Kommutative Algebra

Wolfgang M. Ruppert

Wintersemester 1994/95

Version vom 18. März 1999 [1]

[1] Im Wintersemester 1994/95 am Mathematischen Institut der Universität Erlangen abgehaltene Vorlesung

Inhaltsverzeichnis

KAPITEL 1

Kommutative Ringe

Die Grundobjekte der kommutativen Algebra bilden die kommutativen Ringe.

Definition: Ein *Ring* besteht aus einer Menge R, zwei Operationen $+ : R \times R \to R$ (Addition), $\cdot : R \times R \to R$ (Multiplikation), einer Null $0 \in R$ und einer Eins $1 \in R$, so daß gilt:

- Addition: $(R, +, 0)$ ist eine abelsche Gruppe, d.h. explizit
  - Assoziativität: $a + (b + c) = (a + b) + c$
  - Null: $0 + a = a + 0 = 0$
  - Negatives: Zu jedem $a \in R$ gibt es ein wohlbestimmtes Element $-a \in R$ mit der Eigenschaft $a + (-a) = 0$.
  - Kommutativität: $a + b = b + a$
- Multiplikation: assoziativ mit Eins, explizit:
  - Assoziativität: $a(bc) = (ab)c$
  - Eins: $1 \cdot a = a \cdot 1 = a$
- Addition und Multiplikation
  - Distributivität: $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$

Der Ring heißt kommutativ, falls die Multiplikation kommutativ ist, d.h. $ab = ba$ für alle $a, b \in R$.

Bemerkungen:

1. Es gelten die üblichen Rechenregeln, z.B. $0a = 0$ ($a = 1a = (0 + 1)a = 0a + 1a = 0a + a$, also $0a = 0$), $(-a)b = -(ab)$, $(-a)(-b) = ab$.
2. Für uns hat ein Ring immer eine 1.

Es ist wichtig, eine Sammlung von Beispielen für Ringe zu haben.

Beispiel: Die ganzen Zahlen $\mathbf{Z}$ sind das grundlegende Beispiel eines kommutativen Rings.

Beispiel: Körper sind insbesondere kommutative Ringe. Z.B. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$.

Beispiel: Der triviale Ring $R = \{0\}$ besteht nur aus einem Element mit den offensichtlichen Operationen. Hier ist $0 = 1$. Nur in diesem Fall ist $1 = 0$.

Ist S ein Ring und $R \subseteq S$ eine Teilmenge, die abgeschlossen ist bzgl. Addition und Multiplikation mit $0, 1 \in R$, so ist natürlich auch R ein Ring: ein Unterring oder Teilring von S.

Beispiel: Sei $d \in \mathbf{Z}$ und $R = \{x + y\sqrt{d} \in \mathbf{C} : x, y \in \mathbf{Z}\}$. Man rechnet schnell nach, daß R ein Teilring von $\mathbf{C}$ ist. Ringe dieser Bauart spielen in der Zahlentheorie eine große Rolle.

Sei S ein Ring und $R_i \subseteq S, i \in I$ eine Menge von Teilringen. Dann ist natürlich auch $\cap_{i \in I} R_i$ ein Teilring von S.
Sind jetzt $R \subseteq S$ Ringe und ist $M \subseteq S$ eine Teilmenge von S, so bezeichne $R[M]$ den kleinsten Teilring von S, der R und M enthält. Offensichtlich ist

$$R[M] = \cap\{R' \subseteq S : R' \text{ Ring}, M \subseteq R', R \subseteq R'\}.$$

Beispiele:

1. Sei $d \in \mathbf{Z}$. Dann ist $\mathbf{Z}[\sqrt{d}] = \{x + y\sqrt{d} \in \mathbf{C} : x, y \in \mathbf{Z}\}$. Weshalb?

2. Was ist $\mathbf{Z}[\frac{1}{2}](\subseteq \mathbf{Q})$? Es gilt:
$$\mathbf{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \in \mathbf{Q} : a \in \mathbf{Z}, n \geq 0\}.$$
3. Sei R ein Ring mit $\mathbf{Z} \subseteq R \subseteq \mathbf{Q}$. Dann gibt es eine Menge von Primzahlen $\{p_i : i \in I\}$ mit
$$R = \mathbf{Z}[\frac{1}{p_i} : i \in I].$$
Beweis als Übung.
4. Allgemein gilt
$$R[M] = \{\sum_{i_1,\ldots,i_n} r_{i_1\ldots i_n} m_1^{i_1} \ldots m_n^{i_n} : r_{i_1\ldots i_n} \in R, m_1, \ldots, m_n \in M\}.$$

Polynomring über R: Sei R ein Ring. Der Polynomring $R[x]$ in einer Unbestimmten x über R besteht dann aus den formalen Ausdrücken
$$\sum_{i=0}^{n} a_i x^i,$$
mit $a_i \in R$, $n \geq 0$. Wichtig ist: $\sum a_i x_i = \sum b_i x_i$ genau dann, wenn für alle $i \geq 0$ gilt $a_i = b_i$. Addition und Multiplikation werden wie folgt erklärt:
$$(\sum a_i x^i) + (\sum b_i x^i) = \sum (a_i + b_i) x^i, \quad (\sum a_i x^i) \cdot (\sum b_i x^i) = \sum_{i \geq 0} (\sum_{j=0}^{i} a_j b_{i-j}) x^i.$$
Damit wird $R[x]$ wieder ein kommutativer Ring.
Durch Adjunktion weiterer Unbestimmter erhält man allgemein Polynomringe über R: $R[x_1, \ldots, x_n]$. Dies geht noch allgemeiner: $R[x_i : i \in I]$.

Beispiel: Sind A und B Ringe, so wird $A \oplus B$ ein Ring durch die Vorschriften
$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$
Ist $A_i, i \in I$ eine Familie von Ringen, so ist auch das Produkt $\prod_{i \in I} A_i$ ein Ring. Die Elemente sind $(a_i)_{i \in I}$ und $0 = (0)_{i \in I}, 1 = (1)_{i \in I}$. j

Beispiel: Sei M eine Menge, R ein Ring und $\mathcal{F}(M, R)$ die Menge aller Funktionen von M in R. Dann wird dies ein Ring durch die Vorschrift
$$(f + g)(m) = f(m) + g(m), \quad (f \cdot g)(m) = f(m) g(m).$$
0 und 1 werden durch die konstanten Funktionen 0 und 1 gegeben. Durch Auswahl spezieller Funktionen erhält man manchmal Unterringe.

Beispiele:

1. Die Menge $\mathcal{C}(\mathbf{R})$ aller stetigen Funktionen von $\mathbf{R}$ in $\mathbf{R}$ bilden einen Ring. Die Teilmenge $\mathcal{C}_0(\mathbf{R})$ aller stetigen Funktionen auf $\mathbf{R}$ mit kompaktem Träger bilden allerdings keinen Ring, da die Eins fehlt.
2. Sei $U \subseteq \mathbf{C}$ eine offene Teilmenge von $\mathbf{C}$. Die holomorphen Funktionen auf U bilden dann einen Ring $\mathcal{O}(U)$.

Das wichtigste Beispiel eines nichtkommutativen Ringes bilden die Matrizenringe:

Matrizenringe: Sei R ein kommutativer Ring und $n \in \mathbf{N}$. Die $n \times n$-Matrizen mit Einträgen aus R bilden dann einen Ring $M_n(R)$. Für $n \geq 2$ (und $0 \neq 1$) ist dieser nicht kommutativ.

Wir wollen noch ein weiteres wichtiges Beispiel kennenlernen:

Formale Potenzreihen: Sei R ein kommutativer Ring. Wir betrachten dann die formalen Potenzreihen mit der Unbestimmten x

$$\sum_{i\geq 0} a_i x^i$$

wo $a_i \in R$. Die Menge aller dieser Ausdrücke bezeichnen wir mit $R[[x]]$. Wieder sind zwei Potenzreihen per definitionen genau dann gleich, wenn alle Koeffizienten übereinstimmen. Addition und Multiplikation werden wie folgt definiert

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i, \quad \sum a_i x^i \cdot \sum b_i x^i = \sum_i (\sum_{j=0}^{i} a_j b_{i-j}) x^i.$$

Man rechnet leicht nach, daß damit $R[[x]]$ ein kommutativer Ring wird. Man hat die Inklusionen $R \subseteq R[x] \subseteq R[[x]]$.
In analoger Weise kann man auch den Ring der formalen Potenzreihen $R[[x_1, \ldots, x_n]]$ in n Unbestimmten $x_1, \ldots, x_n$ definieren.

Beispiel: Wir rechnen in $R[[x]]$ mit

$$a = \sum_{i\geq 0} x^i = 1 + x + x^2 + x^3 + \ldots.$$

Es gilt

$$(1 - x) \sum_{i\geq 0} x^i = \sum_{i\geq 0} x^i - \sum_{j\geq 1} x^j = 1.$$

Einheiten: Ein Element $a \in R$ eines Ringes R heißt Einheit, falls es ein $b \in R$ gibt mit $ab = ba = 1$. In diesem Fall ist b durch a eindeutig bestimmt. (Ist $ab = ba = 1$ und $ab' = b'a = 1$, so gilt $b = bab' = b'$.) Man schreibt $b = a^{-1}$. Die Einheiten eines Ringes bilden bezüglich der Multiplikation eine Gruppe, die mit $R^\times$ oder R^* bezeichnet wird.

Wir wollen wieder ein paar Beispiele betrachten.

Beispiele:

1. Für die ganzen Zahlen ist $\mathbf{Z}^\times = \{\pm 1\}$.
2. Für einen Körper k ist $k^\times = k \setminus \{0\}$.
3. Sei jetzt $d \in \mathbf{Z}$ keine Quadratzahl, d.h. $\sqrt{d} \notin \mathbf{Q}$. Wir wollen die Einheiten von $\mathbf{Z}[\sqrt{d}]$ bestimmen.
   Behauptung: $x + y\sqrt{d}$ ist genau dann Einheit, wenn $x^2 - dy^2 = \pm 1$ ist.
   Beweis: Ist $x + y\sqrt{d}$ Einheit, so gibt es $u + v\sqrt{d}$ mit $(x + y\sqrt{d})(u + v\sqrt{d}) = 1$, d.h.

   $$(xu + yvd) + (xv + yu)\sqrt{d} = 1.$$

   Dann ist $xv + yu = 0$ (sonst wäre $\sqrt{d} \in \mathbf{Q}$!) und $xu + yvd = 1$. Da x und y teilerfremd sind, gibt es ein $m \in \mathbf{Z}$ mit $u = mx, v = -my$. Einsetzen liefert $m(x^2 - y^2 d) = 1$, also $x^2 - dy^2 = \pm 1$.
   Gilt umgekehrt $x^2 - dy^2 = \pm 1$, so ist

   $$(x + y\sqrt{d})(x - y\sqrt{d}) = \pm 1,$$

   also $x + y\sqrt{d}$ eine Einheit. ■

   Wir betrachten konkret ein paar Fälle:
   (a) $d = -1$: Die Gleichung $x^2 + y^2 = \pm 1$ hat dann 4 Lösungen, was die 4 Einheiten $\pm 1, \pm i$ liefert, also $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$.
   (b) $d \leq -2$: Die Gleichung $x^2 + |d|y^2 = 1$ hat dann nur die Lösungen $x = \pm 1, y = 0$, also $\mathbf{Z}[\sqrt{d}] = \{\pm 1\}$.
   (c) $d \geq 2$. In diesem Fall muß man Lösungen der *Pellschen Gleichung* $x^2 - dy^2 = \pm 1$ suchen. Dies ist nicht trivial. Man kann zeigen, daß es immer nicht triviale Lösungen gibt. Wir geben nur zwei Beispiele:
   (d) $\mathbf{Z}[\sqrt{2}]^\times = \{\pm(1 \pm \sqrt{2})^n : n \geq 0\}$.
   (e) $\mathbf{Z}[\sqrt{61}]^\times = \{\pm(29718 + 3805\sqrt{61})^n : n \in \mathbf{Z}\}$.

4. Was ist $\mathbf{Z}[\frac{1}{2}]^\times$? Wir wissen, wie die Elemente in $\mathbf{Z}[\frac{1}{2}]$ aussehen und wir setzen einfach an:
$$\frac{a}{2^m} \cdot \frac{b}{2^n} = 1, \text{ also } ab = 2^{m+n} \text{ in } \mathbf{Z}.$$
Daraus sieht man sofort $\mathbf{Z}[\frac{1}{2}]^\times = \{\pm 2^n : n \in \mathbf{Z}\}$.
5. Was ist $R[[x]]^\times$? Sei $a = a_0 + a_1 x + a_2 x^2 + \ldots$ gegeben. a ist genau dann Einheit, wenn es $b = b_0 + b_1 x + b_2 x^2 + \ldots$ gibt mit
$$1 + 0x + 0x^2 + \cdots = 1 = ab = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots,$$
d.h. wenn wir $b_0, b_1, b_2, \cdots \in R$ finden mit
$$a_0 b_0 = 1, \quad a_0 b_1 + a_1 b_0 = 0, \quad \ldots, a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = 0, (n \geq 1).$$
Behauptung: $a \in R[[x]]^\times \iff a_0 \in R^\times$.
Beweis: Die eine Richtung ist klar. Sei jetzt umgekehrt a_0 Einheit in R. Dann können wir obiges Gleichungssystem rekursiv nach $b_0, b_1, b_2, \ldots$ auflösen, d.h. wir finden b mit $ab = 1$. ■

Sei R ein Ring. Ein Element $a \in R$ heißt Nullteiler, falls $a \neq 0$ und ein $b \in R$, $b \neq 0$ existiert mit $ab = 0$.

Beispiel: In $R = \mathbf{Z} \times \mathbf{Z}$ gilt $(1,0) \cdot (0,1) = 0$.

Ein Integritätsring ist ein kommutativer Ring R mit $0 \neq 1$ ohne Nullteiler, d.h. $a \neq 0$, $b \neq 0$ impliziert $ab \neq 0$.
Ein Unterring eines Integritätsrings ist wieder ein Integritätsring. Unterringe von Körpern sind Integritätsringe. Wir werden später sehen, daß auch das Umgekehrte gilt, d.h. jeder Integritätsring ist Unterring eines Körpers.

SATZ. *Ist R ein Integritätsring, so auch $R[x]$ und $R[[x]]$.*

Beweis: Es genügt die Aussage für $R[[x]]$ zu zeigen. Sind $a, b \in R[[x]]$ mit $a, b \neq 0$, so kann man schreiben
$$a = a_m x^m + a_{m+1} x^{m+1} + \ldots, b = b_n x^n + b_{n+1} x^{n+1} + \ldots$$
mit $a_m, b_n \neq 0$. Dann ist aber $a_m b_n \neq 0$, also auch
$$ab = a_m b_n x^{m+n} + (a_m b_{n+1} + a_{m+1} b_n) x^{m+n+1} + \cdots \neq 0. \blacksquare$$

Sei R ein kommutativer Ring. Für ein Polynom $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ mit $a_n \neq 0$ heißt n der Grad von f: $grad(f)$. Man setzt manchmal $grad(0) = -\infty$. Damit gilt:

LEMMA. *Für die Gradfunktion gilt:*
1. $grad(f+g) \leq \max(grad(f), grad(g))$,
2. $grad(fg) \leq grad(f) + grad(g)$.
3. *Ist R Integritätsring, so gilt sogar:* $grad(fg) = grad(f) + grad(g)$.

Beweis: Wir betrachten nur die zweite Formel. Sei
$$f = a_0 + a_1 x + \cdots + a_m x^m, \quad g = b_0 + b_1 x + \cdots + b_n x^n$$
mit $a_m, b_n \neq 0$. Dann ist
$$fg = a_0 b_0 + \cdots + a_m b_n x^{m+n},$$
also $grad(fg) \leq m + n$. Ist R Integritätsring, so ist $a_m b_n \neq 0$, also $grad(fg) = m + n$. ■

FOLGERUNG. *Ist R Integritätsring, so gilt*
$$R[x_1, \ldots, x_n]^\times = R^\times.$$

Beweis: Wir können dies induktiv nach der Anzahl der Unbestimmten beweisen. Also können wir uns auf den Beweis von $R^\times = R[x]^\times$ beschränken. Sei $f \in R[x]$, $f = a_0 + \cdots + a_m x^m$ mit $a_m \neq 0$. Dann gilt: f ist Einheit genau dann, wenn es ein $g = b_0 + \cdots + b_n x^n$ gibt mit $b_n \neq 0$ und $fg = 1$. Da wir in einem Integritätsring sind, ist dies gleichwertig mit $m = n = 0$ und $a_0 b_0 = 1$, woraus die Behauptung folgt. ■

Daß diese Aussage i.a. nicht gelten muß, ist Inhalt einer Übungsaufgabe.

KAPITEL 2

Homomorphismen und Ideale

Ein Homomorphismus zwischen zwei Ringen R und S ist eine Abbildung $f : R \to S$ mit $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ und $f(1) = 1$. (Dann ist auch $f(0) = 0$.) Ein Isomorphismus ist ein Homomorphismus, zu dem es einen Homomorphismus $g : S \to R$ gibt mit $fg = id_S$ und $gf = id_R$.

Beispiel: Eine Unterringbeziehung $R \subseteq S$ läßt sich immer als Homomorphismus $R \to S$ deuten.

Beispiel: Ist R irgendein Ring, so gibt es einen kanonischen Ringhomomorphismus $\alpha : \mathbf{Z} \to R$, der durch $\alpha(1) = 1$ bestimmt ist.

Beispiel: (Auswertungsabbildung) Ist M eine Menge, R ein Ring und $m \in M$, so ist

$$\mathcal{F}(M, R) \to R, \quad f \mapsto f(m)$$

ein Ringhomomorphismus.

Beispiel: Die fundamentale Eigenschaft von Polynomen ist, daß man einsetzen darf. Seien R und S kommutative Ringe und $\phi : R \to S$ ein Ringhomomorphismus. Sind $b_1, \ldots, b_n \in S$ so gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\phi} : R[x_1, \ldots, x_n] \to S,$$

der ϕ fortsetzt, d.h. $\phi(r) = \tilde{\phi}(r)$ für $r \in R$ und $\tilde{\phi}(x_i) = b_i$ für $i = 1, \ldots, n$. Explizit:

$$\tilde{\phi}(\sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}) = \sum \phi(a_{i_1 \ldots i_n}) b_1^{i_1} \ldots b_n^{i_n}.$$

Beispiel: Sind M und N zwei Mengen, R ein Ring und $\phi : M \to N$ eine Abbildung, so liefert dies einen Ringhomomorphismus

$$\phi^* : \mathcal{F}(N, R) \to \mathcal{F}(M, R) : f \mapsto f\phi.$$

Bemerkungen: Sei $f : R \to S$ ein Ringhomomorphismus.

1. Dann ist das Bild von f ein Unterring von S, denn: $f(1) = 1$, $f(0) = 0$, $f(a) + f(b) = f(a + b), f(ab) = f(a)f(b)$.
2. Es gilt $f(R^\times) \subseteq S^\times$, denn aus $ab = 1$ folgt $f(a)f(b) = 1$.
3. Die Menge $\{a \in R : f(a) = 0\}$ heißt der Kern von f: $kern(f)$. Der Kern ist i.a. kein Unterring von R, denn: $1 \in kern(f)$ impliziert $1 = f(1) = 0$, d.h. S ist der Nullring. Es gelten aber die Eigenschaften: $a, b \in Kern(f)$ impliziert $a + b \in kern(f)$, $a \in kern(f)$, $r \in R$ impliziert $ra, ar \in kern(f)$ und $0 \in kern(f)$. So etwas nennt man ein Ideal. f ist genau dann injektiv, wenn $kern(f) = 0$ ist. In diesem Fall nennt man f auch eine Einbettung: $f : R \hookrightarrow S$.
4. Man sieht leicht: Ein Ringhomomorphismus ist genau dann ein Isomorphismus, wenn er bijektiv ist.

Definition: Eine Teilmenge I eines Rings R heißt Ideal, wenn gilt: $0 \in I$, $a, b \in I$ impliziert $a + b \in I$ und $a \in I, r \in R$ impliziert $ra, ar \in I$. Ein Ideal ist also ein additive Untergruppe von R, die bezüglich Multiplikation mit Ringelementen abgeschlossen ist: $IR \subseteq I, RI \subseteq I$.

Folgendes Beispiel zeigt, daß Ideale in natürlicher Weise auftreten:

Beispiel: Es seien folgende Polynome aus $\mathbf{R}[x, y]$ gegeben:

$$f = -2 + y + x^2 + xy + y^2, \quad g = 3 - 3x + y - 3x^2 + 3xy + y^2.$$

Bestimme alle Lösungen von $f = g = 0$, d.h. die Menge

$$X = \{(a,b) \in \mathbf{R}^2 : f(a,b) = g(a,b) = 0\}.$$

Wir wird man dies tun? Man wird die Gleichungen umformen, man wird f und g geeignet zu kombinieren versuchen, so daß man etwas über die Lösungen sagen kann. Sei

$$\mathfrak{a} = \{Af + Bg : A, B \text{ Polynome}\}.$$

Dann ist dies ein Ideal in $\mathbf{R}[x,y]$ und jedes Element von $\mathfrak{a}$ verschwindet auf X. Wir versuchen, einfache Elemente in $\mathfrak{a}$ zu konstruieren. Wir versuchen, y zu eliminieren, ganz naiv:

$$\begin{aligned}
f &= (-2+x^2) + (1+x)y + y^2 \\
g &= (3-3x-3x^2) + (1+3x)y + y^2 \\
g_1 = g - f &= (5-3x-4x^2) + 2xy \\
f_1 = 2xf - yg_1 &= (-4x+2x^3) + (5x+6x^2-5)y \\
f_2 = 2xf_1 - (5x+6x^2-5)g_1 &= 28x^4 + 38x^3 - 43x^2 - 40x + 25 = \\
&= (4x^2+2x-5)(7x^2+6x-5)
\end{aligned}$$

Nun ist offensichtlich $\{f_2 = g_1 = 0\} \subseteq \{f = g = 0\} = X$. Die Lösungsmenge der Gleichungen $f_2 = g_1 = 0$ lassen sich leicht bestimmen, da es sich um quadratische Gleichungen handelt:

$$\begin{aligned}
\{f_2 = g_1 = 0\} &= \{(\frac{-3+2\sqrt{11}}{7}, \frac{-6-3\sqrt{11}}{7}), (\frac{-3-2\sqrt{11}}{7}, \frac{-6+3\sqrt{11}}{7}), \\
&\quad (\frac{-1+\sqrt{21}}{4}, \frac{1}{2}), (\frac{-1-\sqrt{21}}{4}, \frac{1}{2})\}.
\end{aligned}$$

Durch Einsetzen sieht man schnell, daß diese Menge gleich X ist. Reell ergeben sich ungefähr die Punkte

$$\{(0.52, -2.28), (-1.38, 0.56), (0.90, 0.50), (-1.40, 0.50)\}.$$

Nun folgt eine Serie von abstrakten Beispielen.

Beispiel: In jedem Ring R sind $0 = \{0\}$ und R (die trivialen) Ideale.

Beispiel: Sei K ein Körper und I ein Ideal in K mit $I \neq 0$. Wähle $a \in I$ mit $a \neq 0$. Ist $x \in K$, so gilt also $x = (xa^{-1})a \in I$, also $R = I$. D.h. ein Körper besitzt nur die trivialen Ideale 0 und K.
Ist $f : K \to R$ ein Ringhomomorphismus mit $R \neq 0$, so besteht wegen $f(1) = 1$ der Kern von f nur aus 0, d.h. f ist injektiv.

Wir wollen jetzt annehmen, daß Ring immer kommutativer Ring bedeutet, sofern nichts anderes gesagt wird.
Ist $M = \{a_i : i \in I\}$ Teilmenge eines Ringes R, so sei

$$(a_i : i \in M) = \{\sum_{i \in M} r_i a_i : r_i \in M, \text{ bis auf endlich viele } = 0\}.$$

$(a_i : i \in M)$ ist ein Ideal und heißt das von $\{a_i : i \in M\}$ erzeugte Ideal. Ist M endlich, so schreibt man $(a_1, \ldots, a_n)$.

SATZ. *Ein kommutativer Ring $R \neq 0$ ist genau dann ein Körper, wenn er nur die trivialen Ideale 0 und R besitzt.*

Beweis: Sei $R \neq 0$ ein kommutativer Ring, der nur 0 und R als Ideale besitzt. Sei $a \in R$, $a \neq 0$. Wir müssen zeigen, daß a invertierbar ist. Wir betrachten das von a erzeugte Ideal (a). Nach unserer Voraussetzung gilt $(a) = R$, insbesondere $1 \in (a)$, d.h. es gibt ein $b \in R$ mit $1 = ba$, d.h. a ist Einheit, was wir zeigen wollten. ■

Beispiel: Wir bestimmen die Ideale in $\mathbf{Z}$. Sei I ein Ideal, $I \neq 0$. Ist $n \in I$, so auch $-n \in I$. Sei $d = \min\{n \in I : n \geq 1\}$. Sei jetzt $n \in I$. Nach dem euklidischen Algorithmus gibt es ein $q \in \mathbf{Z}$ und ein $r \in \mathbf{Z}$ mit $0 \leq r \leq d-1$ und $n = qd + r$. Wegen $n, d \in I$ ist auch $r \in I$, also nach minimaler Wahl von d offensichtlich $r = 0$, d.h. $n = qd$. Damit ist $I = (d)$.

Ideale der Form (a) nennt man Hauptideale. Ein Integritätsring, in dem jedes Ideal Hauptideal ist, heißt Hauptidealring. Der Ring der ganzen Zahlen $\mathbf{Z}$ ist also ein Hauptidealring. Noch ein paar Bemerkungen zu Hauptidealen in einem Integritätsring R:

- Es gilt $(a) \subseteq (b)$ genau dann, wenn $a \in (b)$, was gleichwertig ist mit $a = cb$ mit einem $c \in R$, d.h. $b|a$.
- Es gilt $(a) = (b)$ genau dann, wenn $b = ua$ mit einem $u \in R^\times$, d.h. $a \sim b$, a und b sind assoziiert. *Beweis:* O.E. $a \neq 0$. Aus $(a) = (b)$ folgt $a = cb$ und $b = da$ mit $c, d \in R$, also $a = cda$, was $a(cd-1) = 0$, also $cd = 1$ liefert, woraus der eine Teil der Behauptung folgt. Der andere Teil folgt genauso einfach. ■

SATZ. *Ist k ein Körper, so ist $k[x]$ ein Hauptidealring.*

Zum Beweis des Satzes erinnern wir zuvor etwas allgemeiner an die Polynomdivison:

LEMMA. *Sei R ein kommutativer Ring, $f, g \in R[x]$, so daß der höchste Koeffizient von g eine Einheit ist. Dann gibt es (eindeutig bestimmte) Polynome $q, r \in R[x]$ mit*

$$f = qg + r \text{ und } grad(r) < grad(g).$$

Beweis des Lemmas: Sei

$$f = a_m x^m + a_{m-1}x^{m-1} + \dots, \quad g = b_n x^n + b_{n-1}x^{n-1} + \dots,$$

wo b_n Einheit ist. *Existenz:* Wir machen Induktion nach $grad(f)$. Ist $grad(f) < grad(g)$, so setze $q = 0$ und $r = f$. Wir können jetzt annehmen, daß $m = grad(f) \geq n = grad(g)$ ist. Betrachte

$$\tilde{f} = f - a_m \cdot b_n^{-1} \cdot x^{m-n} \cdot g.$$

Offensichtlich gilt $grad(\tilde{f}) < grad(f)$, nach Induktionsvoraussetzung gibt es also Polynome $\tilde{q}, \tilde{r}$ mit $grad(\tilde{r}) < grad(g)$ und $\tilde{f} = \tilde{q}g + \tilde{r}$. Damit erhält man:

$$f = \tilde{f} + a_m b_n^{-1} x^{m-n} g = (a_m b_n^{-1} x^{m-n} + \tilde{q})g + \tilde{r},$$

woraus alles folgt.
Eindeutigkeit: als Übung. ■

Beweis des Satzes: Sei $\mathfrak{a}$ ein Ideal in $k[x]$ und o.E. $\mathfrak{a} \neq 0$. Wähle ein Polynom $a \neq 0$ minimalen Grades in $\mathfrak{a}$. Ist dann $f \in \mathfrak{a}$, so gibt es mit Polynomdivision Polynome q, r mit $f = qa + r$ und $grad(r) < grad(a)$. Da auch $r \in \mathfrak{a}$, ist $r = 0$, also $f \in (a)$, d.h. $\mathfrak{a} = (a)$. ■

Beispiel: Der Ring $\mathbf{Z}[\sqrt{-2}]$ ist Hauptidealring, nicht jedoch der Ring $\mathbf{Z}[\sqrt{-5}]$ (Übung). Die Hauptidealeigenschaft ist also nicht immer so offensichtlich.

