Seminarausarbeitungen

Kommutative Algebra und Algebraische Geometrie

24. September 2006

Betreut von Ralf Gramlich und Max Horn

Inhaltsverzeichnis

1 Lokalisierung Teil 1 **4**
- 1.1 Einführung . . . 4
- 1.2 Brüche . . . 6
- 1.3 Hom und Tensorprodukt . . . 8

2 Lokalisierung Teil 2 **16**
- 2.1 Konstruktion von Primelementen . . . 16
- 2.2 Ringe und Moduln endlicher Länge . . . 17
- 2.3 Produkte von Integritätsringen . . . 25

3 Assoziierte Primideale und Primärzerlegung **27**
- 3.0 Definitionserinnerungen . . . 27
- 3.1 Assoziierte Primideale . . . 27
- 3.2 Primvermeidung . . . 29
- 3.3 Primärzerlegung . . . 32

4 Primärzerlegung Teil 2 **37**
- 4.1 Definitionserinnerungen . . . 37
- 4.2 Primärzerlegung und Primfaktorzerlegung . . . 38
- 4.3 Der graduierte Fall . . . 39
- 4.4 Informationen aus der Primärzerlegung gewinnen . . . 40
- 4.5 Eindeutigkeit . . . 43
- 4.6 Geometrische Interpretation . . . 45

5 Ganze Abhängigkeit und der Nullstellensatz **47**
- 5.1 Einführung . . . 47
- 5.2 Der Satz von Cayley-Hamilton und Nakayamas Lemma . . . 49
- 5.3 Normale Integritätsbereiche und der Normalisierungsprozess . . . 53

6 Quadriken **56**
- 6.1 Einleitung . . . 56
- 6.2 Der projektive Raum und Quadriken . . . 56
  - 6.2.1 Anmerkung . . . 56
  - 6.2.2 Der projektive Raum . . . 56
  - 6.2.3 Quadriken . . . 57
  - 6.2.4 Quadriken als Bilder von Abbildungen . . . 59
  - 6.2.5 Warum betrachtet man Quadriken in projektiven Räumen? . . . 61

6.3 Der Satz von Witt 62

7 Filtrierungen und das Artin-Rees Lemma 65
7.1 Einführung 65
7.2 Assoziierte graduierte Ringe und Moduln 66
7.3 Die aufgeblasene Algebra 68
7.4 Der Krull Schnitt Satz 69
7.5 Der Tangentialkegel 71

8 Flache Familien 72
8.1 Flachheit 72
8.2 Familien 76

9 Vervollständigungen und das Henselsche Lemma Teil 1 78
9.1 Einführung 78
9.2 Eigenschaften von Vervollständigungen 80

10 Vervollständigungen und das Henselsche Lemma Teil 2 85
10.1 Das Henselsche Lemma 85
10.2 Heben von idempotenten Elementen 89
10.3 Struktursatz von Cohen 91

11 Gröbnerbasen 95
11.1 Monome und Terme 95
11.2 Termordnungen 98
11.3 Berechnung von Gröbnerbasen 103
11.4 Berechnung von Syzygien 108
11.5 Verallgemeinerte Initialideale 110

1 Lokalisierung Teil 1

Oliver Schmitt

1.1 Einführung

Vor der formalen Einführung der Lokalisierung soll in diesem Abschnitt anhand des Beispiels von algebraischen Mengen der Begriff der Lokalisierung motiviert werden. Häufig können Fragestellungen von kommutativen Ringen auf den lokalen Fall reduziert werde, ein lokaler Ring ist ein Ring mit nur einem maximalen Ideal. Die Grundlagen, das heißt was Lokalisierung bedeutet und einige Folgerungen werden im Weiteren erarbeitet werden.
Sei nun $p \in X \subset A_K^r := \{(a_1, ..., a_r) | a_1, ..., a_r \in K\}$, wobei X eine algebraische Menge ist.

Definition 1.1.1. X wird eine **(affine) algebraische Menge** genannt, wenn ein $T \subset K[x_1, ..., x_r]$ existiert, so dass $X = \{(a_1, ..., a_r) \in A_K^r | f(a_1, ..., a_r) = 0 \forall f \in T\}$ ist. Algebraische Mengen sind also die Nullstellenmenge von einer Menge von gegebenen Polynomen.

Definition 1.1.2. Als **Zariski-Topologie** wird die Topologie offener Mengen über dem affinen Raum eines algebraisch abgeschlossenen Körpers K der Form: $D(T) = \{x \in K^n \mid \exists f \in T. f(x) \neq 0\}$ mit $T \subset K[x_1, ..., x_r]$ bezeichnet. Die leere Menge ist als Nicht-Nullstellenmenge des Nullpolynoms und die Grundmenge als solche eines konstanten Polynoms $\neq 0$ also beispielsweise offen.

Nun werden wir beliebige kleine offene Umgebungen um den Punkt p in der Zariski Topologie betrachten. Die offenen Umgebungen ergeben sich als Mengen der Form $X - Y$, wobei Y eine algebraische Teilmenge von X ist, die p nicht enthält, das bedeutet jeder Punkt von Y ist auch in X und Y wird durch die Nullstellen von Polynomfunktionen über K definiert.
Im Allgemeinen ist dieses $X - Y$ keine algebraische Menge. Um dies zu veranschaulichen betrachte das Beispiel der Gausschen Zahlenebene als X und einen beliebigen Punkt als Y über dem Körper der komplexen Zahlen. Die X und Y definierenden Polynomfunktionen sind hier als holomorphe Funktionen aufzufassen, da beliebige Polynomfunktionen über den komplexen Zahlen holomorph sind. Wäre nun $X - Y$ eine algebraische Menge, so müßte die definierende Funktion überall 0 sein, nur an dem Punkt in Y nicht. Eine solche Funktion ist beschränkt durch den Wert, den es an diesem Punkt annimmt, nach dem Satz von Liouville ist eine beschränkte holomorphe Funktion aber konstant, dann

kann die Funktion allerdings nicht die geforderte Gestalt haben.
Betrachten wir nun kleine Umgebungen von p, so bedeutet dies, dass Y eine sehr große Menge ist, dann ist sie anschaulicherweise durch wenige Funktionen definiert, die, da wir Umgebungen um p betrachten, bei p nicht verschwinden. Im Folgenden betrachten wir den Speziallfall sehr kleiner Umgebungen, bei denen Y nur durch eine einzige Funktion, die wir im Folgenden f nennen werden, bestimmt wird, die bei p nicht verschwindet. Wir werden sehen, dass sich $X - Y$ als algebraische Menge in A_K^{r+1} auffassen läßt. Um dies einzusehen müssen wir algebraische Mengen von einer anderen Seite verstehen lernen, dies führt zur folgenden Definition.

Definition 1.1.3. Das **Verschwindungsideal** zu einer algebraischen Menge $X \subset A_K^r$ ist das Ideal $I(X) := \{f \in K[x_1, ..., x_r] | f(a_1, ...a_r) = 0 \text{ für alle } (a_1, ..., a_r) \in X\}$. Der Ring der Funktionen, die auf X nicht völlig verschwinden wird **Koordinatenring** $A(X)$ genannt und ist als $A(X) = K[x_1, ..., x_r]/I(X)$ aufzufassen. Wir sagen X **korrespondiert** zu dem Ideal $I(X)$, im Folgenden, wenn der Zusammenhang ersichtlich ist, auch nur I genannt.

Die Punkte aus $X - Y$ sind die Punkte $x \in X$ mit $f(x) \neq 0$, es gibt also ein $z(x)$ mit $z(x)f(x) = 1$ für $x \in X - Y$. Die Funktion z nennen wir zu f invers und den Vorgang das Invertieren einer Funktion. Invertieren wir alle Funktionen von $A(X)$, die bei p nicht verschwinden, so wird dies der **lokale Ring von X bei p** genannt.

Definition 1.1.4. Als **lokaler Ring** wird im Allgemeinen ein Ring bezeichnet, der nur ein maximales Ideal enthält.

Die Bezeichnung macht in diesem Fall also Sinn, da das maximale Ideal vom lokalen Ring von X bei p gerade die Menge aller Funktionen ist, die bei p verschwinden, alle anderen sind invertierbar und wären sie in einem Ideal enthalten, so wäre das Ideal schon der ganze Ring. In anderen Zusammenhängen wird daher ein lokaler Ring häufig auch als ein Ring definiert, in dem das maximale Ideal gerade aus allen Nichteinheiten besteht.
Korrespondiert X nun zu einem Ideal I dann korrespondiert $X - Y$ durch Projektion auf die ersten r Koordinaten zu einer Teilmenge von A_K^{r+1} definiert durch das Ideal $J = I + (zf - 1) \subset K[x_1, ..., x_r, z]$. Um dies einzusehen sei bemerkt, dass für alle Punkte aus $x \in X - Y$ Funktionen aus I stets 0 ergeben und weiter nach den Betrachtungen oben $z(x)f(x) = 1$ ist. Für alle anderen $x \in X$ werden zwar die Funktionen aus I wieder 0, doch ist dann $f(x) = 0$. Wir können $X - Y$ also als die algebraische Menge in A_K^{r+1} auffassen, die zu J korrespondiert, wobei $X - Y \subset X$ durch Projektion auf die ersten r Koordinaten.

Beispiel 1.1.5. Sei nun $X = A_K^1$ die **affine Gerade** und $Y = \{0\} = \{x_1 | f(x_1) = 0\}$ mit $f(x_1) = x_1$, also der Nullpunkt. $A(X)$ besteht also aus der Funktion $f(x_1) = 0$, da es die ganze Menge A_K^1 umfasst. Betrachtet man nun das Ideal $I(X)$ so ist dies das Nullideal und damit $J = 0 + (zf - 1) = zf - 1$. Damit ist also $A(X - Y) = K[x_1, z]/J = A(X)[z]/(zf - 1)$. Also ist z(x) als Hyperbel in der **affinen Ebene** A_K^2 zu verstehen, da aus $(z(x)f(x) - 1) = 0$ direkt $z(x) = \frac{1}{f(x)} = \frac{1}{x_1}$ folgt.

1.2 Brüche

Sei im Folgenden R ein kommutativer Ring und $U \subset R$ eine multiplikative abgeschlossene Teilmenge von R, das heißt, für $u, v \in U$ folgt $uv \in U$, sowie das "leere Produkt", damit ist 1 gemeint, ist in U. Sei weiter M ein R-Modul.

Definition 1.2.1. Die Lokalisierung von M an U, geschrieben als $M[U^{-1}]$ oder $U^{-1}M$ besteht aus den Äquivalenzklassen (m, u), $m \in M$, $u \in U$ mit $(m, u) \sim (m', u') \Leftrightarrow$ es existiert ein $v \in U$ mit $v(u'm - um') = 0$ in M. Schreibe (m, u) als $\frac{m}{u}$.
$M[U^{-1}]$ ist ein R-Modul vermöge: $\frac{m}{u} + \frac{m'}{u'} := \frac{u'm+um'}{uu'}$ und $r(\frac{m}{u}) := \frac{rm}{u}$.
Der Homomorphismus $\phi : M \to M[U^{-1}]$, $m \mapsto \frac{m}{1}$ wird **natürliche Abbildung** genannt.
Die Lokalisierung ist auch für beliebige Teilmengen $U \subset R$ definiert. Sei hierfür $\overline{U}$ die multiplikativ abgeschlossene Menge aller Produkte von Elementen von U, so definiere: $M[U^{-1}] := M[\overline{U}^{-1}]$.

Bemerkung 1.2.2. Ist $M = R$, so ist die Lokalisierung ein Ring mit der Multiplikation definiert durch $\frac{r}{u} \cdot \frac{r'}{u'} = \frac{rr'}{uu'}$
und $M[U^{-1}]$ ist $R[U^{-1}]$-Modul mit: $\frac{r}{u} \cdot \frac{m}{u'} = \frac{rm}{uu'}$, wobei $r \in R$, $m \in M$, sowie $u, u' \in U$.

Beispiel 1.2.3. Quotientenkörper eines Integritätsringes R:
Der Quotientenkörper $Q(R)$ ist aufzufassen als Lokalisierung $R[U^{-1}]$ mit $U = R - \{0\}$. Als konkretes Beispiel sei hier der Ring der ganzen Zahlen $\mathbb{Z}$ genannt, dessen Quotientenkörper $\mathbb{Q}$ mit $U = \mathbb{Z} - \{0\}$ auch durch $\mathbb{Q} = \mathbb{Z}[U^{-1}]$ ausgedrückt werden kann.

Proposition 1.2.4. (i) *Sei $U \subset R$ multiplikativ abgeschlossene Teilmenge, M ein R-Modul, dann gilt: $\frac{m}{1} = 0 \Leftrightarrow$ es existiert ein $u \in U$ mit $um = 0$.*

(ii) *Ist weiter M endlich erzeugt, so gilt: $M[U^{-1}] = 0 \Leftrightarrow$ es existiert ein u mit $uM = 0$.*

Beweis. zu a) Angenommen es existiert ein $u \in U$ mit $um = 0$, so gilt: $(0, u) \sim (m, 1)$, da $1 \cdot (1 \cdot 0 - um) = 0$.
Ist umgekehrt $(0, u') \sim (m, 1)$ so folgt: $v'(1 \cdot 0 - u'm) = 0$ mit $v' \in U \Leftrightarrow v'u'm = 0$. Nun ist $u = v'u' \in U$ das gesuchte Element und a) gezeigt.
zu b) Angenommen es existiert ein $u \in U$ mit $u \cdot M = 0$ so folgt $(m', u') \sim (0, v)$ für alle $(m', u') \in M[U^{-1}]$, da $u(m'v - u' \cdot 0) = um'v = 0$. Also ist $M[U^{-1}] = 0$.
Ist umgekert $M[U^{-1}] = 0$. Seien m_i die Erzeuger von M. Insbesondere also $(m_i, u') \sim (0, 1)$ existieren $u_i \in U$ mit $u_i(m_i - 0 \cdot u') = u_i m_i = 0$. Da R kommutativ ist, ist $u := \prod_i u_i$ das gesuchte u mit $uM = 0$. □

Definition 1.2.5. Es ist der **Quotientenring K(R)** definiert als $R[U^{-1}]$ mit $u \in U$, genau dann, wenn $u \in R$ kein Nullteiler ist. Nach Proposition 1.2.4 ist $K(R)$ die größte Lokalisierung von R, bei welcher der natürliche Homomorphismus ϕ injektiv ist.

Bemerkung 1.2.6. Es gilt: $P \subset R$ Primideal, daraus folgt, dass $R - P$ multiplikativ abgeschlossen ist.

Sei $P \subset R$ Primideal, sowie M ein R-Modul und $U = R - P$.
Schreibe: $R_P := R[U^{-1}]$, $M_P := M[U^{-1}]$, sowie für den **Klassenkörper** von R nach P: $\kappa(P) = R_P/P_P$, wobei $\frac{r}{u} \in P_P$, falls $\frac{r}{u} \in R_P$ und $r \in R$ ist.
Ist R ein Integritätsbereich, so dass 0 also ein Primideal ist, dann gilt für den Quotientenkörper von R: $Q(R) = R_0 = \kappa(0)$.

Definition 1.2.7. Sei $\phi : M \to N$ ein R-Modul-Homomorphismus sowie U eine multiplikativ abgeschlossene Teilmenge von R, dann existiert ein Homomorphismus $\phi[U^{-1}] : M[U^{-1}] \to N[U^{-1}]$ mit $\frac{m}{u} \mapsto \frac{\phi(m)}{u}$, der die **Lokalisierung von** ϕ genannt wird. Dadurch wird die Lokalisierung zu einem Funktor von der Kategorie der R-Moduln in die Kategorie der $R[U^{-1}]$-Moduln.

Bemerkung 1.2.8. Ist $\phi : R \to S$ ist ein Ringhomomorphismus, wobei Elemente von U auf Einheiten in S abgebildet werden, so exisitiert eine eindeutige Erweiterung $\phi' : R[U^{-1}] \to S$. Dies wird die **universelle Eigenschaft der Lokalisierung** genannt. Die Erweiterung ist ein Homomorphismus, da $\frac{r}{u}$ auf $\phi(r)\phi(u)^{-1}$ abgebildet wird, die Relationen erhält. Da die Inverse eindeutig ist, ist auch ϕ' eindeutig.

Proposition 1.2.9. *Sei $\phi : R \to R[U^{-1}]$ die natürliche Abbildung $r \mapsto \frac{r}{1}$.*

(i) *Für jedes Ideal $I \subset R[U^{-1}]$ gilt $I = \phi^{-1}(I)R[U^{-1}]$. Die Abbildung $I \mapsto \phi^{-1}(I)$ ist eine Injektion von der Menge der Ideale von $R[U^{-1}]$ in die Menge der Ideale von R. Sie erhält Inklusionen und Intersektionen und bildet Primideale auf Primideale ab.*

(ii) *Es sind äquivalent:*

  (a) *Ein Ideal $J \subset R$ ist von der Form $\phi^{-1}(I)$ für ein Ideal $I \subset R[U^{-1}]$.*
  (b) $J = \phi^{-1}(IR[U^{-1}])$
  (c) *für alle $u \in U$ gilt: u ist kein Nullteiler mod J in dem Sinne, dass für $r \in R$ und $ru \in J$ folgt $r \in J$.*

(iii) *Insbesondere: $I \mapsto \phi^{-1}(I)$ ist eine Bijektion zwischen Primidealen aus $R[U^{-1}]$ und jenen aus R.*

Beweis. zu a) Falls $a \in \phi^{-1}(I)R[U^{-1}]$ so ist $a = i'\frac{r}{u} = \frac{i'r}{u} = \frac{i'}{1}\frac{r}{u} \in I$. Ist umgekehrt $i \in I$, so ist $i = \frac{r}{u}$. Da $i \cdot \frac{u}{1} = \frac{r}{1} \in I$ ist folgt $r \in \phi^{-1}(I)$, also $r \cdot \frac{1}{u} \in \phi^{-1}(I)R[U^{-1}]$. Also ist $I = \phi^{-1}(I)R[U^{-1}]$.
Sei nun weiter $\phi^{-1}(I) = \phi^{-1}(J) \Rightarrow I = \phi^{-1}(I)R[U^{-1}] = \phi^{-1}(J)R[U^{-1}] = J$. Also ist ϕ^{-1} injektiv.
Ist $\phi : R \to S$ ein beliebiger Homomorphismus , dann erhält die Abbildung $I \mapsto \phi^{-1}(I)$, die Teilmengen auf Teilmengen abbildet Inklusionen und Intersektionen. Ist weiter ϕ ein Ringhomomorphismus und $I \subset S$ ein Ideal, dann ist $\phi^{-1}(I)$ ein Ideal von R. Weiterhin induziert ϕ mit dem Homomorphiesatz eine Inklusion $R/\phi^{-1}(I) \cong X \subset S/I$. Ist nun I prim, so folgt: S/I ist ein Integritätsbereich und es folgt $R/\phi^{-1}(I)$ ist ein Integritätsbereich und das ist äquivalent dazu, dass $\phi^{-1}(I)$ prim ist.

zu b) (i) $\Rightarrow$ (ii), also $J = \phi^{-1}(I)$. Nach a) gilt: $JR[U^{-1}] = \phi^{-1}(I)R[U^{-1}] = I$, somit $\phi^{-1}(JR[U^{-1}]) = \phi^{-1}(I)$.
(ii) $\Rightarrow$ (i) gilt, da $JR[U^{-1}]$ ein Ideal von $R[U^{-1}]$ ist.
(i, ii) $\Rightarrow$ (iii), Da es zwischen R und $R[U^{-1}]$ den natürlichen Homomorphismus gibt und nach (i) $J = \phi(I)^{-1}$ ist, folgt nach Argument wie im Beweis von a), dass $R/J \cong X \subset R[U^{-1}]/I$. Da für jedes $u \in U$ gilt: $u \notin I$, sonst $1 \in I$ und damit $I = R$ impliziert u aus R/J die Existenz eines $u_x \in X$, was eine Einheit in $R[U^{-1}]/I$ ist. Angenommen es existiert ein $t \in R/J$ mit $tu = 0$, das impliziert die Existenz eines $t_x \in X \subset R[U^{-1}]/I$ mit $t_x u_x = 0$, dann kann u_x aber keine Einheit sein, ein Widerspruch, also ist kein $u \in U$ ein Nullteiler mod J.
(iii) $\Rightarrow$ (ii) Ist $r \in J$ so folgt $r \in \phi^{-1}(r \cdot \frac{1}{1}) \Rightarrow J \subset \phi^{-1}(JR[U^{-1}])$. Ist umgekehrt $r \in \phi^{-1}(JR[U^{-1}]) \Rightarrow \frac{r}{1} \in JR[U^{-1}] \Rightarrow \frac{r}{1} = \frac{j}{u}$ für ein $j \in J$ und ein $u \in U$. Also: $(r, 1) \sim (j, u)$ somit folgt es existiert ein u' mit $u'(ru - j) = 0 \Rightarrow u'ur = u'j \in J$, da nun u ebenso wie u' keine Nullteiler mod J sind, folgt $r \in J$. Das impliziert $\phi^{-1}(JR[U^{-1}]) \subset J$ und schließlich: $J = \phi^{-1}(JR[U^{-1}])$.

zu c) Die Abbildung $I \mapsto \phi^{-1}(I)$ ist nach a) injektiv und surjektiv, da für jedes $u \in U$ aber $u \notin P$, wobei P ein Primideal von R ist, folgt, dass u kein Nullteiler mod P ist und somit $P = \phi^{-1}(P')$ für ein Primideal $P' \subset R[U^{-1}]$. □

Folgerung 1.2.10. *Die Lokalisierung eines noetherschen Ringes ist noethersch.*

Beweis. Sei $I \subset R[U^{-1}]$ ein Ideal. Nach Proposition 1.2.9 folgt: $I = \phi^{-1}(I)R[U^{-1}]$. Also wird I von einer Liste von Erzeugern von $\phi^{-1}(I)$ erzeugt. Da R noethersch ist, ist diese endlich, es folgt direkt, dass $\phi^{-1}(I)$ und damit I auch endlich erzeugt sind. □

1.3 Hom und Tensorprodukt

Im Folgenden werden zunächst einige Beobachtungen über die Homomorphismengruppe zweier Moduln und über das Tensorprodukt gegeben. Anschließend wird ein Zusammenhang zwischen dem Tensorprodukt und Lokalisierung hergestellt, der den Beweis einiger Lemmata möglich macht. Seien im Folgenden M, N R-Moduln.

Definition 1.3.1. $\mathrm{Hom}_R(M, N)$ ist die Homomorphismengruppe der Homomorphismen $M \to N$ zwischen den Moduln M und N.

Bemerkung 1.3.2. Hom_R wird durch folgende Definitionen zum R-Modul: $(\phi{+}\psi)(u) := \phi(u) + \psi(u)$ und $(r\phi)(m) := r\phi(m) = \phi(rm)$ für $r \in R$ und $\phi \in \mathrm{Hom}_R(M, N)$.

Hier nun einige weitere Eigenschaften:

Lemma 1.3.3. $\mathrm{Hom}_R(R, N) \cong N$ *mittels* $\phi \mapsto \phi(1)$.

Lemma 1.3.4. *Seien* $\alpha : M' \to M$ *und* $\beta : N \to N'$ *Homomorphismen, dann gibt es einen induzierten Homomorphismus* $\mathrm{Hom}_R(\alpha, \beta) : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N')$, $\phi \mapsto \beta\phi\alpha$.

Lemma 1.3.5. Hom *bringt direkte Summen im ersten und direkte Produkte im zweiten Argument zu direkten Produkten wie folgt:*
$\mathrm{Hom}_R(\bigoplus_i M_i, N) = \prod_i \mathrm{Hom}_R(M_i, N)$
$\mathrm{Hom}_R(M, \prod_i N_i) = \prod_i \mathrm{Hom}_R(M, N_i)$

Definition 1.3.6. Eine Komposition von Abbildungen der Form $M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$ heißt **exakt**, falls $ker(\psi) = im(\phi)$ ist.

Definition 1.3.7. Eine Komposition von Abbildungen der Form $0 \to M' \to M \to M'' \to 0$ heißt **kurze exakte Sequenz**, falls die Sequenz überall exakt ist.

Lemma 1.3.8. Hom *ist ein linksexakter Funktor, das bedeutet:*
Ist $0 \to A \to B \to C$ *eine exakte Sequenz, so folgt, dass*
$0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C)$ *exakt ist.*
Ebenso gilt, falls:
$A \to B \to C \to 0$ *eine exakte Sequenz ist, so ist*
$0 \to \mathrm{Hom}_R(C, N) \to \mathrm{Hom}_R(B, N) \to \mathrm{Hom}_R(A, N)$ *auch exakt.*

Beispiel 1.3.9. Bestimme $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m))$. Da ein Homomorphismus von der zyklischen Gruppen $\mathbb{Z}/(n)$ nach $\mathbb{Z}/(m)$ durch das Bild der 1 eindeutig festgelegt ist wird im Folgenden dieses Bild betrachtet und daraus eine Isomorphie hergeleitet. Da $\phi(n) = \phi(0) = 0$ ist folgt $\phi(n) = n\phi(1) = xm$ für ein $x \in \mathbb{Z}/(m)$, somit teilen n und m also $n\phi(1)$ und damit ist $n\phi(1)$ ein Vielfaches von $kgV(n, m)$. Somit können wir schreiben $n\phi(1) = y \cdot kgV(n, m) = y\frac{nm}{ggT(n,m)}$ und damit $\phi(1) = \frac{ym}{ggT(n,m)}$ für jedes y ist ϕ ein unterschiedlicher Homomorphismus, solange $\phi(1) < m$ ist, da $\frac{ym}{ggT(n,m)} = \frac{(y+zggT(n,m))m}{ggT(n,m)}$ ist. Hieraus folgt direkt: $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \cong X \subset \mathbb{Z}/(m) \cong \mathbb{Z}/ggT(n, m)$ vermöge $\phi \mapsto \phi(1) \mapsto y$.

Bilineare Abbildungen werden in vielerlei Fragestellungen benötigt, dies sind Abbildungen $\psi : M \times N \to P$, welche die folgenden Bedingung erfüllen: $\psi((am+a'm') \times (bn+b'n')) = ab\psi(m \times n) + a'b\psi(m' \times n) + ab'\psi(m \times n') + a'b'\psi(m' \times n')$ zwischen R-Moduln M, N und P. ψ ist im allgemeinen kein Homomorphismus.
Man könnte mit Blick auf bilineare Abbildungen das Tensorprodukt $M \otimes_R N$ zunächst einmal informell definieren als den Modul mit gerade genug Relationen, so dass $M \times N \to M \otimes_R N$ bilinear ist.

Definition 1.3.10. Ist $\psi : M \times N \to P$ eine R-bilineare Abbildung, so gibt es einen eindeutigen Homomorphismus $\phi : M \otimes_R N \to P$ mit $\psi(m \times n) = \phi(m \otimes n)$. Dies wird auch manchmal **universelle Eigenschaft des Tensorprodukts** genannt. Völlig gleichwertig kann man das Tensorprodukt auch aus den Relationen der Bilinearität wie folgt definieren: $M \otimes_R N$ ist der Modul mit Erzeugern $\{m \otimes n | m \in M, n \in N\}$ und Relationen entsprechend der Bilinearität, nämlich $(am+a'm') \otimes (bn+b'n') = ab(m \otimes n) + a'b(m' \otimes n) + ab'(m \otimes n') + a'b'(m' \otimes n')$. Insbesondere also: $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$. Aus der Definition des Tensorproduktes folgt, dass die Abbildung $m \times n \mapsto m \otimes n$ eine bilineare Abbildung von $M \times N \to M \otimes_R N$ ist. Weiter folgt: Ist $\phi : M \otimes_R N \to P$ ein

Homomorphismus, dann ist die Abbildung $\psi : M \times N \to P$ definiert durch $\psi(m \times n) := \phi(m \otimes n)$ bilinear. Ist der Ring R aus dem Kontext klar ersichtlich, so wird $M \otimes N$ häufig als $M \otimes N$ abgekürzt.

Bemerkung 1.3.11. (i) Nicht jedes Element von $M \otimes_R N$ läßt sich als $m \otimes n$ schreiben. Jedes Element hat in der Regel viele Darstellungen der Form $\sum_i m_i \otimes n_i$ mit $m_i \in M$ und $n_i \in N$.

(ii) Es ist gewöhnlich nicht einfach zu entscheiden, ob zwei Elemente $\sum_i m_i \otimes n_i$ und $\sum_i m'_i \otimes n'_i$ gleich sind.

Es folgen noch einige Eigenschaften des Tensorprodukts, die einige Ähnlichkeit zu obigen Eigenschaften der Homomorphismengruppe aufweisen.

Lemma 1.3.12. *$M = M \otimes_R R = R \otimes_R M$ durch Isomorphismen $1 \otimes m \mapsto m \otimes 1 \mapsto m$. Weiter ist $M \otimes_R N \cong N \otimes_R M$ durch $m \otimes n \mapsto n \otimes m$.*

Lemma 1.3.13. *Sind $\alpha : M' \to M$ und $\beta : N \to N'$ Homomorphismen, so existiert ein Homomorphismus $\alpha \otimes \beta : M' \otimes_R N' \to M \otimes_R N$ mit $m' \otimes n' \mapsto \alpha(m') \otimes \beta(n')$.*

Lemma 1.3.14. *Das Tensorprodukt erhält direkte Summen in folgendem Sinne: Falls $M = \oplus_i M_i$ so folgt $M \otimes_R N = \oplus_i (M_i \otimes_R N)$.*

Definition 1.3.15. Als **Kokern** eines Homomorphismus wird die Bildmenge faktorisiert nach dem Bild des Homomorphismus bezeichnet. Also: Sei $\phi : A \to B$ ein Modulhomomorphismus, dann ist $coker(\phi) := B/im(\phi)$.

Lemma 1.3.16. *Das Tensorprodukt erhält Kokerne. Sei $\alpha : M' \to M$ eine Abbildung mit $coker(\phi) = M''$, so ist für jeden Modul N der Kokern des induzierten Homomorphismus $\alpha \otimes 1 : M' \otimes_R N \to M \otimes_R N$ gleich $M'' \otimes_R N$. Dies wird häufig in Form von exakten Sequenzen geschrieben, in diesem Sinne erhält das Tensorprodukt rechtsexakte Sequenzen. In Formeln heißt das:*
$M' \to M \to M'' \to 0 \Rightarrow M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$.

Bemerkung 1.3.17. Ist M ein R-Modul und S eine R-Algebra, dann ist $S \otimes_R M$ ein R-Modul und ein S-Modul vermöge: $s(t \otimes m) := st \otimes m$ für $s, t \in S$ und $m \in M$.
Sind A und B beide R-Algebren, so ist $A \otimes_R B$ auch eine R-Algebra mit der Multiplikation $(a \otimes b)(c \otimes d) = (ac) \otimes (bd)$.

Beispiel 1.3.18. Charakterisierung von $\mathbb{Z}/(n) \otimes \mathbb{Z}/(m)$. Behauptung: $\mathbb{Z}/(n) \otimes \mathbb{Z}/(m) \cong \mathbb{Z}/(ggt(n, m))$. Nach der universellen Eigenschaft von Tensorprodukten reicht es zu zeigen, dass $\beta : \mathbb{Z}/(n) \times \mathbb{Z}/(m) \to \mathbb{Z}/(ggt(m, n))$ mit $a \times b \mapsto ab$ bilinear ist und der induzierte Homomorphismus $\mathbb{Z}/(n) \otimes \mathbb{Z}/(m) \to \mathbb{Z}/(ggt(m, n))$ einen wohldefinierten Umkehrhomomorphismus hat. Es ist $\beta(am + a'm', bn + b'n') = (am + a'm')(bn + b'n') = abmn + ab'mn' + a'bm'n + a'b'm'n' = ab\beta(m, n) + ab'\beta(m, n') + a'b\beta(m', n) + a'b'\beta(m', n')$. Es folgt also, dass $\beta' : \mathbb{Z}/(n) \otimes \mathbb{Z}/(m) \to \mathbb{Z}/(ggt(m, n))$ ein Homomorphismus ist. Betrachte nun weiter die Abbildung $\alpha : c \mapsto 1 \otimes c$. Es ist $\beta \circ \alpha(k) = \beta(1 \otimes k) = k$, sowie

$\alpha \circ \beta(k \otimes j) = \alpha(kj) = 1 \otimes kj = k(1 \otimes j) = k \otimes j$. Ist nun α wohldefiniert und ein Homomorphismus, so ist die Behauptung gezeigt. Es gilt $ggt(m,n) = um + vn$ mit $u, v \in \mathbb{Z}$, sei nun $a = b$ in $\mathbb{Z}/ggt(m,n)$ und damit $\alpha(a) = \alpha(b + ggt(m,n)) = \alpha(b + um + vn) = 1 \otimes (b + um + vn) = 1 \otimes b + 1 \otimes um + 1 \otimes vn = 1 \otimes b + m(1 \otimes u) = 1 \otimes b + m \otimes u = 1 \otimes b = \alpha(b)$. Weiter ist $\beta(rc + sd) = 1 \otimes (rc + sd) = 1 \otimes rc + 1 \otimes sd = r(1 \otimes c) + s(1 \otimes d) = r\beta(c) + s\beta(d)$. Damit ist die Isomorphie gezeigt.

Beispiel 1.3.19. Charakterisierung von $K[x] \otimes_K K[y]$ als K-Algebra. Betrachte den Algebra-Homomorphismus $\phi : K[x,y] \to K[x] \otimes_K K[y]$ mit $\sum_{i,j} a_{ij} x^i y^j \mapsto \sum_{i,j} a_{ij}(x^i \otimes y^j)$. Dass dies ein Homomorphismus ist, wird im Folgenden gezeigt, danach die Bijektivität: $\phi(\sum_{i,j} a_{ij} x^i y^j + \sum_{i,j} b_{ij} x^i y^j) = \phi(\sum_{i,j}(a_{ij} + b_{ij}(x^i y^j))) = \sum_{i,j}(a_{ij} + b_{ij})(x^i \otimes y^j) = \sum_{i,j} a_{ij}(x^i \otimes y^j) + \sum_{i,j} b_{ij}(x^i \otimes y^j)$. Weiter ist $\phi(k \sum_{i,j} a_{ij} x^i y^j) = \phi(\sum_{i,j} k a_{ij} x^i y^j) = \sum_{i,j} k a_{ij}(x^i \otimes y^j) = k \sum_{i,j} a_{ij}(x^i \otimes y^j) = k\phi(k \sum_{i,j} a_{ij} x^i y^j)$ und zuletzt: $\phi((\sum_{i,j} a_{ij} x^i y^j)) \cdot (\sum_{k,l} b_{kl} x^k y^l)) = \phi(\sum_{i,j,k,l} a_{ij} b_{kl} x^{i+k} y^{j+l}) = \sum_{i,j,k,l}(a_{ij} + b_{kl})(x^{i+k} \otimes y^{j+l}) = \sum_{i,j}(a_{ij})(x^i \otimes y^j) \cdot \sum_{k,l}(b_{kl})(x^k \otimes y^l) = \phi(\sum_{i,j} a_{ij} x^i y^j \cdot \phi(\sum_{k,l} a_{kl} x^k y^l))$. Der Homomorphismus ist nun injektiv. Denn falls $\phi(p(x)) = 0$ ist, so muss schon jeder Faktor $a_{ij} = 0$ sein, und damit ist nur $\phi(0) = 0$ möglich. Surjektiv ist er, da alle Erzeuger des Tensorproduktes, das sind nach der Definition die $p(x) \otimes q(y)$ darstellbar sind, dies folgt aus der Bilinearität des Tensorproduktes, $p(x) \otimes q(y)$ wird nach jedem Summanden zerlegt und die vorfaktoren schließlich aus beiden Argumenten vorgezogen, dann ist das Urbild direkt ablesbar.

Lemma 1.3.20. *Der $R[U^{-1}]$-Modul-Homomorphismus*

$$\sigma : R[U^{-1}] \otimes_{R[U^{-1}]} M \to M[U^{-1}] : \frac{r}{u} \otimes m \mapsto \frac{rm}{u}$$

ist ein Isomorphismus.

Beweis. Um zu zeigen, dass der natürliche Homomorphismus ein Isomorphismus ist, reicht es zu zeigen, dass es einen Umkehrhomomorphismus gibt. Betrachte hierfür die Abbildung $\beta : M[U^{-1}] \to R[U^{-1}] \otimes_{R[U^{-1}]} M$ mit $\frac{m}{u} \mapsto \frac{1}{u} \otimes m$.
Zeige nun, dass dies wohldefiniert und ein Homomorphismus ist. Bezüglich der Homomorphie gilt: $\beta(\frac{r}{v}\frac{m}{u}) = \frac{1}{vu} \otimes rm = \frac{rv}{v}(\frac{1}{vu} \otimes m) = \frac{r}{v}(\frac{1}{u} \otimes m) = \frac{r}{v}\beta(\frac{m}{u})$ und weiter: $\beta(\frac{m}{u} + \frac{m'}{u'}) = \beta(\frac{u'm + um'}{uu'}) = \frac{1}{uu'} \otimes (u'm + um') = \frac{1}{uu'} \otimes u'm + \frac{1}{uu'} \otimes um' = \frac{1}{u} \otimes m + \frac{1}{u'} \otimes m' = \beta(\frac{m}{u}) + \beta(\frac{m'}{u'})$.
Zur Wohldefiniertheit der Abbildung muss gezeigt werden: Aus (m',u') $\sim$ (m,u), also $\frac{m}{u} = \frac{m'}{u'}$ folgt $\beta(\frac{m}{u}) = \beta(\frac{m'}{u'})$. Es existiert also ein $v \in U$ mit $vu'm = vum'$. Und somit $\beta(\frac{m}{u}) = \frac{1}{u} \otimes m = \frac{vu}{vu'u} \otimes m = \frac{1}{vu'u} \otimes vu'm = \frac{1}{vu'u} \otimes vum' = \frac{vu}{vu'u} \otimes m' = \frac{1}{u'} \otimes m' = \beta(\frac{m'}{u'})$.
Damit ist β also auch wohldefiniert.
Nun gilt: $\sigma \circ \beta(\frac{m}{u}) = \sigma(\frac{1}{u} \otimes m) = \frac{m}{u}$. Sowie $\beta \circ \sigma(\frac{r}{u} \otimes m) = \beta(\frac{rm}{u}) = \frac{1}{u} \otimes rm = \frac{r}{u} \otimes m$.
Also ist β der gesuchte Umkehrhomomorphismus und die Isomorphie gezeigt. □

Definition 1.3.21. Ein R-Modul F heißt **flach** falls für jeden Monomorphismus $M' \to M$ von R-Moduln die induzierte Abbildung $F \otimes_R M' \to F \otimes_R M$ wieder ein Monomorphismus ist. In der Form von exakten Sequenzen gesprochen heißt dies: Ist $0 \to M' \to M \to M''$ eine exakte Sequenz, so ist auch $0 \to F \otimes_R M' \to F \otimes_R M \to F \otimes_R M''$ exakt. Wie oben bereits bemerkt erhält das Tensorprodukt allgemein rechtsexakte Sequenzen.

Ist der Modul zusätzlich flach, so erhält das Tensorprodukt wie gerade beschrieben auch linksexakte Sequenzen und damit alle kurzen exakten Sequenzen. Daraus folgt, dass beliebige exakte Sequenzen beim tensorieren mit flachen Moduln erhalten werden.

Proposition 1.3.22. *Für jede multiplikativ abgeschlossene Teilmenge $U \subset R$ ist der Ring $R[U^{-1}]$ als R-Modul flach, das bedeutet: Lokalisierung bildet Untermoduln auf Untermoduln ab und erhält Kerne und Kokerne.*

Beweis. Es sei eine Injektion $M' \subset M$ gegeben. Es ist zu zeigen, dass $R[U^{-1}] \otimes_R M' \to R[U^{-1}] \otimes_R M$ ist eine Injektion. Nach 1.3.20 ist dies gleichbedeutend mit: $\phi : M'[U^{-1}] \to M[U^{-1}]$ ist injektiv. Ist nun $\phi(\frac{m}{u}) = 0$, so folgt: es existiert ein $v \in U$ mit $vm = 0$ in M, also auch in $M' \subset M$. Dies impliziert $\frac{m}{u} = 0$ in $M'[U^{-1}]$. □

Folgerung 1.3.23. *Lokalisierung erhält endliche Schnitte, das heißt: Sind $M_1, ..., M_t \subset M$ Untermoduln, dann gilt: $(\bigcap_j M_j)[U^{-1}] = \bigcap_j (M_j[U^{-1}])$.*

Beweis. Die Beweisidee ist, dass Schnitte als Kerne von Homomorphismen konstruiert werden können. Der Untermodul $\bigcap_i M_i$ ist Kern der Abbildung $M \to \bigoplus_i M/M_i$. Da Lokalisierung Kerne, Quotienten und direkte Summen erhält, folgt: $(\bigcap_i M_i)[U^{-1}]$ ist Kern der Abbildung $M[U^{-1}] \to (\bigoplus_i M/M_i)[U^{-1}] = \bigoplus_i (M/M_i)[U^{-1}] = \bigoplus_i (M[U^{-1}]/M_i[U^{-1}])$. Folglich gilt $(\bigcap_i M_i)[U^{-1}] = \bigcap_i (M_i[U^{-1}])$. □

Bemerkung 1.3.24. Die Aussage über Schnitte gilt nur im endlichen Fall.

Definition 1.3.25. Der Träger der Menge M, geschrieben $Supp(M)$, ist die Menge der Primideale P, so dass $M_P \neq 0$.

Folgerung 1.3.26. *Ist M endlich erzeugter R-Modul und P Primideal in R so folgt für $P \in Supp(M)$ ist äquivalent damit, dass P den Annihilator von M enthält.*

Beweis. Angenommen $p \notin P$ ist Element des Annihilators, so ist nach Proposition 1.2.4 $M_P = 0$, da $pM = 0$ ist. Ist umgekehrt $M_P = 0$ so existiert $p \in P$ aus dem Annihilator und damit $P \notin Supp(M)$. □

Lemma 1.3.27. *Sei R ein Ring und M ein R-Modul.*

(i) *Für $m \in M$ gilt: $m = 0 \Leftrightarrow m$ ist 0 in jeder Lokalisierung M_L von M mit einem maximalen Ideal L.*

(ii) *$M = 0 \Leftrightarrow M_L = 0$ für jedes maximale Ideal L von R.*

Beweis. Zu a) m wird 0 in der Lokalisierung M_L genau dann, wenn der Annihilator I von m nicht in L ist, da mit $M_L = M[U^{-1}]$, wobei $U = R - L$ und $I \subset L$ folgt, dass kein $v \in U$ existiert mit $vm = 0$.
Weiter ist $m = 0$ genau dann, wenn dessen Annihilator $I = R$ ist, dies ist äquivalent zu: I ist nicht Teilmenge eines maximalen Ideals von R, da nach Zorns Lemma jedes Ideal außer R selbst in einem maximalen Ideal enthalten ist.
Zu b) $M = 0$ ist äquivalent dazu, dass für alle $m \in M, m = 0$ ist, nach a) ist dies bedeutungsgleich mit: alle m sind 0 in jeder Lokalisierung mit einem maximalen Ideal $L \subset R$. Und das wieder äquivalent zu $M_L = 0$ für alle maximalen Ideale L. □

Folgerung 1.3.28. *Ist $\phi : M \to N$ ein R-Modul-Homomorphismus, dann ist ϕ ein Monomorphismus (Epimorphismus, Isomorphismus) genau dann, wenn für jedes maximale Ideal $L \subset R$ die Lokalisierung $\phi_L : M_L \to N_L$ ein Monomorphismus (Epimorphismus, Isomorphismus) ist.*

Beweis. Zu Monomorphismus: ϕ ist ein Monomorphismus so ist $ker(\phi) = 0$. Betrachte die exakte Sequenz $0 \to M \xrightarrow{\phi} N$, dann ist nach 1.3.22 auch $0 \to M_L \xrightarrow{\phi_L} N_L$ exakt. Demnach ist $ker(\phi_L) = 0$ und somit ϕ_L injektiv. Sei nun umgekehrt ϕ_L injektiv für jedes maximale Ideal L. Betrachte die exakte Sequenz $0 \to ker(\phi) \to M \xrightarrow{\phi} N$, es ergibt sich wie eben die exakte Sequenz: $0 \to ker(\phi)_L \to M_L \xrightarrow{\phi_L} N_L$. Ist nun ϕ_L injektiv, so folgt, dass $ker(\phi) = 0$ ist für alle maximalen Ideale L, nach Lemma 1.3.27 b) ist also $ker(\phi) = 0$ und damit ϕ injektiv.
Zu Epimorphismus: Sei ϕ surjektiv, es folgt aus $M \xrightarrow{\phi} N \xrightarrow{\psi} 0$ exakt, dass auch $M_L \xrightarrow{\phi_L} N_L \xrightarrow{\psi_L} 0$ exakt ist, also ist $im(\phi_L) = ker(\psi_L) = N_L$. Ist umgekehrt ϕ_L) surjektiv für alle maximalen Ideale L dann sei $C = N/im(\phi)$ Kokern von ϕ. Aus M $\xrightarrow{\phi} N \to C \to 0$ ist exakt folgt $M_L \xrightarrow{\phi_L} N_L \to C_L \to 0$ ist exakt. Ist nun ϕ_L surjektiv so folgt $C_L = 0$ und nach 1.3.27 b) ist $C = 0$. Damit dann $im(\phi) = N$ und folglich ist ϕ surjektiv.
Zu Isomorphismus: Nehme die Argumente vom Monomorphismus und Epimorphismus zusammen. □

Beispiel 1.3.29. Allgemeine Form des chinesischen Restsatzes: Sei R ein Ring und $Q_1, ..., Q_n$ Ideale von R mit $Q_i + Q_j = R$ für alle $i \neq j$. Dann ist $R/(\bigcap_i Q_i)$ isomorph zu $\prod_i R/Q_i$.

