m} = Ext^\nu_{B_\mathfrak{m}}(l, B_\mathfrak{m})$$

Es folgt, daß gilt

$$t(A_\mathfrak{n}) = t(B_\mathfrak{m}) = n$$

Da die Dimension der beiden Ringe nach Cohen-Seidenberg übereinstimmt ist auch $A_\mathfrak{n}$ ein Cohen-Macaulay Ring.

Später werden wir zeigen, daß der Polynomring A sogar *regulär* ist. Daraus folgt auch, daß alle Lokalisierungen Cohen-Macaulay sind.

XIII Die homologische Dimension von Moduln und Ringen

Im folgenden sei A ein (nötherscher) lokaler Ring, $\mathfrak{m}$ sein maximales Ideal; sein Restklassenkörper sei $k = A/\mathfrak{m}$.

Die injektive homologische Dimension.

Zur Wiederholung: Ein Modul I heißt *injektiv* , wenn sich jeder Homomorphismus von einem Untermodul eines Moduls M in I zu einem Homomorphismus von ganz M in I fortsetzen läßt. Man zeigt dann mit Hilfe schrittweiser Fortsetzung und mit transfiniter Induktion, daß es genügt, diese Bedingung nur für Untermoduln von $M = A$, also Ideale zu fordern.

Satz 13.1 *Ein A-Modul M ist genau dann injektiv, wenn eine der folgenden äquivalenten Eigenschaften erfüllt ist:*

(1) $\mathrm{Ext}^i_A(X, M) = 0 \qquad \forall i > 0 \qquad \forall$ *A-Moduln X.*

(2) $\mathrm{Ext}^1_A(X, M) = 0 \qquad\qquad\quad \forall$ *endlichen A-Moduln X.*

Beweis:
(2) $\Longrightarrow$ M ist injektiv: Sei $\mathfrak{a}$ ein Ideal von A und $X = A/\mathfrak{a}$. Wir betrachten die kurze exakte Folge

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow X \longrightarrow 0$$

und die zugehörige lange exakte Kohomologiesequenz

$$0 \to \mathrm{Hom}(X, M) \to \mathrm{Hom}(A, M) \to \mathrm{Hom}(\mathfrak{a}, M) \to \mathrm{Ext}^1(X, M) = 0 \to \cdots$$

Der Homomorphismus

$$\mathrm{Hom}(A, M) \to \mathrm{Hom}(\mathfrak{a}, M)$$

ist also für alle Ideale $\mathfrak{a}$ surjectiv; d.h jeder Homomorphismus

$$\mathfrak{a} \longrightarrow M$$

läßt sich zu einem Homomorphismus

$$A \longrightarrow M$$

fortsetzen. Damit ist M injektiv.

Sei

$$M \to I^0 \to I^1 \to \cdots$$

eine Auflösung von M durch injektive Moduln I^j. Diese Auflösung hat die Länge $\leq n$, wenn $I^j = 0$ für $j > n$. Dabei ist n eine natürliche Zahl ≥ 0 oder ∞. Ist $n \neq \infty$, so schreiben wir für diese Auflösung auch

$$M \to I^0 \to I^1 \to \cdots \to I^n \to 0.$$

Definition 13.2 *Sei $M \neq 0$ ein A-Modul. Wir definieren die injektive homologische Dimension* $\mathrm{dih}_A(M)$ *von M durch:*

$$\mathrm{dih}_A(M) = \inf_{\text{M besitzt eine injektive Auflösung der Länge} \leq n} n$$

Sei J ein injektiver Modul und

$$0 \longrightarrow M \longrightarrow J \longrightarrow B \longrightarrow 0$$

eine kurze exakte Folge. Es gilt für einen beliebigen Modul X

$$\mathrm{Ext}^i_A(X, J) = 0 \quad i > 0.$$

Durch Auswerten der langen Kohomologiesequenz erhält man:

$$\mathrm{Ext}^i_A(X, M) \cong \mathrm{Ext}^{i-1}_A(X, B) \quad i > 1.$$

Allgemeiner sei eine exakte Folge

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^n \to K \to 0$$

mit injektiven Moduln I^ν gegeben. Durch injektives Auflösen von K erhält man daraus eine injektive Auflösung von M. Diese exakte Folge kann in kurze exakte Folgen zerlegt werden:

$$0 \to M \to I^0 \to B^1 \to 0$$

$$0 \to B^1 \to I^1 \to B^2 \to 0$$

$$\vdots$$

$$0 \to B^n \to I^n \to K \to 0.$$

B^i ist das Bild von I^{i-1} in I^i. Durch mehrfache Anwendung der vorhergehenden Überlegung erhält man:

Lemma 13.3 *Mit den vorhergehenden Bezeichnungen gilt:*

$$\mathrm{Ext}^i_A(X, M) \cong \mathrm{Ext}^{i-n-1}_A(X, B) \quad i > n + 1.$$

Mit Hilfe von Satz 13.1 und Lemma 13.3 erhält man:

Satz 13.4 *Sei $M \neq 0$ ein A-Modul,$n > 0$. Folgende Aussagen sind äquivalent:*

(1) $\quad \dim_A < n$

(2) $\quad \mathrm{Ext}^i_A(X, M) = 0 \qquad \forall i \geq n \qquad \forall \quad A - Moduln\ X$

(3) $\quad \mathrm{Ext}^n_A(X, M) = 0 \qquad\qquad\quad \forall \quad endlichen\ A - Moduln\ X$

(4) Für jede exakte Folge

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^{n-2} \to K \to 0$$

mit injektiven Moduln I^ν ist auch K injektiv.

Satz 13.5 *Sei M ein endlicher A-Modul, $n \geq 0$ eine natürliche Zahl. Folgende Eigenschaften sind äquivalent.*

(1) $\quad \dim_A(M) \leq n.$

(2) $\quad \mathrm{Ext}^i_A(k, M) = 0 \qquad \forall i > n.$

Beweis: (2) sei erfüllt. Wir zeigen für alle endlichen A-Moduln X durch Induktion nach $\dim(X)$:

$$\mathrm{Ext}^i_A(X, M) = 0 \ i > n.$$

Erster Fall:

$$X \cong A/\mathfrak{p}, \mathfrak{p} \text{ Primideal.}$$

Sei $X \ncong k$, also $\dim(X) > 0$. Dann gibt es einen Nichtnullteiler a von X. Sei $Y = X/aX$. $\dim(Y) <$dim(X). Wir betrachten zur kurzen exakten Folge

$$0 \longrightarrow X \xrightarrow{a} X \longrightarrow Y \longrightarrow 0$$

die lange Kohomologiesequenz

$$\cdots \longrightarrow \mathrm{Ext}^i_A(X, M) \xrightarrow{a} \mathrm{Ext}^i_A(X, M) \longrightarrow \mathrm{Ext}^{i+1}_A(Y, M) \longrightarrow \cdots .$$

Nach Induktionsvoraussetzung gilt:

$$\mathrm{Ext}^i_A(Y, M) = 0 \ i > n.$$

Also ist für $i > n$

$$\mathrm{Ext}^i_A(X, M) = a\mathrm{Ext}^i_A(X, M).$$

Weil M und X nöthersch sind, ist auch $\mathrm{Ext}^i_A(X, M)$ noethersch. Nach dem Lemma von Nakayama ist also

$$\mathrm{Ext}^i_A(X, M) = 0 \quad i > n.$$

Allgemeiner Fall: Zu einem endlichen Modul $X \neq 0$ gibt es eine Kette von Untermoduln

$$0 = X_0 \subset X_1 \subset X_2 \cdots \subset X_r = X$$

und Primideale $\mathfrak{p}_j$ mit

$$F_j = X_j/X_{j-1} \cong A/\mathfrak{p}_j \;\; j = 1 \cdots r.$$

Es gilt

$$\dim(F_j) \leq \dim(X).$$

Wir können nach Teil 1 des Beweises annehmen:

$$\mathrm{Ext}^i_A(F_j, M) = 0 \quad i > n.$$

Wir betrachten zu den kurzen exakten Folgen

$$0 \longrightarrow X_{j-1} \longrightarrow X_j \longrightarrow F_j \longrightarrow 0$$

die zugehörigen langen exakten Kohomologiesequenzen und erhalten

$$\mathrm{Ext}^i_A(X_j, M) = 0 \quad i > n \quad j = 1 \cdots .r$$

Die projektive homologische Dimension.

Dual zur injektiven homologischen Dimension wird die projektive homologische Dimension eines Moduls mit Hilfe projektiver an Stelle injektiver Auflösungen erklärt. Viele Schlußweisen sind ähnlich.

Satz 13.6 *Äquivalent sind folgende Aussagen über einen A-Modul M:*

(1) M ist projektiv.

(2) $\mathrm{Ext}^i_A(M, X) = 0 \qquad \forall i > 0 \qquad \forall$ *A-Moduln X.*

(3) $\mathrm{Ext}^1_A(M, X) = 0 \qquad \forall$ *A-Moduln X.*

Ist M nöthersch so sind zu diesen beiden Aussagen drei weitere äquivalent:

(4) $\mathrm{Ext}^1_A(M, X) = 0 \qquad \forall$ *endlichen* $A -$ *Moduln X.*

(5) $\mathrm{Tor}^A_1(M, k) = 0.$

(6) M ist frei.

Beweis: (5) $\Longrightarrow$ (6). Sei M ein endlicher A-Modul, und seien $m_1, \cdots, m_n \in M$ Elemente, deren Bilder im k-Vektorraum $M \otimes_A k = M/mM$ eine Basis bilden. Nach dem Lemma von Nakayama erzeugen die Elemente $m_1, \cdots, m_n \in M$ den A-Modul M. Sei

$$F = A^n = Ae_1 \oplus \cdots \oplus Ae_n$$

der freie A-Modul vom Rang n mit den "Basiselementen" $e_1, \cdots, e_n$. Der Homomorphismus

$$F \longrightarrow M$$

$$e_i \longmapsto m_i$$

ist surjectiv, der induzierte Homomorphismus $F/\mathfrak{m}F \longrightarrow M/\mathfrak{m}M$ von k-Vektorräumen ein Isomorphismus . Sei K sein Kern.Wir betrachten die kurze exakte Folge

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

und die zugehörige lange exakte Homologiesequenz

$$\cdots \to \ \mathrm{Tor}_1^A(M,k) = 0 \to K/\mathfrak{m}K \to F/\mathfrak{m}F \stackrel{\cong}{\to} M/\mathfrak{m}M \to 0.$$

Es folgt, daß $K/\mathfrak{m}K$ verschwindet und damit nach dem Lemma von Nakayama auch der endliche A-Modul K. Deshalb ist der Homomorphismus

$$F \longrightarrow M$$

ein Isomorphismus.

Sei

$$\cdots \to P_1 \to P_0 \to M$$

eine Auflösung von M durch projektive Moduln P_j. Diese Auflösung hat die *Länge* $\leq n$, wenn $P_j = 0$ für $j > n$. Dabei ist n eine natürliche Zahl ≥ 0 oder ∞.

Definition 13.7 *Sei $M \neq 0$ ein A-Modul. Wir definieren die (projektive) homologische Dimension* $\mathrm{dh}_A(M)$ *von M durch:*

$$\mathrm{dh}_A(M) = \inf_{\text{M besitzt eine projektive Auflösung der Länge} \leq n} n$$

Ähnlich wie Lemma 13.3 beweist man:

Lemma 13.8 *Gegeben sei eine exakte Folge*

$$0 \to K \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

mit projektiven Moduln P_ν. Dann gilt für jeden A-Modul X:

$$\begin{aligned} \mathrm{Ext}_A^i(M,X) &\cong \mathrm{Ext}_A^{i-n}(K,X) \\ \mathrm{Tor}_i^A(M,X) &\cong \ \mathrm{Tor}_{i-n}^A(K,X) \end{aligned} \qquad i > n.$$

Bemerkung: Ist M nöthersch, so gibt es zu $n \geq 0$ immer eine solche exakte Folge mit endlichen Moduln P_ν, K.