Beispiel: Ist k ein Körper, so ist (x, y) kein Hauptideal im Polynomring $k[x, y]$, d.h. $k[x, y]$ ist kein Hauptidealring.
Beweis: Angenommen, es gäbe ein Polynom $f(x, y)$ mit $(x, y) = (f(x, y))$. Dann gäbe es Polynome g und h mit $x = gf$ und $y = hf$. Für können nun die Gradfunktionen $grad_x$ und $grad_y$ benutzen:

$$0 = grad_y(x) = grad_y(g) + grad_y(f), \quad 0 = grad_x(y) = grad_x(h) + grad_x(f),$$

d.h. f muß konstant sein. Dann wäre aber $(f) = k[x, y]$, während (x, y) nur Polynome enthält, die $x = 0, y = 0$ eingesetzt, verschwinden. Also ist (x, y) kein Hauptideal. ■

Beispiel: Ist k ein Körper, so hat jedes Ideal in $R = k[[x]]$ die Gestalt (x^n) mit $n \geq 0$ oder 0, insbesondere ist R Hauptidealring.
Beweis: Sei $f \in k[[x]], f \neq 0$. Dann läßt sich f schreiben

$$f = a_n x^n + a_{n+1}x^{n+1} + \dots = x^n(a_n + a_{n+1}x + \dots)$$

mit $a_n \neq 0$. Nun ist aber $a_n + a_{n+1}x + \dots$ eine Einheit. Sei jetzt $I = (f_i : i \in L)$ ein Ideal, o.E. $f_i \neq 0$. Jedes f_i hat die Gestalt $f_i = u_i x^{n_i}$ mit einer Einheit u_i und $n_i \geq 0$. Dann gilt aber offensichtlich

$$I = (f_i : i \in L) = (x^{n_i} : i \in L) = (x^{\min\{n_i : i \in L\}}),$$

woraus unsere Behauptung sofort folgt.

Beispiel: Sei X eine Menge, R ein Integritätsring und S ein Teilring von $\mathcal{F}(X,R)$. Ist $Y \subseteq X$ eine Teilmenge, so ist

$$I(Y) = \{f \in S : f(Y) = 0\}$$

ein Ideal in S. Umgekehrt kann man die Nullstellenmengen von Funktionen betrachten: Ist $F \subseteq S$ eine Menge von Funktionen, so sei

$$N(F) = \{x \in X : f(x) = 0 \text{ für alle } f \in F\} = \cap_{f\in F} N(f).$$

Sei jetzt R ein kommutativer Ring. Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale, so auch $\mathfrak{a}\cap\mathfrak{b}$ und $\mathfrak{a}+\mathfrak{b} = \{a+b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$. Das Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ wird definiert durch

$$\mathfrak{ab} = (ab : a \in \mathfrak{a}, b \in \mathfrak{b}) = \{a_1b_1 + \cdots + a_nb_n : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \geq 0\}.$$

(I.a. ist $\mathfrak{ab} \neq \{ab : a \in \mathfrak{a}, b \in \mathfrak{b}\}$.) Man rechnet schnell folgende Eigenschaften nach: $\mathfrak{ab} \subseteq \mathfrak{a}\cap\mathfrak{b}$ und $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{ab}+\mathfrak{ac}$.
Obige Bildungen verallgemeinern sich sofort zu endlichen Summen und Produkten. Ist $\mathfrak{a}_i, i \in I$ eine Familie von Idealen, so ist auch $\cap_{i\in I}\mathfrak{a}_i$ ein Ideal.

Bemerkungen: Sei $f : R \to S$ ein Ringhomomorphismus.

1. Ist $\mathfrak{b}$ ein Ideal in S, so ist $f^{-1}(\mathfrak{b})$ ein Ideal in R.
2. Ist $\mathfrak{a}$ Ideal in R, so muß $f(\mathfrak{a})$ kein Ideal in S sein. Z.B. $f : \mathbf{Z} \to \mathbf{Q}$ bildet das Ideal $(2) = \{0, \pm2, \pm4, \dots\}$ in kein Ideal von $\mathbf{Q}$ ab.

LEMMA. *Sei $f : R \to S$ ein surjektiver Ringhomomorphismus. Dann gilt:*

1. *Ist $\mathfrak{a}$ ein Ideal in R, so ist $f(\mathfrak{a})$ ein Ideal in S.*
2. *Für ein Ideal $\mathfrak{b}$ in S gilt: $f(f^{-1}(\mathfrak{b})) = \mathfrak{b}$.*
3. *Für ein Ideal $\mathfrak{a}$ in R gilt: $f^{-1}(f(\mathfrak{a})) = \mathfrak{a} + kern(f)$. Gilt insbesondere $kern(f) \subseteq \mathfrak{a}$, so ist $f^{-1}(f(\mathfrak{a})) = \mathfrak{a}$.*
4. *Die Abbildung $\mathfrak{a} \mapsto f(\mathfrak{a})$ liefert eine Bijektion zwischen den Idealen von R, die $kern(f)$ enthalten, und den Idealen von S.*

Beweis:

1. Dies folgt sofort aus der Tatsache, daß jedes $s \in S$ die Form $f(r)$ mit $r \in R$ hat.
2. Natürlich gilt $f(f^{-1}(\mathfrak{b})) \subseteq \mathfrak{b}$. Da aber f surjektiv ist, gilt sogar $f(f^{-1}(\mathfrak{b})) = \mathfrak{b}$.
3. Die Richtung $\supseteq$ ist klar. Sei also $x \in f^{-1}(f(\mathfrak{a}))$. Dann ist $f(x) \in f(\mathfrak{a})$, d.h. es gibt $a \in \mathfrak{a}$ mit $f(x) = f(a)$. Also ist $x - a \in kern(f)$, also $x \in \mathfrak{a} + kern(f)$, was wir zeigen wollten.
4. Die Surjektivität und Injektivität folgt sofort aus 2. und 3. ■

Faktorringe - Restklassenringe: Sei R ein kommutativer Ring und $\mathfrak{a}$ ein Ideal in R. Wir definieren eine Relation auf R durch

$$x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad x - y \in \mathfrak{a}.$$

Dies ist eine Äquivalenzrelation auf R. Die Äquivalenzklassen haben die Form $x + \mathfrak{a} = \{x + a : a \in \mathfrak{a}\}$. Wir schreiben auch $\overline{x}$ für die Klassen von x. Die Menge der Äquivalenzklassen wird mit $R/\mathfrak{a}$ bezeichnet. Wir wollen $R/\mathfrak{a}$ zu einem Ring machen. Dazu genügt es zu zeigen, daß Addition und Multiplikation mit der Äquivalenzrelation verträglich sind.

- Seien $x_1 \equiv y_1 \bmod \mathfrak{a}$, d.h. $x_1 = y_1 + a_1$ mit $a_1 \in \mathfrak{a}$ und $x_2 \equiv y_2 \bmod \mathfrak{a}$, d.h. $x_2 = y_2 + a_2$ mit $a_2 \in \mathfrak{a}$.
- Nun ist

$$(x_1 + x_2) - (y_1 + y_2) = a_1 + a_2 \in \mathfrak{a}, \text{ d.h. } x_1 + x_2 \equiv y_1 + y_2 \bmod \mathfrak{a}.$$

- Weiter

$$x_1x_2 - y_1y_2 = a_1y_2 + a_2y_1 \in \mathfrak{a}, \text{ d.h. } x_1x_2 \equiv y_1y_2 \bmod \mathfrak{a}.$$

Also ist die Addition und Multiplikation durch

$$\overline{x} + \overline{y} = \overline{x+y} \text{ und } \overline{x} \cdot \overline{y} = \overline{xy}$$

wohldefiniert. Man sieht auch sofort, d.h. $\overline{0}$ das Nullelement und $\overline{1}$ das Einselement ist. Also ist $R/\mathfrak{a}$ ein kommutativer Ring.

Wir haben einen natürlichen Ringhomomorphismus

$$f : R \to R/\mathfrak{a}, x \mapsto \overline{x},$$

der surjektiv ist und den Kern $\mathfrak{a}$ hat. (Jedes Ideal tritt also als Kern eines Ringhomomorphismus auf.)

Für können jetzt viele neue Ringe konstruieren.

Beispiel: Die Ideale in $\mathbf{Z}$ haben die Form (n). Der Restklassenring läßt sich für $n \geq 1$ schreiben

$$\mathbf{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

hat also n Elemente. Für $n = 0$ ist $\mathbf{Z}/(0) = \mathbf{Z}$.

Bemerkung: Für das praktische Rechnen ist es gut, wenn man ein geeignetes Repräsentantensystem für die Restklassen hat, wie bei $\mathbf{Z}/(n)$.

Beispiel: Sei R ein Ring und $f(x)$ ein normiertes Polynom vom Grad n. Wie rechnet man dann in dem Ring $S = R[x]/(f(x))$?

- Ist $a(x) \in R[x]$, so gibt es eindeutig bestimmte $b(x), c(x)$ mit
$$a(x) = b(x)f(x) + c(x) \text{ und } grad(c) < n,$$
d.h. $a(x) \equiv c(x) \bmod (f(x))$, in jeder Äquivalenzklasse liegt also ein Polynom vom Grad $< n$.
- Sind $a(x), b(x)$ Polynome vom Grad $< n$ mit $a(x) \equiv b(x) \bmod (f(x))$, so gilt $a(x) - b(x) \in (f(x))$, also $a(x) = b(x)$. D.h.
$$\{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} : a_0, \ldots, a_{n-1} \in R\}$$
ist ein Repräsentantensystem für $R[x]/(f(x))$.
- Wie rechnet man mit dem Repräsentantensystem? Die Addition ist klar. Um $a(x)$ und $b(x)$ zu multiplizieren, teilt man $a(x)b(x)$ durch $f(x)$: $a(x)b(x) = q(x)f(x) + c(x)$ mit $grad(c) < n$. Dann ist $c \equiv ab \bmod f$.

Beispiel: Sei k ein Körper. Die Polynome aus $k[x_1, \ldots, x_n]$ kann man dann als Funktionen auf dem Vektorraum k^n auffassen. Ist X eine Teilmenge von k^n, so ist

$$\mathfrak{a} = \{f \in k[x_1, \ldots, x_n] : f(P) = 0 \text{ für alle } P \in X\}$$

ein Ideal. Wann liefern zwei Polynome $f, g \in k[x_1, \ldots, x_n]$ die gleiche Funktion auf X? Genau dann, wenn $f(P) = g(P)$ für alle $P \in X$, d.h. $f \equiv g \bmod \mathfrak{a}$. Also können wir die Elemente aus $k[x_1, \ldots, x_n]/\mathfrak{a}$ als Funktionen auf X auffassen.

Idealbeziehung: Sei $\mathfrak{a}$ Ideal in R. Nach unserem Lemma über surjektive Ringhomomorphismen, ist klar, daß die Ideale von $R/\mathfrak{a}$ in Bijektion zu den Idealen von R stehen, die $\mathfrak{a}$ enthalten. Insbesondere kommt jedes Ideal von $R/\mathfrak{a}$ von R her.

Satz (Homomorphiesatz). *Sei $f : R \to S$ ein Ringhomomorphismus und $\mathfrak{a}$ ein Ideal in R mit $\mathfrak{a} \subseteq kern(f)$. Dann faktorisiert f in der Form*

$$f : R \to R/\mathfrak{a} \to S.$$

Der Homomorphismus $g : R/\mathfrak{a} \to S$ hat den Kern $kern(f)/\mathfrak{a}$.

Beweis: Wir müssen definieren: $g(\overline{a}) = f(a)$. Dies ist wohldefiniert: $\overline{a_1} = \overline{a_2}$ liefert $a_1 - a_2 \in \mathfrak{a} \subseteq kern(f)$, also $f(a_1) = f(a_2)$. Daß g ein Ringhomomorphismus ist, ist dann klar. ■

FOLGERUNG. *Ist $f : R \to S$ ein Ringhomomorphismus, so gilt*

$$R/kern(f) \simeq f(R),$$

ist insbesondere f surjektiv, so ist $S \simeq R/kern(f)$.

Beispiel: Sei $d \in \mathbf{Z}$ kein Quadrat. Dann ist

$$\mathbf{Z}[x]/(x^2 - d) \simeq \mathbf{Z}[\sqrt{d}].$$

Beweis: Betrachte den Ringhomomorphismus $\phi : \mathbf{Z}[x] \to \mathbf{Z}[\sqrt{d}]$ mit $\phi(x) = \sqrt{d}$, der offensichtlich surjektiv ist. Wir bestimmen den Kern von ϕ. Natürlich ist $x^2 - d \in kern(\phi)$. Sei jetzt $f \in \mathbf{Z}[x], f \in kern(\phi)$. Wir machen Polynomdivision durch $x^2 - d$ und erhalten

$$f(x) = (x^2 - d)g(x) + (ax + b)$$

mit $a, b \in \mathbf{Z}$ und $g(x) \in \mathbf{Z}[x]$. Nun gilt:

$$0 = \phi(f(x)) = a\sqrt{d} + b,$$

also $a = b = 0$, d.h. $f \in (x^2 - d)$, also $kern(\phi) = (x^2 - d)$. Nach dem Homomorphiesatz gilt dann

$$\mathbf{Z}[x]/(x^2 - d) \simeq \mathbf{Z}[\sqrt{d}].\blacksquare$$

Beispiel: Sei R ein Ring und $a \in R$. Dann sieht man wie eben, daß der Einsetzungshomomorphismus $\varphi : R[x] \to R, x \mapsto a$ einen Isomorphismus

$$R[x]/(x - a) \simeq R$$

induziert. Daraus folgt induktiv sofort:

$$R[x_1, \ldots, x_n]/(x_{m+1}, \ldots, x_n) \simeq R[x_1, \ldots, x_m].$$

Wir geben jetzt zwei sehr wichtige Definitionen, die später ausführlich erörtert werden:

Definition: Sei R ein kommutativer Ring. Ein Ideal $\mathfrak{p}$ heißt prim bzw. Primideal, wenn $R/\mathfrak{p}$ ein Integritätsring ist. Ein Ideal $\mathfrak{m}$ heißt maximal, wenn $R/\mathfrak{m}$ ein Körper ist.

Bemerkungen:

1. Jedes maximale Ideal ist prim.
2. Ein Ideal $\mathfrak{m}$ ist genau dann maximal, wenn $\mathfrak{m} \neq R$ und für jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ folgt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.
3. Jedes Ideal $\mathfrak{a} \neq R$ ist in einem maximalen Ideal enthalten.
4. Ein Ideal $\mathfrak{p}$ ist genau dann prim, wenn $\mathfrak{p} \neq R$ und aus $ab \in \mathfrak{p}$ folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
5. Genau dann ist ein Ring Integritätsring, wenn 0 Primideal ist.

Beispiel: Sei k Körper und $R = k[x_1, \ldots, x_n]$. Wegen $R/(x_{m+1}, \ldots, x_n) \simeq k[x_1, \ldots, x_m]$ sind alle Ideale

$$(x_1) \subseteq (x_1, x_2) \subseteq \ldots (x_1, \ldots, x_n) \subseteq R$$

Primideale. Davon ist $(x_1, \ldots, x_n)$ allein maximal.

Bemerkung: Seien $a, b \in \mathbf{Z}$. Das von a und b erzeugte Ideal ist ein Hauptideal, d.h. $(a, b) = (d)$ mit einer ganzen Zahl d. Es gilt dann $(a) \subseteq (d)$, also $d|a$ und analog $d|b$, also ist d ein gemeinsamer Teiler von a und b. Nun gibt es $x, y \in \mathbf{Z}$ mit $d = xa + yb$. Ist e ein gemeinsamer Teiler von a und b, so teilt also e auch d, d.h. d ist der größte gemeinsame Teiler von a und b. Also

$$(a) + (b) = (a, b) = (ggT(a, b)).$$

Analog zeigt man $(a) \cap (b) = (kgV(a, b))$. a und b sind genau dann teilerfremd, wenn $(a) + (b) = \mathbf{Z}$ ist.

Man definiert nun allgemein: Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ eines Ringes R heißen teilerfremd, wenn $\mathfrak{a} + \mathfrak{b} = R$ gilt. Damit können wir den chinesischen Restsatz formulieren:

SATZ (Chinesischer Restsatz). *Sei R ein kommutativer Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale. Sind $x_1, \ldots, x_n \in R$, so gibt es ein $x \in R$ mit $x \equiv x_i \bmod \mathfrak{a}_i$ für alle i.*

Beweis:

1. *Behauptung:* Es gibt $a_1 \in R$ mit der Eigenschaft $a_1 \equiv 1 \bmod \mathfrak{a}_1$ und $a_1 \equiv 0 \bmod \mathfrak{a}_i$ für $i \neq 1$.
   Beweis: Für $i \neq 1$ sind $\mathfrak{a}_1$ und $\mathfrak{a}_i$ teilerfremd, d.h. es gibt $b_i \in \mathfrak{a}_1$, $c_i \in \mathfrak{a}_i$ mit $b_i + c_i = 1$. Setze nun $a_1 = c_2 c_3 \dots c_n$. Dann ist $a_1 \equiv 0 \bmod \mathfrak{a}_i$ für $i \neq 1$ und
   $$a_1 = (1 - b_2) \dots (1 - b_n) \equiv 1 \bmod \mathfrak{a}_1.$$
2. Genauso gibt es allgemein $a_i \in R$ mit $a_i \equiv 1 \bmod \mathfrak{a}_i$ und $a_1 \equiv 0 \bmod \mathfrak{a}_j$ für $i \neq j$.
3. Setze jetzt
   $$x = x_1 a_1 + \dots + x_n a_n.$$
   Dann ist $x \equiv x_i \bmod \mathfrak{a}_i$ für alle i, was zu zeigen war. ■

Im ersten Beweisschritt haben wir gesehen: $a_1 \in \mathfrak{a}_2 \dots \mathfrak{a}_n$, also

$$1 = (1 - a_1) + a_1 \in \mathfrak{a}_1 + \mathfrak{a}_2 \dots \mathfrak{a}_n,$$

d.h. die Ideale $\mathfrak{a}_1$ und $\mathfrak{a}_2 \dots \mathfrak{a}_n$ sind teilerfremd. Damit haben wir den ersten Teil des folgenden Lemmas bewiesen:

LEMMA. *Sind $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ paarweise teilerfremde Ideale, so gilt:*

1. *$\mathfrak{a}_1$ und $\mathfrak{a}_2 \dots \mathfrak{a}_n$ teilerfremd.*
2. $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n = \mathfrak{a}_1 \dots \mathfrak{a}_n$.

Beweis: Zunächst ist klar: $\mathfrak{a}_1 \dots \mathfrak{a}_n \subseteq \mathfrak{a}_i$, also auch $\mathfrak{a}_1 \dots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$. Wir müssen also nur noch die Umkehrung zeigen. Wir machen dies durch Induktion nach n:
$n = 2$: $\mathfrak{a}_1 + \mathfrak{a}_2 = R$ liefert $a_1 \in \mathfrak{a}_1$ und $a_2 \in \mathfrak{a}_2$ mit $a_1 + a_2 = 1$. Ist jetzt $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, so ist $x = xa_1 + xa_2$ und $xa_1, xa_2 \in \mathfrak{a}_1\mathfrak{a}_2$, also $x \in \mathfrak{a}_1\mathfrak{a}_2$.
Sei jetzt $n \geq 3$. Nach dem ersten Teil des Lemmas gilt

$$\mathfrak{a}_1 \dots \mathfrak{a}_n = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \dots \mathfrak{a}_n = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \dots \mathfrak{a}_n) = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_n,$$

was wir zeigen wollten. ■

FOLGERUNG. *Sei R ein kommutativer Ring und $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ paarweise teilerfremde Ideale. Dann ist der natürliche Ringhomomorphismus*

$$f : R \to \prod_{i=1}^{n} R/\mathfrak{a}_i = (R/\mathfrak{a}_1) \times \dots \times (R/\mathfrak{a}_n)$$

surjektiv mit $kern(f) = \cap_{i=1}^{n} \mathfrak{a}_i$, d.h. f induziert

$$R/\prod_{i=1}^{n} \mathfrak{a}_i = R/\cap_{i=1}^{n} \mathfrak{a}_i \simeq \prod_{i=1}^{n} R/\mathfrak{a}_i.$$

Beweis: Die Surjektivität von f ist der chinesische Restsatz. Weiter gilt $x \in kern(f) \iff x \in \mathfrak{a}_1, \dots, x \in \mathfrak{a}_n \iff x \in \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$, woraus alles folgt. ■

Beispiel: Die natürliche Zahl n habe die Primfaktorzerlegung

$$n = p_1^{m_1} \dots p_r^{m_r}.$$

Dann gilt

$$\mathbf{Z}/(n) \simeq \mathbf{Z}/(p_1^{m_1}) \times \dots \times \mathbf{Z}/(p_r^{m_r}).$$

Daß die Teilerfremdheit beim chinesischen Restsatz wesentlich ist, zeigt das Beispiel $\mathbf{Z}/(p^2) \not\simeq \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. In $\mathbf{Z}/(p^2)$ ist $\overline{p} \neq 0$, in $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ ist $(\overline{p}, \overline{p}) = 0$.

Beispiel:

1. Was ist $\mathbf{Q}[x]/(x^2-1)$? Wegen
$$1 = \frac{1}{2}(x+1) - \frac{1}{2}(x-1) \in (x+1) + (x-1)$$
sind $(x+1)$ und $(x-1)$ teilerfremde Ideale in $\mathbf{Q}[x]$. Also
$$\mathbf{Q}[x]/(x^2-1) \simeq \mathbf{Q}[x]/(x+1) \times \mathbf{Q}[x]/(x-1) \simeq \mathbf{Q} \times \mathbf{Q},$$
wobei wir $\mathbf{Q}[x]/(x-a) \simeq \mathbf{Q}$ benutzt haben. Der Isomorphismus wird dabei durch die Abbildung $f(x) \mapsto (f(-1), f(1))$ induziert.

2. Was ist $\mathbf{Z}[x]/(x^2-1)$? Hier sind $(x-1)$ und $(x+1)$ keine teilerfremden Ideale wegen
$$(x+1, x-1) = (2, x-1) \text{ und } \mathbf{Z}[x]/(x+1, x-1) \simeq \mathbf{Z}/(2).$$
Die Abbildung $\phi : \mathbf{Z}[x] \to \mathbf{Z} \times \mathbf{Z}, f \mapsto (f(1), f(-1))$ hat den Kern (x^2-1), induziert also
$$\mathbf{Z}[x]/(x^2-1) \hookrightarrow \mathbf{Z} \times \mathbf{Z},$$
ist aber nicht surjektiv wegen $f(1) \equiv f(-1) \bmod 2$. Das Bild ist $\{(a,b) \in \mathbf{Z} \times \mathbf{Z} : a \equiv b \bmod 2\}$.

Anhang: Faktorielle Ringe

Ein Element a eines Ringes R heißt irreduzibel, wenn es keine Einheit ist und wenn aus $a = bc$ folgt, daß b oder c eine Einheit ist.
Ein Integritätsring R heißt faktoriell, wenn sich jedes $a \neq 0$ modulo Einheiten eindeutig als Produkt von irreduziblen Elementen schreiben läßt. Man kann dann ein Repräsentantensystem von irreduziblen Elementen P wählen, so daß jedes $a \neq 0$ eine eindeutige Darstellung
$$a = u \cdot \prod_{p \in P} p^{v_p(a)}$$
hat. Daraus folgt auch sofort: Ist p irreduzibel, so ist (p) ein Primideal.

Folgende Ergebnisse sind aus der Algebra-Vorlesung bekannt:

1. Jeder Hauptidealring ist faktoriell.
2. Ist R faktoriell, so auch $R[x]$.
3. Der Polynomring $k[x_1, \ldots, x_n]$ über einem Körper k ist faktoriell.

Daß sich faktoriell nicht auf Faktorringe vererbt, zeigt folgendes Beispiel:

Beispiel: Der Ring $\mathbf{Z}[x]$ ist faktoriell, das Ideal (x^2+5) ist prim. Der Ring $\mathbf{Z}[x]/(x^2+5) \simeq \mathbf{Z}[\sqrt{-5}]$ ist aber nicht faktoriell. (Übung: $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.)

Beispiel: Es gibt auch faktorielle Ringe R, so daß $R[[x]]$ nicht faktoriell ist.

LEMMA. *Sei R faktoriell und $\mathfrak{p}$ ein Primideal $\neq 0$. Dann gibt es ein irreduzibles Element p mit $(p) \subseteq \mathfrak{p}$. D.h. die minimalen Primideale $\neq 0$ sind Hauptideale und werden von irreduziblen Elementen erzeugt.*

Beweis: Wähle $a = up_1 \ldots p_n \in \mathfrak{p}$. Nach der Primidealeigenschaft gibt es ein $p = p_i$ mit $p \in \mathfrak{p}$, woraus die Behauptung folgt. Es ist sofort klar, daß für zwei irreduzible Elemente p_1, p_2 mit $(p_1) \subseteq (p_2)$ sofort $(p_1) = (p_2)$ folgt. ■

Anhang: Noethersche Ringe

Ein kommutativer Ring R heißt noethersch, falls jedes Ideal in R endlich erzeugt ist, d.h. die Gestalt $(f_1, \ldots, f_n)$ mit endlich vielen $f_1, \ldots, f_n \in R$ hat. Gleichwertig damit: Jede aufsteigende Folge von Idealen

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

wird stationär, d.h. es gibt ein n mit $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$. Oder: Jede nichtleere Menge von Idealen enthält ein maximales Element (bzgl. Inklusion).

Folgendes ist aus der Algebra-Vorlesung bekannt:

1. Körper und Hauptidealringe sind noethersch.
2. Ist R noethersch, so auch $R[x]$.
3. Der Polynomring $k[x_1, \ldots, x_n]$ über einem Körper k ist noethersch.
4. Ist R noethersch, so auch $R/\mathfrak{a}$ für jedes Ideal $\mathfrak{a}$.

Beispiel: Der Ring $\mathbf{Z}[\sqrt{-5}] \simeq \mathbf{Z}[x]/(x^2+5)$ zeigt, daß ein noetherscher Ring nicht faktoriell sein muß.

Beispiel: Für einen Körper k ist $R = k[x_1, x_2, x_3, \ldots]$ faktoriell, nicht jedoch noethersch. $((x_1, x_2, x_3, \ldots)$ ist nicht endlich erzeugt.