Beweis. Betrachte: $\phi : R \to \prod_i R/Q_i$ mit $\phi(r) = (\pi_1(r), ..., \pi_n(r))$ mit π_i als kanonischer Projektion, $\pi_i : R \to R/Q_i$.
Behauptung: $ker(\phi) = \bigcap_i Q_i$. Sei $x \in ker(\phi) \Rightarrow \phi(x) = 0 \Rightarrow \pi_i(x) = 0 \Rightarrow x \in Q_i$ für alle $i. \Rightarrow x \in \bigcap_i Q_i)$. Also ist $ker(\phi) \subset \bigcap_i Q_i)$. Sei umgekehrt $x \in \bigcap_i Q_i) \Rightarrow \pi(x) = 0$ für alle $i \Rightarrow \phi(x) = 0 \Rightarrow x \in ker(\phi)$. Somit: $\bigcap_i Q_i) \subset ker(\phi)$. Insgesamt also $ker(\phi) = \bigcap_i Q_i)$ wie behauptet.
Sei weiter L ein maximales Ideal von R. Behauptung: Höchstens eines der Q_i ist in L enthalten. Angenommen: Q_i und $Q_j \subset L$ mit $i \neq j \Rightarrow Q_i + Q_j \subset L \Rightarrow L = R$. Ein Widerspruch, der die Behauptung zeigt.
Als nächstes wird gezeigt, dass die Abbildung $\phi_L : R[U^{-1}] \to \prod_i R/Q_i$ für alle maximalen Ideale surjektiv ist, daraus folgt nach dem Korollar 1.3.28, dass ϕ selbst surjektiv ist. Da $(\prod_i R/Q_i)[U^{-1}] \cong \prod_{-1}(R/Q_i[U^{-1}])$ betrachte $\phi_L : \frac{r}{u} \mapsto \frac{\pi_i(r)}{u}$. Sei $Q_i \subset L \Rightarrow Q_j \nsubseteq$ für $j \neq i \Rightarrow Q_j \subset U$, daher geht $\frac{r}{u}$ in jeder Faktorisierung nach Q_j mit $j \neq i$ durch Lokalisierung an U auf 0. Folglich ist: $\phi_L(\frac{r}{u}) = (0, ..., 0, \frac{\pi_i(r)}{u}, 0, ..., 0)$ und da π_i surjektiv ist, ist ϕ_L surjektiv, folglich auch ϕ. Nach dem Homomorphiesatz ist $R/ker(\phi) \cong im(\phi)$, das bedeutet aber gerade: $R/(\bigcap_i Q_i) \cong \prod_i R/Q_i$. □

Proposition 1.3.30. *a) Sei R ein Ring und S eine R-Algebra. Sind M, N R-Moduln so folgt: Es existiert ein eindeutiger S-Modulhomomorphismus $\alpha_M : S \otimes_R \mathrm{Hom}_R(M, N) \to$*

$\mathrm{Hom}_S(S\otimes_R M, S\otimes_R N)$ *der* $1\otimes\phi \in S\otimes_R \mathrm{Hom}_R(M,N)$ *auf den S-Modulhomomorphismus* $1\otimes_R \phi : S\otimes_R M \to S\otimes_R N \in \mathrm{Hom}_S(S\otimes_R M, S\otimes_R N)$ *abbildet. Ist S flach über R und M endlich präsentiert so folgt, dass* α_M *ein Isomorphismus ist.*
b) Insbesondere: Ist M endlich präsentiert so folgt, dass $\mathrm{Hom}_R(M,N)$ *lokalisiert in dem Sinne, dass* α *einen natürlichen Isomorphismus* $\mathrm{Hom}_{R[U^{-1}]}(M[U^{-1}], N[U^{-1}]) \cong \mathrm{Hom}_R(M,N)[U^{-1}]$ *für jede Teilmenge* $U \subset R$ *bedeutet.*

Beweis. Zunächst einmal soll begründet werden, dass b) ein Spezialfall von a) ist. Setze in a) hierfür $S = R[U^{-1}]$. Es gilt: $R[U^{-1}] \oplus_R M \cong M[U^{-1}]$ sowie $R[U^{-1}] \oplus_R N \cong N[U^{-1}]$ nach 1.3.20. Da $R[U^{-1}]$ flach ist folgt aus a), dass $\mathrm{Hom}_R(M,N)[U^{-1}]$ isomorph zu $\mathrm{Hom}_{R[U^{-1}]}(M[U^{-1}], N[U^{-1}])$ ist. Bleibt also a) zu zeigen. Die Abbildung $\alpha' : \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_S(S\otimes M, S\otimes N)$ mit $\phi \mapsto 1\otimes\phi$ (das ist der Homomorphismus $s\otimes m \mapsto s\otimes\phi(m)$) ist ein R-Modul-Homomorphismus, da $\alpha'(\phi+\psi) = 1\otimes(\phi+\psi) = 1\otimes\phi + 1\otimes\psi = \alpha'(\phi)+\alpha'(\psi)$ und $\alpha'(r\phi) = 1\otimes r\phi = r(1\otimes\phi) = r\alpha'(\phi)$. $\mathrm{Hom}_S(S\otimes M, S\otimes N)$ ist auch ein S-Modul $\Rightarrow \alpha'$ kann zu einem eindeutigen Homomorphismus α_M zwischen S-Moduln wie in der Proposition angegeben erweitert werden.
Sei nun S flach und M endlich präsentiert. Sei zunächst $M = R$ so folgt $\mathrm{Hom}_R(R,N) \cong N, S\otimes_R R = S$ weiter ist $\mathrm{Hom}_S(S\otimes_R R, S\otimes_R N) = \mathrm{Hom}_S(S, S\otimes_R N) \cong S\otimes_R N$ und $\alpha_R : S\otimes_R N \to S\otimes_R N$ ist die identische Abbildung. Sei nun weiter $M = \bigoplus_1^m R$. Da Hom und das Tensorprodukt direkte Summen erhalten gilt: $\alpha_{\bigoplus_1^m R} = \bigoplus_1^m \alpha_R$. Da nun aber jedes α_R ein Isomorphismus ist, ist es auch $\alpha_{\bigoplus_1^m R}$. Also ist α_M für M als freier Modul ein Isomorphismus, denn jeder freie Modul hat die Darstellung $\bigoplus_1^m R$.
Sei M schließlich ein endlich präsentierter Modul, seien F, G freie Moduln, dann gibt es Homomorphismen und eine exakte Sequenz mit $F \xrightarrow{\phi} G \xrightarrow{\psi} M \to 0$. Da das Tensorpodukt rechtsexakte Sequenzen erhält, folgt $S\otimes F \xrightarrow{\phi'} S\otimes G \xrightarrow{\psi'} S\otimes S\otimes M \to 0$ ist exakt. Weiter folgt aus den Eigenschaften von Hom, dass $0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(G,N) \to \mathrm{Hom}_R(F,N)$ und $0 \to \mathrm{Hom}_S(S\otimes M, S\otimes N) \to \mathrm{Hom}_S(S\otimes G, S\otimes N) \to \mathrm{Hom}_S(S\otimes F, S\otimes N)$ exakte Sequenzen sind. Da S über R flach ist erhält das Tensorprodukt mit S auch linksexakte Sequenzen, daher ist $0 \to S\otimes \mathrm{Hom}_R(M,N) \to S\otimes \mathrm{Hom}_R(G,N) \to S\otimes \mathrm{Hom}_R(F,N)$ auch eine exakte Sequenz. Betrachte nun das Diagramm von Abbildungen:

$$\begin{array}{ccccccc}
0 & \longrightarrow & S\otimes \mathrm{Hom}_R(M,N) & \xrightarrow{\phi^{o'}} & S\otimes \mathrm{Hom}_R(G,N) & \xrightarrow{\psi^{o'}} & S\otimes \mathrm{Hom}_R(F,N) \\
 & & \downarrow{\scriptstyle \alpha_M} & & \downarrow{\scriptstyle \alpha_G} & & \downarrow{\scriptstyle \alpha_F} \\
0 & \longrightarrow & \mathrm{Hom}_S(S\otimes M, S\otimes N) & \xrightarrow{\phi'^{o}} & \mathrm{Hom}_S(S\otimes G, S\otimes N) & \xrightarrow{\psi'^{o}} & \mathrm{Hom}_S(S\otimes F, S\otimes N)
\end{array}$$

wobei α_G und α_F nach den Überlegungen über freie Moduln oben Isomorphismen sind und die Zeilen nach Argumentation oben exakt sind. Weiter kommutiert das Diagramm, wie sich beispielsweise für den ersten Teil elementar nachrechnen läßt: $\alpha_G \circ \phi^{o'}(s\otimes\sigma) = \alpha_G((s\otimes\sigma\circ\phi)) = s\otimes_R \sigma\circ\phi = \phi'^{o}(s\otimes_R \phi) = \phi'^{o}\circ\alpha_M(s\otimes\sigma)$.
Zeige nun, dass α_M ein Isomorphismus ist. Zunächst Injektivität: Sei $x \in ker(\alpha_M) \Rightarrow \alpha_G\circ\phi^{o'}(x) = \phi'^{o}\circ\alpha_M(x) = 0$. Da α_G ein Isomorphismus ist, muss $\phi^{o'}(x) = 0$ sein. $\phi^{o'}$ ist

aber nach der exakten Sequenz injektiv $\Rightarrow x = 0 \Rightarrow \alpha_M$ ist injektiv. Für die Surjektivität gilt: Sei $y \in \mathrm{Hom}_S(S \otimes M, S \otimes N)$. Da α_G ein Isomorphismus ist, existiert ein z mit $\alpha_G(z) = \phi'^o(y)$. Gelingt es nun ein Urbild von z zu finden, so ist die Surjektivität gezeigt. Da nach der exakten Sequenz $ker(\psi^{o'}) = im(\phi o')$ ist, existiert ein a mit $\phi^{o'}(a) = z$. Das ist äquivalent zu $\psi^{o'}(z) = 0$, also $z \in ker(\psi^{o'})$. Da das Diagramm kommutiert folgt: $\alpha_F \circ \psi^{o'}(z) = \psi'^o \circ \alpha_G(z) = \psi'^o \circ \phi'^o(y) = 0$, wobei die letzte Gleichheit aus der exakten Sequenz folgt, $\phi'^o(y)$ ist im Bild von ϕ'^o und folglich im Kern von ψ'^o. Da α_F ein Isomorphismus ist, folgt $\psi^{o'}(z) = 0 \Rightarrow$ da z im Kern von $\psi^{o'}$ ist liegt es im Bild von $\phi^{o'}$, es existiert also ein a mit $z = \phi^{o'}(a)$. Weiter ist $\phi'^o \circ \alpha_M(a) = \alpha_G \circ \phi^{o'}(a) = \alpha_G(z) = \phi'^o(y)$. Da ϕ'^o injektiv ist $\Rightarrow \alpha_M(a) = y$. Damit ist die Isomorphie gezeigt. □

2 Lokalisierung Teil 2

Catherina Köhl

2.1 Konstruktion von Primelementen

Das Komplement eines Primideals ist multiplikativ abgeschlossen, denn sind f, g nicht im Ideal, so auch fg nicht — Anderes wäre ein Widerspruch zur Primeigenschaft des Ideals. Dazu gibt es eine Art Umkehrung:

Proposition 2.1.1. *Sei R ein kommutativer Ring, $U \subset R$ eine multiplikativ abgeschlossene Teilmenge, und $I \subset R$ ein Ideal, das maximal ist unter denen, die U leer schneiden. Dann ist I Primideal.*

Beweis. Angenommen, f sowie g seien nicht in I. Wir betrachten die Mengen $I + (f)$ und $I + (g)$. Wegen der Maximalitätseigenschaft von I schneidet jedes Ideal von R, das I als echte Teilmenge enthält, die Menge U nichtleer – so ist also also auch der Schnitt von $I+(f)$ bzw. $I+(g)$ mit U nichtleer. Daher gibt es in U Elemente der Form $af+i$ und $bg+j$ mit $i, j \in I$. Wäre fg nun in I, so wäre ebenfalls $(af+i)(bg+j) = abfg+ibg+jaf+ij$ in I – da $i, j \in I$. Ausserdem gilt $(af+i)(bg+j) \in U$, da U multiplikativ abgeschlossen ist, was aber ein Widerspruch zur Voraussetzung $I \cap U = \emptyset$ ist. Daher gilt $fg \notin I$. Da f, g in $R \backslash I$ beliebig gewählt waren, haben wir die Gültigkeit der Implikation

$$f, g \notin I \Longrightarrow fg \notin I,$$

bewiesen, und also ist I Primideal. □

Überhaupt – und netterweise – haben Ideale, die bezogen auf eine bestimmte Eigenschaft maximal sind, im Allgemeinen die Tendenz dazu, prim zu sein, wofür wir einen Grund gerade sahen.

Eine Variante obigen Beweises zeigt uns den Zusammenhang zur Lokalisierung:

Nach Lokalisierung 1 - Proposition 1.2.9 ist die „Umkehrung“ $I \mapsto \phi^{-1}(I)$ der natürlichen Abbildung eine Injektion von Idealen aus $R[U^{-1}]$ in solche aus R, die Inklusionen und Schnitte erhält und außerdem Primideale auf Primideale abbildet. Nun ist I maximal unter den Idealen in R, die U nicht schneiden. Wäre $IR[U^{-1}]$ nicht maximal – Hier ist jetzt von tatsächlicher Maximalität von einem Ideal die Rede! – in $R[U^{-1}]$, so gäbe es

$$IR[U^{-1}] \subset H \subset R[U^{-1}].$$

Da ϕ^{-1} Inklusionen erhält und $IR[U^{-1}] = \phi^{-1}(IR[U^{-1}])R[U^{-1}]$, wäre demnach auch

$$I \subseteq P := \phi^{-1}(IR[U^{-1}]) \subset \phi^{-1}(H) \subset R.$$

Solch ein echtes Ideal $\phi^{-1}(H) \subset R$ kann es aber nicht geben:

Wegen der Maximalitätseigenschaft von I muss es ein $u \in \phi^{-1}(H) \cap U$ geben, da jedes Ideal, das I echt enthält, U schneidet. Alle $v \in U$ sind in $R[U^{-1}]$ aber invertierbar, so dass u und $u^{-1} \in \phi^{-1}(H)R[U^{-1}] = H$ (Prop. 1.2.9), also $uu^{-1} = 1 \in H$. Damit ist aber $H = R[U^{-1}]$, also sind die Inklusionen in der Annahme nicht mehr echt, ein Widerspruch.

$IR[U^{-1}]$ ist also ein maximales Ideal in $R[U^{-1}]$, und maximale Ideale sind Prim.

⌈ Denn: Ist $J \subset R$ ein maximales Ideal und wäre $fg \in J$, aber $f, g \notin J$, so wäre das von J und f erzeugte Ideal gleich R, da J maximal ist. Die Elemente in R lassen sich also als $j + rf$ darstellen, mit $j \in J, r \in R$, so also auch die 1, die ja in R enthalten ist. Es ist also $1 = j + rf$, also $g = jg + rfg$. Damit muss $g \in J$ sein, da $jg \in J$ und $rfg \in J$. Das steht aber im Widerspruch zu der Annahme $f, g \notin J$, also ist jedes maximale Ideal prim. ⌋

Nach Lokalisierung I - Proposition 1.2.9 ist also – wegen $IR[U^{-1}]$ prim – auch P prim. Nun ist $I \subseteq P$ und P kann U nicht schneiden, weil – genauso wie oben mit H – dann $1 \in IR[U^{-1}] = PR[U^{-1}]$ und somit $IR[U^{-1}] = R[U^{-1}]$ wäre. Also ist $I = P$ und somit I prim.

Bemerkung 2.1.2. Bemerkenswert ist hierbei, dass man für beliebiges U durch Zorns Lemma (Auswahlaxiom) immer ein I wie in der Proposition finden kann:
Nehmen wir uns ein Ideal I_0, das U leer schneidet und basteln daraus beliebige Ketten $I_0 \subset I_1 \subset ...$ von Idealen, die alle U nicht schneiden. Jede dieser Ketten besitzt ein maximales Element – nämlich $\bigcup_{j=0}^{\infty} I_j$. Also gibt es nach Zorn insgesamt ein maximales Element M, das dieselben Voraussetzungen erfüllt wie unser I.

2.2 Ringe und Moduln endlicher Länge

In diesem Kapitel beschäftigen wir uns mit Ringen und Moduln endlicher Länge, ihren Strukturen, der Anzahl ihrer maximalen Ideale und deren Zusammenhängen mit den Eigenschaften noethersch und artinsch.

Einige benötigte Definitionen vorab:

Definition 2.2.1. Sei M ein Modul. Eine **Kette** von Untermoduln von M ist eine Sequenz von Untermodulen mit strikten Inklusionen:

$$M = M_0 \supset M_1 \supset \cdots \supset M_n.$$

Die Zahl n nennt man dabei die **Länge** dieser Kette.

Eine Kette heißt **Kompositionsreihe**, wenn jedes M_j/M_{j+1} ein einfacher Modul ungleich null ist, d.h. er hat keine echten Untermoduln ungleich null. Demnach ist eine Kompositionsreihe eine maximale Kette von Untermoduln von M.

Als **Länge von** M definieren wir die kleinste Länge, die eine endliche Kompositionsreihe von M annimmt, bzw. ∞, wenn M keine endliche Kompositionsreihe hat.

Bemerkung 2.2.2. Wir werden später zeigen, dass je zwei Kompositionsreihen eines Moduls M die gleiche Länge haben.

Definition 2.2.3. Ein Modul M heißt **artinsch**, wenn jede absteigende Folge von Untermoduln stationär wird, d.h. für jede absteigende Folge

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq ...$$

gibt es ein $n \in \mathbb{N}$, so dass

$$M_n = M_{n+1} = M_{n+2} = \cdots$$

M heißt **noethersch**, wenn jede aufsteigende Kette von Untermoduln stationär wird, d.h. es gibt ein $n \in \mathbb{N}$, so dass

$$M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M_{n+1} = \cdots$$

Bemerkung 2.2.4. Später in Satz 2.2.7 werden wir sehen, dass für Ringe noethersch aus artinsch folgt.

Der nächste Satz sagt etwas über die Struktur von Moduln endlicher Länge. Er beinhaltet den Satz von Jordan-Hölder für Moduln und den Chinesischen Restsatz.

Satz 2.2.5. *Sei R ein kommutativer Ring und M ein R-Modul. Der Modul M hat genau dann eine endliche Kompositionsreihe, wenn er artinsch und noethersch ist.*

Besitzt M eine endliche Kompositionsreihe $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ der Länge n, so gilt:

(a) Jede Kette von Untermoduln von M hat Länge höchstens n und kann zu einer Kompositionsreihe erweitert werden.

(b) Die Summe der Lokalisierungsabbildungen $M \to M_P$ für Primideale P liefert uns einen Isomorphismus von R-Moduln

$$M \cong \bigoplus_P M_P,$$

wobei die Summe über alle maximalen Ideale P dergestalt, dass $M_i/M_{i+1} \cong R/P$ für ein i, gebildet wird. Die Anzahl der M_i/M_{i+1}, die isomorph zu R/P sind, ist genau die Länge von M_P als Modul über R_P, und also unabhängig von der gewählten Kompositionsreihe.

(c) Es gilt $M = M_P$ genau dann, wenn M von einer Potenz von P annihiliert wird.

Beweis. Angenommen, M ist artinsch und noethersch, es erfüllt also sowohl eine absteigende, als auch eine aufsteigende Kettenbedingung. Durch die aufsteigende Kettenbedingung (noethersch) können wir einen maximalen echten Untermodul $M_1 \subset M$ wählen, davon wiederum einen maximalen echten Untermodul $M_2 \subset M_1$ usw. Diese Kette von maximalen Untermoduln muss nach der absteigenden Kettenbedingung (artinsch) stationär werden, und zwar bei $M_n = 0$ (da 0 ein echter Untermodul eines jeden Moduls ist). Damit ist $M = M_0 \subset M_1 \subset ... \subset M_n = 0$ eine Kompositionsreihe und M hat also endliche Länge n. (Die Umkehrung werden wir als Folgerung aus (a) sehen.)

(a) Sei $M' \subset M$ ein echter Untermodul; wir werden zeigen, dass die Länge von M' kleiner als die Länge von M ist.

Dazu schneiden wir die Elemente der Kompositionsreihe von M mit M' und erhalten dadurch eine kürzere Kompositionsreihe von M':

$$(M' \cap M_i)/(M' \cap M_{i+1}) \cong (M' \cap M_i + M_{i+1})/(M' \cap M_{i+1}) \subseteq M_i/M_{i+1}.$$

Da M_i/M_{i+1} einfach ist, gilt entweder $(M' \cap M_i)/(M' \cap M_{i+1}) = 0$, oder $(M' \cap M_i)/(M' \cap M_{i+1})$ ist einfach und $(M' \cap M_i) + M_{i+1} = M_i$.

Wir beweisen nun, dass letzteres nicht für alle i sein kann, wodurch gezeigt wäre, dass M' kürzere Länge hat als M. Wären sämtliche $(M' \cap M_i)/(M' \cap M_{i+1}) \neq 0$, so wäre auch $M_i \subseteq M'$ für alle i. Damit gälte $M = M_0 \subseteq M'$, im Widerspruch zur Annahme. Also ist $(M' \cap M_i)/(M' \cap M_{i+1})$ nicht für alle i einfach – und vermutlich für sehr viel weniger als n, da $(M' \cap M_i)/(M' \cap M_{i+1}) = 0$ für alle $M' \subseteq M_i \subseteq M$.

Daraus folgt nun, dass wir die Sequenz $M' \subseteq M' \cap M_1 \subseteq ... \subseteq M' \cap M_n = 0$ verkürzen können, indem wir die $M' \cap M_i$ mit $M' \cap M_i = M' \cap M_{i+1}$ auslassen. Die so erhaltene Kette ist eine Kompositionsreihe von M', denn – s.o. – die Quotienten ihrer aufeinander folgenden Glieder sind einfach, aber ungleich null. Und sie hat Länge kleiner n.
Da dieses Verfahren auf sämtliche Kompositionsreihen von M anwendbar ist, also auch auf seine kürzeste, gibt es mindestens eine Kompositionsreihe von M', die kürzer ist als die Länge (gleich die Länge der kürzesten Kompositionsreihe) von M. Also ist nach Definition die Länge von M' kleiner als die Länge von M.

Wir nehmen nun an, dass $M = N_0 \subset N_1 \subset ... \subset N_k$ eine Kette von Untermoduln ist. Wie wir gerade gezeigt haben ist Länge $N_1 <$ Länge M. Die Länge der Kette $N_1 \subset ... \subset N_k$ ist $k - 1 \leq$ Länge N_1. Da Länge $N_1 <$ Länge M folgt also, dass $k \leq$ Länge M.
Die Länge jeder Kette von Untermoduln von M ist also kürzer als die Länge von M.

Da die Länge n von M definiert ist als die Länge der kürzesten maximalen Kette in M ist die Länge jeder maximalen Kette in $M \geq n$. Wie wir gerade gezeigt haben ist die Länge jeder Kette in M kleiner gleich n. Also hat jede maximale Kette in M Länge n.

Indem wir eine Kette in M solange erweitern um Zwischenmodule zwischen alle Elemente M_i, M_{i+1}, deren Quotient nicht einfach ist, bis alle diese Quotienten einfach

sind, können wir aus jeder Kette eine Kompositionsreihe herstellen. Und also ist n eine einheitliche Grenze für die Länge aller aufsteigenden, wie auch absteigenden Ketten, so dass M also artinsch und noethersch ist.

(b) Wir erinnern uns, dass für ein Primideal P definiert wurde $R_P := R[U^{-1}]$, wobei $U = R - P$.

Da $\bigoplus_P M_P$ ein R-Modul ist, genügt es nach 1.3.28 zu zeigen, dass die im Satz gegebene Abbildung für die Lokalisierung an jedem maximalen R-Ideal einen solchen Isomorphismus liefert.

Wir beginnen mit dem Fall, dass M Länge 1 hat, wenn M also ein einfacher Modul ist. Dadurch ist also $M = R/P$ für ein maximales Ideal $P = annM$.

Entweder gilt nun $P = Q$ oder $P \neq Q$. Falls $P = Q$, dann ist $R/P = R/Q$ ein Körper, da P maximales Ideal ist. Die Lokalisierung an Q ist die Adjunktion der Inversen aller Elemente, die nicht in Q sind, also ist

$$(R/Q)_Q = (R/Q)[((R/Q) - Q)^{-1}] = R/Q,$$

da eben R/Q bereits ein Körper ist und also alle Elemente außer der 0 – d.h. die Nebenklasse $Q = 0 + Q$ – bereits invertierbar sind. Falls $P \neq Q$, so $P \nsubseteq Q$, da P maximal. Wir betrachten R und Q als R-Moduln, also ist $P_Q = P[(R - Q)^{-1}]$ und $R_Q = R[(R - Q)^{-1}]$. Da, wie bereits gesagt, $P \nsubseteq Q$ gibt es $p \in R - Q$ und $p \in P$, also $1 = p \cdot p^{-1} \in P_Q$. Also ist $R \subseteq P_Q$, und da die adjungierten Inversen sowieso gleich sind, gilt $P_Q = R_Q$.
Also ist $(R/P)_Q = R_Q/P_Q = 0$.

Hieraus folgt insbesondere, dass für zwei verschiedene Primideale Q und Q' gilt $(M_Q)_{Q'} = 0$.

Kehren wir nun zurück zum allgemeinen Fall, dass M Länge $n < \infty$ hat. Die Kompositionsreihen von M lokalisiert ergeben eine Sequenz von Untermodulen

$$M_Q = (M_0)Q \supseteq (M_1)Q \supseteq ... \supseteq (M_n)Q = 0.$$

Die – unlokalisierten – Moduln M_i/M_{i+1} haben Länge 1. Damit zeigt unser oben gezeigter Fall von Länge $M = 1$, dass $(M_i/M_{i+1})_Q = M_i/M_{i+1}$, falls $Q = annM_i/M_{i+1}$, und $(M_i/M_{i+1})_Q = 0$ sonst. Also hat M_Q eine endliche Kompositionsreihe, die einer Unterreihe einer Kompositionsreihe von M entspricht. (Wir lokalisieren die Kompositionsreihe von M an Q und kürzen sie um gleiche Elemente $(M_i)_Q = (M_{i+1})_Q$. Entsprechend kann man auch sagen man behält diejenigen Elemente $(M_i)_Q$ für die gilt $M_i/M_{i+1} \cong R/Q$.)
Insbesondere ist $M_Q = 0$, wenn keines der M_i/M_{i+1} isomorph zu R/Q ist.

Sei nun $\alpha : M \to \oplus M_P$ die Summe über alle Lokalisierungsabbildungen mit P Primideal. Das ist das Gleiche wie diese Summe über alle P, für die für irgendwelche $M_i/M_{i+1} \cong R/Q$ gilt – die restlichen M_P sind ohnehin 0.

Für sämtliche maximale Ideale Q und Moduln M gilt $(M_Q)_Q = M_Q$, also ist die Identität ein Teil der Lokalisierung von α:

$$\alpha_Q : M_Q \to \left(\bigoplus_{P \text{ maximales Ideal}} M_P \right)_Q = \bigoplus_{P \text{ maximales Ideal}} ((M_P)_Q)$$

Ist aber $P \neq Q$ und hat M endliche Länge, dann haben wir bereits gesehen, dass $(M_P)_Q = 0$. Also ist α_Q die Identitätsabbildung für jedes maximale Ideal Q, und also ist α ein Isomorphismus.

(c) Angenommen, M wird von einer Potenz eines maximalen Ideals P annihiliert.

Sei $Q \neq P$ ein anderes maximales Ideal, dann existiert ein Element $p \in P \backslash Q$. Dieses p verhält sich wie eine Einheit auf M_Q. Da eine Potenz von p sich auf M wie die 0 verhält, muss $M_Q = 0$ sein, da andernfalls kein Element gleichzeitig Einheit und 0 sein kann.

Also ist nach (b) $M \cong M_P$.

Umgekehrt, angenommen $M \cong M_P$. Die in (b) vorgestellte Darstellung von Lokalisierung zeigt, dass für alle i gilt $M_i/M_{i+1} \cong R/P$.

Nun ist entweder $PM \subseteq M_1$ oder $PM + M_1 = M$, da M/M_1 nach Voraussetzung einfach ist – denn träfen beide Bedingungen nicht zu, so wäre $PM + M_1 \subset M$ und es gäbe also ein echtes Untermodul von $M/M_1 = (PM + M_1)/M_1$, was ein Widerspruch zur Einfachheit wäre.

Angenommen, es gilt der zweite Fall, $PM + M_1 = M$. Dann ist

$$R/P = M/M_1 = (PM + M_1)/M_1 = PM/(PM \cap M_1).$$

Da, wenn man R/P mit P multipliziert, 0 das Ergebnis ist (P annihiliert R/P), muss dies auch für $PM/(PM \cap M_1)$ wahr sein, also $P^2M \subseteq M_1$. Somit ist in beiden Fällen $P^2M \subseteq M_1$.

Indem man nun per Induktion das Untermodul M_2 von M_1 betrachtet usw. und die gleiche Argumentation verwendet, erhält man jeweils, dass $P^kM \subseteq M_d$ für ein k mit $d \leq k \leq 2d$.

Es gilt also insbesondere $P^kM \subseteq M_n = 0$ für ein k mit $n \leq k \leq 2n$, also $P^kM = 0$.

□

Wir kehren nun zu artinschen Ringen zurück. Die Tatsache, dass artinsche Ringe noethersch sind, was wir als Ergebnis des nächsten Satzes sehen werden, stimmt sogar für nicht kommutative Ringe (mit der Eins). Dieser allgemeinere Fall ist jedoch wesentlich schwieriger und wer sich damit befassen möchte, wende sich vertrauensvoll der Lektüre von Hopkins [6] zu.

Definition 2.2.6. Die **Länge** eines Moduls M ist das Supremum der Längen n der Ketten von Untermoduln von M:

$$0 = N_0 \subset N_1 \subset ... \subset N_n = M$$

Satz 2.2.7. *Sei R ein Ring, dann sind äquivalent:*

(a) R ist noethersch und alle Primideale in R sind maximal.

(b) R hat endliche Länge als R-Modul.

(c) R ist artinsch.

Beweis. Wenn diese Bedingungen erfüllt sind, hat R nur endlich viele maximale Ideale.

a ⇒ b: Angenommen, R ist noethersch und hat nicht endliche Länge. Sei $I \subset R$ ein maximales Ideal dergestalt, dass R/I nicht endliche Länge hat. Wir finden ein solches I, da R eben noethersch ist, also I endliche Länge hat.
Wir behaupten, dass I prim ist.

Ist in der Tat $ab \in I$, und $a \notin I$, dann können wir eine exakte Sequenz – d.h. $bild(f_i) = kern(f_{i+1})$ – formen, wobei $(I : a)$ definiert ist als das Ideal, das von I und allen b mit $ab \in I$ erzeugt wird:

$$0 \to R/(I : a) \xrightarrow{a} R/I \to R/(I + (a)) \to 0.$$

Da $I \subsetneq I + (a)$, hat der Modul $R/(I + (a))$ endliche Länge. Wenn $b \notin I$, dann enthält $(I : a)I$ ebenfalls, so dass $R/(I + (a))$ auch endliche Länge hat.
Fügen wir Kompositionsreihen von $R/(I+(a))$ und $R/(I : a)$ zusammen, so erhalten wir eine Kompositionsreihe von R/I. Diese hat dann aber ebenfalls endliche Länge, im Widerspruch zu unserer Annahme. Es muss also $b \in I$ gelten, also ist I Prim.

Nehmen wir nun an, dass alle Primideale in R maximal sind. Wenn R nicht endliche Länge hätte, dann wäre das oben konstruierte Primideal I ein maximales Ideal und R/I wäre ein Körper, was im Widerspruch zu einer Konstruktionsannahme steht, da Körper einfach sind und also endliche Länge haben (als Modul).
Also hat R endliche Länge.

b ⇒ c: Diesen Beweis haben wir gerade implizit in Satz 1.2.6 hinter uns.

c ⇒ a: Angenommen R sei artinsch. Unser Hauptziel ist es zu zeigen, dass 0 ein Produkt von maximalen Idealen von R ist. Da R artinsch ist, also die absteigende Kettenbedingung erfüllt, können wir unter all den Idealen, die Produkte von maximalen Idealen von R sind, dasjenige finden, das am Kleinsten ist. Wir nennen es J und möchten also zeigen, dass $J = 0$.

Für jedes maximale Ideal M von R impliziert die Minimalität von J, dass $MJ = J$ – da das Produkt zweier Ideale wieder ein Ideal ist, das in beiden enthalten ist; J

darf aber wegen seiner Minimalität nicht mehr kleiner werden, sonst wäre es eben nicht minimal. Also ist insbesondere $J \subset M$.
Da J^2 ebenfalls ein Produkt maximaler Ideale ist, folgt $J^2 = J$. Ist $J \neq 0$, so können wir ein Ideal I auswählen, das minimal ist unter denen, die J nicht annihilieren. Da $(IJ)J = IJ^2 = IJ \neq 0$, und $IJ \subset I$, muss $IJ = I$ gelten.
Da I das Ideal J nicht annihiliert muss es ein Element $f \in I$ geben für das gilt $fJ \neq 0$. Und da I minimal ist muss ebenso gelten $I = (f)$. Da $IJ = I$, existiert ein Element $g \in J$ für das gilt $f = fg$, oder äquivalent $(1-g)f = 0$. Da g in jedem maximalen Ideal vorhanden ist, ist $1-g$ in keinem, also ist $1-g$ eine Einheit. Also ist $f = 0$.
Also ist in der Tat $J = 0$.

Wir haben also nun $0 = M_1M_2...M_t$ für maximale Ideale M_i von R. Für jedes s ist der Quotient $M_1M_2...M_s/M_1M_2...M_{s+1}$ ein Vektorraum über R/M_{s+1}.
Jeder Untervektorraum ist ein Untermodul, entsprechend einem Ideal von R, das $M_1M_2...M_{s+1}$ enthält. Dementsprechend korrespondiert jede absteigende Kette von Untervektorräumen mit einer absteigenden Kette von Idealen von R. Und da R artinsch ist, ist jede solcher Ketten endlich. Also ist auch $M_1M_2...M_{s+1}$ endlichdimensional über R/M_{s+1} und insbesondere eine endliche Kompositionsreihe.
Also hat jede Kompositionsreihe von R endliche Länge, und R selbst ist von endlicher Länge.
Nach Theorem 1.2.6 ist R noethersch.

Angenommen, P ist ein Primideal von R. Da $P \supset 0 = M_1M_»...M_t$, ist $P \supset M_i$ für ein i. Da M_i ein maximales Ideal ist, folgt $P = M_i$, und P ist also maximal.
Insbesondere ist jedes maximale Ideal eines von den M_i, so dass es davon nur endlich viele gibt.

□

Nun besehen wir uns unsere bisherigen Ergebnisse im geometrischen Kontext:

Folgerung 2.2.8. *Sei X eine affine algebraische Menge über einem Körper k. Die folgenden Aussagen sind äquivalent:*

(a) X ist endlich.

(b) $A(X)$ ist ein endlichdimensionaler Vektorraum über k, dessen Dimension der Anzahl Punkte in X entspricht.

(c) $A(X)$ ist artinsch.

Beweis. **a** ⇒ **b:** $A(X)$ ist der Polynomring von Funktionen über der Menge X.
Wenn X endlich ist, so ist $A(X) = \prod_{x \in X} A(x) = \prod_{x \in X} k$ ein direktes Produkt von so vielen Kopien des zugrundeliegenden Körpers, wie es Punkte in X gibt.

b ⇒ **c:** Wenn R eine k-Algebra ist, die als k-Vektorraum endlichdimensional ist, so ist jede absteigende Kette von Untervektorräumen von R endlich. Und also ist jede absteigende Kette von Idealen von R endlich.

c ⇒ a: Wenn der Ring $A(X)$ artinsch ist, so gilt nach Satz 1.2.8, dass er nur endlich viele maximale Ideale hat. Da die Punkte in X den maximalen Idealen entsprechen, ist X endlich.

□

Durch die Kombination von Satz 1.2.8 und Satz 1.2.6b erhalten wir eine Aussage über die Struktur von artinschen Ringen:

Folgerung 2.2.9. *Jeder artinsche Ring ist ein endliches direktes Produkt von lokalen artinschen Ringen*

Beweis. Da R als Modul über sich selbst endliche Länge hat folgt aus Satz 1.2.6, dass die Summe der endlich vielen Lokalisierungsabbildungen $R \to \oplus_i R_{M_i}$ ein Isomorphismus von R-Moduln ist. Die R-Algebra $\prod_i R_{M_i}$, das direkte Produkt der Lokalisierungen, ist genau $\oplus_i R_{M_i}$, wenn man sie als R-Modul betrachtet – da direkte Summe und Produkt hier im endlichen Fall gleich sind.
Da jede Abbildung $R \to R_{M_i}$ eine Abbildung von Ringen ist, ist der R-Modul-Isomorphismus $R \to \oplus_i R_{M_i}$ auch noch ein Isomorphismus von Ringen. Und also ist R das direkte Produkt von endlich vielen artinschen Ringen. □

In ganz ähnlicher Weise können wir Moduln von endlicher Länge über noetherschen Ringen charakterisieren:

Folgerung 2.2.10. *Sei R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann sind äquivalent:*

(a) M hat endliche Länge.

(b) Ein endliches Produkt von maximalen Idealen $\prod_{i=1}^{n} P_i$ annihiliert M.

(c) Alle Primideale, die den Annihilator von M beinhalten, sind maximal.

(d) $R/annM$ ist ein artinscher Ring.

Beweis. **a ⇒ b:** Wenn M endliche Länge hat, so ist M nach Satz 1.2.6b und c eine direkte Summe von Moduln, und jeder dieser Moduln wird von einer Potenz eines gewissen Primideals annihiliert. Das Produkt dieser Primideale und ihrer Potenzen annihiliert also M, und da R noethersch ist, sind dies maximale Ideale.

b ⇒ c: Angenommen, ein Produkt maximaler Ideale $\prod_{i=1}^{n} P_i$ annihiliert M und ein Primideal P enthält den Annihilator von M: $P \supseteq \prod_{i=1}^{n} P_i$. Da P Prim ist muss also gelten $P = P_i$ für ein i, und also ist P maximal.

c ⇒ d: Dies folgt direkt aus Satz 1.2.8.

d ⇒ a: Sei $S = R/annM$, und angenommen S ist artinsch. Nach Satz 1.2.8 hat S endliche Länge als S-Modul und R-Modul. Weil M endlich erzeugter S-Modul ist – da endlich erzeugter R-Modul – ist es ein homomorphes Bild von einer endlichen direkten Summe von Kopien von S. Also ist M ein Modul von endlicher Länge.

□

Aus Folgerung 1.2.11 schließen wir, dass man jeder endlich erzeugte Modul in ein Modul endlicher Länge verwandeln können – durch Lokalisation an einem Primideal, das minimal über dem Annihilator ist:

Folgerung 2.2.11. *Sei R ein noetherscher Ring, $M \neq 0$ ein endlich erzeugter R-Modul, I der Annihilator von M und P ein Primideal, das I enthält.*
Der R_P-Modul M_P ist ein Modul ungleich null von endlicher Länge genau dann, wenn P minimal ist unter den Primidealen, die I enthalten.

Beweis. Wenn P ein Primideal ist, das minimal ist unter denen, die I enthalten, so ist P_P nilpotent in R_P/I_P. Also annihiliert eine Potenz von $P_P M_P$, und Folgerung 1.2.11 zeigt uns, dass M_P endliche Länge hat.
Umgekehrt, angenommen, M_P hat endliche Länge über R_P. Der Annihilator von M_P ist I_P. Also folgt, erneut nach Folgerung 1.2.11, dass jedes Primideal von R_P/I_P maximal ist. Die Primideale von R_P/I_P entsprechen den Primidealen von R, die I enthalten und in P enthalten sind. Also ist P minimal unter denen, die I enthalten. □

Ein sehr nützlicher Spezialfall dieser Ergebnisse ist, wenn $M = R/I$, so dass also $I = annM$.

Folgerung 2.2.12. *Sei I ein Ideal eines noetherschen Ringes R. Die folgenden Bedingungen sind äquivalent für ein Primideal P, das I enthält:*

(a) P ist minimal unter den Primidealen, die I enthalten.

(b) R_P/I_P ist artinsch.

(c) In der Lokalisierung R_P gilt $P_P^n \subset I_P$ für hinreichend großes n.

Beweis. **a ⇒ b:** Wenn P minimal ist unter den Primidealen, die I enthalten, so ist P_P das einzige Primideal von R_P/I_P. Nach Folgerung 1.2.11 ist R_P/I_P artinsch.

b ⇒ c: Angenommen, R_P/I_P ist artinsch. Nach Satz 1.2.8 hat R_P/I_P endliche Länge, und nach Satz 1.2.6c wird es von einer Potenz von P_P annihiliert. Also gilt $P_P^n \subset I_P$ für hinreichend große n.

c ⇒ a: Angenommen, $P_P^n \subset I_P$. Wenn Q ein Primideal von R ist, so dass $I \subset Q \subset P$, so gilt nach Lokalisierung, dass $P_P^n \subset Q_P$ – da $P_P^n \subset I_P$ nach Voraussetzung. Also gilt $P_P = Q_P$, und $P = Q$. Also ist P minimal unter den Primidealen, die I enthalten. □

2.3 Produkte von Integritätsringen

In einer anderen Richtung können wir Lokalisierung verwenden, um noethersche Ringe zu charakterisieren, die direkte Produkte von Integritätsringen sind.

Proposition 2.3.1. *Sei R ein noetherscher Ring. Dann ist R endliches direktes Produkt von Integritätsringen genau dann, wenn für jedes maximale Ideal P von R der lokale Ring R_P ein Integritätsring ist.*

Beweis. Angenommen, $R = \prod_i R_i$ ist ein direktes Produkt von Integritätsringen R_i. Ein Primideal P von R kann nicht jedes der Einselemente e_i von R_i enthalten, da es sonst bereits ganz R wäre. Wenn aber $e_i \notin P$, so ist $R_P = (R_i)_P$ ein Integritätsbereich, da e_i jedes R_j annihiliert, für das $j \neq i$ gilt.

Umgekehrt, angenommen, dass jede Lokalisierung von R an einem maximalen Ideal ein Integritätsring ist.
Sei $\{Q_i\}$ die Menge von minimalen Primidealen von R. Da der Schnitt von Primidealen in einer absteigenden Sequenz erneut ein Primideal ist, ist diese Menge nicht leer. Es gibt allerdings – der Beweis wird in Kapitel 3 geführt – nur endlich viele Q_i.
Wir müssen nun noch zeigen, dass die Abbildung $\phi : R \to \prod_i R/Q_i$ ein Isomorphismus ist.
Nach Lokalisierung I - Folgerung 1.3.28 reicht es aus zu zeigen, dass ϕ ein Isomorphismus wird, nachdem man an einem maximalen Ideal P von R lokalisiert hat. Die minimalen Primideal von R_P sind die Lokalisierungen der minimalen Primideale von R, die in P enthalten sind. Da nach Voraussetzung R_P ein Integritätsring ist, gibt es nur ein Q_i, das diese Bedingung erfüllt – nämlich das, das lokalisiert das Nullideal ergibt. Da zusätzlich R_P ein Integritätsbereich ist, kann es auch keine Elemente $\neq 0$ darin geben (in der lokalisierten Version). Nennen wir es Q_1. Damit haben wir $(Q_1)_P = 0, (Q_i)_P = R$ für $i \neq 1$. Es folgt, dass $(\prod_i R/Q_i)_P = (R/Q_1)_P = R_P$ und ϕ wird lokalisiert zu einem Isomorphismus wie verlangt. □

Bemerkung 2.3.2. In der Tat verwendet man bei dem Beweis, dass ein gegebener Ring ein Integritätsring ist, häufig – mit Mitteln der lokalen Algebra – dass der Ring lokal ein Integritätsring ist, wie in unserem gerade geführten Beweis. Benutzt man Proposition 1.3.1, so reicht es aus die Möglichkeit auszuschließen, dass der Ring andere idempotente Elemente außer 0 und 1 enthält.

3 Assoziierte Primideale und Primärzerlegung

Bettina Birkmeier

3.0 Definitionserinnerungen

Definition 3.0.1. Sei R ein Ring. Dann ist ein R**-Modul** M eine abelsche Gruppe mit einer Abbildung $R \times M \mapsto M$, geschrieben $(r, m) \mapsto rm$, mit den folgenden Eigenschaften für alle $r, s \in R$ und $m, n \in M$:

$$r(sm) = (rs)m \text{ (Assoziativität)}$$
$$r(m+n) = rm + rn$$
$$(r+s)m = rm + sm \text{ (Distributivität)}$$
$$1m = m \text{ (Identität).}$$

Die Ideale I des Rings R und die zugehörigen Faktorringe R/I sind R-Moduln.

Definition 3.0.2. Sei R ein Ring und M ein R-Modul. Dann ist der **Annihilator** von M definiert als:

$$ann\ M = \{r \in R | rM = 0\}.$$

Definition 3.0.3. Ein **Nullteiler** in einem Ring R ist ein Element $0 \neq r \in R$ für das es ein Element $0 \neq s \in R$ gibt, so dass $rs = 0$**.** Ein Element ungleich 0, das kein Nullteiler ist, heißt **Nichtnullteiler.**

3.1 Assoziierte Primideale

Sei R ein Ring und M ein R-Modul.

Definition 3.1.1. Ein Primideal P von R ist **assoziiert** mit M, wenn P der Annihilator eines Elements in M ist. Die Menge aller Primideale assoziiert mit M wird geschrieben als $Ass_R M$ oder einfach $AssM$ wenn keine Verwechslungsgefahr besteht.

Bemerkung 3.1.2. Aus Traditionsgründen gibt es eine Ausnahme: Wenn I ein Ideal von R ist, dann werden die assoziierten Primideale des Moduls R/I assoziierte Primideale von I genannt. Dies führt in der Regel jedoch nicht zu Verwechslungen, da die assoziierten Primideale von I als Modul normalerweise nicht interessant sind.

Bemerkung 3.1.3. Aus der Definition ist klar, dass P genau dann ein assoziiertes Primideal von M ist, wenn R/P isomorph zu einem Untermodul von M ist. Alle assoziierten Primideale von M enthalten den Annihilator von M.

Beispiel 3.1.4 (nach [4] Aufgabe 3.1)**.** Sei $R = \mathbb{Z}$ der Ring der ganzen Zahlen. Dann sind $\mathbb{Z}/i\mathbb{Z}$ ($i \in I$) endlich erzeugte $\mathbb{Z}$-Moduln. $Ass(\mathbb{Z}/i\mathbb{Z})$ ist die Menge der Vielfachen der Primteiler von von i.

Satz 3.1.5. *[Haupteigenschaften assoziierter Primideale]*
Sei R ein Noetherscher Ring und M ein endlich erzeugter R-Modul ungleich 0.

(i) *$AssM$ ist eine endliche, nichtleere Menge von Primidealen von denen jedes ann M enthält. Die Menge $AssM$ enthält alle minimalen Primideale unter denen, die ann M enthalten.*

(ii) *Die Vereinigung der assoziierten Primideale von M besteht aus 0 und der Menge der Nullteiler von M.*

(iii) *Die Bildung der Menge $AssM$ kommutiert mit der Lokalisierung an einer beliebigen multiplikativ abgeschlossenen Menge U in dem Sinne, dass*

$$Ass_{R[U^{-1}]}M[U^{-1}] = \{PR[U^{-1}] | P \in AssM \text{ und } P \cap U = \emptyset\}.$$

Der Beweis dieses Satzes wird am Ende des nächsten Abschnitts gegeben werden.

Definition 3.1.6. Die **Primideale minimal über einem Ideal** I sind die Primideale, welche minimal sind unter den Primidealen, die I enthalten.

Bemerkung 3.1.7. So wie es in jedem Ring maximale Ideale gibt, so gibt es auch in jedem Ring Primideale die minimal sind über einem gegebenen Ideal I.

Um dies einzusehen stellen wir zuerst fest, dass wenn eine Menge von Primidealen in einem Ring R totalgeordnet ist durch Inklusion, dann der Schnitt dieser Primideale wieder prim ist. Nach Zorns Lemma gibt es eine maximale totalgeordnete Teilmenge der Primideale, die I enthalten, und der Schnitt der Primideale in dieser Teilmenge ist notwendigerweise minimal über I. Nach Satz 3.1.5 (i) ist die Menge der Primideale minimal über I endlich wenn R Noethersch ist.

Dieses Ergebnis verallgemeinert die Tatsache, dass ein Polynom ungleich 0 über einer Variablen nur endlich viele Wurzeln haben kann.

Definition 3.1.8. Die Primideale in $AssM$, die nicht minimal sind, werden **eingebettete** Primideale von M genannt.

Wenn R ein graduierter Noetherscher Ring ist und M ein endlich erzeugter R-Modul, dann sind die assoziierten Primideale von R homogen, wie in [4] Proposition 3.12 festgestellt wird. Dies erlaubt es graduierte Versionen aller Resultate in diesem Kapitel zu erstellen.

Folgerung 3.1.9. *Sei R ein Noetherscher Ring und sei M ein endlich erzeugter R-Modul ungleich 0 und I ein Ideal von R. Dann gilt: I enthält einen Nichtnullteiler von M oder I annihiliert ein Element von M.*

Um dies zu beweisen müssen wir wissen, dass ein Ideal, das in einer Vereinigung von Primidealen enthalten ist, bereits in einem von ihnen enthalten ist. Diese Tatsache wird Primvermeidung genannt.

3.2 Primvermeidung

Lemma 3.2.1 (Primvermeidung)**.** *Seien $I_1, ..., I_n, J$ Ideale eines Rings R mit $J \subset \cup_j I_j$. Wenn R einen unendlichen Körper enthält oder wenn höchstens zwei der I_j nicht prim sind, dann ist J in einem der I_j enthalten. Wenn R graduiert ist, J erzeugt wird von homogenen Elementen von Grad größer 0 und alle I_j prim sind, dann reicht es anzunehmen, dass die homogenen Elemente von J in $\cup_j I_j$ enthalten sind, um zu schließen, dass J in einem der I_j enthalten ist.*

Beweis. Wenn R einen unendlichen Körper enthält, dann ist das Ergebnis trivial: Kein Vektorraum über einem unendlichen Körper kann eine endliche Vereinigung von echten Teilräumen sein. Im anderen Fall führen wir eine Induktion über n durch. Der Fall $n = 1$ ist trivial. Wir nehmen an, dass J nicht in einer kleineren Vereinigung der I_j enthalten ist, also können wir Elemente $x_i \in J$ finden, die nicht in $\cup_{j \neq i} I_j$ sind. Wenn also $J \subset \cup I_j$ folgt $x_i \in I_i$. Wenn $n = 2$, dann ist $x_1 + x_2$ weder in I_1 noch in I_2, was ein Widerspruch zur Annahme ist. Wenn $n > 2$ ist, dann können wir annehmen, dass I_1 prim ist und $x_1 + x_2 x_3 ...$ ist in keinem der I_j, was wieder ein Widerspruch ist.

Im graduierten Fall können wir den gleichen Beweis verwenden, indem wir die x_i so potenzieren, dass x_1 und $x_2 x_3 ...$ den gleichen Grad haben. Die Annahme, dass jedes I_j prim ist, brauchen wir um sicherzustellen, dass für jedes j die Potenzen von x_i nicht in I_j sind für $j \neq i$. □

Bemerkung 3.2.2. Für Lemma 3.2.1 haben wir nicht angenommen, dass R Noethersch ist, so dass das Lemma auch im nichtnoetherschen Fall verwendet werden kann, wie z.B. in [4] Proposition 13.10. Der Beweis benutzt auch nur dass J ein Unterring (ohne 1-Element) von R ist.

Der Name „Primvermeidung“ kommt von der folgenden typischen Anwendung: Wenn ein Ideal I nicht enthalten ist in einem einer endlichen Anzahl von Primidealen P_j, dann gibt es ein Element von I das es „vermeidet“ in einem der P_j enthalten zu sein.

Mit Hilfe von Lemma 3.2.1 können wir jetzt die Folgerung 3.1.9 beweisen.

Beweis von Folgerung 3.1.9. Nach Satz 3.1.5 ist ein Ideal, das aus Nullteilern von M besteht, in der Vereinigung der assoziierten Primideale von M enthalten. Nach Lemma 3.2.1 ist es in einem von ihnen enthalten. □

Satz 3.1.5 impliziert, dass $AssM$ nicht leer ist, wenn M ungleich 0 ist. Der erste Schritt im Beweis ist es also die Existenz eines assoziierten Primideals direkt zu zeigen.

Proposition 3.2.3. *Sei R ein Ring und M ein R-Modul ungeleich 0. Wenn I ein Ideal von R ist, das maximal ist unter den Idealen von R, die Annihilatoren von Elementen von M sind, dann ist I prim (und gehört damit zu $AssM$). Insbesondere wenn R noethersch ist, so ist $AssM$ nicht leer.*

Beweis. Wenn $rs \in I$ und $s \notin I$, dann ist zu zeigen, dass $r \in I$. Sei $m \in M$ so, dass $ann\ m = I$, dann gilt $rsm = 0$, aber $sm \neq 0$. Also folgt (r, I) ist enthalten im Annihilator von sm und aus I maximal folgt $(r) + I = I$. Also $r \in I$. □

Diese Proposition ist die Basis für eine typische Anwendung der assoziierten Primideale. Wenn $x \in M$ ein Element eines beliebigen Moduls über einem beliebigen (nicht notwendigerweise Noetherschen) Ring R ist, dann können wir nach Lokalisierung Teil 1 Lemma 1.3.27 testen, ob $x = 0$ gilt, indem wir prüfen, ob x nach 0 geht in der Lokalisierung M_P für jedes Primideal P oder sogar einfach nur für jedes maximale Ideal P. Wenn R Noethersch ist, dann reicht es dies für die assoziierten Primideale zu prüfen. Wenn M endlich erzeugt ist, dann sind dies nur endlich viele.