Ähnlich wie Satz 13.4 im injektiven Fall beweist man mit Hilfe von Satz 13.6 und Lemma 13.8:

Satz 13.9 *Sei M ein von 0 verschiedener A-Modul. Äquvivalent sind folgende Aussagen:*

(1) $\mathrm{dh}_A(M) < n$

(2) $\mathrm{Ext}_A^i(M,X) = 0 \qquad \forall i \geq n \qquad \forall$ *A-Moduln X.*

(3) $\mathrm{Ext}_A^n(M,X) = 0 \qquad \forall$ *A-Moduln X.*

(4) Für jede exakte Folge

$$0 \to K \to P_{n-2} \to \cdots \to P_1 \to P_0 \to M \to 0$$

mit projektiven Moduln P_ν ist auch K projektiv.

Ist M nöthersch, so sind zwei weitere Aussagen zu diesen äquvivalent:

(5) $\mathrm{Ext}_A^n(M,X) = 0 \qquad \forall$ *endlichen A-Moduln X.*

(6) $\mathrm{Tor}_n^A(M,k) = 0.$

Definition 13.10 *Die globale homologische Dimension eines Ringes A:*

$$\mathrm{gldh}(A) = \sup_{M\,A-\mathrm{Modul}} \mathrm{dh}(M).$$

Satz 13.11 *Folgende Aussagen sind äquivalent:*

(1) $\operatorname{gldh}(A) < n.$

(2) $\operatorname{dih}_A(X) < n \quad \forall \quad A-$ *Moduln* $X.$

(3) $\operatorname{dih}(X) < n \quad \forall \quad$ *endlichen* $A-$ *Moduln* $X.$

(4) $\operatorname{Tor}_n^A(k,k) = 0.$

Beweis: (4)$\Longrightarrow \operatorname{dh}(k) < n \Longrightarrow \operatorname{Ext}_A^i(k,X) = 0 \; \forall i \geq n \; \forall \; A-$Moduln $X \Longrightarrow$ (3) $\Longrightarrow$ $\operatorname{Ext}_A^n(M,X) = 0 \quad \forall \; A-$ Moduln $M \; \forall$ endlichen $\; A-$ Moduln $X \Longrightarrow \operatorname{dh}_A(M) <$ $n \; \forall$ endlichen $A-$Moduln $M \Longrightarrow \operatorname{Ext}_A^n(M,X) = 0 \; \forall$ endlichen A-Moduln $M \; \forall \; A-$ Moduln $X \Longrightarrow$ (2) $\Longrightarrow$ (1).

Aufgaben:

Sei $\mathfrak{p}$ *ein Primideal von* A*, sei* M *ein* A*-Modul und* N *ein* $A_\mathfrak{p}$*-Modul. Sei* $\mathbb{Z}$ *der Ring der ganzen Zahlen und* $\mathfrak{q}$ *ein Primideal von* $\mathbb{Z}$*. Zeige:*

(1) $\operatorname{dih}_{A_\mathfrak{p}}(M_\mathfrak{p}) \leq \operatorname{dih}_A(M).$

(2) $\operatorname{dih}_{A_\mathfrak{p}}(N) = \operatorname{dih}_A(N).$

(3) $\operatorname{dh}_{A_\mathfrak{p}}(M_\mathfrak{p}) \leq \operatorname{dh}_A(M).$

(4) $\operatorname{gldh}(A_\mathfrak{p}) \leq \operatorname{gldh}(A).$

(5) $\operatorname{gldh}(\mathbb{Z}_\mathfrak{q}) = \dim(\mathbb{Z}_\mathfrak{q}).$

XIV Gorensteinringe.

Gorensteinringe spielen eine Rolle in der Dualitätstheorie für die Kohomologiegruppen kohärenter Garben auf einem vollständigen Schema über einem Körper. Genau dann ist der dualisierende Komplex –bis auf Verschiebung– ein Geradenbündel, wenn alle lokalen Ringe der Strukturgarbe Gorensteinringe sind.

Wie im vohergehenden Abschnitt sei A ein (nötherscher) lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper $k = A/\mathfrak{m}$.

Definition 2.0 *Der Ring A heißt Gorensteinring, wenn gilt:*

$$\mathrm{dih}_A(A) < \infty.$$

Ein Primärideal $\mathfrak{q} \subseteq \mathfrak{m}$ zum maximalen Ideal $\mathfrak{m}$ heißt *irreduzibel,* wenn gilt:

$$\mathfrak{q} = \mathfrak{a} \cap \mathfrak{b} \quad \mathfrak{a}\ ,\ \mathfrak{b} \subseteq \mathfrak{m} \ \text{ Ideale } \Longrightarrow \mathfrak{q} = \mathfrak{a} \vee \mathfrak{q} = \mathfrak{b}.$$

Ziel dieses Paragraphen ist es, folgenden Satz zu beweisen:

Theorem 14.1 *Sei A ein Gorensteinring. Dann ist A ein Cohen-Maccauly-Ring. Jedes von einem Parametersystem, d.h. von einer maximalen A-Folge erzeugte Ideal ist irreduzibel.*

Umkehrung: Sei A ein Cohen-Maccauly-Ring und erzeuge ein Parametersystem ein irreduzibles Primärideal. Dann ist A ein Gorensteinring.

Für einen Gorensteinring gilt:

$$\mathrm{dih}_A(A) = \dim(A).$$

Wir behandeln zuerst den Fall $\dim(A) = 0$.

Lemma 14.3 *Sei A ein Gorensteinring mit* $\mathrm{codh}(A) = 0$. *Dann gilt:*

$$\mathrm{dih}_A(A) = 0.$$

Beweis: Sei $\mathrm{dih}_A(A) = n > 0$. Wegen $\mathrm{codh}(A) = 0$ enthält A einen zu k isomorphen Untermodul. Es gibt also eine kurze exakte Folge

$$0 \longrightarrow k \longrightarrow A \longrightarrow M \longrightarrow 0.$$

Wir betrachten die zugehörige lange exakte Kohomologiesequenz:

$$\cdots \longrightarrow \mathrm{Ext}^n_A(A, A) = 0 \longrightarrow \mathrm{Ext}^n_A(k, A) \longrightarrow \mathrm{Ext}^{n+1}_A(M, A) = 0 \longrightarrow \cdots$$

und erhalten:

$$\mathrm{Ext}^n_A(k, A) = 0.$$

Nach Satz 12.5 ist also $\mathrm{dih}_A(A) \leq n - 1$. Widerspruch!

Sei $\dim(A) = 0$. Dann ist $\mathfrak{m} \in \mathrm{Ass}(A)$ und $V = \mathrm{Hom}_A(k, A) = \{a \in A; \mathfrak{m}a = 0\}$ ein von Null verschiedener Vektorraum über dem Restklassenkörper k. $\dim_k(V)$ bezeichnet die *Vektorraumdimension* von V, nicht die Krullsche Dimension $\dim(V)$ des A-Moduls V.

Lemma 14.4 *Sei* $\mathrm{dih}_A(A) = 0$. *Dann gilt:*

$$\dim(A) = 0$$
$$\mathrm{Hom}_A(k, A) \cong k.$$

Beweis: Sei $\dim(A) > 0$. Dann gibt es ein Primideal $\mathfrak{p} \neq \mathfrak{m}$ in $\mathrm{Ass}(A)$. Sei $M = A/\mathfrak{p}$, $s \in \mathfrak{m}$ ein Element, das nicht in $\mathfrak{p}$ enthalten ist, S die von s erzeugte multiplikative Menge und $N = M_S$. Weil $\mathfrak{p}$ assoziert zu A ist, gibt es einen injektiven Homomorphismus

$$M \longrightarrow A.$$

Weil A injektiv ist, läßt er sich fortsetzen zu einem Homomorphismus

$$N \longrightarrow A.$$

Dieser muß ebenfalls injektiv sein. Der A-Untermodul N von A ist deshalb nöthersch. Anderseits enthält N eine unendliche aufsteigende Kette von Untermoduln:

$$M \subset \frac{M}{s} \subset \frac{M}{s^2} \subset \cdots \subset N.$$

Widerspruch!

Sei $V = \mathrm{Hom}_A(k, A) \cong k^n$, $n > 0.V \subseteq A$. Dann gibt es eine k-lineare Abbildung $V \longrightarrow V \subseteq A$, die verschieden ist von der Multiplikation mit einem Element aus $k = A/\mathfrak{m}$. Diese Abbildung wird aufgefaßt als ein A-Homomorphismus

$$V \longrightarrow A,$$

läßt sich also fortsetzen zu einem A-Homomorphismus

$$f : A \longrightarrow A.$$

Ein solcher Homomorphismus ist aber die Multiplikationsabbildung mit dem Element $a = f(1)$. Widerspruch!

Lemma 14.5 *Sei* $\dim(A) = 0$ $V = \mathrm{Hom}_A(k, A)$. *Folgende Aussagen sind äquivalent:*

(1) $\dim_k(V) = 1$.

(2) 0 *ist ein irreduzibles Ideal.*

Satz 14.6 *Gorensteinringe der Dimension 0. Äquivalent sind folgende Eigenschaften:*

(1) $\operatorname{dih}_A(A) = 0.$

(2) $\dim(A) = 0. \quad \dim_k(\operatorname{Hom}_A(k, A)) = 1.$

(3) $\dim(A) = 0. \quad 0$ *ist ein irreduzibles Ideal in* $A.$

Solche Gorensteinringe der Dimension 0 nennt man auch Quasifrobeniusringe.
Beweis: (2) $\Longrightarrow$ (1) : Jeder endliche A-Modul M hat enliche Länge $\ell(M)$. Sei

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

eine kurze exakte Folge solcher Moduln.Dann ist die Folge

$$0 \longrightarrow \operatorname{Hom}_A(W, A) \longrightarrow \operatorname{Hom}_A(V, A) \longrightarrow \operatorname{Hom}_A(U, A)$$

auch exakt und es gilt:

$$\ell(U) + \ell(W) = \ell(V)$$

$$\ell(\operatorname{Hom}_A(U, A)) + \ell(\operatorname{Hom}_A(W, A)) \geq \ell(\operatorname{Hom}_A(V, A)).$$

Durch Induktion nach $\ell(M)$ folgert man wegen $\ell(k) = \ell(\operatorname{Hom}_A(k, A)) = 1$:

$$\ell(\operatorname{Hom}_A(M, A)) \leq \ell(M).$$

Wir betrachten zur kurzen exakten Folge

$$0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow k \longrightarrow 0$$

die lange exakte Kohomologiesequenz

$$0 \to \operatorname{Hom}_A(k, A) \to \operatorname{Hom}_A(A, A) = A \to \operatorname{Hom}_A(\mathfrak{m}, A) \to \operatorname{Ext}^1_A(k, A) \to \operatorname{Ext}^1_A(A, A) = 0 \to \cdots$$

und erhalten daraus für die Längen:

$$\begin{aligned} 0 \leq \ell(\operatorname{Ext}^1_A(k, A)) &= \ell(\operatorname{Hom}_A(k, A)) + \ell(\operatorname{Hom}_A(\mathfrak{m}, A)) - \ell(A) \\ &\leq \ell(k) + \ell(\mathfrak{m}) - \ell(A) = \ell(A) - \ell(A) = 0. \end{aligned}$$

Daraus ergibt sich:

$$\ell(\operatorname{Ext}^1_A(k, A)) = 0$$

Also ist:

$$\operatorname{Ext}^1_A(k, A) = 0.$$

Durch Induktion nach der Länge von M erhält man daraus für jeden endlichen A-Modul M:

$$\operatorname{Ext}^1_A(M, A) = 0.$$

Daraus folgt wegen Satz 13.1, daß A ein injektiver A-Modul ist.