LEMMA. *In einem noetherschen Ring R ist jedes $a \in R, a \neq 0$ Produkt von irreduziblen Elementen: $a = f_1 f_2 \ldots f_n$ mit f_i irreduzibel.*

Beweis: Sei $M = \{(a) : a \neq 0, a$ ist nicht Produkt von endlich vielen irreduziblen Elementen$\}$. Angenommen, M ist nicht leer. Dann wählen wir ein maximales Element in M: (a). Dies kann nicht irreduzibel sein, also $a = bc$ und $(a) \subset (b), (a) \subset (c)$. Gleichheit kann nicht gelten. Also sind b und c Produkt von irreduziblen Elementen, mithin auch a: ein Widerspruch. ■

SATZ. *Ist R noethersch, so auch $R[[x]]$.*

KAPITEL 3

Polynomideale — Gröbner-Basen

In diesem Abschnitt sei k ein Körper und $R = k[x_1, \ldots, x_n]$ der Polynomring über k in n Unbestimmten. Nach dem Hilbertschen Basissatz sind alle Ideale endlich erzeugt, d.h. haben die Gestalt $\mathfrak{a} = (f_1, \ldots, f_r)$.

Probleme:

1. Seien $f_1, \ldots, f_r \in R$ gegeben. Bestimme die Lösungen von
$$f_1 = \cdots = f_r = 0.$$
Wir haben bereits an einem Beispiel gesehen, daß dazu die Betrachtung des Ideals $\mathfrak{a} = (f_1, \ldots, f_r)$ sinnvoll ist. Es erhebt sich die Frage: Gibt es *einfache* Polynome in $\mathfrak{a}$.
2. Sei jetzt $\mathfrak{a} = (f_1, \ldots, f_r)$.
3. Kann man überprüfen, ob ein $f \in R$ in $\mathfrak{a}$ liegt, d.h. ob es $g_1 \ldots, g_r \in R$ gibt mit
$$f = g_1 f_1 + \cdots + g_r f_r.$$
4. Damit in Zusammenhang steht die Frage: Kann man ein schönes Repräsentantensystem für $R/\mathfrak{a}$ finden.
5. Für $n = 1$ sind alle diese Fragen einfache zu beantworten, da wir den euklidischen Algorithmus, d.h. Polynomdivision haben.
6. Gibt es eine gute Polynomdivision auch für mehrere Veränderliche?

Für das Monom $x_1^{a_1} \ldots x_n^{a_n}$ schreiben wir abkürzend auch x^a. Dabei ist $a = (a_1, \ldots, a_n)$. Wir nennen auch a den Grad von x^a. Um Polynome vernünftig vergleichen zu können, wählen wir eine Totalordnung $>$ auf der Menge der Monome $\{x^a\}$, die multiplikativ sein soll, d.h. $x^a > x^b$ impliziert $x^a x^c > x^b x^c$. Dies entspricht einer Totalordung auf $\mathbf{N}^n$ mit der Eigenschaft: $a > b$ impliziert $a + c > b + c$.

Lexikographische Ordnung: $x^a > x^b$ genau dann, wenn der erste Koeffizient $\neq 0$ in $a - b$ positiv ist. D.h. es gibt ein i mit $1 \leq i \leq n$ und
$$a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i > b_i.$$
Für zwei Variable x und y mit $x > y$ heißt das z.B.
$$x^7 > x^6 y^3 > x^6 y^2 > x^2 y^8 > y^9 > 1.$$

Natürliche gibt es auch andere multiplikative Totalordnungen auf der Menge der Monome. (Vgl. die Übungen.)

Wir fixieren eine solche Ordnung auf den Monomen, wobei wir hier bei den Beispielen immer die lexikographische Ordnung gewählt haben. Ist nun $f \in R$ mit $f \neq 0$, so können wir schreiben
$$f = c_1 x^{a_1} + \cdots + c_m x^{a_m} \text{ mit } x^{a_1} > \cdots > x^{a_m}.$$
Wir definieren $L(f) = c_1 x^{a_1}$ als den Leitterm von f und $grad(f) = a_1$ als den Grad von f.

Wir wollen nun einen Divisionsalgorithmus konstruieren: Sind $f_1, \ldots, f_r \in R$ und $f \in R$ gegeben, so suchen wir $g_1, \ldots, g_r, h \in R$ mit
$$f = g_1 f_1 + \cdots + g_r f_r + h,$$
wo h möglichst klein sein soll, was auch immer das heißt.

Beispiel: Wir wollen $f = xy^2+x+1$ durch $f_1 = xy+1$ und $f_2 = y+1$ teilen. Wir legen die lexikographische Ordnung zugrunde mit $x > y$. Zunächst ist

$$L(f) = xy^2, \quad L(f_1) = xy, \quad L(f_2) = y.$$

Wegen $L(f_1)|L(f)$, also $L(f) = yL(f_1)$, ziehen wir yf_1 ab:

$$f = yf_1 + 0 \cdot f_2 + (x - y + 1).$$

Der Rest hat $L(x - y + 1) = x$, was kein Vielfaches von $L(f_1)$ oder $L(f_2)$ ist. Sollen wir aufhören?
In $x - y + 1$ kommt das Monom $-y$ vor, das $-y = -L(f_2)$ erfüllt. Damit können wir den Rest noch kleiner machen:

$$f = yf_1 - f_2 + (x + 2).$$

Kein Monom in $x + 2$ ist durch $L(f_1)$ oder $L(f_2)$ teilbar. Wir hören auf.

Divisionsalgorithmus: Sei eine Liste $F = [f_1, \ldots, f_r]$ von Polynomene gegeben.

1. Setze
$$g := f, \quad g_1 := 0, \ldots, g_r := 0, \quad h := 0.$$
(Dann ist $f = g_1f_1 + \cdots + g_rf_r + h + g$. Man versucht g auf die anderen Terme aufzuteilen.)
2. Such den minimalen Index i mit $L(f_i)|L(g)$.
   (a) Gibt es kein i, so setze
   $$h := h + L(g), \quad g := g - L(g).$$
   Gehe nach 3.
   (b) Gibt es ein i, d.h. $L(g) = qL(f_i)$, so setze
   $$g := g - qf_i, \quad g_i := g_i + q.$$
   Dadurch wird g bzgl. der Ordnung der Monome kleiner. Gehe jetzt nach 3.
3. Ist $g \neq 0$ so gehe nach 2. Ist $g = 0$, so haben wir eine Zerlegung
   $$f = g_1f_1 + \cdots + g_rf_r + h.$$
   Wir schreiben auch $R_F(f) = g$ für den Rest. Aus dem Algorithmus folgt außerdem noch $grad(g_if_i) \leq grad(f)$.

FOLGERUNG. *Durch den beschriebenen Divisionsalgorithmus erreichen wir eine Darstellung*

$$f = g_1f_1 + \cdots + g_rf_r + h,$$

wo $h = 0$ oder kein Monom aus h ist durch eines der $L(f_i)$ teilbar. Außerdem: $grad(g_if_i) \leq grad(f)$.

Bemerkung: Im Computeralgebrasystem MAPLE ist dieser Divisionsalgorithmus implementiert:

- $with(grobner)$; ruft das entsprechende Packet auf.
- Die Funktion
  $$normalf(f, [f_1, \ldots, f_r], [x_1, \ldots, x_n], plex)$$
  gibt dann den Divisionsrest an.

Beispiel: Wir nehmen unser erstes Beispiel, aber mit verschiedener Reihenfolge der f_i:

$$f_1 = y + 1, \quad f_2 = xy + 1, \quad f = xy^2 + x + 1.$$

Zunächst ist also $g = xy^2 + x + 1$ und $g_1 = g_2 = h = 0$. Wegen $L(f_1)|L(g)$ wird

$$g := g - xyf_1 = -xy + x + 1, \quad g_1 = xy.$$

Weiter ist $L(g) = -xL(f_1)$, also

$$g := g - (-x)f_1 = 2x + 1, \quad g_1 := g_1 + (-x) = xy - x.$$

Da jetzt kein Monom von g durch $L(f_1)$ oder $L(f_2)$ teilbar ist, sind wir fertig:

$$f = (xy - x)f_1 + 0 \cdot f_2 + (2x + 1).$$

Ein Vergleich mit unserer ersten Rechnung zeigt, daß die Reihenfolge der f_i's eine Rolle spielt. Daraus ziehen wir eine einfache Folgerung: Wir haben

$$(x + 2) - (2x + 1) = -x + 1 \in (xy + 1, y + 1),$$

aber kein Monom von $-x+1$ ist durch $L(f_1)$ oder $L(f_2)$ teilbar. Folglich kann man am Divisionsalgorithmus i.a. nicht ablesen, ob f zum Ideal (f_1, f_2) gehört oder nicht.

Wir wollen nun die Leitterme etwas näher betrachten.

Definition: Ist $\mathfrak{a} \in R$ ein Ideal, so heißt

$$L(\mathfrak{a}) = (L(f) : f \in \mathfrak{a}, f \neq 0)$$

das Leittermideal von $\mathfrak{a}$.

Warnung: Aus $\mathfrak{a} = (f_1, \ldots, f_r)$ folgt noch nicht $L(\mathfrak{a}) = (L(f_1), \ldots, L(f_r))$.

Beispiel: Mit $f_1 = xy + 1, f_2 = y + 1$ gilt

$$(L(f_1), L(f_2)) = (xy, y),$$

aber

$$x = L(x - 1) \in L((f_1, f_2)), \quad x \notin (xy, y).$$

Also $(x, y) \subseteq L((f_1, f_2))$. Zeige zur Übung $(x, y) = L((f_1, f_2))$.

Das Leittermideal ist ein spezielles Beispiel eines Monomialideals:

Definition: Ein Ideal $\mathfrak{a}$ in R heißt Monomialideal, wenn es von Monomen erzeugt wird.

LEMMA. *Seien $x^{a_1}, \ldots, x^{a_r}$ Monome und $\mathfrak{a} = (x^{a_1}, \ldots, x^{a_r})$ das davon erzeugte Monomialideal. Dann gilt für ein $f \in R$: f ist genau dann in $\mathfrak{a}$, wenn jedes Monom aus f durch eines der Monome x^{a_i} teilbar ist.*

Beweis: Ist g_i ein Polynom, so ist jedes Monom aus $g_i x^{a_i}$ durch x^{a_i} teilbar. Also ist jedes Monom aus

$$g_1 x^{a_1} + \cdots + g_r x^{a_r}$$

durch eines der Monome x^{a_i} teilbar. Da jedes $f \in \mathfrak{a}$ obige Gestalt hat, folgt die eine Richtung der Behauptung. Die andere Richtung ist aber trivial. ■

DEFINITION. Sei $\mathfrak{a}$ ein Ideal in R. Polynome $f_1, \ldots, f_r \in \mathfrak{a}$ heißen eine Gröbner-Basis von $\mathfrak{a}$, wenn gilt

$$L(\mathfrak{a}) = (L(f_1), \ldots, L(f_r)).$$

Da R noethersch ist, existieren natürlich immer Gröbner-Basen. Allerdings ist die Definition nicht konstruktiv.

Eine einfache Bemerkung ist

SATZ. *Ist $f_1, \ldots, f_r$ eine Gröbner-Basis von $\mathfrak{a}$, so gilt*

$$\mathfrak{a} = (f_1, \ldots, f_r).$$

D.h. $f_1, \ldots, f_r$ erzeugen auch das Ideal.

Beweis: Sei $f \in \mathfrak{a}$. Wir müssen zeigen, daß $f \in (f_1, \ldots, f_r)$ gilt. Wir machen unseren Divisionsalgorithmus:

$$f = g_r + \cdots + g_r f_r + h,$$

wo dann kein Monom von h durch eines der Monome $L(f_i)$ teilbar ist. Nun ist aber $h \in \mathfrak{a}$, also $L(h) \in L(\mathfrak{a}) = (L(f_1), \ldots, L(f_r))$, also ist $h = 0$, was wir zeigen wollten. ■

Gröbner-Basen besitzen eine Reihe wichtiger Eigenschaften.

SATZ. *Sei $F = [f_1, \ldots, f_r]$ Gröbner-Basis des Ideals $\mathfrak{a}$. Sei $f \in R$. Dann gibt es eine Darstellung*

$$f = g_1 f_1 + \cdots + g_r f_r + h,$$

wo kein Monom aus h durch eines der $L(f_i)$ teilbar ist. h ist durch diese Bedingung eindeutig bestimmt. Insbesondere $h = R_F(f)$.

Beweis: Die Existenz der Darstellung folgt aus dem Divisionsalgorithmus. Zur Eindeutigkeit: Sei

$$f = g_1 f_1 + \cdots + g_r f_r + h = g_1' f_1 + \cdots + g_r' f_r + h',$$

wo jeweils kein Monom aus h und h' durch eines der Monome $L(f_i)$ teilbar ist. Nun ist $h - h' \in \mathfrak{a}$, also $L(h - h') \in (L(f_1), \ldots, L(f_r))$, was aber sofort $L(h - h') = 0$, also $h = h'$ impliziert. ■

FOLGERUNG. *Sei $f_1, \ldots, f_r$ eine Gröbner-Basis von $\mathfrak{a}$. Dann gilt für ein Polynom f:*

$$f \in \mathfrak{a} \quad \Longleftrightarrow \quad R_F(f) = 0.$$

Beweis: Ist $R_F(f) = 0$, so ist natürlich $f \in \mathfrak{a}$. Ist umgekehrt $f \in \mathfrak{a}$, so schreibt man $f = g_1 f_1 + \cdots + g_r f_r + 0$, wegen der Eindeutigkeit des Restes ist also $R_F(f) = 0$. ■

Genauso einfach folgt:

FOLGERUNG. *Ist $f_1, \ldots, f_r$ eine Gröbner-Basis, so hängt der Rest beim Divisionsalgorithmus nicht von der Reihenfolge der f_i's ab.*

Wie kann man nun erkennen, wann $f_1, \ldots, f_r$ eine Gröbner-Basis bilden?

Seien $f, g \in R, f, g \neq 0$. Wähle a, b minimal mit

$$\alpha x^a L(f) = \beta x^b L(g) = x^c$$

und definiere

$$S(f, g) = \alpha x^a f - \beta x^b g.$$

Da sich die Leitterme herausheben, ist klar, daß $grad(S(f, g)) < a + grad(f) = b + grad(g)$.

Beispiel: Sei $f_1 = xy + 1, f_2 = y^2 + 1$. Dann ist $L(f_1) = xy, L(f_2) = y^2$, also

$$S(f_1, f_2) = y f_1 - x f_2 = y - x.$$

Ist $F = [f_1, \ldots, f_r]$ eine Gröbner-Basis von $(f_1, \ldots, f_r)$, so ist $R_F(S(f_i, f_j)) = 0$ für alle $i < j$. Von dieser Aussage gilt auch die Umkehrung:

SATZ. *$F = [f_1, \ldots, f_r]$ ist genau dann eine Gröbner-Basis, wenn für alle $i < j$ gilt:*

$$R_F(S(f_i, f_j)) = 0.$$

Beweis: Wir nehmen an, daß die Bedingung gilt. Sei jetzt $f \in (f_1, \ldots, f_r), f \neq 0$. Wir wollen zeigen: $L(f) \in (L(f_1), \ldots, L(f_r))$. Wir können schreiben

$$f = g_1 f_1 + \cdots + g_r f_r.$$

Sei $a = \max(grad(g_i f_i), i = 1 \ldots r)$ und $\ell = \#\{i : a = grad(g_i f_i)\}$. Wir nehmen an, in obiger Darstellung von f ist zunächst a minimal gewählt und dann ℓ.

- Ist $grad(f) = a$, so gibt es ein i mit $grad(f) = grad(g_i f_i)$, also unterscheiden sich $L(f)$ und $L(g_i f_i)$ nur um eine Konstante, also $L(f) \in (L(f_i)) \in (L(f_1), \ldots, L(f_r))$.
- Jetzt nehmen wir an $grad(f) < a$. Dann müssen sich beim Aufsummieren von $g_1 f_1 + \cdots + g_r f_r$ Leitterme herausheben. Also ist $\ell \geq 2$. Wir werden zeigen, daß ℓ verkleinert werden kann und erhalten dann einen Widerspruch zur Minimalitätsvoraussetzung. O.E. $a = grad(g_1 f_1) = grad(g_2 f_2)$.
  - Wähle wieder minimal a_1, a_2 mit

    $$\alpha_1 x^{a_1} L(f_1) = \alpha_2 x^{a_2} L(f_2) = x^c.$$

    Dann ist $S(f_1, f_2) = \alpha_1 x^{a_1} f_1 - \alpha_2 x^{a_2} f_2$. Mit dem Divisionsalgorithmus und der Eigenschaft $R_F(S(f_1, f_2)) = 0$ finden wir eine Darstellung

    $$S(f_1, f_2) = h_1 f_1 + \cdots + h_r f_r$$

    mit $grad(h_i f_i) < c$.

– Nun ist $L(g_2) = \beta x^{a_2} x^b$ und $a_2 + b + grad(f_2) = a$. Damit wird

$$\begin{aligned} g_2 f_2 &= L(g_2) f_2 + (g_2 - L(g_2)) f_2 \\ &= \beta x^{a_2} x^b f_2 + (g_2 - L(g_2)) f_2 \\ &= \frac{\beta}{\alpha_2} x^b (\alpha_1 x^{a_1} f_1 - \sum h_i f_i) + (g_2 - L(g_2)) f_2. \end{aligned}$$

Hier gilt nun

$$grad(x^b h_i f_i) < b + c = a, \quad grad((g_2 - L(g_2) f_2) < a, \quad grad(x^b x^{a_1} f_1) = b + c = a.$$

Ersetzt man also $g_2 f_2$ durch obige Summe, so erniedrigt sich ℓ mindestens um 1. Dies ist aber ein Widerspruch zur Minimalitätsvoraussetzung. ■

Beispiel: Wir nehmen wieder $f_1 = xy + 1, f_2 = y + 1$. Dann ist $S(f_1, f_2) = f_1 - x f_2 = -x + 1$ und $R_F(S(f_1, f_2)) = -x + 1 \neq 0$. Also ist $[f_1, f_2]$ keine Gröbner-Basis. Da $f_3 = x - 1 \in (f_1, f_2)$ testen wir, ob $F = [f_1, f_2, f_3]$ eine Gröbner-Basis ist:

$$S(f_1, f_2) = -x + 1, \quad S(f_1, f_3) = y + 1, \quad S(f_2, f_3) = x + y.$$

Man sieht schnell, daß immer $R_F(S(f_i, f_j)) = 0$ ist, d.h. wir haben jetzt eine Gröbner-Basis.

Algorithmus zur Berechnung der Gröbner-Basis: Sei $\mathfrak{a} = (f_1, \ldots, f_r)$ gegeben. Wir betrachten die Liste $F = [f_1, \ldots, f_r]$.

Berechne für alle $i < j$ den Rest $R_F(S(f_i, f_j))$. Ist $R_F(S(f_i, f_j)) = 0$, so gehe zum nächsten Paar (i, j). Ist $R_F(S(f_i, f_j)) \neq 0$, so setze $f_{r+1} = R_F(S(f_i, f_j))$, erweitere F um f_{r+1} und fange von vorne an.
(Klar ist $f_{r+1} \in \mathfrak{a}$, aber

$$(L(f_1), \ldots, L(f_r)) \subset\neq (L(f_1), \ldots, L(f_r), L(f_{r+1})) \subseteq L(\mathfrak{a}).$$

Da R noethersch ist, hört der Prozeß irgendwann auf.)

Bemerkung: In MAPLE gibt es die Funktion $gbasis(F, X, plex)$ zur Berechnung einer Gröbner-Basis.

Beispiel: Wir betrachten wieder ein Beispiel aus dem zweiten Paragraphen:

$$f = -2 + y + x^2 + xy + y^2, \quad g = 3 - 3x + y - 3x^2 + 3xy + y^2.$$

Legt man lexikographische Ordnung zugrunde mit $x > y$, so ist

$$f = x^2 + xy + y^2 + y - 2, \quad g = -3x^2 + 3xy - 3x + y^2 + y + 3.$$

Man rechnet, wo sich F erweitert:

$$f_3 = R_{[f_1, f_2]}(S(f_1, f_2)) = 2xy - x + \frac{4}{3}y^2 + \frac{4}{3}y - 1, \quad f_4 = R_{[f_1, f_2, f_3]}(S(f_1, f_3)) = \frac{7}{9}y^3 + \frac{17}{18}y^2 - \frac{5}{3}y + \frac{1}{2}.$$

Dann stellt man fest, daß dies eine Gröbner-Basis ist. Nun ist

$$L(f_1) = x^2, \quad L(f_2) = -3x^2, \quad L(f_3) = 2xy, L(f_4) = \frac{7}{9}y^3,$$

also $L(\mathfrak{a}) = (x^2, xy, y^3)$. Also bildet auch f_1, f_3, f_4 eine Gröbner-Basis von $\mathfrak{a}$. Oder auch f_2, f_3, f_4. Eine Eindeutigkeit gibt es also so nicht.

Wir hatten schon bemerkt, daß man mit Gröbner-Basen feststellen kann, ob ein Polynom zu einem Ideal gehört: Ist F Gröbner-Basis von $\mathfrak{a}$, so gilt: $f \in \mathfrak{a} \iff R_F(f) = 0$.
Dafür jetzt ein Beispiel:

Beispiel: Sei $f_1 = xz - y^2, f_2 = x^3 - z^2$ und $\mathfrak{a} = (f_1, f_2)$. Liegt das Polynom $f = -4x^2y^2z^2 + y^6 + 3z^5$ in $\mathfrak{a}$?
Zunächst rechnet man aus, daß $R_{[f_1, f_2]}(f) = -3y^6 + 3z^5$, woraus also noch nichts folgt.
Wir berechnen eine Gröbner-Basis mit MAPLE ($x > y > z$). Man erhält:

$$F = [x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, xz - y^2, y^6 - z^5],$$

woraus man sofort sieht, daß $R_{[f_1,f_2]}(f) \in \mathfrak{a}$ ist, also auch $f \in \mathfrak{a}$. Es ist

$$L(\mathfrak{a}) = (x^3, x^2y^2, xy^4, xz, y^6).$$

Daraus sieht man z.B. schon, daß $g = xy + x - 5z^2$ nicht in $\mathfrak{a}$ liegt, wegen $L(g) = xy \notin L(\mathfrak{a})$.
Manchmal wirkt eine Änderung der Ordnung der Monome Wunder: Wählt man $y > x > z$, so ist $R_{[f_1,f_2]}(f) = 0$ und $[f_1, f_2]$ bereits Gröbner-Basis.

Bemerkung: Ist $F = [f_1, \ldots, f_r]$ Gröbner-Basis eines Ideals $\mathfrak{a}$ und $L(f_i)$ Vielfaches von einem $L(f_j)$ mit $i \neq j$, so ist

$$L(\mathfrak{a}) = (\{L(f_1), \ldots, L(f_r)\}) = (\{L(f_1), \ldots, L(f_r)\} \setminus \{L(f_i)\}),$$

also ist auch $\{f_1, \ldots, f_r\} \setminus \{f_i\}$ eine Gröbner-Basis von $\mathfrak{a}$. Diesen Prozeß kann man fortsetzen, bis man eine sogenannte minimale Gröbner-Basis erhält:

DEFINITION. Eine Gröbner-Basis $f_1, \ldots, f_r$ eines Ideals $\mathfrak{a}$ heißt minimal, wenn für alle i gilt: $L(f_i)$ ist kein Vielfaches von $L(f_j)$ für alle $j \neq i$.

Jedes Ideal hat minimale Gröbner-Basen, aber eindeutig sind sie nicht, wie obiges Beispiel zeigt. Es wäre schön, wenn wir Eindeutigkeit irgendwie erzielen könnten.

Wir wollen zwei minimale Gröbner-Basen $F = [f_1, \ldots, f_r]$ und $G = [g_1, \ldots, g_s]$ miteinander vergleichen: Wegen $L(f_i) \in (L(g_1), \ldots, L(g_s))$ gibt es ein j mit $L(g_j)|L(f_i)$. Wegen $L(g_j) \in (L(f_1), \ldots, L(f_r))$ gibt es ein ℓ mit $L(f_\ell)|L(g_j)$. Also $L(f_\ell)|L(f_i)$, was wegen der Minimalität von F zur Folge hat, daß $\ell = i$ ist, also unterscheiden sich $L(f_i)$ und $L(g_j)$ nur um eine Konstante, d.h. jedem f_i läßt sich ein g_{j_i} zuordnen, so daß sich $L(f_i)$ und $L(g_{j_i})$ nur um eine Konstante unterscheiden. Da auch eine umgekehrte Zuordnung existiert, folgt insbesondere:

FOLGERUNG. *Minimale Gröbner-Basen eines Ideals $\mathfrak{a}$ haben gleich viele Elemente.*

Wir wollen versuchen, eine minimale Gröbner-Basis $F = [f_1, \ldots, f_r]$ von $\mathfrak{a}$ noch weiter zu vereinfachen. Nach Normierung können wir annehmen:

- Alle $L(f_i)$ haben Koeffizienten 1, d.h. $L(f_i) = x^{a_i}$.
- $L(f_1) > L(f_2) > L(f_3) > \cdots > L(f_r)$.

Schreibt man $f_i = x^{a_i} + g_i$, so können wir Polynomdivision mit g_i machen und erhalten

$$g_i = \sum_{j>i} h_{ij} f_j + r_i,$$

wo kein Monom von r_i in $L(\mathfrak{a}) = (L(f_1), \ldots, L(f_r))$ liegt. Wegen $r_i - g_i \in \mathfrak{a}$ und $L(f_i) = L((f_i + r_i - g_i)$ bilden auch die $f_i - g_i + r_i = x^{a_i} + r_i$ eine Gröbner-Basis von $\mathfrak{a}$. So etwas nennt man eine reduzierte Basis.

DEFINITION. Eine Gröbner-Basis $f_1, \ldots, f_r$ heißt reduziert, wenn gilt:

- Alle $L(f_i)$ haben Koeffizienten 1.
- Für alle i liegt kein Monom von f_i in $(\{L(f_1), \ldots, L(f_r)\} \setminus \{L(f_i)\})$.

Eine reduzierte Gröbner-Basis ist also insbesondere minimal.

SATZ. *Jedes Ideal $\mathfrak{a} \neq 0$ hat eine (bis auf Reihenfolge) eindeutig bestimmte reduzierte Gröbner-Basis.*

Beweis: Die Existenz haben wir oben schon konstruktiv gezeigt. Seien jetzt $f_i = x^{a_i} + r_i$ und $g_i + x^{a_i} + s_i$, $i = 1, \ldots, r$ reduzierte Gröbner-Basen von $\mathfrak{a}$. Dann ist $r_i - s_i \in \mathfrak{a}$, also $L(r_i - s_i) \in (x^{a_1}, \ldots, x^{a_r})$, was aber sofort $r_i = s_i$ impliziert, also die Behauptung. ■

Bemerkung: Damit kann man jetzt die Gleichheit zweier Ideale testen: Die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ sind gleich, wenn ihre reduzierten Gröbner-Basen gleich sind.