Folgerung 3.2.4. *Sei M ein Modul über dem Noetherschen Ring R.*

(i) *Wenn $m \in M$, dann gilt $m = 0$ genau dann, wenn m in M_P für jedes maximale assoziierte Primideal P von M nach 0 geht.*

(ii) *Wenn $K \subset M$ ein Untermodul ist, dann gilt $K = 0$ genau dann, wenn $K_P = 0$ für alle $P \in AssM$.*

(iii) *Wenn $\varphi : M \to N$ ein Homomorphismus von M auf einen R-Modul N ist, dann ist φ ein Monomorphismus genau dann, wenn die Lokalisierung $\varphi_P : M_P \to N_P$ ein Monomorphismus für jedes assoziierte Primideal P von M ist.*

Beweis. .

(i) Angenommen $m \neq 0$. Da R Noethersch ist, gibt es ein Primideal das maximal ist unter den Annihilatoren der Elemente von M, und dieses Primideal ist ein assoziiertes Primideal von M nach Proposition 3.2.3. Daraus folgt, dass $ann\ m$ enthalten ist in einem maximalen assoziierten Primideal P, also gilt $\frac{m}{1} \neq 0$ in M_P.

(ii) Wenn $K = 0$ dann gilt $K_P = 0$ für alle P. Wenn $K \neq 0$ wählt man ein $0 \neq m \in K$ und wendet (i) an.

(iii) Nach Proposition Lokalisierung Teil 1 Proposition 1.3.22 gilt $(ker\varphi)_P = ker(\varphi_P)$. (iii) folgt, indem man $K = ker\varphi$ in (ii) einsetzt.

□

Lemma 3.2.5.

(i) *Wenn $M = M' \oplus M''$, dann gilt $AssM = (AssM') \cup (AssM'')$.*

(ii) *Allgemeiner: Wenn* $0 \to M' \to M \to M'' \to 0$ *eine kurze exakte Sequenz von* R*-Moduln ist, dann gilt* $AssM' \subset AssM \subset (AssM') \cup (AssM'')$.

Beweis.

(i) Gegeben (ii) reicht es einzusehen, dass $AssM'' \subset AssM$.

(ii) $AssM' \subset AssM$ ist klar aus der Definition. Für $AssM \subset (AssM' \cup AssM'')$ nehmen wir an, dass $P \in AssM \setminus AssM'$. Wenn $x \in M$ P als Annihilator hat, so dass $Rx \cong R/P$, dann folgt aus P prim, dass jeder Untermodul von Rx, der ungleich 0 ist, P als Annihilator hat. Hieraus folgt, dass $Rx \cap M' = 0$. Also ist Rx isomorph zu seinem Bild in M''. Das bedeutet $P \in AssM''$.

□

Beispiel 3.2.6 (nach [4] Aufgabe 3.1)**.** Sei $R = \mathbb{Z}$ der Ring der ganzen Zahlen. Nach dem Struktursatz für endlich erzeugte abelsche Gruppen ist jede endlich erzeugte abelsche Untergruppe von $\mathbb{Z}$ ($\mathbb{Z}$-Modul) von der Form:

$$\mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} (\mathbb{Z}/d_i\mathbb{Z}).$$

Nach dem Satz über die Untergruppen von $\mathbb{Z}^n$ können wir die d_i so wählen, dass d_i ein Teiler von d_{i+1} ist. $Ass(\mathbb{Z}/d_i\mathbb{Z})$ ist die Menge der Vielfachen der Primteiler von d_i und wir können Lemma 3.2.5 (i) anwenden und erhalten $Ass(\mathbb{Z}/d_i\mathbb{Z}) \subset Ass(\mathbb{Z}/d_{i+1}\mathbb{Z})$.

$Ass\mathbb{Z}^k$ ist dann nur $\{0\}$ und wenn wir wiederum Lemma 3.2.5 (i) anwenden erhalten wir als assoziierte Primideale der ganzen Gruppe $Ass(\mathbb{Z}/d_r\mathbb{Z})$.

Proposition 3.2.7. *Sei* R *ein Noetherscher Ring und* M *ein endlich erzeugter* R*-Modul. Dann hat* M *eine Filtrierung* $0 = M_0 \subset M_1 \subset ... \subset M_n = M$*, so dass gilt* $M_{i+1}/M_i \cong R/P_i$ *für ein Primideal* P_i.

Beweis. Wenn $M \neq 0$ ist, dann hat nach Proposition 3.2.3 M mindestens ein assoziiertes Primideal, sagen wir P_1, so dass es einen Untermodul $M_1 \cong R/P_1$ gibt. Wenn wir diese Argumentation nochmals anwenden auf M/M_1, dann produzieren wir M_2 und so weiter. Diese Kette bricht irgendwann ab, denn die Untermoduln von M erfüllen die aufsteigende-Ketten-Bedingung und das bedeutet, dass irgendein M_n gleich M ist. □

Wenn wir Lemma 3.2.5 induktiv anwenden, dann sehen wir, dass die assoziierten Primideale von M unter den Primidealen P_i sind, die in Proposition 3.2.7 auftauchen. Dies beweist die Endlichkeit in Satz 3.1.5.

Definition 3.2.8. Die Moduln M, die eine Filtrierung wie in Proposition 3.2.3 zulassen und für die zusätzlich jedes P_i ein assoziiertes Primideal von M ist, werden **rein** genannt.

Nun können wir den Beweis des Satzes 3.1.5 führen.

Beweis von Satz 3.1.5. .

(ii) Die Aussage folgt direkt aus Proposition 3.2.3. Wenn r ein Element ungleich 0 von M annihiliert, dann ist r enthalten in einem maximalen annihilierenden Ideal.

(iii) Wenn $P \in AssM$ ist, dann gibt es eine Inklusion $R/P \subset M$. Durch Lokalisierung erhalten wir eine Injektion $R[U^{-1}]/PR[U^{-1}] \subset M[U^{-1}]$. Wenn also $PR[U^{-1}]$ ein Primideal von $R[U^{-1}]$ ist (d.h. $P \cap U = \emptyset$, also $PR[U^{-1}]$ immer noch ein Ideal ist) dann ist $PR[U^{-1}] \in AssM[U^{-1}]$.

Andersherum nehmen wir an, dass Q ein Primideal von $R[U^{-1}]$ ist, das assoziert ist zu $M[U^{-1}]$. Dann können wir schreiben $Q = PR[U^{-1}]$ mit einem Primideal P von R und $P \cap U = \emptyset$. Es gibt eine Injektion $\varphi : R[U^{-1}]/PR[U^{-1}] \to M[U^{-1}]$. Da P endlich erzeugt ist, gilt nach Lokalisierung Teil 1 Proposition 1.3.30:

$$Hom_{R[U^{-1}]}(R[U^{-1}]/PR[U^{-1}], M[U^{-1}]) = Hom_R(R/P, M)[U^{-1}].$$

Also können wir schreiben $\varphi = u^{-1}f$ für ein $f \in Hom_R(R/P, M)$ und $u \in U$. Da u kein Nullteiler von R/P ist folgt dass f eine Injektion ist, was den Beweis von (iii) vervollständigt.

(i) Es bleibt zu zeigen, dass wenn P ein über *ann* M minimales Primideal ist, dann $P \in AssM$. Nach (iii) können wir lokalisieren und nehmen an, dass R lokal ist mit einem maximalen Ideal P. Nach Proposition 3.2.3 ist die Menge $AssM$ nicht leer, und da P das einzige Primideal ist, das *ann* M enthält, folgt $P \in AssM$.

□

3.3 Primärzerlegung

Für den Rest des Kapitels seien R ein Noetherscher Ring und M ein endlich erzeugter R-Modul.

Definition 3.3.1. Ein Untermodul N eines Moduls M wird **primär** genannt, wenn $Ass(M/N)$ aus nur einem Primideal besteht; wenn $Ass(M/N) = P$, dann heißt N **P-primär**. Ein Modul M ist **koprimär**, wenn 0 ein primärer Untermodul ist, d. h. wenn $Ass(M)$ aus nur einem Primideal besteht.

Bemerkung 3.3.2. Aus Lemma 3.2.5 ist leicht ersichtlich, dass ein Schnitt von P-primären Untermoduln P-primär ist.

Folgerung 3.3.3. *Sei P ein Primideal eines Rings R und $N_1, ..., N_t \subset M$ R-Moduln. Wenn jedes N_i ein P-primärer Untermodul von M ist, dann ist auch $\cap_i N_i$ P-primär.*

Beweis. Für die Induktion reicht es den Fall $t = 2$ zu zeigen. Angenommen M/N_1 und M/N_2 sind P-koprimär. Nach Lemma 3.2.5 (i) ist P das einzige assoziierte Primideal von $M/N_1 \oplus M/N_2$. Da es eine Injektion von $M/(N_1 \cap N_2)$ nach $M/N_1 \oplus M/N_2$ gibt, folgt aus Lemma 3.2.5 (ii), dass $M/(N_1 \cap N_2)$ auch koprimär ist. □

Für den Beweis der nächsten Proposition brauchen wir eine Folgerung, die aus Lokalisierung Teil 2 Proposition 1.1.1 folgt.

Folgerung 3.3.4. *Wenn I ein Ideal in einem Ring R ist, dann gilt*

$$rad\ I = \{f | f^n \in I \text{ für ein } n\} = \bigcap_{\{P | P \text{ ist Primideal und } I \subset P\}} P.$$

Insbesondere ist der Schnitt aller Primideale von R das Radikal von (0), welches die Menge aller nilpotenten Elemente von R ist.

Beweis. Die Menge $rad\ I$ ist in der rechten Seite enthalten. Wenn f nicht in $rad\ I$ ist, dann ist ein Ideal maximal unter denen, die I enthalten und disjunkt sind von $\{f^n | n \geq 1\}$, prim, also ist f nicht enthalten in der rechten Seite. □

Proposition 3.3.5. *Sei P ein Primideal von R. Dann sind die folgenden Aussagen äquivalent:*

(i) *M ist P-koprim.*

(ii) *P ist minimal über $ann\ M$ und jedes Element außerhalb P ist ein Nichtnullteiler von M.*

(iii) *Eine Potenz von P annihiliert M und jedes Element außerhalb P ist ein Nichtnullteiler von M.*

Beweis.

$(i) \Rightarrow (ii)$ Da P das einzige assoziierte Primideal von M ist, folgt aus Satz 3.1.5 (i), dass P minimal ist über $ann\ M$. Aus Satz 3.1.5 (ii) folgt, dass jedes Element, das nicht in P liegt, Nichtnullteiler von M ist.

$(ii) \Rightarrow (iii)$ Da die Elemente, die nicht in P sind, alle Nichtnullteiler von M sind, reicht es zu zeigen, dass die Aussage nach Lokalisierung an P gilt. Also können wir annehmen, dass R ein lokaler Ring ist mit maximalem Ideal P. Da P minimal ist über $ann\ M$, folgt aus Folgerung 3.3.4, dass P Radikal von $ann\ M$ ist; also ist P nilpotent modulo $ann\ M$.

$(iii) \Rightarrow (i)$ Da P nilpotent ist modulo $ann\ M$, ist es auch minimal unter den Primidealen, die $ann\ M$ enthalten, und ist ein assoziiertes Primideal von M nach Satz 3.1.5 (i). Da jedes Element außerhalb von P ein Nichtnullteiler ist, ist jedes assoziierte Primideal von M enthalten in P nach Satz 3.1.5 (ii). Also ist P das einzige assoziierte Primideal von M.

□

Bemerkung 3.3.6. Die klassische Definition deckt nur den wichtigsten Fall ab, in dem $M = R/I$ ist für ein Ideal $I \neq 0$ von R. Dann zeigt Proposition 3.3.5 (ii), dass I P-primär ist genau dann, wenn I eine Potenz von P enthält und für alle $r, s \in R$ die Bedingungen $rs \in I$ und $r \notin P$ implizieren dass $s \in I$.

Man kann sich die Situation auch für Lokalisierungen denken: Proposition 3.3.5 (ii) zeigt, dass M P-koprimär ist genau dann, wenn P minimal ist über dem Annihilator von M und wenn M einbettet nach M_P. Allgemein gilt, dass wenn M ein Modul ist und P ein minimales Primideal über dem Annihilator von M ist, dann ist der Untermodul $M' \subset M$ definiert durch $M' = ker(M \to M_P)$ P-primär, da es eine Injektion von M/M' nach $(M/M')_P = M_P$ gibt. In dieser Situation wird M' **P-primäre Komponente** von 0 in M genannt. Sie hängt nur von M und P ab.

Primärzerlegung besteht also daraus, ein beliebiges Untermodul M' von M als Schnitt von primären Untermoduln zu schreiben.

Satz 3.3.7. *Sei R ein Noetherscher Ring und M ein endlich erzeugter R-Modul. Dann ist jeder echte Untermodul M' von M der Schnitt von endlich vielen primären Untermoduln. Diese Zerlegung heißt* **Primärzerlegung**. *Wenn $P_1, ..., P_n$ Primideale sind und $M' = \bigcap_{i=1}^{n} M_i$ mit M_i ein P_i-primärer Untermodul, so gilt:*

(i) *Jedes assoziierte Primideal von M/M' ist unter den P_i.*

(ii) *Wenn der Schnitt irredundant ist (d.h. kein M_i kann weggelassen werden) dann sind die P_i genau die assoziierten Primideale von M/M'.*

(iii) *Wenn der Schnitt minimal ist (d.h. es gibt keinen Schnitt mit weniger Termen) dann ist jedes assoziierte Primideal von M/M' gleich einem P_i für genau einen Index i. Wenn P_i minimal ist über dem Annihilator von M/M', dann ist M_i P_i-primäre Komponente von 0 in M'.*

(iv) *Minimale Primärzerlegungen lokalisieren im folgenden Sinne: Angenommen $M' = \bigcap_{i=1}^{n} M_i$ ist eine minimale Primärzerlegung. Wenn U eine multiplikativ abgeschlossene Teilmenge von R ist und $P_1, ..., P_t$ Primideale unter den P_i sind, die nicht in U sind, dann gilt:*

$M'[U^{-1}] = \cap_{i=1}^{t} M_i[U^{-1}]$

ist eine maximale Primärzerlegung über $R[U^{-1}]$.

Der Beweis hierzu wird nach einigen Bemerkungen gegeben werden.

Bemerkung 3.3.8. Im Fall von (iii) wird der Modul M_i oft **P_i-primäre Komponente von** M in der gegebenen Zerlegung genannt.

Wir zeigen zuerst die Existenz einer etwas feineren, aber weniger kanonischen Zerlegung.

Definition 3.3.9. Ein Untermodul $N \subset M$ ist **irreduzibel**, wenn N nicht der Schnitt von zwei strikt größeren Untermoduln ist.

Zuerst behaupten wir, dass jeder Untermodul von M als Schnitt von endlich vielen irreduziblen Untermoduln geschrieben werden kann. Andererseits gilt nach der aufsteigende-Ketten-Bedingung für Untermoduln von M, dass wir ein Untermodul $N \subset M$ wählen können, das maximal ist unter den Untermoduln, die nicht Schnitt von irreduziblen Untermoduln sind. Insbesondere ist N selbst nicht irreduzibel, also Schnitt von zwei strikt größeren Untermoduln N_1 und N_2. Aus der Maximalität von N folgt, dass beide N_i Schnitte von irreduziblen Untermoduln sind und es folgt, dass N dies auch ist. Dieser Widerspruch beweist die Behauptung und zeigt, dass es eine **irreduzible Zerlegung** $M' = \cap_i M_i$ gibt mit M_i irreduzibel für alle i.

Jetzt zeigen wir, dass jede irreduzible Zerlegung eine Primärzerlegung ist. Also zeigen wir, dass jeder irreduzible Untermodul $N \subset M$ primär ist oder äquivalent dass M/N koprimär ist. Sonst hätte M/N mindestens zwei assoziierte Primideale P und Q, also würde es ein Untermodul isomorph zu R/P und ein anderes isomorph zu R/Q enthalten. Der Annihilator von jedem Element ungleich 0 in R/P ist P, analog für Q, so dass sich diese beiden Untermoduln von M/N nur in 0 überschneiden können. Daher ist 0 reduzibel. Aus den Urbildern dieser Untermoduln in M sehen wir, dass N reduzibel ist: ein Widerspruch. Also ist M/N koprimär, und daher sind irreduzible Zerlegungen Primärzerlegungen.

Die Aussagen in Satz 3.3.7 sind Aussagen über M/M'. Um die Notation zu vereinfachen faktorisieren wir M' aus und nehmen daher an, dass $M' = 0$.

Beweis von Satz 3.3.7.

(i) Angenommen $0 = \bigcap_i M_i$ ist eine Primärzerlegung. Dann gilt $M \subset \oplus M/M_i$, also gilt nach Lemma 3.2.5 dass jedes Primideal in $AssM$ unter den Primidealen P_i auftaucht.

(ii) Jetzt nehmen wir an, dass die gegebene Zerlegung irredundant ist, so dass für jedes j gilt $\bigcap_{i\neq j} M_i \neq 0$. Da $M_j \cap \bigcap_{i\neq j} M_i = 0$ ist gilt:

$\bigcap_{i\neq j} M_i = (\bigcap_{i\neq j} M_i)/(M_j \cap \bigcap_{i\neq j} M_i) \cong (\bigcap_{i\neq j} M_i + M_j)/M_j \subset M/M_j$.

Da dieser Modul P_j-koprimär ist, ist es auch $\bigcap_{i\neq j} M_i$. Aus Lemma 3.2.5 folgt, dass P_j ein assoziiertes Primideal von M ist. Zusammen mit (i) beweist das (ii).

(iii) Angenommen die gegebene Zerlegung ist minimal. Nach Folgerung 3.3.3 ist der Schnitt von P-primären Untermoduln P-primär, also impliziert die Minimalität, dass die P_i disjunkt sind. Mit (ii) zeigt dies die erste Aussage von (iii).

Für die zweite Aussage nehmen wir an, dass P_i minimal ist über dem Annihilator von M. Wir müssen zeigen, dass M_i der Kern der Lokalisierungsabbildung $\alpha : M \to M_{P_i}$ ist. Seien $\beta : M \to M/M_i$ Projektionsabbildung, $\delta : M/M_i \to (M/M_i)_{P_i}$ Lokalisierungsabbildung und $\gamma : M_{P_i} \to (M/M_i)_{P_i}$ die Projektion von M_{P_i} auf $M_{P_i}/M_{iP_i} = (M/M_i)_{P_i}$. Der Kern von β ist M_i. Um zu zeigen, dass der Kern von α auch M_i ist, reicht es zu zeigen dass sowohl γ als auch δ Monomorphismen sind. Da M_i P_i-primär ist, ist dies offensichtlich für δ.

Da $\cap_j M_j = 0$ ist, ist die natürliche Abbildung $\varphi : M \to \oplus M/M_j$ ein Monomorphismus. Nach Lokalisierung Teil 1 Proposition 1.3.22 erhält Lokalisierung Monomorphismen, so dass $\varphi_{P_i} : (M \to \oplus M/M_j)_{P_i}$ ein Monomorphismus ist. Die Abbildung γ ist die i-te Komponente von φ_{P_i}. Da P_i minimal ist über dem Annihilator von M, wissen wir dass P_j nicht enthalten ist in P_i für $j \neq i$. Da M/M_j P_j-koprimär ist, haben wir $(M/M_j)_{P_i} = 0$ für $j \neq i$, so dass die j-te Komponente von φ_{P_i} verschwindet und wir sehen, dass γ ein Monomorphismus ist.

(iv) Wenn $U \cap P_i = \emptyset$ ist, dann ist $P_i[U^{-1}]$ ein Primideal von $R[U^{-1}]$ und nach Satz 3.1.5 (iii) ist $M_i[U^{-1}]$ $P_i[U^{-1}]$-primär. Wenn $U \cap P_i \neq \emptyset$ dann sehen wir aus Proposition 3.3.5 (iii), dass $M_i[U^{-1}] = M[U^{-1}]$. Daraus folgt $0 = \bigcap_{i=1}^{t} M_i[U^{-1}]$ ist eine Primärzerlegung. Um zu sehen, dass sie minimal ist, reicht es nach (ii) zu zeigen, dass die assoziierten Primideale von $M[U^{-1}]$ die assoziierten Primideale von M sind, welche disjunkt sind von U, und dies folgt aus Satz 3.1.5 (iii).

□

4 Primärzerlegung Teil 2

Daniel Schüssler

4.1 Definitionserinnerungen

Sei hier R ein noetherscher Ring, M ein endlich erzeugter R-Modul, N ein Untermodul. (Einige der Definitionen ergeben auch bei weniger Voraussetzungen Sinn).

Die Menge der **assoziierten Primideale von** M ist definiert als

$$\operatorname{Ass}(M) := \{P \subset R \mid P \text{ Primideal und } P = \operatorname{ann} m \text{ für ein } m \in M\}.$$

(P muss nicht nur m annihilieren, sondern der ganze Annihilator von m sein!)

$\operatorname{Ass} M$ ist endlich, nichtleer und enthält alle Primideale, die minimal über $\operatorname{ann} M$ sind. Die Vereinigung der assoziierten Primideale ist genau die 0 zusammen mit den Nullteilern auf M. Ausnahmefall für Ideale: $\operatorname{Ass}(I) := \operatorname{Ass}(R/I)$.

N heißt **P-primär** in M wenn $\operatorname{Ass} M/N = \{P\}$.

M heißt **P-koprimär** wenn $\operatorname{Ass} M = \{P\}$.

Primärzerlegung von N in M Eine Darstellung $N = \cap_i M_i$, so dass M_i P_i-primär.

Unter den P_i kommen alle Elemente von $\operatorname{Ass} M/N$ vor.

Die Primärzerlegung heißt **irredundant**, wenn man keines der M_i weglassen kann; in diesem Fall kommen unter den P_i genau die Elemente von $\operatorname{Ass} M/N$ vor.

Die Zerlegung heißt **minimal**, wenn es keine mit weniger Termen gibt. Dann kommen unter den P_i genau die Elemente von $\operatorname{Ass} M/N$ und jedes nur einmal vor.

Bsp. 1: $R = \mathbb{Z}, M = \mathbb{Z}/(2^n) \oplus \mathbb{Z}/(3^m) \oplus \mathbb{Z}/(5^l) \Rightarrow$
$0 = 0 \oplus \mathbb{Z}/(3^m) \oplus \mathbb{Z}/(5^l) \cap \mathbb{Z}/(2^n) \oplus 0 \oplus \mathbb{Z}/(5^l) \cap \mathbb{Z}/(2^n) \oplus \mathbb{Z}/(3^m) \oplus 0$

Bsp. 2: $R = \mathbb{Z}, M = \mathbb{Z} \oplus \mathbb{Z}/(p)$

Sei $n \geq 0$ beliebig.

$0 = \underbrace{0 \oplus \mathbb{Z}/(p)}_{(0)\text{-primär}} \cap \underbrace{(p^n) \oplus 0}_{(p)\text{-primär}}$

(nicht eindeutig!)

Bsp. 3: $M = R = K[x, y]$

$N = (x^2, xy) N = \underbrace{(x)}_{(x)\text{-primär}} \cap \underbrace{(x^2, y)}_{(x,y)\text{-primär}} = (x) \cap \underbrace{(x^2, xy, y^2)}_{(x,y)\text{-primär}}$

(darauf gehen wir später genauer ein).

4.2 Primärzerlegung und Primfaktorzerlegung

Hier soll der Zusammenhang zwischen der Primärzerlegung und der aus faktoriellen Ringen bekannten eindeutigen Primfaktorzerlegung (Zerlegung in Primelemente) geklärt werden.

Satz 4.2.1. *Sei R ein noetherscher Integritätsring.*

a) Sei $f \in R$ und $f = u \prod p_i^{e_i}$, wobei u eine Einheit von R sei und die p_i Primelemente, die verschiedene Ideale erzeugen (d.h. sie unterscheiden sich nicht nur um eine Einheit); die e_i seien natürliche Zahlen.
Dann ist $(f) = \cap(p_i^{e_i})$ eine minimale Primärzerlegung von (f).

b) R ist faktoriell genau dann, wenn jedes Primideal, dass minimal über einem Hauptideal ist auch selbst ein Hauptideal ist.

Beweis. zu a)
Beobachtung: Sei p prim. Dann gilt $fg \in (p^e) \Rightarrow g \in (p^e)$ oder $f \in (p)$.
Beweis: Induktion über e.

- Fall $e = 0$: $g \in (p^0) = R$ ist immer erfüllt.
- Die Aussage gelte für $e-1$. Sei $fg \in (p^e)$, $f \notin (p)$. Insbesondere $fg \in (p)$; und weil (p) prim ist $g \in (p)$. Es folgt $f\frac{g}{p} \in (p^{e-1})$ (Da R Integritätsbereich ist), also nach Induktionsvoraussetzung $\frac{g}{p} \in (p^{e-1})$ und somit $g \in (p^e)$.

Eine Primärzerlegung ist eine Darstellung eines Untermoduls als Schnitt von primären Untermoduln. Wir betrachten hier Ideale als R-Untermoduln von R.

Zunächst zeigen wir also, dass die $(p_i^{e_i})$ auch wirklich (p_i)-primäre Ideale sind, d.h.: $\operatorname{Ass} R/(p_i^{e_i}) = \{(p_i)\}$.

„$\subseteq$“ : Sei Q ein zu $R/(p_i^{e_i})$ assoziiertes Primideal, also $Q = \operatorname{ann} \tilde{f}$ für ein $\tilde{f} = f + (p_i^{e_i}) \in R/(p_i^{e_i})$, $f \in R$.

- $(p_i^{e_i})$ annihiliert $\tilde{f}$ sicher, also $(p_i^{e_i}) \subseteq Q$ und, weil Q prim ist, $(p_i) \subseteq Q$
- Sei nun umgekehrt $q \in Q$. Es gilt $\tilde{f} \neq 0$ (da sonst $Q = \operatorname{ann} 0 = R$ und daher Q nicht prim wäre), also $f \notin (p_i^{e_i})$. Aus $Q = \operatorname{ann} \tilde{f}$ ergibt sich $q\tilde{f} = 0$, was gleichbedeutend ist mit $qf \in (p_i^{e_i})$. Nach der Beobachtung folgt aus den letzten beiden Aussagen $q \in (p_i)$, also $Q \subseteq (p_i)$.

Insgesamt also $Q = (p_i)$.

„$\supseteq$“ : (p_i) ist der Annihilator der Äquivalenzklasse von $p_i^{e_i - 1}$. Alternativ verwendet man einfach die Tatsache, dass $\operatorname{Ass} R/(p_i^{e_i})$ nicht leer ist.

Wir beweisen nun $(f) = \cap(p_i^{e_i})$.

$(f) = \prod(p_i^{e_i})$ ist klar. Da das Produkt von Idealen immer in ihrem Schnitt enthalten ist, müssen wir nur noch die Richtung $\prod(p_i^{e_i}) \supseteq \bigcap(p_i^{e_i})$ zeigen.

Wenn wir zeigen können, dass $(g)(p^e) \supseteq (g) \cap (p^e)$ für alle g, die nicht von p geteilt werden, p prim, folgt die Aussage offenbar per Induktion (denn p_{i+1} teilt $p_1^{e_1} \dots p_i^{e_i}$ nicht,

da es dann einen der Faktoren $p_j$teilen müsste und p_j dann auch p_i, was im Widerspruch zur Voraussetzung stünde, dass sie verschiedene Ideale erzeugen).

Sei also $gh \in (g) \cap (p^e)$. Aus $gh \in (p^e), g \notin (p)$ folgt mit der Beobachtung $h \in (p^e)$ also $gh \in (g)(p^e)$ wie gewünscht.

Damit ist gezeigt, dass $(f) = \cap(p_i^{e_i})$ eine Primärzerlegung ist. Nach Satz 3.3.7. (i) sind also die zu $R/(f)$ assoziierten Primideale höchstens die (p_i) (In einer Primärzerlegung kommt jedes assoziierte Primideal vor). Andererseits ist jedes Element von (p_i) ein Nullteiler auf $R/(f)$ (es ist nämlich $ap_i \frac{f}{p_i} \in (f)$). Nach Folgerung 3.1.9. ist ein Ideal, dass nur aus Nullteilern besteht, in einem der assoziierten Primideale enthalten. Da die assoziierten Primideale, wie eben festgestellt, aber alle von der Form (p_j) sind, ist (p_i) selbst in $\operatorname{Ass} R/(f)$.

Insgesamt also $\operatorname{Ass} R/(f) = \{(p_1), \ldots, (p_n)\}$. Weil zu jedem (p_i) genau eines der Ideale in unserer Primärzerlegung primär ist, folgt mit Satz 3.3.7. (iii), dass die Zerlegung minimal ist.

Ich denke, dass dies außerdem die einzige minimale Zerlegung ist, da die (p_i) alle minimal (bezüglich Inklusion) sind und nach Satz 3.3.7 (iii) die P-primären Untermoduln für minimale P eindeutig bestimmt sind.

zu b)

„⇒“: Sei R faktoriell. Nach Teil a) sind die zu $R/(f)$ assoziierten Primideale genau die (p_i). Nach Satz 3.1.5 (i) enthält $\operatorname{Ass} R/(f)$ alle Primideale, die minimal über $\operatorname{ann} R/(f)$, also (f), sind. Diese über (f) minimalen Primideale sind also Hauptideale.

„⇐“: Bekanntlich kann man in jedem noetherschen Ring ein Element in irreduzible Elemente zerlegen (andernfalls könnte immer weiter einen Faktor in zwei nicht-Einheiten aufspalten und würde damit immer größere Ideale erhalten). Um die Eindeutigkeit der Zerlegung zu beweisen, reicht es zu zeigen, dass in R jedes irreduzible Element prim ist.

Sei dazu $f \in R$ irreduzibel. Nach Bemerkung 3.1.7. gibt es ein Primideal P, dass minimal über (f) ist. Nach Voraussetzung $P = (p)$ für ein $p \in R$. $f \in P$ bedeutet $f = pr$. Da f irreduzibel ist, muss r eine Einheit sein und somit $(f) = (p)$ (und Erzeuger von Primidealen sind prim).

□

4.3 Der graduierte Fall

Definition 4.3.1. Ein *graduierter Ring* ist ein Ring R mit einer Zerlegung $R = R_0 \oplus R_1 \oplus \ldots$ als additive abelsche Gruppe so, dass $R_iR_j \subseteq R_{i+j}$. (Beispiel: Polynomringe).

Ein *homogenes Element* ist ein Element eines der R_i.

Ein *homogenes Ideal* ist ein Ideal, dass von homogenen Elementen erzeugt wird (es wird i.A. nicht nur homogene Elemente enthalten).

Ein *graduierter R-Modul* ist ein R-Modul mit einer Zerlegung $M = \bigoplus_{i\in\mathbb{Z}} M_i$ als additive abelsche Gruppe so, dass $R_iM_j \subseteq M_{i+j}$.

Ein *homogener Modul* ist ein Untermodul (eines graduierten Moduls), der von homogenen Elementen erzeugt wird.

Sei R ein graduierter noetherscher Ring und M ein endlich erzeugter graduierter R-Modul. In diesem Fall sind die zu M assoziierten Primelemente homogen, es kann eine Primärzerlegung der 0 in M in homogene Moduln gefunden werden und M erlaubt eine Filtrierung wie in Proposition 3.2.7. mit homogenen M_i und P_i. Die wesentliche Idee dazu ist

Proposition 4.3.2. *Sei $m \in M$ und $P = \operatorname{ann} m$. Wenn P prim ist, so ist P ein homogenes Ideal und P ist der Annihilator eines homogenen Elementes.*

Beweis. Jedes $f \in R$ hat eine eindeutige Darstellung als Summe $f = \sum_{i=1}^{s} f_i$ mit $f_i \neq 0$ und $f_i \in R_{d_i}$ mit $d_1 < \ldots < d_s$. Es reicht zu zeigen, dass für jedes $f \in P$ all diese homogenen Komponenten in P enthalten sind (da P dann von den homogenen Komponenten seiner Erzeuger erzeugt wird).

Dies beweisen wir durch Induktion über s. Der Fall $s = 0$ ist klar. Gelte nun, dass für jedes $f \in P$, das aus $s-1$ Komponenten besteht, die Komponenten schon in f enthalten sind. Wenn wir zeigen können, dass $f_1 \in P$, so ist auch $\sum_{i=2}^{s} f_i = f - f_1 \in P$ und somit alle $f_i \in P$. Wegen $P = \operatorname{ann} m$ bedeutet $f \in P \;\; fm = 0$ und wir möchten zeigen, dass $f_1 \in P$.

Auch m hat eine eindeutige Darstellung $m = \sum_{i=1}^{t} m_i$ mit $m_i \neq 0$ und homogen vom Grad e_i mit aufsteigenden e_i. Wir verschachteln nun in der obigen Induktion eine Induktion über t; wir beweisen die Aussage „für alle m mit t oder weniger Komponenten gilt $fm = 0 \Rightarrow f_1 m = 0$“.

$t = 0$ klar. Die Aussage gelte nun für $t-1$. Wir betrachten $I := \operatorname{ann} f_1 m \supseteq \operatorname{ann} m = P$

- Fall $I = P$:

  Im Produkt $fm = (\sum_{i=1}^{s} f_i)(\sum_{i=1}^{t} m_i)$ ist $f_1 m_1$ der einzige Term vom Grad $d_1 + m_1$. Das Produkt ist in jeder Komponente 0, also $f_1 m_1 = 0$.

  Daraus erhalten wir $f_1 m = \sum_{i=2}^{t} f_1 m_i$, d.h. $f_1 m$ hat weniger Komponenten als m. Es ist $f(f_1 m) = 0$ (weil $fm = 0$), also folgt nach Induktionsvoraussetzung $f_1(f_1 m) = 0$, also $f_1 \in \operatorname{ann} f_1 m = I = P$.

- Fall $I \supsetneq P$:

  Sei also $g \in I \backslash P$. Es ist $g f_1 m = 0$, also $g f_1 \in \operatorname{ann} m = P$. Weil P prim ist folgt $f_1 \in P$.

Damit ist bewiesen, dass P homogen ist.

Für jeden homogenen Erzeuger h von P ist $hm = 0$, also wieder durch „Komponentenvergleich“ $hm_i = 0$ für alle i und somit $Pm_i = 0$, d.h. $P \subseteq \operatorname{ann} m_i$.

Aus $P = \operatorname{ann} m \supseteq \cap_i \operatorname{ann} m_i \supseteq P$ folgt $P = \cap_i \operatorname{ann} m_i \supseteq \prod_i \operatorname{ann} m_i$. Weil P prim ist, ist also $\operatorname{ann} m_i \subseteq P$ für eines der i. $\rightsquigarrow \operatorname{ann} m_i = P$. □

4.4 Informationen aus der Primärzerlegung gewinnen

Sei hier stets R ein noetherscher Ring und M ein endlich erzeugter R-Modul.

Sei $0 = \cap_i M_i$ eine minimale Primärzerlegung der 0 (Erinnerung: das bedeutet insbesondere, dass die M_i P_i-primär sind, wobei die P_i die assoziierten Primideale von $M/0 = M$ sind.) In Satz 3.3.7. (iii) haben wir gesehen, dass die M_i, die zu minimalen Primidealen P_i gehören, eindeutig bestimmt sind (nämlich $M_i = \ker(M \to M_{P_i}) =$ Kern der Lokalisierungsabbildung nach dem Komplement von $P_i = \{x \in M | ux = 0 \text{für ein} u \in R \backslash P\}$).

Andererseits sind die M_i, die zu nicht-minimalen P_i gehören, i.A. nicht eindeutig bestimmt (man nennt diese nicht-minimalen Primideale auch *eingebettete Primideale*. Die geometrische Bedeutung ist, dass aus $P \supseteq Q$ folgt $Z(P) \subseteq Z(Q)$, d.h. die Nullstellenmenge ist in eine Größere „eingebettet“.). In diesem Abschnitt soll gezeigt werden, dass aber zumindest bestimmte Teil-Schnitte in der obigen Primärzerlegung eindeutig bestimmt sind.

Definition 4.4.1. Sei I ein Ideal. Setze

$$H_I^0(M) := \{m \in M : I^n m = 0 \text{für hinreichend große } n\}.$$

Das ist offenbar ein Untermodul von M (für die Summe von zwei Elementen nehme man das Größere ihrer n).

Bemerkung 4.4.2. $H_I^0(M)$ hängt nur von dem Radikal des Ideals ab.

Beweis. $I \subseteq \operatorname{rad}(I)$, also $\operatorname{rad}(I)^n m = 0 \Rightarrow I^n m = 0$.

Sei umgekehrt $I^n m = 0$. Da R noethersch ist, ist $\operatorname{rad}(I) = (f_1, \ldots, f_k)$ endlich erzeugt. Per Definition von rad gibt es zu jedem j ein e_j mit $f_j^{e_j} \in I$. Sei $e = \max_j e_j$.

Die Elemente von $\operatorname{rad}(I)^{ke}$ sind von der Form $g = \prod_j^{ke}(\sum_i^k r_{i,j} f_i)$. Wenn man das ausmultipliziert, enthält jeder Summand ein Produkt von ke vielen der f_i. Also muss mindestens eines der f_i mindestens in der Potenz e vorkommen. Nach Konstruktion ist $f_i^e \in I$. Also ist der Summand $(= f_i^e \cdot \text{Rest})$ in I und da dies für alle Summanden gilt, ist $g \in I \rightsquigarrow \operatorname{rad}(I)^{ke} \subseteq I \rightsquigarrow \operatorname{rad}(I)^{nke} \subseteq I^{nke} \rightsquigarrow \operatorname{rad}(I)^{nke} m = 0$.

(Und offenbar gilt $I^n m = 0 \Rightarrow I^{n'} m = 0$ für $n' > n$). □

Proposition 4.4.3. *Sei $I \subseteq R$ ein Ideal und sei $A = \{P \in \operatorname{Ass} M | P \supseteq I\}$ die Menge der assoziierten Primideale von M, die I enthalten.*

a) Sei $0 = \cap_i M_i$ eine Primärzerlegung der 0 (0 als Untermodul von M) und seien die M_i jeweils P_i-primär. Dann gilt $H_I^0(M) = \bigcap_{i: P_i \notin A} M_i$. Insbesondere ist dieser Schnitt unabhängig von der gewählten Primärzerlegung.

b) Es gibt ein Element $f \in I$ so, dass gilt: $P \in A$ genau dann wenn ($P \in \operatorname{Ass} M$ und $f \in P$). (d.h. die assoziierten Primideale, die I enthalten sind genau die, die f enthalten). Für jedes solche f gilt:

$H_I^0(M) = \ker(M \to M[f^{-1}])$.

c) $\operatorname{Ass} M$ zerfällt in die Mengen $\operatorname{Ass} H_I^0(M) = A$ und $\operatorname{Ass} M/H_I^0(M) = (\operatorname{Ass} M) \backslash A$.

$H_I^0(M)$ ist durch diese Eigenschaft eindeutig bestimmt.

Beweis. Erinnerung: Sei N Untermodul von M, J ein Ideal. Definiere: $(N :_M J) := \{m \in M | Jm \subseteq N\}$. (Das ist ein Untermodul).

zu a)

In dieser Notation können wir schreiben:

$H^0_I(M) = \bigcup_{n=0}^{\infty}(0 :_M I^n) =: (0 :_M I^\infty)$.

Da nach Voraussetzung $0 = \cap_i M_i$, erhalten wir:

(*) $\quad H^0_I(M) = \bigcap_i (M_i :_M I^\infty)$

(Begründung: Sei $m \in M$

„$\subseteq$“: $I^n m = 0 \Rightarrow I^n m \in M_i$ für alle i.

„$\supseteq$“: Für jedes i ist $I^{n_i} m \subseteq M_i$ für hinreichend großes n_i. Nimmt man $n = \max_i n_i$, ist $I^n m \subseteq \cap M_i = 0$.)

Wir betrachten nun die $(M_i :_M I^\infty)$ für verschiedene i. M_i ist P_i-primär, also ist $M/M_i P_i$-koprimär.

- Fall $P_i \supseteq I$: Nach Proposition 3.3.5 (iii) folgt: Eine Potenz von P_i annihiliert M/M_i, mit anderen Worten: $(M_i :_M P_i^n) = M$ (für hinreichend große n). Zusammen mit $P_i^n \supseteq I^n$ erhalten wir $(M_i :_M I_i^n) = M \rightsquigarrow (M_i :_M I^\infty) = M$. Da der ganze Modul das Neutralelement des Schnittes ist, kann $(M_i :_M I^\infty)$ aus (*) weggelassen werden.

- Fall $P_i \not\supseteq I$: Nach dem anderen Satz aus Proposition 3.3.5 (iii) ist jedes Element außerhalb P_i ein Nichtnullteiler auf M/M_i. Also enthält I einen Nichtnullteiler y auf M/M_i. Das bedeutet, auf M zurückgezogen, dass y Elemente außerhalb M_i wieder auf solche abbildet. Per Induktion gilt das auch für y^n. Also gilt $(M_i :_M I^\infty) = M_i$ (Elemente aus M_i werden sicher wieder in M_i abgebildet, alle anderen wegen dem y^n nicht).

Insgesamt ergibt (*) also: $H^0_I(M) = \bigcap_{i:P_i \not\supseteq I} M_i = \bigcap_{i:P_i \notin A} M_i$

zu b)

I ist nach Konstruktion von A nicht Teilmenge eines der Ideale aus $(\operatorname{Ass} M)\backslash A$; nach dem Primvermeidungs-Satz ist es also nicht Teilmenge ihrer Vereinigung. Also lässt sich f so wählen, dass $f \notin P$ für alle $P \in (\operatorname{Ass} M)\backslash A$ und $f \in I$ also $f \in P$ für alle $P \in A$.

Betrachten wir nun die Lokalisierung nach dem von f erzeugten multiplikativen Untermonoid $\{f^n\}$. $N := \ker(M \to M[f^{-1}])$. Nach Proposition 1.2.4 (a) ist aber gerade $N = \{m \in M | f^n m = 0 \text{für ein } n \in \mathbb{N}\}$. Man sieht leicht, dass man in lezterem Ausdruck das f auch durch (f) ersetzen kann, also $N = H^0_{(f)}(M)$.

Jetzt wenden wir (a) für $I = (f)$ an. Nach Konstruktion von f gilt für alle $P \in \operatorname{Ass} M$, dass $(f) \subseteq P$ genau dann wenn $I \subseteq P$. Also ist $H^0_{(f)}(M)$ derselbe Schnitt wie $H^0_I(M)$.

zu c)

Nach Teil (a) haben wir eine Primärzerlegung von $H^0_I(M)$:

$H^0_I(M) = \bigcap_{i:P_i \notin A} M_i$

Wählen wir die Primärzerlegung $0 = \cap_i M_i$ irredundant, so ist auch die von $H^0_I(M)$ irredundant (könnte man ein M_i weglassen, so könnte man das auch in der Zerlegung der 0). Nach Satz 3.3.7 (ii) sind bei einer irredundanten Primärzerlegung die zu den

M_i gehörenden Primideale P_i genau die assoziierten Primideale von $M/H^0_I(M)$, also $\operatorname{Ass}(M/H^0_I(M)) = (\operatorname{Ass} M)\backslash A$.

Wir wenden Lemma 3.2.5 (ii) auf die kurze exakte Sequenz $0 \to H^0_I(M) \to M \to M/H^0_I(M) \to 0$ an und erhalten:

$\operatorname{Ass} H^0_I(M) \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} H^0_I(M) \cup \operatorname{Ass}(M/H^0_I(M))$.

Wie eben festgestellt, ist letztere Menge $(\operatorname{Ass} M)\backslash A$, also enthält wegen der zweiten Inklusion $\operatorname{Ass} H^0_I(M)$ mindestens A. Sei umgekehrt $Q \in \operatorname{Ass} H^0_I(M), Q = \operatorname{ann} m$. Per Definition von $H^0_I(M)$ ist $I^n m = 0$ für ein n. Also $I^n \subseteq Q$. Weil Q prim ist, folgt $I \subseteq Q$, also $Q \in A$. Damit ist $A = \operatorname{Ass} H^0_I(M)$ bewiesen.

Nun zum zweiten Teil der Aussage. Sei N ein Untermodul von M mit $\operatorname{Ass} N = A$ und $\operatorname{Ass}(M/N) = (\operatorname{Ass} M)\backslash A$.

Wir wählen f wie in Teil b). Nach b) reicht es also zu zeigen, dass $N = \ker(M \to M[f^{-1}])$.

„$\subseteq$“: Zu zeigen ist $f^n N = 0$. Sei $0 = \cap_i M_i$ eine minimale Primärzerlegung der 0 in N, also sind wegen $\operatorname{Ass} N = A$ die M_i P_i-primär mit $P_i \in A$. Nach Proposition 3.3.5 annihiliert eine Potenz $P_i^{n_i}$ von P_i den Modul N/M_i, was gleichbedeutend ist mit $P_i^{n_i} N \subseteq M_i$. Nach Konstruktion von f ist $f \in P_i \rightsquigarrow f^{n_i} \in P_i^{n_i} \rightsquigarrow f^{n_i} N \subseteq M_i$. Da dies für alle i gilt, folgt $f^n N = 0$ (wobei $n = \max_i n_i$).

„$\supseteq$“: Sei $m \in \ker(M \to M[f^{-1}])$, also $f^n m = 0$. Insbesondere $f^n m \equiv 0$ in M/N. Nach Satz 3.1.5. (ii) ist jeder Nullteiler von M/N in einem der Primideale aus $\operatorname{Ass}(M/N)$ enthalten, aber nach Konstruktion ist f in keinem dieser Primideale enthalten und, weil sie prim sind, f^n auch nicht. Also $m \equiv 0$, d.h. $m \in N$. □

Noch ein paar Worte zum Fall, dass I ein Primideal P ist. Dann ist $H^{(0)}_P(M)_P \subseteq M_p$ der eindeutig bestimmte größte Untermodul endlicher Länge. Diese Länge nennt man die Vielfachheit von P in M.

Bemerkung 4.4.4. P ist assoziiert zu M genau dann, wenn die Vielfacheit von P in M nicht Null ist.

Beweis. Sei P assoziiert zu M. Offensichtlich ist $P \in A$, d.h. nach (c) aus dem vorhergehenden Satz $P \in \operatorname{Ass} H^{(0)}_P(M)$. Mindestens ein $m \in H^{(0)}_P(M)$ wird also nur von P annihiliert und geht daher unter der Lokaliserung nicht auf 0, also ist der lokalisierte Modul nicht 0.

Umgekehrt existiere $m \in H^{(0)}_P(M)$ mit $rm \neq 0$ für alle $r \in R\backslash P$. Nach Konstruktion von $H^{(0)}_P(M)$ ist $P^n m = 0$ für ein n. Diese beiden Eigenschaften zeigen nach Proposition 3.3.5. (iii), dass Rm P-koprim ist, also $\{P\} = \operatorname{Ass} Rm \subseteq \operatorname{Ass} M$.

□

4.5 Eindeutigkeit

In diesem Abschnitt soll das Phänomen diskutiert werden, dass in einer Primärzerlegung die Terme, die zu eingebetteten Primidealen gehören, nicht eindeutig bestimmt sind.

Proposition 4.5.1. *Sei R ein lokaler noetherscher Ring und M ein endlich erzeugter R-Modul mit zwei assoziierten Primidealen, nämlich ein Primideal Q, das minimal über dem Annihilator von M ist, und das maximale Ideal P. Sei weiter $0 = M' \cap M''$ eine (minimale) Primärzerlegung mit M' Q-primär, M'' P-primär.*

Nach Satz 3.3.7. (iii) ist $M' = \ker(M \to M_Q)$ eindeutig bestimmt.

Im Gegensatz dazu kann M'' ein beliebiger Untermodul mit den Eigenschaften

a) $M'' \supseteq P^d M$ *für ein* d

b) $M'' \cap M' = 0$

sein, insbesondere ist $M'' = P^d M$ für jedes hinreichend große d eine mögliche Wahl.

Beweis. Erfülle M'' die beiden Eigenschaften. Wir zeigen mit Proposition 3.3.5. (c), dass M'' P-primär (M/M'' P-koprimär) ist. Der erste Satz der Proposition ist gerade (a). Es bleibt zu zeigen, dass alle Nullteiler auf M/M'' in P liegen. Sei also $rm \in M''$, $r \notin P$. Weil der Ring R lokal und P sein maximales Ideal ist, ist r eine Einheit und daher $m \in M''$. Modulo M'' bedeutet das, das r nur die Null auf die Null abbildet, d.h. r ist kein Nullteiler auf M/M''.

Zusammen mit Eigenschaft (b) folgt, dass tatsächlich eine Primärzerlegung vorliegt.

Zur letzten Bemerkung: (a) ist offensichtlich erfüllt. Für (b) nehmen wir eine Primärzerlegung $0 = M' \cap N''$, N'' P-primär. Dann ist $P^d M \subseteq N''$ für d hinreichend groß, also $M' \cap P^d M \subseteq M' \cap N'' = 0$. □

Man könnte vielleicht denken, dass sich das Problem vermeiden lässt, indem man M'' maximal wählt (unter denen, die (a) und (b) erfüllen). Jedoch liegt auch dann keine Eindeutigkeit vor; der Grund ist im Wesentlichen, dass das Komplement eines Vektorraums nicht eindeutig ist. Nehmen wir beispielsweise einen Körper k und die Lokalisierung $R = k[x]_{(x)}$ des Polynomrings in einer Variablen [für $k = \mathbb{C}$ sind das quasi alle rationalen Funktionen, die in 0 keine Singularität haben]. Sei $M = R \oplus R/(x)$, und sei e ein Erzeuger des zweiten Summanden. Dies ist ein Beispiel für den oben diskutierten Fall: Es ist $Q = (0)$, $P = (x)$ und $M' = Re$ (denn M' besteht aus den Elementen, die von einem Element außerhalb von Q auf 0 abgebildet werden, und das ist genau der zweite Summand, da R ein Integritätsbereich ist).