Lemma 14.7 *Sei a ein Nichtnullteiler von A und $B = A/aA$. Dann gilt:*

$$\mathrm{dih}_B(B) = \mathrm{dih}_A(A) - 1.$$

Beweis: Sei M ein B-Modul, N ein A-Modul. M ist dann auch ein A-Modul. $\mathrm{Hom}_A(B, N)$ ist auf natürliche Weise ein B-Modul. Wir benutzen folgende "natürliche" Identität:

$$\mathrm{Hom}_B(M, \mathrm{Hom}_A(B, N)) = \mathrm{Hom}_A(M, N).$$

Sei N injektiv. Dann ist der Funktor $\mathrm{Hom}_A(M, N)$ in der Variablen M exakt, damit der Funktor $\mathrm{Hom}_B(M, \mathrm{Hom}_A(B, N))$ in der Variablen M. Also ist $\mathrm{Hom}_A(B, N)$ dann ein injektiver B-Modul. Sei der Komplex $I^\bullet$:

$$0 \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots$$

eine injektive Auflösung des A-Moduls A. $\mathrm{Hom}_A(B, I^\bullet) = J^\bullet$ ist dann ein Komplex von injektiven B-Moduln:

$$0 \longrightarrow J^0 \longrightarrow J^1 \longrightarrow \cdots$$

Man berechnet die Kohomologiegruppen $\mathrm{Ext}^\nu_A(B, A)$ mit Hilfe der projektiven Auflösung

$$0 \longrightarrow A \xrightarrow{a} A \longrightarrow B$$

des A-Moduls B und erhält:

$$\mathrm{H}^\nu(J^\bullet) = \mathrm{Ext}^\nu_A(B, A) = \begin{cases} B & \text{falls } \nu = 1 \\ 0 & \text{sonst} \end{cases}.$$

Also ist der Homomorphismus

$$J^0 \longrightarrow J^1$$

injektiv und damit der injektive Modul J^0 *direkter Summand* des injektiven B-Moduls J^1. $\tilde{J}^0 = J^1/J^0$ ist dann ebenfalls injektiv. Sei $\tilde{J}^i = J^{i+1}$ für $i > 0$. Man hat dann eine injektive Auflösung des B- Moduls B durch den Komplex $\tilde{J}^\bullet$:

$$0 \longrightarrow \tilde{J}^0 \longrightarrow \tilde{J}^1 \longrightarrow \cdots$$

$$\mathrm{H}^\nu(\tilde{J}^\bullet) = \begin{cases} B & \text{falls } \nu = 0 \\ 0 & \text{sonst} \end{cases}.$$

Man erhält daraus:

$$\mathrm{dih}_B(B) \leq \mathrm{dih}_A(A) - 1.$$

Gleichheit erhält man mit Hilfe von Satz 13.4 aus folgenden Identitäten:

$$\mathrm{Hom}_B(k, J^\bullet) = \mathrm{Hom}_A(k, I^\bullet),$$

$$\mathrm{H}^i(\mathrm{Hom}_B(k, \tilde{J}^\bullet)) = \mathrm{H}^{i+1}(\mathrm{Hom}_B(k, J^\bullet))$$

und daraus folgend

$$\mathrm{Ext}^i_B(k, B) \cong \mathrm{Ext}^{i+1}_A(k, A).$$

Theorem 14.1 beweist man jetzt durch Induktion nach $\mathrm{codh}(A)$ mit Hilfe von Lemma 14.3, Satz 14.6 (Induktionsanfang) und Lemma 14.7 (Induktionschluß) Man benutzt:
$\mathfrak{b} \subseteq \mathfrak{a}$ *seien Ideale von* A. *Genau dann ist das Ideal* $\mathfrak{a}$ *irreduzibel, wenn sein Bild in* $A/\mathfrak{b}$ *irreduzibel ist.*

Aufgaben:

Sei $\mathfrak{p}$ *ein Primideal des Gorensteinringes* A. *Dann ist auch* $A_\mathfrak{p}$ *Gorensteinring.*

Sei A *ein Quasifrobeniusring. Für alle endlichen* A*-Moduln* M *gilt:*

$$\mathrm{Hom}_A(\mathrm{Hom}_A(M, A)) \cong M.$$

Sei A *ein Gorensteinring der Dimension 1. Für einen Untermodul* M *eines endlichen freien Moduls gilt:*

$$\mathrm{Ext}^i_A(M, A) = 0 \quad \forall\ i > 0.$$
$$\mathrm{Hom}_A(\mathrm{Hom}_A(M, A)) \cong M.$$

Sei p *eine Primzahl,* $n > 0$ *und* $\mathbb{Z}$ *der Ring der ganzen Zahlen. Dann ist* $\mathbb{Z}/p^n\mathbb{Z}$ *ein Quasifrobeniusring.*

XV Reguläre lokale Ringe.

Die im folgenden Abschnitt behandelten regulären Ringe spielen in der algebraischen Geometrie eine wichtige Rolle. Sei X ein endlich erzeugtes Schema über einem algebraisch abgeschlossenen Körper. Ein Punkt von X ist ein glatter, d.h. nicht singulärer Punkt von X genau dann, wenn der lokale Ring der Strukturgarbe in diesem Punkt regulär ist. Siehe auch die Aufgaben am Ende dieses Abschnitts.

Sei wieder A ein (nötherscher) lokaler Ring, m sein maximales Ideal und $k = A/m$ sein Restklassenkörper.

Definition 15.1. *Der Ring A heißt regulär, wenn eine der folgenden äquivalenten Eigenschaften gelten:*

(1) $\quad \mathrm{gldh}(A) < \infty.$

(2) $\quad \mathrm{dih}_A(M) < \infty \quad \forall$ *Moduln* M.

(3) $\quad \mathrm{dh}_A(M) < \infty \quad \forall$ *endlichen Moduln* M.

(4) $\quad \mathrm{dh}_A(k) < \infty.$

(5) $\quad \mathrm{Tor}_n^A(k,k) = 0 \quad$ *für eine natürliche Zahl* $n > 0$.

Siehe Satz 13.6 .

Lemma 15.2 *Sei M ein endlicher A-Modul endlicher projektiver homologischer Dimension; sei $n > 0$. Dann sind folgenden Behauptungen äquivalent:*

(1) $\quad \mathrm{dh}_A(M) < n.$

(2) $\quad \mathrm{Ext}_A^i(M, A) = 0 \quad \forall\ i \geq n.$

Beweis. (2) $\Longrightarrow$ (1) : Sei $d = \mathrm{dh}_A(M) \geq n$. Wegen Satz 1.9 genügt es zu zeigen:

$$\mathrm{Ext}_A^d(M, X) = 0 \quad \forall \text{ endlichen Moduln } X.$$

Diese Behauptung ist richtig für $X = A$, damit auch für alle endlichen freien Moduln $X \cong A^r$. Zu einem beliebigen endlichen A-Modul X gibt es eine kurze exakte Folge

$$0 \longrightarrow Y \longrightarrow F \longrightarrow X \longrightarrow 0$$

mit einem endlichen freien A-Modul F. Wir betrachten die zugehörige lange exakte Kohomologiesequenz

$$\cdots \to 0 = \mathrm{Ext}_A^d(M, F) \to \mathrm{Ext}_A^d(M, X) \to \mathrm{Ext}_A^{d+1}(M, Y) = 0 \to \cdots$$

und erhalten

$$\mathrm{Ext}_A^d(M, X) = 0.$$

Mit Hilfe von Theorem 14.1 und Lemma 15.2 erhält man:

Satz 15.3. *Ein regulärer Ring A ist ein Gorensteinring, insbesondere ein Cohen-Maccauly-Ring. Es gilt:*

$$\mathrm{gldh}(A) = \dim(A) = \mathrm{codh}(A).$$

Folgerung 15.4. *Ein lokaler Ring A der Dimension Null ist genau dann regulär, wenn er ein Körper ist, d.h. wenn gilt:*

$$A = k.$$

Denn: $\mathrm{gldh}(A) = 0 \Longrightarrow k$ ist projektiver, damit freier A-Modul.

Übungsaufgabe:

Lemma 15.5 *seien $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ Primideale von A; es gelte:*

$$\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n \cup \mathfrak{m}^2 = \mathfrak{m}.$$

Dann gilt für einen Index s:

$$\mathfrak{p}_s = \mathfrak{m}.$$

Man wende dieses Lemma auf die Menge der assoziierten Primideale an. Dann erhält man:

Folgerung 15.6 *Sei* $\mathrm{codh}(A) > 0$. *Das ist z.B. der Fall, wenn A ein regulärer Ring der Dimension* $\dim(A) > 0$ *ist. Dann gibt es einen Nichtnullteiler a von A, der nicht in $\mathfrak{m}^2$ enthalten ist:*

$$a \in \mathfrak{m} \setminus \mathfrak{m}^2.$$

Lemma 15.7 *Sei $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ und $B = A/aA$. Dann ist k ein direkter Summamd des B-Moduls $M = \mathfrak{m}/a\mathfrak{m} = \mathfrak{m} \otimes_A B$. Genauer: Für das maximale Ideal $\tilde{\mathfrak{m}} = \mathfrak{m}/Aa$ von B gilt:*

$$M \cong k \oplus \tilde{\mathfrak{m}}.$$

Beweis: Wähle Elemente

$$b_1, \cdots, b_s \in \mathfrak{m}$$

so, daß die Bilder von $a, b_1, \cdots, b_s$ im Vektorraum $\mathfrak{m}/\mathfrak{m}^2$ über dem Körper k eine Basis bilden. Nach Nakayama erzeugen dann die Elemente $a, b_1, \cdots, b_s$ das Ideal $\mathfrak{m}$.

$$Aa + Ab_1 + \cdots + Ab_s = \mathfrak{m}$$

$$Aa \cap (Ab_1 + \cdots + Ab_s) \subseteq a\mathfrak{m} \subseteq Aa$$

Seien $\overline{a}, \overline{b}_1, \cdots, \overline{b}_s$ die Bilder der Elemente in M, sei $N = A\overline{b}_1 + \cdots + A\overline{b}_s$ Dann gilt:

$$A\overline{a} + N = M$$

$$A\overline{a} \cap N = 0$$

Damit ist M direkte Summe von $A\overline{a}$ und$N$.

$$A\overline{a} \oplus N = M$$

Es gilt

$$A\overline{a} \cong k.$$

Der Kern der natürliche Abbildung

$$M = \mathfrak{m}/a\mathfrak{m} \longrightarrow \tilde{\mathfrak{m}} = \mathfrak{m}/Aa$$

ist $A\overline{a}$, und N wird bei dieser Abbildung isomorph auf $\tilde{\mathfrak{m}}$ abgebildet.