Elimination: Wir betrachten jetzt die lexikographische Ordnung auf den Monomen von $R = k[x_1, \ldots, x_n]$. Für $f \in R$ gilt dann trivialerweise:

$$f \in k[x_i, x_{i+1}, \ldots, x_n] \quad \Longleftrightarrow \quad L(f) \in k[x_i, x_{i+1}, \ldots, x_n].$$

Wir wenden dies jetzt an:

SATZ. *Sei $F = \{f_1, \ldots, f_r\}$ Gröbner-Basis eines Ideals $\mathfrak{a} \subseteq R$. Sei $k[x_1, \ldots, x_n]$ mit der lexikographischen Ordnung versehen. Sei $S = k[x_i, \ldots, x_n]$. Dann ist $\mathfrak{a} \cap S$ ein Ideal in S und $F \cap S$ ist eine Gröbner-Basis von $\mathfrak{a} \cap S$.*

Beweis: Wegen $f \in S \iff L(f) \in S$ gilt die erste Gleichheit in der folgenden Gleichung

$$L(\mathfrak{a} \cap S) = L(\mathfrak{a}) \cap S = (L(f_1), \ldots, L(f_r)) \cap S = (\{L(f_1), \ldots, L(f_r)\} \cap S).$$

Damit folgt die Behauptung.
Andere Möglichkeit:
Sei $f \in \mathfrak{a} \cap S$. Dann ist $L(f) \in L(\mathfrak{a}) = (L(f_1), \ldots, L(f_r))$, also gibt es ein j mit $L(f_j)|L(f)$. Wegen $L(f) \in S$ ist auch $L(f_j) \in S$, also

$$L(f) \in (\{L(f_1), \ldots, L(f_r)\} \cap S).$$

Wegen $L(f) \in S \iff f \in S$ ist $\{f_1, \ldots, f_r\} \cap S$ eine Gröbner-Basis von $\mathfrak{a} \cap S$. ■

Bei der lexikographischen Ordnung kann man also leicht Variablen eliminieren.

Beispiel: Sei $f = x^3 + ax + b$ und $g = 3x^2 + a$. Das Polynom f hat bzgl. x mehrfache Nullstellen, wenn f und g gleichzeitig 0 werden. Wir führen die Ordnung $x > a > b$ ein und berechnen die Gröbner-Basis von f und g:

$$3x^2 + a, \quad 2ax + 3b, \quad 9bx - 2a^2, \quad 4a^3 + 27b^2.$$

Beispiel: Welche Gleichungen erfüllt die Kurve $\{(t, t^2, t^3) \in k^3 : t \in k\}$? Wir haben die Gleichungen $x = t, y = t^2, z = t^3$ und wollen t eliminieren. Wir berechnen die Gröbner-Basis von $x - t, y - t^2, z - t^3$ bzgl. der Anordnung $t > x > y > z$ und erhalten:

$$t - x, \quad x^2 - y, \quad xy - z, \quad xz - y^2, \quad y^3 - z^2.$$

Beispiel: Durch folgende Gleichungen werden 2 Geraden in k^3 parametrisiert:

$$P(t) = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t \begin{pmatrix} -1 \\ 4 \\ 2 \end{pmatrix}, \qquad Q(t) = \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix} + t \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}.$$

Bildet man die Verbindungsgerade $P(t) + u[Q(t) - P(t)]$ und läßt t variieren, so entsteht eine Regelflache. Ausgeschrieben lauten die Gleichungen

$$f = 1 - t - 3u + 3ut - x = 0, \quad g = 2 + 4t + u - 5ut - y = 0, \quad h = 3 + 2t - 2u - ut - z = 0.$$

Wählt man jetzt die lexikographische Ordnung mit $t > u > x > y > z$ und berechnet die Gröbner-Basis, so erhält man

$$\begin{aligned} &t - 11x - 7 + 12z - 9y, \\ &-5 + u + 7z - 5y - 6x, \\ &28 + 87x - 98z + 72y + 84z^2 - 123yz - 149xz + 45y^2 + 109yx + 66x^2. \end{aligned}$$

Das letzte Polynom liefert die Gleichung der Regelfläche.

Beispiel: Berechne eine Gröbner-Basis für das Ideal (f, g) bzgl. der lexikographischen Ordnung $x > y$, wo

$$f = -5x^5 + 54x^3y + 66x^2y + 77, \qquad g = -62x^2y^2 - 26xy^3 - 18x + 31y^3.$$

Wie groß werden die Koeffizienten? Warum?

Sei $\mathfrak{a}$ ein Ideal. Für die Anwendung wichtige Fragen sind folgende:

- Wie groß kann die Gröbner-Basis von $\mathfrak{a}$ werden?
- Kann man Schranken für die auftretenden Grade angeben?
- Wie groß können die Koeffizienten werden?

Meines Wissens gibt es noch keine vernünftigen Antworten auf diese Fragen.

Beispiel: Wir legen $x > y > z$ zugrunde und berechnen die Gröbner-Basis von

$$f = x^9 - yz^7, \qquad g = xy^7 - z^8.$$

Man erhält:

$$\begin{array}{l} x^9 - yz^7, \quad -y^8z^7 + x^8z^8, \quad x^7z^{16} - y^{15}z^7, \quad x^6z^{24} - y^{22}z^7, \\ x^5z^{32} - y^{29}z^7, \quad x^4z^{40} - y^{36}z^7, \quad x^3z^{48} - y^{43}z^7, \quad x^2z^{56} - y^{50}z^7, \\ xy^7 - z^8, \quad xz^{64} - y^{57}z^7, \quad -z^{72} + y^{64}z^7. \end{array}$$

Zum Abschluß geben wir noch eine alte Abschätzung von G. Hermann an: Der Totalgrad $deg(x^a)$ eines Monoms $x_1^{a_1} \dots x_n^{a_n}$ ist die Summe $a_1 + \dots + a_n$. Der Totalgrad $deg(f)$ eines Polynoms f ist das Maximum der Totalgrade der auftretenden Monome.

SATZ. *Seien $f_1, \dots, f_r$ Polynome in den Unbestimmten $x_1, \dots, x_n$ vom Totalgrad $\leq d$. Ist $f \in (f_1, \dots, f_r)$, so gibt es eine Darstellung*

$$f = g_1 f_1 + \dots + g_r f_r \text{ mit } deg(g_i) \leq deg(f) + 2(rd)^{2^{n-1}}.$$

Beispiel: Für $r = 2, n = 2$ lautet die Schranke

$$deg(g_i) \leq deg(f) + 8d^2,$$

für $r = 2, n = 3$

$$deg(g_i) \leq deg(f) + 32d^4.$$

KAPITEL 4

Bruchrechnung – Lokalisierung

Wir wollen jetzt die bekannte Bruchrechnung etwas verallgemeinern. Sei A ein kommutativer Ring. Wir wollen dann Brüche $\frac{a}{s}$ einführen mit

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \text{ und } \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$$

als Addition und Multiplikation. Als Nennermenge brauchen wir eine Menge S, die multiplikativ ist:

DEFINITION. Eine Teilmenge $S \subseteq A$ heißt multiplikativ, wenn $1 \in S$ und mit $x, y \in S$ auch $xy \in S$ gilt.

Sei nun S eine multiplikative Teilmenge von A. Auf $A \times S$ führen wir Äquivalenzrelation ein durch

$$(a, s) \sim (b, t) \iff (at - bs)u = 0 \text{ für ein } u \in S.$$

Wir zeigen die Transitivität: Sei $(a_1, s_1) \sim (a_2, s_2)$ und $(a_2, s_2) \sim (a_3, s_3)$, d.h. es gibt $u, v \in S$ mit

$$(a_1 s_2 - a_2 s_1)u = 0, \quad (a_2 s_3 - a_3 s_2)v = 0.$$

Daraus folgt:

$$\begin{aligned} 0 &= (a_1 s_2 - a_2 s_1)u s_3 v + (a_2 s_3 - a_3 s_2)v s_1 u = \\ &= a_1 s_2 s_3 uv - a_3 s_1 s_2 uv = (a_1 s_3 - a_3 s_1)uv s_2, \end{aligned}$$

also $(a_1, s_1) \sim (a_3, s_3)$. ■

Bemerkung: Daß man die etwas umständliche Definition von $\sim$ braucht, zeigt eine Übungsaufgabe.

Die Menge der Äquivalenzklassen wird mit $S^{-1}A$ oder $A[S^{-1}]$ bezeichnet. Die Äquivalenzklasse von (a, s) schreiben wir auch $\frac{a}{s}$. Durch obige Addition und Multiplikation wird $S^{-1}A$ zu einem kommutativen Ring. (Zur Übung zeige man, daß alles wohldefiniert ist.) Die Null ist $\frac{0}{1}$, die Eins $\frac{1}{1}$. Wir haben einen natürlichen Ringhomomorphismus

$$\phi_S : A \to S^{-1}A, \quad a \mapsto \frac{a}{1}.$$

SATZ. *Sei S eine multiplikative Teilmenge von A und $\phi_S : a \to S^{-1}A$ die natürliche Abbildung.*

1. *$kern(\phi_S) = \{a \in A : as = 0$ für ein $s \in S\}$.*
2. *ϕ_S ist genau dann injektiv, wenn S keine Nullteiler enthält. In diesem Fall kann man A als Unterring von $S^{-1}A$ auffassen.*
3. *$S^{-1}A = 0 \iff 0 \in S$.*

Beweis:

1. $$a \in kern(\phi_S) \iff \frac{a}{1} = \frac{0}{1} \iff as = 0 \text{ für ein } s \in S.$$
2. Folgt trivialerweise.
3. Ist $0 \in S$, so gibt es nur eine Äquivalenzklasse. Ist umgekehrt $S^{-1}A = 0$, so ist $(0, 1) \sim (1, 1)$, also gibt es ein $s \in S$ mit $1 \cdot s = 0$, also $s = 0$. ■

Beispiel: Ist A ein Integritätsring, so ist $S = A\backslash\{0\}$ eine multiplikative Teilmenge. Die Äquivalenzrelation reduziert sich auf: $(a,s) \sim (b,t)$ genau dann, wenn $at = bs$. $S^{-1}A$ ist der Quotientenkörper $Quot(A)$ von A. Da ϕ_S injektiv ist, kann man A als Teilring von $Quot(A)$ auffassen.
Beispiel: Für den Quotientenkörper von $k[x_1,\dots,x_n]$ schreibt man auch $k(x_1,\dots,x_n)$: den Körper der rationalen Funktionen in n Unbestimmten mit Koeffizienten in k.

Es folgen nun die zwei wichtigsten Beispiele:

Beispiel: Sei $f \in A$. Dann ist $S = \{1, f, f^2, f^3, \dots\}$ eine multiplikative Teilmenge von A. Für $S^{-1}A$ schreibt man auch A_f:

$$A_f = \{\frac{a}{f^n} : a \in A, n \geq 0\}.$$

Lokalisierung in einem Primideal $\mathfrak{p}$: Sei $\mathfrak{p}$ ein Primideal in A. Dann ist $S = A \setminus \mathfrak{p}$ eine multiplikative Teilmenge. $S^{-1}A$ heißt in diesem Fall auch die Lokalisierung von A in $\mathfrak{p}$ und man schreibt dafür $A_\mathfrak{p}$:

$$A_\mathfrak{p} = \{\frac{a}{s} : a \in A, s \notin \mathfrak{p}\}.$$

Motivation: Sei $A = \mathbf{R}[x]$. Die Elemente kann man auch als Funktionen auf $\mathbf{R}$ auffassen. Die Elemente des Quotientenkörpers $\mathbf{R}(x)$ sind nicht überall definiert. Was ist in 1 definiert? Die Elemente von

$$\{\frac{f(x)}{g(x)} : f, g \in \mathbf{R}[x], g(1) \neq 0\}.$$

Das ist aber nichts anderes als die Lokalisierung von $\mathbf{R}[x]$ im Primideal $(x-1)$.

Bemerkungen:

1. Für $s, t \in S$ gilt die Kürzungsregel:
$$\frac{sa}{st} = \frac{a}{t}.$$
2. Sind S und T multiplikative Teilmengen von A mit $S \subseteq T$, so faktorisiert ϕ_T in natürlicher Weise:
$$A \to S^{-1}A \to T^{-1}A,$$
wo die letzte Abbildung $S^{-1}A \to T^{-1}A$ einfach durch $\frac{a}{s} \mapsto \frac{a}{s}$ gegeben ist.
3. Ist A ein Integritätsring und S eine multiplikative Teilmenge mit $0 \notin S$, so ist $S \subseteq A \setminus \{0\}$, also erhält man:
$$A \to S^{-1}A \to Quot(A).$$
Da die gesamte Abbildung injektiv ist, kann man auch schreiben
$$A \subseteq S^{-1}A \subseteq Quot(A).$$

Sei jetzt S eine multiplikative Teilmenge von A. Für $s \in S$ gilt dann $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1} = 1$, d.h. $\phi_S(s) = \frac{s}{1}$ ist Einheit in $S^{-1}A$. Also

$$\phi_S(S) \subseteq (S^{-1}A)^\times.$$

Dadurch wird der Ring $S^{-1}A$ auch ausgezeichnet:

SATZ. *Sei S multiplikative Teilmenge von A. Ist $f : A \to B$ ein Ringhomomorphismus mit $f(S) \subseteq B^\times$, so gibt es einen eindeutig bestimmten Ringhomomorphismus $g : S^{-1}A \to B$ mit*

$$f = g \circ \phi_S = (A \to S^{-1}A \to B).$$

Beweis: Eindeutigkeit: Wie muß g aussehen, wenn es existiert? Sei $a \in A$ und $s \in S$:

$$f(a) = g(\frac{a}{1}), \quad f(s) = g(\frac{s}{1}), \quad \text{also } g(\frac{a}{s}) = f(s)^{-1}f(a).$$

Existenz: Wir müssen definieren $g(\frac{a}{s}) = f(s)^{-1}f(a)$. Zu zeigen bleibt nur, daß dies wohldefiniert ist: Sei also $\frac{a}{s} = \frac{a'}{s'}$, d.h. es gibt ein $t \in S$ mit $(as' - a's)t = 0$. Wir wenden f an: $(f(a)f(s') - f(a')f(s))f(t) = 0$. Da $f(t)$ Einheit ist, folgt $f(a)f(s') = f(a')f(s)$ und daraus sofort die Behauptung. ■

Faktorielle Ringe: Sei A ein faktorieller Ring und $\mathbf{P}$ ein Repräsentantensystem für die irreduziblen Elemente (modulo Einheiten). Jedes $a \in A, a \neq 0$ hat also eine eindeutige Darstellung

$$a = u \prod_{p \in \mathbf{P}} p^{v_p(a)},$$

wo u Einheit und $v_p(a) \geq 0$ ist. Jedes $a \in Quot(A), a \neq 0$ hat eine eindeutige Darstellung

$$a = u \prod_{p \in \mathbf{P}} p^{v_p(a)},$$

wo $u \in A^\times$ und $v_p(a) \in \mathbf{Z}$ ist.
Sei jetzt S eine multiplikative Teilmenge von A mit $0 \notin S$.
Sei $p \in \mathbf{P}$.
Behauptung: p wird Einheit in $S^{-1}A$ genau dann, wenn $(p) \cap S \neq \emptyset$.
Beweis: Gilt $(p) \cap S \neq \emptyset$, so wird p Einheit in $S^{-1}A$. Ist umgekehrt p Einheit in $S^{-1}A$, so gibt es $\frac{a}{s} \in S^{-1}A$ mit $1 = \frac{pa}{s}$. Also ist $s \in S \cap (p)$. ■Damit folgt jetzt schnell, daß auch $S^{-1}A$ faktoriell ist und

$\mathbf{P}_S = \{p \in \mathbf{P} : (p) \cap S = \emptyset\}$ ein Repräsentantensystem für die irreduziblen Elemente.

Wir wollen nun die Ideale in $S^{-1}A$ betrachten. Ist $\mathfrak{a}$ Ideal in A, so ist

$$S^{-1}\mathfrak{a} := \{\frac{a}{s} : a \in \mathfrak{a}, s \in S\}$$

ein Ideal in $S^{-1}A$.

SATZ. *Jedes Ideal in $S^{-1}A$ hat die Gestalt $S^{-1}\mathfrak{a}$ mit einem Ideal $\mathfrak{a}$ in A. Außerdem gelten die Rechenregeln:*

$$S^{-1}(\mathfrak{a}+\mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}, S^{-1}(\mathfrak{a}\mathfrak{b}) = S^{-1}\mathfrak{a}S^{-1}\mathfrak{b}, S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}.$$

Beweis: Sei $\mathfrak{b}$ ein Ideal in $S^{-1}A$. Dann ist $\mathfrak{a} := \phi_S^{-1}(\mathfrak{b})$ ein Ideal in A. Offensichtlich ist $\phi_S(\mathfrak{a}) \subseteq \mathfrak{b}$, also auch $S^{-1}\mathfrak{a} \subseteq \mathfrak{b}$. Sei jetzt $\frac{a}{s} \in \mathfrak{b}$. Dann ist auch $\frac{a}{1} \in \mathfrak{b}$, also $a \in \mathfrak{a}$, also $\frac{a}{s} \in S^{-1}\mathfrak{a}$. Damit folgt die erste Behauptung. Die Rechenregeln lassen wir als Übungsaufgabe. ■

FOLGERUNG. *Ist A Hauptidealring, so auch $S^{-1}A$, wenn $0 \notin S$. Ist A noethersch, so auch $S^{-1}A$.*

Wir wollen jetzt noch die Primideale genauer untersuchen. Dazu eine wichtige Bemerkung:

LEMMA. *Ist $f : A \to B$ ein Ringhomomorphismus und $\mathfrak{p}$ ein Primideal in B, so ist $f^{-1}(\mathfrak{p})$ ein Primideal in A.*

Beweis: f induziert einen Homomorphismus $A \to B \to B/\mathfrak{p}$. Der Kern ist $f^{-1}\mathfrak{p}$, also haben wir eine Einbettung

$$A/f^{-1}\mathfrak{p} \hookrightarrow B/\mathfrak{p}.$$

Da eine Unterring eines Integritätsrings wieder ein Integritätsring ist, folgt die Behauptung. ■

SATZ. *Die Zuordnung $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ liefert eine Bijektion zwischen*

$$\{\mathfrak{p} \subseteq A : \mathfrak{p} \text{ Primideal mit } \mathfrak{p} \cap S = \emptyset\} \to \{\text{Primideale von } S^{-1}A\}.$$

Beweis:

- Ist $\mathfrak{q}$ ein Primideal ist $S^{-1}A$, so ist $\mathfrak{p} := \phi_S^{-1}(\mathfrak{q})$ ein Primideal in A und wie zuvor $\mathfrak{q} = S^{-1}\mathfrak{p}$. Natürlich ist $S \cap \mathfrak{p} = \emptyset$, denn sonst würde $S^{-1}\mathfrak{p}$ die 1 enthalten, was nicht geht.
- Sei $\mathfrak{p}$ ein Primideal mit $S \cap \mathfrak{p} = \emptyset$.
  Behauptung: $\mathfrak{q} = S^{-1}\mathfrak{p}$ ist ein Primideal.
  Beweis: Angenommen $\mathfrak{q} = S^{-1}A$. Dann gäbe es $p \in \mathfrak{p}, s \in S$ mit $\frac{p}{s} = \frac{1}{1}$, also gäbe es ein $t \in S$ mit $(p-s)t = 0$, was $st \in S \cap \mathfrak{p}$, also einen Widerspruch lieferte. Sei nun $\frac{a_1}{s_1}\frac{a_2}{s_2} \in \mathfrak{q}$. Dann ist auch $\frac{a_1 a_2}{1} \in \mathfrak{q}$, also gibt es $p \in \mathfrak{p}, s \in S$ mit $\frac{a_1 a_2}{1} = \frac{p}{s}$ und demnach $t \in S$ mit $(a_1 a_2 s - p)t = 0$. Also ist $a_1 a_2 \in \mathfrak{p}$ wegen $s \notin \mathfrak{p}$, also $\frac{a_1}{s_1}$ oder $\frac{a_2}{s_2}$ in $\mathfrak{q}$.

- Sei $\mathfrak{p}$ Primideal in A mit $S \cap \mathfrak{p} = \emptyset$. Klar ist $\mathfrak{p} \subseteq \phi_S^{-1}(S^{-1}\mathfrak{p})$. Sei umgekehrt $a \in \phi_S^{-1}(S^{-1}\mathfrak{p})$. Dann ist $\frac{a}{1} = \frac{p}{s}$ mit einem $p \in \mathfrak{p}$ und einem $s \in S$. Wie zuvor folgt $a \in \mathfrak{p}$. Also haben wir
$$\mathfrak{p} = \phi_S^{-1}(S^{-1}\mathfrak{p}).$$
Damit folgt alles. ■

Bemerkung: Im allgemeinen gilt nicht: $\mathfrak{a} = \phi_S^{-1}(S^{-1}\mathfrak{a})$, auch wenn $\mathfrak{a} \cap S = \emptyset$ gilt.
Beispiel: Sei $A = \mathbf{Z}$ und $S = \{1, 2, 4, 8, 16, \dots\}$ und $\mathfrak{a} = (6)$. Dann ist $S^{-1}\mathfrak{a} = \{\frac{3n}{2^m} : n \in \mathbf{Z}, m \in \mathbf{N}\}$, also $\phi_S^{-1}(S^{-1}\mathfrak{a}) = (3)$.

Beispiel: Wir betrachten die Lokalisierung von A im Primideal $\mathfrak{p}$. Sei $S = A \setminus \mathfrak{p}$. Die Primideale $\mathfrak{q}$ mit $\mathfrak{q} \cap S = \emptyset$ sind genau die in $\mathfrak{p}$ enthaltenen Primideale. Also stehen die Primideale von $A_\mathfrak{p}$ in Bijektion zu den in $\mathfrak{p}$ enthaltenen Primidealen von A. Offensichtlich ist dann $\mathfrak{p}A_\mathfrak{p}$ das größte Primideal von $A_\mathfrak{p}$. Dies ist ein Beispiel für einen lokalen Ring.

DEFINITION. Ein Ring R heißt lokaler Ring, wenn er genau ein maximales Ideal $\mathfrak{m}$ besitzt. $R/\mathfrak{m}$ heißt der Restklassenkörper von R.

Bemerkung: Sei $(R, \mathfrak{m})$ ein lokaler Ring. Ist $x \notin \mathfrak{m}$, so ist $(x) \not\subseteq \mathfrak{m}$, also muß $(x) = R$ gelten, d.h. x ist Einheit: $R = \mathfrak{m} \cup R^\times$.

Durch Lokalisierung wird ein Ring i.a. einfacher. Daher kann man hoffen, Eigenschaften der Lokalisierungen leichter zu überprüfen. Dann sollte man von der lokalen Situation auf die globale schließen können. Wir geben ein paar Anwendungen.
Wir wollen jetzt noch Vorteile lokaler Ringe betrachten.

SATZ. *Sei $(R, \mathfrak{m})$ ein noetherscher lokaler Integritätsring, aber kein Körper. Wird $\mathfrak{m}$ von einem Element π erzeugt, so ist R Hauptidealring.*

Beweis:

1. *Behauptung:* Jedes $a \neq 0$ hat eine Zerlegung $a = u \cdot \pi^m$, wo u Einheit ist.
Beweis: Ist a durch π^n teilbar, so schreibe $a = a_n\pi^n$. Wegen $a = a_n\pi^n = a_{n-1}\pi^{n-1}$ gilt $a_{n-1} = \pi a_n$, also $(a_{n-1}) \subset (a_n)$. Also
$$(a_0) \subset (a_1) \subset (a_2) \subset \dots.$$
Da R noethersch ist, kann dies nicht beliebig weitergehen. Sei m maximal mit $a = a_m\pi^m$. Wäre $a_m \in \mathfrak{m} \in (\pi)$, so könnte man nochmals π ausklammern. Also ist a_m Einheit.

2. Die Zerlegung ist eindeutig: Sei $u\pi^m = v\pi^n$. Ist $m = n$, so sind wir fertig. Sei o.E. $n > m$. Dann ist $u = v\pi^{n-m} \in \mathfrak{m}$, ein Widerspruch.
3. Für zwei Elemente $a = u\pi^m$ und $b = v\pi^n$ (u, v Einheiten) gilt:
$$(b) \subseteq (a) \quad \Longleftrightarrow \quad a|b \quad \Longleftrightarrow \; m \leq n.$$
4. Wegen $(\pi^{n_1}, \dots, \pi^{n_r}) = (\pi^{\min n_i})$ folgt sofort, daß die einzigen Ideale
$$(0) \subset \dots \subset (\pi^3) \subset (\pi^2) \subset (p) \subset R$$
sind. Also ist hier Hauptidealring. ■

DEFINITION. Ein faktorieller Ring R mit (bis auf Einheiten) genau einem irreduziblen Element π heißt diskreter Bewertungsring. Jedes $a \neq$ in R hat eine eindeutige Darstellung
$$a = u \cdot \pi^{v(a)},$$
wo u Einheit und $v(a) \geq 0$ ist. Die Funktion v heißt auch Bewertung.

Aus obigem Beweis folgt unmittelbar:

SATZ. *Für einen Ring R sind äquivalent:*

- *R ist diskreter Bewertungsring.*
- *R ist lokaler noetherscher Ring, dessen maximales Ideal von einem Element $\neq 0$ erzeugt wird.*

Beispiel: Sei $\mathfrak{o}$ der Ring der auf ganz $\mathbf{C}$ holomorphen Funktionen. Der Quotientenkörper von $\mathfrak{o}$ ist dann der Körper $\mathfrak{m}$ der auf $\mathbf{C}$ meromorphen Funktionen. (Produktsatz) Sei $a \in \mathbf{C}$. Die Menge $\mathfrak{p} = \{f \in \mathfrak{o} : f(a) = 0\}$ ist ein Ideal in $\mathfrak{o}$. Jedes $f \in \mathfrak{o}$ hat in $z = a$ eine Taylorreihenentwicklung:

$$f = c_0 + c_1(z-a) + c_2(z-a)^2 + \ldots,$$

woraus man sofort sieht: $\mathfrak{p} = (z-a)$. Dann ist die Lokalisierung von $\mathfrak{o}$ in $\mathfrak{p}$:

$$\mathfrak{o}_\mathfrak{p} = \{f \in \mathfrak{m} : f \text{ in } a \text{ definiert}\}.$$

Da jedes $f \in \mathfrak{o}_\mathfrak{p}, f \neq 0$ sich eindeutig in der Form

$$f = u(z-a)^n \text{ mit } u(a) \neq 0, n \geq 0$$

schreiben läßt, ist $\mathfrak{o}_\mathfrak{p}$ ein diskreter Bewertungsring. Die Bewertung ist die Nullstellenordnung.

Beispiel: Wir betrachten den Ring $R = \mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[x]/(x^2+5)$, der kein Hauptidealring und auch nicht faktoriell ist $(2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}))$. Das Ideal (2) ist kein Primideal, denn

$$R/(2) \simeq \mathbf{Z}[x]/(2, x^2+5) \simeq \mathbf{F}_2[x]/((x+1)^2).$$

Aber $\mathfrak{p} = (2, 1+\sqrt{-5})$ ist Primideal, sogar maximal, denn

$$R/\mathfrak{p} \simeq \mathbf{Z}[x]/(2, x+1, x^2+5) = \mathbf{Z}[x]/(2, x+1) \simeq \mathbf{F}_2.$$

Zeige, daß $\mathfrak{p}$ kein Hauptideal ist. Wir wollen aber zeigen, daß $R_\mathfrak{p}$ ein diskreter Bewertungsring ist. Nun ist in $Quot(R)$:

$$\frac{2}{1+\sqrt{-5}} = \frac{2(1-\sqrt{-5})}{6} = \frac{1-\sqrt{-5}}{3} \in R_\mathfrak{p},$$

also $2 \in (1+\sqrt{-5})R_\mathfrak{p}$ und damit $\mathfrak{p}R_{pp} = (1+\sqrt{-5})R_\mathfrak{p}$. Nach unserem Satz ist damit $R_\mathfrak{p}$ diskreter Bewertungsring. Für die Bewertung v gilt: $v(1+\sqrt{-5}) = 1$. Wegen

$$\frac{1-\sqrt{-5}}{1+\sqrt{-5}} = \frac{-2-\sqrt{-5}}{3} \in (R_\mathfrak{p})^\times$$

gilt $v(1-\sqrt{-5}) = 1$ und damit $v(2) = 2$.