Bemerkung 4.5.2. M'' kann in dieser Situation ein beliebiger nichttrivialer Untermodul mit $M'' \cap Re = 0$ sein. Die maximalen M'' sind genau die Komplemente des zweiten Summands Re (in dem Sinne, dass sie zusammen den ganzen Modul aufspannen und der Schnitt 0 ist); dies sind wiederum genau die von Elementen der Form $(1, ue)$, $u \in k$ erzeugten Untermoduln.

Beweis. (eventuell unnötig umständlich)

Sei $M'' \subseteq M$ Untermodul mit $M'' \cap Re = 0$.

Die Untermoduln von $M = R^2/(0 \oplus (x))$ entsprechen bijektiv den Untermoduln $N \subseteq R^2$ mit $N \supseteq 0 \oplus (x)$ (via der kanonischen Projektion π). R ist ein Hauptidealring; ein Untermodul eines freien Moduls über einem Hauptidealring ist frei und von höchstens gleichem Rang, also ist auch M'' von höchstens 2 Elementen f_1, f_2 erzeugt.

Jedes Element $\neq 0$ von R lässt sich schreiben als Produkt von x^n und einer Einheit. Sei also $f_i = (x^{n_i}\varepsilon_i, u_i e), n_1 \leq n_2$. Dann ist $f_2 - x^{n_2-n_1}\frac{\varepsilon_2}{\varepsilon_1} f_1 = (0, (\frac{\varepsilon_2}{\varepsilon_1}u_1 - u_2)e)$. Wegen $M'' \cap Re = 0$ ist das 0, also liegt f_2 im Erzeugnis von f_1, d.h. $M'' = Rf_1$.

Nun können wir obige Behauptungen beweisen. Es ist $(x^{n_1+1})M = (x^{n_1+1}) \oplus 0 = (x)f_1 \subseteq Rf_1 = M''$, also erfüllt M'' Eigenschaft (a) und wir haben eine Primärzerlegung.

Die restlichen Aussagen sind in dieser Darstellung klar: M'' ist maximal genau dann, wenn $n_1 = 0$, also in der ersten Komponente von f_1 eine Einheit steht, und genau diese f_1 erzeugen Komplemente von Re. □

Da man je zwei solche Erzeuger $(1, ue), (1, u'e)$ durch einen Automorphismus ineinander überführen kann (nämlich $\varphi : (r, s) \mapsto (r, s+(u'-u)re)$), sind sie in gewisser Hinsicht ununterscheidbar und es gibt kein „ausgezeichnetes“ (nicht willkürlich ausgewähltes) M''.

Es gibt jedoch einige Spezialfälle, in denen bestimmte Teilräume ausgezeichnete Komplemente haben und es daher auch ausgezeichnete Primärzerlegungen gibt.

Bemerkung: Als Ring ist $R/(x) \cong k$: Sei $\varphi : k[x] \to k$ die Projektion auf den konstanten Term; dadurch werden Elemente außerhalb von (x) auf Einheiten abgebildet. Also gibt es nach der universellen Eigenschaft der Lokalisierung eine Fortsetzung $\varphi' : k[x]_{(x)} \to k$, $\varphi'(p/q) = \varphi(p)\varphi(q)^{-1}$. Es ist $\ker\varphi' = (x)$ und φ' surjektiv, also $k[x]_{(x)}/(x) \cong k$.

4.6 Geometrische Interpretation

Wir betrachten hier den Fall, dass k ein algebraisch abgeschlossener Körper und $I \subseteq S = k[x_1, \ldots, x_r]$ ein Ideal ist. Wir werden versuchen, einer Primärzerlegung von I ihre geometrische Bedeutung „anzusehen“. Sei $I = \cap_j I_j$ eine minimale Primärzerlegung. Dann ist $Z(I) = \cup_i Z(I_j)$ (Erinnerung: Je kleiner das Ideal, desto größer die Nullstellenmenge. Denn für kleinere Ideale muss die Nullstellenmenge ja *weniger* Bedingungen erfüllen). Wenn I ein radikales Ideal ist, ist jedes I_j ein Primideal, das minimal über I ist, und die Primärzerlegung ist einfach eine Darstellung von $Z(I)$ als Vereinigung irreduzibler algebraischer Mengen (algebraischer Varietäten) $Z(I_j)$. Im allgemeinen Fall kann man aber algebraisch noch weitere Informationen gewinnen. Wir können das hier nur informell tun; formalisiert wird das Ganze in der Theorie der *Garben*.

Sei jetzt $I \subseteq S = k[x, y]$ ein zum maximalen Ideal (x, y) primäres Ideal.

Bemerkung 4.6.1. In diesem Fall ist $Z(I)$ der Ursprung der affinen Ebene.

Beweis. Die Nullstellenmenge hängt nur vom Radikal eines Ideals ab ($f^d(x) = 0 \Leftrightarrow f(x) = 0$, da $f(x) \in k$ und k ein Körper ist).

Offensichtlich ist $Z((x, y)) = 0$. Wir zeigen, dass für ein P-primäres Ideal I gilt $P = \mathrm{rad}(I)$.

Nach Bemerkung 3.3.6 ist einerseits $P^n \subseteq I$, also $P \subseteq \mathrm{rad}(I)$.

Andererseits gilt, auch nach 3.3.6, $\forall r, s \in S : rs \in I, r \notin P \Rightarrow s \in I$. Da I ein echtes Ideal ist, folgt insbesondere für $s = 1$, dass $I \subseteq P$. Also $f \in \mathrm{rad}(I) \Rightarrow f^n \in I \Rightarrow f^n \in P \Rightarrow f \in P$. □

Welches geometrische Objekt X sollten wir beispielsweise mit dem (x, y)-primären Ideal (x^2, y) verbinden? Die Grundidee ist, dass X das geometrische Objekt sein sollte, welches den Koordinatenring S/I bestimmt. Sei

$$f = a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2 + a_6x^3 + \dots$$

ein Polynom. Aus der Kongruenzklasse von f modulo (x^2, y) können wir die Skalare $a_0 = f(0, 0)$ und $a_1 = \partial f/\partial x(0, 0)$ ablesen (das hängt nicht von der Wahl des Repräsentanten ab, da Elemente von (x^2, y) an diesen beiden Größen nichts ändern). Das bedeutet für X, dass wir, wenn wir eine Funktion auf X einschränken, den Wert der Funktion im Ursprung sehen sollte (also sollte der Ursprung in X sein), und wir sollten den Wert der ersten Ableitung der Funktion in x-Richtung im Ursprung „sehen“. Das zugehörige geometrische Objekt ist der Ursprung zusammen mit einem Tangentialvektor in x-Richtung im Ursprung.

Ganz ähnlich können wir $I = (x^2, xy, y^2) = (x, y)^2$ betrachten. In diesem Fall kann man an der Kongruenzklasse von f modulo I den Wert von f im Ursprung sowie die erste Ableitung von f in eine beliebige Richtung erkennen. Intuitiv kann man sich X als die „infinitesimale Umgebung erster Ordnung“ des Ursprungs vorstellen.

Allgemeiner sind für $I = (x, y)^n$ alle Ableitungen von f bis zur $n - 1$-ten sichtbar (modulo I), also ist das entsprechende geometrische Objekt die infinitesimale Umgebung $n - 1$-ter Ordnung.

Betrachten wir nun den höherdimensionalen Fall. Das Ideal (x) entspricht $Z((x))$, also der y-Achse. Modulo (x^2) sieht man die Werte von f auf der y-Achse und die Werte aller partiellen Ableitungen in x-Richtung auf der ganzen y-Achse. Das zugehörige Objekt ist die y-Achse zusammen mit „Tangentialvektoren“ in x-Richtung in jedem Punkt der y-Achse, d.h. die infinitesimale Umgebung erster Ordnung der y-Achse.

Ausgehend von diesen Ideen können wir versuchen, beliebige Primärzerlegungen zu interpretieren. Beispielsweise entspricht für das Ideal $I = (x^2, xy)$ die Primärzerlegung $I = (x) \cap (x^2, xy, y^2)$ der y-Achse zusammen mit der infinitesimalen Umgebung erster Ordnung des Ursprungs. Die Primärzerlegung ist hier nicht eindeutig: Es ist auch $I = (x) \cap (x^2, y)$. Das spiegelt sich geometrisch darin wieder, dass die Beschreibungen „man sieht den Wert von f auf der y-Achse und alle ersten Ableitungen im Ursprung“ und „man sieht den Wert von f auf der y-Achse und die erste Ableitung in x-Richtung im Ursprung“ gleichbedeutend sind, denn die erste Ableitung in y-Richtung im Ursprung sieht man ja ohnehin, weil man die ganze y-Achse sieht.

5 Ganze Abhängigkeit und der Nullstellensatz

Silke Möser

5.1 Einführung

Das Problem, Gleichungen zu lösen und etwas über die Lösungen auszusagen, ist fundamental in der kommutativen Algebra und der Mathematik überhaupt. Um dieses Ziel zu erreichen, ist es oft wichtig, die Lösung(en) von Polynomgleichungen in einer Variablen zu adjungieren: Gegeben ein Ring R und ein Polynom $p(x) \in R[x]$, kann der Ring $R[x]/(p)$ als das Ergebnis betrachtet werden, wenn man zu R die Nullstellen des Polynoms p so frei wie möglich adjungiert. Dabei ist die hinzugefügte Nullstelle das Bild von x. Die Beschäftigung mit Lokalisierung und der damit verwandten Primärzerlegung, mit der wir uns in den letzten beiden Kapiteln befasst haben, kann dabei aufgefasst werden als der Fall, in dem p ein lineares Polynom ist, dessen konstanter Term eine Einheit ist, das heißt zum Beispiel $p(x) = ax - 1$. In diesem Kapitel werden wir uns mit einem anderen wichtigen Fall beschäftigen, nämlich dem, dass p ein **monisches** Polynom ist.

Definition 5.1.1. Ein Polynom p heißt **monisch**, wenn der Leitkoeffizient 1 ist, also p von der Form $p(x) = x^n + r_1x^{n-1} + ... + r_n$ ist.

Die folgende Proposition werden wir später als Anwendung des Satzes von Cayley-Hamilton beweisen.

Proposition 5.1.2. *Sei R ein Ring und $J \subseteq R[x]$ ein Ideal im Polynomring in einer Variablen über R. Sei $S := R[x]/J$ und sei s das Bild von x in R.*

(a) S wird genau dann von höchstens n Elementen als R-Modul erzeugt, wenn J ein monisches Polynom mit Grad höchstens n enthält. In diesem Fall wird S von $1, s, ..., s^{n-1}$ erzeugt. Insbesondere ist S genau dann ein endlich erzeugter R-Modul, wenn J ein monisches Polynom enthält.

(b) S ist genau dann ein endlich erzeugter freier R-Modul, wenn J von einem monischen Polynom erzeugt wird. In diesem Fall hat S eine freie Basis der Form $1, s, ..., s^{n-1}$.

Definition 5.1.3. Ist S eine R-Algebra und $p(x)$ ein Polynom mit Koeffizienten in R, dann sagen wir, ein Element $s \in S$ **erfüllt** p, falls $p(s) = 0$ ist. Wir bezeichnen s als

ganz über R, falls s ein monisches Polynom mit Koeffizienten in R erfüllt. Die Gleichung $p(s) = 0$ wird dann **Gleichung ganzer Abhängigkeit** oder **ganze Gleichung** genannt. Sind alle Elemente von S ganz über R, so sagen wir, S ist ganz über R.

Der folgende Satz, den wir ebenfalls später als Anwendung von Cayley-Hamilton beweisen werden, ist das zweite wichtige Resultat, das diese Theorie interessant macht.

Satz 5.1.4. *Seien R ein Ring und S eine R-Algebra. Die Menge aller über R ganzen Elemente von S ist eine R-Unteralgebra von S. Insbesondere ist S ganz über R, falls S von Elementen erzeugt wird, die ganz sind über R.*

Definition 5.1.5. Sei S eine R-Algebra. Dann ist der **ganze Abschluss** oder die **Normalisierung** von R in S der Ring aller Elemente von S, die ganz über R sind.

Die wichtigsten Beispiele hiervon treten auf, wenn R ein Integritätsbereich und S sein Quotientenkörper ist. In diesem Fall nennt man die Unteralgebra der über R ganzen Elemente von S einfach Normalisierung von R. Ein Integritätsbereich, der gleich seiner eigenen Normalisierung ist, wird **normal** genannt.

Beispiele 5.1.6. *(1) Die Ringe $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i] \subset \mathbb{Q}[i]$ und $\mathbb{Z}[x]/(x^2+4) \cong \mathbb{Z}[2i] \subset \mathbb{Q}[i]$ sind interessant, da ihre Arithmetik der von $\mathbb{Z}$ ähnelt. Aber der Ring $\mathbb{Z}[i]$ ist „schöner" als $\mathbb{Z}[2i]$. Zum Beispiel gibt es in $\mathbb{Z}[i]$ eine eindeutige Primfaktorzerlegung, die es im zweiten Ring nicht gibt. Es ist zum Beispiel $2i \cdot 2i = -2 \cdot 2$. (Dies gilt auch in $\mathbb{Z}[i]$. Dort kann jedoch $2i = 2 \cdot i$ weiter zerlegt werden und i ist eine Einheit.) Wir werden später sehen, dass $\mathbb{Z}[i]$ die Normalisierung von $\mathbb{Z}[2i]$ ist.*

(2) Betrachten wir den Ring $R := \mathbb{Z}\left[\sqrt{5}\right] = \mathbb{Z}\left[1+\sqrt{5}\right] \subset \mathbb{Q}\left[\sqrt{5}\right]$ und den größeren Ring $S := \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{5}\right]$. Im ersten Ring sieht man wegen $\left(1+\sqrt{5}\right)\left(1-\sqrt{5}\right) = -4 = -2\cdot 2$, dass es in dort keine eindeutige Primfaktorzerlegung gibt. Denn $1+\sqrt{5}$, $1-\sqrt{5}$ und 2 können nicht weiter zerlegt werden und unterscheiden sich nicht durch Einheiten von R. Angenommen man kann $1+\sqrt{5}$ weiter zerlegen in $1+\sqrt{5} = ab$ mit $a, b \in \mathbb{Z}\left[\sqrt{5}\right]$, dann haben a und b eine Darstellung als $a = a_1 + a_2\sqrt{5}, b = b_1 + b_2\sqrt{5}$ mit $a_i, b_i \in \mathbb{Z}$ und es folgt $1+\sqrt{5} = ab = \left(a_1 + a_2\sqrt{5}\right)\left(b_1 + b_2\sqrt{5}\right) = (a_1b_1 + 5a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{5}$. Daraus folgt nun aber $a_1b_1 + 5a_2b_2 = a_1b_2 + a_2b_1 = 1$, was nur die Lösungen $\{a, b\} = \left\{1+\sqrt{5}, 1\right\}$ hat. Ebenso zeigt man, dass $1-\sqrt{5}$ und 2 keine weitere Zerlegung besitzen. Um zu sehen, dass sich $1+\sqrt{5}$ und $1-\sqrt{5}$ nicht durch Einheiten von R unterscheiden, betrachtet man den Quotienten $\frac{1+\sqrt{5}}{1-\sqrt{5}} = \frac{\left(1+\sqrt{5}\right)^2}{-4} = -\frac{1}{2}\left(3+\sqrt{5}\right) \notin R$, ebenso für die beiden anderen Fälle.

In S gilt jedoch $1+\sqrt{5} = 2\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)$ und $1-\sqrt{5} = 2\left(\frac{1}{2}-\frac{1}{2}\sqrt{5}\right) = 2\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}-\sqrt{5}\right)$. Außerdem gilt $\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)\left(\frac{1}{2}-\frac{1}{2}\sqrt{5}\right) = -1$, sodass sowohl $\frac{1}{2}+\frac{1}{2}\sqrt{5}$ als auch $\frac{1}{2}+\frac{1}{2}\sqrt{5}$ Einheiten sind. Die beiden Faktorisierung sind in S also im Wesentlichen gleich. Man kann zeigen, dass S eine eindeutige Zerlegung in Primfaktoren besitzt. Der Grund, dass S „besser" ist als R, ist wieder, dass S die Normalisierung von R ist.

Obwohl sogar normale Ringe im Allgemeinen keine eindeutige Primzahlfaktorzerlegung besitzen, werden wir später sehen, dass sie sie immer lokal besitzen, während dies für nicht-normale Ringe nicht gilt.

Definition 5.1.7. Sei K ein Zahlkörper, das heißt eine endliche Körpererweiterung von $\mathbb{Q}$. Dann nennt man die Menge aller Elemente von K, die monische Gleichungen mit Koeffizienten in $\mathbb{Z}$ erfüllen, den Ring der **ganzen algebraischen Zahlen** in K.

5.2 Der Satz von Cayley-Hamilton und Nakayamas Lemma

Der klassische Satz von Cayley-Hamilton sagt, dass eine lineare Abbildung auf einem endlich-dimensionalen Vektorraum von ihrem charakteristischen Polynom annihiliert wird. Hamilton hat dies 1853 für lineare Abbildungen im $\mathbb{R}^3$ bewiesen. Cayley erwähnte 1858 den allgemeinen Fall, scheint den Satz aber auch nur bis zu 3×3-Matrizen überprüft zu haben. Wir brauchen jedoch eine allgemeinere Version des Satzes.

Satz 5.2.1 (Cayley-Hamilton)**.** *Seien R ein Ring, $I \subseteq R$ ein Ideal und M ein von n Elementen erzeugter R-Modul. Ferner sei φ ein Endomorphismus von M. Falls*

$$\varphi(M) \subseteq IM,$$

dann gibt es ein monisches Polynom

$$p(x) = x^n + p_1 x^{n-1} + ... + p_n$$

mit $p_j \in I^j$ für alle j, sodass $p(\varphi) = 0$ als Endomorphismus von M.

Beweis. Seien $m_1, ..., m_n$ Erzeuger von M. Wegen $\varphi(M) \subseteq IM$ können wir $\varphi(m_i)$ als Linearkombination der m_j schreiben, indem wir Koeffizienten aus I benutzen:

$$\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j, \text{ mit } a_{ij} \in I$$

Wir können M als Modul über dem Polynomring $R[x]$ betrachten, indem wir x wie φ wirken lassen. Sei nun A die $n \times n$-Matrix mit den Einträgen a_{ij} und sei $\mathbf{1} = (\delta_{ij})$ die $n \times n$-Einheitsmatrix. Bezeichne m den Spaltenvektor mit den Einträgen m_j. Dann folgt aus den obigen Gleichungen

$$(x\mathbf{1} - A) \cdot m = 0.$$

Multipliziert man die linke Seite der Gleichung mit der Adjunkten von $x1 - A$, erhält man

$$[\det(x\mathbf{1} - A)]\,\mathbf{1} \cdot m = 0,$$

also (falls man dies zeilenweise betrachtet) $\det(x\mathbf{1} - A)\, m_i = 0$ für alle i; damit gilt, da jedes Element von M als Linearkombination der m_i geschrieben werden kann,

$$[\det(x\mathbf{1} - A)]\, M = 0.$$

Es folgt, dass das Polynom $p(x) = \det(x\mathbf{1} - A)$ die geforderte Eigenschaft $p(\varphi) = 0$ hat. Außerdem sieht man, dass der j-te Koeffizient p_j von p in I^j ist und dass das Polynom monisch ist. □

Folgerung 5.2.2. *Sei R ein Ring und M ein endlich erzeugter R-Modul.*

(a) Falls $\alpha : M \to M$ ein Epimorphismus (ein surjektiver Homomorphismus) von R-Moduln ist, dann ist α ein Isomorphismus.

(b) Falls $M \cong R^n$, dann ist jede n-elementige Teilmenge von M, die M erzeugt, eine freie Basis. Insbesondere ist der Rang n von M wohl definiert.

Beweis. (a) Wir können M als $R[t]$-Modul auffassen, indem wir t durch $tm := \alpha(m)$ auf M wirken lassen. Setzen wir $I = (t) \subset R[t]$, so gilt, da α surjektiv ist, $IM = M = \varphi(M)$ für $\varphi = id$ und wir können den Satz von Cayley-Hamilton anwenden. Damit bekommen wir ein Polynom p mit $p(id)M = (id^n + p_{n-1}id^{n-1} + ... + p_0)M = (id + p_{n-1} + ... + p_0)M = 0$, wobei alle $p_i \in I = (t)$ sind. Deshalb gibt es ein Polynom $q(t)$ mit $(1 - q(t)t)M = 0$, oder äquivalent $1 - q(\alpha)\alpha = 0$. Folglich ist $q(\alpha)$ ein Inverses zu α und α somit ein Isomorphismus.

(b) Eine Menge von n Erzeugern von M entspricht einer Surjektion $\beta : R^n \to M$, die die Basiselemente des R^n auf die gegebenen Erzeuger von M abbildet. Da M frei von Rang n ist, gibt es einen Isomorphismus $\gamma : M \to R^n$. Die Abbildung $\beta\gamma : M \to M$ ist dann eine Surjektion und deshalb ein Isomorphismus nach (a). Es folgt, dass auch $\beta = (\beta\gamma)\gamma^{-1}$ ein Isomorphismus ist. Demnach bilden die gegebenen Erzeuger eine freie Basis.

Um zu beweisen, dass der Rang eines endlich erzeugten freien Moduls wohl definiert ist, nehmen wir an $R^n \cong R^m$. Falls $n \neq m$ ist, nehmen wir $m < n$ an. Wir können eine Basis der Länge m zu einer Basis der Länge n erweitern, indem wir einige Elemente hinzufügen, die gleich 0 sind. Diese n Erzeuger bilden dann keine freie Basis mehr, was der ersten Aussage von Teil (b) wiederspricht. Also muss gelten $m = n$ und der Rang ist wohl definiert.

□

Bemerkung 5.2.3. Der Rang eines freien Moduls über einem nicht-kommutativen Ring ist im Allgemeinen **keine** wohl definierte Invariante.

Als nächstes verwenden wir diese Ergebnisse, um Proposition 5.1.2 zu beweisen.

Beweis von Proposition 5.1.2. (a) Die Potenzen von x erzeugen $R[x]$ als R-Modul, also wird S von ihren Bildern, den Potenzen von s, erzeugt. Angenommen J enthält ein monisches Polynom p vom Grad n. Jede Potenz s^d von s mit $d \geq n$ kann wegen $0 = s^{d-n}p(s) = s^d + r_1 s^{d-1} + ...$ als Linearkombination der kleineren Potenzen geschrieben werden. Also wird S von den ersten n Potenzen von s erzeugt.

Nehmen wir umgekehrt an, dass S als R-Modul von n Elementen erzeugt wird. Wir können die Multiplikation mit s als Endomorphismus des R-Moduls S betrachten. Mit $I = R$ gilt $\varphi(S) = sS \subseteq IS$ und mit dem Satz von Cayley-Hamilton erhält man ein monisches Polynom p von Grad n mit $p(s) = 0$. Für dieses Polynom gilt $p \in J$.

(b) Angenommen J wird von einem monischen Polynom p vom Grad n erzeugt. Wir wissen aus Teil (a), dass S von den ersten n Potenzen von s erzeugt wird. Um zu zeigen, dass diese auch linear unabhängig sind, nehmen wir an, es gibt Elemente $a_i \in R$ mit $\sum_{i=0}^{n-1} a_i s^i = 0$. Definiert man nun $q(x) = \sum_{i=0}^{n-1} a_i x^i$, so gilt $q(s) = 0$ und damit $q \in J = (p)$. Da p monisch ist, hat jedes Vielfache von p, das nicht 0 ist, Grad mindestens n. Es muss also $q = 0$ gelten. Dies zeigt, dass S ein freier R-Modul ist, mit den ersten n Potenzen von s als freie Basis.

Sei nun umgekehrt S ein freier R-Modul und n der Rang von S. Da S als R-Modul von n Elementen erzeugt werden kann, folgt mit Teil (a), dass es in J ein monisches Polynom p vom Grad n gibt. Außerdem folgt aus Teil (a), dass S als R-Modul von den Elementen $1, s, ..., s^{n-1}$ erzeugt wird. Da S frei vom Rang n ist, zeigt Folgerung 5.2.2 (b), dass diese Potenzen eine Basis von S als R-Modul bilden.

Um zu zeigen, dass J von p erzeugt wird, sei $f \in J$ ein beliebiges Polynom und q sein Rest bei Division durch p. Dann ist $q \in J$ und $deg(q) < n$. Man kann q wie oben als lineare Relation zwischen den ersten n Potenzen von s auffassen. Da diese jedoch eine freie Basis von S bilden, folgt $q = 0$. Also war f wie behauptet ein Vielfaches von p.

□

Definition 5.2.4. Wir sagen, dass eine R-Algebra S, die als R-Modul endlich erzeugt ist, endlich über R ist.

Diese Eigenschaft ist stärker, als ganz zu sein. Das folgende Resultat erweitert die in Proposition 5.1.2 aufgezeigte Verbindung auf Ringe, die von mehr als einem Element erzeugt werden.

Folgerung 5.2.5. *Eine R-Algebra S ist genau dann endlich über R, wenn S als R-Algebra von endlich vielen ganzen Elementen erzeugt wird.*

Beweis. Nehmen wir zunächst an, dass S endlich über R ist. Für $s \in S$ ist die Multiplikation mit s ein Endomorphismus von S und der Satz von Cayley-Hamilton zeigt, dass s eine ganze Gleichung erfüllt.

Die Umkehrung zeigen wir durch Induktion. Angenommen S wird von t Elementen erzeugt. Sei nun S' die Unteralgebra von S, die von den ersten $t-1$ Erzeugern erzeugt wird. Nach Induktionsvoraussetzung können wir annehmen, dass S' endlich über R ist. Angenommen S' wird als R-Modul von einer endlichen Menge von Elementen $\{s_i\}$ erzeugt. Der letzte Erzeuger, s, ist ganz über R und deshalb auch ganz über S'. Nach Proposition 5.1.2 gibt es eine endiche Menge von Erzeugern von S als S'-Modul, diese seien $\{t_j\}$. Dann wird S als R-Modul von den Produkten $s_i t_j$ erzeugt. □

Folgerung 5.2.6. *Ist S eine R-Algebra und $s \in S$, so ist s genau dann ganz über R, wenn es einen S-Modul N und einen endlich erzeugten R-Untermodul $M \subseteq N$ gibt, der von keinem von 0 verschiedenen Element von S annihiliert wird, sodass $sM \subseteq M$. Insbesondere ist s genau dann ganz, wenn $R[s]$ ein endlich erzeugter R-Modul ist.*

Beweis. Angenommen s ist ganz über R. Setze $N := S$. Nach Proposition 5.1.2 ist $M := R[s] \subseteq S$ ein endlich erzeugter R-Modul.

Wir können die Multiplikation mit s als Endomorphismus von M betrachten. Mit dem Satz von Cayley-Hamilton erhalten wir ein monisches Polynom p mit Koeffizienten in R, für das $p(s)\,M = 0$ gilt. Aus unserer Annahme, dass M von keinem von 0 verschiedenen Element annihiliert wird, folgt $p(s) = 0$ als Element von S. Damit ist s ganz wie behauptet.

Die letzte Behauptung folgt, da $1 \in R$ von keinem von 0 verschiedenen Element von S annihiliert wird. □

Nun wollen wir auch Theorem 5.1.4 beweisen. Es wäre nahe liegend dies zu beweisen, indem wir Gleichungen aufstellen, die von zwei ganzen Elementen erfüllt werden und daraus die Gleichungen folgern, die von ihrer Summe und ihrem Produkt erfüllt werden. Dies werden wir im Prinzip auch tun, die benötigten Polynome sind allerdings im Allgemeinen sehr kompliziert. Der Satz von Cayley-Hamilton gibt sie implizit.

Beweis von Satz 5.1.4. Seien $s, s' \in S$ ganz über R. Wir müssen zeigen, dass $s + s'$ und ss' ganz über R sind. Definiere $M := R[s], M' := R[s'] \subseteq S$. Nach Proposition 5.1.2 sind M und M' endlich erzeugte Moduln. Wir definieren MM' als den von allen paarweisen Produkten von Elementen von M und M' aufgespannte Modul. Da es dafür ausreichen würde, paarweise Produkte der Erzeuger von M und M' zu benutzen, ist auch MM' endlich erzeugt. Es gilt

$$\begin{aligned} ss'MM' &= sMs'M' \subseteq MM' \\ (s+s')\,MM' &\subseteq sMM' + s'MM' \subseteq MM' + MM' = MM', \end{aligned}$$

also sind nach Folgerung 5.2.6 $s + s'$ und ss' ganz. Dies zeigt, dass die ganzen Elemente einen Unterring bilden. □

Als nächstes betrachten wir zwei weitere Konsequenzen des Satzes von Cayley-Hamilton, die in den folgenden beiden Kapiteln von großer Bedeutung sein werden.

Folgerung 5.2.7. *Ist M ein endlich erzeugter R-Modul und I ein Ideal in R mit $IM = M$, dann gibt es ein Element $r \in I$ mit $(1 - r)\,M = 0$, das heißt r wirkt auf M wie die Identität.*

Beweis. Wende Satz 5.2.1 auf $\varphi = id$ an. Aus $p(id)\,M = 0$ wird dann

$$(1 + p_1 + ... + p_n)\,M = 0,$$

mit p_j in $I^j \subseteq I$. Wir können also $r = -(p_1 + ... + p_n)$ wählen. □

Das nächste Resultat, genannt Nakayamas Lemma, ist außerordentlich nützlich für die Theorie von lokalen Ringen. Um es in seiner allgemeinsten Form formulieren zu können, benutzen wir die folgende Definition.

Definition 5.2.8. Das **Jacobson-Radikal** eines Ringes R ist der Schnitt aller maximalen Ideale von R.

Folgerung 5.2.9 (Nakayamas Lemma)**.** *Sei I ein Ideal, das im Jacobson Radikal eines Rings R enthalten ist und sei M ein endlich erzeugter R-Modul.*

(a) Falls $IM = M$, so gilt $M = 0$.

(b) Falls die Bilder von $m_1, ..., m_n \in M$ in M/IM diesen als R-Modul erzeugen, so wird M von $m_1, ..., m_n$ als R-Modul erzeugt.

Beweis. (a) Wenden wir Folgerung 5.2.7 an, so erhalten wir $r \in I$ mit $(1-r)M = 0$. Da r in jedem maximalen Ideal enthalten ist, ist $1-r$ in keinem maximalen Ideal enthalten. (Sonst wäre auch $1 = r + (1-r)$ enthalten.) Also ist $1-r$ eine Einheit. Wegen $(1-r)M = 0$ folgt $M = 0$.

(b) Sei $N = M/\left(\sum_i Rm_i\right)$. Es gilt $N/IN = M/\left(IM + \left(\sum_i Rm_i\right)\right) = M/M = 0$, also $IN = N$. Wir können also Teil (a) anwenden und erhalten $N = 0$, also $M = \sum_i Rm_i$. □

5.3 Normale Integritätsbereiche und der Normalisierungsprozess

Wir haben schon angedeutet, dass es einen Zusammenhang zwischen Normalität und eindeutiger Primfaktorzerlegung gibt. Die folgende Proposition zeigt diesen Zusammenhang.

Proposition 5.3.1. *Sei R ein Ring. Ist R faktoriell, so ist R normal.*

Beweis. Sei R faktoriell und $\frac{r}{s}$ mit $r, s \in R$ ein Bruch, der ganz über R ist. Wir können annehmen, dass r und s teilerfremd sind, und wollen zeigen, dass $\frac{r}{s} \in R$. Ist

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + ... + a_0 = 0$$

die von $\frac{r}{s}$ erfüllte ganze Gleichung, dann folgt nach Muliplikation mit s^n

$$r^n + sa_{n-1}r^{n-1} + ... = r^n + s(a_{n-1}r^{n-1} + ...) = 0$$

Also ist r^n durch s teilbar. Da aber r und s teilerfremd sind, muss s also eine Einheit von R sein. Demnach muss $\frac{r}{s} \in R$ sein. □

Proposition 5.3.1 zeigt sofort, dass der Ring $\mathbb{Z}$ normal ist. Ist K ein Körper, so sind $K[x_1, ..., x_r]$ und $\mathbb{Z}[x_1, ..., x_r]$ faktoriell und somit normal.

Falls $R \subseteq S$ Ringe sind und $f(x) \in R[x]$ ein monisches Polynom mit einer Nullstelle in S, dann ist diese Nullstelle nach Definition ganz über R. Eine Nullstelle α zu besitzen ist aber dasselbe wie einen linearen Faktor $(x-\alpha)$ zu besitzen. Das folgende Resultat zeigt, dass etwas ähnliches für jeden Faktor gilt, ob linear oder nicht. Da $\mathbb{Z}$ normal ist, wie wir schon bewiesen haben, verallgemeinert es die Aussage, dass ein monisches Polynom mit Koeffizienten in $\mathbb{Z}$, das irreduzibel in $\mathbb{Z}$ ist, auch irreduzibel in $\mathbb{Q}$ ist.

Proposition 5.3.2. *Seien $R \subseteq S$ Ringe und $f \in R[x]$ ein monisches Polynom. Falls f in $S[x]$ faktorisiert werden kann als $f = gh$, mit g und h monisch, so sind die Koeffizienten von g und h ganz über R.*

Beweis. Adjungiert man eine Nullstelle α_1 von g zu S, sieht man durch Division in $S[\alpha_1] \cong S[x]/(g)$, dass g faktorisiert werden kann zu $g = (x - \alpha_1)g_1$, wobei der Grad von g_1 um 1 kleiner ist als der Grad von g. Setzt man dies induktiv fort, erhält man eine Erweiterung T von S und Elemente α_i und β_i von T, sodass $g = \prod_i (x - \alpha_i)$ und $h = \prod_i (x - \beta_i)$ in $T[x]$. Da alle α_i und β_i Nullstellen des monischen Polynoms f sind, ist der Unterring T' von T, der als R-Algebra von den Elementen α_i, β_i erzeugt wird, ganz über R. Da die Koeffizienten von g und h elementarsymmetrische Funktionen in den α_i bzw. β_i sind, sind auch sie ganz über R. □

Bemerkung 5.3.3. Ist R ein Ring und $f = gh \in R[x]$ eine Faktorisierung eines monischen Polynoms in nicht-monische Polynome, so sind, da f monisch ist, die Leitkoeffizienten von g und h zueinander inverse Einheiten von S. Multipliziert man g und h mit dem Leitkoeffizienten des jeweils anderen Polynoms, erhält man eine Faktorisierung von f in zwei monische Polynome, auf die man Proposition 5.3.2 anwenden kann.

Als Folgerung erhalten wir eine schwache Umkehrung von Proposition 5.3.1, die die Verbindung zwischen Normalität und eindeutiger Primfaktorzerlegung weiter vertieft.

Folgerung 5.3.4. *Ist R ein normaler Integritätsbereich, so ist jedes monische, irreduzible Polynom in $R[x]$ prim.*

Beweis. Sei f ein monisches, irreduzibles Polynom und Q der Quotientenkörper von R. Nach Proposition 5.3.2 bleibt f auch in Q irreduzibel. Da Q faktoriell ist, ist $P := fQ[x]$ prim. Da $R[x]/(f)$ frei über R ist, ist die (kanonische) Abbildung $R[x]/(f) \to Q \otimes_R R[x]/(f) \cong Q[x]/P$ ein Monomorphismus. Also ist (f) prim in $R[x]$. □

Normalisierung kommutiert mit Lokalisierung.

Proposition 5.3.5. *Seien $R \subseteq S$ Ringe und U eine multiplikativ abgeschlossene Teilmenge von R. Ist S' der ganze Abschluss von R in S, so ist $S'[U^{-1}]$ der ganze Abschluss von $R[U^{-1}]$ in $S[U^{-1}]$.*

Beweis. Ein Element von S, das ganz über R ist, ist sicherlich ganz über $R[U^{-1}]$. Also ist $S'[U^{-1}]$ ganz über $R[U^{-1}]$.

Für die andere Inklusion müssen wir zeigen, dass, falls $\frac{s}{u} \in S[U^{-1}]$ ganz über $R[U^{-1}]$ ist, es ein Element $v \in U$ gibt, sodass sv ganz ist über R. Ist

$$\left(\frac{s}{u}\right)^n + \left(\frac{r_1}{u_1}\right)\left(\frac{s}{u}\right)^{n-1} + ... = 0$$

eine ganze Gleichung für $\frac{s}{u}$, so können wir diese mit $(uu_1...u_n)^n$ multiplizieren und erhalten

$$(su_1...u_n)^n + r_1(uu_2...u_n)(su_1...u_n)^{n-1} + ... = 0.$$

Dies ist eine ganze Gleichung für $suu_1...u_n$. Wir können also $v := uu_1...u_n$ wählen. □

Ist R ein noetherscher Integritätsring, so könnte man hoffen, dass der ganze Abschluss S von R (im Quotientenkörper oder einer endlichen Körpererweiterung) wieder noethersch ist. Ist S als R-Algebra endlich erzeugt, so ist dies auch richtig nach Folgerung 5.2.5. Im Allgemeinen kann eine über einem Ring R ganze Algebra aber eine unendliche Vereinigung endlicher Algebren sein. Falls diese Vereinigung wirklich unendlich ist, muss S nicht noethersch sein. Im Fall von affinen Ringen jedoch gilt diese Aussage immer.

Satz 5.3.6 (Emmy Noether)**.** *Ist R ein endlich erzeugter Integritätsbereich über einem Körper oder über $\mathbb{Z}$, und L eine endliche Körpererweiterung des Quotientenkörpers von R, so ist der ganze Abschluss von R in L ein endlich erzeugter R-Modul.*

Beweis. Siehe [4], Kapitel 13 □

6 Quadriken

Angela Armakola, Alexandra Fischer

6.1 Einleitung

In diesem Vortrag beschäftigen wir uns mit Quadriken im Zusammenhang mit projektiven Räumen. Wir beginnen mit einigen Definitionen und Beispielen von Quadriken und sehen dann anhand des Satzes von Witt, dass man mit Quadriken Automorphismen von Teilräumen auf Vektorräume erhält.

6.2 Der projektive Raum und Quadriken

6.2.1 Anmerkung

In der Renaissance wurde die Malerei wesentlich durch die Entdeckung der Zentralsperspektive, also der geometrischen Konstruktion der Raumtiefe mithilfe eines Fluchtliniensystems, geprägt. Der Maler musste also mathematische Regeln beachten, um auf einer Leinwand (einer zweidimensionalen Fläche) ein dreidimensionales Bild malen zu können. Diese legten fest, dass der Horizont waagerecht auf Augenhöhe des Betrachters liegt. Um einem Bild räumliche Tiefe zu verleihen, laufen all seine parallel zum Erdboden verlaufenden Tiefenlinien auf einen Fluchtpunkt zu, der auf der Horizontlinie liegt. Damit wird die Darstellung des Raumes durch geometrische Regeln festgelegt, sodass ein einheitlicher Raumeindruck entsteht. In der Entdeckung der Zentralperspektive kann man also den Beginn der projektiven Geometrie sehen.

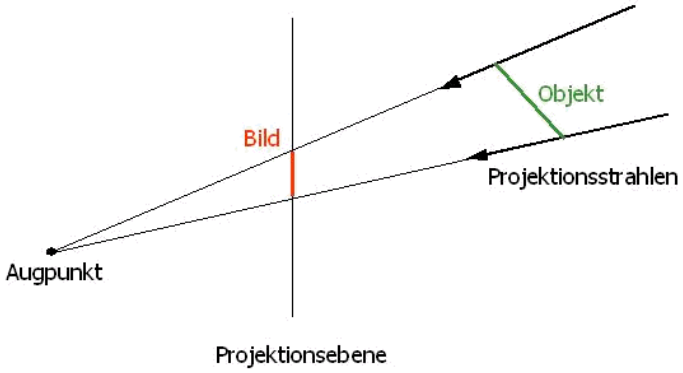
6.2.2 Der projektive Raum

Definition 6.2.1. Sei E ein endlichdimensionaler Vektorraum über einem Körper K mit $dim(E) = n+1$. Der *n-dimensionale projektive Raum* P^n ist die Menge aller durch den Ursprung 0 von E laufenden Geraden (Menge der eindimensionalen Unterräume).

Man bezeichnet die Elemente von P^n als *Punkte*.

Bemerkung 6.2.2. Man kann manche Begriffe der Theorie der Vektorräume auch als Begriffe der projektiven Geometrie interpretieren: Eine projektive Gerade P^1 ist also ein eindimensionaler projektiver Raum, die projektive Ebene P^2 ein zweidimensionaler projektiver Raum, eine projektive Hyperebene $H \subset P^n$ ist ein 1-kodimensionaler projektiver $(n-1)$-dimensionaler Unterraum.

Bemerkung 6.2.3. Jede affine Ebene lässt sich zu einer projektiven Ebene erweitern, indem man neue Punkte (Fernpunkte) hinzufügt. Zu jeder Klasse paralleler Geraden gehört genau ein solcher Fernpunkt oder unendlich ferner Punkt. (Er kann mit der Richtung dieser Geraden oder auch mit der Geradenmenge selbst identifiziert werden.) Der unendlich ferne Punkt wird als Schnittpunkt von je zwei parallelen Geraden dieser Richtung festgelegt.
Die Gesamtheit aller unendlich fernen Punkte einer Ebene, also alle in ihr enthaltenen Geradenrichtungen, bildet die unendlich ferne Gerade der Ebene.



6.2.3 Quadriken

Definition 6.2.4. Eine *Bilinearform* ist eine Abbildung $Q_0 : V \times V \to K$ mit folgenden Eigenschaften: Für alle $v, v', w, w' \in V$ und $\lambda, \mu \in K$ gilt:

(i) $Q_0(v + v', w) = Q_0(v, w) + Q_0(v', w), Q_0(\lambda v, w) = \lambda Q_0(v, w)$ und

(ii) $Q_0(v, w + w') = Q_0(v, w) + Q_0(v, w'), Q_0(v, \mu w) = \mu Q_0(v, w)$.

Eine Bilinearform heisst *symmetrisch*, falls für alle $v \in V$, $w \in V$ gilt:

$$Q_0(v, w) = Q_0(w, v).$$

Definition 6.2.5. Eine Abbildung $Q : V \to K$, welche durch $Q(v) = Q_0(v, v)$ definiert ist, nennt man die zur symmetrischen Bilinearform Q_0 assoziierte *quadratische Form*. Die zu Q_0 assoziierte lineare Abbildung $Q^* : VtoV^*$, wobei V^* der Dualraum ist, ist gegeben durch

$$Q^* : x \mapsto (y \mapsto Q_0(x, y)).$$

Ist Q^* injektiv folgt, dass Q_0 oder Q nicht ausgeartet (regulär) ist, so dass für alle $y \in V$ aus $Q_0(x, y) = 0$, dann $x = 0$.
Man erhält somit also eine bijektive Entsprechung zwischen quadratischen Formen und symmetrischen Bilinearformen für $char(K) \neq 2$.

Definition 6.2.6 (Quadrik (quadratische Hyperfläche))**.** Eine Quadrik ist gegeben als Nullstellenmenge eines homogenen quadratischen Polynoms, welche die zur symmetrischen Bilinearform Q_0 assoziierte quadratische Form ist.

Bemerkung 6.2.7. Weil die quadratische Form $Q(v)$ durch die Restriktion der Bilinearform $Q_0(v,v)$ auf die Diagonale definiert ist, ist die Ableitung dQ in irgendeinem Punkt v genau die lineare Form $2Q_0(v,\cdot)$, das ist $2Q^*(v)$. Folglich gilt für irgendeinen Punkt $[v] \in Q$:

(i) Falls $Q^*(v) \neq 0 \in V^*$, dann ist die Quadrik $Q \subset P^n$ glatt in $[v]$, oder

(ii) falls $Q^*(v) = 0$, dann ist Q singulär in $[v]$.

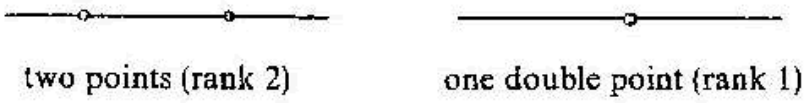
Definition 6.2.8 (Rang einer Quadrik)**.** Eine Quadrik Q kann mit einer geschickt gewählten Basis in folgender Form geschrieben werden:

$$Q(x) = x_0^2 + x_1^2 + \ldots + x_k^2.$$

Die Quadrik Q hat damit den Rang $rk(Q) = k + 1$. Eine Quadrik heisst glatt, wenn $rk(Q) = n + 1$, wenn also die zugehörige Bilinearform Q_0 nicht degeneriert ist.

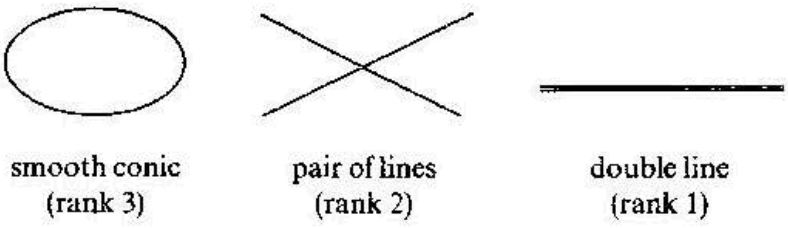
Beispiel 6.2.9. In P^1 gibt es zwei Typen von Quadriken:

- Zwei Punkte (Rang 2)
- Einen Doppelpunkt (Rang 1)



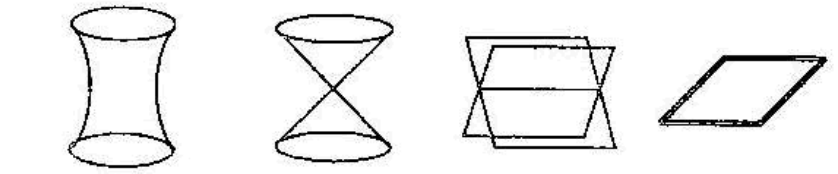
Beispiel 6.2.10. In P^2 gibt es drei Typen von Quadriken:

- Ellipse (Rang 3)
- Geradenpaar (Rang 2)
- doppelte Gerade (Rang 1)



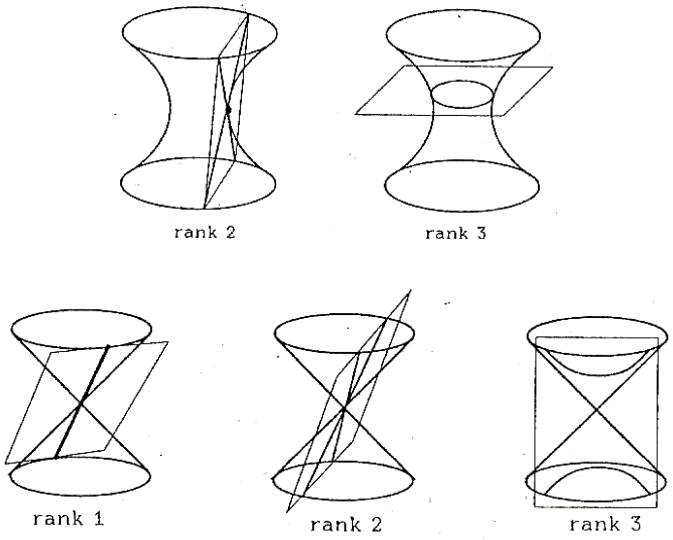
Beispiel 6.2.11. In P^3 gibt es vier Typen von Quadriken:

- einschaliges Hyperboloid (Rang 4)
- asymptotischer Kegel (Rang 3)
- zwei Ebenen (Rang 2)
- doppelte Ebene (Rang 1)



Kegelschnitte

Schneidet man eine Quadrik mit einer Hyperebene H, so erhält man wieder eine Quadrik. Für den Rang von $Q' = Q \cap H$ gilt: $rk(Q) - 2 \leq rk(Q') \leq rk(Q)$.
Ist die Hyperebene eine Tangentialebene in einem glatten Punkt $x \in Q$, so ist $Q' = (Q \cap T_xQ) \subset T_xQ \cong P^{n-1}$ mit $rk(Q') = rk(Q) - 2$.



6.2.4 Quadriken als Bilder von Abbildungen

Jede glatte Quadrik lässt sich als Bild einer Abbildung darstellen. So wäre eine Ellipse das Bild unter der Veronese Abbildung:

$$v_2 : P^1 \to P^2 : [\alpha, \beta] \longmapsto [\alpha^2, 2\alpha\beta, \beta^2] \ ,$$

d.h. sie bildet die homogenen Koordinaten eines Punktes $p \in P^1$ auf die homogenen Koordinaten der Quadrik $p^2 \subset P^2$.

Umgekehrt lässt sich die Ellipse mittels einer Projektion

$$\pi : P^2 \to P^1 : x \longmapsto T_xQ \cap P^1$$

in die Ebene einbetten. Betrachtet man das zugehörige Bild, wird deutlich, dass (die Ellipse) $Q \subset P^2$ isomorph zu P^1 ist. Der unendlich ferne Punkt, welcher P^1 auszeichnet, ist die Schnittmenge mit derjenigen Tangente, die parallel zu P^1 verläuft. Somit ist π ein Isomorphismus.