Lemma 15.8 *Sei $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ ein Nichtnullteiler von A. Genau dann ist der Ring A regulär, wenn der Faktorring $B = A/Aa$ regulär ist*

Beweis: Durch Betrachtung der kurzen exakten Folge

$$0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow k \longrightarrow 0$$

erhält man:

$$\mathrm{dh}_A(k) < \infty \Longleftrightarrow \mathrm{dh}_A(\mathfrak{m}) < \infty$$

Weil nach Lemma 15.7 k direkter Summand von $\mathfrak{m}/a\mathfrak{m}$ ist gilt:

$$\mathrm{gldh}(B) = \mathrm{dh}_B(k) \leq \mathrm{dh}_B(\mathfrak{m}/a\mathfrak{m}) \leq \mathrm{gldh}(B)$$

Es genügt also zu zeigen:

$$\mathrm{dh}_A(\mathfrak{m}) = \mathrm{dh}_B(\mathfrak{m}/a\mathfrak{m})$$

Mit Hilfe der projektiven Auflösung

$$0 \longrightarrow A \xrightarrow{a} A \longrightarrow B$$

des A-Moduls B berechnet man:

$$\mathrm{Tor}_i^A(\mathfrak{m}, B) = \begin{cases} \mathfrak{m}/a\mathfrak{m} & \text{falls } i = 0 \\ 0 & \text{sonst} \end{cases}$$

Ist $F \cong A^n$ ein endlicher freier A-Modul, so ist $F \otimes_A B \cong B^n$ ein endlicher freier B-Modul. Sei der Komplex $F_\bullet$:

$$\cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow 0$$

eine Auflösung von $\mathfrak{m}$ durch endliche projektive, damit freie A-Moduln. Wir betrachten den Komplex $G_\bullet = F_\bullet \otimes_A B$:

$$\cdots \longrightarrow G_1 \longrightarrow G_0 \longrightarrow 0$$

von endlichen freien B-Moduln G_i. Es gilt:

$$\mathrm{H}_i(G_\bullet) = \mathrm{Tor}_i^A(\mathfrak{m}, B) = \begin{cases} \mathfrak{m}/a\mathfrak{m} & \text{falls } i = 0 \\ 0 & \text{sonst} \end{cases}$$

Es folgt, daß $G_\bullet$ eine projektive Auflösung des B-Moduls $\mathfrak{m}/a\mathfrak{m}$ ist.Ferner gilt:

$$F_\bullet \otimes_A k = G_\bullet \otimes_B k$$

Es folgt:

$$\mathrm{Tor}_i^A(\mathfrak{m}, k) = \mathrm{Tor}_i^B(\mathfrak{m}/a\mathfrak{m}, k) \quad i \geq 0$$
$$\mathrm{Tor}_n^A(\mathfrak{m}, k) = 0 \Leftrightarrow \mathrm{Tor}_n^B(\mathfrak{m}/a\mathfrak{m}, k) = 0$$

Wegen Satz 13.9 folgt die gesuchte Gleichung:

$$\mathrm{dh}_A(\mathfrak{m}) = \mathrm{dh}_B(\mathfrak{m}/a\mathfrak{m})$$

Ziel dieses Paragraphen ist das folgende

Theorem 15.9 *Äquivalent sind folgende Aussagen:*

(1) *A ist ein regulärer Ring.*

(2) *Das maximale Ideal $\mathfrak{m}$ wird durch eine A-Folge erzeugt.*

(3) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim(A)$.

Bemerkung: Nach Nakayama erzeugen Elemente von m, deren Bilder im Vektorraum $\mathfrak{m}/\mathfrak{m}^2$ über dem Körper k eine Basis bilden, das maximale Ideal $\mathfrak{m}$, und es gilt deshalb immer $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq \dim(A)$.

Beweis: Der Beweis des homologischen Teils, der Äquivalenz von (1) und (2), ergibt sich durch Induktion nach $\dim(A)$ aus Folgerung 15.4, Folgerung 15.6 und Lemma 15.8 .

Es bleibt zu zeigen: (3) $\Longrightarrow$ (2). Das geschieht ebenfalls durch Induktion nach $\dim(A)$ mit Hilfe des Satzes:

Satz 15.10 *Noch eine Charakterisierung eines regulären lokalen Ringes A. Sei*

$$\dim(A) = n > 0$$

und seien $a_1, \cdots, a_n \in \mathfrak{m}$ Elemente, die das maximale Ideal $\mathfrak{m}$ von A erzeugen. Seien $x_1, \cdots, x_n$ die Bilder in $\mathfrak{m}/\mathfrak{m}^2$. Dann ist der assozierte graduierte Ring

$$G(A) = k \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \mathfrak{m}^3/\mathfrak{m}^4 \oplus \cdots$$

ein Polynomring in den n "Variablen" $x_1, \cdots, x_n$ Insbesondere folgt, daß jedes der Elemente a_i ein Nichtnullteiler von A ist, durch Induktion nach n allgemeiner, daß die Elemente $a_1, \cdots, a_n$ eine A-Folge bilden.

Beweis: Wir benutzen die Beschreibung der Dimension dim(A) durch das Samuelpolynom $S(t)$ von A, bzw. das Hilbertpolynom $P(t)$ des graduierten Ringes $G(A)$.

$$S(t) - S(t-1) = P(t)$$

Der Grad $\deg(S)$ von S ist die Dimension von A; damit gilt:

$$\deg(P) = n - 1.$$

Sei

$$R = k[z_1, \cdots, z_n]$$

der Polynomring in den Variablen $z_1, \cdots, z_n$ über dem Körper k. Sein Hilbertpolynom $Q(t)$ hat ebenfalls den Grad $n-1$. Wir betrachten den Ringhomomorphismus über k:

$$R \longrightarrow G(A)$$
$$z_i \longmapsto x_i$$

Er ist surjectiv, weil die Elemente $x_1, \cdots, x_n$ den Ring $G(A)$ über k erzeugen. Sei $\mathfrak{I} \subseteq R$ das homogene Kernideal dieses Homomorphismus und $Q_{\mathfrak{I}}(t)$ das Hilbertpolynom von $\mathfrak{I}$. Es gilt:

$$P(t) + Q_{\mathfrak{I}}(t) = Q(t).$$

Sei $\mathfrak{I} \neq 0$ und $f \neq 0$ ein homogenes Element vom Grad s in $\mathfrak{I}$. Es gilt für das Hilbertpolynom $Q_{\mathfrak{J}}(t)$ des homogenen Ideals $\mathfrak{J} = Rf \subseteq \mathfrak{I}$:

$$Q_{\mathfrak{J}}(t) = Q(t-s) \quad , \quad Q_{\mathfrak{J}}(t) \leq Q_{\mathfrak{I}}(t) \leq Q(t) \text{ für große } t$$

Daraus folgt, daß $Q(t)$ und $Q_{\mathfrak{I}}(t)$ den gleichen "höchsten" Koeffizienten haben; es gilt also:

$$\deg(P) = \deg(Q - Q_{\mathfrak{I}}) < \deg(Q) = n - 1 = \deg(P).$$

Das ist ein Widerspruch! Also ist $I = 0$ und

$$R \cong G(A).$$

Wir zeigen noch, daß $a = a_1$ ein Nichtnullteiler von A ist. Sei $b \neq 0$ ein Element aus $\mathfrak{m}$ mit

$$ab = 0.$$

Es gibt eine natürliche Zahl s mit

$$b \in \mathfrak{m}^s \quad , \quad b \notin \mathfrak{m}^{s+1}.$$

Sei $\overline{b}$ das Bild von b in $\mathfrak{m}^s/\mathfrak{m}^{s+1} \subseteq G(A)$. Es gilt:

$$\overline{b} \neq 0 \ , \ x_1\overline{b} = 0$$

Das ist ein Widerspruch!

Folgerung 15.11 *Ein regulärer lokaler Ring A ist Integritätsbereich.*

Beweis: Man benutze Satz 15.10, bzw. die Beweismethode für den zweiten Teil dieses Satzes!

Aufgaben:

Sei $\mathfrak{p}$ ein Primideal des regulären Ringes A. Dann ist auch $A_{\mathfrak{p}}$ regulär. (Siehe Aufgaben zu § 1)

Sei A regulär und seien $x_1, \cdots, x_r \in \mathfrak{m}$ Elemente, deren Bilder im Vektorraum $\mathfrak{m}/\mathfrak{m}^2$ über k linear unabhängig sind und $\mathfrak{I}$ das von diesen Elementen erzeugte Ideal. Dann ist $A/\mathfrak{I}$ ein regulärer Ring der Dimension $\dim(A) - r$.

Sei $R = K[z_1, \cdots, z_1]$ ein Polynomring über dem Körper K. Zeige–zumindest für einen algebraisch abgeschlossenen Grundkörper K–:

(1) Für jedes Primideal $\mathfrak{p}$ von R ist $R_{\mathfrak{p}}$ regulär. ($\mathfrak{p}$ maximal genügt!)

(2) Seien $P_1, \cdots, P_r$ r Polynome aus R und $\mathfrak{I}$ das von ihnen erzeugte Ideal. Sei $a = (a_1, \cdots, a_n) \in K^n$ ein Punkt mit

$$P_1(a) = \cdots = P_n(a) = 0$$

und sei $\mathfrak{m}$ das von den Elementen $z_1 - a_1, \cdots, z_n - a_n$ erzeugte maximale Ideal von R. Wir betrachten die Funktionalmatrix im Punkte a :

$$T = (t_{ij}) = \begin{pmatrix} \frac{\partial P_1}{\partial z_1}(a) & \cdots & \frac{\partial P_1}{\partial z_n}(a) \\ \vdots & & \vdots \\ \frac{\partial P_n}{\partial z_1}(a) & \cdots & \frac{\partial P_n}{\partial z_n}(a) \end{pmatrix}$$

Sei der Rang von T gleich r. Dann ist $R_{\mathfrak{m}}/\mathfrak{I}R_{\mathfrak{m}}$ ein reguläre Ring der Dimension $n - r$. (Geometrische Interpretation?)

Anleitung:Betrachte den Anfang der "Taylorentwicklung":

$$P_i(z) = t_{i1}(z_1 - a_1) + \cdots + t_{in}(z_n - a_n) \quad \textit{modulo} \quad \mathfrak{m}^2$$

Bemerkung: Es gilt allgemeiner, daß $A = R_{\mathfrak{m}}/\mathfrak{I}R_{\mathfrak{m}}$ genau dann regulär ist, wenn gilt:

$$\textit{Rang}(T) = n - \dim(A)$$

Beweise : Der formale Potenzreihenring $K[[z_1, \ldots, z_n]]$ –die $(z_1, \ldots, z_n)$-adische Komplettierung des Polynomringes R– ist ein regulärer lokaler Ring.

XVI Moduln endlicher homologischer Dimension

Auch in diesem Abschnitt ist A ein noetherscher lokaler Ring mit dem maximalen Ideal $\mathfrak{m}$ und dem Restklassenkörper $k = A/\mathfrak{m}$ und $M \neq 0$ ein endlicher A-Modul. Ziel ist es folgenden Zusammenhang zwischen der Tiefe $\mathrm{t}(M)$ eines Moduls und seiner homologischen Dimension $\mathrm{dh}_A(M)$ zu beweisen, falls $\mathrm{dh}_A(M) < \infty$.

Theorem. *Sei $M \neq 0$ ein Modul endlicher homologische Dimension. Dann gilt*

$$\mathrm{dh}_A(M) + \mathrm{t}(M) = \mathrm{t}(A)$$

Dazu beweisen wir zuerst einige Lemmata.