Beispiel: Wir betrachten den Ring $A = \mathbf{Q}[X,Y]/(X+Y+X^2+Y^2)$. Die Bilder von X und Y in A bezeichnen wir mit x und y. Da $X+Y+X^2+Y^2$ irreduzibel ist, ist A ein Integritätsring. Wegen

$$(X+Y+X^2+Y^2) \subseteq (X,Y)$$

ist $\mathfrak{m} = (x,y)$ ein maximales Ideal in A. Ist $A_\mathfrak{m}$ ein diskreter Bewertungsring? Es ist

$$A_\mathfrak{m} = \{\frac{f(x,y)}{g(x,y)} : g(0,0) \neq 0\}.$$

Wird $\mathfrak{m}$ von einem Element erzeugt? Wegen $x+y+x^2+y^2 = 0$ gilt $y(1+y) = -x-x^2$, also $y = -\frac{x+x^2}{1+y}$ in $A_\mathfrak{m}$, also $(x,y) = (x)$. Also ist $A_\mathfrak{m}$ ein diskreter Bewertungsring.

Sei $\mathfrak{p}$ Primideal in A. Sei $f : A \to A/\mathfrak{p} \subseteq Quot(A/\mathfrak{p})$ die nach $Quot(A/\mathfrak{p})$ fortgesetzte Restklassenabbildung. Ist $s \notin \mathfrak{p}$, dann ist $f(s) \neq 0$, also Einheit in $Quot(A/\mathfrak{p})$. Also induziert f die Abbildung

$$A_\mathfrak{p} \to Quot(A/\mathfrak{p}), \quad \frac{a}{s} \mapsto \frac{f(a)}{f(s)}.$$

Offensichtlich ist die Abbildung surjektiv und hat Kern $\mathfrak{p}A_\mathfrak{p}$, woraus sofort folgt:

LEMMA. *Für ein Primideal $\mathfrak{p}$ in A gilt:*

$$A_{pp}/\mathfrak{p}A_{pp} \simeq Quot(A/\mathfrak{p}).$$

Wir wollen noch ein Beispiel geben.

SATZ. *Sei A ein Integritätsring. Dann gilt:*

$$A = \cap_{\mathfrak{m}\ maximal} A_\mathfrak{m}.$$

Beweis: Ist K der Quotientenkörper, so liegen alle $A_{\mathfrak{m}}$ in K, also macht obiger Durchschnitt Sinn. Klar ist $A \subset \cap A_{\mathfrak{m}}$. Sei umgekehrt $r \in \cap A_{\mathfrak{m}}$. Betrachte $\mathfrak{a} = \{a \in A : ar \in A\}$. Dies ist ein Ideal in A (Nennerideal). Ist $1 \in \mathfrak{a}$, so sind wir fertig. Andernfalls gibt es ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$. Dies widerspricht aber $r \in A_{\mathfrak{m}}$. ■

KAPITEL 5

Moduln

Sei R ein kommutativer Ring. Ein R-Modul M ist besteht aus einer abelschen Gruppe $(M,+)$ und einer Operation $R \times N \to M$ mit den Eigenschaften

$$a(x+y) = ax + ay, \quad (a+b)x = ax + bx, \quad (ab)x = a(bx), \quad 1x = x$$

für alle $a, b \in R, x, y \in M$.

Beispiele:

1. Ist $R = k$ ein Körper, so sind die k-Moduln die k-Vektorräume.
2. Jedes R-Ideal $\mathfrak{a}$ ist ein R-Modul.
3. Die $\mathbf{Z}$-Moduln sind genau die abelschen Gruppen.
4. Ist k ein Körper, V ein k-Vektorraum und $\phi : V \to V$ ein Endomorphismus, so wird V zu einem $k[x]$-Modul durch
$$f(x) \cdot v = f(\phi)(v).$$
5. Ist M ein R-Modul, $\mathfrak{a}$ ein Ideal in R, so ist auch
$$\mathfrak{a}M = \{\sum a_i m_i : a_i \in \mathfrak{a}, m_i \in M\}$$
ein R-Modul.

Ein R-Modulhomomorphismus $f : M \to N$ ist eine R-lineare Abbildung. In der üblichen Weise bilden die Homomorphismen wieder einen R-Modul:

$$Hom_R(M,N) = \{f : M \to N : f \text{ linear}\}.$$

Auch Kern und Bild eines Homomorphismus werden wie übliche definiert. Im Fall $M = N$ spricht man auch von Endomorphismen. Man setzt $End_R(M) = Hom_R(M,M)$. Durch Verknüpfung wird $End_R(M)$ sogar zu einem (i.a. nicht kommutativen) Ring.

Ist $N \subseteq M$ ein Untermodul von M, so definiert man für $x, y \in M$: $x \equiv y \bmod N \iff x - y \in N$. Dies ist eine Äquivalenzrelation, die Menge der Äquivalenzklassen wird mit M/N bezeichnet und hat wieder die Struktur eines R-Moduls. Sind $M_i, i \in I$ Untermoduln von M, so kann man die Summe $\Sigma_{i \in I} M_i \subseteq M$ betrachten.

Ist $f : M \to N$ ein R-Modulhomomorphismus, so heißt $N/Bild(f)$ der Kokern von f. Man hat wieder eine Isomorphie:

$$M/kern(f) \simeq Bild(f).$$

Außerdem hat man noch folgenden

SATZ. 1. *Sind $L \subseteq M \subseteq N$ R-Moduln, so gilt*

$$N/M \simeq (N/L)/(M/L).$$

2. *Sind M und N Untermoduln eines Moduls L, so gilt:*

$$(M+N)/M \simeq N/(M \cap N).$$

Beweis:

1. Betrachte den natürlichen Homomorphismus $f : N \to (N/L)/(M/L)$, der offensichtlich surjektiv ist und den Kern M hat. Daraus folgt sofort die Behauptung.

2. Betrachte den natürlichen Homomorphismus $f : N \to (M+N)/M$. Er ist surjektiv. Der Kern ist $M \cap N$, also folgt die Behauptung. ■

Ist $M_i, i \in I$ eine Familie von R-Moduln, so kann man die direkte Summe $\oplus_{i\in I} M_i$ und das direkte Produkt $\prod_{i\in I} M_i$ betrachten.
Ein R-Modul M heißt frei, wenn $M \simeq \oplus_{i\in I} R$ gilt. Man kann dies auch so formulieren: M ist genau dann frei, wenn es eine Teilmenge $\{e_i : i \in I\} \subseteq M$ gibt, so daß sich jedes Element aus M eindeutig in der Form $\sum_{i\in I} x_i e_i$ schreiben läßt, mit $x_i \in R$, alle bis auf endlich viele $= 0$.

Beispiele:

1. Ist k ein Körper, so sind alle k-Moduln= k-Vektorräume frei.
2. Ist R ein Integritätsring und $\mathfrak{a}$ ein Ideal, so ist $\mathfrak{a}$ genau dann ein freier R-Modul, wenn $\mathfrak{a}$ ein Hauptideal ist.
   Beweis: Ist $\mathfrak{a} = (f)$ ein Hauptideal und $\mathfrak{a} \neq 0$, so läßt sich jedes $a \in \mathfrak{a}$ eindeutig als $a = xf$ darstellen, also $\mathfrak{a} \simeq R$. Sei umgekehrt $\mathfrak{a}$ ein freier R-Modul und $e_i, i \in I$ eine Basis von $\mathfrak{a}$. Wäre $\#I > 1$, so gäbe es $i, j \in I, i \neq j$, also $0 = e_j e_i - e_i e_j$, und 0 hätte mehrere Darstellungen. Also bleibt nur $\#I = 1$, d.h. $\mathfrak{a} = Re$, d.h. $\mathfrak{a}$ ist Hauptideal.

Ein R-Modul M heißt endlich erzeugt, wenn es endlich viele $m_1, \ldots, m_n \in M$ gibt mit $M = \sum_{i=1}^n Rm_i$. Dafür kann man auch sagen: M ist Bild eines freien Moduls R^n.

Die endlich erzeugten Moduln spielen eine wesentliche Rolle.

Erinnerung an Determinanten: Sei R ein kommutativer Ring. Dann ist auch auf dem Matrizenring $M_n(R)$ die Determinante *det* definiert. Es gilt der Entwicklungssatz.
Sei $A = (a_{ik}) \in M_n(R)$ und A_{ij} die Untermatrix von A, die durch Streichen der i-ten Zeile und j-ten Spalte entsteht. Dann ist auch $b_{ij} := (-1)^{i+j} det(A_{ji}) \in R$ und es gilt:

$$det(A) = \sum_j (-1)^{i+j} a_{ij} det(A_{ij}) = \sum a_{ij} b_{ji}.$$

Ersetzt man die i-te Zeile durch die k-te Zeile, so wird natürlich die Determinante 0, aber die vorigen Untermatrizen bleiben gleich, also

$$0 = \sum_j (-1)^{i+j} a_{kj} det(A_{ij}) = \sum_j a_{kj} b_{ji}.$$

Dies liefert sofort $AB = det(A)E$, wo E die Einheitsmatrix bezeichnet. Analog zeigt man $AB = det(A)E$. B heißt die zu A adjungierte Matrix.

SATZ. *Sei M ein endlich erzeugter R-Modul, $\mathfrak{a}$ ein Ideal in R, $\phi \in End_R(M)$ mit $\phi(M) \subseteq \mathfrak{a}M$. Dann genügt ϕ einer Gleichung*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

mit $a_i \in \mathfrak{a}$.

Beweis: Sei $x_1, \ldots, x_n$ ein Erzeugendensystem von M. Dann gilt $\phi(x_i) \in \mathfrak{a}M$, also gibt es $a_{ij} \in \mathfrak{a}$ mit $\phi(x_i) = \sum_j a_{ij} x_j$. Wir rechnen jetzt mit Matrizen über dem Ring $R[\phi] \subseteq M_n(R)$. Sei A die Matrix $(\phi\delta_{ij} - a_{ij})$. Dann gilt $A \cdot x = 0$, wo x den Spaltenvektor bezeichnet, der von den x_i gebildet wird. Multipliziert man mit der adjungierten Matrix von A, so erhält man $det(A)x_i = 0$ für alle i, also ist $det(A) = 0$ in $End_R(M)$. In der üblichen Weise folgt die Behauptung. ■

FOLGERUNG. *Ist M ein endliche erzeugter R-Modul und $\mathfrak{a}$ ein Ideal in R mit $\mathfrak{a}M = M$, dann gibt es ein $x \equiv 1 \bmod \mathfrak{a}$ mit $xM = 0$.*

Beweis: Wähle im Satz $\phi = 1$, dann gibt es $a_1, \ldots, a_n \in \mathfrak{a}$ mit $E + a_1E + \cdots + a_nE = 0$ in $End_R(M)$, d.h mit $x = 1 + a_1 + \cdots + a_n \in R$ ist $xM = 0$. ■

FOLGERUNG (Lemma von Nakayama). *Ist $(R, \mathfrak{m})$ ein lokaler Ring und M ein endlich erzeugter Modul mit $M = \mathfrak{m}M$, so folgt $M = 0$.*

Beweis: Nach der letzten Folgerung gibt es ein $x \equiv 1 \bmod \mathfrak{m}$ mit $xM = 0$. Hier ist aber x Einheit, also folgt $M = 0$. ■

FOLGERUNG. *Sei wieder $(R, \mathfrak{m})$ ein lokaler Ring, M ein endlich erzeugter Modul und N ein Teilmodul mit $M = N + \mathfrak{m}M$. Dann folgt $M = N$.*

Wir wollen dies anwenden: Der Modul $M/\mathfrak{m}M$ wird von $\mathfrak{m}$ annuliert, also können wir $M/\mathfrak{m}M$ auch als $k = R/\mathfrak{m}$-Vektorraum auffassen. Wir bezeichen das Bild von $x \in M$ in $M/\mathfrak{m}M$ mit $\overline{x}$. Mit diesen Bezeichnungen gilt:

LEMMA. *Seien $x_1, \ldots, x_n \in M$. Dann sind äquivalent:*

- *$x_1, \ldots, x_n$ erzeugen M als R-Modul,*
- *$\overline{x_1}, \ldots, \overline{x_n}$ erzeugen $M/\mathfrak{m}M$ als k-Vektorraum.*

Beweis: Die eine Richtung ist klar. Seien jetzt $x_1, \ldots, x_n \in M$ so, daß ihre Bilder $M/\mathfrak{m}M$ als k-Vektorraum erzeugen. Sei $N = \sum_{i=1}^{n} Rx_i$. Dann gilt $M = N + \mathfrak{m}M$ und nach dem letzten Lemma folgt $M = N$. ■

Exakte Sequenzen: Eine Folge von R-Moduln

$$\cdots \to M_{i-1} \to M_i \to M_{i+1}$$

mit $f_i : M_{i-1} \to M_i$ heißt exakt an der Stelle M_i, wenn $Bild(f_i) = Kern(f_{i+1})$. Die Sequenz heißt exakt, wenn sie an jeder Stelle exakt ist. Insbesondere:

$$0 \to M' \to M \text{ ist exakt} \iff M' \to M \text{ ist injektiv},$$
$$M \to M'' \to 0 \text{ ist exakt} \iff M \to M'' \text{ ist surjektiv}.$$

Eine exakte Sequenz $0 \to M' \to M \to M'' \to 0$ heißt auch kurze exakte Sequenz. Ist $f : M' \to M$ und $g : M \to M''$, so ist die Exaktheit äquivalent mit f injektiv, g surjektiv und $Bild(f) = Kern(g)$.

Beispiel: Ist N ein Untermodul von M, so ist

$$0 \to N \to M \to M/N \to 0$$

exakt.

Tensorprodukt: Seien M, N, P drei R-Moduln. Eine Abbildung $f : M \times N \to P$ heißt bilinear, wenn gilt:

$$f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y), \quad f(ax, y) = af(x, y),$$
$$f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2), \quad f(x, ay) = af(x, y).$$

Folgender Satz definiert das Tensorprodukt:

SATZ. *Sind M und N zwei R-Moduln, so gibt es einen R-Modul T und eine bilineare Abbildung $g : M \times N \to T$ mit der Eigenschaft: Ist $f : M \times N \to P$ bilinear, so gibt es genau eine lineare Abbildung $f' : T \to P$ mit $f = f' \circ g$. (f faktorisiert also über T.) Das Paar (T, g) ist bis auf Isomorphie eindeutig bestimmt und heißt das Tensorprodukt von M und N.*

Beweis:
Eindeutigkeit: Angenommen, wir haben noch ein Paar (T', g'), das obige Eigenschaften erfüllt. Wegen der universellen Eigenschaft von (T, g) gibt es ein $j : T \to T'$ mit $g' = j \circ g$. Analog gibt es ein $j' : T' \to T$ mit $g = j' \circ g'$. Es folgt $g = j' \circ j \circ g$ und aus der Eigenschaft von (T, g) folgt, $j' \circ j = id$. Analog $j \circ j' = id$. Also ist j ein Isomorphismus und $g' = j \circ g$.
Existenz:

1. Sei F der freie R-Modul mit der Basis $\{(x, y) : x \in M, y \in N\}$. Die Elemente in F haben also die Gestalt
$$\sum a_i(x_i, y_i) \text{ mit } a_i \in R, x_i \in M, y_i \in N.$$
Sei G der Untermodul von F, der von allen Ausdrücken der Form
$$(x_1 + x_2, y) - (x_1, y) - (x_2, y), (ax, y) - a(x, y), (x, y_1 + y_2) - (x, y_1) - (x, y_2), (x, ay) - a(x, y)$$
erzeugt wird.

2. Sei $T = F/G$. Mit $x \otimes y$ bezeichnen wir das Bild des Basiselements (x, y) in T. Die Elemente aus T haben dann die Form $\sum a_i x_i \otimes y_i$. Es gelten die Rechenregeln:
$$\begin{aligned}(x_1 + x_2) \otimes y &= x_1 \otimes y + x_2 \otimes y,\\ x \otimes (y_1 + y_2) &= x \otimes y_1 + x \otimes y_2,\\ (ax) \otimes y &= a(x \otimes y) = x \otimes (ay).\end{aligned}$$
Definiert man jetzt $g : M \times N \to T$ durch $g(x, y) = x \times y$, so ist g bilinear.
3. Sei jetzt $f : M \times N \to P$ eine bilinear Abbildung. Definiere $\overline{f} : F \to P$ durch
$$\overline{f}(\sum a_i(x_i, y_i)) = \sum a_i f(x_i, y_i).$$
Da f bilinear ist, verschwindet $\overline{f}$ auf allen Erzeugern von G, also auf ganz G. D.h. wir erhalten eine lineare Abbildung $f' : T \to P$ mit $f'(x \otimes y) = f(x, y)$. Es ist klar, daß f' dadurch eindeutig bestimmt ist. ■

Bemerkung: Für das Tensorprodukt von M und N schreiben wir $M \otimes N$ oder $M \otimes_R N$. Es wird als R-Modul erzeugt von den Tensoren $x \otimes y$. Sind M und N endlich erzeugt, so auch $M \otimes N$.

Bemerkung: Analog wie eben erhält man auch ein Tensorprodukt $M_1 \otimes M_2 \otimes \cdots \otimes M_n$, wenn man multilineare Abbildungen $f : M_1 \times \cdots \times M_n \to P$ studiert.

Beispiel: Sei k ein Körper und seien V und W zwei Vektorräume mit Basen $v_1, \ldots, v_m$ und $w_1, \ldots, w_m$. Dann wird $V \otimes W$ offensichtlich erzeugt von den mn Elementen $v_i \otimes w_j$. Da es mn linear unabhängige bilineare Abbildungen $V \times W \to k$ gibt, bilden die $v_i \otimes w_j$ auch eine Basis. Insbesondere: $dim(V \otimes W) = (dimV)(dimW)$.

Beispiel: Was ist $\mathbf{Z}/(2) \otimes_{\mathbf{Z}} \mathbf{Z}/(3)$? Sei $a \in \mathbf{Z}/(2), b \in \mathbf{Z}/(3)$. Dann gilt:
$$a \otimes b = (3a) \otimes b = a \otimes (3b) = a \otimes 0 = 0,$$
also $\mathbf{Z}/(2) \otimes \mathbf{Z}/(3) = 0$.

Beispiel: Ist $M' \subseteq M$ ein Untermodul, so kann man i.a. $M' \otimes N$ nicht als Untermodul von $M \otimes N$ auffassen, d.h. die kanonische Abbildung $M' \otimes N \to M \otimes N$ ist i.a. nicht injektiv.
Wähle $R = \mathbf{Z}$ und $M' = 2\mathbf{Z}, M = \mathbf{Z}, N = \mathbf{Z}/(2)$.

- In $\mathbf{Z} \otimes \mathbf{Z}/(2)$ gilt $2 \otimes 1 = 1 \otimes 2 = 0$.
- In $(2\mathbf{Z}) \otimes \mathbf{Z}/(2)$ gilt $2 \otimes 1 \neq 0$.
  Beweis: Definiere $f : (2\mathbf{Z} \times \mathbf{Z}/(2) \to \mathbf{Z}/(2)$ durch $f(x, y) = \frac{\overline{x}}{2} \cdot y$. Die Abbildung f ist bilinear, also faktorisiert sie über das Tensorprodukt: $f(x, y) = f'(x \otimes y)$. Damit
  $$f'(2 \otimes 1) = f(2, 1) = 1 \neq 0, \text{ also } 2 \otimes 1 \neq 0.$$

Da das Tensorprodukt manchmal zusammen brechen kann, ist es nützlich zu wissen, wann so etwas nicht passiert.

LEMMA. *Ist F ein freier R-Modul mit Basis $e_i, i \in I$, so läßt sich jedes $x \in M \otimes F$ eindeutig in der Form*
$$x = \sum m_i \otimes e_i$$
schreiben.

Beweis:

1. Sei $m \in M$ und $a \in F$. Dann gibt es eine Darstellung
$$a = \sum r_i e_i \text{ mit } r_i \in R.$$
Also gilt
$$m \otimes a = \sum (r_i m) \otimes e_i.$$

2. Da jedes Element aus $M \otimes F$ die Form $\sum m_j \otimes a_j$ hat, folgt mit 1., daß sich jedes Element als
$$\sum m_i \otimes e_i$$
schreiben läßt.
3. Wir müssen noch zeigen, daß die Darstellung eindeutig ist. Dazu genügt es zu zeigen: Ist $x = \sum m_i \otimes e_i = 0$, so alle m_i.
4. Definiere eine bilineare Abbildung $f_i : M \times F \to M$ durch
$$f_i(m, \sum_j r_j e_j) = r_j m.$$
Diese faktorisiert über $M \otimes F$, d.h. es gibt eine lineare Abbildung $g_i : M \otimes F \to M$ mit
$$g_i(m \otimes (\sum_j r_j e_j)) = r_j m,$$
also wegen $x = 0$:
$$0 = g_i(x) = \sum_j g_i(m_j \otimes e_j) = m_i,$$
woraus die Behauptung folgt. ■

SATZ. *Seien M, N, P R-Moduln. Für das Tensorprodukt gelten folgende Rechenregeln, wobei die Abbildungen kanonisch sind.*

1. $M \otimes N \simeq N \otimes M$.
2. $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P)$.
3. $M \otimes (\oplus_{i \in I} N_i) \simeq \oplus_{i \in I}(M \otimes N_i)$.
4. $R \otimes M \simeq M$.

Beweis: Wir überlassen die Regeln als Übungsaufgabe. Teil 4 folgt auch aus obigem Lemma: Jedes $x \in R \otimes M$ hat eine eindeutige Darstellung $x = 1 \otimes m$. ■

Basiswechsel: Sei $f : A \to B$ ein Ringhomomorphismus. Dann wird B zu einem A-Modul durch die Vorschrift $a \cdot b := f(a)b$. Da B gleichzeitig A-Modul und Ring ist, sagt man auch, B ist eine A-Algebra.

1. Ist N ein B-Modul, so wird durch die Vorschrift
$$A \times N \to N, \quad (a, n) \mapsto f(a)n$$
N zu einem A-Modul. Man spricht von Einschränkung von Skalaren.
2. Ist M ein A-Modul, so sei $M_B := B \otimes_A M$. Durch
$$B \times M_B \to M_B, \quad (b, b' \otimes m) \mapsto (bb') \otimes m$$
wird M_B zu einem B-Modul. Man spricht von Erweiterung von Skalaren.

Beispiel: Ist $\mathfrak{a}$ ein Ideal in R, so hat man einen Ringhomomorphismus $f : R \to R/\mathfrak{a}$. Ist M ein R-Modul, so $R/\mathfrak{a} \otimes M$ ein $R/\mathfrak{a}$-Modul. Wie sieht er aus?

LEMMA. *Sei M ein R-Modul und $\mathfrak{a}$ ein Ideal in R. Dann gilt:*
$$R/\mathfrak{a} \otimes_R M \simeq M/\mathfrak{a}M.$$

Beweis: Die Abbildung $f : R/\mathfrak{a} \times M \to M/\mathfrak{a}M, (\overline{r}, m) \mapsto rm$ ist wohldefiniert und bilinear, faktorisiert also übers Tensorprodukt: $g : R/\mathfrak{a} \otimes M \to M/\mathfrak{a}M$ mit $g(\overline{r} \otimes m) = \overline{rm}$. Natürlich ist g surjektiv. Sei $x = \sum_i \overline{r_i} \otimes m_i \in kern(g)$. Wegen
$$x = \sum_i \overline{1} \otimes r_i m_i = \overline{1} \otimes (\sum_i r_i m_i)$$
können wir $x = \overline{1} \otimes m$ anschreiben. Wegen $g(x) = 0$ ist $m \in \mathfrak{a}M$, also $m = \sum a_j n_j$ mit $a_j \in \mathfrak{a}$ und $n_j \in M$, also
$$x = \sum_j \overline{a_j} \otimes n_j = 0,$$
was wir zeigen wollten. ■

Wir geben eine einfache Anwendung:

SATZ. *Für natürliche Zahlen m, n gilt:*

$$R^m \simeq R^n \quad \Longleftrightarrow \quad m = n.$$

Beweis: $\leftarrow$ ist klar. Sei $R^m \simeq R^n$. Wähle ein maximales Ideal $\mathfrak{m}$ in R. Dann gilt natürlich auch $R/\mathfrak{m} \otimes R^m \simeq R/\mathfrak{m} \otimes R^n$, und mit den Eigenschaften des Tensorprodukts: $(R/\mathfrak{m})^m \simeq (R/\mathfrak{m})^n$. Nun ist aber $R/\mathfrak{m}$ ein Körper, also folgt für Vektorräume über Körpern: $m = n$. ■

Bei Basiswechsel ist noch folgender Satz wichtig:

SATZ. *Sei B eine A-Algebra und M und N A-Moduln. Dann gilt:*

$$B \otimes_A (M \otimes_A N) \simeq (B \otimes_A M) \otimes_B (B \otimes_A N).$$

Beweis: ■

Bruchrechnung für Moduln: Sei M ein R-Modul und S eine multiplikative Teilmenge von R. Wir definieren auf $M \times S$ eine Äquivalenzrelation durch

$$(m, s) \sim (m', s') \iff (s'm - sm')t = 0 \text{ für ein } t \in S.$$

Die Äquivalenzklasse von (m, s) wird mit $\frac{m}{s}$ bezeichnet, die Menge der Äquivalenzklassen mit $S^{-1}M$. Durch

$$\frac{a}{t} \cdot \frac{m}{s} = \frac{am}{st}, \quad \frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'}$$

wird $S^{-1}M$ zu einem $S^{-1}M$-Modul.
Ist $\mathfrak{p}$ ein Primideal und $S = R \setminus \mathfrak{p}$, so schreibt man $M_\mathfrak{p}$ statt $S^{-1}M$ und nennt dies die Lokalisierung von M in $\mathfrak{p}$.