Analog dazu kann man eine glatte Quadrik in P^3 (Einschaliges Hyperboloid) als Bild der Segre-Abbildung

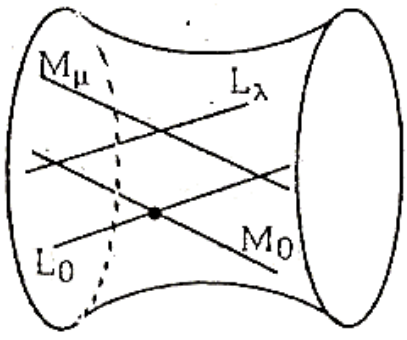
$$\sigma_{1,1} : P^1 \times P^1 \to P^3 : [x_0, x_1] \times [y_0, y_1] \longmapsto [x_0y_0, x_0y_1, y_0x_1, x_1y_1]$$

darstellen.

Desweiteren ergeben die Fasern zweier Projektionen $\pi_i : Q \cong P^1 \times P^1 \to P^1$ Geraden in P^3, sodass die Quadrik zwei Familien von Geraden aufweist, in jedem Punkt $x \in Q$ schneiden sich jeweils genau zwei Geraden, die jeweils einer der beiden Familien von Geraden angehören. Nach welchen Regeln diese Geraden verlaufen und wie der Isomorphismus $Q \cong P^1 \times P^1$ aussieht, läßt sich mit Hilfe der vorangegangen Überlegungen herleiten:

Wie wir vorher gesehen haben, ist der Schnitt einer Quadrik mit der Tangentialebene in irgendeinem (glatten) Punkt, wieder eine Quadrik, welche den Rang $rk(Q \cap T_xQ) = rk(Q) - 2$ hat. Im vorliegenden Fall bedeutet dies, dass für jedes x, der Schnitt $Q \cap T_xQ$ die Vereinigung zweier verschiedener Geraden ist. Da jede Gerade, welche auf Q liegt und den Punkt x enthält, in dieser Schnittmenge liegt, sieht man nochmals, dass sich in jedem Punkt von Q genau zwei Geraden schneiden.

Sei x_0 ein fester Punkt von Q und seien L_0 und M_0 die beiden eindeutigen Geraden durch x_0. Jeden Punkt $\lambda \in L_0$ schneide eine Gerade in M_λ, eine andere Gerade in Q, sodass andererseits jeder Punkt $\mu \in M_0$ von einer Gerade $L_\mu \subset Q$ geschnitten wird.



Insofern: Q enthält also zwei Familien von Geraden, die jeweils durch P^1 parametrisiert werden. Für die Familien von Geraden L_μ und M_λ gilt:

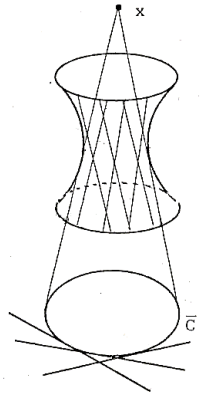
(i) Die Geraden von L_μ bzw. M_λ sind disjunkt,

(ii) keine Gerade kann gleichzeitig zu beiden Geradenfamilien gehören, und

(iii) jede Gerade L_μ muss jede Gerade M_λ treffen, da die Gerade $T_\lambda Q \cap T_\mu Q$ Q in zwei Punkten schneidet, x_0 und einem Punkt von $L_\mu \cap M_\lambda$.

Jeder Punkt aus Q lässt sich also als Schnittpunkt von zwei Geraden auffassen, die jeweils einer der beiden Familien angehören: Da die beiden Geraden L und M durch den Punkt x aus der Schnittmenge von Q und einer Ebene bestehen, muss eine der beiden Geraden L_0 treffen und daher von der Form M_λ sein, und eine der beiden Geraden muss M_0 treffen und daher von der Form L_μ sein. So erhält man einen Isomorphismus von Q mit $L_0 \times M_0 \cong P^1 \times P^1$.

Eine andere Möglichkeit eine glatte Quadrik $Q \subset P^3$ darzustellen, ergibt sich aus der Projektion von Q auf eine Ebene durch einen Punkt $x \notin Q$. Die meisten Geraden durch x schneiden Q zweimal, sodass man Q als zweiblättrige Überlagerung von P^2 ansehen kann.
Die Menge der Punkte $p \in Q$, für welche die Gerade $\overline{px}$ tangential zu Q verläuft, also $x \in T_pQ$, ist $C = Q \cap H$, wobei H eine zu P^2 parallele Ebene ist. Somit stellt π_x Q als doppelte Überlagerung der Ebene P^2 dar, verzweigt entlang der konischen Kurve $\overline{C} \subset P^2$. Man sieht nochmals: Jede Gerade (der beiden Familien von Geraden in Q) schneidet C genau einmal. Das Bild dieser Gerade trifft $\overline{C}$ einmal, ist also eine Tangente an $\overline{C}$.



6.2.5 Warum betrachtet man Quadriken in projektiven Räumen?

Betrachte eine Quadrik Q in $\mathbb{R}^3$, z.B. einen asymptotischen Kegel. Dann ist der Schnitt des asymptotischen Kegels mit einer Hyperebene wieder eine Quadrik (im zweidimensionalen Raum). Es ergeben sich folgende Kegelschnitte:

- Ellipse
- Hyperbel

- Parabel

Der Vorteil der projektiven Geometrie liegt nun darin, dass alle drei Kegelschnitte projektiv äquivalent sind, d.h. es reicht aus, eines der drei Objekte zu betrachten, nämlich die Ellipse.

6.3 Der Satz von Witt

Sei E ein endlichdimensionaler metrischer Vektorraum mit symmetrischer Bilinearform über einem kommutativen Körper K mit $char(K) \neq 2$, d.h. $1 + 1 \neq 0$.

Satz 6.3.1 (Satz von Witt (spätere Version des Satzes)). *Jeder Isomorphismus α eines Unterraumes $A \subseteq E$ auf einen Unterraum $B \subseteq E$ läßt sich zu einem Automorphismus von E fortsetzen.*

Vorab ein paar Definitionen

Definition 6.3.2. Seien U und V Untervektorräume von E. Dann ist die orthogonale Summe $U \perp V$ das kartesische Produkt $U \times V$ mit: Für $u \in U$, $u' \in U$ und $v \in V$, $v' \in V$, $\lambda \in K$ gilt:

(i) $(u, v) + (u', v') = (u + v, u' + v')$

(ii) $\lambda(u, v) = (\lambda u, \lambda v)$

Beschreibe die Matrix A eine quadratische Form F auf U und die Matrix B eine quadratische Form G auf V, dann ist die quadratische Form $F \perp G$ auf $U \perp V$ durch die diagonale Blockmatrix $\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$ gegeben.

Definition 6.3.3. Ein Unterraum heißt *nicht ausgeartet*, falls das Radikal $rad(U) := U \cap U^{\perp}$ gleich 0 ist. Dazu äquivalent ist $det(A) \neq 0$, wobei A die Gram-Matrix der Bilinearform ist

Definition 6.3.4. Zwei metrische Vektorräume A und B heissen *kongruent* oder *isomorph*, wenn sie sich linear so aufeinander abbilden lassen, dass dabei alle Skalarprodukte invariant sind.

Satz 6.3.5 (Wittscher Kürzungssatz:). *Seien f, f', g, h reguläre quadratische Formen, ferner sei*

$$f \cong f', \quad f \perp g \ \cong \ f' \perp h.$$

Dann ist $g \cong h$.

Rückführung des Wittschen Kürzungssatz auf den Satz von Witt :

Die quadratischen Formen f, f', g, h seien auf den metrischen Vektorräumen A, B, C, D definert, d.h: $f : A \to K$, $f' : B \to K$, $C :\to K$, $h : D \to K$.
Dann gilt:
$A \cong B$, $A \perp C \cong B \perp D$. Sei weiterhin o.B.d.A. $E = A \perp C = B \perp D$. Daraus kann man folgern, dass C bzw. D das orthogonale Komplement zu A bzw. B ist. Dann lässt sich nach dem Satz von Witt der Isomorphismus $\alpha : A \to B$ zu einem Automorphismus $\gamma : E \to E$ fortsetzen mit $\gamma(C) = D$.

Vom Wittschen Kürzungssatz zum Wittschen Satz:

Der Wittsche Kürzungssatz ist ein Sonderfall des Wittschen Satzes für nicht ausgeartete Untervektorräume A und B.

Seien A und B nicht ausgeartet, dann sind es auch die orthogonalen Komplemente $A^\perp$ und $B^\perp$. Sei α ein Isomorphismus und sei Q eine quadratische Form auf E, dann sei $Q|_A = f$, $Q|_B = f'$, $Q|_C = g$, $Q|_D = h$.

Dann gilt nach Voraussetzung : $Q \cong f \perp g \cong f' \perp h$, und vermöge α ist $f \cong f'$.

Nach dem Wittschen Kürzungssatz ist $g \cong h$, daraus folgt $A^\perp \cong B^\perp$,
d.h. es existiert ein Isomorphismus $\beta : A^\perp \to B^\perp$.

Jeder beliebige Vektor $x \in E$ lässt sich schreiben als $x = a + c$ mit $a \in A$, $c \in A^\perp$, damit ist $\gamma : a + c \longmapsto a^\alpha + c^\beta$ ein Automorphismus von E, der α fortsetzt.

Damit haben wir gezeigt, dass der Wittsche Kürzungssatz und der Wittsche Satz einander entsprechen.

Beweis des Wittschen Satzes (eindimensionaler Fall). Sei $dim(A) = m = 1$. Sei $A = aK$ und $B = bK$ mit $aa = bb \neq 0$, $b = a^\alpha$. Erster Fall: $a - b$ nicht ausgeartet. Einen beliebigen Vektor $x \in E$ kann man schreiben als $x = k(a-b)+h$ mit $h \in (a-b)^\perp$. Dann wäre eine Spiegelung σ an der Hyperebene $(a-b)^\perp$ erklärt durch $x^\sigma = -k * (a-b) + h$. Setzt man $h = \frac{a+b}{2}$ und $k = \frac{1}{2}$.
Dann ist $x = a$ und $x^\sigma = b$. Damit setzt σ den Isomorphismus α fort und ist der gesuchte Automorphismus.
Zweiter Fall: $a - b$ ist ausgeartet Daraus folgt , dass $a + b$ nicht ausgeartet ist, da sonst $a * a = b * b = \frac{(a+b)^2+(a-b)^2}{4} = 0$. Nach Fall Eins wäre dann σ eine Spiegelung an der Hyperebene $(a+b)^\perp$. Einen beliebigen Vektor $x \in E$ kann man nun schreiben als $x = k(a+b) + h$ mit $h \in (a+b)^\perp$ und $x^\sigma = -k(a+b) + h$. Setzt man $h = \frac{(a-b)}{2}$ und $k = \frac{1}{2}$, dann ist $x = a$ und $x^\sigma = -b$.
Ist $\tau : x \longmapsto -x$ eine Spiegelung am Ursprung , so ist $\gamma = \tau \circ \sigma$ der gesuchte Automorphismus.

Jetzt beweisen wir den Wittschen Kürzungssatz: Schreibe f, g, h als Diagonalformen $(a_1, \ldots, a_m)$, $(b_1, \ldots, b_k)$, $(c_1, \ldots, c_k)$, wobei a_i, b_i, c_i die Diagonalelemente der jeweiligen Matrizen sind.

Induktionsverankerung: Für $m = 1$ lautet die Behauptung:

$$(a_1, b_1, \ldots, b_k) \cong (a_1, c_1, \ldots, c_k) \Rightarrow (b_1, \ldots, b_k) \cong (c_1, \ldots, c_k).$$

Das entspricht dem obigen Beweis für den eindimensionalen Fall. Für $m > 1$ folgt nach dem obigen Fall für $m = 1$: $(a_1, a_2, \ldots, a_m, b_1, \ldots, b_k) \cong (a_1, a_2, \ldots, a_m, c_1, \ldots, c_k) \Rightarrow (a_2, \ldots, a_m, b_1, \ldots, b_k) \cong (a_2, \ldots, a_m, c_1, \ldots, c_k)$.
Daraus folgt nach Induktionsvoraussetzung die Behauptung. Damit ist auch der Satz von Witt für nicht ausgeartete Räume bewiesen. □

7 Filtrierungen und das Artin-Rees Lemma

Verena Moock, Yulian Pastarmov

7.1 Einführung

In diesem Kapitel werden wir zwei Konstruktionen beschreiben – der assoziierte graduierte Ring und die aufgeblasene Algebra – die aus einer absteigenden multiplikativen Filtrierung eines Ringes R bestehen; das heißt aus einer Sequenz von Idealen

$$R = I_0 \supset I_1 \supset I_2 \cdots \supset \text{ wobei } I_i I_j \subset I_{i+j} \text{ für alle } i, j \text{ erfüllt ist.}$$

Eine dritte solche Konstruktion, die Rees-Algebra, wird am Ende des nächsten Kapitels behandelt, und wirft etwas Licht auf die Ergebnisse, die wir am assoziierten graduirten Ring zu prüfen haben. Kapitel 7 im Eisenbud wird einem vierten Beispiel gewidmet, der Vervollständigung. Die Rees-Algebra verwendet man, um Informationen über R zu erhalten. Dazu zieht man den Vergleich zu einem ähnlichen, auf gewisser Weise einfacheren Ring heran.

Diese Konstruktionen werden am häufigsten in Fällen verwendet, wo die I_j die Potenzen eines einzigen Ideals sind, $I_j = I^j$; sie werden als I-adische Filtrierung bezeichnet. In Anwendungen wird I oft als maximales Ideal eines lokalen noetherschen Rings R gewählt, und dem Leser wird nicht viel fehlen, wenn er sich vorstelle, dies sei es stets der Fall.

Da die Veralgemeinerung bezüglich Moduln sehr hilfreich ist, werden wir außerdem auch die I-adische Filtrierung eines Moduls M betrachten: Sei $M \supset IM \supset I^2M \supset \dots$. Aber wenn man diese Terme einer I-adischen Filtrierung von M mit einem Untermodul $M' \subset M$ schneidet, erhält man im Allgemeinen keine I-adische Filtrierung von M'. Ein Schlüsselergebnis der Theorie, das Artin-Rees Lemma, zeigt, dass die induzierte Filtrierung oft stabil im folgenden Sinne ist:

Definition 7.1.1. Sei R ein Ring, $I \subset R$ ein Ideal und M ein R-Modul. Eine Filtrierung $M = M_0 \supset M_1 \supset \dots$ wird eine **I-Filtrierung** genannt, wenn $IM_n \subset M_{n+1}$ für alle $n \geq 0$. Eine I-Filtrierung wird **I-stabil** genannt, wenn zusätzlich $IM_n = M_{n+1}$ für genügend große n gilt. Allgemein kann man dann diese Gleichung umformen zu $M_{i+n} = I^i M_n$, für alle $i \geq 0$. Wenn das Ideal I als bekannt vorausgesetzt wird, spricht man schlicht von **stabilen Filtrierungen.**

Eine I-stabile Filtrierung ist bestimmt, wenn eine genügend große endliche Anzahl von M_i bekannt ist; in diesem Sinne liegt eine **endlich erzeugte Filtrierung** vor.

Lemma 7.1.2 (Artin-Rees)**.** *Sei R ein noetherscher Ring, $I \subset R$ ein Ideal, $M' \subset M$ endlich erzeugte R-Moduln. Wenn $M = M_0 \supset M_1 \supset \ldots$ eine I-stabile Filtrierung ist, so ist die induzierte Filtrierung $M' \supset M' \cap M_1 \supset M' \cap M_2 \supset \ldots$ auch I-stabil. D. h. es existiert eine natürliche Zahl n, so dass für alle $i \geq 0$ gilt: $M' \cap M_{i+n} = I^i(M' \cap M_n)$.*

Der Beweis folgt nach Proposition 7.3.2, nachdem einige grundlegende Konstruktionen eingeführt wurden. Für eine interessante neue Entwicklung in dieser Theorie vergleiche man Huneke [7].

7.2 Assoziierte graduierte Ringe und Moduln

Definition 7.2.1. Sei I ein Ideal eines Rings R. Man definiere den **assoziierten graduierten Ring** $gr_I R$ von R bezüglich I als graduierten Ring

$$gr_I R := R/I \oplus I/I^2 \oplus \cdots .$$

Hier ist die Multiplikation in $gr_I R$ wie folgt gegeben: Sei $a \in I^m/I^{m+1}$ und $b \in I^n/I^{n+1}$, man nehme Repräsentanten a' und b' von a und b in I^m und I^n entsprechend, man definiere $ab \in I^{m+n}/I^{m+n+1}$ als Bild von $a'b'$. Man beachte, dass dieses wohldefiniert modulo I^{m+n+1} ist.

Generell sei $\mathcal{J} = M = M_0 \supset M_1 \supset \ldots$ eine I-Filtrierung eines R-Moduls M. Sei

$$gr_{\mathcal{J}} M := M/M_1 \oplus M_1/M_2 \oplus \cdots .$$

Mache $gr_{\mathcal{J}} M$ folgendermaßen zu einem graduierten $gr_I R$-Modul: Wenn $a \in I^m/I^{m+1}$ und $b \in M_n/M_{n+1}$ Repräsentanten $a' \in I^m$ und $b' \in I^n$ haben, dann ist $a \cdot b$ definiert als die Klasse von $a' \cdot b'$ in M_{m+n}/M_{m+n+1} . Die Annahme, dass $\mathcal{J}$ eine I-Filtrierung ist, gewährleistet die Wohldefiniertheit.

Proposition 7.2.2. *Sei I ein Ideal in einem Ring R und man nehme an, dass M ein endlich erzeugter R-Modul ist. Wenn $\mathcal{J} : M = M_0 \supset M_1 \supset \ldots$ eine I-stabile Filtrierung von endlich erzeugten Untermoduln von M ist, dann ist $gr_{\mathcal{J}} M$ ein endlich erzeugter Modul über $gr_I R$.*

Beweis. Man nehme an, dass $IM_i = M_{i+1}$ für alle $i \geq n$. Offensichtlich gilt $(I/I^2)(M_i/M_{i+1}) = M_{i+1}/M_{i+2}$ für alle $i \geq n$. Daher erzeugt die Vereinigung aller Mengen von Erzeugern der Moduln $M_0/M_1, \ldots, M_n/M_{n+1} gr\, M$. Da jedes M_i endlich erzeugt ist, kann jedes dieser Mengen von Erzeugern endlich gewählt werden. □

Sei M ein R-Modul mit Filtrierung $\mathcal{J} : M = M_0 \supset M_1 \supset \ldots$. Es gibt keinen interessanten natürlichen Homomorphismus von M nach $gr\, M$, aber es existiert eine interessante Abbildung von Mengen, die wie folgt definiert ist: Gegeben $f \in M$. Sei m

die größte Zahl, so dass $f \in M_m$, und man definiere die Initial-Form von f, bezeichnet als $in(f)$, durch

$$in(f) := f \; modulo \; M_{m+1} \in M_m/M_{m+1} \subset gr\, M,$$

oder durch

$$in(f) := 0 \; wenn \; f \in \cap_{m=1}^{\infty} M_m.$$

Man nehme nun an, dass $I \subset R$ ein Ideal sei, sowie $\mathcal{J}$ eine Filtrierung von M. Man setze $G = gr_I\, R$. Sei $M' \subset M$ ein Untermodul, man definiere $in(M')$ als den G-Untermodul von $gr\, M$, der erzeugt wird von allen $in(f)$ für alle $f \in M'$. Der Untermodul $in(M')$ wird im Allgemeinen nicht erzeugt durch die Initialformen einer gegebenen Menge von Erzeugern von M'. Gilt beispielsweise

$$J = (xy + y^3, x^2) \subset R = k[x, y],$$

und $I = (x, y)$, dann ist $in(x^2) = x^2 + I^3$ und $in(xy+y^3) = xy+I^3$ bei Berücksichtigung der I-adischen Filtrierung. Allerdings erzeugen x^2 und xy nicht $in(J)$. Zum Beispiel:

$$x(xy + y^3) - y(x^2) = xy^3 \in J,$$

somit

$$y^2(xy + y^3) - xy^3 = y^5 \in J,$$

folglich $y^5 \in in(J)$. In der Tat gilt $in(J) = (x^2 + I^3, xy + I^3, y^5 + I^5)$. Ein erster Hinweis, warum die Konstruktion des assoziierten graduierten Ring interessant ist, ist die Tatsache, dass $gr_I\, R$ eine graduierte Algebra über dem Raum R/I ist, wenn I ein maximales Ideal ist. Es ist häufig sogar eine endlich erzeugte Algebra, sofern I endlich erzeugtes Ideal ist. Daher gibt gr_I eine Möglichkeit, beliebige lokale noethersche Ringe in endlich erzeugte graduierte Ringe umzuformen. Als Beispiel wenden wir dies auf die Theorie der Hilbert-Funktionen an.

Definition 7.2.3. Wenn R ein lokaler Ring mit maximalem Ideal I ist, dann lautet die **Hilbert-Funktion von R** folgendermaßen:

$$H_R(n) = dim_{R/I}\, I^n/I^{n+1}.$$

Allgemeiner: Sei M ein endlich erzeugter R-Modul, dann definiert man:

$$H_M(n) = dim_{R/I}\, I^n M/I^{n+1}M.$$

Da jene lediglich die Hilbert-Funktionen von $gr_I\, R$ und $gr_I\, M$ sind, wobei $gr_I\, M$ ein endlich erzeugter $gr_I\, R$-Modul ist, weiß man außerdem, dass sie für große n mit Polynomen $P_R(n)$ und $P_M(n)$ vom Grad $\leq H_R(1)-1$ übereinstimmen, und dass H_R und H_M darüber hinaus in Termen von Binomialkoeffizienten beschrieben werden können. Diese Funktionen sind sehr wichtig in der Dimensionstheorie.

Manchmal ist es möglich, schöne Eigenschaften von R aus schönen Eigenschaften von $gr_I\, R$ zu erhalten. Mit dieser Absicht muss sicher gestellt sein, dass sämtliche Elemente von R von $gr_I\, R$ berücksichtigt werden, was der Fall wäre, wenn ein Element von

R in jeder Potenz von I enthalten wäre. Glücklicherweise gilt in den meisten Fällen $\cap_j I^j = 0$. Das benötigte Werkzeug, um dies zu beweisen, ist das Artin-Rees Lemma. Der Beweis dieses Lemmas verwendet ein anderes Konstrukt von großem geometrischen und algebraischen Interesse:

7.3 Die aufgeblasene Algebra

Definition 7.3.1. Wenn R ein Ring ist und $I \subset R$ ein Ideal, dann ist die **aufgeblasene Algebra von I in R** die R-Algebra

$$B_I R := R \oplus I \oplus I^2 \oplus \cdots \cong R[tI] \subset R[t].$$

Man beachte, dass $B_I R / I B_I R = R/I \oplus I/I^2 \oplus \cdots = gr_I R$, der assoziierte graduierte Ring.

Der geometrische Kontext, in welchem die aufgeblasene Algebra auftritt, erklärt den Namen: Sofern R die Koordinaten-k-Algebra einer affinen algebraischen Menge ist und I das Ideal einer algebraischen Untermenge $Y \subset X$, dann kann man eine algebraische Menge Z durch den Prozess des **Aufblasens von** $Y \subset X$ erhalten: Seien $a_1, \ldots, a_n$ die k-Algebra Erzeuger von R und $g_0, \ldots, g_s$ die Erzeuger von I als Ideal von R. Die Algebra $B_I R$ ist das homomorphe Bild des Rings $k[x_1, \ldots, x_r,\ y_0, \ldots, y_s]$ durch die Abbildung $x_i \to a_i,\ y_j \to g_j t$. Der Kern dieser Abbildung ist ein Ideal, welches offensichtlich homogen in den Variablen y_j ist. Insofern korrespondiert es zu der algebraischen Teilmenge $Z \subset \mathbf{A^r} \times \mathbf{P^s}$. Die Projektions-Abbildung $\mathbf{A^r} \times \mathbf{P^s} \to \mathbf{A^r}$ bildet Z auf X ab und ist ein Isomorphismus bezüglich des Urbildes von Y. Die Menge Z wird die Aufblasung von Y in X genannt. Das Urbild von Y in Z korrespondiert zu dem Ring $B_I R / I B_I R = gr_I R$. Dieses Urbild, welches den Namen **Ausnahmemenge** trägt, ist die projektive Varietät assoziiert zum graduierten Ring $gr_I R$.

Wenn M ein R-Modul ist und $\mathcal{J} : M = M_0 \supset M_1 \supset \cdots$ eine I-Filtrierung, dann wird die direkte Summe

$$B_{\mathcal{J}} M := M \oplus M_1 \oplus \cdots$$

auf natürliche Weise zum graduierten Modul über dem aufgeblasenen Ring $B_I R$. Hierbei sei $a = (k_0, k_1, \ldots, k_n)$ Element aus $B_I R$ und $b = (m_0, m_1, \ldots, m_l)$ Element aus $B_{\mathcal{J}} M$, dann ist $a \cdot b$ definiert als $(m_0 k_0, m_1 k_0 + m_0 k_1, \ldots, \sum_{j=0}^{p} m_j k_{p-j}, \ldots, m_l k_n)$. Die Beziehung zwischen endlich erzeugten Moduln und stabilen Filtrierungen wird durch diese Konstruktion verdeutlicht.

Proposition 7.3.2. *Sei R ein Ring, $I \subset R$ ein Ideal und M ein endlich erzeugter R-Modul mit I-Filtrierung $\mathcal{J} : M = M_0 \supset M_1 \supset \cdots$ von den endlich erzeugten Moduln M_i. Die Filtrierung heißt $\mathcal{J}$-stabil genau dann, wenn die $B_I R$-Moduln $B_{\mathcal{J}} M$ endlich erzeugt sind.*

Beweis. Wenn $B_{\mathcal{J}} M$ endlich erzeugt ist, dann müssen die Erzeuger in der direkten Summe der ersten n Terme, für ein existierendes n, liegen. Ersetzt man diese durch ihre homogene Komponenten, erkennt man, dass $B_{\mathcal{J}} M$ von Elementen der Moduln M_i erzeugt wird, für verschiedene $i \leq n$. □

Natürlich wird dann

$$M_n \oplus M_{n+1} \oplus \cdots$$

als $B_{\mathcal{J}}M$-Modul erzeugt von M_n, d.h.

$$M_{n+i} = I^i M_n$$

für alle $i \geq 0$, somit ist $\mathcal{J}$ stabil. Andererseits, wenn $\mathcal{J}$ stabil ist, so dass $M_{n+i} = I^i M_n$, für ein n und alle $i \geq 0$, wird $B_{\mathcal{J}}M$ erzeugt von der Vereinigung von Mengen der Erzeugern von $M_0, M_1, \ldots, M_n$.

Mit dieser Konstruktion wird das Artin-Rees Lemma zu einem Korollar des Hilbert-Basis-Satzes.

Beweis von Lemma 7.1.2. Sei

$$\mathcal{J} : M = M_0 \supset M_1 \supset M_2 \supset \cdots$$

$$\mathcal{J}' : M' = M'_0 \supset \underbrace{M' \cap M_1}_{M'_1} \supset \underbrace{M' \cap M_2}_{M'_2} \cdots$$

die induzierte Filtrierung auf M'. $B_{\mathcal{J}}M$ ist graduierter Modul über dem aufgeblasenen Ring $B_I R$. Natürlich ist dann der Modul $B_{\mathcal{J}'}M'$ ein graduierter $B_I R$-Untermodul von $B_{\mathcal{J}}M$. Wenn $\mathcal{J}$ eine stabile Filtrierung ist, dann ist $B_{\mathcal{J}}M$ endlich erzeugt, laut Proposition 7.3.2. Weil $B_{\mathcal{J}}M$ eine endlich erzeugte R-Algebra ist, ist sie noethersch und somit ist der Untermodul $B_{\mathcal{J}'}M'$ ebenfalls endlich erzeugt (siehe Kapitel 1.5 in [4]. Proposition 7.3.2 zeigt, dass $\mathcal{J}'$ eine stabile Filtrierung von M'. ist. □

7.4 Der Krull Schnitt Satz

Als erste wichtige Anwendung wird der Satz von Krull [4] eingeführt. (Hier angegeben in der Form von Chevalley [5])

Folgerung 7.4.1 (Krull Schnitt Satz)**.** *Sei $I \subset R$ Ideal in einem noetherschen Ring R. Wenn M ein endlich erzeugter R-Modul ist, dann existiert ein Element $r \in I$, so dass*

$$(1 - r)(\cap_{j=1}^{\infty} I^j M) = 0. \tag{7.4.1}$$

Wenn R zusätzlich ein Integritätsring oder ein lokaler Ring ist und I ein echtes Ideal, dann gilt:

$$\bigcap_{j=1}^{\infty} I^j = 0. \tag{7.4.2}$$

Beweis. Nach dem Lemma von Artin-Rees, angewendet auf den Untermodul $\cap_{j=1}^{\infty} I^j M \subset M$, existiert eine ganze Zahl n, so dass

$$\begin{aligned} \bigcap_{j=1}^{\infty} I^j M &= \left(\bigcap_{j=1}^{\infty} I^j M\right) \cap I^{n+1} M && (7.4.3) \\ &= I\left(\left(\bigcap_{j=1}^{\infty} I^j M\right) \cap I^n M\right) && (7.4.4) \\ &= I\left(\bigcap_{j=1}^{\infty} I^j M\right). && (7.4.5) \end{aligned}$$

Die erste Aussage erlangt ihre Gültigkeit als Konsequenz des Satzes von Cayley-Hamilton, Korollar 4.2.7 aus [4]. Da laut Voraussetzung M endlich erzeugt ist, gilt Gleiches für $\cap I^j M$. Gleichung 7.4.5 lässt auf die Existenz eines Elementes $r \in I$ schließen, bei dem $1 - r$ den Schnitt annuliert.

Um die zweite Aussage einzusehen, nimmt man $M = R$. Dann reicht es aus zu zeigen, dass in den gegebenen Fällen $1-r$ kein Nullteiler ist. Weil I ein echtes Ideal ist, existiert mindestens ein $r \neq 1$, so dass $1 - r \neq 0$. Falls R ein Integritätsring ist, ist der Beweis komplett. In dem Fall, dass R lokal ist, muss I in dem maximalen Ideal enthalten sein. Ebenfalls ist auch r Element dessem, somit also eine Nicht-Einheit, $1-r$ also eine Einheit und kein Nullteiler. Schlussfolgernd ist $\bigcap_{j=1}^{\infty} I^j = 0$. □

Folgerung 7.4.2. *Sei R ein noetherscher lokaler Ring und I ein echtes Ideal von R. Wenn $gr_I R$ ein Integritätsring ist, dann ist auch R ein Integritätsring.*

Beweis. Wenn $f \cdot g = 0$ in R, dann ist $in(f) \cdot in(g) = 0$ in $gr_I R$, somit ist entweder $in(f)$ oder $in(g)$ gleich 0. Nach dem Krull Schnitt Satz gilt, $\cap_{n=1}^{\infty} I^n = 0$, woraus folgt, dass f oder g gleich 0 ist. □

Beispiel 7.4.3. Sowohl der Satz von Krull als auch Korollar 7.4.2 sind nicht allgemein gültig im nicht-noetherschen Fall. Sei beispielsweise R der Ring von Keimen von $\mathcal{C}^\infty$-Funktionen über $(\mathbf{R}, 0)$ und x die Koordinatenfunktion. Sei

$$g(x) := e^{-\frac{1}{x^2}} \in R,$$

eine $\mathcal{C}^\infty$-Funktion deren Graph in der Abbildung 7.4 gezeigt wird. Der Ring R ist lokal mit maximalen Ideal I, erzeugt von der Funktion x. Da $g(x)/x^n$ in $\mathcal{C}^\infty$, für alle n, folgt

$$g(x) \in \bigcap_{1}^{\infty} I^n.$$

In diesem Fall ist $\cap_1^\infty I^n$ die Menge aller Keime von Funktionen, die im Ursprung verschwinden. Diese sind auf die Art flach, dass alle ihre Ableitungen im Ursprung auch

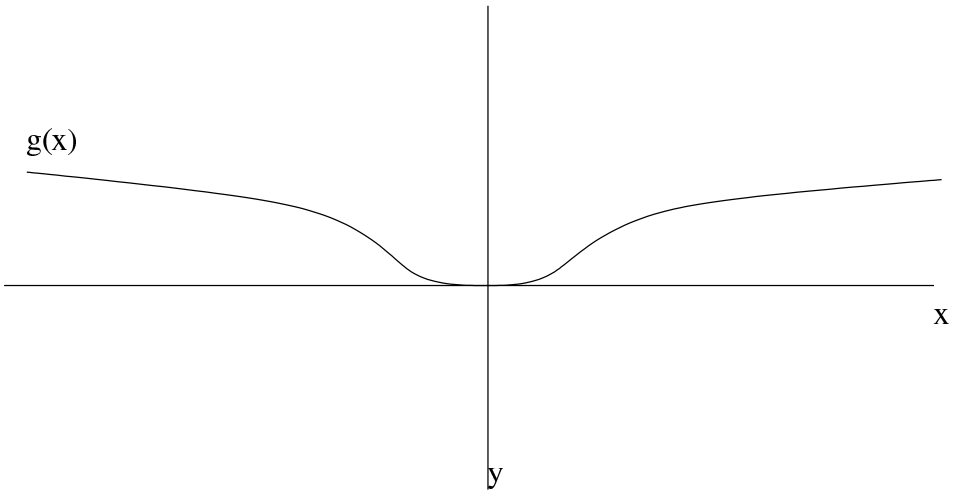


Abbildung 7.1: Graph von $g(x)$

verschwinden. Wahrhaftig gilt $I(\cap_1^\infty I^n) = \cap_1^\infty I^n$. Die $\mathcal{C}^\infty$ Funktionen der Form $1 - r$, mit $r \in (x)$, sind dabei die $\mathcal{C}^\infty$-Keime mit dem Wert 1 im Punkt 0. Daher wird $g(x)$ beispielsweise nicht annuliert von einer solchen Funktion. Also ist Korollar 7.4.1 nicht zutreffend.

7.5 Der Tangentialkegel

Die Tatsache, dass der assoziierte graduierte Ring zu der außergewöhnlichen Menge in der Aufblasung korrespondiert, hat eine einfache und schöne geometrische Konsequenz. Sei

$$R = k[x_1, \ldots, x_r]/J,\ I = (x_1, \ldots, x_r)$$

wobei k ein algebraisch abgeschlossener Körper ist. Sei $X = Z(J) \subset A^r$ und man nehme an, dass $J \subset I$, so dass $0 \in X$. Der **Tangentialkegel** von X in 0 ist der Kegel, zusammengesetzt aus allen Geraden, die durch die begrenzenden Positionen der Sekanten zu X und durch den Punkt 0 verlaufen. Man kann zeigen, dass das Ideal $in_I(J) \subset k[x_1, \ldots, x_r]$ den Tangentialkegel definiert. Der Koordinatenring des Tangentialkegels $gr_{(x_1,\ldots,x_r)}R$ ist somit bestimmt.

8 Flache Familien

Karsten Hayn

8.1 Flachheit

Definition 8.1.1. Ein Modul M über einem Ring R heißt *flach*, wenn für alle Inklusionen $N' \subset N$ von R-Moduln die induzierte Abbildung $M \otimes_R N' \to M \otimes_R N$ auch eine Inklusion ist.
In exakten Sequenzen bedeutet das, dass wenn $0 \to N' \to N \to N''$ eine exakte Sequenz ist, auch $0 \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N''$ exakt ist.

Beispiel 8.1.2. Sei K ein Körper, $R = K[t]$ der Polynomring über K und $S := R[x]/(x-t)$. Als R-Algebra ist $S \cong R$. Da $R \otimes_R N = N$ für alle R-Moduln N ist R flach als R-Algebra.

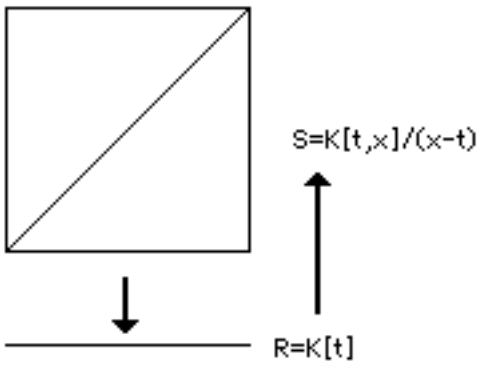


Abbildung 8.1: Beispiel 8.1.2

Beispiel 8.1.3. Sei $S = R[x]/(tx-1)$. Wir können S als die Lokalisierung $R[t^{-1}]$ betrachten. Wie wir schon wissen sind Lokalisierungen flach und damit ist S flach.

Seien M, N R-Moduln und $\ldots \to F_{i+1} \to F_i \to F_{i-1} \to \ldots \to M \to 0$ eine freie Auflösung (siehe [4] S.45) von M als R-Modul.

Definition 8.1.4. Die *Homologie* in F_i vom Komplex $F_{i+1} \xrightarrow{g} F_i \xrightarrow{h} F_{i-1}$ ist $ker(h)/im(g)$. Sie gibt also an, „wie weit“ die Sequenz von der Exaktheit entfernt ist.

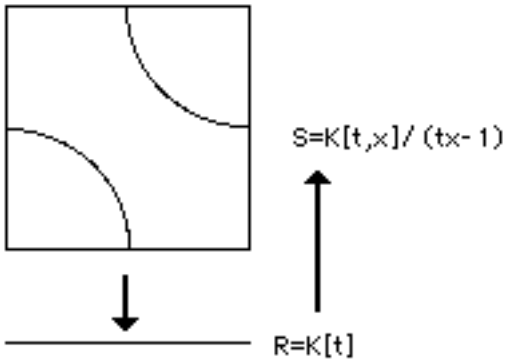


Abbildung 8.2: Beispiel 8.1.3

Definition 8.1.5. $Tor_i^R(M,N)$ ist die Homologie von $F_i \otimes_R N$ in dem Komplex $F_{i+1} \otimes_R N \to F_i \otimes_R N \to F_{i-1} \otimes_R N$.

Proposition 8.1.6. (i) *Sei M oder N frei, dann ist $Tor_i^R(M,N) = 0$ für $i > 0$.*

(ii) *Für jede kurze exakte Sequenz $0 \to M' \to M \to M'' \to 0$ von R-Moduln und jeden R-Modul N gibt es eine lange exakte Sequenz von Tor:*

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \to$$

$$Tor_i^R(M',N) \to Tor_i^R(M,N) \to Tor_i^R(M'',N) \to$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \to$$

$$Tor_1^R(M',N) \to Tor_1^R(M,N) \to Tor_1^R(M'',N) \to$$

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$$

(iii) *Sei $x \in R$ kein Nullteiler und M ein R-Modul. Dann gilt:*

$$Tor_0^R(R/(x),M) = M/xM$$

$$Tor_1^R(R/(x),M) = (0:_M x)$$

$$Tor_i^R(R/(x),M) = 0 \quad fr\ i > 1$$

Beweis. Beweis siehe [4] Seite 161-162. □

Lemma 8.1.7. *Sei R ein Ring, M ein R-Modul und I ein Ideal von R. Dann ist die Abbildung $I \otimes_R M \to M$ injektiv genau dann wenn $Tor_1^R(R/I,M) = 0$.*
Der Modul M ist flach genau dann wenn $Tor_1^R(R/I,M) = 0$ für alle endlich erzeugten Ideale I.

Beweis. Wie wir aus Proposition 8.1.6 (ii) wissen, erhalten wir von der kurzen exakten Sequenz $0 \to I \to R \to R/I \to 0$ eine lange exakte Sequenz die $Tor_1^R(R,M) \to Tor_1^R(R/I,M) \to I \otimes M \xrightarrow{g} R \otimes M$ enthält. Nun ist $Tor_1^R(R,M) = 0$ nach 8.1.6 (i) und $R \otimes M = M$. Damit ist g die Multiplikation $I \otimes M \to M$ womit die erste Behauptung gezeigt ist.
Nehmen wir also an, dass die Voraussetzungen des zweiten Teils erfüllt sind. Dies bedeutet das $N = R$ und $N' = I$ (wobei N, N', I wie in Definition 8.1.1). $I \otimes M \to M$ ist eine injektive Abbildung für alle Ideale I' von R. Nun ist aber jedes Element $x \neq 0 \in I' \otimes_R M$ die (endliche) Summe von Elementen $r' \otimes m$ für $m \in M, r' \in I'$. Deshalb wird x auf ein Element ungleich Null in M abgebildet.
Andererseits wird der Modul $N \otimes_R M$ von den Elementen $\{n \otimes_R m \mid n \in N, m \in M\}$ erzeugt. Deshalb benötigt man für die Aussage, dass ein $x \in N' \otimes_R M$ auf 0 in $N \otimes_R M$ abgebildet wird, nur endlich viele Elemente von N und wir können annehmen, dass N endlich erzeugt ist.
Es ist uns nun möglich eine Sequenz von Untermoduln

$$N' = N_0 \subset N_1 \subset \ldots \subset N_p = N$$

so zu wählen, daß alle N_{i+1}/N_i von je einem Element erzeugt werden. Es reicht nun zu zeigen, dass jede Abbildung $N_i \otimes M \to N_{i+1} \otimes M$ injektiv ist. Um das zu tun, reicht es am Anfang anzunehmen, dass N/N' ein zyklischer Modul ist und deshalb $N/N' \cong R/I$. Proposition 8.1.6 (ii) liefert uns wieder, dass die kurze exakte Sequenz $0 \to N' \to N \to N/N' \to 0$ eine lange exakte Sequenz liefert, die $Tor_1^R(N/N', M) \to N' \otimes M \to N \otimes M$ enthält. Da aber nun nach Vorausetzung $Tor_1^R(R/I, M) = 0$ ist und da $Tor_1^R(N/N', M) = Tor_1^R(R/I, M)$ ist das Lemma bewiesen. □

Später zeigt sich, dass es in den meisten Fällen reicht, die maximalen Ideale zu überprüfen (Satz 8.1.12).

Beispiel 8.1.8. Sei K ein Körper, $R = K[t]/(t^2)$ und M ein R-Modul. Dann ist M flach genau dann, wenn die Multiplikation mit t von M nach tM einen Isomorphismus $M/tM \to tM$ induziert.

Beweis. Um das Lemma benutzen zu können, müssen wir die Ideale von R überprüfen. Das einzige nichttriviale Ideal von R ist (t) und isomorph zu $R/(t)$ als R-Modul mit dem Isomorphismus $R/(t) \to (t)$, der die 1 auf t abbildet. Wendet man nun Lemma 8.1.7 an, erhält man, dass M flach ist genau dann, wenn

$$M/tM \cong R/(t) \otimes M \cong (t) \otimes_R M \to R \otimes_R M = M$$

ein Monomorphismus ist. (Man bildet die Klasse eines Elements $m \in M$ auf $tm \in M$ ab.) Da dies aber eine Verknüpfung des Epimorphismus $M/tM \to tM$ (induziert durch die Multiplikation mit t) und der Inklusion $tM \subset M$ ist, gilt unsere Behauptung. □

Folgerung 8.1.9. *Sei $a \in R$ kein Nullteiler in R und M ein flacher R-Modul. Dann ist a kein Nullteiler auf M.*
Wenn R ein Hauptidealring ist, gilt auch die Umkehrung: M ist flach als R-Modul genau dann, wenn M torsionsfrei ist.

Beweis. Sei $I = Ra$ wobei $a \in R$ kein Nullteiler ist. Wenn M flach ist, dann ist für alle $I \subset R$ die Abbildung $\varphi : I \otimes_R M \to R \otimes_R M = M$ injektiv. Nun ist aber $I \otimes_R M \cong R \otimes_R M = M$ (als Modul), da $I \cong R$ (als Modul) mit dem Isomorphismus der a auf 1 abbildet. Also wird φ zu einer Multiplikation mit a. Dies ist ein Monomorphismus genau dann, wenn a kein Nullteiler auf M ist.
Sei R nun ein nullteilerfreier Hauptidealring, dann ist kein Ideal (außer dem Nullideal) durch einen Nullteiler erzeugt. Nun wenden wir Lemma 8.1.7 an, was für $I \neq 0$ mit Proposition 8.1.6 (ii) liefert, dass M flach ist genau dann, wenn für alle $c \neq 0 \in R$ gilt, dass sie keine Nullteiler in M sind. Das bedeutet aber gerade, dass M torsionsfrei ist. □

Beispiel 8.1.10. Sei $S = R[x]/(tx - t)$. Dann ist S nicht flach, denn $t(x - 1) = 0$ in S, also hat S eine Torsion.

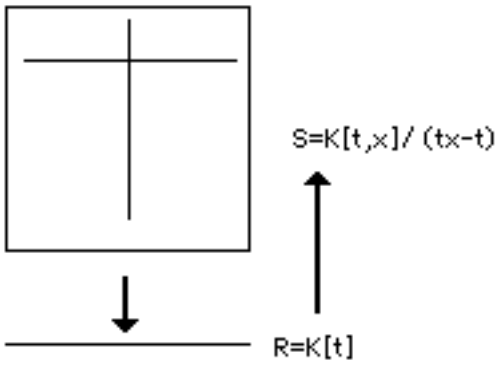


Abbildung 8.3: Beispiel 8.1.10

Folgerung 8.1.11. *Sei K ein Körper und $R := K[t]$ ein Polynomring in einer Variablen. Sei S ein noetherscher Ring, der flach über K ist.*
Sei U die Menge der Elemente der Form $1 - ts$ für $s \in S$. Wenn die Faser S/tS über dem Primideal (t) ein Integritätsring ist, dann ist $S[U^{-1}]$ ein Primideal.

Beweis. Beweis siehe [4] Seite 167, Corollary 6.7. □

Satz 8.1.12. Lokales Kriterium für Flachheit
Sei $(R, \mathfrak{m})$ ein lokaler noetherscher Ring und sei $(S, \mathfrak{n})$ eine lokale noethersche R-Algebra mit $\mathfrak{m}S \subset \mathfrak{n}$. Sei M ein endlich erzeugter S-Untermodul, dann ist M flach als R-Modul genau dann, wenn $Tor_1^R(M, N) = 0$.

Beweis. Beweis siehe [4] Seite 168-169, Theorem 6.8. □

Lemma 8.1.13. *Sei R ein Ring, M ein R-Modul und $x \in R$ kein Nullteiler in R und M. Dann gilt für alle $(R/(x))$-Moduln N, dass*

$$Tor_i^{R/(x)}(N, M/xM) = Tor_i^R(N, M)$$

Beweis. Beweis siehe [4] Seite 170, Lemma 6.10. □

Bemerkung 8.1.14. Sei $R \to R'$ ein Ringhomomorphismus und M ein flache R-Modul. Dann ist $R' \otimes_R M$ flach als R'-Modul.

Beweis. Wenn die Annahmen gelten, haben wir:

$$(R' \otimes_R M) \otimes_{R'} N = M \otimes_R N$$

für alle R'-Moduln N, womit $R' \otimes M$ flach ist. □

Dies lässt sich in einem wichtigen Spezialfall umkehren.

Folgerung 8.1.15. *Sei $(R, \mathfrak{m})$ ein lokaler noetherscher Ring und sei $(S, \mathfrak{n})$ eine lokale noethersche R-Algebra mit $\mathfrak{m}S \subset \mathfrak{n}$. Sei weiter M ein endlich erzeugter S-Modul und $x \in \mathfrak{m}$ kein Nullteiler in R und M. Dann ist M flach über R genau dann wenn M/xM flach über $R/(x)$ ist.*

Beweis. Sei M flach, dann ist $M/xM = R/(x) \otimes_R M$ flach über $R/(x)$, wie wir eben gezeigt haben. Also können wir annehmen, dass M/xM flach über $R/(x)$ ist und müssen zeigen, dass M flach über R ist. Sei $K := R/\mathfrak{m}$ der Restklassenkörper von R.
Nun gilt, dass $Tor_1^{R/(x)}(K, M/xM) = 0$, da M/xM flach über $R/(x)$ ist und nach Lemma 8.1.13 ist $Tor_1^R(K, M) = 0$, was uns mit Satz 8.1.12 liefert, dass M flach ist. □

8.2 Familien

Der Begriff einer *Familie* lässt sich leider nicht so leicht definieren wie der der Flachheit. Das typische Beispiel von Familien sind Kurven in der affinen Ebene über einem Körper. Man möchte also Objekte haben, die „ahnlich“ sind und mit „ihren Parametern variere“. Die „mächtigste“ Definition ist wohl zu sagen, das Familien Morphismen sind: Sei $\varphi : X \to B$ ein Morphismus zwischen Varietäten. Dann sind die Urbilder der Punkte in B (die Fasern von φ) Varietäten in einer Familie, definiert durch die Punkte von B. Leider ist es möglich, dass diese Definition zu umfassend ist und Objekte in die Familie nimmt, die nichts mit den anderen gemeinsam haben. Um dies zu vermeiden nimmt man als Bedingung hinzu, dass die Familie flach ist (d.h. wenn wir die Familie als R-Algebra S darstellen soll S flach über R sein).

Definition 8.2.1. Ein n-dimensionaler Multiindex ist ein Vektor $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_n)$ wobei $\alpha_i \in \mathbb{Z}$. Für Multiindizes α, β und $x = (x_1, x_2, \ldots x_n) \in \urcorner^n$ definiert man

- $\alpha + \beta := (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots \alpha_n + \beta_n)$
- $|\alpha| := (|\alpha_1| + |\alpha_2| + \ldots + |\alpha_n|)$
- $\alpha \leq \beta \Leftrightarrow (\alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2, \ldots \alpha_n \leq \beta_n) \; \forall \; i$
- $\alpha! = (\alpha_1!, \alpha_2!, \ldots \alpha_n!)$

- $x^\alpha := (x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_2^{\alpha_n})$

Beispiel 8.2.2. *Die Familie von Kurven auf projektiven Ebenen*
Für einen festen Rang d und einen 3-elementigen Multiindex α vom Rang d sei x_α eine unbestimmte Variable. Sei weiter $R = K[\{x_\alpha\}]$ der Polynomring an x_α und

$$S := R[y_0, y_1, y_2] / \sum_\alpha x_\alpha y^\alpha$$

eine R-Algebra. (Wir schreiben y^α für das Monom $y_0^\alpha y_1^\alpha y_2^\alpha$) Dies entspricht geometrisch der Familie aller projektiven Kurven vom Rang d. Sie wird flach wenn wir ein beliebiges $x_\alpha \neq 0$ invertieren und entspricht dann der Lokalisierung $S[x_\alpha^{-1}]$ (was eine $R[x_\alpha^{-1}]$-Algebra ist). S ist im Gegenteil zu $S[x_\alpha^{-1}]$ nicht flach.