Lemma. *Es sei $\mathrm{t}(A) = 0$ und $\mathrm{dh}_A(M) < \infty$. Dann ist M projektiv, also frei; es gilt also*

$$\begin{aligned} \mathrm{dh}_A(M) &= 0 \\ \mathrm{t}(M) &= 0 \end{aligned}$$

Beweis. Mit Hilfe von Induktion nach $\mathrm{dh}_A(M)$ führt man den allgemeinen Fall auf den Fall $\mathrm{dh}_A(M) \leq 1$ zurück. Sei also

$$0 \longrightarrow G \xrightarrow{\ j\ } F \longrightarrow M \longrightarrow 0$$

eine kurze exakte Folge mit zwei endlichen, nicht verschwindenden, freien Moduln F, G. Wir müssen zeigen

$$\mathrm{Tor}_1^A(M, k) = \mathrm{Kern}(G/\mathfrak{m}G \to F/\mathfrak{m}F) = 0$$

Weil die Tiefe $\mathrm{t}(A)$ von A verschwindet, gibt es ein von Null verschiedenes Element $a \in \mathfrak{m}$ mit $\mathfrak{m}a = 0$. Sei $g \in G$ ein Element mit $j(g) \in \mathfrak{m}F$. dann gilt $j(ag) = aj(g) = 0$. Weil j injektiv ist folgt $ag = 0$ und daraus $g \in \mathfrak{m}$. □

Lemma. *Sei $\mathrm{t}(A) > 0$, $\mathrm{t}(M) > 0$. dann gibt es ein Element $0 \neq t \in \mathfrak{m}$, das weder Nullteiler von A noch von M ist.*

Beweis. Nach Voraussetzung gilt $\mathfrak{m} \notin \mathrm{Ass}(A) \cup \mathrm{Ass}(M)$. Angenommen, es würde gelten

$$\bigcup_{\mathfrak{p} \in \mathrm{Ass}(A) \cup \mathrm{Ass}(M)} \mathfrak{p} = \mathfrak{m}$$

Dann wäre $\mathfrak{m} \subseteq \mathfrak{p}$ für ein Primideal $\mathfrak{p} \in \mathrm{Ass}(A) \cup \mathrm{Ass}(M)$, also $\mathfrak{m} = \mathfrak{p} \in \mathrm{Ass}(A) \cup \mathrm{Ass}(M)$. Widerspruch! □

Lemma. *Sei* $\mathrm{t}(A) > 0$, $\mathrm{t}(M) > 0$, *und sei* $t \in \mathfrak{m}$ *ein Nichtnullteiler von* A *und von* M. *Sei* $B = A/tA$, $N = M/tM$. *Dann gilt*

$$\begin{aligned} \mathrm{t}(B) &= \mathrm{t}(A) - 1 \\ \mathrm{t}(N) &= \mathrm{t}(M) - 1 \\ \mathrm{dh}_B(N) &= \mathrm{dh}_A(M) \end{aligned}$$

Beweis. Es sei der Komplex $F_\bullet$ eine Auflösung des Moduls M durch endliche freie A-Moduln F_ν. Dann ist $G_\bullet = F_\bullet \otimes_A B$ ein Komplex von endlichen freien B-Moduln. Es gilt $H_\nu(G_\bullet) = \mathrm{Tor}_\nu^A(M, B)$. Man berechnet $\mathrm{Tor}_\nu^A(M, B)$ mit Hilfe der exakten Folge

$$0 \longrightarrow A \xrightarrow{t} A \longrightarrow B \longrightarrow 0$$

und erhält

$$\mathrm{Tor}_\nu^A(M, B) = \begin{cases} M/tM = N & \nu = 0 \\ 0 & \text{sonst} \end{cases}$$

Also ist $G_\bullet$ eine Auflösung des B-Moduls N durch freie B-Moduln. Es gilt

$$\mathrm{Tor}_\nu^B(N, k) = H_\nu(G_\bullet \otimes_B k) = H_\nu(F_\bullet \otimes_A k) = \mathrm{Tor}_\nu^A(M, k) \text{ für } \nu \geq 0$$

Es folgt

$$\mathrm{dh}_B(N) = \mathrm{dh}_A(M)$$

□

Beweis des Theorems. Der Beweis erfolgt durch Induktion nach $\mathrm{t}(A)$. Der Induktionsanfang – $\mathrm{t}(A) = 0$ – wurde im ersten Lemma bewiesen. Ist $\mathrm{dh}_A(M) = 0$, so ist M frei und $\mathrm{t}(M) = \mathrm{t}(A)$. Seien $\mathrm{t}(A) > 0$ und $\mathrm{t}(M) > 0$. Dann gibt es nach dem zweiten Lemma einen gemeinsamen Nichtnullteiler t für A und M. Mit Hilfe des dritten Lemmas führt man die gesuchte Aussage auf die entsprechende, nach Induktionsvoraussetzung schon bewiesene Aussage für den A/tA-Modul M/tM zurück.

Es bleibt noch der Fall $\mathrm{t}(A) > 0$, $\mathrm{t}(M) = 0$, $\mathrm{dh}_A(M) > 0$. Betrachte eine kurze exakte Folge

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

mit einem endlichen freien Modul F. Dann ist $\mathrm{dh}_A(K) = \mathrm{dh}_A(M) - 1$. Aus den Tiefebedingungen erhält man $\mathrm{Hom}_A(k, F) = 0$ und $\mathrm{Hom}_A(k, M) \neq 0$. Man betrachte zu der kurzen exakten Folge die lange exakte EXT-Folge

$$0 \to \mathrm{Hom}_A(k, K) \to \mathrm{Hom}_A(k, F) \to \mathrm{Hom}_A(k, M) \to \mathrm{Ext}_A^1(k, K) \to \ldots$$

Man erhält $\mathrm{Hom}_A(k, K) = 0$ und $\mathrm{Ext}_A^1(k, K) \neq 0$; also ist $\mathrm{t}(K) = 1$. Die gesuchte Aussage für M folgt aus der ensprechenden für den Modul K. K und A erfüllen aber die Voraussetzungen unter denen die Behauptung schon bewiesen wurde. □

XVII Eindeutige Primfaktorzerlegung in regulären lokalen Ringen

Nach Kaplanski

Im folgenden sind alle betrachteten Ringe nöthersche Integritätsbereiche.

Eindeutige Primfaktorzerlegung.

Eine Nichteinheit a eines Ringes A heißt *unzerlegbar*, wenn gilt

$$a = bc \Rightarrow b \text{ oder } c \text{ ist Einheit}$$

Ein Element $a \neq 0$ heißt *Primelement* , wenn das von a erzeugte Ideal Aa ein Primideal ist. Offenbar ist ein Primelement unzerlegbar. Weil der Integritätsbereich A nöthersch angenommen wurde, besitzt jedes Element $a \neq 0$ des Ringes A eine Zerlegung

$$a = \epsilon a_1 \dots a_r$$

der Länge r mit einer Einheit ϵ und unzerlegbaren Elementen a_ν. $r = 0$ bedeutet, daß a eine Einheit ist. Eine solche Zerlegung nennen wir eine Zerlegung der Länge r in unzerlegbare Elemente.

Definition. Der Ring A besitzt eindeutige Primfaktorzerlegung, wenn für jedes von Null verschiedene Element aus A eine Zerlegung in unzerlegbare Elemente eindeutig ist bis auf die Reihenfolge und bis auf Abänderung der auftretenden Elemente um Einheiten. Wir nennen A einen ZPE-Ring. Insbesondere haben dann alle Zerlegungen eines Elementes a in unzerlegbare Elemente die gleiche Länge.

Satz. *Der Ring A ist ein ZPE-Ring genau dann, wenn jedes unzerlegbare Element a ein Primideal $\mathfrak{p} = Aa$ erzeugt, wenn also ein Element $a \neq 0$ genau dann unzerlegbar ist, wenn es Primelement ist.*

Beweis. Sei A ein ZPE-Ring, a unzerlegbar und $\mathfrak{p} = Aa$. Seien α, β zwei von Null verschiedene Elemente mit $\alpha\beta \in Aa$. Dann ist $\alpha\beta = xa$. Aus der ZPE-Eigenschaft folgt $a|\alpha$ oder $a|\beta$.

Seien umgekehrt alle unzerlegbaren Elemente Primelemente. Wir betrachten zwei Zerlegungen einer Nichteinheit $a \neq 0$ in unzerlegbare Elemente, damit in Primelemente:

$$a = \epsilon a_1 \dots a_r = \epsilon' b_1 \dots b_s$$

Dann ist $r, s \geq 1$. Weil Ab_1 ein Primideal ist, gibt es ein Element a_ν, etwa a_1, das in Ab_1 liegt. Es gilt $a_1 = ub_1$. Weil a_1 unzerlegbar ist, ist u eine Einheit. Durch Induktion nach einer der Längen r oder s beweist man die gesuchte Eindeutigkeitsaussage. □

Sei $a \in A$ eine von Null verschiedene Nichteinheit und $\mathfrak{p} \subseteq A$ ein minimales assoziertes Ideal des Moduls A/Aa. Dann gilt für die Höhe von $\mathfrak{p}$

$$h(\mathfrak{p}) = dim A_\mathfrak{p} = 1$$

Lemma. *Äquivalent sind folgende beiden Aussagen:*

(1) *A ist ZPE-Ring.*
(2) *Jedes Primideal der Höhe 1 von A ist Primideal.*

Zum Beweis. (1) $\Rightarrow$ (2): Sei $\mathfrak{p}$ ein Primideal der Höhe 1. $\mathfrak{p}$ enthält ein unzerlegbares Element a. a ist Primelement, $Aa = \mathfrak{q}$ also ein von Null verschiedenes Primideal.

$$0 \neq \mathfrak{q} \subseteq \mathfrak{p}$$

Weil $h(p) = 1$, folgt $Aa = \mathfrak{q} = \mathfrak{p}$.

(2) $\Rightarrow$ (1): Sei a ein unzerlegbares Element und $\mathfrak{p}$ ein minimales assoziertes Primideal von A/Aa. Dann enthält $\mathfrak{p}$ das Element a und es gilt nach Voraussetzung $\mathfrak{p} = A\alpha$. Es folgt $a = \alpha\beta$. Da a unzerlegbar ist, ist β eine Einheit, damit $Aa = \mathfrak{p}$; a erzeugt ein Primideal. $\square$

Endliche projektive Moduln über einem nicht lokalen Ring.

Sei M ein endlicher Modul über dem nötherschen Ring A. Für das folgende Lemma ist es unnötig anzunehmen, wie sonst vorausgesetzt, daß A Integritätsbereich ist.

Lemma. *Folgende Eigenschaften des Moduls M sind äquivalent.*

(1) *M ist projektiver Modul.*
(2) *Für alle Primideale* $\mathfrak{p}$ *ist* $M_\mathfrak{p}$ *projektiver, damit freier* $A_\mathfrak{p}$*-Modul.*
(3) *Für alle maximalen Ideale* $\mathfrak{m}$ *ist* $M_\mathfrak{m}$ *projektiver, damit freier* $A_\mathfrak{m}$*-Modul.*

Beweis. (1) $\Rightarrow$ (2): Der projektive A-Modul ist direkter Summand eines freien A-Moduls F. Für jede multiplikative Menge $S \subseteq A$ ist dann der A_S-Modul M_S direkter Summand des freien A_S-Moduls F_S, damit projektiver A_S-Modul.

(2) $\Leftrightarrow$ (3): Sei $\mathfrak{p}$ ein Primideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$, das $\mathfrak{p}$ enthält. Es gilt

$$A_\mathfrak{p} = (A_\mathfrak{m})_{\mathfrak{p}_\mathfrak{m}}$$
$$M_\mathfrak{p} = (M_\mathfrak{m})_{\mathfrak{p}_\mathfrak{m}}$$

(2) $\Rightarrow$ (1): Es gibt einen endlichen freien A-Modul F und eine exakte Folge

$$F \longrightarrow M \longrightarrow 0$$

Wir werden für einen endlichen A-Modul X zeigen, daß die Folge

$$Hom_A(X, F) \longrightarrow Hom_A(X, M) \longrightarrow 0$$

exakt ist. Für $X = M$ folgt dann, daß sich die identische Abbildung von M auf sich zu einem Homomorphismus $M \to F$ liften läßt. Damit ist M direkter Summand von F, also projektiv.