SATZ. *Ist S ein multiplikative Teilmenge von R und M ein R-Modul, so gilt (als $S^{-1}R$-Moduln)*

$$S^{-1}R \otimes_R M \simeq S^{-1}M.$$

Beweis: Die R-bilineare Abbildung $S^{-1}R \times M \to S^{-1}M$ mit $(\frac{a}{s}, m) \mapsto \frac{am}{s}$ ist wohldefiniert und faktorisiert übers Tensorprodukt:

$$f : S^{-1}R \otimes M \to S^{-1}M, \quad f(\frac{a}{s} \otimes m) = \frac{am}{s}.$$

(Natürlich ist f auch $S^{-1}R$-linear.) f ist surjektiv. Sei

$$x = \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes m_i \in kern(f).$$

Ist $s = s_1 s_2 \dots s_n$, so läßt sich in der üblichen Weise x auch schreiben als $x = \frac{1}{s} \otimes m$. Nun gilt in $S^{-1}M$: $\frac{m}{s} = 0$, d.h. es gibt $t \in S$ mit $mt = 0$. Damit wird

$$x = \frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = 0,$$

also ist f auch injektiv. ■

SATZ. *Die Operation S^{-1} ist exakt, d.h. ist $M' \to M \to M''$ exakt in M, so ist $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ exakt in $S^{-1}M$.*

Beweis: Sei $f : M' \to M$ und $g : M \to M''$. Für $\frac{m}{s} \in S^{-1}M$ gilt dann:

$$\begin{aligned}
\frac{m}{s} \in Kern(S^{-1}g) &\iff \frac{g(m)}{s} = 0 \\
&\iff tg(m) = 0 \text{ für ein } t \in S \\
&\iff g(tm) = 0 \text{ für ein } t \in S \\
&\iff tm = f(m') \text{ für ein t} \in S \text{ und ein } m' \in M' \\
&\iff \frac{m}{s} = \frac{f(m')}{st} \in Bild(S^{-1}f). \blacksquare
\end{aligned}$$

FOLGERUNG. *Ist $M \subseteq N$ Untermodul von N, so $S^{-1}M$ Untermodul von $S^{-1}N$.*

Beweis: $M \subseteq N$ induziert die exakte Sequenz $0 \to M \to N$. Nach dem Satz ist auch $0 \to S^{-1}M \to S^{-1}N$ exakt, also kann $S^{-1}M$ als Untermodul von $S^{-1}N$ aufgefaßt werden. ■

SATZ. *Sei S multiplikative Teilmenge eines Ringes R.*

1. *Sind N und P Untermoduln von M, so gilt*
$$S^{-1}(N+P) = S^{-1}N + S^{-1}P, \quad S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P, \quad S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N.$$
2. *Sind M und N R-Moduln, so liefert $f(\frac{m}{s} \otimes \frac{n}{t}) = \frac{m \otimes}{st}$ einen Isomorphismus*
$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \simeq S^{-1}(M \otimes_R N).$$

Beweis: als Übung. ■

Exakte Sequenzen und Tensorprodukt: Wir haben bereits in einem Beispiel gesehen, daß $M' \subseteq M$ noch nicht $M' \otimes N \subseteq M \otimes N$ impliziert. Anders ausgedrückt: Aus der Exaktheit von $0 \to M' \to M$ folgt nicht die Exaktheit von $0 \to M' \otimes N \to M \otimes N$. Dagegen gilt aber:

SATZ. *Ist $M' \to M \to M'' \to 0$ exakt und N ein R-Modul, so ist auch $M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ exakt. (Das Tensorprodukt ist rechtsexakt.)*

Beweis: Sei $f : M' \to M$ und $g : M \to M''$ gegeben mit $M' \to M \to M'' \to 0$ exakt. Man erhält dann induzierte Abbildungen $f_1 : M' \otimes N \to M \otimes N$ und $g_1 : M \otimes N \to M'' \otimes N$. Offensichtlich ist g_1 surjektiv und $g_1 \circ f_1 = 0$. Wir müssen also nur noch $Bild(f_1) = Kern(g_1)$ zeigen. Äquivalent dazu ist, daß die induzierte Abbildung
$$g_2 : M \otimes N/f_1(M' \otimes N) \to M'' \otimes N$$
injektiv ist. Wir definieren nun $h : M'' \times N \to M \otimes N/Bild(f_1)$ wie folgt: Sei $m'' \in M$ und $n \in N$ gegeben. Wähle $m \in M$ mit $g(m) = m''$. Setze $h(m'', n) = m \otimes n \bmod Bild(f_1)$. Dies ist wohldefiniert, denn gilt $g(m_0) = m''$, so ist $g(m_0 - m) = 0$, also $m_0 - m \in Kern(g) = Bild(f)$, d.h. es gibt $m' \in M'$ mit $m_0 = m + f(m')$. Damit gilt:
$$m_0 \otimes n = m \otimes n + f(m') \otimes n \equiv m \otimes n \bmod Bild(f_1).$$
Damit folgt sofort die Bilinearität von h, denn mit $g(m_1) = m_1'', g(m_2) = m_2''$ gilt auch $g(m_1 + m_2) = m_1'' + m_2''$. Also erhält man eine induzierte Abbildung
$$h_1 : M'' \otimes N \to M \otimes N/Bild(f_1).$$
Die zusammengesetzte Abbildung
$$g_2 \circ h_1 : M'' \otimes N \to M \otimes N/Bild(f_1) \to M'' \otimes N$$
ist offensichtlich die Identität, also ist g_2 injektiv, was noch zu zeigen war. ■

DEFINITION. Ein R-Modul F heißt flach, wenn für alle R-Moduln M' und M gilt:
$$0 \to M' \to M \to 0 \to M' \otimes F \to M \otimes F.$$

Zusammen mit dem vorangeganenen Satz folgt, daß Tensorieren einer kurzen exakten Sequenz mit einem flachen Modul F wieder eine exakte Sequenz liefert. Es gilt aber sogar mehr:

SATZ. *Ist F ein flacher Modul und $M' \to M \to M''$ exakt, so ist auch $M' \otimes F \to M \otimes F \to M'' \otimes F$ exakt.*

Beweis: Sei $f : M' \to M$ und $g : M \to M''$. Die Exaktheit liefert drei exakte Sequenzen:
$$M' \to Bild(f) \to 0, \quad 0 \to Bild(f) \to M \to Bild(g) \to 0, \quad 0 \to Bild(g) \to M''.$$
Tensorieren mit F erhält die Exaktheit. Dann setzt man wieder zusammen und erhält die Behauptung. ■

SATZ. *Sei R ein Ring.*

1. *Jeder freie R-Modul F ist flach.*
2. *Ist S eine multiplikative Teilmenge von R, so ist $S^{-1}R$ ein flacher R-Modul.*

Beweis: Sei $F = \oplus_{i\in I} R$. Ist $0 \to M' \to M$ exakt, so auch $0 \to M' \otimes R \to M \otimes R$, woraus man durch Aufaddieren erhält $0 \to \oplus_{i\in I} M' \otimes R \to \oplus_{i\in I} M \otimes R$, also $0 \to M' \otimes F \to M \otimes F$. Die zweite Behauptung kennen wir bereits. ■

Ein $m \in M$ heißt Torsionselement, wenn es $a \in R$ gibt mit $am = 0$ aber $a \neq 0, m \neq 0$. Ein Modul hat Torsion, wenn er Torsionselemente besitzt.

Gegenbeispiel: Sei R ein Integritätsring und M ein R-Modul mit Torsion. Dann ist M nicht flach. Denn ist $m \in M$ mit $m \neq 0$ und $am = 0$ mit $a \neq 0$, so ist $f : R \to R, x \mapsto ax$ injektiv, nicht jedoch die induzierte Abbildung $M \to M, n \mapsto an$.

Für einen Hauptidealring ist das auch das einzige Hindernis.

SATZ. *Sei R ein Hauptidealring. Dann gilt für einen R-Modul M:*

$$M \text{ flach} \quad \Longleftrightarrow \quad M \text{ torsionsfrei.}$$

Wir geben dafür im Augenblick keinen Beweis. Ist M endlich erzeugt, so ist der Beweis einfach. (Übungsaufgabe.)
Im allgemeinen reicht aber auch *torsionsfrei* nicht aus, um Flachheit zu haben.

Beispiel: Sei k ein Körper und $R = k[x, y]$. Das Ideal $\mathfrak{m} = (x, y)$ ist ein torsionsfreier R-Modul, aber nicht flach. Dazu betrachten wir die Inklusion $f : \mathfrak{m} \to R$. Durch Tensorieren mit $\mathfrak{m}$ entsteht $g : \mathfrak{m} \otimes \mathfrak{m} \to \mathfrak{m}$. Nun ist $a = x \otimes y - y \otimes x \in \mathfrak{m} \otimes \mathfrak{m}$ mit $g(a) = 0$. Wir zeigen, daß $a \neq 0$ gilt.
Definiere eine R-bilineare Abbildung $\phi : \mathfrak{m} \times \mathfrak{m} \to R/\mathfrak{m} = k$ durch

$$\phi(f(x, y), g(x, y)) = \frac{f(t, t)}{t}|_{t=0} \cdot \frac{g(t, -t)}{t}|_{t=0}.$$

(Bilinearität als Übungsaufgabe.) Dies induziert eine Abbildung des Tensorprodukts: $\psi : \mathfrak{m} \otimes_R \mathfrak{m} \to R/\mathfrak{m}$. Nun ist

$$\psi(x \otimes y) = -1 \text{ und } \psi(y \otimes x) = 1,$$

also $\psi(a) = -2 \neq 0$ und damit $a \neq 0$, was wir zeigen wollten.

Zum Abschluß noch ein Satz für die lokale Situation:

SATZ. *Sei $(R, \mathfrak{m})$ ein lokaler Ring und M ein endlich erzeugter R-Modul. Dann gilt:*

$$M \text{ flach} \quad \Longleftrightarrow \quad M \text{ frei.}$$

Beweis: Sei M ein endlich erzeugter flacher R-Modul.

1. Wir zeigen zunächst: Sind $x_1, \ldots, x_n \in M$ linear unabhängig modulo $\mathfrak{m}M$, dann auch in M.
   Beweis: durch Induktion nach n. Da der Induktionsanfang $n = 1$ implizit in den weiteren Überlegungen enthalten ist, führen wir ihn nicht explizit aus. Seien jetzt $x_1, \ldots, x_n \in M$ linear unabhängig modulo $\mathfrak{m}M$. Sei $a_1x_1 + \cdots + a_nx_n = 0$. Betrachte die lineare Abbildung $f : R^n \to R$ mit $f(r_1, \ldots, r_n) = \sum a_i r_i$. Sei $L \subseteq R^n$ der Kern von f. Die exakte Sequenz $0 \to L \to R^n \to R$ bleibt nach Tensorieren mit M exakt: $0 \to L \otimes M \to M^n \to M$, wegen $\sum a_i x_i = 0$ gibt es also $b_{ij} \in R, y_j \in M$ mit
   $$\sum_i a_i b_{ij} = 0, \quad x_i = \sum_j b_{ij} y_j.$$
   Wegen $x_1 \notin \mathfrak{m}M$ sind nicht alle b_{1j} in $\mathfrak{m}$. O.E. $b_{11} \notin \mathfrak{m}$. Also ist $b_{11} \in R^\times$. Aus $\sum_i a_i b_{i1} = 0$ folgt dann eine Darstellung $a_1 = c_2a_2 + \cdots + c_na_n$. Damit gilt:
   $$0 = a_2(x_2 + c_2x_1) + \cdots + a_n(x_n + c_nx_1) = 0.$$
   Da natürlich auch $x_2 + c_2x_1, \ldots, x_n + c_nx_1$ linear unabhängig modulo $\mathfrak{m}M$ sind, folgt nach Induktionsannahme: $a_2 = \cdots = a_n = 0$, also auch $a_1 = 0$. Dies war behauptet.
2. Wähle jetzt $x_1, \ldots, x_n \in M$ so, daß sie eine Basis modulo $\mathfrak{m}M$ bilden. Nach Nakayama gilt dann $M = Rx_1 + \cdots + Rx_n$ und nach dem eben gezeigten sind $x_1, \ldots, x_n$ linear unabhängig. Also ist M ein freier Modul. ■

Anhang: Noethersche Moduln

Es kann sein, daß ein A-Modul M endlich erzeugt ist, M aber einen Untermodul M' enthält, der nicht endlich erzeugt ist.

Beispiel: $A = k[x_1, x_2, x_3, \dots$ und $M = A$, $M' = (x_1, x_2, x_3, \dots)$.

DEFINITION. Ein A-Modul M heißt noethersch, wenn eine der äquivalenten Bedingungen erfüllt ist:

1. Jeder Untermodul von M ist endlich erzeugt.
2. Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element.
3. Jede Kette $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ von Untermoduln von M wird stationär, d.h. es gibt ein n mit $M_n = M_{n+1} = \dots$.

Die Äquivalenz ist einfach zu zeigen.

SATZ. *Untermoduln und Faktormoduln eines noetherschen Moduls sind noethersch. Anders ausgedrückt: Ist M ein noetherscher Modul und N ein Untermodul, so sind auch N und M/N noethersch.*

Beweis: klar. ■

SATZ. *Ist M ein Modul und N ein Untermodul derart, daß N und M/N noethersch sind, dann ist auch M noethersch.*

Beweis: Sei $\phi : M \to M/N$ die kanonische Abbildung. Sei U ein Untermodul von M. Da M/N noethersch ist, gibt es $u_1, \dots, u_m \in M$ mit $\phi(U) = A\phi(u_1) + \dots + A\phi(u_m)$. Da N noethersch ist, gibt es $v_1, \dots, v_n \in U \cap N$ mit $U \cap N = Av_1 + \dots + Av_n$. Dann folgt schnell $U = Au_1 + \dots + Au_m + Av_1 + \dots + Av_n$, d.h. auch U ist endlich erzeugt. ■

Die letzten beiden Sätze lassen sich auch so zusammenfassen: Für eine exakte Sequenz von A-Moduln $0 \to M' \to M \to M'' \to 0$ gilt:

$$M \text{ noethersch} \iff M' \text{ und } M'' \text{ noethersch.}$$

FOLGERUNG. *Sind $M_1, \dots, M_n$ endlich viele noethersche Moduln, so ist auch $M_1 \oplus \dots \oplus M_n$ noethersch.*

Beweis: Es genügt den Fall $n = 2$ zu zeigen. Dieser folgt aber nach der letzten Bemerkung aus der exakten Sequenz $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$. ■

SATZ. *Ist A ein noetherscher Ring und M ein endlich erzeugter A-Modul, so ist auch M noethersch.*

Beweis: Ist $M = Ax_1 + \dots + Ax_n$, so ist $\phi : A^n \to M, (a_1, \dots, a_n) \mapsto a_1x_1 + \dots + a_nx_n$ surjektiv, M also Faktormodul des noetherschen Moduls $A^n = A \oplus \dots \oplus A$, also selbst noethersch. ■

KAPITEL 6

Das Spektrum eines Ringes

Wir fangen gleich mit der Definition an:

DEFINITION. Für einen kommutativen Ring R heißt

$$Spec(R) = \{\mathfrak{p} : \mathfrak{p} \text{ Primideal in } R\}$$

das Spektrum von R. Die Elemente des Spektrums werden auch als Punkte bezeichnet.

Beispiele:

1. Sei k ein Körper. Dann gilt $Spec(k) = \{(0)\}$.
2. Was ist $Spec(k[x])$ für einen Körper k? Jedes Ideal in $k[x]$ ist Hauptideal, also gilt:
$$Spec(k[x]) = \{0\} \cup \{(p(x)) : p(x) \text{ normiert und irreduzibel}\}.$$
3. Ist k algebraisch abgeschlossen, so gilt:
$$Spec(k[x]) = \{0\} \cup \{(x-a) : a \in k\},$$
die Punkte des Spektrums stehen also bis auf (0) in Bijektion zu den Punkten der affinen Geraden k^1.

Beispiel: Sei k algebraisch abgeschlossener Körper und $R = k[x,y]$. Wir wollen $Spec(R)$ bestimmen.

- Natürlich ist (0) ein Primideal.
- Ist $f \neq 0, f \in R$, so ist (f) genau dann Primideal, wenn f irreduzibel ist.
- Sei $\mathfrak{p}$ ein Primideal, das sich nicht von einem Element erzeugen läßt. Durch Elimination sieht man, daß es Polynome $f(x), g(y) \neq 0$ in $\mathfrak{p}$ gibt. Da k algebraisch abgeschlossen ist, gibt es $a, b \in k$ mit $(x-a, y-b) \in \mathfrak{p}$. Nun ist aber $(x-a, y-b)$ maximales Ideal. Also folgt schon $\mathfrak{p} = (x-a, y-b)$.
- Wir haben also
$$Spec(R) = \{(0)\} \cup \{(f) : f \text{ irreduzibel}\} \cup \{(x-a, y-b) : a, b \in k\}.$$
Die maximalen Ideale $(x-a, y-b)$ stehen in Bijektion zu den Punkten der affinen Ebene k^2, die Primideale (f) liefern irreduzible Kurven $f = 0$ in der affinen Ebene k^2. Außerdem gilt: $(f) \subseteq (x-a, y-b) \iff f(a,b) = 0$, d.h. (a,b) liegt auf der Kurve $f = 0$.

Hier bietet sich gleich eine neue Definition an:

DEFINITION. Die Höhe $h(\mathfrak{p})$ eines Primideals $\mathfrak{p} \in Spec(R)$ ist das Supremum aller n, so daß es eine Primidealkette

$$\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$$

gibt. Die Krulldimension $dim(R)$ von R ist $\sup\{h(\mathfrak{p}) : \mathfrak{p} \in Spec(R)\}$.

Beispiele: Sei k algebraisch abgeschlossener Körper.

1. Für $R = k[x]$ hat (0) Höhe 0, die Ideale $(x-a)$ Höhe 1. Der Ring $k[x]$ hat Krulldimension 1.
2. Für $R = k[x,y]$ hat (0) Höhe 0, die Primideale (f) Höhe 1, die maximalen Ideale $(x-a, y-b)$ Höhe 2. Der Ring hat Krulldimension 2.

Sei nun R ein Hauptidealring. (0) ist ein Primideal. (f) ist ein Primideal, wenn f irreduzibel ist. Sind f und g irreduzibel mit $(f) \subseteq (g)$, so gilt $g|f$, also $f \sim g$, d.h. $(f) = (g)$. Daraus erhält man sofort:

SATZ. *Ist R Hauptidealring, so gilt*

$$Spec(R) = \{0\} \cup \{(f) : f \text{ irreduzibel}\}.$$

R hat Krulldimension 1.

Beispiel: $Spec(\mathbf{Z}) = \{(0), (2), (3), (5), (7), (11), (13), \dots\}$.

DEFINITION. Für $\mathfrak{p} \in Spec(R)$ sei $\kappa(\mathfrak{p}) = Quot(R/\mathfrak{p})$ der Restklassenkörper im Punkt $\mathfrak{p}$. Für $f \in R$ sei $f(\mathfrak{p})$ (der Wert von f im Punkt $\mathfrak{p}$) das Bild von f unter der kanonischen Abbildung

$$R \to R/\mathfrak{p} \to \kappa(\mathfrak{p}).$$

Durch diese Definition kann man $f \in R$ als Funktion auf $Spec(R)$ auffassen. Die Funktionswerte liegen allerdings im allgemeinen in verschiedenen Körpern.

Beispiel: Sei $R = \mathbf{C}[x]$. Für $\mathfrak{p} = (x - a)$ ist $\kappa(\mathfrak{p}) = \mathbf{C}$. Ist $f \in R$ und schreibt man

$$f = c_0 + c_1(x - a) + c_2(x - a)^2 + \dots,$$

so ist $f \equiv c_0 \bmod \mathfrak{p}$, also c_0 das Bild von f in $\kappa(\mathfrak{p})$: $f(\mathfrak{p}) = c_0 = f(a)$. In diesem Fall stimmt also obige Definition mit dem üblichen Gebrauch überein.

Wir wollen nun eine Topologie auf $Spec(R)$ einführen. Dazu definieren wir:

DEFINITION. Für eine Teilmenge $S \subseteq R$ sei

$$V(S) = \{\mathfrak{p} \in Spec(R) : S \subseteq \mathfrak{p}\}.$$

LEMMA. *Es gelten folgende Eigenschaften:*

1. *Ist (S) das von $S \subseteq R$ erzeugte Ideal, so ist $V((S)) = V(S)$.*
2. *$S_1 \subseteq S_2$ impliziert $V(S_1) \supseteq V(S_2)$.*
3. *$V(S) = \emptyset \iff (S) = R$.*
4. *$V(\cup_{i\in I} S_i) = \cap_{i\in I} V(S_i)$ für jede Familie von Teilmengen S_i.*
5. *$V(\sum_{i\in I} \mathfrak{a}_i) = \cap_{i\in I} V(\mathfrak{a}_i)$ für jede Familie von Idealen $\mathfrak{a}_i$.*
6. *$V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ für Ideale $\mathfrak{a}$ und $\mathfrak{b}$.*

Beweis: Bis auf die letzte Eigenschaft ist alles unmittelbar klar.
$\supseteq$: Wegen $\mathfrak{a} \supseteq \mathfrak{a}\cap\mathfrak{b}$ gilt nach 2. $V(\mathfrak{a}) \subseteq V(\mathfrak{a}\cap\mathfrak{b})$, analog $V(\mathfrak{b}) \subseteq V(\mathfrak{a}\cap\mathfrak{b})$, also auch $V(\mathfrak{a})\cup V(\mathfrak{b}) \subseteq V(\mathfrak{a}\cap\mathfrak{b})$.
$\subseteq$: Angenommen, diese Aussage wäre falsch. Dann gäbe es ein Primideal $\mathfrak{p}$ mit $\mathfrak{a}\cap\mathfrak{b} \subseteq \mathfrak{p}$, aber $\mathfrak{a} \not\subseteq \mathfrak{p}$ und $\mathfrak{b} \not\subseteq \mathfrak{p}$. Wähle $a \in \mathfrak{a} \setminus \mathfrak{p}$ und $b \in \mathfrak{b} \setminus \mathfrak{p}$. Dann ist $ab \in \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, also müßte $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ gelten: ein Widerspruch zur Annahme. ■

Was wir eben bewiesen haben, kann man auch eigenständig formulieren:

FOLGERUNG. *Ist $\mathfrak{p}$ ein Primideal und $\mathfrak{a}, \mathfrak{b}$ Ideale, so gilt:*

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ oder } \mathfrak{b} \subseteq \mathfrak{p}.$$

Analog:

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ oder } \mathfrak{b} \subseteq \mathfrak{p}.$$

Obige Eigenschaften von V zeigen, daß die Teilmengen $V(S)$ die Axiome der abgeschlossenen Teilmengen einer Topologie erfüllen. Wir denken uns $Spec(R)$ mit dieser Topologie versehen. Sie heißt Zariski-Topologie.

Beispiel: Sei R ein Hauptidealring und $\mathbf{P}$ ein Repräsentantensystem der irreduziblen Elemente, also

$$Spec(R) = \{0\} \cup \{(p) : p \in \mathbf{P}\}.$$

Sei $\mathfrak{a}$ ein Ideal in R. Ist $\mathfrak{a} = 0$, so gilt $V(\mathfrak{a}) = Spec(R)$. Ist $\mathfrak{a} \neq 0$, $\mathfrak{a} = (f)$ mit $f \neq 0$, so sei $f = u \cdot p_1^{n_1} \dots p_r^{n_r}$ mit u Einheit und $n_i \geq 1$. Dann ist

$$V(\mathfrak{a}) = \{(p_1), \dots, (p_r)\}.$$

Man sieht so schnell: $X \subseteq Spec(R)$ mit $0 \notin X$ ist genau dann abgeschlossen, wenn X endlich ist.

Beispiel: Sei $R = \mathbf{C}[x, y]$. Sind $a, b \in \mathbf{C}$, so ist $(x - a, y - b)$ maximales Ideal, also

$$V((x - a, y - b) = \{(x - a, y - b)\}.$$

Ist $f(x, y)$ ein irreduzibles Polynom, so ist

$$V(f) = \{(f)\} \cup \{(x - a, y - b) : f(a, b) = 0\}.$$

Wir wollen nun untersuchen, wann $V(\mathfrak{a}) = V(\mathfrak{b})$ gilt. Dazu brauchen wir noch eine Idealkonstruktion:

DEFINITION. Für ein Ideal $\mathfrak{a}$ heißt

$$\sqrt{\mathfrak{a}} = \{f \in R : f^n \in \mathfrak{a} \text{ für ein } n \geq 1\}$$

das Radikalideal von $\mathfrak{a}$. Für $\mathfrak{a} = 0$ besteht $\sqrt{0}$ aus den nilpotenten Elementen und heißt Nilradikal von R. Bezeichnung $nil(R)$.

Wir müssen noch zeigen, daß $\sqrt{\mathfrak{a}}$ wirklich ein Ideal ist. Seien $f, g \in \sqrt{\mathfrak{a}}$, o.E. $f^n, g^n \in \mathfrak{a}$. Dann gilt

$$(f + g)^{2n} = \sum_{i=1}^{2n} \binom{2n}{i} f^i g^{2n-i} \in \mathfrak{a},$$

also $f + g \in \sqrt{\mathfrak{a}}$, was die Behauptung zeigt.

Natürlich gilt $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, also

$$V(\sqrt{\mathfrak{a}}) \subseteq V(\mathfrak{a}).$$

Ist nun $\mathfrak{p}$ ein Primideal mit $\mathfrak{a} \subseteq \mathfrak{p}$, so gilt auch $\sqrt{\mathfrak{a}} \subseteq \mathfrak{p}$, denn ist $f \in \sqrt{\mathfrak{a}}$, so gilt für ein n die Aussage $f^n \in \mathfrak{a} \subseteq \mathfrak{p}$, also auch $f \in \mathfrak{p}$. Folglich:

$$V(\mathfrak{a}) \subseteq V(\sqrt{\mathfrak{a}}).$$

Damit haben wir bewiesen:

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

Wir wollen nun noch $\sqrt{\mathfrak{a}}$ genauer bestimmen.

LEMMA. *Sei S eine multiplikative Teilmenge in R, $\mathfrak{a}$ ein Ideal mit $S \cap \mathfrak{a} = \emptyset$. Dann gibt es ein Primideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$ und $S \cap \mathfrak{p} = \emptyset$.*

Beweis: Sei $M = \{\mathfrak{b} : \mathfrak{a} \subseteq \mathfrak{b}, \mathfrak{b} \cap S = \emptyset\}$. Dann ist M nicht leer und durch Inklusion geordnet. Jede Kette $\{\mathfrak{b}_i : i \in I\}$ in M besitzt ein maximales Element in M, nämlich $\cup_{i \in I} \mathfrak{b}_i$. Nach dem Zornschen Lemma gibt es maximale Elemente in M. Sei $\mathfrak{p}$ ein solches. Seien $f, g \in R$ mit $f, g \notin \mathfrak{p}$. Dann gilt $\mathfrak{p} + (f), \mathfrak{p} + (g) \notin M$, also gibt es $s, t \in S$ und $a, b \in R$, $p, q \in \mathfrak{p}$ mit

$$p + af = s, \quad q + bg = t,$$

und somit $st = pq + pbg + afq + abfg \in S$. Dann ist $abfg \notin \mathfrak{p}$, also auch $fg \notin \mathfrak{p}$, woraus folgt, daß $\mathfrak{p}$ ein Primideal ist. ■

FOLGERUNG. *Für ein Ideal $\mathfrak{a}$ gilt:*

$$\sqrt{\mathfrak{a}} = \cap\{\mathfrak{p} \in Spec(R) : \mathfrak{a} \subseteq \mathfrak{p}\} = \cap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}.$$

Beweis: $\subseteq$: Klar wegen $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.
$\supseteq$: Sei $f \in \cap V(\mathfrak{a})$, aber $f \notin \sqrt{\mathfrak{a}}$. Definiere $S = \{1, f, f^2, f^3, \dots\}$. Dann ist S eine multiplikative Teilmenge mit $S \cap \mathfrak{a} = \emptyset$. Also gibt es ein Primideal $\mathfrak{p}$ mit $S \cap \mathfrak{p} = \emptyset$ und $\mathfrak{a} \subseteq \mathfrak{p}$. Dann wäre aber $f \notin \mathfrak{p}$: ein Widerspruch. ■

FOLGERUNG. $V(\mathfrak{a}) = V(\mathfrak{b}) \iff \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$.