Definition 8.2.3. Sei R ein Ring und $I \subset R$ ein Ideal von R. Die *Rees-Algebra von R bezüglich I* ist die R-Algebra

$$\mathcal{R}(R, I) := \sum_{n=-\infty}^{\infty} I^n t^{-n} = R[t, t^{-1}I] \subset R[t, t^{-1}]$$

wobei $I^n := R$ falls $n \leq 0$.

Folgerung 8.2.4. *Sei R eine Algebra über einem Körper K, dann ist die Rees-Algebra $S := \mathcal{R}(R, I)$ flach über $K[t]$. Sei $\bigcap_{d=1}^{\infty} I^d = 0$ dann sind die Elemente der Form $1 - ts$ mit $s \in S$ keine Nullteiler von $\mathcal{R}(R, I)$.*

Beweis. Für den ersten Teil reicht es nach Lemma 8.1.7 zu zeigen, dass $\mathcal{R}(R, I)$ torsionsfrei als $K[t]$-Modul ist. Da $\mathcal{R}(R, I) \subset R[t, t^{-1}]$ folgt dies direkt.
Falls $p(1 - ts) = 0$ für $s \in S$, muss gelten, dass $p = qt \mod t$ für $q \in S$. Da aber t kein Nullteiler ist gilt $q(1 - ts) = 0$. Durch Wiederholung von diesem Argument bekommen wir das $p \in t^n S$ für alle n. Wenn man aber $p := \sum_{i=-j}^{j} p_i t^i$ für $p_i \in R$ schreibt zeigt sich das $p_i \in I^n$ für alle n sein muss, also ist $p = 0$ und somit die Aussage gezeigt. □

9 Vervollständigungen und das Henselsche Lemma Teil 1

Hanno Schülldorf

9.1 Einführung

Definition 9.1.1. Sei R eine abelsche Gruppe und sei $R = \mathfrak{m}_0 \supset \mathfrak{m}_1 \supset \mathfrak{m}_2 \ldots$ eine Folge von Untergruppen (eine absteigende Filtrierung). Wir definieren die **Vervollständigung** $\hat{R}$ von R bezüglich der $\mathfrak{m}_i$ als den inversen Grenzwert der Faktorgruppen $R/\mathfrak{m}_i$:

$$\hat{R} := \varprojlim R/\mathfrak{m}_i := \{g = (g_1, g_2, \ldots) \in \prod_i R/\mathfrak{m}_i \,|\, g_j \equiv g_i \mod \mathfrak{m}_i \quad \forall j > i\}.$$

Falls R ein Ring ist und die $\mathfrak{m}_i$ Ideale sind, dann ist jedes der $R/\mathfrak{m}_i$ ein Ring und somit ist auch $\hat{R}$ ein Ring. $\hat{R}$ hat eine Filtrierung nach Idealen

$$\hat{\mathfrak{m}}_i := \{g = (g_1, g_2, \ldots) \in \hat{R} \,|\, g_j = 0 \quad \forall j \leq i\},$$

und es folgt aus den Definitionen, dass $\hat{R}/\hat{\mathfrak{m}}_i = R/\mathfrak{m}_i$.
Der mit Abstand wichtigste Fall ist die $\mathfrak{m}$-adische Filtrierung (bei der R ein Ring ist mit der Filtrierung nach Idealen der Form $\mathfrak{m}_i = \mathfrak{m}^i$ für ein Ideal $\mathfrak{m}$ von R), für die wir $\hat{R}_\mathfrak{m}$ schreiben. In diesem Fall schreiben wir $\hat{\mathfrak{m}}$ für $\hat{\mathfrak{m}}_1$. Der Einfachheit halber werden wir uns von nun an auf die $\mathfrak{m}$-adische Filtrierung beschränken; die Generalisierung ist in den meisten Fällen aber nicht sehr schwierig.

Beispiel 9.1.2. Sei $p \in \mathbb{Z}$ eine Primzahl. Der Ring $\hat{\mathbb{Z}}_{(p)}$ heisst Ring der **p-adischen Zahlen**. Sei also $R = \mathbb{Z}$ und sei $\mathfrak{m} = p\mathbb{Z}$. Betrachte die Abbildung $\mathbb{Z} \to \hat{\mathbb{Z}}_{(p)}$ mit

$$x \mapsto (x + p\mathbb{Z}\,,\, x + p^2\mathbb{Z}\,, \ldots).$$

Eine p-adische ganze Zahl ist also ein Tupel, in dem der n-te Eintrag der Restklasse modulo der n-ten Potenz von p entspricht. Addition erfolgt nicht komponentenweise, sondern mit Übertrag, wenn man eine höhere Potenz von p überschreitet. Also ergibt z.B. im Ring der 2-adischen ganzen Zahlen

$$(1, 3, 7, 7, 7, \ldots) + (1, 1, 5, 13, 13, \ldots) = (0, 0, 4, 4, 20, \ldots).$$

Ein naheliegendes Ergebnis erhalten wir für Polynomringe:

Beispiel 9.1.3. Sei $R = S[x_1, \ldots, x_n]$ ein Polynomring über dem Ring S. Die Vervollständigung von S bezüglich des Ideals $\mathfrak{m} = (x_1, \ldots, x_n)$. ist der Ring der formalen Potenzreihen

$$\hat{R}_\mathfrak{m} \cong S[[x_1, \ldots, x_n]].$$

Denn durch die Abbildung $S[[x_1, \ldots, x_n]] \to R/\mathfrak{m}^i$, die f auf $f + \mathfrak{m}^i$ abbildet, erhalten wir eine Abbildung

$$S[[x_1, \ldots, x_n]] \to \hat{R}_\mathfrak{m}$$

mit der Abbildungsvorschrift

$$f \mapsto (f + \mathfrak{m}, f + \mathfrak{m}^2, \ldots) \in \hat{R}_\mathfrak{m} \subset \prod R/\mathfrak{m}^i.$$

Die Umkehrabbildung erhalten wir, wenn wir $(f_1 + \mathfrak{m}, f_2 + \mathfrak{m}^2, \ldots) \in \hat{R}_\mathfrak{m}$ (wobei die f_i Polynome sind und $f_i = f_j +$(Terme vom Grad $> \min\{i, j\}$) auf die Potenzreihe $f_1 + (f_2 - f_1) + (f_3 - f_2) + \ldots$. Dies ist eine wohldefinierte Potenzreihe, denn der Grad von $f_{i+1} - f_i$ ist mindestens $i + 1$, und zwar unabhängig von der Wahl von f_i in $f_i + \mathfrak{m}^i$.

Polynomringe und Potenzreihenringe werden im zweiten Teil des Kapitels, in dem das Henselsche Lemma besprochen wird, näher untersucht. Wir machen stattdessen weiter mit einer

Bemerkung 9.1.4. Wenn $\mathfrak{m}$ ein maximales Ideal von R ist, dann ist $\hat{R}_\mathfrak{m}$ ein lokaler Ring mit maximalem Ideal $\hat{\mathfrak{m}}$.

Beweis. Da $R/\mathfrak{m}$ ein Körper ist, ist auch $\hat{R}_{\hat{\mathfrak{m}}}/\hat{\mathfrak{m}}\hat{R}_{\hat{\mathfrak{m}}} = R/\mathfrak{m}$ ein Körper. Sei nun $G = (g_1, g_2, \ldots) \in \hat{R}_\mathfrak{m} \subset \prod_i R/\mathfrak{m}^i$ nicht in $\hat{\mathfrak{m}}$, also ist $g_1 \neq 0$, und somit sind alle g_i nicht in $\mathfrak{m}(R/\mathfrak{m}^i)$. Also ist jedes g_i eine Einheit in R. Aus der Bedingung $g_j \equiv g_i \mod \mathfrak{m}^i$ für $j > i$ folgt, dass $g_j^{-1} \equiv g_i^{-1} \mod \mathfrak{m}^i$ für $j > i$, und somit ist das Element $h := (g_1^{-1}, g_2^{-1}, \ldots)$ in $\hat{R}_\mathfrak{m}$ und das inverse Element zu g. □

Definition 9.1.5. Wenn die natürliche Abbildung $R \to \hat{R}_\mathfrak{m}$ ein Isomorphismus ist, so ist R **vollständig bezüglich** $\mathfrak{m}$. Wenn $\mathfrak{m}$ ein maximales Ideal ist, so ist R ein **vollständiger lokaler Ring**.

Zum Schluss dieser Einführung wollen wir noch kurz darauf eingehen, woher der Begriff "Vervollständigung" kommt. Es ist üblich, Elemente von $\hat{R}$ als Grenzwerte von Folgen oder Reihen von Elementen von R zu definieren. Wir sagen, dass eine Folge von Elementen $a_1, a_2 \ldots \in \hat{R}$. gegen ein Element $a \in \hat{R}$ **konvergiert**, wenn es für jedes $n \in \mathbb{N}$ ein $i(n) \in \mathbb{N}$ gibt, so dass $a - a_{i(n)} \in \hat{\mathfrak{m}}_n$. Es folgt, dass eine Folge (a_i) von Elemten aus $\hat{R}_\mathfrak{m}$ genau dann in $\hat{R}_\mathfrak{m}$ konvergiert, wenn die Folge eine Cauchy-Folge ist in dem Sinne, dass $\forall\, n \in \mathbb{N}\ \exists\, i(n) \in \mathbb{N}$, so dass

$$a_i - a_j \in \hat{\mathfrak{m}}_n\ \forall\, i, j \geq i(n). \tag{9.1.1}$$

Wenn $a_i \in R$, so ist diese Bedingung identisch zu $a_i - a_j \in \mathfrak{m}^n\ \forall\, i, j \geq i(n)$.

Der „Grenzwert“einer konvergenten Folge von Elementen aus $\hat{R}$ ist definiert als das Element aus $\prod_n R/\mathfrak{m}^n$, dessen n-te Koordinate die gleiche ist wie die von $a_{i(n)}$. Wir schreiben $a = \lim(a_i)$.

Der einfachste Weg, Folgen, die der Bedingung (7.1.1) genügen, aufzuschreiben, ist als Partialsumme von Elementen von R, deren i-ter Term in $\mathfrak{m}^i$ liegt:

$$a_i = \sum_{j=i}^{i} b_j, \quad b_i \in \mathfrak{m}^i.$$

In diesem Fall definieren wir die unendliche Summe $\sum_{j=1}^{\infty} b_i$ als den Grenzwert der a_i. Dies ist übrigens genau das, was wir im Fall der Potenzreihen machen - mit dem Ideal $\mathfrak{m}$, das von den Variablen eines Polynomrings erzeugt wird.

Proposition 9.1.6. *Sei R vollständig bzgl. eines Ideals $\mathfrak{m}$. Dann sind alle Elemente der multiplikativ abgeschlossenen Menge $U := \{1 - a \,|\, a \in \mathfrak{m}\}$ Einheiten in R.*

Beweis. Wenn $a \in \mathfrak{m}$, so ist $b = 1 + a + a^2 + \cdots$ eine Potenzreihe, die in R konvergiert. Das Produkt $(1-a)b$ ist der Grenzwert der Reihe $(1-a) + (1-a)a + (1-a)a^2 + \cdots$. Die i-te Partialsumme dieser Reihe ist $1 - a^i$, also konvergiert diese Reihe gegen 1. □

Folgerung 9.1.7. *Sei R ein lokaler Ring mit maximalem Ideal P. Dann ist der Ring der formalen Potenzreihen $R[[x_1, \ldots, x_n]]$ ein lokaler Ring mit dem maximalen Ideal $P + (x_1, \ldots, x_n)$.*

Beweis. Ein Element j, das nicht in $P + (x_1, \ldots, x_n)$ liegt, hat einen konstanten Term u ausserhalb von P, also ist u eine Einheit. Das Element $u^{-1}f$ ist von der Form $1 + g(x)$ mit $g(x) \in (x_1, \ldots, x_n)$. Also ist $u^{-1}f$ eine Einheit, und somit auch f. □

9.2 Eigenschaften von Vervollständigungen

In diesem Abschnitt wollen wir uns einigen Eigenschaften und Anwendungen von Vervollständigungen zuwenden. Zunächst behandeln wir den Zusammenhang zwischen vollständigen Ringen und den assoziierten graduierten Ringen, danach werden wir zeigen, dass mit R auch $\hat{R}$ noethersch ist. Später werden wir noch exakte Sequenzen und Flachheit behandeln.

Zuerst beobachten wir, dass aus $\hat{R}/\hat{\mathfrak{m}}_n = R/\mathfrak{m}^n$ die Gleichung $\hat{R} = \lim \hat{R}/\hat{\mathfrak{m}}_n$ folgt; also ist $\hat{R}$ vollständig bezüglich der Filtrierung nach den $\hat{\mathfrak{m}}_n$. Darüber hinaus, wenn wir $\operatorname{gr} \hat{R}$ für den assoziierten graduierten Ring bezüglich dieser Filtrierung schreiben, induziert die natürliche Abbildung $R \to \hat{R}$ einen Isomorphismus $\operatorname{gr}_{\mathfrak{m}} R = \operatorname{gr} \hat{R}$.

Proposition 9.2.1. *Sei R ein vollständiger Ring bezüglich einer Filtrierung nach Idealen $\mathfrak{m}_i$. Sei $\operatorname{gr} R$ der assoziierte graduierte Ring von R bezüglich dieser Filtrierung und für $a \in R$ bezeichne $\operatorname{in}(a)$ die Initialform bezüglich dieser Filtrierung. Sei $I \subset R$ ein Ideal in $\operatorname{gr} R$ und $a_1, \ldots, a_s \in I$. Wenn $\operatorname{in}(a_1), \ldots, \operatorname{in}(a_s)$ das Ideal $\operatorname{in}(I)$ in $\operatorname{gr} R$ erzeugen, dann erzeugen $a_1, \ldots, a_s$ das Ideal I.*

Beweis. Sei $I' = (a_1, \ldots, a_s)$. OBdA sei $a_i \neq 0$ fr $1 \leq i \leq s$. Dann können wir ein $d \in \mathbb{N}$ wählen, so dass $a_i \notin \mathfrak{m}_d$ fr $1 \leq i \leq s$. Sei nun $f \in I$ mit Initialform $\mathrm{in}(f)$ vom Grad e. Dann können wir die Initialform von f schreiben als $\mathrm{in}(f) = \sum_j G_j \mathrm{in}(a_j)$ mit $G_j \in \mathrm{gr}_{\mathfrak{m}} R$ homogen vom Grad $\deg(\mathrm{in}(f)) - \deg(\mathrm{in}(a_j))$ und vom Grad 0, falls $\deg(\mathrm{in}(f)) - \deg(\mathrm{in}(a_j)) < 0$. Wenn wir nun $g_j \in R$ so wählen, dass $\mathrm{in}(g_j) = G_j$ ist, so liegt $f - \sum_j g_j a_j$ in $\mathfrak{m}_{e+1}$. Dies wiederholen wir, bis wir schliesslich ein Element $f' \in I'$ erhalten, so dass $f - f' \in \mathfrak{m}_{d+1}$ ist. Und wenn wir soweit sind, dann gilt für die oben definierten G_j, dass $\deg(G_j) \geq e - d > 0$, und somit können wir $g_j \in \mathfrak{m}_{e-d}$ wählen. Dies wiederholen wir erneut und definieren $g_j^{(i)} \in \mathfrak{m}_{e-d+i}$ so, dass

$$f - \sum_j g_j^{(0)} a_j - \sum_j g_j^{(1)} a_j - \sum_j g_j^{(2)} a_j - \ldots - \sum_j g_j^{(n)} a_j = f - \sum_j \sum_{i=0}^{n} g_j^{(i)} a_j \in \mathfrak{m}_{e+n+1}.$$

Die Reihe $\sum_{i=0}^{\infty} g_j^{(i)}$ konvergiert in R, ihr Grenzwert sei h_j. Weil Grenzwerte endliche Summen und Produkte erhalten, erhalten wir $f = \sum_j h_j a_j \in I'$. Also wird das Ideal I von $a_1, \ldots, a_s$ erzeugt. □

Wir betrachten nun die $\mathfrak{m}$-adische Filtrierung $\mathfrak{m}^i$ von R und die Vervollständigung $\hat{R} = \hat{R}_{\mathfrak{m}}$. Sei $\hat{\mathfrak{m}}_n$ der Kern der natürlichen Abbildung $\hat{R} \to R/\mathfrak{m}^n$. Damit besteht $\hat{\mathfrak{m}}_n$ aus allen Elementen von $\hat{R} \subset \prod_j R/\mathfrak{m}^j$, deren Komponente in $R/\mathfrak{m}^j$ in $\mathfrak{m}^n$ liegt für alle j (und daher 0 sind, falls $j \leq n$). Beachte, dass $\mathfrak{m}^n \hat{R} \subset (\hat{\mathfrak{m}}_1)^n \subset \hat{\mathfrak{m}}_n$. Das folgende Resultat zeigt unter anderem, dass im noetherschen Fall Gleichheit herrscht.

Satz 9.2.2. *Sei R ein noetherscher Ring und sei $\mathfrak{m}$ ein Ideal von R. Sei $\hat{R}$ die Vervollständigung von R bezüglich $\mathfrak{m}$. Dann gilt:*

(i) *$\hat{R}$ ist ein noetherscher Ring.*

(ii) *$\hat{R}/\mathfrak{m}^j \hat{R} = R/\mathfrak{m}^j$. Also ist $\hat{R}$ vollständig bezüglich $\mathfrak{m}\hat{R}$, und $\mathrm{gr}_{\mathfrak{m}\hat{R}} \hat{R} = \mathrm{gr}_{\mathfrak{m}} R$.*

Beweis. (i) Wie oben schon erwähnt, ist $\mathrm{gr}\, \hat{R} = \mathrm{gr}_{\mathfrak{m}} R$. Da R ein noetherscher Ring ist, ist auch $R/\mathfrak{m}$ noethersch und $\mathfrak{m}/\mathfrak{m}^2$ ist ein endlich erzeugter R-Modul. Der Ring $\mathrm{gr}_{\mathfrak{m}} R$ wird erzeugt als $R/\mathfrak{m}$-Algebra von jeder Erzeugermenge für $\mathfrak{m}/\mathfrak{m}^2$. Nach dem Hilbertschen Basissatz ist $\mathrm{gr}_{\mathfrak{m}} R$ noethersch. Sei nun $I \subset \hat{R}$ ein Ideal von $\hat{R}$. Dann wird das Ideal $\mathrm{in}(I)$ von den Initialformen endlich vieler Elemente $a_1, \ldots, a_s \in I$ erzeugt. Es folgt nach Proposition 9.2.1, dass die a_i das Ideal I erzeugen, also ist I endlich erzeugt.

(ii) Wieder verwenden wir, dass $\mathrm{gr}\, \hat{R} = \mathrm{gr}_{\mathfrak{m}} R$. Um zu zeigen, dass $\hat{R}/\mathfrak{m}^j \hat{R} = R/\mathfrak{m}^j$ gilt, zeigen wir, dass $\hat{\mathfrak{m}}_n = \mathfrak{m}^n \hat{R}_{\mathfrak{m}}$. Dazu genügt es nach Proposition 9.2.1 zu zeigen, dass die beiden Ideale die gleichen Initial-Ideale in $\mathrm{gr}\, \hat{R}$ besitzen. Dies ist aber offensichtlich der Fall, da beide Initial-Ideale aus allen Elementen vom Grad $\geq n$ bestehen. Also sind die beiden Ringe gleich. Daraus folgt nun auch direkt die andere Aussage.

□

Jetzt wenden wir uns der Frage nach der Flachheit von vollständigen Ringen zu. Dazu benötigen wir zwei Resultate, von denen das erste uns ein Kriterium dafür liefert, unter welchen Bedingungen zwei Filtrierungen die gleiche Vervollständigung ergeben. Das zweite Resultat untersucht, inwiefern Vervollständigungen exakte Sequenzen erhalten.

Sei also $R = \mathfrak{n}_0 \supset \mathfrak{n}_1 \supset \ldots$ eine weitere Filtrierung von R. Die entsprechenden Vervollständigungen bezeichnen wir mir $\hat{R}_\mathfrak{m}$ bzw. $\hat{R}_\mathfrak{n}$. Das folgende Lemma besagt, dass zwei Filtrierungen die gleiche Vervollständigung liefern, wenn sie im folgenden Sinn vergleichbar sind:

Lemma 9.2.3. *Wenn für jedes $\mathfrak{n}_j$ ein $\mathfrak{m}_i$ existiert, so dass $\mathfrak{m}_i \subset \mathfrak{n}_j$ und für jedes $\mathfrak{m}_j$ ein $\mathfrak{n}_i$ existiert, so dass $\mathfrak{n}_i \subset \mathfrak{m}_j$, dann gibt es einen natürlichen Isomorphismus $\hat{R}_\mathfrak{m} \cong \hat{R}_\mathfrak{n}$.*

Beweis. Betrachten wir zunächst den einfachen Fall, dass die $\mathfrak{n}_j$ einfach Teilmengen der $\mathfrak{m}_i$ sind. Die Bedingung des Lemmas besagt, dass in diesem Fall unendlich viele $\mathfrak{m}_i$ unter den $\mathfrak{n}_j$ sein müssen. In diesem Fall induziert die Projektion auf das Unterprodukt

$$\prod_i R/\mathfrak{m}_i \to \prod_j R/\mathfrak{n}_j$$

einen natürlichen Isomorphismus $\hat{R}_\mathfrak{m} \cong \hat{R}_\mathfrak{n}$.
Im allgemeinen Fall können wir injektive Abbildungen $\alpha, \beta, \gamma : \mathbb{N} \to \mathbb{N}$ wählen, so dass $\mathfrak{m}_j \supset \mathfrak{n}_{\alpha(i)} \supset \mathfrak{m}_{\beta(j)} \supset \mathfrak{n}_{\gamma(j)}$, und diese Abbildungen induzieren Abbildungen $R/\mathfrak{n}_{\gamma(j)} \to R/\mathfrak{m}_{\beta(j)} \to R/\mathfrak{n}_{\alpha(j)} \to R/\mathfrak{m}_j$ und somit natürliche Abbildungen wie folgt:

$$\begin{array}{ccccccc} \hat{R}_\mathfrak{n} & & \hat{R}_\mathfrak{m} & & \hat{R}_\mathfrak{n} & & \hat{R}_\mathfrak{m} \\ \| & & \| & & \| & & \| \\ \varprojlim R/\mathfrak{n}_\gamma^j & \to & \varprojlim R/\mathfrak{m}_\beta^j & \to & \varprojlim R/\mathfrak{n}_\alpha^j & \to & \varprojlim R/\mathfrak{m}_j \end{array}$$

Da die unteren Isomorphismen oben schon behandelt wurden, sind wir fertig. □

Im nächsten Schritt untersuchen wir, unter welchen Bedingungen Vervollständigungen exakte Sequenzen erhalten. Im allgemeinen ist die Grenzwertbildung nicht rechts-exakt.

Lemma 9.2.4. *Sei R ein noetherscher Ring und $\mathfrak{m}$ ein Ideal von R. Sei $0 \to A \to B \to C \to 0$ eine kurze exakte Sequenz von endlich erzeugten R-Moduln. Dann ist auch*

$$0 \to \varprojlim A/\mathfrak{m}^j A \to \varprojlim B/\mathfrak{m}^j B \to \varprojlim C/\mathfrak{m}^j C \to 0$$

eine kurze exakte Sequenz. Die Vervollständigung bezüglich der $\mathfrak{m}$-adischen Filtrierung erhält also exakte Sequenzen von endlich erzeugten Moduln.

Beweis. Die zweite Aussage folgt aus der ersten, weil jede exakte Sequenz

$$\ldots \to A_{n+1} \xrightarrow{\varphi_n} A_n \to A_{n-1} \to \ldots$$

als „Komposition“von kurzen exakten Sequenzen geschrieben werden kann:

$$0 \to \mathrm{im}\varphi_{n+1} \to A_n \to \mathrm{im}\varphi_n \to 0.$$

Um die erste Aussage zu beweisen, zeigen wir zunächst, dass $\varprojlim B/\mathfrak{m}^j B \to \varprojlim C/\mathfrak{m}^j C$ ein Epimorphismus ist: Sei dazu $(c_j + \mathfrak{m}^j C) \in \varprojlim C/\mathfrak{m}^j C$. Wir müssen zeigen, dass es ein Element $(b_j + \mathfrak{m}^j B) \in \varprojlim B/\mathfrak{m}^j B$ gibt, das auf $c_j + \mathfrak{m}^j C$ abgebildet wird. Das bedeutet, dass es eine Folge von Elementen $b_j \in B$ gibt, so dass

(i) $b_j \mapsto c_j \mod \mathfrak{m}^j C$ und

(ii) $b_j \equiv c_j \mod \mathfrak{m}^j B$ für $i < j$ (es reicht, dies für $i = j - 1$ zu zeigen).

Dies beweisen wir induktiv: nachdem wir $b_1, \ldots, b_j$ so gewählt haben, dass sie (i) und (ii) genügen, nehmen wir uns ein beliebiges Element b'_{j+1}, das auf $c_{j+1} \mod \mathfrak{m}^{j+1} C$ abgebildet wird. Sowohl b'_{j+1} als auch b_j werden auf dasselbe Element c_j abgebildet. Aber da die Sequenz $A/\mathfrak{m}^j A \to B/\mathfrak{m}^j B \to C/\mathfrak{m}^j C \to 0$ exakt ist (weil tensieren rechtsexakt ist), gibt es ein Element $A_{j+1} \in A$ mit $a_{j+1} \mapsto b_j - b'_{j+1} \mod \mathfrak{m}^j$. Das Element $b_{j+1} := bj + 1' + a_{j+1}$ erfüllt beide Bedingungen. Es bleibt zu zeigen, dass

$$0 \to \varprojlim A/\mathfrak{m}^j A \to \varprojlim B/\mathfrak{m}^j B \to \varprojlim C/\mathfrak{m}^j C \tag{9.2.2}$$

exakt ist. Dazu wäre es schön, wenn wir $\varprojlim A/\mathfrak{m}^j A$ durch $\varprojlim A/(A \cap \mathfrak{m}^j B)$ ersetzen könnten, denn die Sequenz 9.2.2 würde dann zum Grenzwert der exakten Sequenz

$$0 \to \varprojlim A/(A \cap \mathfrak{m}^j B) \to \varprojlim B/\mathfrak{m}^j B \to \varprojlim C/\mathfrak{m}^j C,$$

und es ist nicht schwer zu zeigen, dass dieser Grenzwert exakt ist (also dass der inverse Limes von links-exakten Sequenzen links-exakt ist). Um diese Umformung machen zu können, müssen wir zeigen, dass die Filtrierung von A durch die Untermoduln $A \cap \mathfrak{m}^j B$ die gleiche Vervollständigung ergibt wie die Filtrierung durch die Untermoduln $\mathfrak{m}^j A$. Es ist klar, dass $A \cap \mathfrak{m}^j B \supset \mathfrak{m}^j A$. Und nach dem Artin-Rees-Lemma 7.1.2 gibt es ein $k \in \mathbb{N}$, so dass $A \cap \mathfrak{m}^j B = \mathfrak{m}^{j-k}(A \cap \mathfrak{m}^k B) \subset \mathfrak{m}^{j-k} A$. Also ergeben nach Lemma 9.2.3 beide Filtrierungen die gleiche Vervollständigung, also können wir die gewünschte Umformung vornehmen. Und der Beweis, dass

$$0 \to \varprojlim A/(A \cap \mathfrak{m}^j B \to \varprojlim B/\mathfrak{m}^j B \to \varprojlim C/\mathfrak{m}^j C$$

links-exakt ist, folgt direkt aus der Definition des inversen Limes: wenn $(b_1, b_2, \ldots) \in \varprojlim B/\mathfrak{m}^j B$ gegen $(0, 0, \ldots) \in \varprojlim C/\mathfrak{m}^j C$. konvergiert, dann konvergiert jedes b_j gegen 0 in $C/\mathfrak{m}^j C$. Also ist $b_j \in A/A \cap \mathfrak{m}^j B$ und $(b_1, b_2, \ldots) \in \varprojlim A/A \cap \mathfrak{m}^j B$, was zu zeigen war. □

Zum Schluss folgt nun eines der wichtigsten Resultate über Vervollständigungen, das ausserordentlich nützlich ist, wenn es um den Informationstransfer zwischen dem Ring R und seiner Vervollständigung $\hat{R}$ geht.

Satz 9.2.5. *Sei R ein noetherscher Ring und sei $\mathfrak{m}$ ein Ideal von R. Sei $\hat{R}$ die Vervollständigung von R bezüglich $\mathfrak{m}$. Dann gilt:*

(i) *Wenn M ein endlich erzeugter R-Modul ist, dann ist die natürliche Abbildung*

$$\hat{R} \otimes_R M \to \varprojlim M/\mathfrak{m}^j M =: \hat{M}$$

ein Isomorphismus. Insbesondere, wenn S ein Ring ist, der endlich erzeugt als R-Modul ist, ist $\hat{R} \otimes_R S$ die Vervollständigung von S bezüglich des Ideals $\mathfrak{m}S$.

(ii) *$\hat{R}$ ist flach als R-Modul.*

Beweis. (i) Wir beginnen zunächst mit dem Fall $M = R$, bei dem die Aussage des Satzes einfach die Definition von $\hat{R}$ ist. Per Definition kommutiert $\varprojlim$ mit endlich-diskreten Summen, also ist die Aussage wahr für endlich erzeugte freie Moduln. Nun sei M ein beliebiger endlich erzeugter Modul und sei $F \to G \to M \to 0$ eine freie Präsentierung von M. Da $\varprojlim$ nach Lemma 9.2.4 exakte Sequenzen erhält, folgt, dass im folgenden Diagramm die obere Zeile rechts-exakt ist.

$$\begin{array}{ccccccc} \hat{F} & \to & \hat{G} & \to & \hat{M} & \to & 0 \\ \uparrow & & \uparrow & & \uparrow & & \\ \hat{R} \otimes_R F & \to & \hat{R} \otimes_R G & \to & \hat{R} \otimes_R M & \to & 0 \end{array}$$

Die untere Zeile ist rechts-exakt wegen der Rechts-Exaktheit des Tensor-Produkts, und wie wir bereits gezeigt haben, sind die linken vertikalen Abbildungen Isomorphismen. Also muss auch die rechte vertikale Abbildung ein Isomorphismus sein.

(ii) Nach Satz 6.1 in [4] genügt es zu zeigen, dass die Abbildung

$$I \otimes_R \hat{R} \to I\hat{R} \subset \hat{R}$$

ein Monomorphismus für endlich erzeugte Ideale ist. Nach Teil (i) müssen wir also zeigen, dass die Abbildung $\hat{I} \to \hat{R}$ ein Monomorphismus ist. Dies folgt aber direkt aus Lemma 9.2.4.

□

10 Vervollständigungen und das Henselsche Lemma Teil 2

Thomas Klöppel

10.1 Das Henselsche Lemma

Im vorigen Abschnitt dieses Kapitels haben wir Vervollständigungen definiert, grundlegende Eigenschaften herausgearbeitet und einige Anwendungen besprochen. In diesem Abschnitt wird ein weiteres wichtiges Ergebnis für vollständige Ringe dargestellt, das Henselsche Lemma, dessen Grundidee eng mit dem Newton-Verfahren verwandt ist. Bevor wir diesen Satz beweisen können, benötigen wir noch ein weiteres Ergebnis, das Eigenschaften von Abbildungen zwischen dem Ring der formalen Potenzreihen $R[[x_1, \ldots, x_n]]$ und einer vollständigen R-Algebra S beschreibt.

Satz 10.1.1. *Sei R ein Ring und sei S eine vollständige R-Algebra bezüglich eines Ideals $\mathfrak{n}$. Für beliebig vorgegebene $f_1, \ldots, f_n \in \mathfrak{n}$ gilt:*

(i) *Es existiert ein eindeutig bestimmter R-Algebra Homomorphismus*

$$\varphi : R[[x_1, \ldots, x_n]] \to S,$$

der für alle i die Unbestimmte x_i auf f_i abbildet und konvergente Folgen erhält. Die Abbildung φ bildet Potenzreihen $g(x_1, \ldots, x_n)$ auf $g(f_1, \ldots, f_n) \in S$ ab.

(ii) *Falls die induzierte Abbildung $R \to S/\mathfrak{n}$ ein Epimorphismus ist und die Elemente $f_1, \ldots, f_n$ das Ideal $\mathfrak{n}$ erzeugen, dann ist auch φ ein Epimorphismus.*

(iii) *Falls die induzierte Abbildung von assoziierten graduierten Ringen*

$$\mathrm{gr}\varphi : R[x_1, \ldots, x_n] \cong \mathrm{gr}_{(x_1,\ldots,x_n)} R[[x_1, \ldots, x_n]] \to \mathrm{gr}_{\mathfrak{n}} S$$

ein Monomorphismus ist, so ist φ ein Monomorphismus.

Beweis. (i) Die eindeutig definierte Abbildung von R-Algebren $R[x_1, \ldots, x_n] \to S/\mathfrak{n}^t$, die x_i auf die Klasse von f_i abbildet, ist bereits durch die Abbildung über dem faktorisierten Definitionsbereich

$$R[[x_1, \ldots, x_n]]/(x_1, \ldots, x_n)^t = R[x_1, \ldots, x_n]/(x_1, \ldots, x_n)^t \to S/\mathfrak{n}^t$$

vollständig beschrieben. Es wird also eine eindeutig bestimmte Abbildung $R[[x_1,\dots,x_n]] \to S/\mathfrak{n}^t$ induziert, die x_i auf die Klasse von f_i abbildet. Da S als inverser Grenzwert der $S/\mathfrak{n}^t$ angesehen werden kann, existiert eine eindeutig bestimmte Abbildung $\varphi : R[[x_1,\dots,x_n]] \to S$, die wie gewünscht x_i auf f_i abbildet.
Das Bild von $g + (x_1,\dots,x_n)^t$ in $S/\mathfrak{n}^t$ ist $g(f_1,\dots,f_n) + \mathfrak{n}^t$ für jedes t, also ist das Bild von g in S durch $g(f_1,\dots,f_n)$ gegeben, da S ist vollständig bezüglich des Ideals $\mathfrak{n}$ ist.

(ii) Aus den Voraussetzungen des Satzes folgt direkt, dass die Abbildung

$$(x_1,\dots,x_n)/(x_1,\dots,x_n)^2 \to \mathfrak{n}/\mathfrak{n}^2$$

surjektiv ist und somit die Abbildung

$$\mathrm{gr}\varphi : \mathrm{gr}_{(x_1,\dots,x_n)}R \to \mathrm{gr}_{\mathfrak{n}}S$$

ebenfalls. Betrachte nun ein beliebiges Element $g \in S$, $g \neq 0$. Dann gibt es, da S vollständig ist und somit $\bigcap \mathfrak{n}^j = 0$, eine größte Zahl i mit $g \in \mathfrak{n}^i$. Da die Abbildung $\mathrm{gr}\varphi$ surjektiv ist, können wir ein $g_1 \in (x_1,\dots,x_n)^i$ wählen, dessen Initialform auf die Initialform von g abgebildet wird. Daraus folgt, dass $g - \varphi(g_1) \in \mathfrak{n}^{i+1}$.
Iteriert man diesen Prozess, so erhält man eine Folge von Elementen $g_j \in (x_1,\dots,x_n)^{i+j-1}$, so dass $g = \sum_{j=1}^{\infty} \varphi(g_j)$. Die Abbildung φ erhält unendliche Summen, was auf $g = \varphi(\sum_{j=1}^{\infty} g_j)$ führt, d. h. φ ist surjektiv.

(iii) Falls $0 \neq g \in R[[x_1,\dots,x_n]]$, dann ist $\mathrm{in}(g)$ nicht das Nullmonom. Sei d der Grad dieses Monoms. Nach Voraussetzung gilt damit

$$\mathrm{gr}\varphi(\mathrm{in}(g)) \neq 0$$

in dem Summand des graduierten Rings $\mathrm{gr}_{\mathfrak{n}}S$ mit Grad d. Andererseits gilt

$$g \equiv \mathrm{in}(g) \mod (x_1,\dots,x_n)^{d+1},$$

also gilt auch die Äquivalenz $\varphi(g) \equiv \mathrm{gr}\varphi(\mathrm{in}(g)) \mod \mathfrak{n}^{d+1}$ und daher $\varphi(g) \neq 0$.

□

Bevor wir zum Henselschen Lemma kommen, wollen wir noch eine Folgerung dieses Ergebnisses für Endomorphismen im Ring der formalen Potenzreihen in einer Unbekannten zeigen.

Folgerung 10.1.2. *Sei $f \in xR[[x]]$ eine formale Potenzreihe. Falls φ der Endomorphismus ist, der auf R die Identität darstellt und x auf f abbildet, also*

$$\varphi : R[[x]] \to R[[x]]; \quad x \mapsto f,$$

dann ist φ isomorph genau dann, wenn $f'(0)$ eine Einheit in R ist. Dabei ist die Ableitung von f ausgewertet in der 0 durch die Beziehung $f(x) = f'(0)x + (Terme\ hhere\ Ordnung)$ erklärt.

Beweis. Sei zunächst φ ein Isomorphismus. Die Elemente aus $R[[x]]\backslash(x)$ besitzen einen nichtverschwindenden konstanten Term. Nach Konstruktion von φ erhält diese Abbildung diese Teilmenge und, da es sich um einen Isomorphismus handelt, folgt $\varphi((x)) = (x)$. Insbesondere ist das Bild $\varphi(x) = f$ des Erzeugenden x von (x) ebenfalls ein erzeugendes Element von (x). Daraus können wir schließen, dass $f + (x^2)$ die Menge $(x)/(x^2)$ erzeugt. Aus $f \equiv f'(0)x \mod (x^2)$ folgt dann, dass $f'(0)$ eine Einheit in R ist.
Für die Umkehrung nehmen wir nun an, dass $f'(0) = u$ eine Einheit von R ist. Wir wissen, dass $\mathrm{gr}_{(x)}R[[x]] = R[x]$ und dass

$$\mathrm{gr}\varphi : R[x] \to R[x]; \quad x \mapsto ux$$

ein Isomorphismus ist. Nach Satz 10.1.1 ist somit φ injektiv. Um die Surjektivität einzusehen schreiben wir $f = ux + hx^2 = (u + hx)x$ für ein $h \in R[[x]]$. Da $u + hx$ eine Einheit in $R[[x]]$ ist, sehen wir, dass f das Ideal (x) erzeugt. Nun wenden wir wieder 10.1.1 an und erhalten die Surjektivität von φ. Damit ist φ ein Isomorphismus. □

Nun haben wir alle Werkzeuge bereitgestellt um das Henselsche Lemma zu beweisen.

Satz 10.1.3. ***Das Henselsche Lemma***
Sei R ein Ring, der vollständig ist bezüglich eines Ideals $\mathfrak{m}$, und sei $f(x) \in R[x]$ ein Polynom. Falls a eine näherungsweise Wurzel von f im Sinne von

$$f(a) \equiv 0 \mod f'(a)^2\mathfrak{m}$$

darstellt, dann existiert eine Wurzel b von f in der Nähe von a, das heißt

$$f(b) = 0 \qquad \textit{und} \qquad b \equiv a \mod f'(a)\mathfrak{m}.$$

Darüber hinaus ist b eindeutig bestimmt, falls $f'(a)$ kein Nullteiler von R ist.

Beweis. Zur Vereinfachung setzen wir $f'(a) = e$. Wir können $h(x)$ derart wählen, dass

$$f(a + ex) = f(a) + f'(a)ex + h(x)(ex)^2 = f(a) + e^2(x + x^2h(x)).$$

Nach Satz 10.1.1 existiert ein Ringhomomorphismus $\varphi : R[[x]] \to R[[x]]$, der auf R die Identität ist und x auf $x + x^2h(x)$ abbildet. Nach Folgerung 10.1.2 ist φ ein Isomorphismus. Wenden wir nun φ^{-1} auf die obige Gleichung an, so erhalten wir

$$f(a + e\varphi^{-1}(x)) = f(a) + e^2x.$$

Nach Voraussetzung können wir $f(a) = e^2c$ für ein $c \in \mathfrak{m}$ schreiben. Nach Satz 10.1.1 existiert ein Algebrahomomorphismus ψ, der wiederum die Identität auf R ist und x auf $-c$ abbildet. Wenden wir es nun diese Gleichung an, ergibt sich

$$f(a + e\psi\varphi^{-1}(x)) = 0.$$

Damit ist $b = a + e\psi\varphi^{-1}(x)$ das gewünschte Element.
Nun nehmen wir an, dass e kein Nullteiler ist und zeigen die Eindeutigkeit des Elementes

b. Dazu nehmen wir an, dass b und b_1 zwei Wurzeln von f sind, die sich beide von a nur um Elemente von $e\mathfrak{m}$ unterscheiden, also $b = a+er$ und $b_1 = a+er_1$ mit $r, r_1 \in \mathfrak{m}$. Nach Satz 10.1.1 existieren Homomorphismen von Ringen $\beta, \beta_1 : R[[x]] \to R[[x]]$, die jeweils auf R die Identität sind und $\beta(x) = r$ bzw. $\beta_1(x) = r_1$. Wenden wir nun die beiden Abbildungen auf die obigen Gleichungen an:

$$\begin{aligned} 0 &= f(a+er) = f(a) + e^2(r + r^2h(r)), \\ 0 &= f(a+er_1) = f(a) + e^2(r_1 + r_1^2h(r_1)). \end{aligned}$$

Subtrahieren wir diese beiden Gleichungen und beachten, dass e kein Nullteiler ist, so erhalten wir $r + r^2h(r) = r_1 + r_1^2h(r_1)$, was äquivalent ist zu $\beta\varphi(x) = \beta_1\varphi(x)$. Aus der in Satz 10.1.1 gezeigten Eindeutigkeit einer solchen Abbildung können wir nun $\beta\varphi = \beta_1\varphi$ schließen. Da aber φ ein Isomorphismus ist, heißt das $\beta = \beta_1$ und damit $r = r_1$. Damit ist die Eindeutigkeit des Elementes b gezeigt. □

Wir wollen an dieser Stelle direkt anhand eines kleinen Beispieles zeigen, dass manche Fragestellungen mithilfe des Henselschen Lemmas stark vereinfacht werden können.

Beispiel 10.1.4. Wir betrachten dazu die in Abschnitt 7.1 eingeführten p-adischen ganzen Zahlen $\hat{\mathbb{Z}}_{(p)}$. Das Henselsche Lemma gibt uns ein vollständiges und einfach zu überprüfendes Kriterium, ob ein Element c eine Quadratwurzel besitzt.
Wir können $c \in \hat{\mathbb{Z}}_{(p)}$ eindeutig als $c = p^n b$ für ein $n \in \mathbf{N}$ und für ein nicht durch p teilbares Element b schreiben. Damit ist c genau dann eine Quadratzahl, wenn n gerade ist und b eine Quadratzahl ist. Wir müssen also entscheiden, ob b ein Quadrat ist. Falls $b = a^2$, dann ist auch das Bild $\bar{b}$ von b im Körper $\hat{\mathbb{Z}}_{(p)}/p\hat{\mathbb{Z}}_{(p)} = \mathbb{Z}/(p)$ das Quadrat des Bildes $\bar{a}$ von a.
Für die Umkehrung betrachten wir nun das Polynom $f(x) = x^2 - b \in \hat{\mathbb{Z}}_{(p)}[x]$. Die Ableitung ist durch $f'(x) = 2x$ gegeben. Ist nun b eine Quadratzahl $\mod p$, sprich $b \equiv a^2 \mod p$, dann hat also $\bar{f}(x)$ das Element a als Wurzel. Wir betrachten nun zwei Fälle:

- $p \neq 2$:
  $f'(\bar{a}) = 2\bar{a} \neq 0$ im Körper $\mathbb{Z}/p\mathbb{Z}$. Somit können wir das Henselsche Lemma anwenden und schließen, dass b eine p-adische Quadratwurzel besitzt.

- $p = 2$:
  Nehmen wir an, dass $b \equiv 1 \mod 8$. Dann können wir $a = 1$ wählen und erhalten $f'(a) = 2$ und $f(a) = 1 - b \equiv 0 \mod (2^2p = 8)$. Daher können wir auch hier das Henselsche Lemma anwenden und erkennen, dass b in diesem Fall eine 2-adische Quadratwurzel besitzt. Die Bedingung $b \equiv 1 \mod 8$ ist keine echte Einschränkung, denn, falls b eine Quadratwurzel besitzt, dann gilt $b = (1+2a)^2 = 1 + 4(a + a^2)$, da b ungerade ist. Das Element $a + a^2$ ist aber immer durch 2 teilbar und somit gilt die geforderte Äquivalenz für b.

In beiden Fällen sehen wir, dass eine leicht zu überprüfende Bedingung, tatsächlich ausreicht zu entscheiden, ob b eine Quadratwurzel beitzt.

Bemerkung 10.1.5. Ein Ring muss nicht unbedingt vollständig sein um das Henselsche Lemma zu erfüllen. Zum Beispiel kann man zeigen, dass Ringe von konvergenten Potenzreihen über $\mathbf{R}$ oder $\mathbf{C}$ ebenfalls diese Eigenschaft haben. Daher definiert man einen Ring R mit maximalem Ideal $\mathfrak{m}$ als **henselsch**, wenn er das Henselsche Lemma erfüllt. Zu jedem beliebigen Ring R mit maximalem Ideal $\mathfrak{m}$ existiert ein Ring S, der R enthält und henselsch ist bezüglich $\mathfrak{m}S$. S wird dann **Henselisierung von R bezüglich $\mathfrak{m}$.**

Bevor wir in den nächsten beiden Abschnitten tieferliegende Anwendungen des Henselschen Lemmas vorstellen werden, wollen wir hier einen Spezialfall des Satz über die impliziten Funktion als direkte Folgerung zeigen.

Folgerung 10.1.6. *Sei $f(t,x)$ ein Polynom in zwei Unbestimmten über einem Körper k und sei $x=a$ ein einfache Nullstelle von $f(0,x)$. Dann existiert eine eindeutig bestimmte Potenzreihe $x(t)$ mit $x(0)=a$ und $f(t,x(t))=0$.*

Beweis. Wende Satz 10.1.3 mit $R=k[[t]]$ und $\mathfrak{m}=(t)$ an. Dann ist $f\in R[x]$. Da a eine einfache Nullstelle des Polynoms ist, gilt $f'(a)\not\equiv 0 \mod \mathfrak{m}$ und somit $f'(a)\neq 0$. Aus $f(a)\equiv 0 \mod f'(a)^2\mathfrak{m}$ folgt dann mit Hilfe des Henselschen Lemmas die Existenz von $x(t)$. □

10.2 Heben von idempotenten Elementen

Definition 10.2.1. Sei A eine (nicht notwendigerweise kommutative) Algebra über einem kommutativen Ring R und seien $e_1,\ldots,e_n\in A$. Die e_i heißen **idempotent**, falls $e_i^2=e_i$. Man bezeichnet die e_i als **orthogonale idempotente** Elemente, falls zusätzlich $e_ie_j=e_je_i=0$ für $i\neq j$ gilt. Die Elemente 0 und 1 heißen **triviale Idempotente.** Eine Menge $\{e_1,\ldots,e_n\}$ von orthogonaler idempotenter Elemente heißt **vollständig**, falls $\sum e_i=1$. Jede nichtvollständige Menge $\{e_1,\ldots,e_n\}$ orthogonaler idempotenter Elemente kann durch Hinzufügen des Elementes $f:=1-\sum e_i$ vervollständigt werden.

Beispiel 10.2.2. Sei M ein R-Modul, dass sich als direkte Summe von Untermodulen $M=\bigoplus_{i=1}^n M_i$ schreiben lässt. Sei $A=\mathrm{Hom}_R(M,M)$ die Endomorphismenalgebra von M. Definiere $e_i\in A$ als Projektion von M auf das Submodul M_i mit Kern $\bigoplus_{i\neq j}M_j$. Dann bilden die e_i ein vollständige Menge von orthogonalen Idempotenten von A.
Wir wollen nun die Umkehrung untersuchen. Sei dafür $\{e_1,\ldots,e_n\}$ eine vollständige Menge orthogonaler idempotenter Elemente von A. Für ein beliebiges $m\in M$ gilt $m=1m=\sum_i e_i(m)$, d. h. die Mengen $e_i(M)$ erzeugen zusammen M. Sei nun $m\in e_i(M)\cap\sum_{i\neq j}e_j(M)$. Wir können m schreiben als $m=e_i(n)$ für ein $n\in M$ und sehen sofort, dass $e_j(m)=e_je_i(n)=0$ für $i\neq j$. Andererseits gilt aber $m=\sum_{i\neq j}e_j(n'_j)$ für bestimmte $n'_j\in M$, was auf $\sum_{i\neq j}e_j(m)=\sum_{i\neq j}e_j(\sum_{i\neq j}e_j(n'_j))=\sum_{i\neq j}e_j(n'_j)=m$, also $m=0$, führt. Daher gilt $M=\bigoplus e_i(M)$.
Also existiert eine bijektive Beziehung zwischen vollständigen Mengen orthogonaler idempotenter Elemente der Endomorphismenalgebra von M und Zerlegungen von M in direkte Summen.