Wir betrachten die exakte Folge endlicher A-Moduln.

$$Hom_A(X, F) \longrightarrow Hom_A(X, M) \longrightarrow K \longrightarrow 0$$

und müssen zeigen, daß der Kokern K verschwindet. Sei $\mathfrak{p}$ ein Primideal von A. Weil M endlicher A-Modul ist, gilt für einen beliebigen A-Modul Y

$$(Hom_A(X,Y))_\mathfrak{p} = Hom_{A_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$$

Da Lokalisierung ein exakter Funktor ist, sind die Folgen

$$F_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow 0$$

und

$$Hom_{A_\mathfrak{p}}(X_\mathfrak{p}, F_\mathfrak{p}) \longrightarrow Hom_{A_\mathfrak{p}}(X_\mathfrak{p}, M_\mathfrak{p}) \longrightarrow K_\mathfrak{p} \longrightarrow 0$$

exakt. Da $M_\mathfrak{p}$ projektiver $A_\mathfrak{p}$-Modul ist, muß $K_\mathfrak{p}$ verschwinden. Das gesuchte Ergebnis folgt dann aus dem

Lemma. *Sei K ein beliebiger A-Modul. Wenn für alle Primideale $\mathfrak{p}$ von A der Modul $K_\mathfrak{p}$ verschwindet, so verschwindet auch K.*

Beweis: Wegen der Exaktheit des Lokalisierungsfunktors genügt es die Behauptung für alle endlichen Untermoduln zu beweisen. Wir können also annehmen, daß K endlicher A-Modul ist. Sei $\mathfrak{a} = \{x \in A | xK = 0\}$ der Annulator von M. Sei $\mathfrak{p}$ ein Primideal. Weil K endlicher Modul ist folgt aus dem Verschwinden von $K_\mathfrak{p}$, daß es ein Element

$$s \notin \mathfrak{p}$$

gibt mit $sK = 0$. Deshalb gibt es kein Primideal, daß den Annulator $\mathfrak{a}$ umfaßt. Es gilt also $\mathfrak{a} = A$. Es folgt $K = AK = 0$. $\square$

Die äußeren Potenzen eines Moduls.

Sei M ein A-Modul und $n \geq 1$ eine natürliche Zahl. Wir betachten multilineare Abbildungen $\phi(x_1, \ldots, x_n)$

$$\phi : M \times \cdots \times M \longrightarrow X$$

des n-fachen kartesischen Produkts von M mit sich selbst in einen beliebigen A-Modul X. ϕ ist also in jeder Variablen bei festgehaltenen anderen Variablen ein A-Homomorphismus $M \longrightarrow X$. Eine solche Abbildung heißt *alternierend* , wenn gilt:

$$\phi(x_1, \ldots, y, \ldots, y, \ldots, x_n) = 0$$

Es folgt

$$\phi(x_1, \ldots, u, \ldots, v, \ldots, x_n) = -\phi(x_1, \ldots, v, \ldots, u, \ldots, x_n)$$

Man sieht leicht ein, daß es unter allen diesen alternierenden Abbildungen eine universelle

$$\pi : M \times \cdots \times M \longrightarrow \bigwedge^n M$$

gibt. Diese hat also folgende universelle Abbildungseigenschaft:
Zu jeder – n-fach – alternierenden Abbildung

$$\phi : M \times \cdots \times M \longrightarrow X$$

gibt es genau einen A-Homomorphismus

$$f : \bigwedge^n M \longrightarrow X$$

mit

$$\phi = f \circ \pi.$$

$\bigwedge^n M$ ist – zusammen mit der Abbildung π – durch diese universelle Eigenschaft eindeutig bis auf Isomorphie gekennzeichnet und heißt die n-fache *äußere Potenz* von M. Sie läßt sich als Faktormodul des n-fachen Tensorproduktes

$$M \otimes \cdots \otimes M$$

von M-mit sich selbst nach einem von naheliegenden "Relationen" erzeugten Untermodul konstruieren. Insbesondere ist die äußere Potenz ein endlicher A-Modul, falls M ein endlicher A-Modul ist. Man setzt schließlich $\bigwedge^0 M = A$. $\bigwedge^n$ ist auf natürliche Weise ein allerdings nicht additiver Funktor. Ist $f : M \longrightarrow N$ surjektiv, so ist auch $\bigwedge^n(f)$ surjektiv. Man zeigt folgendes

Lemma. *Es gilt*

(1) $\bigwedge^1 M = M$
(2) $\bigwedge^n(M \oplus N) = \bigoplus_{\nu+\mu=n,\nu\geq 0,\mu\geq 0}(\bigwedge^\nu M \otimes \bigwedge^\mu N)$
(3) *Ist F ein freier Modul vom Rang r, so gilt*

$$\bigwedge^n F = \begin{cases} A & n = r \\ 0 & n > r \end{cases}$$

(4) *Wird M von r Elementen erzeugt, so verschwindet $\bigwedge^n M$ für $n > r$.*

Kaplanskis Beweis

Im folgenden ist A ein regulärer lokaler Ring, $\mathfrak{m}$ sein maximales Ideal und $k = A/\mathfrak{m}$ der Restklassenkörper. A ist dann ein nötherscher Integritätsbereich. Ist die Krullsche Dimension $dim(A) = 0$, so ist $A = k$. Sei $dim(A) > 0$. Dann gibt es ein $s \in \mathfrak{m} \setminus \mathfrak{m}^2$. As ist ein Primideal der Höhe 1. Ist $dim(A) = 1$, so ist As das einzige von 0 verschiedene Primideal. A ist also für $dim(A) \leq 1$ ein ZPE-Ring. Ein endlicher projektiver A-Modul ist frei, weil A lokal ist. Jeder endliche A-Modul besitzt eine endliche Auflösung durch endliche projektive, damit freie A-Moduln.

Lemma. *Sei $S \subseteq A$ eine multiplikative Menge und N ein endlicher projektiver Modul über dem Ring $B = A_S$. Dann gibt es zwei endliche freie B-Moduln F, G so daß gilt*

$$G \cong F \oplus N$$

Beweis. Es gibt einen endlichen nicht unbedingt projektiven A-Modul M mit

$$N = M_S.$$

M besitzt dann eine endliche Auflösung durch endliche freie A-Moduln. Da der Lokalisierungsfunktor exakt ist, erhält man daraus durch lokalisieren eine entsprechende Auflösung des B-Moduls $N = M_S$. Es gibt also eine exakte Folge

$$0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to N \to 0$$

mit endlichen freien B-Moduln F_ν. Wir beweisen die Aussage des Lemmas nach der Länge n der Auflösung von N. Klar ist der Fall $n = 0$. Sei $n \geq 1$. Sei

$$K = \text{ Kern}(F_0 \longrightarrow N) = \text{ Bild}(F_1 \longrightarrow F_0)$$

Weil M projektiv ist, gilt

$$F_0 \cong K \oplus N$$

K ist projektiv und es gibt eine exakte Folge

$$0 \to F_n \to F_{n-1} \to \cdots \to F_2 \to F_1 \to K \to 0$$

Nach Induktionsvoraussetzung gibt es endliche freie B-Moduln F', G' mit

$$G' \cong F' \oplus K$$

Durch Addition erhält man

$$F' \oplus F_0 \cong G' \oplus N$$

$F = G', G = F' \oplus F_0$ sind die gesuchten endlichen freien Moduln.

Theorem. *Ein regulärer lokaler Ring A ist ein ZPE-Ring.*

Beweis. Der Beweis erfolgt durch vollständige Induktion nach der Krullschen Dimension $dim(A)$. Wir können annehmen, daß $dim(A) \geq 2$. Sei $\mathfrak{p}$ ein Primideal der Höhe 1. Wir müssen zeigen, daß $\mathfrak{p}$ ein Haupideal ist. Äquivalent dazu: $\mathfrak{p}$ ist ein projektiver, daher freier A-Modul.

Wähle ein Element $s \in \mathfrak{m} \setminus \mathfrak{m}^2$. Ist $s \in \mathfrak{p}$ so stimmen die beiden Primideale As und $\mathfrak{p}$ überein. Sei $s \notin \mathfrak{p}$. Sei $S = \{1, s, s^2, s^3, \dots\}$. Dann ist $S \cap \mathfrak{p} = \emptyset$. Sei K der Quotientenkörper von A. Für den Quotientenring $B = A_S$ gilt

$$A \subseteq B \subseteq K.$$

Die Zuordnung $\mathfrak{P} \mapsto \mathfrak{P}_S \subseteq B$ stiftet eine eineindeutige Beziehung zwischen den Primidealen $\mathfrak{P}$ von A mit $\mathfrak{P} \cap S = \emptyset$ und allen Primidealen von B. Sei $\mathfrak{Q}$ ein Primideal von B. Dann gibt es also ein Primideal $\mathfrak{P}$ von A, das s nicht enthält mit $\mathfrak{Q} = \mathfrak{P}_S$. Dann ist $\mathfrak{P} \neq \mathfrak{m}$ und seine Höhe ist kleiner als $dim(A)$. Es gilt dann

$$\begin{aligned} B_\mathfrak{Q} &= A_\mathfrak{P} \\ dim(B_\mathfrak{Q}) &= dim(A_\mathfrak{P}) \\ &< dim(A) \end{aligned}$$

$B_\mathfrak{Q}$ ist also ein regulärer lokaler Ring, dessen Dimension kleiner als die von A ist. Da $s \notin \mathfrak{p}$, ist auch $\mathfrak{q} = \mathfrak{p}_S$ ein Primideal von B der Höhe 1. $\mathfrak{q}_\mathfrak{Q} = \mathfrak{p}_\mathfrak{P}$

ist dann entweder ein Primideal der Höhe 1 von $B_{\mathfrak{Q}}$ oder es gilt $\mathfrak{q}_{\mathfrak{Q}} = B_{\mathfrak{Q}}$. Nach Induktionsvoraussetzung ist also $\mathfrak{q}_{\mathfrak{Q}}$ für alle Primideale $\mathfrak{Q}$ von B ein projektivrt $B_{\mathfrak{Q}}$-Modul. Also ist $N = \mathfrak{q} = \mathfrak{p}_S$ ein projektiver B-Modul. Nach dem vorhergehenden Lemma gibt es freie B-Moduln $F = B^n, G = B^m$ mit $N \oplus B^n = B^m$. Nach Übergang zum Quotientenkörper K, also Nenneraufnahme nach allen von Null verschiedenen Elementen wird daraus $K \oplus K^n = K^m$. Also ist $m = n + 1$.

$$B^n \oplus N = B^{n+1}$$

Durch Übergang zur $n+1$-ten äußeren Potenz erhält man mit Hilfe der Formeln für die äußere Potenz einer direkten Summe

$$B \cong \bigwedge^{n+1} B^{n+1} \cong \bigwedge^{n} B^n \otimes \bigwedge^{1} N \oplus \cdots \cong B \otimes N \oplus \cdots \cong N \oplus R$$