FOLGERUNG. *Es gibt eine Bijektion zwischen den Zariski-abgeschlossenen Teilmengen von $Spec(R)$ und den Radikalidealen von R, d.h. den Idealen $\mathfrak{a}$ mit $\sqrt{\mathfrak{a}} = \mathfrak{a}$.*

Beweis: Jede abgeschlossene Menge Y hat die Gestalt $Y = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ und außerdem gilt

$$\sqrt{\mathfrak{a}} = \cap\{\mathfrak{p} \in Y\}.\blacksquare$$

Wir wollen nun spezielle offene Teilmengen von $X = Spec(R)$ betrachten. Für ein $f \in R$ gilt:

$$V(f) = \{\mathfrak{p} \in Spec(R) : f \in \mathfrak{p}\} = \{\mathfrak{p} \in Spec(R) : f(\mathfrak{p}) = 0\}.$$

Wir definieren die offenen Menge

$$D(f) = X \setminus V(f) = \{\mathfrak{p} : f(\mathfrak{p}) \neq 0\}.$$

Eigenschaften:

1. Sei $U \subseteq X$ offen, d.h. $U = X \setminus V(\mathfrak{a})$ mit einem Ideal $\mathfrak{a} = (f_i : i \in I)$. Nun gilt: $V(\mathfrak{a}) = V(\sum_{i\in I} Rf_i) = \cap_{i\in I} V(f_i)$, also
$$U = X \setminus \cap_{i\in I} V(f_i) = \cup_{i\in I} D(f_i).$$
Also bilden die $D(f)$'s eine Basis für die offenen Mengen der Topologie.
2. $D(f) = X \iff V(f) = \emptyset \iff f \in R^\times$.
3. $D(f) = \emptyset \iff V(f) = Spec(R) \iff f \in nil(R)$.
4. $D(f) = D(g) \iff V(f) = V(g) \iff \sqrt{(f)} = \sqrt{(g)}$.
5. $D(f) \cap D(g) = X \setminus (V(f) \cup V(g)) = X \setminus V(fg) = D(fg)$.
6. $Spec(R)$ ist (quasi)kompakt.
Beweis: Sei $X = \cup_{i\in I} U_i$ eine Überdeckung durch offene Mengen. Nach 1. können wir (nach Verfeinerung) annehmen $X = \cup_{i\in I} D(f_i)$. Also gilt $\emptyset = \cap V(f_i) = V(\cup Rf_i)$, d.h. $(f_i : i \in I) = R$. Nun ist $1 \in R$, also gibt es eine endliche Summe $1 = \sum_{j=1}^n g_{i_j} f_{i_j}$. Damit ist
$$X = X \setminus V(1) = X \setminus V(f_{i_1}, \ldots, f_{i_n}) = D(f_{i_1}) \cup \cdots \cup D(f_{i_n}).$$
Daraus folgt die Behauptung.

Für eine Teilmenge $S \subseteq Spec(R)$ sei $\overline{S}$ der Zariski-Abschluß von S, d.h. die kleinste abgeschlossene Menge, die S umfaßt, und

$$I(S) = \{f \in R : f(\mathfrak{p}) = 0 \text{ für alle } \mathfrak{p} \in S\}.$$

Das ist das Ideal, der auf S verschwindenden Funktionen. Dann zeigt man leicht folgenden Satz:

SATZ. *Für ein Ideal $\mathfrak{a}$ und eine Teilmenge $S \subseteq Spec(R)$ gelten:*

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} \quad \textit{und } V(I(S)) = \overline{S}.$$

Beweis: Es gilt:

$$f \in I(V(\mathfrak{a})) \iff f(\mathfrak{p}) = 0 \text{ für alle } \mathfrak{p} \supseteq \mathfrak{a} \iff f \in \cap_{\mathfrak{p}\in V(\mathfrak{a})} \mathfrak{p} = \sqrt{\mathfrak{a}}.$$

Für den zweiten Teil sei $V(\mathfrak{a})$ eine abgeschlossene Menge mit $S \subseteq V(\mathfrak{a})$. Dann folgt $\sqrt{\mathfrak{a}} = I(V(\mathfrak{a})) \subseteq I(S)$ und damit $V(I(S)) \subseteq V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a})$, d.h. $V(I(S))$ ist die kleinste abgeschlossene Menge, die S umfaßt. $\blacksquare$

Sei nun $\mathfrak{p}$ ein Punkt von $Spec(R)$. Dann gilt:

$$\mathfrak{p} \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{p},$$

also ist die kleinste abgeschlossene Menge, die $\mathfrak{p}$ enthält $V(\mathfrak{p})$:

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}).$$

Im allgemeinen sind also die Punkte von $Spec(R)$ nicht abgeschlossen. Ein Punkt $\mathfrak{p}$ ist genau dann abgeschlossen, wenn $\mathfrak{p}$ ein maximales Ideal ist.

Beispiel: In $Spec(\mathbf{Z})$ gilt: $\overline{\{(o)\}} = Spec(\mathbf{Z})$.

DEFINITION. Sei X ein topologischer Raum. Eine nichtleere abgeschlossene Teilmenge $S \subseteq X$ heißt irreduzibel, wenn S sich nicht als Vereinigung von echt kleineren abgeschlossenen Teilmengen schreiben läßt. Ein Punkt x einer abgeschlossenen Teilmenge heißt generischer Punkt von S, wenn $\overline{\{x\}} = S$ gilt.

Hat eine abgeschlossene Teilmenge $S \subseteq X$ einen generischen Punkt x, so ist natürlich S irreduzibel. Für $Spec(R)$ gilt auch die Umkehrung:

SATZ. *Sei $S \subseteq Spec(R)$ eine abgeschlossene und irreduzible Teilmenge. Dann hat S einen generischen Punkt.*

Beweis: Sei $\mathfrak{a} = I(S)$. Wir wollen zunächst zeigen, daß $\mathfrak{a}$ ein Primideal ist. Wegen $S \neq \emptyset$ ist $\mathfrak{a} \neq R$. Sei nun $fg \in \mathfrak{a}$. Dann gilt

$$S = V(\mathfrak{a}) \subseteq V(fg) = V(f) \cup V(g), \text{ also } S = (S \cap V(f)) \cup (S \cap V(g)).$$

Aus der Irreduzibilität von S folgt $S \subseteq V(f)$ oder $S \subseteq V(g)$, d.h. $f \in \mathfrak{a}$ oder $g \in \mathfrak{a}$. Also ist $\mathfrak{a}$ ein Primideal. Damit ist aber

$$S = V(\mathfrak{a}) = \overline{\{\mathfrak{a}\}},$$

woraus die Behauptung folgt. ■

FOLGERUNG. *Die abgeschlossenen irreduziblen Teilmengen von $Spec(R)$ sind genau die Mengen $V(\mathfrak{p})$ mit $\mathfrak{p} \in Spec(R)$.*

Für noethersche Ringe erhalten wir folgenden Zerlegungssatz:

SATZ. *Ist R noethersch, so läßt sich jede abgeschlossene Teilmenge $Y \subseteq Spec(R)$ zerlegen*

$$Y = Y_1 \cup \cdots \cup Y_r,$$

wo die Y_i irreduzible abgeschlossene Mengen sind. Läßt man Y_j's weg, wenn es ein $i \neq j$ gibt mit $Y_j \subseteq Y_i$, so wird die Zerlegung eindeutig. Anders geschrieben: Es gibt Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ mit $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ für $i \neq j$ mit

$$Y = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r) = \overline{\{\mathfrak{p}_1\}} \cup \cdots \cup \overline{\{\mathfrak{p}_r\}}.$$

Beweis: Existenz einer Zerlegung: Jede abgeschlossene Menge hat die Gestalt $V(\mathfrak{a})$. Sei

$$M = \{\mathfrak{a} \text{ Ideal: } V(\mathfrak{a}) \text{ ist nicht endliche Vereinigung von irreduziblen abgeschlossenen Mengen}\}.$$

Wäre $M \neq \emptyset$, so gäbe es ein maximales Element $\mathfrak{a} \in M$. Speziell ist dann $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ nicht irreduzibel, d.h. $V(\mathfrak{a}) = V(\mathfrak{b}) \cup V(\mathfrak{c})$ mit $\mathfrak{b} = \sqrt{\mathfrak{b}}$, $\mathfrak{c} = \sqrt{\mathfrak{c}}$ und $V(\mathfrak{b}) \subset V(\mathfrak{a}), V(\mathfrak{c}) \subset V(\mathfrak{a})$, also $\mathfrak{a} \subset \mathfrak{b}$ und $\mathfrak{a} \subset \mathfrak{c}$. Wegen der Maximalität von $\mathfrak{a}$ liegen $\mathfrak{b}$ und $\mathfrak{c}$ nicht in M, also sind $V(\mathfrak{b})$ und $V(\mathfrak{c})$ endliche Vereinigung von irreduziblen abgeschlossenen Mengen, also auch $V(\mathfrak{a})$: ein Widerspruch. Damit ist $M = \emptyset$ und jedes $V(\mathfrak{a})$ hat die Form

$$V(\mathfrak{a}) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r).$$

Durch Weglassen von $V(\mathfrak{p}_i)$'s, die in einem anderen $V(\mathfrak{p}_j)$ enthalten sind, erhalten man die gewünschte Darstellung.
Eindeutigkeit: Sei

$$V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r) = V(\mathfrak{q}_1) \cup \cdots \cup V(\mathfrak{q}_s)$$

mit $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ für $i \neq j$ und $\mathfrak{q}_i \not\subseteq \mathfrak{q}_j$ für $i \neq j$. Betrachte $\mathfrak{p}_i$. Es ist in der linken Seite enthalten, also auch in der rechten, also gibt es einen Index $f(i)$ mit $\mathfrak{p}_i \in V(\mathfrak{q}_{f(i)}$, d.h. $\mathfrak{q}_{f(i)} \subseteq \mathfrak{p}_i$. Aus Symmetriegründen gibt es auch zu jedem $j = 1, \ldots, s$ einen Index $g(j)$ mit $\mathfrak{p}_{g(j)} \subseteq \mathfrak{q}_j$. Damit gilt

$$\mathfrak{p}_i \supseteq \mathfrak{q}_{f(i)} \supseteq \mathfrak{p}_{g(f(i))},$$

woraus sofort $g \circ f = id$ und $\mathfrak{p}_i = \mathfrak{q}_{f(i)}$ folgt. Analog $f \circ g = id$. Also gilt $r = s$ und die zweite Darstellung entsteht durch Permutation der Indizes. ■

FOLGERUNG. *In einem noetherschen Ring R gibt es nur endlich viele minimale Primideale.*

Beweis: Es ist $Spec(R) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r)$, wobei die $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ genau die minimalen Primideale sind. ■

Morphismen: Ist $f : R \to S$ ein Ringhomomorphismus und $\mathfrak{q} \in Spec(S)$, so ist $f^{-1}\mathfrak{q} \in Spec(R)$. Also erhalten wir eine Abbildung

$$f^* : Spec(S) \to Spec(R), \mathfrak{q} \mapsto f^{-1}(\mathfrak{q}).$$

Beispiele:

1. $\mathbf{Z} \subseteq \mathbf{Q}$ induziert $Spec(\mathbf{Q}) \to Spec(\mathbf{Z}), (0) \mapsto (0)$.
2. Für eine Primzahl p liefert $\mathbf{Z} \to \mathbf{Z}/(p)$ den Morphismus $Spec(\mathbf{Z}/(p)) \to Spec(\mathbf{Z}), (0) \mapsto (p)$.
3. Betrachte $\phi : \mathbf{C}[x] \to \mathbf{C}[x]$ mit $\phi(x) = x^2$. Dies liefert $\phi^*(x-a) = (x-a^2)$.

LEMMA. *Ist $\phi : R \to S$ ein Ringhomomorphismus, so gilt*

$$\phi^{*-1} D(f) = D(\phi(f)).$$

Insbesondere zeigt dies, daß ϕ^* stetig ist.

Beweis: Wir haben

$$\begin{aligned} \mathfrak{q} \in \phi^{*-1} D(f) &\iff \phi^* \mathfrak{q} = \phi^{-1}\mathfrak{q} \in D(f) \iff \\ &\iff f \notin \phi^{-1}\mathfrak{q} \iff \phi(f) \notin \mathfrak{q} \iff \\ &\iff \mathfrak{q} \in D(\phi(f)). \quad \blacksquare \end{aligned}$$

Folgender Satz ist fast klar:

SATZ. 1. *Ist $\mathfrak{a}$ ein Ideal in R, so induziert $R \to R/\mathfrak{a}$ einen Homöomorphismus*

$$Spec(R/\mathfrak{a}) \simeq V(\mathfrak{a}) \subseteq Spec(R).$$

2. *Sei $S \subseteq R$ multiplikativ. Dann induziert $R \to S^{-1}R$ einen Homöomorphismus aufs Bild:*

$$Spec(S^{-1}R) \to \{\mathfrak{p} : S \cap \mathfrak{p} = \emptyset\} \subseteq Spec(R).$$

Das Nilradikal $nil(R)$ eines Ringes R war die Menge der nilpotenten Elemente. Wir haben gezeigt, daß auch gilt: $nil(R) = \cap\{\mathfrak{p} : \mathfrak{p} \in Spec(R)\}$. Ein Ring R heißt reduziert, falls $nil(R) = 0$ ist. Für einen Ring R sei $R_{red} = R/nil(R)$. Dann ist R_{red} reduziert. Da alle Primideale von R das Nilradikal enthalten folgt auch sofort

$$Spec(R) \simeq Spec(R_{red}).$$

Beispiel: Der Ring $R = k[x,y]/(x^2, y^2)$ ist nicht reduziert, da x und y nilpotent sind. Offensichtlich ist dann $nil(R) = (x,y)$, also $R_{red} = k[x,y]/(x,y) \simeq k$. Das Spektrum von R besteht nur aus einem Punkt.

Moduln: Sei M ein R-Modul. Dann heißt das Ideal

$$ann(M) = \{r \in R : rm = 0 \text{ für alle } m \in M\}$$

das Annulator von M. Entsprechend heißt für $x \in M$ das Ideal $ann(x) = \{r \in R : rx = 0\}$ der Annulator von x. Für jedes $\mathfrak{p} \in Spec(R)$ ist $M_\mathfrak{p}$ ein $R_\mathfrak{p}$-Modul. Wir nennen

$$supp(M) = \{\mathfrak{p} \in Spec(R) : M_\mathfrak{p} \neq 0\}$$

den Träger von M.

Beispiel: Sei $\mathfrak{a}$ ein Ideal in R und $M = R/\mathfrak{a}$.

- Ist $\mathfrak{a} \not\subseteq \mathfrak{p}$, so gibt es ein $a \in \mathfrak{a}$ mit $a \notin \mathfrak{p}$, also gilt in $M_\mathfrak{p}$: $\frac{\overline{1}}{1} = \frac{\overline{a}}{a} = 0$, also $M_\mathfrak{p} = 0$.
- Ist $\mathfrak{a} \subseteq \mathfrak{p}$, so ist $\frac{\overline{1}}{1} \neq 0$ in $M_\mathfrak{p}$, denn andernfalls gäbe es $s \notin \mathfrak{p}$ mit $s\overline{1} = 0$ in $R/\mathfrak{a}$, was aber $s \in \mathfrak{a} \subseteq \mathfrak{p}$, also einen Widerspruch lieferte. Damit: $M_\mathfrak{p} \neq 0$.

Damit haben wir bewiesen:

$$supp(R/\mathfrak{a}) = V(\mathfrak{a}).$$

SATZ. *Für einen R-Modul M sind äquivalent:*

1. $M = 0$,
2. $M_\mathfrak{p} = 0$ *für alle* $\mathfrak{p} \in Spec(R)$, *d.h.* $supp(M) = \emptyset$,
3. $M_\mathfrak{m} = 0$ *für alle maximalen Ideale* $\mathfrak{m}$.

Beweis: $1 \Rightarrow 2 \Rightarrow 3$ ist klar. Es gelte nun 3. Angenommen $M \neq 0$. Dann gibt es $x \in M$, $x \neq 0$. Der Annulator $ann(x)$ ist in einem maximalen Ideal $\mathfrak{m}$ enthalten: $ann(x) \subseteq \mathfrak{m}$. Nun ist $\frac{x}{1} = 0$ in $M_\mathfrak{m}$, d.h. es gibt $s \notin \mathfrak{m}$ mit $sx = 0$, also $s \in ann(x) \subseteq \mathfrak{m}$, ein Widerspruch. Also ist doch $M = 0$. $\blacksquare$

SATZ. *Sei $\phi : M \to N$ ein Homomorphismus von R-Moduln. Dann sind folgende Aussagen äquivalent:*

1. *ϕ ist injektiv (surjektiv),*
2. *$\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ ist injektiv (surjektiv) für alle $\mathfrak{p} \in Spec(R)$,*
3. *$\phi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ ist injektiv (surjektiv) für alle maximalen Ideale $\mathfrak{m}$.*

Beweis: Wir zeigen nur die Aussagen für injektiv. Für surjektiv geht alles analog.
$1 \Rightarrow 2$: Ist $0 \to M \to N$ exakt, so auch $0 \to M_\mathfrak{p} \to N_\mathfrak{p}$, d.h. $\phi_\mathfrak{p}$ ist injektiv.
$2 \Rightarrow 3$: klar.
$3 \Rightarrow 1$: Sei $M' = kern(\phi)$, also ist $0 \to M' \to M \to N$ exakt. Dann ist auch $0 \to M'_\mathfrak{m} \to M_\mathfrak{m} \to N_\mathfrak{m}$ exakt, wegen der vorausgesetzten Injektivität von $\phi_\mathfrak{m}$ ist also $M'_\mathfrak{m} = 0$ für alle maximalen Ideale $\mathfrak{m}$ und damit nach dem vorangegangenen Satz $M' = 0$, was wir zeigen wollten. ■

Ganz analog ist auch Flachheit eine lokale Eigenschaft:

SATZ. *Für einen R-Modul F sind äquivalent:*

1. *M ist flach,*
2. *$M_\mathfrak{p}$ ist flacher $R_\mathfrak{p}$-Modul für alle Primideale $\mathfrak{p}$.*
3. *$M_\mathfrak{m}$ ist flacher $R_\mathfrak{m}$-Modul für alle maximalen Ideale $\mathfrak{m}$.*

Beweis: $1 \Rightarrow 2 \Rightarrow 3$ ist wieder einfach. Wir zeigen nur $3 \Rightarrow 1$. Sei also $M \to N$ injektiv. Wir müssen zeigen, daß auch $M \otimes F \to N \otimes F$ injektiv ist. Wir wissen, daß $M_\mathfrak{m} \to N_\mathfrak{m}$ injektiv ist, da $F_\mathfrak{m}$ flacher $R_\mathfrak{m}$-Modul ist, ist also auch $M_\mathfrak{m} \otimes_{R_\mathfrak{m}} F_\mathfrak{m} \to N_\mathfrak{m} \otimes_{R_\mathfrak{m}} F_\mathfrak{m}$ injektiv. Dies ist aber das gleiche wie $(M \otimes_R F)_\mathfrak{m} \to (N \otimes F)_\mathfrak{m}$. Nach dem letzten Satz folgt die Injektivität von $M \otimes F \to N \otimes F$. ■

LEMMA. *Sei M ein endlich erzeugter R-Modul. Gilt dann $M \otimes \kappa(\mathfrak{m}) = M \otimes R/\mathfrak{m} = 0$ für alle maximalen Ideale $\mathfrak{m}$, so gilt auch $M = 0$.*

Beweis: Es gilt $0 = M \otimes R/\mathfrak{m} = M/\mathfrak{m}M$, d.h. $M = \mathfrak{m}M$ für alle maximalen Ideale $\mathfrak{m}$. Lokalisieren in $\mathfrak{m}$ liefert $M_\mathfrak{m} = (\mathfrak{m}R_\mathfrak{m})M_\mathfrak{m}$. Nach dem Nakayama-Lemma folgt $M_\mathfrak{m} = 0$, da auch $M_\mathfrak{m}$ endlich erzeugt ist. Nach einem Satz von eben folgt $M = 0$. ■

Bemerkung: Der Satz stimmt nicht mehr, wenn man *endlich ereugt* wegläßt:

Beispiel: Sei $R = \mathbf{Z}$ und $M = \mathbf{Q}$. Für eine Primzahl p ist dann $\mathbf{Q} \otimes_\mathbf{Z} \mathbf{Z}/(p) = 0$, denn $\frac{a}{b} \otimes c = \frac{a}{pb} \otimes pc = 0$. Aber $\mathbf{Q} \neq 0$.

Wir geben noch eine Eigenschaft von $supp(M)$ an:

SATZ. *Ist M ein endlich erzeugter R-Modul, so gilt*

$$supp(M) = V(ann(M)),$$

insbesondere ist $supp(M)$ in $Spec(R)$ abgeschlossen.

Beweis: Sei $M = Rm_1 + \cdots + Rm_r$. Dann gilt: $\mathfrak{p} \in supp(M)$ genau dann, wenn $M_\mathfrak{p} \neq 0$, d.h. es gibt ein i mit $\frac{m_i}{1} \neq 0$ in $M_\mathfrak{p}$, d.h. es gibt ein i mit $ann(m_i) \cap (R \setminus \mathfrak{p}) = \emptyset$, also $ann(m_i) \subseteq \mathfrak{p}$. Damit

$$supp(M) = \cup_i V(ann(m_i)) = V(\cap ann(m_i)) = V(ann(M)).\blacksquare$$

Beispiel: Obiger Satz wird falsch, wenn man *endlich erzeugt* wegläßt. Man nehme $R = \mathbf{Z}$ und

$$M = \oplus_{n \geq 2} \mathbf{Z}/(n).$$

Ist p eine Primzahl, so ist $\mathbf{Z}_{(p)} \otimes \mathbf{Z}/(p) = \mathbf{Z}/(p) \neq 0$, also $M_{(p)} \neq 0$, d.h. $(p) \in supp(M)$. Andererseits ist $\mathbf{Z}_{(0)} \otimes M = \mathbf{Q} \otimes M = 0$, also $(0) \notin supp(M)$. Damit gilt $supp(M) = Spec(\mathbf{Z}) \setminus \{(0)\}$. Der Träger $supp(M)$ ist also weder offen noch abgeschlossen.

KAPITEL 7

Ganze Ringerweiterungen und normale Ringe

Sei A ein Unterring des Rings B. Wir sagen auch, B ist eine Ringerweiterung von A. Ein $x \in B$ heißt ganz über A, wenn x eine Gleichung

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} + a_n = 0$$

mit $a_i \in A$ erfüllt. ($x^n + a_1 x^{n-1} + \cdots + a_n$ ist also ein normiertes Polynom.)

Beispiel: Sei $A = \mathbf{Z}$ und $B = \mathbf{C}$. Dann ist $\sqrt{2}$ ganz über $\mathbf{Z}$, denn $\sqrt{2}$ erfüllt die Gleichung $x^2 - 2 = 0$.

Beispiel: Sind K und L Körper mit $K \subseteq L$, so ist $x \in L$ genau dann ganz über K, wenn x algebraisch über K ist.

SATZ. *Sei B eine Ringerweiterung von A und $x \in B$. Dann sind äquivalent:*

1. *x ist ganz über A,*
2. *$A[x]$ ist ein endlich erzeugter A-Modul,*
3. *Es gibt einen Ring C mit $A \subseteq C \subseteq B$, so daß C als A-Modul endlich erzeugt ist und $x \in C$ ist.*

Beweis: $1 \Rightarrow 2$: Sei $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Dann ist

$$x^n = -a_n - \cdots - a_1 x^{n-1} \in A + Ax + \cdots + Ax^{n-1}.$$

Induktiv sieht man schnell: $x^m \in A + Ax + \cdots + Ax^{n-1}$ für alle $m \geq 1$. Also gilt $A[x] = A + Ax + \cdots + Ax^{n-1}$, d.h. $A[x]$ ist ein endlich erzeugter A-Modul.
$2 \Rightarrow 3$: Wähle $C = A[x]$.
$3 \Rightarrow 1$: Sei $C = Ac_1 + \cdots + Ac_r$, und o.E. $c_1 = 1$. Dann ist $xc_i = \sum a_{ij} c_j$. Wie früher sieht man $det(x\delta_{ij} - a_{ij}) \cdot c_k = 0$, woraus man sofort eine normierte Gleichung von x über A erhält. ■

FOLGERUNG. *Sind $x_1, \ldots, x_n \in B$ ganz über A, so ist der Ring $A[x_1, \ldots, x_n]$ ein endlich erzeugter A-Modul.*

Beweis: durch Induktion nach n. Der Fall $n = 1$ steht im Satz. Wir nehmen nun an, daß der Ring $A' = A[x_1, \ldots, x_{n-1}]$ ein endlich erzeugter A-Modul ist, also $A' = Ay_1 + \cdots + Ay_r$. Da x_n ganz über A ist, ist x_n auch ganz über A', also nach dem Satz $A'[x_n] = A'z_1 + \cdots + A'z_s$. Damit folgt

$$A[x_1, \ldots, x_n] = A'[x_n] = \sum Ay_i z_j,$$

die Behauptung. ■

FOLGERUNG. *Die Menge*

$$C = \{x \in B : x \text{ ist ganz über } A\}$$

ist ein Teilring von B.

Beweis: Zunächst ist $A \subseteq C$. Seien $x, y \in C$. Nach der letzten Folgerung ist $A[x, y]$ ein endlich erzeugter A-Modul. Wegen $x + y, x \cdot y \in A[x, y]$ sind dann auch $x + y$ und $x \cdot y$ ganz über A, d.h. $x + y, xy \in C$. ■

Der Ring C heißt der ganze Abschluß von A in B. Gilt $C = A$, so sagt man, A ist ganz abgeschlossen in B. Ist $C = B$, so sagt man, B ist ganz über A, oder B ist eine ganze Ringerweiterung von A.

Bemerkung: Ist $A \subseteq B$ eine Ringerweiterung und B endlich erzeugter A-Modul, so ist B insbesondere ganz über A. Man sagt, $Spec(B) \to Spec(A)$ ist ein endlicher Morphismus.

Beispiel: Sei $d \in \mathbf{Z}$, $d \neq 1$, d quadratfrei und $K = \mathbf{Q}(\sqrt{d})$. Der ganze Abschluß von $\mathbf{Z}$ in K ist dann $\mathbf{Z}[\sqrt{d}]$ für $d \equiv 2, 3 \bmod 4$ und $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ für $d \equiv 1 \bmod 4$.

SATZ. *Ist B ganz über A, C ganz über B, so ist C ganz über A.*

Beweis: Sei $x \in C$. Dann gibt es $b_1, \ldots, b_n \in B$ mit $x^n + b_1 x^{n-1} + \cdots + b_n = 0$. Der Ring $B' = A[b_1, \ldots, b_n]$ ist endlich erzeugter A-Modul. Da x ganz über B' ist, ist $B'[x]$ endlich erzeugter B'-Modul. Wie zuvor folgt, daß $B'[x]$ endlich erzeugter A-Modul ist. Also ist x ganz über A. ■

FOLGERUNG. *Ist $A \subseteq B$ eine Ringerweiterung und ist C der ganze Abschluß von A in B, so ist C ganz abgeschlossen in B.*

SATZ. *Sei B ganz über A.*

1. *Ist $\mathfrak{b}$ ein Ideal in B und $\mathfrak{a} = A \cap \mathfrak{b}$, so ist $B/\mathfrak{b}$ ganz über $A/\mathfrak{a}$.*
2. *Ist S eine multiplikative Teilmenge von A, so ist $S^{-1}B$ ganz über $S^{-1}A$.*

Beweis: 1. Klar.
2. Sei $\frac{b}{s} \in S^{-1}B$. Da b ganz über A ist, gibt es $a_1, \ldots, a_n \in A$ mit

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0,$$

was sofort

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

liefert, d.h. $\frac{b}{s}$ ist ganz über $S^{-1}A$. ■

SATZ. *Sei $A \subseteq B$ eine ganze Erweiterung von Integritätsringen. Genau dann ist B ein Körper, wenn A ein Körper ist.*

Beweis: Sei A ein Körper und $b \in B$, $b \neq 0$. Dann gibt es $a_1, \ldots, a_n \in A$ mit

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0,$$

wobei wir o.E. $a_n \neq 0$ voraussetzen können. Damit gilt

$$b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = -a_n \in A^\times \subseteq B^\times,$$

also ist auch $b \in B^\times$. Da $b \in B$ beliebig war, muß B ein Körper sein.
Sei nun B ein Körper und $a \in A$, $a \neq 0$. Dann ist $a^{-1} \in B$, also ganz über A, d.h. es gibt $a_1, \ldots, a_n \in A$ mit

$$a^{-n} + a_1 a^{-n+1} + \cdots + a_n = 0,$$

also

$$a^{-1} = -a_1 - a_2 a - \cdots - a_n a^{n-1} \in A.$$

Also ist A ein Körper. ■

Bemerkung: Die Voraussetzung, daß B ein Integritätsring ist, ist wichtig. So ist z.B. $\mathbf{Q} \subseteq \mathbf{Q} \times \mathbf{Q}, x \mapsto (x, x)$ eine ganze Ringerweiterung, denn (a, b) genügt der Gleichung $x^2 - (a+b)x + ab = 0$, aber $\mathbf{Q} \times \mathbf{Q}$ ist kein Integritätsring.