Folgerung 10.2.3. *Sei R ein (kommutativer) lokaler, noetherscher Ring, der vollständig ist bezüglich eines Ideals $\mathfrak{m}$. Falls A eine (nicht notwendigerweise) kommutative R-Algebra ist, die endlich erzeugt als R-Modul ist, dann kann jede Menge orthogonaler idempotenter Elemente von $A/\mathfrak{m}A$ zu einer Menge von Idempotenten von A gehoben werden. Falls A kommutativ ist, so erhalten wir eine eindeutige Hebung.*

Beweis. Wir beginnen den Beweis mit dem zentralen Fall: Sei dazu $\bar{e} \in R/\mathfrak{m}$ eine Idempotente und sei $e \in R$ ein Urbild. Definiere $f(x)$ als das Polynom $x^2 - x \in R[x]$. Damit sind die Idempotenten in R genau die Wurzeln von f. Die Ableitung $f'(e) = 2e - 1$ ist eine Einheit in R, da die Eqivalenzen $(2e-1)^2 \equiv 4e^2 - 4e + 1 \equiv 1 \mod \mathfrak{m}$ und somit $f'(e)\mathfrak{m} = \mathfrak{m}$ gelten. Also ist $f(e) \equiv 0 \mod \mathfrak{m}$ und das Henselsche Lemma garantiert uns die Existenz einer eindeutig bestimmten Wurzel e_1 von $f(x)$ in R, die Urbild von $\bar{e}$ ist.
Um die Folgerung zu beweisen nehmen wir an, dass $\{\bar{e}_1, \ldots, \bar{e}_n\}$ eine Menge orthogonaler idempotenter Elemente von $A/\mathfrak{m}A$ darstellt. Der Beweis erfolgt mittels Induktion über n und Anwendung des zentralen Falls.
Nehmen wir zunächst an, A sei kommutativ. Nach Satz 7.2.5 ist die Algebra A selbst vollständig bezüglich $\mathfrak{m}A$. Daher können wir auch annehmen, dass ohne Einschränkung $A = R$ ist. Nach dem zentralen Fall existiert für jedes i eine eindeutig bestimmte Idempotente $e_i \in R$, die $\bar{e}_i$ hebt. Es bleibt zu zeigen, dass die so entstandenen Elemente orthogonal sind. Falls $i \neq j$, dann $\bar{e}_i\bar{e}_j = 0$, also $e_ie_j \in \mathfrak{m}$. Allerdings gilt für jede positive ganze Zahl d, dass $e_ie_j = e_i^d e_j^d = (e_ie_j)^d \in \mathfrak{m}^d$. Damit ist $e_ie_j \in \cap_d \mathfrak{m}^d = 0$. Damit ist die Orthogonalität gezeigt.
Abschließend zeigen wir nun die Behauptung für den Fall, dass A nicht kommutativ ist. Im Fall $n = 1$, sei e ein beliebiges Elemente von A, das auf $\bar{e}_1$ abgebildet wird. Ersetzen wir nun A durch die R-Unteralgebra, die von e erzeugt wird. Diese Unteralgebra ist wiederum kommutativ und die Behauptung folgt direkt aus den obigen Ergebnissen.
Sei also $n > 1$ und das Ergebnis für Mengen mit $k \leq n-1$ Elementen gezeigt. Das heißt, wir finden eine Menge von orthogonalen Idempotenten $e_1, \ldots, e_{n-1}$, welche den Elemente $\bar{e}_1, \ldots, \bar{e}_{n-1}$ entsprechen. Sei e' ein beliebiges Element in A mit Bild $\bar{e}_n$ in $A/\mathfrak{m}A$. Definieren wir $f := 1 - \sum_{i=1}^{n-1} e_i$, so sieht man sofort, dass $fe_i = e_if = 0$ für alle $i < n-1$. Weiters, falls $\bar{f}$ das Bild von f in $A/\mathfrak{m}A$ ist, dann gilt außerdem $\bar{f}\,\bar{e}_n = \bar{e}_n\bar{f} = \bar{e}_n$. Schließlich definieren wir $e := fe'f$. Dieses neue Element ist äquivalent zu $\bar{e}_n \mod \mathfrak{m}$ und erfüllt die Bedingung $e_i\,e = e\,e_i = 0$ für $i \leq n-1$. An dieser Stelle gehen wir wie beim Induktionsanfang vor und ersetzen A durch die Unteralgebra, die von $e_1, \ldots, e_{n-1}, e$ erzeugt wird. Damit haben wir auch diesen Fall auf den kommutativen Fall zurückgeführt. □

In der nächsten Folgerung wollen wir einen Zusammenhang zwischen Algebren über vollständigen Ringen und den Lokalisierungen untersuchen. Es handelt sich um eine Erweiterung von Folgerung 2.16.

Folgerung 10.2.4. *Sei R ein vollständiger, lokaler, noetherscher Ring. Falls A eine kommutative R-Algebra ist, die endlich erzeugt ist als R-Modul, dann besitzt A nur endlich viele maximale Ideale $\mathfrak{m}_i$. Jede Lokalisierung $A_{\mathfrak{m}_i}$ ist ein vollständiger, lokaler Ring, der endlich erzeugt ist über R. Außerdem entspricht A der direkten Summe über ihren Lokalisierungen: $A = \prod_i A_{\mathfrak{m}_i}$.*

Beweis. Sei $\mathfrak{m}$ ein maximales Ideal von R. Die Voraussetzungen implizieren, dass $A/\mathfrak{m}A$ ein endlich erzeugter Modul über dem Körper $R/\mathfrak{m}$ ist. Nach Satz 2.14 und 2.16 lässt sich $A/\mathfrak{m}A$ als Produkt $\bar{A}_1 \times \ldots \times \bar{A}_n$ von lokalen Ringen $\bar{A}_i$ schreiben. Ist nun $\bar{e}_i$ die Einheit der Unteralgebra $\bar{A}_i$, so bilden diese Elemente eine Menge von orthogonalen Idempotenten in $A/\mathfrak{m}A$. Aufgrund der vorangegangenen Folgerung 10.2.3 lassen sich diese zu einer Menge von Idempotenten $\{e_1, \ldots, e_n\}$ von A heben. Wir definieren nun die Mengen $A_i = e_i A$ und erhalten die Zerlegung $A = A_1 \times \ldots \times A_n$. Jede dieser Mengen A_i ist endlich über R, da sie ein direkter Summand des R-Moduls A ist.
Falls $\mathfrak{n}_i$ ein maximales Ideal von A_i ist, dann gilt nach Folgerung 4.17, dass auch $\mathfrak{n}_i \cap R$ ein maximales Ideal ist und somit $\mathfrak{n}_i \cap R = \mathfrak{m}$. Daraus können wir schließen, dass jedes maximale Ideal von A_i die Menge $\mathfrak{m}A_i$ enthält. Da $A_I/\mathfrak{m}A_i$ ein lokaler Ringe ist, ist auch A_i lokal und $\mathfrak{n}_i$ ist sein eindeutig bestimmtes maximales Ideal. Das Urbild $\mathfrak{m}_i$ von $\mathfrak{n}_i$ unter der Projektion $A = \prod A_i \to A_i$ muss ein maximales Ideal von A sein. Mit den gleichen Argumenten wie zuvor sieht man, dass jedes maximale Ideal von A das Ideal $\mathfrak{m}$ enthalten muss, also entsprechen sie maximalen Idealen von $A/\mathfrak{m}A$ und sind alle unter den $\mathfrak{m}_i$.
In der Lokalisierung $A_\mathfrak{m}$ wird jede Idempotente e_i eine Einheit. Da außerdem $e_i e_j = 0$ für $i \neq j$, erhalten wir $A_{\mathfrak{m}_i} = (A_i)_{\mathfrak{n}_i} = A_i$, womit die Folgerung gezeigt ist. □

10.3 Struktursatz von Cohen

In diesem Abschnitt wollen wir ein Ergebnis zeigen, das etwas über die Struktur von lokalen, vollständigen, noetherschen Ringen aussagt.

Definition 10.3.1. Sei R ein lokaler Ring und $\mathfrak{m}$ das maximale Ideal. Dann heißt ein Körper $\tilde{K} \subset R$ **Koeffizientenkörper**, falls $\tilde{K}$ isomorph zum Restklassenkörper $R/\mathfrak{m}$ ist.

Falls $k \subseteq K$ Körper sind, so wird eine bestimmte Teilmenge des Körpers K **differentielle Basis für K über k** genannt. Wir wollen hier keine Definition angeben, sondern beschränken uns auf eine Charakterisierung des für uns relevanten Falls.

Tatsache 10.3.2. *Sei K eine separabel erzeugte Körpererweiterung über k mit* $\mathrm{char}(k) = 0$*, so ist die differentielle Basis eine transzendente Basis.*

Definition 10.3.3. Seien L_1 und L_2 Teilkörper eines Körpers L, dann schreiben wir $L_1 * L_2$ für die Komposition von L_1 und L_2 also den Körper, der von L_1 und L_2 erzeugt wird.

Definition 10.3.4. Seien $k \subset K$ Körper der Charakteristik p, dann heißt eine Menge von Elementen $\{x_\lambda\}_{\lambda \in \Lambda} \subset K$ eine **p-Basis** von K über k, falls die Menge W von Monomen in x_λ vom Grad $< p$ in jedem der x_λ eine Basis des Vektorraums K über $k * K^p$ ist.

Tatsache 10.3.5. *Sei K eine separabel erzeugte Körpererweiterung über k mit* $\mathrm{char}(k) = p$*, so ist die differentielle Basis eine p-Basis.*

Satz 10.3.6. *Seien $k \subset K$ Körper von Charakteristik p, B ein p-Basis von K über k und sei $q = p^n$ für ein $n \in \mathbf{N}$. Sei W_q die Menge von Monomen in Elementen von B vom Grad $< q$ in jedem Element von B. Dann gilt:*

(i) *$K = k * K^q[B]$. Das bedeutet W_q spannt K als Vektorraum über $k * K^q[B]$ auf.*

(ii) *Falls K separabel über k ist, dann bildet W_q eine Basis des Vektorraums K über $k * K^q[B]$.*

(iii) *Falls K separabel über k ist, dann sind die Elemente von B algebraisch unabhängig über $k * K^{p^\infty} := \bigcap_{q=p^n} k * K^q$.*

Beweis. Siehe [1], Anhang 1 □

Satz 10.3.7. *Sei R ein vollständiger, lokaler, noetherscher Ring mit maximalen Ideal $\mathfrak{m}$ und Restklassenkörper K. R enthalte einen Körper k und K sei separabel über k. Sei B eine differentielle Basis der Körpererweiterung K/k. Dann lässt sich jeder Koeffizientenkörper $\tilde{K} \subset R$, der k enthält, eindeutig einer Menge $\tilde{B} \subset R$ von Repräsentaten von B zuordnen. Dabei wird jedem $\tilde{K}$ die Menge $\tilde{B}$ von Repräsentanten von B zugeordnet, die $\tilde{K}$ enthält. Falls k perfekt ist von Charakteristik $p > 0$, dann enthält k jeden Koeffizientenkörper von R.*

Beweis. Sei R zunächst ein lokaler Ring, der einen Körper k enthält und sei K der Restklssenkörper von R. Falls B eine Teilmenge von K ist, die algebraisch unabhängig ist über k und $\tilde{B}$ eine Menge von Repräsentanten von B, dann besitzt jedes nichttriviale Polynom in Elementen aus $\tilde{B}$ mit Koeffizienten in k ein Bild ungleich der Null in K und ist somit invertierbar in R. Somit enthält R den Körper $k(\tilde{B})$ der rationalen Funktionen in Elementen aus $\tilde{B}$. Dieser Körper ist isomorph zu $k(B)$.
Nehmen wir nun an, dass K separabel über k ist und dass B eine differentielle Basis für K/k darstellt. In Charakteristik 0 ist diese Annahme äquivalent dazu, dass B eine transzendentale Basis für K/k bildet. In Charakteristik $p > 0$ zeigt uns Satz **??**, dass B algebraisch unabhängig über $k * K^{p^\infty}$ ist. In beiden Fällen ist $k(\tilde{B})$ enthalten in R, falls $\tilde{B} \subset R$ eine Mengen von Repräsentanten von B ist. Unter der zusätzlichen Annahmen, dass R vollständig und noethersch ist, werden wir zeigen, dass ein eindeutig bestimmter Koeffizientenkörper $\tilde{K}$ von R existiert, der $k(\tilde{B})$ enthält.
Betrachten wir zuerst den Fall, in dem $\mathrm{char}(k) = 0$ gilt oder allgemeiner, dass K separabel algebraisch über $k(B)$ ist. Nach Zorns Lemma können wir einen Teilkörper $K' \subset K$ wählen, der $k(B)$ enthält und maximal ist unter den Teilkörpern von K, die $k(B)$ enthalten und darüber hinaus eindeutig gehoben werden können zu einem Teilkörper von R , der $k(\tilde{B})$ enthält. Sei $\tilde{K}'$ die Hebung von K' in R. Wir müssen $K = K'$ zeigen. Sei $a \in K$ und sei $f(t)$ das monische, irreduzible Polynom mit Koeffizienten in K' mit $f(a) = 0$. Wir wenden nun die Inverse des Isomorphismus' $\tilde{K}' \to K'$ an und können so f heben zu einem monischen Polynom $\tilde{f}$ mit Koeffizienten in R. Da K separabel über K' ist, sind die Wurzeln von f unterscheidbar, also gilt $f'(a) \neq 0$ in K. Nach dem Henselschen Lemma existiert eine eindeutig bestimmte Wurzel $\tilde{a} \in R$ von f mit Bild a in K. Der

Körper $\tilde{K}'(\tilde{a})$ ist daher der eindeutig bestimmte Körper, der $K'(a)$ hebt und $\tilde{K}'$ enthält. Zusammen mit der Eindeutigkeit von K', erhalten wir, dass $\tilde{K}'(\tilde{a})$ tatsächlich der eindeutig bestimmte Körper ist, der $K'(a)$ hebt und $k(\tilde{B})$ enthält. Da aber K' maximal war, muss auch schon $a \in K'$ gegolten haben. Damit ist in diesem Fall die gewünschte Identität $K' = K$ gezeigt.
Nehmen wir den allgemeinen Fall an, in dem $\mathrm{char}(k) = p > 0$ gilt. Es ist zu zeigen, dass

$$\tilde{K} := \bigcap_{q=p^n, n\geq 1} k * R^q[\tilde{B}]$$

der eindeutig betimmte Koeffizientenkörper von R ist, der k und $\tilde{B}$ enthält. Hierbei bezeichne R^q den Ring von q-ten Potenzen von Elementen von R und $k * R^q[B]$ den kleinsten Teilring von R, der k, R^q und B enthält. Falls k' ein perfekter Körper enthalten in R ist, dann gilt $k' = k'^q \subset R^q$ für jedes $q = p^n$, so dass $k' \subset \tilde{K}$. Das beweist auch die letzte Aussage des Satzes.
Zuerst wollen wir zeigen, dass jeder Koeffizientenkörper $K' \subset R$ in $\tilde{K}$ enthalten sein muss, wenn er k und $\tilde{B}$ enthält. Da $K' \cong K$ durch den Isomorphismus zwischen $\tilde{B}$ und B gilt, ist die Menge $\tilde{B}$ eine p-Basis von K' über k. Hier wenden wir Satz 10.3.6 an und erhalten $K' = k * K'^q[B] \subset k * R^q[\tilde{B}]$ für jedes $q = p^n$, wie gewünscht.
Nun definieren wir einen Homomorphismus $\varphi : K \to R$. Für $a \in K$ und für jedes $q = p^n$, sei a_q ein Repräsentant von a in $k * R^q[\tilde{B}]$. Dieser Repräsentation muss existieren, denn nach Satz 10.3.6 gilt $k * K^q[B] = K$. Sei nun a'_q ein weiterer, solcher Repräsentant von a. Wir behaupten, dass $a_q - a'_q \in \mathfrak{m}^q$, wobei $\mathfrak{m}$ ein maximales Ideal von R ist. Ist das gezeigt, können wir schließen, dass die Folge $a_1, a_p, a_{p^2}, \ldots$ in R gegen einen Grenzwert $\tilde{a} \in R$ konvergiert unabhängig von der Wahl der Repräsentanten a_q. Wir definieren dann $\varphi(a) = \tilde{a}$. Falls $r \in \tilde{K}$ mit Bild $a \in K$, dann können wir $a_q = r$ wählen für alle q. Dadurch erhalten wir $\varphi(a) = r$ und somit $K \subset \varphi(\tilde{K})$. Trivialerweise ist das Bild von $\varphi(a)$ in K gerade a. Die Unabhängigkeit der Wahl der Repräsentanten zeigt $\varphi(a+b) = \varphi(a) + \varphi(b)$ und gleiches gilt für die Multiplikation. Damit ist gezeigt, dass φ ein Homomorphismus ist und $\varphi(K)$ ein Koeffizientenkörper ist, der K enthält. Der vorangegangene Absatz zeigt $\varphi(K) = \tilde{K}$.
Es bleibt zu zeigen, dass in der Tat $a_q - a'_q \in \mathfrak{m}^q$ gilt. Nach Definition sind a_q und a'_q Polynome in den Elementen von $\tilde{B}$ mit Koeffizienten in $k * R^q$. Jede q-te Potenz eines Elementes aus $\tilde{B}$ kann mit den Koeffizienten verrechnet werden und wir können

$$a_q = \sum_{w\in W} u_w r_w^q w, \qquad a'_q \sum_{w\in W} u'_w r'^q_w w$$

schreiben mit $u_w, u'_w \in k$, $r_w, r'_w \in R$ und wobei W die Menge der Monome von bestimmten $b_1, \ldots, b_s \in B$ vom Grad $< q$ in jedem b_i ist. Da $a_q - a'_q \in \mathfrak{m}$ und da W eine Basis für den $k * K^q$-Vektorraum $k * K^q[b_1, \ldots, b_s]$ bildet, folgt $u_w r_w^q - u'_w r'^q_w \in \mathfrak{m}$ für jedes $w \in W$.
Seien nun $\bar{r}_w$ und $\bar{r}'_w$ die Bilder von r_w und r'_w in K. Wir können annehmen, dass $\bar{u}'_w \neq 0 \neq \bar{r}_w$. Da $\bar{u}_w/\bar{u}'_w = (\bar{r}'_w/\bar{r}_w)^q \in k$ und K keine nichttrivialen, rein inseparablen Erweiterungen von k enthält, gilt $(\bar{r}'_w/\bar{r}_w) = v \in k$. Daher gilt

$$(1/u'_w)(u_w r_w^q - u'_w r'^q_w) = v^q r_w^q - r'^q_w = (v r_w - r'_w)^q \in \mathfrak{m}.$$

Da $\mathfrak{m}$ ein Primideal ist, schließen wir $(vr_w - r'_w) \in \mathfrak{m}$ und daher $(vr_w - r'_w)^q \in \mathfrak{m}^q$. Multiplizieren wir den Ausdruck mit u'_w, so erhalten wir $u_w r_w^q - u'_w r_w'^q \in \mathfrak{m}^q$. Daraus schließen wir $a_q - a'_q \in \mathfrak{m}^q$, wie gewünscht. □

Satz 10.3.8. ***Strukturssatz von Cohen***
Sei R ein vollständiger, lokaler, noetherscher Ring mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper K. Falls R einen Körper enthält, dann gilt

$$R \cong K[[x_1 \ldots, x_n]]/I$$

für ein $n \in \mathbf{N}$ und für ein Ideal I.

Beweis. Nach 10.3.7 existiert ein Koeffizientenkörper $K' \subset R$. Sei $a_1, \ldots, a_n$ eine Menge von Erzeugern des maximalen Ideals von R. Da R vollständig ist, existiert nach Satz 10.1.1 (i) eine Abbildung $\varphi : K'[[x_1, \ldots, x_n]] \to R$, die x_i auf a_i abbildet. Satz 10.1.1 (ii) besagt, dass diese Abbildung surjektiv ist. Mit $K' \cong K$ und $I = \ker \varphi$ gilt also $R \cong K[[x_1, \ldots, x_n]]/I$. □

Satz 10.3.9. *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, der entweder die Lokalisierung eines endlich erzeugten Rings über einem Körper oder der Ring $\mathbf{Z}$ ist. Dann besitzt die Vervollständigung $\hat{R}_\mathfrak{m}$ keine nilpotenten Elemente.*

11 Gröbnerbasen

Rebecca Kiesl, Katja Möser, Markus Schupp

11.1 Monome und Terme

In diesem Kapitel beschäftigen wir uns mit einem Polynomring $S = K[x_1, x_2, ..., x_n]$ über einem Körper K, den Idealen des Rings und den endlich erzeugten Moduln über diesem Ring. Gröbnerbasen werden dazu benutzt Fragestellungen über Polynome auf Probleme in Monomen zurückzuführen. In diesem Abschnitt werden wir deshalb einige elementare Definitionen und anschließend auch einige Beispiele betrachten, die zeigen, dass Fragestellungen für Monome einfacher sind als für beliebige Polynome.
Im Folgenden sei $S = K[x_1, ..., x_k]$ immer ein Polynomring mit n Variablen über einem Körper K. Weiter seien alle vorkommenden freien Modulen endlich erzeugt.

Definition 11.1.1. Ein von Monomen erzeugtes Ideal von S wird, wird als *Monomideal* bezeichnet.
Wir schreiben Monome als Multiindizes. D.h. wenn $\alpha = (\alpha_1, \ldots, \alpha_k)$ wird mit x^α das Monom $x_1^{\alpha_1} \cdots x_k^{\alpha_k}$ bezeichnet.

Definition 11.1.2. Sei F ein freier Modul über einem Polynomring S mit Basis $\{e_1, \ldots, e_n\}$.
Ein Element der Form $m = x^\alpha e_i$ wird als *Monom in* F bezeichnet.
Ein *Monomuntermodul* von F ist ein Untermodul, der von Monomen in F erzeugt wird.
Jeder Monomuntermodul lässt sich folgendermaßen schreiben:

$$M = \oplus I_j e_j \subset \oplus S e_j = F$$

wobei I_j das Ideal bezeichnet, das von den Monomen $m \in S$ erzeugt wird, für die gilt, $me_j \in M$
Ein *Term* t *in* F ist ein Monom me_j, das mit einem Skalar $k \in K$ multipliziert wurde: $t = kme_j$

Betrachtet man F als K-Vektorraum, sieht man, dass die Monome eine Vektorraumbasis von F bilden. Jedes Element $f \in F$ lässt sich also eindeutig als endliche Summe von Termen (ungleich 0) in F schreiben.

Definition 11.1.3. Sei $f \in F$. Und sei

$$f = \sum_{j=1}^{n} \sum_{i=1}^{t_j} k_{ij} m_{ij} e_j$$

eine Zerlegung von f wie oben beschrieben. Dann werden die Elemente $k_{ij}m_{ij}e_j$ als Terme von f bezeichnet.

Definition 11.1.4. Seien $m, n \in S$ Monome und seien $u, v \in K, v \neq 0$. Ein Term ume_i heißt *teilbar* durch den Term vne_j, wenn $i = j$ und m in S durch n teilbar ist. Der *Quotient* ist dann definiert als $\frac{um}{vn} \in S$.

Für Monome sind viele Operationen deutlich einfacher als für beliebige Polynome. Man kann z.B. sehr einfach den *größten gemeinsamen Teiler* und das *kleinste gemeinsame Vielfache* bestimmen:

$$ggT(x^\alpha, x^\beta) = x_1^{min(\alpha_1,\beta_1)} x_2^{min(\alpha_2,\beta_2)} \cdots x_n^{min(\alpha_n,\beta_n)},$$

$$kgV(x^\alpha, x^\beta) = x_1^{max(\alpha_1,\beta_1)} x_2^{max(\alpha_2,\beta_2)} \cdots x_n^{max(\alpha_n,\beta_n)}.$$

Diese Operationen kann man analog für die Monome in einem freien Modul F definieren.

Bemerkung 11.1.5. Sei $M \subset F$ ein Untermodul, der von den Monomen $m_1, \ldots, m_t$ erzeugt wird und sei $m \in F$ ein Monom. Es ist $m \in M$ genau dann, wenn m durch eines der m_i teilbar ist. Allgemeiner: Sei $f \in F$ ein beliebiges Element aus F. Dann gilt $f \in M$ genau dann, wenn jedes Monom von f in M enthalten ist.

Wir betrachten nun die Erzeugermenge eines Monomuntermoduls $\{m_1, \ldots, m_n\}$. Ist eines der Monome m_i durch ein anderes Monom teilbar, so erzeugen die Elemente $m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n$ auch den Untermodul. Man kann also ein Element aus der Erzeugermenge entfernen, wenn es durch ein weiteres teilbar ist. Auf diese Weise erhält man eine minimale Erzeugermenge von M. In ihr sind genau die Monome aus M, die bezüglich der Partialordnung, die durch die Teilbarkeit von Monomen in F induziert wird, minimal sind.

Definition 11.1.6. Die Elemente des oben beschriebenen minimalen Erzeugendensystems eines Monomuntermoduls M werden als *minimale Erzeuger von* M bezeichnet.

Wir werden nun die Syzygien eines Monomuntermoduls von einem freien Modul bestimmen. Dies wird deutlich einfacher sein, als im allgemeinen Fall. Wir beginnen mit einer kurzen Einführung über Syzygien:
Im Gegensatz zu Vektorräumen über Körpern, kann es bei Moduln über Ringen nichttriviale Relationen von Erzeugern geben. Diese werden auch Syzygien genannt.

Definition 11.1.7 (Syzygie)**.** Sei R ein Ring und sei M ein R-Modul. Sei weiterhin $m_1, \ldots, m_n \in M$ eine Menge von Erzeugern von M. Wenn $\sum_{i=1}^{n} a_i m_i = 0$, dann ist $(a_1, \ldots a_n) \in R^n$ eine *Syzygie*. Die Menge der Syzygien (in Abhängigkeit einer Menge von Erzeugern) bildet einen Untermodul von R^n.

Satz 11.1.8. *Sei F ein freier Modul über einem Polynomring S mit Basis und sei M ein Monomuntermodul, der von $m_1, \ldots, m_t$ erzeugt wird. Sei*

$$\varphi : \bigoplus_{j=1}^{t} S\varepsilon_j \longrightarrow F, \qquad \text{so dass } \varphi(\varepsilon_j) = m_j$$

ein Homomorphismus von einem freien Modul in F, mit $im(\varphi) = M$. Für jedes Paar von Indizes i, j, für die m_i und m_j die gleichen Basiselemente von F enthalten, definieren wir

$$m_{ij} = \frac{m_i}{ggT(m_i, m_j)}$$
$$\sigma_{ij} = m_{ji}\varepsilon_i - m_{ij}\varepsilon_j.$$

Dann wird $ker\varphi$ von den σ_{ij} erzeugt.

Die Syzygien von M sind hier genau der $ker\varphi$. D.h. wir haben mit diesem Satz schon unser Erzeugendensystem für die Syzygien gefunden. Nun zum Beweis.

Beweis. Die Elemente σ_{ij}liegen im Kern vonφ, denn

$$\varphi(\sigma_{ij}) = m_{ji}\varphi(\varepsilon_i) - m_{ij}\varphi(\varepsilon_j) = \frac{m_j m_i - m_i m_j}{ggT(m_i, m_j)} = 0.$$

Wir müssen also nur zeigen, dass $ker\varphi$ von diesen Elementen erzeugt wird. Wir betrachten nun $ker\varphi$ als Vektorraum über K. Dann lässt sich $ker\varphi$ als direkte Summe folgender Vektorräume schreiben, wobei n alle Monome aus F durchläuft:

$$(ker\varphi)_n = \left\{ \sum_{v=1}^{t} a_v n_v \varepsilon_v \in ker\varphi | m_v \text{ teilt } n, n_v = \frac{n}{m_v} \text{ und } a_v \in K \right\} \text{ für } n \in F.$$

Sei nun $\sigma = \sum_{i=1}^{t} p_i\varepsilon_i \in S^t, \qquad p_i \in S$ eine Syzygie.

Das bedeutet $\sum_{i=1}^{t} p_i m_i = 0$. Wir zerlegen nun das Element p_i weiter: Falls $p_i m_i$ durch ein Monom $n \in F$ teilbar ist, setzen wir $p_{i,n}$ so, dass $p_{i,n} m_i = a_{i,n} n$ für ein $a_{i,n} \in K$. Dann können wir unsere Summe umschreiben: $0 = \sum_{i=1}^{t} p_i m_i = \sum_{i=1, n\in F}^{t} p_{i,n} m_i = \sum_{n\in F} n \sum_{i=1}^{t} p_{i,n} m_i$.

Hieraus folgt aber, dass für jedes einzelne $n \in F$ gilt, dass $\sum_{i=1}^{t} p_{i,n} m_i = 0$. Also gilt $\sum_{i=1}^{t} p_{i,n}\varepsilon_i \in (ker\varphi)_n$.

Wir können uns also auf den Fall eines Monoms $n \in F$ und $\sigma = \sum_{v=1}^{t} a_v n_v \varepsilon_v \in (ker\varphi)_n$ beschränken. Wir zeigen nun, dass σ von den σ_{ij} erzeugt wird, indem wir Induktion

über die Anzahl der Terme in σ durchführen. Das bedeutet, dass wir durch geschicktes subtrahieren von Elementen der σ_{ij} eine Relation mit weniger Termen erhalten:
Sei $\sigma \neq 0$ Da σ eine Syzygie ist, müssen dann mindestens zwei Terme $a_i n_i$ und $a_j n_j \neq 0$ von σ existieren. Somit gilt, dass n durch m_i und m_j teilbar ist. Dann folgt direkt, dass $n_i = \frac{n}{m_i}$ durch folgenden Ausdruck teilbar ist:

$$\frac{kgV(m_i, m_j)}{m_i} = \frac{m_j}{ggT(m_i, m_j)} = m_{ji}.$$

Betrachten wir nun $\sigma - a_i \frac{n_i}{m_{ji}} \sigma_{ij}$, so erhalten wir eine Relation mit weniger Elementen. Durch Induktion folgt dann, dass σ von den σ_{ij} erzeugt wird. □

11.2 Termordnungen

Sei $J \subset S$ ein Monomideal. Dann bildet die Menge B aller Monome, die nicht in J enthalten sind, eine Basis des K-Vektorraums S/J.
Ein ähnliches Resultat würden wir auch gerne für ein beliebiges Ideal I von S und S/I erhalten. Da alle Monome in S eine Vektorraumbasis von S bilden, spannen ihre Bilder S/I auf. Wählt man aus den Bildern der Monome also eine maximale, linear unabhängige Menge, so hat man eine Basis gefunden. Nach Zorns Lemma hat also jedes S/I eine Basis aus Monomen.
Wählt man B als Komplement der Menge der Monome, die in einem Monomideal J liegen, so kann man sehr einfach testen, ob ein Monom in B liegt. Da J von endlich vielen Monomen erzeugt wird, muss man nur testen, ob ein gegebenes Monom durch einen der Erzeuger von J teilbar ist. Ist dies nicht der Fall, so liegt das Monom in B. Falls nun I ein beliebiges Ideal ist, werden wir in Satz 8.2.7 zeigen, dass man B ähnlich wählen kann.
Es folgen einige Vorbemerkungen bevor wir die Konstruktion der Gröbnerbasen beginnen.

Satz 11.2.1. *Sei J ein Monomideal und B die Menge der Monome, die nicht in J enthalten sind. Dann sind die Elemente aus B linear unabhängig modulo einem Ideal I genau dann, wenn J mindestens ein Monom jedes Polynoms in I enthält.*

Beweis. "⇒": Sei B linear unabhängig modulo I. Angenommen es gäbe ein Polynom $p \in I$, so dass j kein Monom aus p enthält. Dann gilt aber, dass alle Monome von p in B liegen und damit $p = k_1 m_1 + \cdots + k_n m_n \in I$, mit $m_i \in B$ für alle i.
Das ist jedoch ein Widerspruch dazu, dass B linear unabhängig ist.
" ⇐" Seien $m_1, \ldots m_n \in B$ und sei $k_1 m_1 + \cdots + k_n m_n \in I$. Da J mindestens ein Monom aus jedem Polynom in I enthält, muss es auch eines der Monome $m_1, \ldots, m_n$ enthalten. Da aber alle m_i in B liegen, folgt hieraus, dass $k_1 = \ldots = k_n = 0$ und damit ist B linear unabhängig modulo I. □

Damit B eine Basis von S/I wird, muss J also auf jeden Fall obige Bedingung erfüllen und minimal sein.

Beispiel 11.2.2. Sei $S = K[x]$ und sei $I = (x + x^2)$. Setzt man nun $J = (x)$, so gilt $B = \{1\}$. Dies ist aber keine Basis von S/I. Wählt man $J = (x^2)$ so gilt $B = \{1, x\}$. Dies ist eine Basis von S/I.
Wir betrachten nun einen etwas allgemeineren Fall.
Sei S ein Polynomring, $I = (m_1 + m_2)$ ein Hauptideal, das von der Summe zweier Monome m_1 und m_2 erzeugt wird. Sei weiterhin m_1 durch m_2 teilbar. Wählen wir nun $J = (m_2)$, so wird B keine Basis sein, da J nicht minimal ist. Es gilt nämlich $m_1, m_2 \in J$ und damit $m_1 \notin B$. Wählen wir aber $J = (m_1)$, so wird B eine Basis.

Um ein Monomideal J zu finden, das von jedem Polynom aus I ein Monom enthält, wollen wir nun eine Methode entwickeln, um ein Monom aus jedem Polynom in S zu wählen. Mit dieser Methode können wir Erzeuger von J finden. Damit J minimal wird, benötigen wir dann allerdings einige weitere Voraussetzungen.

Beispiel 11.2.3. Seien m_1, m_2, m_3 Monome gleichen Grades d und sei
$I = (m_1 + m_2, m_2 + m_3) \cup$(alle Monome vom Grad $> d$).
Wir nehmen an unsere Auswahlmethode liefere für das Polynom $m_1 + m_2$ das Monom m_1 und für $m_2 + m_3$ das Monom m_2. Im Ideal I liegt außerdem das Polynom
$m_1 - m_3 = (m_1 + m_2) - (m_2 + m_3)$.
Von diesem Polynom kann man nun nicht das Monom m_3 wählen, da J sonst nicht minimal wäre.

Falls nun $m_1 > m_2$ für die Relation "m_1 wird vor m_2 ausgewählt" gilt, so muss unsere Relation folgendes erfüllen:

$$m_1 > m_2 > m_3 \implies m_1 > m_3 \text{ (Transitivität)}.$$

Wir müssen also die Monome anordnen und für J die größten Monome der Poynome aus I wählen. Da J ein Ideal sein soll, müssen zwei weitere Bedingungen erfüllt sein:
Zum einen muss die Ordnung die Partialordnung der Teilbarkeit erhalten. Ist also m_2 durch m_1 teilbar, so muss $m_2 > m_1$ gelten.
Zum anderen muss die Ordnung die Multiplikation erhalten. D.h. wenn $m_1 > m_2$ muss auch $nm_1 > nm_2$ gelten.
Die folgende Definition enthält diese beiden Bedingungen.

Definition 11.2.4 (Termordnung)**.** Sei F ein freier S-Modul. Eine *Termordnung* von F ist eine Anordnung $>$ der Monome von F, die folgende Bedingung erfüllt. Seien m_1, m_2 Monome in F und sei $n \neq 1$ ein Monom aus S, dann gilt:

$$m_1 > m_2 \implies nm_1 > nm_2 > m_2.$$

Wir verallgemeinern unsere Notation nun auf Terme. Seien um, vn Terme mit $0 \neq u, v \in K$ und seien m, n Monome mit $m > n$ (bzw. $m \geq n$), dann setzen wir $um > vn$ (bzw. $um \geq vn$). Dies ist zwar keine Partialordnung der Terme, da für $u \neq v$ folgt $um \geq vm$ und $vm \geq um$, trotzdem ist diese Notation nützlich.

Definition 11.2.5. Sei $>$ eine Termordnung von F und sei $f \in F$. Der größte Term von f bezüglich der Termordnung wird als *Initialterm* $in_>(f)$ bezeichnet.
Ist M ein Untermodul von F, so definieren wir $in_>(M)$ als den Monomuntermodul, der von den Initialtermen $in_>(f)$ aller Elemente $f \in M$ erzeugt wird.

Bemerkung 11.2.6. Sei $p \in S, f \in F$ und sei n der Term von p, so dass $n\ in(f)$ maximal wird, dann gilt $in(pf) = n\ in(f)$. Sei weiter $m \neq in(f)$ ein Term von f und $n' \neq n$ ein Term von p, so gilt $n\ in(f) > n'\ in(f) > n'm$.

Satz 11.2.7. *Sei F ein freier S-Modul und sei M ein beliebiger Untermodul von F. Dann gilt für jede Termordnung $>$ auf F, dass die Menge B aller Monome, die nicht in $in_>(M)$ liegen, eine Basis von F/M bildet.*

Beweis. Zuerst zeigen wir, dass B linear unabhängig ist. Angenommen es gäbe eine Abhängigkeitsrelation

$$p = \sum u_i m_i \in M, \text{ mit } m_i \in B \text{ und } 0 \neq u_i \in K,$$

dann wäre $in(p) \in in(M)$. Da aber $in(p)$ einer der Terme $u_i m_i$ ist, die alle in B liegen, ist dies ein Widerspruch.
Nehmen wir nun an, dass B nicht F/M aufspannt. Es gibt also Elemente in F, die nicht von $M \cup B$ erzeugt werden. Von diesen Elementen wählen wir eines mit minimalem Initialterm als f.
Wäre nun $in(f) \in B$, so würde $f - in(f) \notin B$ gelten. Allerdings hat dieses Element einen kleineren Initialterm, woraus ein Widerspruch zur Wahl von f folgt. Also gilt $in(f) \in in(M)$. Also gibt es ein $m \in M$ mit $in(m) = in(f)$. Dann gilt aber $f - m \notin M$. Auch dieses Element hat einen kleineren Initialterm als f, woraus ein ähnlicher Widerspruch folgt. □

Wir werden nun einige wichtige Beispiele für Termordnungen geben. Wir betrachten dabei den Spezialfall $F = S$. Weiterhin kann man durch Umnummerierung der Variablen immer erreichen, dass $x_1 > x_2 > \cdots > x_n$. Die Beispiele, die wir geben, werden alle diese Eigenschaft erfüllen. Auch bei diesen Beispielen werden die Monome wieder als Multiindizes geschrieben: $m = x^\alpha = x_1^{\alpha_1} \cdots x_k^{\alpha_k}, \quad n = x^\beta = x_1^{\beta_1} \cdots x_k^{\beta_k}$

Beispiel 11.2.8 (Lexikographische Ordnung)**.** $m >_{lex} n :\Leftrightarrow \alpha_i > \beta_i$ für das kleinste i, für das gilt $\alpha_i \neq \beta_i$.

Beispiel 11.2.9 (Homogene lexikographische Ordnung)**.** $m >_{hlex} n :\Leftrightarrow deg(m) > deg(n)$ oder $deg(m) = deg(n)$ und $\alpha_i > \beta_i$ für das kleinste i, für das gilt $\alpha_i \neq \beta_i$.

Beispiel 11.2.10 (Lexikographisches Produkt)**.** Sei $>_1, >_2, \ldots$ eine Folge von Termordnungen. Das lexikographische Produkt $>$ dieser Ordnung ist folgendermaßen definiert: $m > n :\Leftrightarrow m >_i n$ für das erste i, in dem m, n verglichen werden können.

Beispiel 11.2.11. Sei $S = K[x]$ der Polynomring in einer Variablen und sei $m \in S$ ein Monom. Nach Voraussetzung gilt für alle Monome $n \neq 1$, dass $nm > m$. Das bedeutet, dass es genau eine Ordnung auf S gibt, nämlich die Ordnung nach dem Grad.

Beispiel 11.2.12. Sei $S = K[x_1, x_2]$ der Polynomring in zwei Variablen. Dann gibt es genau eine Ordnung, die die Partialordnung nach dem Grad erhält und unsere Konvention $x_1 > x_2$ erfüllt:
Seien also $m = x_1^{\alpha_1} x_2^{\alpha_2}$ und $n = x_1^{\beta_1} x_2^{\beta_2}$ Monome gleichen Grades, d.h. $\alpha_1 + \alpha_2 = \beta_1 + \beta_2$.
Sei nun $\alpha_1 > \beta_1$, setze $\varepsilon := \alpha_1 - \beta_1 = \beta_2 - \alpha_2$ und $p = ggT(m, n) = x_1^{\beta_1} x_2^{\alpha_2}$. Dann gilt:

$$m = x_1^{\varepsilon} p,$$
$$n = x_2^{\varepsilon} p.$$

Da aber $x_1 > x_2$, gilt $x_1^{\varepsilon} > x_1^{\varepsilon-1} x_2 > \cdots > x_2^{\varepsilon}$. Damit folgt aber bereits $m > n$.

Im allgemeinen Fall gibt es jedoch verschiedene Ordnungen. Das wichtigste Beispiel hierfür folgt jetzt:

Beispiel 11.2.13 (Umgekehrte lexikographische Ordnung)**.** $m >_{rlex} n \Leftrightarrow deg(m) > deg(n)$ oder $deg(m) = deg(n)$ und $\alpha_i < \beta_i$ für das größte i, für das gilt $\alpha_i \neq \beta_i$.
Achtung: In diesem Beispiel hat sich die Richtung des Ungleichungszeichens $\alpha_i < \beta_i$ geändert.

Der Unterschied zwischen dieser Termordnung und der homogenen lexikographischen Ordnung ist nicht sehr groß. Allerdings werden die Algorithmen, die später beschrieben werden, in der Regel deutlich effizienter werden, wenn man die in diesem Beispiel beschriebene Ordnung verwendet.

Der erste Fall, in dem sich $>_{hlex}$ und $>_{rlex}$ unterscheiden können ist der Fall quadratischer Monome in drei Variablen:

$$x_1 x_3 >_{hlex} x_2^2, \text{ aber}$$
$$x_1 x_3 <_{rlex} x_2^2.$$

Grob gesagt besteht der Unterschied in Folgendem:
$m >_{hlex} n$, wenn m "mehr vom Beginn der Liste der Variablen enthält", während
$m >_{rlex} n$, wenn m "weniger vom Ende der Liste der Variablen enthält".
Die folgende Proposition wird zeigen, dass dieser Unterschied dem Unterschied zwischen einem Unterring und einem Ideal entspricht.

Proposition 11.2.14.

(i) Aus $in_{lex}(f) \in K[x_s, \ldots, x_n]$ für ein s, folgt $f \in K[x_s, \ldots, x_n]$.

(ii) $>_{hlex}$ erhält die Ordnung nach dem Grad und falls f homogenes Polynom ist, mit $in_{hlex}(f) \in K[x_s, \ldots, x_n]$ für ein s, folgt $f \in K[x_s, \ldots, x_n]$.

(iii) $>_{rlex}$ erhält die Ordnung nach dem Grad und falls f homogenes Polynom ist, mit $in_{rlex}(f) \in (x_s, \ldots, x_n)$ für ein s, folgt $f \in (x_s, \ldots, x_n)$.

Beweis. (i) Klar.

(ii) Sei f ein homogenes Polynom mit $in_{hlex}(f) \in K[x_s, \ldots, x_n]$. Angenommen es gäbe ein Monom m in f, so dass $m \notin K[x_s, \ldots, x_n]$. Sei o.B.d.A. $m = x_1 * p$, wobei $p \in K[x_1, \ldots, x_n]$. Dann wäre aber $m >_{hlex} in_{hlex}(f)$. Das ist aber ein Widerspruch.

(iii) Sei f ein homogenes Polynom mit $in_{rlex}(f) \in (x_s, \ldots, x_n)$. Angenommen es gäbe ein Monom m in f, so dass $m \notin (x_s, \ldots, x_n)$. Dann folgt $m \in K[x_1, \ldots, x_{s-1}]$ und damit ist aber $m >_{rlex} in_{rlex}(f)$, woraus ein Widerspruch folgt.

□

Es stellt sich nun die Frage, wie man Termordnungen eines beliebigen freien Moduls mit Basis e_i erhält. Eine Möglichkeit eine solche Termordnung zu erhalten besteht darin, das lexikographische Produkt einer Termordnung der Monome $>$ und einer Ordnung der Basiselemente $\succ$ zu bilden.
Sei nun F ein freier S-Modul mit Basis und sei M ein Untermodul von F. Wie wir bereits gesehen haben, ist es sehr nützlich, die Moduln $in_>(M)$ zu bestimmen, was natürlich bedeutet ein Erzeugendensystem angeben zu können. Wir werden sehen, dass es sinnvoll ist, noch etwas mehr Informationen zu haben. Außer dem Erzeugendensystem möchten wir für jeden Erzeuger ein Element von M kennen, dessen Initialterm dieser Erzeuger ist. Die folgende wichtige Definition wird ein solches System beschreiben:

Definition 11.2.15 (Gröbnerbasis)**.** Eine *Gröbnerbasis* bezüglich einer Ordnung $>$ auf einem freien Modul mit Basis F ist eine Menge von Elementen $g_1, \ldots, g_t \in F$ mit folgender Eigenschaft: Für den von $g_1, \ldots, g_t$ erzeugten Untermodul M von F gilt $in_>(g_1), \ldots, in_>(g_t)$ erzeugen $in_>(M)$. Die Elemente $g_1, \ldots, g_t$ bilden dann eine *Gröbnerbasis für* M.

Beispiel 11.2.16. Als erstes betrachten wir den Fall mit null Variablen. Sei also S ein Körper und sei F ein Vektorraum der Dimension s mit Basis e_i. Wir identifizieren die Elemente aus F als Spaltenvektoren der Länge s. Die einzigen Monome in F sind die Basisvektoren e_i. Sei $>$ also die Termordnung in der $e_1 > e_2 > \ldots$ gilt.
Eine Menge von Elementen $g_1 \ldots, g_t \in F$ kann man als $s \times t$ Matrix G über S betrachten. G ist genau dann eine Gröbnerbasis, wenn G eine maximale linear unabhängige Menge enthält, so dass die Spaltenvektoren ihren ersten von null verschiedenen Eintrag in unterschiedlichen Zeilen haben. D.h. man kann die Matrix dieser maximal linear unabhängigen Menge auf Stufenform bringen (siehe unten).

$$\begin{pmatrix} \bullet & 0 & 0 & 0 & 0 \\ \bullet & 0 & 0 & 0 & 0 \\ \bullet & \bullet & 0 & 0 & 0 \\ \bullet & \bullet & \bullet & 0 & 0 \\ \bullet & \bullet & \bullet & 0 & 0 \\ \bullet & \bullet & \bullet & \bullet & 0 \end{pmatrix}$$

Beispiel 11.2.17. Nun betrachten wir den Fall mit einer Variablen. Sei $S = K[x]$ ein Polynomring über einem Körper K und sei $F = S$. Nach Beispiel 8.2.11 gibt es nur die Termordnung nach dem Grad. Ein Untermodul $M \subset F$ ist also ein Ideal. Das

Monomideal $in(M)$ wird damit von x^d erzeugt, wobei d der kleinste Grad der Polynome in M ist. Insgesamt besteht eine Gröbnerbasis von M aus einer Menge von Erzeugern von M, die ein Element minimalen Grades d enthält. Aus folgendem Lemma folgt übrigens, dass jedes Ideal von einem beliebigen Element minimalen Grades erzeugt wird.

Für jeden Untermodul M von F gibt es eine Gröbnerbasis bezüglich jeder Ordnung $>$. Seien $g_1, \ldots, g_t$ Erzeuger von M, die keine Gröbnerbasis sind, so kann man solange Elemente $g_{t+1}, \ldots, g_u \in M$ hinzunehmen, bis $in(g_1), \ldots in(g_u)$ den Modul $in(M)$ erzeugen. Das geht nach dem Hilbertschen Basissatz. Das folgende Lemma zeigt, dass eine Menge von Elementen in M, deren Initialterme $in(M)$ erzeugen auch schon M erzeugen. Um zu prüfen, ob eine Menge von Elementen in M Gröbnerbasis sind, genügt es zu prüfen, dass die Initialterme $in(M)$ erzeugen.

Lemma 11.2.18. *Sei F freier Modul, seien $N \subset M \subset F$ Untermoduln und sei $in(N) = in(M)$ bezüglich einer Termordnung. Dann folgt $N = M$.*

Beweis. Angenommen $N \neq M$. Dann gäbe es ein Element $f \in M$, $f \notin N$. Wir wählen f so, dass der Initialterm $in(f)$ unter allen Elementen, die nicht in N liegen, minimal ist. Da $in(f) \in in(M) = in(N)$, gibt es ein $g \in N$ mit $in(g) = in(f)$. Dann gilt aber $f - g \in M, f - g \notin N$, aber der Initialterm $in(f - g)$ ist kleiner als der Initialterm $in(f)$. Das ist ein Widerspruch. □

Folgerung 11.2.19. *Wenn wir Gröbnerbasen bestimmen können, so können wir mit diesem Lemma die Frage, ob ein Element in einem Untermodul liegt beantworten: Sei M ein Untermodul eines freien Moduls mit Basis F und sei $f \in F$. Um zu erkennen, ob $f \in M$ gilt, tun wir folgendes: Wähle eine Termordnung auf F und bestimme Gröbnerbasen von M und $M + Sf$. Nach dem Lemma liegt f genau dann in M, wenn $in(M) = in(M + Sf)$. Da $in(M)$ und $in(M + Sf)$ Monomuntermoduln sind, ist dies einfach zu überprüfen.*

11.3 Berechnung von Gröbnerbasen

In diesem Abschnitt des Kapitels über Gröbnerbasen werden wir nun zeigen, wie man aus einer gegebenen Menge von Erzeugern eines Untermoduls M eine Gröbnerbasis für diesen Untermodul berechnet. Dazu führen wir zuerst den Divisionsalgorithmus als wichtigstes Hilfsmittel ein. Danach benutzen wir Buchbergers Kriterium, um daraus den derzeit besten Algorithmus zur Berechnung von Gröbnerbasen, Buchbergers Algorithmus abzuleiten. Abschließend verdeutlichen wir dessen Funktionsweise anhand eines einfachen Beispiels.
Doch zuerst geben wir die Definition eines Standardausdrucks innerhalb der nächsten Proposition:

Proposition 11.3.1. *Sei F ein freier S-Modul mit Basis und einer Termordnung $>$. Für $f, g_1, \ldots, g_t \in F$ existiert ein Ausdruck*

$$f = \sum_{i=1}^{t} f_i g_i + f' \quad \text{mit} \quad f' \in F, f_i \in S$$

wobei kein Monom von f' in $(in(g_1), \ldots, in(g_t))$ ist und $in(f) \geq in(g_i)$ für alle i.
Ein solches f' bezeichnet man als einen ***Rest von*** *f bezüglich $g_1, \ldots, g_t$ und ein Ausdruck $f = \sum f_i g_i + f'$, der die genannten Bedingungen erfüllt, wird als ein* ***Standardausdruck für*** *f durch $g_1, \ldots, g_t$ bezeichnet.*

Als Beweis geben wir einen Algorithmus zur Berechnung eines solchen Standardausdrucks.