Dabei ist R irgendein endlicher B-Modul. N ist also ein nichtverschwindender direkter Summand von B. Da B ein Integritätsbereich ist folgert man daraus leicht $N \cong B$. $\mathfrak{p}_S = \mathfrak{q} = N$ ist ein Hauptideal von B, also von der Form

$$\mathfrak{p}_S = A_S\alpha \ , \ \alpha \in \mathfrak{p}$$

Nach Krulls Durchschnittssatz gilt $\bigcap_n As^n = 0$. Es gibt also ein Element β, das nicht durch s teilbar ist und eine Darstellung $\alpha = s^m\beta$ Weil s nicht im Primideal $\mathfrak{p}$ enthalten ist gilt $\beta \in \mathfrak{p}$. und

$$\mathfrak{p}_S = A_S\beta$$

Behauptung:

$$\mathfrak{p} = A\beta$$

Sei a ein von Null verschiedenes Element von $\mathfrak{p}$. Dann gibt es ein Element $x \in A$ und eine natürliche Zahl $m \geq 0$ mit $a = \frac{x}{s^m}\beta$. Wir wählen eine solche Darstellung mit einer minimalen natürlichen Zahl $m \geq 0$. Angenommen, es sei $m \geq 1$. Es gilt

$$x\beta = s(s^{m-1}a) \in As$$

Da s nach Konstruktion β nicht teilt und weil As ein Primideal ist teilt s das Element x. Es gilt also $y = \frac{x}{s} \in A$ und

$$a = \frac{y}{s^{m-1}}\beta$$

Das ist aber ein Widerspruch zur Minimalität von m. Wir haben also bewiesen, daß $\mathfrak{p} = A\beta$ ein Hauptideal ist. $\square$

Anhang

Es gibt mehrere Computeralgebra Systeme, in die die kommutative Algebra von über einem Körper endlich erzeugten Ringen und Moduln über diesen Ringen implementiert ist. Beispiele:*Macaulay, singular.*

Arbeitspferd dieser Systeme sind **Gröbnerbasen** von Idealen und Moduln.

Gröbner Basen

Siehe auch:
Thomas Becker, Volker Weispfennig: ···
Springer-Verlag, Graduate Texts 141

Sei $K[X_1, \ldots, X_n]$ der Polynomring in n Variablen über dem Körper K, $\mathbb{T}$ die Halbgruppe der Terme $X^a = X_1^{a_1} \ldots X_n^{a_n}$ und $\mathbb{M}$ die Halbgruppe der Monome cX^a , $0 \neq c \in K$. Wir betrachten eine Anordnung auf der Halbgruppe der Terme, die folgende Eigenschsften haben soll

(1) $1 \leq t \; \forall t \in \mathbb{T}$
(2) $u \leq v \Longrightarrow su \leq sv$

Eine solche Anordnung heißt Termordnung. Sie induziert eine Quasiordnung auf der Menge $\mathbb{M}$. Beispiele sind die lexikographische Ordnung–eigentlich die lexikographische Ordnung der Exponententupel– oder die inverse lexikographische Ordnung, die zur umgekehrten Reihenfolge der Variablen gehört. Es ist häufig nützlich, eine dieser Ordnungen, etwa die inverse lexikographische, mit der Totalgrad-Quasiordnung zu verbinden. Solche Ordnungen heißen gemischte Totalgradordnungen. Sei $deg(-)$ der Totalgrad eines Polynom. Die gemischte Totalgradordnung zur inversen lexikographischen Ordnung ist dann gegeben durch:

$$X^a > X^b \Longleftrightarrow$$
$$deg(X^a) > deg(x^b) \text{ oder } deg(x^a) = deg(x^b) \text{ und } a_{i_0} > b_{i_0} \; , \; a_{i_0+1} = b_{i_0+1}, \ldots$$

Eine Variante dieser letzten Termordnung ist die reverse lexikographische Totalgradordnung (Siehe Macaulay)

$$X^a > X^b \Longleftrightarrow$$
$$deg(X^a) > deg(x^b) \text{ oder } deg(x^a) = deg(x^b) \text{ und } a_{i_0} < b_{i_0} \; , \; a_{i_0+1} = b_{i_0+1}, \ldots$$

Wir betrachten im folgenden eine fest vorgegebene Anordnung von $\mathbb{T}$, die die angegebenen Eigenschaften besitzt. Der Begriff Gröbnerbasis bezieht sich immer auf eine solche Anordnung!

Sei $\mathbb{F}$ die Menge der endlichen Teilmengen von $\mathbb{T}$. Auf naheliegende Weise induziert die vorgegebene Termordnung eine Ordnung von $\mathbb{F}$ mit der leeren Menge als kleinstem Element. Man zeigt, daß $\mathbb{T}$ der absteigenden Kettenbedingung genügt und folgert, daß auch $\mathbb{F}$ die absteigende Kettenbedingung erfüllt:Eine bei der Anordnung absteigende Folge ist stationär.

Sei f Polynom. Wir bezeichnen mit $\mathbb{T}(f) \in \mathbb{F}$ die Menge der Terme, die in f auftreten und mit $\mathbb{M}(f)$ die Menge der Monome, die in f vorkommen. Für das Nullpolynom $f = 0$ ist $\mathbb{T}(f)$ die leere Menge. Der führende Term $IN(f)$ von $f \neq 0$ ist das größte Element in $\mathbb{T}(f)$. Das größte Element in $\mathbb{M}(f)$ heißt das führende Monom von f; es ist das Produkt von $IN(f)$ mit einer Konstanten $\neq 0$, dem führenden Koeffizienten. Sei im folgenden eine endliche, nicht leere Menge $\mathcal{P}$ von nicht verschwindenden Polynomen vorgegeben. Wir bezeichnen mit $\mathfrak{I}(\mathcal{P})$ das von $\mathcal{P}$ erzeugte Ideal des Polynomringes. Wir suchen einen euklidischen Restalgorithmus modulo $\mathcal{P}$. Sei f ein von Null verschiedenes Polynom.

Definition. f heißt reduzibel mod $\mathcal{P}$, wenn es ein Monom $m \in \mathbb{M}$ gibt und ein Polynom $p \in \mathcal{P}$, so daß $IN(p)m \in \mathbb{M}(f)$. Sei c der führende Koeffizient von p. Das Polynom $g = f - c^{-1}pm$ heißt das durch Elimination von $IN(p)m$ mod p reduzierte Polynom. Entsteht ein Polynom g aus f durch eine Kette solcher *elementarer* Reduktionsschritte mit Polynomen $p \in \mathcal{P}$, so schreibt man:

$$f \underset{\mathcal{P}}{\longrightarrow} g,$$

abgekürzt auch einfach

$$f \longrightarrow g.$$

Man sagt, daß g durch Reduktion mod P aus f ensteht. f heißt topreduziebel mod $\mathcal{P}$, wenn sogar gilt

$$IN(f) = IN(p)m$$

für passende Elemente $m \in \mathbb{T}$, $p \in \mathcal{P}$. Ein mod $\mathcal{P}$ nicht reduzibles Polynom heißt auch irreduzibel mod $\mathcal{P}$, kurz einfach irreduzibel.

Sei $f \underset{\mathcal{P}}{\longrightarrow} g$. Dann gilt

$$\mathbb{T}(f) > \mathbb{T}(g)$$

Eine absteigend geordnete Folge von endlichen Mengen von Termen ist stationär. Es folgt:

Lemma. *Eine Kette aufeinanderfolgender Reduktionsschritte mod $\mathcal{P}$ muß abbrechen.*

Definition und Lemma. *Gegeben sei ein Polynom f. Ein Polynom g heißt eine Normalform von f mod $\mathcal{P}$, wenn g nicht reduzibel mod $\mathcal{P}$ ist, also zum Beispiel das Nullpolynom ist und wenn gilt*

$$f \underset{\mathcal{P}}{\longrightarrow} g$$

Abgekürzt: g ist Normalform von f. Aus dem vorherigen Lemma erhält man: Jedes Polynom besitzt mindestens eine Normalform mod $\mathcal{P}$.

Warnung. Die Normalform ist im allgemeinen nicht eindeutig bestimmt.

Lemma.

(1) *Gegeben seien Polynome f, g, h mit $f - g \underset{\mathcal{P}}{\longrightarrow} h$. Dann gibt es Polynome f_1, g_1 mit $f \underset{\mathcal{P}}{\longrightarrow} f_1$, $g \underset{\mathcal{P}}{\longrightarrow} g_1$ und $f_1 - g_1 = h$.*

(2) *Angenommen für je zwei elementare Reduktionsschritte* $f \underset{\mathcal{P}}{\longrightarrow} h$, $f \underset{\mathcal{P}}{\longrightarrow} k$ *gibt es ein Polynom* j *mit* $h \underset{\mathcal{P}}{\longrightarrow} j$ *und* $k \underset{\mathcal{P}}{\longrightarrow} j$. *Dann gibt es für beliebige Reduktionen* $f \underset{\mathcal{P}}{\longrightarrow} h$, $f \underset{\mathcal{P}}{\longrightarrow} k$ *ein Polynom* j *mit* $h \underset{\mathcal{P}}{\longrightarrow} j$ *und* $k \underset{\mathcal{P}}{\longrightarrow} j$.

.

Zum Beweis.

(1) Wenn $f - g \underset{\mathcal{P}}{\longrightarrow} h$ ein elementarer Reduktionsschritt ist, kann man f_1, g_1 explizit angeben. Den allgemeinen Fall führt man durch Induktion nach der Anzahl der elementaren Reduktionsschritte auf diesen elementaren Fall zurück.
(2) Man nutzt die absteigende Kettenbedingung in $\mathbb{F}$ und beweist die Behauptung durch "artinsche Induktion" nach $\mathbb{T}(f)$.

Mit Hilfe dieses Lemmas zeigt man:

Satz. *Sei* $\mathfrak{I} = \mathfrak{I}(\mathcal{P})$ *Folgende Aussagen über die Menge* $\mathcal{P}$ *sind äquivalent:*

(1) *Jedes Polynom* f *besitzt eine eindeutig bestimmte Normalform.*
(2) *Eine der äquivalenten Aussagen von Teil (2) des vorhergehenden Lemmas ist für* $\mathcal{P}$ *erfüllt.*
(3) *Für* $f \in \mathfrak{I}$ *gilt* $f \underset{\mathcal{P}}{\longrightarrow} 0$.
(4) *Jedes Polynom* $f \in \mathfrak{I}$ *is topreduzibel mod* $\mathcal{P}$.
(5) *Die mod* $\mathcal{P}$ *nicht reduziblen Polynome bilden ein System von eindeutigen Repräsentanten mod* $\mathfrak{I}$.

Beweis von (1) $\Rightarrow$ (3). Ein Polynom $f \in \mathfrak{I}$ läßt sich darstellen als Summe $f = m_1 g_1 + \cdots + m_n g_n$ mit Monomen m_ν und Polynomen $g_\nu \in \mathcal{P}$. Wir beweisen die gesuchte Aussage durch Induktion nach der Anzahl m. Nach Induktionsvoraussetzung gilt $f - m_n g_n \underset{\mathcal{P}}{\longrightarrow} 0$. Dann gibt es wegen des vorhergehenden Lemmas, Teil (1), ein Polynom h mit:

$$f \underset{\mathcal{P}}{\longrightarrow} h \ , \ m_n g_n \underset{\mathcal{P}}{\longrightarrow} h.$$

Man kann h noch durch eine Normalform ersetzen. Dann ist h auch eine Normalform von $m_n g_n$. Wegen $m_n g_n \underset{\mathcal{P}}{\longrightarrow} 0$ und der vorausgesetzten Eindeutigkeit der Normalform ist $h = 0$.

Definition. Die Menge $\mathcal{P}$ heißt Gröbnerbasis des Ideals $\mathfrak{I} = \mathfrak{I}(\mathcal{P})$, wenn eine der äquivalenten Bedingungen des vorhergehenden Satzes erfüllt ist. Ist f ein Polynom, so schreibt man für die eindeutig bestimmte Normalform von f mod $\mathcal{P}$, den Rest mod $\mathcal{P}$, auch

$$f \bmod \mathcal{P}$$

Die Gröbnerbasis $\mathcal{P}$ heißt reduziert, wenn gilt

(1) Die führenden Monome von Polynomen aus $\mathcal{P}$ sind normiert, haben also den Koeffizienten 1.
(2) Jedes $p \in \mathcal{P}$ ist irreduzibel mod $\mathcal{P} \setminus \{p\}$.

Existenzsatz von Gröbnerbasen. *Jedes Ideal* $(\neq 0)$ *besitzt eine reduzierte Gröbnerbasis. Eine reduzierte Gröbnerbasis ist eindeutig bestimmt.*

Bemerkung. Nichtreduzierte Gröbnerbasen sind nicht eindeutig. Für die meisten Anwendungen, z.B. Prüfung der Zugehörigkeit eines Polynoms zu einem Ideal , genügt es irgendeine nichtreduzierte Gröbnerbasis des Ideals zu verwenden.

Zur Existenz. Man betrachte die partielle Ordnung der Teilbarkeit in der Menge $\mathbb{T}$ der Terme. Eine absteigende Kette von Termen bei dieser Teilbarkeitsordnung ist stationär. In einer unendlichen Menge von Termen gibt es immer ein Paar von Termen s, t mit $s|t$. Daraus folgt: Zu jeder nicht leeren Menge M von Termen ist die Teilmenge B aller minimalen Terme bzgl. der Teilbarkeitsanordnung endlich. Zu jedem Element von M gibt es einen Teiler in der Menge B, der Basis von M. Sei M die Menge der führenden Terme der Polynome $\neq 0$ des Ideals und B die Basis von M. Zu jedem $t \in B$ gibt es ein Polynom f_t mit führendem Koeffizienten 1 so daß gilt $IN(f_t) = t$. Man zeigt, daß die Menge dieser Polynome f_t eine Gröbnerbasis des Ideals ist. Die Auswahl von f_t zu t ist nicht eindeutig. Betrachte die Menge aller endlichen Teilmengen $\mathbb{F}$ der Menge $\mathbb{T}$ aller Terme. Die vorgegebene Termordnung induziert auf naheliegende Weise eine Ordnung auf dieser Menge. Man wähle f_t in der Menge der Polynome des Ideals mit führendem Term t und führendem Koeffizienten 1, so daß die Menge der Terme $\mathbb{T}(f_t)$ von f_t minimal ist. Man kann dann zeigen, daß f_t eindeutig bestimmt ist und daß die Menge der so bestimmten Polynome f_t eine reduzierte Gröbnerbasis ist.

Wie kann man konstruktiv entscheiden ob eine Menge von erzeugenden Elementen eines Ideals eine Gröbnerbasis ist? Dazu folgende Überlegungen. Seien f, g zwei von 0 verschiedene Polynome, cX^a das führende Monom von f, dX^b das führende Monom von g und der Term $m = s_1X^a = s_2X^b$ das kleinste gemeinsame Vielfache von X^a und X^b. Das s-Polynom von f und g ist

$$spoly(f, g) = ds_1 f - cs_2 g$$

Lemma. *Sei* $\mathcal{P}$ *eine nicht leere endliche Teilmenge von Polynomen* $\neq 0$. *Folgende Aussagen sind äquivalent.*

(1) $\mathcal{P}$ *ist eine Gröbnerbasis von* $\mathfrak{J}(\mathcal{P})$.

(2) *Seien* p_1, p_2 *Elemente aus* $\mathcal{P}$. *Dann verschwindet jede Normalform mod* $\mathcal{P}$ *von* $spoly(p_1, p_2)$

(3) *Für je zwei Polynome* $p_1, p_2 \in \mathcal{P}$ *gilt*

$$spoly(p_1, p_2) \underset{\mathcal{P}}{\longrightarrow} 0$$

Das heißt, daß sich diese s-Polynome auf irgendeine Weise zu 0 *mod* $\mathcal{P}$ *reduzieren lassen.*

Beweis. Wir nehmen an, daß die Bedingung (3) erfüllt ist. Es folg dann sofort: Für je zwei Polynome $p_1, p_2 \in \mathcal{P}$ und zwei Monom m_1, m_2 für die die führenden Monome von m_1p_1 und m_2p_2 gleich sind, gilt

$$m_1p_1 - m_2p_2 \underset{\mathcal{P}}{\longrightarrow} 0$$

Wir folgern die zweite der charakterisierenden Eigenschaften für Gröbnerbasen. Gegeben seien zwei elementare Reduktionen

$$f \underset{\mathcal{P}}{\longrightarrow} h_1 = f - m_1 p_1 \ , \ f \underset{\mathcal{P}}{\longrightarrow} h_2 = f - m_2 p_2$$

Dabei sind m_1, m_2 Monome und g_1, g_2 Polynome aus $\mathcal{P}$. Dann gilt $h_2 - h_1 = m_1 p_1 - m_2 p_2$. Es genügt zu zeigen

$$m_1 p_1 - m_2 p_2 \underset{\mathcal{P}}{\longrightarrow} 0$$

Diese Behauptung wurde bereits bewiesen, falls die führenden Terme von $m_1 p_1$ und $m_2 p_2$ gleich sind; denn dann sind nach Voraussetzung auch die führenden Monome dieser beiden Monome gleich. Wenn das nicht der Fall ist, sei z.B. $IN(m_1 p_1) < IN(m_2 p_2)$. Dann läßt sich $m_1 p_1 - m_2 p_2$ in zwei elementaren Reduktionsschritten zu Null reduzieren:

$$m_1 p_1 - m_2 g_2 \underset{\mathcal{P}}{\longrightarrow} m_1 p_1 \underset{\mathcal{P}}{\longrightarrow} 0$$

□

Bemerkung. Das Entscheidungsproblem ist durch dieses Lemma gelöst. Zu je zwei Polynomen der endlichen Menge $\mathcal{P}$ konstruiere man irgendeine Normalform h. Das ist immer konstruktiv möglich. Genau dann ist $\mathcal{P}$ Gröbnerbasis, wenn jedes dieser endlich vielen Polynome h verschwindet. Man hat damit ein konstruktives Entscheidungsverfahren.

Dieses im Lemma ist der Kernpunkt, wenn man einen Algorithmus zur Konstruktion von Gröbnerbasen, oder sogar reduzierten Gröbnerbasen finden will. Mit etwas Fantasie kann man leicht einen solchen Algorithmus konstruieren; etwa folgendermaßen: Zu je zwei Polynomen aus $\mathcal{P}$ berechnet man jeweils eine Normalform h des s-Polynoms dieser beiden Polynome. Verschwinden alle diese h, so ist $\mathcal{P}$ bereits Gröbnerbasis. Wenn nicht, so vergrößert man $\mathcal{P}$ durch Hinzunahme eines solchen nichtverschwindenden h und führt den gleichen Versuch mit der neuen Menge durch. usw.... Es gibt keine Folge t_ν von Termen mit $t_\nu \nmid t_\mu \ \forall \nu < \mu$. Deshalb muß dieses Verfahren schließlich mit einer Gröbnerbasis abbrechen. Sonst hätte die Folge der führenden Terme der schrittweise hinzugenommenen h diese Eigenschaft. Dieser Algorithmus ist natürlich für eine effiziente Anwenung sehr verbesserungsbedürftig. Er kann auch so verändert werden, daß er sogar eine reduzierte Gröbnerbasis liefert. Leider müssen alle Algorithmen bei großen Variablenzahlen im allgemeinen sehr langsam werden, wie die Abschätzungen im Abschnitt Komplexität zeigen. Siehe auch Weispfennig.

Anwendungen

Sei $\mathcal{P}$ Gröbnerbasis des Ideals $\mathfrak{I}$.

(1) Test auf Zugehörigkeit zu einem Ideal:
Ein Polynom f gehört genau dann zu $\mathfrak{I}$, wenn die Normalform f mod $\mathcal{P}$ verschwindet.

(2) Bestimmung des Durchschnitts $\mathfrak{I} \cap K[X_s, \ldots, X_n]$.
Bei einer geeigneten Termordnung, etwa der lexikographischen, ist $\mathcal{P} \cap K[X_s, \ldots, X_n]$ Gröbnerbasis von $\mathfrak{I} \cap K[X_s, \ldots, X_n]$.

Die tieferen Anwendungen findet man im Handbuch zu Macaulay; sie erfordern Methoden der kommutativen Algebra.

Zur Komplexität

Sei n die Anzahl der Variablen des betrachteten Polynomringes. Wir wollen der Einfachheit annehmen, daß die vorgegebene Termordnung eine gemischte Totalgradordnung ist.

Sei F eine endliche Menge von nicht verschwindenden Polynomen. Wir bezeichnen mit $maxdeg(F)$ das Maximum der Totalgrade der Polynome, den Maximalgrad von F. Sei G eine reduzierte Gröbnerbasis des von F erzeugten Ideals. Man kann zeigen, daß $maxdeg(G)$ das Minimum der Maximalgrade von beliebigen Gröbnerbasen dieses Ideals ist. Siehe die Bemerkung zur Konstruktion der reduzierten Gröbnerbasis und die dritte der vier äquvalenten definierenden Eigenschaften einer Gröbnerbasis. Das Wachstumsverhalten von $maxdeg(G)$ in Abhängigkeit von n und $maxdeg(F)$ ist ein Maß für die Komplexität, eine Gröbnerbasis zu finden. Folgende Resultate werden in Weißpfennigs Buch zitiert.

Aus einer Vermutung von Lazard erhält man folgende obere Schranke

$$maxdeg(G) \leq ((n+1).(maxdeg(F)+1))^{((n+1)2^{(dim(F)+1)})}$$

Dabei ist $dim(F)$ die Dimension der affinen algebraischen Mannigfaltigkeit, die durch das von F erzeugte Ideal definiert wird.

Ein weiteres vollständig bewiesenes Resultat besagt im wesentlichen, daß die doppelt exponentielle Abhängigkeit der oberen Schranke in Abhängigkeit von der Variablenzahl nicht verbessert werden kann.

Macauly spuckt übrigens als Zwischenresultate bei der Bestimmung von Gröbnerbasen homogener Ideale die immer weiter wachsenden Grade der gerade in Arbeit befindlichen Polnome aus.

Verallgemeinerung auf freie Moduln.

Sei $F = K[X_1, \ldots, X_n]^s$ ein endlicher freier Modul über einem Polynomring und seien die Elemente $e_i = (0, \ldots, 0, 1, 0, \ldots 0)$ die kanonischen Basiselemente von F. Terme des freien Moduls sind dann die Elemente $X^a e_i$. Sei eine Termordnung für die Terme X^a des Polynomringes vorgegeben. Macaulay betrachtet dann folgende Termordnung für die Terme von F

$$X^a e_i > X^b e_j \Leftrightarrow X^a > X^b \text{ oder } X^a = X^b \text{ und } i > j$$

Mit Hilfe dieser Termordnung kann man alle bisherigen Begriffe und Resultat auf Teilmengen von F übertragen. Man führt die Sätze über Untermoduln von F auf Sätze für in Z homogene Ideale im Polynomring $K[X_1, \ldots, X_n][Z_1, \ldots, Z_s]$ zurück. Dabei wird dieser Polynomring mit eine geeigneten bzgl. Z gemischten Totalgraduierung versehen.