Algorithmus 11.3.2 (Divisionsalgorithmus)**.** Sei F ein freier S-Modul mit Basis und einer Termordnung $>$. Für $f, g_1, \ldots, g_t \in F$ können wir einen Standardausdruck

$$f = \sum_u m_u g_{s_u} + f'$$

für f bezüglich $g_1, \ldots, g_t$ durch induktives Definieren der Indizes s_u und der Terme m_u konstruieren.

Seien $s_1, \ldots, s_p$ und $m_1, \ldots, m_p$ schon so gewählt, dass

$$f'_p := f - \sum_{u=1}^{p} f_u g_{s_u} \neq 0$$

und sei m der maximale Term von f'_p, der durch $in(g_i)$ für mindestens ein i teilbar ist. Dann wähle:

$$s_{p+1} = i,$$
$$m_{p+1} = \frac{m}{in(g_i)}.$$

Dieser Vorgang terminiert entweder wenn $f'_p = 0$ oder kein $in(g_i)$ ein Monom von f'_p teilt. In diesem Fall ist f'_p dann ein Rest f' von f.

Ein mit diesem Algorithmus produzierter Standardausdruck ist nicht eindeutig. Er hängt von der Wahl des i's ab, wenn f'_p durch mehrere $in(g_i)$ teilbar ist. Daher kann f verschiedene Reste f' bezüglich $g_1, \ldots, g_t$ besitzen.
Wenn die $g_1, \ldots, g_t$ eine Gröbnerbasis für einen Untermodul M von F bilden, erhalten wir mit diesem Algorithmus durch den Rest f' gerade einen Ausdruck für $f \; mod \; M$ in F/M.
Mit Hilfe des Divisionsalgorithmus können wir nun zu einem gegebenen Untermodul M von F mit Erzeugern $g_1, \ldots, g_t$ eine Gröbnerbasis und die Syzygien zwischen den Erzeugern berechnen. Dazu erst noch mal einige Notationen, die wir im Folgenden benutzen werden.

Schreibweise 11.3.3. Sei F ein freier S-Modul mit endlicher Basis e_i, einer Termordnung $>$ und seien $g_1, \ldots, g_t \in F$ ungleich 0. Außerdem sei $\bigoplus_{i=1}^{t} S\varepsilon_i$ ein weiterer freier S-Modul mit Basis $\{\varepsilon_i\}$ und

$$\varphi : \bigoplus_{i=1}^{t} S\varepsilon_i \longrightarrow F \quad \text{mit} \quad \varphi(\varepsilon_i) = g_i.$$

Für jedes Paar von Indizes i, j, so dass $in(g_i)$ und $in(g_j)$ das gleiche Basiselement von F beinhalten, definiere:

$$m_{ij} = \frac{in(g_i)}{ggT(in(g_i), in(g_j))} \in S$$

und

$$\sigma_{ij} = m_{ji}\varepsilon_i - m_{ij}\varepsilon_j.$$

Dann erzeugen laut Satz 11.1.8

die σ_{ij} die Syzygien der $in(g_i)$. Für jedes dieser Paare i, j wählen wir einen Standardausdruck

$$\varphi(\sigma_{ij}) = m_{ji}g_i - m_{ij}g_j = \sum_u f_u^{ij} g_u + h_{ij}$$

für $m_{ji}g_i - m_{ij}g_j$ bezüglich $g_1, \ldots, g_t$. Die m_{ij} sind gerade so gewählt, dass sich die Initialterme in dieser Summe gegenseitig aufheben. Daher gilt $in(f_u^{ij} g_u) < in(m_{ji}g_i)$.
Falls $in(g_i)$ und $in(g_j)$ verschiedene Basiselemente von F beeinhalten setzen wir $h_{ij} = 0$.

Nun haben wir alles um Buchbergers Kriterium zu aufzustellen.

Satz 11.3.4 (Buchbergers Kriterium)**.** *Die Elemente $g_1, \ldots, g_t$ bilden eine Gröbnerbasis für $M = (g_1, \ldots, g_t)$ genau dann, wenn $h_{ij} = 0$ für alle Paare von Indizes i, j.*

Beweis. "⇒" Sei $M = (g_1, \ldots, g_t) \subset F$. An dem Standardausdruck für $m_{ji}g_i - m_{ij}g_j (\in M)$ sehen wir, dass $h_{ij} \in M$ sein muss, da auch $\sum f_u^{ij} g_u$ in M ist. Bilden die g_i nun eine Gröbnerbasis für M, dann folgt aus dem Nachsatz zum Divisionsalgorithmus, dass h_{ij} gleich 0 ist.

"⇐" Nun gelte $h_{ij} = 0$ für alle Indizes ij. Dann gilt

$$\varphi(\sigma_{ij}) = \sum_u f_u^{ij} g_u \quad \text{mit} \quad in(f_u^{ij} g_u) < in(m_{ji}g_i).$$

Wenn die $g_1, \ldots, g_t$ keine Gröbnerbasis für $M = (g_1, \ldots, g_t)$ bilden, dann können wir ein $f = \sum_u f_u \varepsilon_u \in \bigoplus S\varepsilon_i$ mit $f_u \in S$ finden, so dass $in(\varphi(f))$ in $in(M)$ ist (da $\varphi(f) \in M$); aber $in(\varphi(f))$ liegt nicht in $(in(g_1), \ldots, in(g_t))$, da $(in(g_1), \ldots, in(g_t))$ eine echte Teilmenge von $in(M)$ ist.
Sei nun m das maximale Monom, welches in den Termen $in(f_u g_u)$ auftaucht. Die g_i in F haben die Form $\sum_j \alpha_{ij} e_j$ mit $\alpha_{ij} \in S$. Daher hat m die Form $n_u \alpha_{ij} e_j$, wobei n_u ein Term von f_u ist. Nun wählen wir f so, dass m minimal wird und auch die Anzahl, mit der m in den $in(f_u g_u)$ auftaucht, minimal ist. Da $in(\varphi(f))$ nicht in $(in(g_1), \ldots, in(g_t))$ liegt, m aber schon, folgt daher, dass sich die Terme der $f_u g_u$, die m enthalten, gegenseitig aufheben müssen. Andernfalls wäre $in(f) = m$ wegen der Maximalität von m. Also müssen mindestens zwei der $f_u g_u$ den Term m beinhalten. Durch Umnummerierung der g_i können wir o.B.d.A. annehmen, dass dies $in(f_1 g_1)$ und $in(f_2 g_2)$ sind. Da $m = n_u \alpha_{ij} e_j$ können wir $in(f_1 g_1)$ und $in(f_2 g_2)$ als $n_1 m_1$ und $n_2 m_2$ schreiben, wobei n_1, n_2 jeweils Terme aus f_1, f_2 und m_1, m_2 Monome in F mit gleichem Basiselement sind. Die Terme $n_1 m_1$ und $n_2 m_2$ unterscheiden sich dann nur durch einen Skalar. Daher ist n_1 durch

$\frac{m_2}{ggT(m_1,m_2)} = m_{21}$ teilbar und es gibt einen Term n in S mit $nm_{21} = n_1$.
Betrachten wir nun

$$f' = f - n(\sigma_{12} - \sum_u f_u^{12} g_u) \in \bigoplus S\varepsilon_i$$

und dessen Ausdruck $\sum_u f'_u \varepsilon_u$ in den Basiselemente von $\bigoplus S\varepsilon_i$. Da wir $h_{ij} = 0$ vorausgesetzt haben, folgt, dass $\varphi(\sigma_{12}) = \sum_u f_u^{12} g_u$ und daher $\varphi(f) = \varphi(f')$. Da die Terme von $\varphi(nf_u^{ij}\varepsilon_u)$ Terme von $\varphi(f')$ sind, sind sie auch Terme von $\varphi(f)$, und somit kleiner als m. Der Term $n_1\varepsilon_1$ aus f und der Term $nm_{21}\varepsilon_2$ aus $n\sigma_{12}$ heben sich gegenseitig auf. Der Rest von $n\sigma_{12}$, also $nm_{12}\varepsilon_2$, addiert sich mit $n_2\varepsilon_2$ aus f. Daher verschwindet der Term m wenigstens einmal und da alle anderen dazukommenden Terme kleiner als m sind, folgt, dass m in $in(f'_u g_u)$ weniger häufig auftaucht als in $in(f_u g_u)$. Das ist ein Widerspruch zu unserer Wahl von f. Daher müssen die $g_1, \ldots, g_t$ eine Gröbnerbasis für M bilden. □

Mit Buchbergers Kriterium und dem Divisionsalgorithmus können wir nun Buchbergers Algorithmus zur Berechnung von Gröbnerbasen aufstellen.

Algorithmus 11.3.5 (Buchbergers Algorithmus)**.** Sei M ein Untermodul von F mit Erzeugern $g_1, \ldots, g_t$. Berechne die Reste h_{ij} wie in der Notation gegeben. Falls alle $h_{ij} = 0$, bildet $\{g_1, \ldots, g_t\}$ schon eine Gröbnerbasis für M. Andernfalls ergänze $\{g_1, \ldots, g_t\}$ mit $h_{ij} \neq 0$ und wiederhole den Prozess.
Dieser Prozess terminiert nach endlich vielen Schritten, da der durch die Initialterme von $g_1, \ldots, g_t, h_{ij}$ erzeugte Untermodul echt größer ist, als der nur durch die Initialterme von $g_1, \ldots, g_t$ erzeugte Untermodul und wir nur endlich erzeugte Moduln betrachten.

Beispiel 11.3.6. Seien $S = K[x, y, z]$, $F = S$ mit der umgekehrten lexikographischen Ordnung und $x > y > z$. Wir berechnen nun eine Gröbnerbasis für $M = (g_1, g_2, g_3)$ mit

- $g_1 = x^2$,
- $g_2 = y^2$,
- $g_3 = xy + yz$.

Zuerst berechnen wir die m_{ij}:

$$\begin{array}{rcl} m_{12} &=& \frac{in(g_1)}{ggT(in(g_1),in(g_2))} \\ &=& \frac{x^2}{ggT(x^2,y^2)} \\ &=& x^2 \end{array} \qquad \begin{array}{rcl} m_{21} &=& \frac{in(g_2)}{ggT(in(g_1),in(g_2))} \\ &=& \frac{y^2}{ggT(x^2,y^2)} \\ &=& y^2 \end{array}$$

$$\begin{array}{rcl} m_{13} &=& \frac{in(g_1)}{ggT(in(g_1),in(g_3))} \\ &=& \frac{x^2}{ggT(x^2,xy)} \\ &=& \frac{x^2}{x} \\ &=& x \end{array} \qquad \begin{array}{rcl} m_{31} &=& \frac{in(g_3)}{ggT(in(g_1),in(g_3))} \\ &=& \frac{xy}{ggT(x^2,xy)} \\ &=& \frac{xy}{x} \\ &=& y \end{array}$$

$$\begin{array}{rcl} m_{23} & = & \frac{in(g_2)}{ggT(in(g_2),in(g_3))} \\ & = & \frac{y^2}{ggT(y^2,xy)} \\ & = & \frac{y^2}{y} \\ & = & y \end{array} \qquad \begin{array}{rcl} m_{32} & = & \frac{in(g_3)}{ggT(in(g_2),in(g_3))} \\ & = & \frac{xy}{ggT(y^2,xy)} \\ & = & \frac{xy}{y} \\ & = & x \end{array}$$

Dann berechnen wir die h_{ij}:

$$\begin{aligned} m_{21} \cdot g_1 - m_{12} \cdot g_2 &= y^2 \cdot x^2 - x^2 \cdot y^2 \\ &= 0 \qquad\qquad \Rightarrow h_{12} = 0 \end{aligned}$$

$$\begin{aligned} m_{31} \cdot g_1 - m_{13} \cdot g_3 &= y \cdot x^2 - x \cdot (xy + yz) \\ &= -xyz \\ &= -z \cdot g_3 + yz^2 \qquad\qquad \Rightarrow h_{13} = yz^2 \end{aligned}$$

$$\begin{aligned} m_{23} \cdot g_3 - m_{32} \cdot g_2 &= x \cdot y^2 - y \cdot (xy + yz) \\ &= -y^2 z \\ &= -z \cdot g_2 \qquad\qquad \Rightarrow h_{23} = 0 \end{aligned}$$

Da $h_{13} \neq 0$ erweitern wir die g_i durch $h_{13} = g_4 = yz^2$ und wiederholen den Prozess:

$$\begin{array}{rcl} m_{14} & = & \frac{in(g_1)}{ggt(in(g_1),in(g_4))} \\ & = & \frac{x^2}{ggt(x^2,yz^2)} \\ & = & x^2 \end{array} \qquad \begin{array}{rcl} m_{41} & = & \frac{in(g_4)}{ggt(in(g_1),in(g_4))} \\ & = & \frac{yz^2}{ggt(x^2,yz^2)} \\ & = & yz^2 \end{array}$$

$$\begin{array}{rcl} m_{24} & = & \frac{in(g_2)}{ggt(in(g_2),in(g_4))} \\ & = & \frac{y^2}{ggt(y^2,yz^2)} \\ & = & y \end{array} \qquad \begin{array}{rcl} m_{42} & = & \frac{in(g_4)}{ggt(in(g_2),in(g_4))} \\ & = & \frac{yz^2}{ggt(y^2,yz^2)} \\ & = & z^2 \end{array}$$

$$\begin{array}{rcl} m_{34} & = & \frac{in(g_3)}{ggt(in(g_3),in(g_4))} \\ & = & \frac{xy}{ggt(xy,yz^2)} \\ & = & x \end{array} \qquad \begin{array}{rcl} m_{43} & = & \frac{in(g_4)}{ggt(in(g_3),in(g_4))} \\ & = & \frac{yz^2}{ggt(xy,yz^2)} \\ & = & z^2 \end{array}$$

$$\begin{aligned} m_{41} \cdot g_1 - m_{14} \cdot g_4 &= yz^2 \cdot x^2 - x^2 \cdot yz^2 \\ &= 0 \qquad\qquad \Rightarrow h_{14} = 0 \end{aligned}$$

$$\begin{aligned} m_{42} \cdot g_2 - m_{24} \cdot g_4 &= z^2 \cdot y^2 - y \cdot yz^2 \\ &= 0 \qquad\qquad \Rightarrow h_{24} = 0 \end{aligned}$$

$$\begin{aligned} m_{43} \cdot g_3 - m_{34} \cdot g_4 &= z^2 \cdot (xy + yz) - x \cdot yz^2 \\ &= yz^3 \\ &= z \cdot g_4 \qquad\qquad \Rightarrow h_{34} = 0 \end{aligned}$$

Daraus folgt, dass $g_1, \ldots, g_4$ eine Gröbnerbasis für M bilden.

11.4 Berechnung von Syzygien

Zusätzlich zu der Berechnung einer Gröbnerbasis für M liefert uns Buchbergers Algorithmus eine effektive Methode zur Berechnung von Syzygien zu einer gegebenen Menge $\{g_1, \ldots, g_t\}$ von Elementen von F. Der nächste Satz beweist sogar, dass die so berechneten Syzygien schon alle Syzygien auf dieser Menge erzeugen. Dazu erweitern wir zunächst unsere Notation.

Schreibweise 11.4.1. Für jedes Paar von Indizes i, j, für welches $in(g_i)$ und $in(g_j)$ das gleiche Basiselement von F beinhalten, setze:

$$\tau_{ij} = m_{ji}\varepsilon_i - m_{ij}\varepsilon_j - \sum_u f_u^{ij}\varepsilon_u.$$

Satz 11.4.2 (Satz von Schreyer)**.** *Sei $g_1, \ldots, g_t$ eine Gröbnerbasis. Definiere eine Termordnung $>$ auf $\bigoplus S\varepsilon_i$ durch $m\varepsilon_u > n\varepsilon_v$ genau dann, wenn*

$$in(mg_u) > in(ng_v)$$

oder

$$in(mg_u) = k \cdot in(ng_v) \text{ für einen Skalar } k \in K, \text{ aber } u < v.$$

Dann erzeugen die τ_{ij} die Syzygien auf den g_i. Die τ_{ij} bilden sogar eine Gröbnerbasis für die Syzygien bezüglich $>$ und es gilt $in(\tau_{ij}) = m_{ji}\varepsilon_i$.

Beweis. Zuerst zeigen wir, dass $m_{ji}\varepsilon_i$ der Initialterm von τ_{ij} ist. Die m_{ij} sind gerade so gewählt, dass sich bei $\varphi(\sigma_{ij}) = m_{ji}g_i - m_{ij}g_j$ die Initialterme gegenseitig aufheben, d.h. $m_{ji}in(g_i) = m_{ij}in(g_j)$. Daher ist dieser Term größer als jeder andere Term in $\sum_u f_u^{ij} g_u$. Mit der Definition von $>$ folgt dann, dass $in(\tau_{ij})$ entweder $m_{ji}\varepsilon_i$ oder $-m_{ij}\varepsilon_j$ ist. Da $i < j$ ist, gilt $m_{ji}\varepsilon_i > m_{ij}\varepsilon_j$ und daher ist $m_{ji}\varepsilon_i$ der Initialterm von τ_{ij}.
Nun zeigen wir, dass die τ_{ij} eine Gröbnerbasis für die Syzygien bilden. Dazu sei $\tau = \sum_v f_v\varepsilon_v$ mit $f_v \in S$ eine Syzygie, d.h. $\varphi(\tau) = 0$. Wir müssen zeigen, dass $in(\tau)$ in dem

von den $in(\tau_{ij})$ erzeugten Untermodul liegt, d.h. $in(\tau) = \sum_{i,j} s_{ij} in(\tau_{ij})$ mit $s_{ij} \in S$. Nun setzen wir $n_v \varepsilon_v = in(f_v \varepsilon_v)$ mit $n_v \in S$ für jeden Index v. Da diese Terme verschiedene Basiselemente von $\bigoplus S\varepsilon_i$ enthalten, können sie sich nicht gegenseitig aufheben, und wir haben $in(\tau) = n_i \varepsilon_i$ für einen Index i. Jetzt nehmen wir alle Indizes v, für die gilt $n_v in(g_v) = k \cdot n_i in(g_i)$ für einen Skalar $k \in K$ und bilden darüber die Summe $\sigma = \sum_{v \in X} n_v \varepsilon_v$, wobei $X = \{v | n_v in(g_v) = k \cdot n_i in(g_i)\}$. Da $n_i \varepsilon_i$ der Initialterm von τ ist, gilt $v \geq i$ für alle diese v in σ. Da $\varphi(\tau) = 0$ muss sich das Bild von $in(\tau)$ mit anderen Termen aus $\varphi(\tau)$ aufheben. Genau diese Terme haben wir in σ gesammelt. Daher gilt $\varphi(\sigma) = 0$.
D.h. σ ist eine Syzygie über $in(g_v)$ für $v \geq i$. Laut Satz 11.1.8 werden alle solche Syzygien (die $in(g_i)$ sind Monome) durch die dort beschriebenen $\sigma_{uv} = m_{vu}\varepsilon_u - m_{uv}\varepsilon_v$ mit $u, v \geq i$ erzeugt, d.h. $\sigma = \sum_{u,v \geq i} s_{uv} \sigma_{uv}$ mit $s_{uv} \in S$. Sammeln wir auf beiden Seiten die Einträge, die ε_i enthalten, erhalten wir $n_i \varepsilon_i = \sum_{j>i} s_{ij} m_{ji} \varepsilon_i$ und sind fertig. □

Um nun für eine gegebene Menge $\{g_1, \ldots, g_t\}$ in F die Syzygien zu berechnen, benutzen wir zuerst Buchbergers Algorithmus um eine Gröbnerbasis für $(g_1, \ldots, g_t)$ und die Syzygien für diese zu berechnen. Falls dabei zusätzliche g_i entstehen, müssen wir diese nur durch ihren Ausdruck in den ursprünglichen $g_1, \ldots, g_t$ in den Syzygien ersetzen.
Diese Erweiterung von Buchbergers Algorithmus zur Berechnung von Syzygien führen wir nochmal anhand eines Beispiels vor. Dazu erweitern wir einfach das Beispiel aus dem letztem Abschnitt.

Beispiel 11.4.3 (Fortsetzung von Beispiel 11.3.6)**.** Seien $S = K[x, y, z]$, $F = S$ mit der umgekehrten lexikographischen Ordnung und $x > y > z$. Sei $M = (g_1, g_2, g_3)$ mit

- $g_1 = x^2$,
- $g_2 = y^2$,
- $g_3 = xy + yz$.

Aus Buchbergers Algorithmus erhalten wir zusätzlich $g_4 = yz^2$ und

$$\begin{aligned}
\tau_{12} &= y^2\varepsilon_1 - x^2\varepsilon_2 \\
\tau_{13} &= y\varepsilon_1 - x\varepsilon_3 + z\varepsilon_3 - \varepsilon_4 = y\varepsilon_1 - (x - z)\varepsilon_3 - \varepsilon_4 \\
\tau_{14} &= yz^2\varepsilon_1 - x^2\varepsilon_4 \\
\tau_{23} &= x\varepsilon_2 - y\varepsilon_3 + z\varepsilon_2 = (x + z)\varepsilon_2 - y\varepsilon_3 \\
\tau_{24} &= z^2\varepsilon_2 - x\varepsilon_4 \\
\tau_{34} &= z^2\varepsilon_3 - x\varepsilon_4 - z\varepsilon_4
\end{aligned}$$

Jetzt setzen wir $\tau_{13} = 0$ und ersetzen ε_4 durch den dadurch entstehenden Ausdruck in ε_1 und ε_3. Damit erhalten wir

$$\begin{aligned}\tau_{14} &= yz^2\varepsilon_1 - x^2(y\varepsilon_1 - (x-z)\varepsilon_3)\\ &= (yz^2 - x^2y)\varepsilon_1 + (x^3 - x^2z)\varepsilon_3\end{aligned}$$

$$\begin{aligned}\tau_{24} &= z^2\varepsilon_2 - x(y\varepsilon_1 - (x-z)\varepsilon_3)\\ &= -xy\varepsilon_1 + z^2\varepsilon_2 - (x-z)\varepsilon_3\end{aligned}$$

$$\begin{aligned}\tau_{34} &= z^2\varepsilon_3 - (x+z)(y\varepsilon_1 - (x-z)\varepsilon_3)\\ &= -(xy - yz)\varepsilon_1 + x^2\varepsilon_3\end{aligned}$$

Die Syzygien von g_1, g_2 und g_3 werden durch τ_{12}, τ_{23}, τ_{14}, τ_{24} und τ_{34} erzeugt.

11.5 Verallgemeinerte Initialideale

Bis jetzt haben wir Gröbnerbasen immer in Bezug auf eine vorher gewählte Menge von festen Variablen eines Polynomringes und einer festen Menge von Erzeugern eines freien Moduls über diesem Polynomring betrachtet. Die berechneten Gröbnerbasen hingen dabei sehr stark von der Wahl der Variablen und der Basis ab. Nun wollen wir durch allgemeine Änderungen der gewählten Mengen sogenannte *verallgemeinerte Initialideale* berechnen, die nur noch von der Wahl der Termordnung abhängen. Wir werden uns hier auf Ideale beschränken, die Ergebnisse können jedoch auf Untermoduln von graduierten freien Moduln erweitert werden. Im ganzen Kapitel sei $S = K[x_1, \ldots, x_r]$ und $>$ eine Termordung auf S, die die Ordnung nach dem Grad erhält und für die $x_1 > \ldots > x_r$ gilt. Alle betrachteten Ideale sind homogen. Anstatt Transformationen in den Koordinaten vorzunehmen, werden wir ein Ideal unter einer allgemeinen linearen Transformation abbilden und dessen Initialideal zu den gegeben Koordinaten angeben.

Zuerst benötigen wir einige Notationen für die benutzten Transformationsgruppen.

Schreibweise 11.5.1. Wir bezeichnen die *allgemeine lineare Gruppe* der invertierbaren $r \times r$ -Matrizen mit GL. Diese Gruppe wirkt als eine Gruooe von Algebra-Automorphismen auf S wie folgt: Sei g eine Matrix mit Eintrag g_{ij} an der Stelle (i,j) und $x_i \in S$. Wir definieren $g(x_j)$ als $\sum_i g_{ij}x_i$. Für ein beliebiges Monom $m = \prod_j x_j^{a_j}$ von S definiere $g(m)$ als $gm = \prod_j (\sum_i g_{ij}x_i)^{a_j}$.
Einige Untergruppen von GL spielen eine besondere Rolle. Mit $\mathcal{B}$ bezeichen wir die Gruppe der invertierbaren oberen Dreiecksmatrizen oder *Borel-Untergruppe* von GL. Entprechend ist $\mathcal{B}'$ die Gruppe der invertierbaren unteren Dreiecksmatrizen.
$\mathcal{U}$ bezeichnet die *unipotente Untergruppe von* $\mathcal{B}$, d.h. alle oberen Dreiecksmatrizen mit Einsen auf den Diagonalen. $\mathcal{U}$ wird erzeugt von den *elementaren oberen Dreiecksmatrizen* γ_{ij}^c für $i < j$ und $c \in K$, wobei $\gamma_{ij}^c x_u = x_u$ für $u \neq j$ und $\gamma_{ij}^c x_i = cx_i + x_j$. Genauso wird $\mathcal{B}'$ von den Diagonalmatrizen und den *elementaren unteren Dreiecksmatrizen* $\gamma_{ij}'^c$ erzeugt. Hierbei ist $\gamma_{ij}'^c x_u = x_u$ für $u \neq i$ und $\gamma_{ij}'^c x_i = x_i + cx_j$.

Außerdem benötigen wir die Definition einer äußeren Algebra.

Definition 11.5.2. Sei V ein Modul über einem kommutativen Ring K mit Einselement. Dann ist die *Tensoralgebra* definiert als

$$TV = \bigoplus_{n\geq 0} V^{\otimes n} = K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \dots$$

Die *äußere Algebra* oder *Grassmann-Algebra* $\bigwedge V$ ist definiert als der Quotient von TV nach dem zweiseitigen Ideal, das von den Elementen $v \otimes v$, $v \in V$ erzeugt wird.
Elemente der Form $v_1 \wedge v_2 \wedge \dots \wedge v_k$ mit $v1, \dots, v$ in V heißen k-Vektoren. Der von allen k-Vektoren erzeugte Unterraum von von $\bigwedge V$ heißt k-te äußere Potenz von V und wird mit $\bigwedge^k V$ bezeichnet.
Sind V, W zwei Vektorräume (bzw. Moduln), so entsprechen die Homomorphismen

$$\bigwedge^k V \to W$$

den alternierenden k-multilinearen Abbildungen

$$V \times \dots \times V \to W.$$

Sei $V \subset S_d$ ein t-dimensionaler Unterraum von Formen vom Grad d. Dann können wir V als eindimensionalen Unterraum $L = \bigwedge^t V \subset \bigwedge^t S_d$ auffassen. Wenn V die Basis $f_1, \dots, f_t$ besitzt, so wird L von $f := f_1 \wedge \dots \wedge f_t$ erzeugt. Wir definieren ein *Monom von* $\wedge^t S_d$ als ein Element der Form $n = n_1 \wedge \dots \wedge n_t$, wobei die n_i Monome vom Grad d in S sind. Wenn die n_i nicht alle paarweise verschieden sind, ist $n = 0$. Ein *Term von* $\wedge^t S$ ist definiert als ein Produkt $a \cdot n$ mit $a \in K$ und einem Monom n. Wir bezeichnen $a \cdot n = a \cdot n_1 \wedge \dots \wedge n_t$ als *Standardausdruck*, falls die n_i so geordnet sind, dass $n_1 > \dots > n_t$.
Wir ordnen die Monome von $\wedge^t S$ durch lexikographische Ordnung der Standardausdrücke. D.h. wenn $n = n_1 \wedge \dots \wedge n_t$ und $n' = n'_1 \wedge \dots \wedge n'_t$ Standardausdrücke sind, dann gilt $n > n'$ genau dann, wenn $n_i > n'_i$ für das kleinste i mit $n_i \neq n'_i$. Wie in Kapitel 11.2 erweitern wir dies zu einer Ordnung auf den Termen und definieren den Initialterm als den größten Term bezüglich der gegeben Ordnung. Wir können die f_i linear mit sich selbst kombinieren ohne V zu ändern. So können wir erreichen, dass die $in(f_i)$ alle verschieden sind und $in(f_1) > \dots > in(f_t)$. Durch diese Wahl ist $in(f_1) \wedge \dots \wedge in(f_t)$ ein Standardausdruck für den Initialterm von f.

Nun haben wir alle Hilfsmittel zusammen, um die Existenz des verallgemeinerten Initialideals zu zeigen.

Satz 11.5.3. *Sei $I \subset S$ ein homogenes Ideal. Es gibt eine bezüglich der Zariski-Topologie offene Menge $U = \mathcal{B}'U \subset GL$, die $\mathcal{U}$ nichttrivial schneidet, und ein Monomideal $J \subset S$, so dass für alle $g \in U$ gilt $in(gI) = J$. Für jedes $d \geq 0$ gilt, wenn der Teil J_d von J, der die Formen vom Grad d enthält, Dimension t hat, dann wird $\wedge^t J_d$ vom größten Monom von $\wedge^t S_d$, das in einem $\wedge^t(gI_d)$ mit $g \in GL$ auftaucht, erzeugt.*

Offen bezüglich der Zariski-Topologie bedeutet, dass das Komplement von U gerade die gemeinsame Nullstellenmenge einer Menge von Polynomen ist. Zariski-offene Mengen sin also „groß“, da ihre Komplemente Nullmengen sind. U enthält also fast alle Elemente aus GL, d.h. $J = in(gI)$ für fast alle $g \in GL$.

Definition 11.5.4. Seien I, J wie im Satz. Dann heißt J das *verallgemeinerte Initialideal* von I. Wir schreiben $J = Gin(I)$.

Wir führen den Beweis in mehreren Schritten. Zuerst zeigen wir, dass das Ideal J existiert und die gewünschten Eigenschaften hat. Die anderen Behauptungen ergeben sich dann aus dem folgenden Lemma und dem anschließenden Satz.

Beweis. Betrachte den Teil I_d von I, der die Formen vom Grad d enthält. Sei $f_1, \ldots, f_t$ eine Basis von I_d und sei $h = (h_{ij})$ ein Matrix aus Variablen. Dann ist $h(f_1 \wedge \ldots \wedge f_t) = h(f_1) \wedge \ldots \wedge h(f_t)$ eine Linearkombination von Monomen in $\wedge^t S$ mit Koeffizienten aus Polynomen in den h_{ij}. Wir nehmen an, $m = m_1 \wedge \ldots \wedge m_t$ sei das erste Monom mit einem Koeffizienten ungleich 0 und $p_d(h_{11}, \ldots, h_{rr})$ sei dieser Koeffizient. Sei U_d die Menge $\{g = (g_{ij}) \in \mathcal{G} | p_d(g_{11}, \ldots, g_{rr}) \neq 0\}$. Der Grad-$d$-Teil des Initialideals von gI ist genau dann $(m_1, \ldots m_t)$, wenn $g \in U_d$. Wir schreiben J_d für den Unterraum von S_d, der von $m_1, \ldots m_t$ erzeugt wird.
Als nächstes zeigen wir, dass $J := \bigoplus J_d$ ein Ideal ist. Es genügt dabei zu zeigen, dass $S_1 J_d \subset J_{d+0}$ für jedes d gilt. Da U_d und U_{d+1} offen und dicht sind, gibt es ein Element $g \in U_d \cap U_{d+1}$. Nun gilt $in(gI)_d = J_d$ und $in(gI)_{d+1} = J_{d+1}$, woraus die Behauptung folgt.
Das Ideal J erfüllt die letzte Aussage des Satzes per Definition. Wir zeigen nun, dass $U = \bigcap_{d=1}^{\infty} U_d$ offen bezüglich der Zariski-Topologie und dicht in GL ist. Da jedes U_d nach Konstruktion offen und dicht ist, genügt es zu zeigen, dass U schon ein endlicher Schnitt von U_d ist. Wir nehmen an, J sei von Formen vom Grad $\leq e$ erzeugt und zeigen, dass tatsächlich gilt $U = \bigcap_{d=1}^{e} U_d$.
Angenommen $g \in \bigcap_{d=1}^{e} U_d$. Wir wissen, dass $in(gI_d) = J_d$ für alle $d \leq e$. Also gilt $in(gI) \supseteq J$. Da $dim_K J_d = dim_K I_d = dim_K (gI)_d$ für jedes d, sehen wir, dass $in(gI) = J$ wie gewünscht. □

Als nächstes zeigen wir, dass $U = \mathcal{B}'U$. Das folgende Lemma gibt uns sogar noch etwas mehr.

Lemma 11.5.5. *Sei $I_d \subset S_d$ ein Unterraum der Dimension t und $b \in \mathcal{B}'$. Dann gilt $in(\wedge^t I_d) = in(\wedge^t b I_d)$.*

Beweis. Da $\mathcal{B}'$ von den Diagonalmatrizen und den elementaren unteren Dreiecksmatrizen erzeugt wird, genügt es die Behauptung für eine solche Matrix b zu zeigen. Wähle eine Basis $f_1, \ldots, f_t$ für I_d und sei $m_i = in(f_i)$. Durch Umsortieren der Basis können wir immer erreichen, dass $m_1 > \ldots > m_t$. Die Diagonalmatrizen verändern nur die Koeffizienten der Terme von $f = f_1 \wedge \ldots \wedge f_t$ durch Skalare ungleich 0, also stimmt die Behauptung für Diagonalmatrizen.
Sei nun $b = \gamma_{ij}^{'c}$ eine elementare untere Dreicksmatrix. Für jedes Monom $n = x_i^w m \in S_d$,

mit m nicht teilbar durch x_i, ist bn darstellbar als n plus eine Linearkombination von Monomen der Form $n' = x_i^{w-s}x_j^s$ mit $0 < s \leq w$. Da $x_i > x_j$ ist, gilt immer $n' < n$. Deshalb ist $in(bf_i) = m_i$ für $1 \leq i \leq t$, also $in(bf) = m_1 \wedge \ldots \wedge m_t = in(f)$. □

Nun müssen wir noch zeigen, dass U von $\mathcal{U}$ nichttrivial geschnitten wird. Die Menge $\mathcal{B}'\mathcal{U}$ ist eine dichte offene Teilmenge von GL. Also enthält die dichte Menge U ein Element der Form bu mit $b \in \mathcal{B}$ und $u \in \mathcal{U}$. Da $U = \mathcal{B}'U$ folgt, dass $u = b^{-1}bu \in U$.

Der nächste Satz zeigt, dass verallgemeinerte Initialideale spezielle Monomideale sind.

Satz 11.5.6 (Galligo, Bayer, Stillman)**.** *Sei $I \subset S$ ein homogenes Ideal. Dann gilt für alle $g \in \mathcal{B}$, dass $g(Gin(I)) = Gin(I)$.*

Beweis. Wenn wir I durch gI mit einem passenden g ersetzen, können wir nach Satz 11.5.3 annehmen, dass $in(I) = Gin(I)$. Sei $i < j$ und $\gamma_{ij}^1 = 1 + \gamma$ eine elementare obere Dreiecksmatrix, wobei γ eine strikte obere Dreiecksmatrix mit nur einem Eintrag ungleich 0 ist. Zusammen mit den Diagonalmatrizen erzeugen solchen Matrizen die Borel-Gruppe $\mathcal{B}$. Die Diagonalmatrizen halten jedes Ideal fest, denn sie multiplizieren nur die Variablen mir Skalaren aus K. Deshalb genügt es zu zeigen, dass $(1+\gamma)(in(I_d)) = in(I_d)$ für jeden Grad d gilt.
Wir wählen ein Basis $f_1, \ldots, f_t$ für I_d mit $in(f_1) > \ldots > in(f_t)$. Sei $f = f_1 \wedge \ldots \wedge f_t$ der entprechende Erzeuger des eindimensionalen Unterraums $\wedge^t I_d \subset \wedge^t S_d$. Der Initialterm von f ist dann $in(f) = in(f_1) \wedge \ldots \wedge in(f_t)$.
Falls $(1+\gamma)(in(I_d)) \neq in(I_d)$, dann ist auch $(1+\gamma)(in(f)) \neq in(f)$. Da γ eine strikte obere Dreiecksmatrix ist, sind die Terme von $(1+\gamma)(in(f))$, die nicht $in(f)$ sind, alle größer als $in(f)$. Sei am einer dieser Terme, wobei $a \neq 0$ ein Skalar ist und m ein Monom aus $\wedge^t S_d$. Wir müssen zeigen, dass für geeignete Diagonalmatrizen δ das Monom m mit einem Koeffizienten ungleich 0 in $(1+\gamma)\delta f$ auftaucht. Dies wäre ein Widerpruch zur letzten Behauptung aus Satz 11.5.3, was beweisen würde, dass doch $(1+\gamma)(in(I_d)) = in(I_d)$.
Für jeden Term $n = an_1 \wedge \ldots \wedge n_t \in \wedge^t S_d$ definieren wir das *Gewicht* von n als das Monom $w = \prod_s n_i \in S$. Sei $f_w \in \wedge^t S_d$ die Summe aller Terme in f mit Gewicht w, dann gilt $f = \sum_w f_w$. Weiter sei w_0 das Gewicht von $in(f)$. Verschiedene Terme von f können gleiche Gewichte haben, aber $in(f)$ ist der einzige Term mit Gewicht w_0. Wenn δ eine Diagonalmatrix ist und $\delta(x_i) = \delta_i x_i$ mit $\delta_i \in K^\times$, dann ist

$$\delta f = \sum_w w(\delta_1, \ldots, \delta_r) f_w,$$

wobei $w(\delta_1, \ldots, \delta_r) \in K^\times$ durch Ersetzen von x_i durch δ_i im Monom w entsteht. Also gilt

$$\begin{aligned}(1+\gamma)\delta f &= \sum_w (1+\gamma)(w(\delta_1, \ldots, \delta_r) f_w) \\ &= \sum_w w(\delta_1, \ldots, \delta_r)(1+\gamma) f_w \\ &= w_0(\delta_1, \ldots, \delta_r)(1+\gamma) in(f) + \sum_{w \neq w_0} w(\delta_1, \ldots, \delta_r)(1+\gamma) f_w.\end{aligned}$$

Also hat der Koeffizient von m in $(1+\gamma)\delta f$ die Form

$$c(\delta_1,\ldots,\delta_r) := aw_0(\delta_1,\ldots,\delta_r) + \sum_{w\neq w_0} a_w w(\delta_1,\ldots,\delta_r),$$

wobei $a_w \in K$ der Koeffizient von m in $(1+\gamma)f_w$ ist. Da der Term $aw_0(\delta_1,\ldots,\delta_r)$ nicht 0 ist, ist auch das Polynom c nicht das Nullpolynom. Da wir angenommen haben, dass der Grundkörper K unendlich ist, folgt, dass für genügend allgemeine Werte der $\delta_1,\ldots,\delta_r$ der Wert $c(\delta_1,\ldots,\delta_r)$ nicht 0 ist. Das war aber, was wir zeigen mussten. □

Nun geben wir noch eine Charakterisierung von borel-fixierten Idealen, also solchen, die durch Anwenden einer Matrix $b \in \mathcal{B}$ nicht verändert werden.
Um auch den Fall von Grundkörpern mit Charakteristik $p \neq 0$ betrachten zu können, ist eine „neue“ Partialordnung auf den natürlichen Zahlen nützlich.

Definition 11.5.7. Seien $a, b \in \mathbb{N}$. Schreibe $a \prec_p b$, falls $\binom{b}{a} \not\equiv 0 \ mod\ p$.

Für Charakteristik 0 ist das gerade die normale Ordung auf $\mathbb{N}$. Für $p > 0$ gab Gauss die folgende Bescheibung.

Proposition 11.5.8 (Gauss)**.** *Sei p eine Primzahl. Es gilt $a \prec_p b$ genau dann, wenn $a_i \leq b_i$ für allei mit $a = \sum a_i p^i$ und $b = \sum b_i p^i$ mit $0 \leq a_i, b_i < p$.*

Für den Beweis benötigen wir folgendes Lemma.

Lemma 11.5.9 (Lucas)**.** *Sei $a = \sum a_i p^i$ und $b = \sum b_i p^i$ mit $0 \leq a_i, b_i < p$. Dann gilt $\binom{b}{a} \equiv \prod_i \binom{b_i}{a_i} (mod\ p)$.*

Beweis. Betrachte

$$(t+1)^b = (t+1)^{\sum b_i p^i} = \prod (t+1)^{b_i p^i} \equiv \prod (t^{p^i}+1)^{b_i} (mod\ p).$$

Auf der linken Seite taucht der Term $\binom{b}{a} t^a$ auf. Der entprechende Term auf der rechten Seite hat den Koeffizienten $\prod_i \binom{b_i}{a_i}$. □

Nun können wir Proposition 11.5.8 beweisen.

Beweis. Falls $a \prec_p b$, ist $\binom{b}{a} \not\equiv 0\ (mod\ p)$. Also ist auch $0 \not\equiv \prod_i \binom{b_i}{a_i} (mod\ p)$, d.h. $a_i \leq b_i$. Falls $a_i \leq b_i \leq p$, ist das Produkt aus dem Lemma nicht 0, also auch nicht $\binom{b}{a}$. □

Der nächste Satz liefert eine kombinatorische Charakterisierung borel-fixierter Ideale.

Satz 11.5.10. *Sei $J \subset S = K[x_1,\ldots,x_r]$ ein Ideal und sei $charK = p \geq 0$.*

(i) *J wird von der Gruppe der invertierbaren Diagonalmatrizen genau dann fixiert, wenn J von Monomen erzeugt wird.*

(ii) *J ist genau dann Borel-fixiert, wenn J von Monomen erzeugt wird und für alle $i < j$ und alle Erzeuger von J gilt: Wenn m durch x_j^t teilbar ist, aber durch keine höhere Potenz von x_j, dann gilt $\left(\frac{x_i}{x_j}\right)^s m \in J$ für alle $i < j$ und $s \prec_p t$.*

Für den Beweis benötigen wir noch eine weitere Termordnung.

Definition 11.5.11. Wir definieren eine *Gewichtsfunktion* λ für S als eine lineare Funktion $\mathbb{R}^r \to \mathbb{R}$. Jede Gewichtsfunktion definiert eine partielle Ordnung $>_\lambda$ auf den Monomen von S, die sogenannte *zu λ assoziierte Gewichtsordnung*, durch $m = x^\alpha >_\lambda n = x^\beta$ genau dann, wenn $\lambda(\alpha) > \lambda(\beta)$. Für $g \in S$ ist $in_\lambda(g)$ definiert als die Summe aller Terme von g, die maximal bezüglich $>_\lambda$ sind.

Beweis von Satz 11.5.10. (i) Jedes Monomideal wird von Diagonalmatrizen fixiert, denn diese multiplizieren nur die Variablen mit Skalaren aus K.
Sei nun umgekehrt J von Diagonalmatrizen fixiert und $f \in J$. Es genügt zu zeigen, dass ein beliebiges Monom von f in J liegt. Wähle eine Gewichtsfunktion λ, so dass $in_\lambda(f)$ ein Monom ist, also nur ein Monom von f maximales Gewicht bezüglich λ hat. Wir werden zeigen, dass $in_\lambda(f) \in J$.
Sei w das Gewicht von $in_\lambda(f)$. Sei $\lambda_i = \lambda(x_i)$. Wenn wir auf f eine Diagonalmatrix $g_c = diag(c^{-\lambda_1}, \ldots, c^{-\lambda_r})$ anwenden, ersetzen wir jede Variable x_i durch $c^{-\lambda_i} x_i$, also wird $in_\lambda(f)$ mit c^{-w} multipliziert und alle anderen Terme von f mit strikt größeren Potenzen von c. Wir haben nun also die Darstellung $c^w g_c f = in_\lambda(f) + cF(c, x)$ für ein Polynom $F(c, x)$. Betrachte die Abbildung $\varphi : A^1_K \to S$ vom eindimensionalen affinen Raum über K nach S mit $\varphi(c) = c^w g_c f = in_\lambda(f) + cF(c, x)$. Da J von den Diagonalmatrizen fixiert wird, ist $\varphi(c) \in J$ für $c \neq 0$. Da J abgeschlossen bzgl. der Zariski Topologie ist, also die gemeinsame Nullstellenmenge von Polynomen, kann es nicht sein, dass $\varphi(0)$ nicht in J liegt. Deshalb liegt $\varphi(0) = in_\lambda(f)$ in J.

(ii) Wenn J borel-fixiert ist, dann wird J nach (i) von Monomen erzeugt, denn die Diagonalmatrizen sind eine Teilmenge von $\mathcal{B}$. Für einen monomialen Erzeuger m von J betrachten wir die Wirkung einer elementaren oberen Dreiecksmatrix $\gamma = \gamma_{ij}^c$ auf m. Wir schreiben hierzu $m = x_j^t m'$, wobei m' nicht durch x_j teilbar ist. Dann gilt

$$\gamma m = (cx_i + x_j)^t m' = \sum_{s \prec_p t} \binom{t}{s} (cx_i)^s x_j^{t-s} m' = \sum_{s \prec_p t} \binom{t}{s} c^s \left(\frac{x_i}{x_j}\right)^s m.$$

Da J von γ nicht verändert wird, muss jedes $\left(\frac{x_i}{x_j}\right)^s m$ mit $s \prec_p t$ ein Monom eines Polynoms aus J sein. Da J ein Monomideal ist, enthält J alle Monome, die in seinen Polynomen auftauchen, also auch das Monom $\left(\frac{x_i}{x_j}\right)^s m$.
Für die andere Richtung nehmen wir an, dass ein J Monomideal ist, dass die Bedingungen von (ii) erfüllt. Die obige Formel zeigt, dass für jeden monomialen Erzeuger m von J das Polynom γm eine Summe von Monomen aus J ist. Da J von

Monomen erzeugt wird, gilt $\gamma J = J$. Für Diagonalmatrizen gilt die Behauptung wegen (i), also gilt sie auch für $\mathcal{B}$.

□

Zum Schluss noch ein Beispiel zu diesem Satz. Der Einfachheit halber beschränken wir uns auf den Fall, dass alle Erzeuger den gleichen Grad haben und $charK = 0$.

Beispiel 11.5.12. Sei $S = K[x_1, x_2]$. Wir betrachten das Ideal $J = (x_1^d, x_1^{d-1}x_2, \ldots, x_1x_2^{d-1})$. Um zu zeigen, dass J borel-fixiert ist, müssen wir die Bedingungen aus Teil (ii) des Satzes überprüfen. Dazu betrachten wir die Erzeuger m_i von J:

- $m_1 = x_1^d$ ist nicht teilbar durch x_2
- $m_{i+1} = x_1^{d-i}x_2^i$ für $i \geq 0$ ist teilbar durch x_2^i aber nicht durch x_2^{i+1}. Nun müssen wir also $\left(\frac{x_1}{x_2}\right)^s m_{i+1}$ für $s \leq i+1$ betrachten.

$$\left(\frac{x_1}{x_2}\right)^s m_{i+1} = \left(\frac{x_1}{x_2}\right)^s x_1^{d-i}x_2^i = x_1^{d-(i-s)}x_2^{i-s}$$

  Dies ist wieder ein Erzeuger von J.

Also ist das Ideal J borel-fixiert.

Lässt man einen dieser Erzeuger weg, ist J nicht mehr zwangsläufig borel-fixiert, wie das folgende Beispiel zeigt.

Beispiel 11.5.13. Sei $J = (x_1^3, x_1x_2^2)$, dann ist $m_2 = x_1x_2^2$ durch x_2^2 teilbar, aber $\left(\frac{x_i}{x_j}\right)^s m_2 = x_1^2x_2$, was nicht in J liegt.

Es lässt sich nachprüfen, dass auch Produkte, Schnitte, Summen und Quotienten von borel-fixierten Idealen wieder borel-fixiert sind.

Literaturverzeichnis

[1] Michele Audin, *Geometry*, Springer, Berlin, 2003.

[2] Markus Brodmann, *Algebraische Geometrie: Eine Einführung*, Birkhäuser Verlag, Basel, 1989.

[3] Claude Chevalley, *The Theory of Local Rings*, Ann. of Math. (2) 44, 1943, 690–708.

[4] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, 1995.

[5] Joe Harris, *Algebraic Geometry*, Springer, 1992.

[6] C. Hopkins, Rings with minimal condition for left ideals, *Annals of Math.* **40**, 1939, 712–730.

[7] Creig Huneke, *Free Resolutions in Commutative Algebra and Algebraic Geometry*, Sundance 90, 1992.

[8] Wolfgang Krull, *Beiträge zur Arithmetik kommutativer Integritatsbereiche*, VIII. Math. 48, 1943, 533–552.

[9] Hanfried Lenz, *Vorlesungen über projektive Geometrie*, Akademische Verlagsgesellschaft, Leipzig, 1965.