FOLGERUNG. *Sei $A \subseteq B$ eine ganze Ringerweiterung, $\mathfrak{q} \subseteq B$ ein Primideal und $\mathfrak{p} = \mathfrak{q} \cap A$. Dann ist $\mathfrak{q}$ genau dann maximales Ideal in B, wenn $\mathfrak{p}$ maximales Ideal in A ist.*

Beweis: Die Behauptung folgt sofort aus dem vorangegangenen Satz, wenn man beachtet, daß auch $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ eine ganze Ringerweiterung ist. ■

FOLGERUNG. *Sei $A \subseteq B$ eine ganze Ringerweiterung. Sind $\mathfrak{q} \subseteq \mathfrak{q}'$ Primideale in B mit $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$, so ist $\mathfrak{q} = \mathfrak{q}'$.*

Beweis: Wir lokalisieren in $\mathfrak{p}$, d.h. wähle $S = A \setminus \mathfrak{p}$. Dann ist $S^{-1}B$ ganz über $A_\mathfrak{p}$. Nun ist $\mathfrak{p}A_\mathfrak{p}$ maximales Ideal. Die Ideale $\mathfrak{q}S^{-1}B$ und $\mathfrak{q}'S^{-1}B$ müssen nach der letzten Aussage also auch maximal sein. Also $\mathfrak{q}S^{-1}B = \mathfrak{q}'S^{-1}B$. Damit folgt schon $\mathfrak{q} = \mathfrak{q}'$, da die Primideale von $S^{-1}B$ in Bijektion zu den zu S disjunkten Primidealen von B stehen. ■

SATZ. *Sei $A \subseteq B$ eine ganze Ringerweiterung. Zu jedem Primideal $\mathfrak{p}$ von A gibt es ein Primideal $\mathfrak{q}$ von B mit $\mathfrak{q} \cap A = \mathfrak{p}$. D.h. $Spec(B) \to Spec(A)$ ist surjektiv.*

Beweis: Wir lokalisieren in $S = A \setminus \mathfrak{p}$ und erhalten $A_\mathfrak{p} \subseteq B_\mathfrak{p}$, wo $B_\mathfrak{p} = S^{-1}B$ bedeutet. Sei $\mathfrak{m}$ ein maximales Ideal in $B_\mathfrak{p}$. Dann ist $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ nach unseren Sätzen. Sei nun $\mathfrak{q}$ das Primideal in B mit $S^{-1}\mathfrak{q} = \mathfrak{m}$. Dann gilt

$$S^{-1}(\mathfrak{q} \cap A) = S^{-1}\mathfrak{q} \cap S^{-1}A = \mathfrak{m} \cap A_\mathfrak{p} = S^{-1}(\mathfrak{p}),$$

also $\mathfrak{q} \cap A = \mathfrak{p}$. ■

Beispiel: Sei $A = \mathbf{Z}$ und $B = \mathbf{Z}[i]$. Dann gilt (Beweis als Übung):

- Über (0) liegt (0).
- Über (2) liegt $(1+i)$.
- Ist $p \equiv 3 \bmod 4$, so liegt über (p) nur (p).
- Ist $p \equiv 1 \bmod 4$, so ist p Summe von 2 Quadraten: $p = a^2 + b^2$. Über (p) liegen die 2 verschiedenen Primideale $(a + bi)$ und $(a - bi)$.

FOLGERUNG. *Ist $A \subseteq B$ eine ganze Ringerweiterung, so ist $Spec(B) \to Spec(A)$ eine abgeschlossene Abbildung, d.h. abgeschlossene Mengen werden in abgeschlossene Mengen abgebildet.*

Beweis: Sei $\mathfrak{b}$ ein Ideal in B und $\phi : A \to B$ die Inklusion. Dann gilt $\phi^*V(\mathfrak{b}) \subseteq V(\mathfrak{b} \cap A)$. Sei $\mathfrak{p} \in V(\mathfrak{b} \cap A)$. Wir betrachten die Ringerweiterung $A/(\mathfrak{b} \cap A) \subseteq B/\mathfrak{b}$. Zu $\overline{\mathfrak{p}}$ gibt es ein Primideal $\overline{\mathfrak{q}}$, das über $\overline{\mathfrak{p}}$ liegt. Liften nach B liefert ein Primideal $\mathfrak{q}$ mit $\mathfrak{q} \supset \mathfrak{b}$ und $\mathfrak{q} \cap A = \mathfrak{p}$. Also ist $\phi^*V(\mathfrak{b}) = V(\mathfrak{b} \cap A)$. ■

SATZ (Going-up). *Sei $A \subseteq B$ eine ganze Ringerweiterung. Sind $\mathfrak{p} \subseteq \mathfrak{p}'$ Primideale in A und ist $\mathfrak{q}$ ein Primideal in B mit $\mathfrak{q} \cap A = \mathfrak{p}$, so gibt es ein Primideal $\mathfrak{q}'$ in B mit $\mathfrak{q} \subseteq \mathfrak{q}'$ und $\mathfrak{q}' \cap A = \mathfrak{p}'$.*

Beweis: Sei $\overline{A} = A/\mathfrak{p}$ und $\overline{B} = B/\mathfrak{q}$. Dann ist $\overline{B}$ ganz über $\overline{A}$. Zu $\overline{\mathfrak{p}'}$ gibt es nach dem vorangegangenen Satz ein Primideal $\overline{\mathfrak{q}'}$ in $\overline{B}$ mit $\overline{\mathfrak{q}'} \cap \overline{B} = \overline{\mathfrak{p}'}$. Sei $\mathfrak{q}'$ das Urbild von $\overline{\mathfrak{q}'}$ unter $B \to B/\mathfrak{q}$. Dann gilt $\mathfrak{q} \subseteq \mathfrak{q}'$ und $\mathfrak{q}' \cap A = \mathfrak{p}'$. ■

Induktiv erhält man daraus sofort die folgende Version:

SATZ (Going-up). *Sei $A \subseteq B$ eine ganze Ringerweiterung. Sind $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ Primideale in A und $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ Primideale in B mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für $i = 1, \ldots, m$, so existieren Primideale $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ in B mit $\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ und $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für $i = 1, \ldots, n$.*

FOLGERUNG. *Sind $A \subseteq B$ Ringe und ist B ganz über A, so gilt $dim(A) = dim(B)$.*

Beweis: Gibt es eine Primidealkette $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$ in A, so läßt sich dazu eine in B finden: $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_r$. Ist umgekehrt $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_r$ eine Primidealkette in B, so ist $(A \cap \mathfrak{q}_0) \subset \cdots \subset (A \cap \mathfrak{q}_r)$ eine Primidealkette in A. Hieraus folgt sofort die Behauptung. ■

Ein Integritätsring A heißt ganz abgeschlossen, wenn er ganz abgeschlossen in seinem Quotientenkörper ist. In diesem Fall nennt man den Integritätsring A auch normal.

Beispiel: Sei $\alpha \in \mathbf{C}$ algebraisch über $\mathbf{Q}$ und $K = \mathbf{Q}(\alpha)$. (So etwas nennt man einen algebraischen Zahlkörper.) Der ganze Abschluß von $\mathbf{Z}$ in K wird dann mit $\mathfrak{o}_K$ bezeichnet und heißt der Ring der ganzen Zahlen von K. Eigenschaften von $\mathfrak{o}_K$ werden in der Algebraischen Zahlentheorie studiert. Insbesondere gilt $dim(\mathfrak{o}_K) = 1$.

Beispiel: Der Ring $A = k[x,y]/(y^2 - x^3)$ ist nicht ganz abgeschlossen.
Beweis: Betrachte $t = \frac{y}{x} \in Quot(A)$. Offensichtlich ist $t \notin A$, sonst hätte man eine Relation $\frac{y}{x} = f(x,y) + g(x,y)(y^2 - x^3)$ über $k[x,y]$. Andererseits ist $t^2 = \frac{y^2}{x^2} = x$, d.h. t ist ganz über A. ■

SATZ. *Jeder faktorielle Ring ist ganz abgeschlossen.*

Beweis: Sei A ein faktorieller Ring mit Quotientenkörper K. Sei $\frac{a}{b} \in K$ ganz über A, d.h. es gibt $a_1, \ldots, a_n \in A$ mit

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

O.E. können wir annehmen, daß a und b teilerfremd sind. Durch Multiplikation mit b^n folgt

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0,$$

insbesondere $b|a^n$. Da a und b teilerfremd sind, muß b eine Einheit sein, d.h. $\frac{a}{b} \in A$. Also ist A ganz abgeschlossen. ■

Genauso einfach geht der Beweis des folgenden Satzes:

SATZ. *Seien $A \subseteq B$ Ringe und C der ganze Abschluß von A in B. Ist S eine multiplikative Teilmenge von A, so ist $S^{-1}C$ der ganze Abschluß von $S^{-1}A$ in $S^{-1}B$.*

Ganz abgeschlossen zu sein ist eine lokale Eigenschaft:

SATZ. *Für einen Integritätsring A sind äquivalent:*

1. *A ist ganz abgeschlossen,*
2. *$A_\mathfrak{p}$ ist ganz abgeschlossen für alle Primideale $\mathfrak{p}$,*
3. *$A_\mathfrak{m}$ ist ganz abgeschlossen für alle maximalen Ideale $\mathfrak{m}$.*

Beweis: $1 \Rightarrow 2$: zuvor. $2 \Rightarrow 3$: klar.
$3 \Rightarrow 1$: Sei $x \in Quot(A)$ ganz über A. Dann ist x auch ganz über $A_\mathfrak{m}$, also nach Voraussetzung $x \in A_\mathfrak{m}$. Wir hatten aber bereits gesehen $A = \cap A_\mathfrak{m}$, woraus $x \in A$ folgt. ■

Zur Übung zeige man folgenden Satz:

SATZ. *Ist A ganz abgeschlossener Integritätsring, so ist auch der Polynomring $A[x_1, \ldots, x_n]$ ganz abgeschlossen.*

Von praktischer Bedeutung ist folgender Satz:

SATZ. *Sei A ein ganz abschlossener Integritätsring mit Quotientenkörper K und L eine algebraische Körpererweiterung von K. Ein $\alpha \in L$ ist genau dann ganz über A, wenn das Minimalpolynom von α über K Koeffizienten in A hat.*

Beweis: Sei $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ das Minimalpolynom von α über K. Gilt $a_i \in A$ für alle i, so ist natürlich α ganz über A. Sei jetzt umgekehrt α ganz über A. Sei $\overline{K}$ ein algebraischer Abschluß von K mit $L \subseteq \overline{K}$. Das Polynom $f(x)$ zerfällt als $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$, wo alle $\alpha_i \in \overline{K}$ und konjugiert über K sind. Also sind alle α_i ganz über A. Daher ist $A[\alpha_1, \ldots, \alpha_n]$ ein endlich erzeugter A-Modul. Nun sind aber $a_1, \ldots, a_n$ elementarsymmetrische Ausdrücke in den α_i's, also $a_1, \ldots, a_n \in A[\alpha_1, \ldots, \alpha_n]$. Daher sind die a_i's ganz über A und in K. Da A ganz abgeschlossen ist, folgt $a_1, \ldots, a_n \in A$. ■

SATZ. *Sei $A \subseteq B$ eine ganze Ringerweiterungen von Integritätsringen, K der Quotientenkörper von A, L der Quotientenkörper von B. Außerdem sei A ganz abgeschlossen und $L|K$ eine normale Körpererweiterung. Sind dann $\mathfrak{q}$ und $\mathfrak{q}'$ Primideale in B, die über dem gleichen Primideal $\mathfrak{p}$ von A liegen, d.h. $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$, dann gibt es einen Körperautomorphismus σ von L über K mit $\sigma(\mathfrak{q}) = \mathfrak{q}'$.*

Zum Beweis des Satzes benötigen wir folgendes Lemma:

LEMMA. *Ist $\mathfrak{a}$ ein Ideal und sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ Primideale mit $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, so gibt es ein i mit $\mathfrak{a} \subseteq \mathfrak{p}_i$.*

Beweis des Lemmas: (Vergleiche dies mit der Aussage für Untervektorräume eines Vektorraums.) Wir machen einen Induktionsbeweis. Im Fall $n = 1$ ist alles klar. Die Aussage gelte für $n - 1$ Primideale. Sei nun $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ vorausgesetzt.

- Wir können annehmen, daß $\mathfrak{a} \not\subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n-1}$, sonst sind wir nach Induktionsvoraussetzung bereits fertig. Wähle $a \in \mathfrak{a}$ mit $a \notin \mathfrak{p}_1, \ldots, a \notin \mathfrak{p}_{n-1}$. Nach Voraussetzung ist dann $a \in \mathfrak{p}_n$.

- Wir können annehmen, daß $\mathfrak{a}\mathfrak{p}_1 \dots \mathfrak{p}_{n-1} \not\subseteq \mathfrak{p}_n$, denn andernfalls ist $\mathfrak{a} \subseteq \mathfrak{p}_n$ (fertig) oder $\mathfrak{p}_i \subseteq \mathfrak{p}_n$ für ein $i < n$ und wir können wieder die Induktionsvoraussetzung anwenden. Wähle $b \in \mathfrak{a}\mathfrak{p}_1 \dots \mathfrak{p}_{n-1}$ mit $b \notin \mathfrak{p}_n$. Dann gilt auch $b \in \mathfrak{a}$ und $b \in \mathfrak{p}_1, \dots, b \in \mathfrak{p}_{n-1}$.

Betrachte jetzt $a + b$. Offensichtlich ist $a + b \in \mathfrak{a}$, aber $a + b \notin \mathfrak{p}_1, \dots, \mathfrak{p}_n$, ein Widerspruch. Also war die Annahme $\mathfrak{a} \not\subseteq \mathfrak{p}_n$ falsch. Damit folgt die Behauptung. ■

Beweis des Satzes: Wir beweisen den Satz nur im Fall, daß $L|K$ endlich algebraisch ist. Sei $G = \{\sigma_1, \dots, \sigma_n\}$ die Gruppe die Körperautomorphismen von L über K.
Behauptung: $\mathfrak{q}' \subseteq \sigma_1\mathfrak{q} \cup \dots \cup \sigma_n\mathfrak{q}$.
Beweis: Angenommen, dies wäre falsch. Dann gibt es ein $x \in \mathfrak{q}'$ mit $x \notin \sigma_i\mathfrak{q}$. Da $L|K$ normal ist, ist $\prod \sigma_i x$ rein inseparabel über K, d.h. es gibt eine Potenz $y = (\prod \sigma_i x)^N \in K$. Mit x sind auch alle $\sigma_i x$ ganz über A, also ist auch $y \in K$ ganz über A. Da A ganz abgeschlossen ist, gilt $y \in A$. Nun ist $y \in A \cap \mathfrak{q} = \mathfrak{p} \subseteq \mathfrak{q}'$. Also gibt es ein σ mit $\sigma x \in \mathfrak{q}$ und damit $x \in \sigma^{-1}\mathfrak{q}$, ein Widerspruch zur Annahme. Daher ist die Behauptung richtig.
Es gibt also ein i mit $\mathfrak{q}' \subseteq \sigma_i\mathfrak{q}$. Da beide Primideale über $\mathfrak{p}$ liegen, folgt schon $\mathfrak{q}' = \sigma_i\mathfrak{q}$, was wir zeigen wollten. ■

Beispiele:

1. Im Fall $\mathbf{Z} \subseteq \mathbf{Z}[i]$ ist die Aussage des Satzes schön zu sehen.
2. Die Aussage kann nicht mehr so stimmen, wenn $L|K$ nicht normal ist. Sei $A = \mathbf{Z}$ und $B = \mathbf{Z}[\alpha]$ mit $\alpha = \sqrt[3]{2}$. Dann sind $\mathfrak{q} = (5, \alpha + 2)$ und $\mathfrak{q}' = (5, \alpha^2 - 2\alpha + 1)$ Primideale in B, die über dem Primideal (5) von $\mathbf{Z}$ liegen. Wegen $B/\mathfrak{q} \simeq \mathbf{F}_5$ und $B/\mathfrak{q}' \simeq \mathbf{F}_{25}$ können $\mathfrak{q}$ und $\mathfrak{q}'$ nicht durch einen Isomorphismus ineinander überführt werden.

Satz (Going-down). *Sei $A \subseteq B$ eine ganze Ringerweiterung von Integritätsringen und A sei ganz abgeschlossen. Sind $\mathfrak{p} \supseteq \mathfrak{p}'$ Primideale in A und ist $\mathfrak{q}$ ein Primideal in B mit $\mathfrak{q} \cap A = \mathfrak{p}$, so gibt es ein Primideal $\mathfrak{q}'$ in B mit $\mathfrak{q}' \cap A = \mathfrak{q}$ und $\mathfrak{q} \supseteq \mathfrak{q}'$.*

Beweis: Sei $K = Quot(A)$ und L die normale Hülle von $Quot(B)$. Sei C der ganze Abschluß von A (oder B) in L. Sei $\mathfrak{q}_0$ ein Primideal in C, das über $\mathfrak{q}$ liegt. Nach going-up gibt es Primideale $\mathfrak{p}_0 \supseteq \mathfrak{p}'_0$ in C, die über $\mathfrak{p} \supseteq \mathfrak{p}'$ liegen. Da sowohl $\mathfrak{p}_0$ als auch $\mathfrak{q}_0$ über $\mathfrak{p}$ von A liegen, lassen sie sich durch einen Automorphismus ineinander überführen. O.E. $\mathfrak{q}_0 = \mathfrak{p}_0$. Dann gilt aber $B \cap \mathfrak{p}_0 \supseteq B \cap \mathfrak{p}'_0$ und $B \cap \mathfrak{p}'_0$ liegt über $\mathfrak{p}'$, woraus die Behauptung folgt. ■

Geometrische Interpretation von Going-down: Die Voraussetzungen seien wie im letzten Satz. Was heißt dies für $\phi^* : Spec(B) \to Spec(A)$? (Wir nehmen noch an, daß B noethersch ist.) Sei $\mathfrak{p} \in Spec(A)$. Dann gilt

$$\phi^{*-1}V(\mathfrak{p}) = V(\mathfrak{q}_1) \cup \dots \cup V(\mathfrak{q}_r),$$

wo die $V(\mathfrak{q}_i)$ die irreduziblen Komponenten sind.
Behauptung: $\phi^*\mathfrak{q}_i = \mathfrak{p}$.
Beweis: Wäre $\phi^*\mathfrak{q}_i \supset \mathfrak{p}$, so gäbe es $\mathfrak{q}'$ mit $\mathfrak{q}_i \supset \mathfrak{q}'$ und $\phi^*\mathfrak{q}' = \mathfrak{p}$, also $\mathfrak{q}' \in V(\mathfrak{q}_1) \cup \dots \cup V(\mathfrak{q}_r)$, ein Widerspruch.
Dies kann man auch anders ausdrücken: Ist $X \subseteq Spec(A)$ irreduzibel und $Y \subseteq Spec(B)$ eine irreduzible Komponente von $\phi^{*-1}X$, dann wird der generische Punkt von Y auf den generischen Punkt von X abgebildet. (Vgl. Aufgabe 38, wo in einem Beispiel geometrisch gezeigt wird, daß Going down nicht gilt.)

Wir kommen nun zu einer wichtigen Eigenschaft ganz abgeschlossener Ringe im eindimensionalen Fall:

Satz. *Sei $(R, \mathfrak{m})$ ein lokaler noetherscher Integritätsring der Dimension 1. Dann gilt:*

$$R \text{ ist ganz abgeschlossen} \iff R \text{ ist diskreter Bewertungsring.}$$

Beweis: Die eine Richtung ist einfach: Ein diskreter Bewertungsring ist faktoriell, insbesondere also ganz abgeschlossen. Sei jetzt R ganz abgeschlossen in seinem Quotientenkörper K. Wir haben früher bereits gesehen, daß es genügt zu zeigen, daß $\mathfrak{m}$ ein Hauptideal ist. Wir gehen in mehreren Schritten vor.
Sei $a \in \mathfrak{m}, a \neq 0$ und $\mathfrak{m} = (x_1, \dots, x_r)$, o.E. $x_i \neq 0$. Da in R nur die 2 Primideale 0 und $\mathfrak{m}$ existieren und $\{x_i^n : n \geq 0\} \cap \mathfrak{m} \neq \emptyset$ gilt, enthält R_{x_i} nur ein Primideal, nämlich 0, ist also ein Körper, also $R_{x_i} = K$.

Dann gibt es $n_i \geq 0$ und $y_i \in R$ mit $\frac{1}{a} = \frac{y_i}{x_i^{n_i}}$, woraus sofort $x_i^{n_i} = y_i a \in (a)$ folgt. Damit sieht man leicht, daß es ein n gibt mit $\mathfrak{m}^n \subseteq (a)$. Wähle n mit dieser Eigenschaft minimal, d.h. $\mathfrak{m}^{n-1} \not\subseteq (a)$. Wähle $b \in \mathfrak{m}^{n-1}, b \notin (a)$. Dann ist $\frac{b}{a} \notin R$, aber wegen $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$ gilt $\frac{b}{a}\mathfrak{m} \subseteq R$.
Wäre $\frac{b}{a}\mathfrak{m} \subseteq \mathfrak{m}$, so wäre $\frac{b}{a}$ ganz über R, also $\frac{b}{a} \in R$, da R ganz abgeschlossen ist: ein Widerspruch. Also bleibt nur der Fall $\frac{b}{a}\mathfrak{m} = R$. Dies liefert sofort $\mathfrak{m} = \frac{a}{b}R$, also ist $\mathfrak{m}$ Hauptideal, was zu zeigen war. ■

Bemerkung: Geometrisch läßt sich dies so interpretieren: Kurvensingularitäten löst man durch Normalisierung auf.

Beispiel: Sei k algebraisch abgeschlossener Körper und $A = k[X,Y]/(Y^2 - X^2 - X^3)$. Die Bilder von X und Y in A werden mit x und y bezeichnet. Dann gilt also $y^2 = x^2 + x^3$. Sei $K = Quot(A)$. Es gilt:

$$Spec(A) = \{(y^2 - x^2 - x^3)\} \cup \{(x - a, y - b) : a, b \in k, b^2 = a^2 + a^3\}.$$

Sei $t = \frac{y}{x}$. Dann gilt $t^2 = 1 + x$. Also ist t ganz über A. Da $t \notin A$, ist A nicht ganz abgeschlossen. Nun gilt aber $x = t^2 - 1$ und $y = tx = t(t^2 - 1)$, also $A \subseteq k[t]$. Da $k[t]$ faktoriell ist, ist $k[t]$ ganz abgeschlossen. D.h. der ganze Abschluß von A ist $k[t]$. Die induzierte Abbildung $Spec(k[t]) \to Spec(A)$ bildet die Punkte $(t-1)$ und $(t+1)$ auf den *singulären* Punkt (x, y) ab. (Geometrische Interpretation!)

Wir kommen nun zu einem weiteren wichtigen Satz:

Satz (Noetherscher Normalisierungssatz). *Sei A eine endlich erzeugte k-Algebra über einem Körper k. Dann gibt es über k algebraisch unabhängige $x_1, \ldots, x_r \in A$, so daß A über $k[x_1, \ldots, x_r]$ ganz ist. (Insbesondere ist A dann ein endlich erzeugter $k[x_1, \ldots, x_r]$-Modul und $dim(A) = r$.)*

Zur Erinnerung: $x_1, \ldots, x_r \in A$ heißen algebraisch abhängig über k, wenn es ein Polynom $f(X_1, \ldots, X_r) \neq 0$ mit Koeffizienten in k gibt mit $f(x_1, \ldots, x_r) = 0$.

Beweis: Wir beweisen den Satz nur für den Fall, daß k unendlich ist.

1. Sei A von $u_1, \ldots, u_n$ über k als Ring erzeugt, d.h. $A = k[u_1, \ldots, u_n]$. Nach Umbenennung kann man annehmen, daß $u_1, \ldots, u_r$ algebraisch unabhängig über k sind, und daß $u_{r+1}, \ldots, u_n$ algebraisch von $u_1, \ldots, u_r$ abhängen.
2. Wir machen jetzt Induktion nach n. Im Fall $n = r$ sind wir fertig. Sei also $n > r$ vorausgesetzt. u_n ist algebraisch über $k[u_1, \ldots, u_{n-1}]$. Also gibt es ein Polynom $f(x_1, \ldots, x_n) \neq 0$ mit $f(u_1, \ldots, u_n) = 0$.
3. Zerlege f in homogene Bestandteile: $f = f_0 + f_1 + \cdots + f_d$, wo f_i homogen vom Grad i ist und $f_d \neq 0$. Da k als unendlich vorausgesetzt war, gibt es $c_1, \ldots, c_{n-1} \in k$ mit $f(c_1, \ldots, c_{n-1}, 1) \neq 0$. Wir definieren $v_i = u_i - c_i u_n$ für $i = 1, \ldots, n-1$ und ersetzen jetzt die $u_1, \ldots, u_{n-1}$ durch $v_1, \ldots, v_{n-1}$. Dann gilt
$$\begin{aligned} 0 &= f(v_1 + c_1 u_n, \ldots, v_{n-1} + c_{n-1} u_n, u_n) = \\ &= f_d(v_1 + c_1 u_n, \ldots, v_{n-1} + c_{n-1} u_n, u_n) + \cdots = \\ &= f_d(c_1, \ldots, c_{n-1}, 1) u_n^d + \ldots, \end{aligned}$$
d.h. u_n ist ganz über $k[v_1, \ldots, v_{n-1}]$.
4. Wendet man jetzt die Induktionsvoraussetzung auf $k[v_1, \ldots, v_{n-1}]$ an, so findet man Elemente $x_1, \ldots, x_r \in k[v_1, \ldots, v_{n-1}]$, die algebraisch unabhängig sind und die Eigenschaft haben, daß $k[v_1, \ldots, v_{n-1}]$ ganz über $k[x_1, \ldots, x_r]$ ist. Dann ist natürlich auch A ganz über $k[x_1, \ldots, x_r]$, woraus die Behauptung folgt. ■

Beispiel: Sei k ein algebraisch abgeschlossener Körper und $A = k[x,y]/(xy - 1)$. Es ist

$$Spec(A) = \{(0)\} \cup \{(x - a, y - \frac{1}{a}) : a \in k, a \neq 0\}.$$

A ist nicht ganz über $k[x]$, sonst wäre $Spec(A) \to Spec(k[x])$ surjektiv, was nicht der Fall ist. Wir setzen an: $x = u + cy$ und erhalten

$$0 = xy - 1 = (u + cy)y - 1 = cy^2 + uy - 1.$$

Wählt man also $c = 1$, d.h. $u = x - y$, so gilt $y^2 + uy - 1 = 0$, d.h. A ist ganz über $k[u]$.

Wir wenden jetzt diesen Normalisierungssatz an, um verschiedene Versionen des Hilbertschen Nullstellensatzes zu zeigen.

Sei $R = k[x_1, \ldots, x_n]$ der Polynomring über einem Körper k und $\mathfrak{m}$ ein maximales Ideal in R. Wie sieht $\mathfrak{m}$ aus?

1. Wir wenden den Normalisierungssatz auf die endlich erzeugte k-Algebra $R/\mathfrak{m}$ an: $R/\mathfrak{m}$ ist also ganz über einem Polynomring $k[y_1, \ldots, y_r]$. Da aber $R/\mathfrak{m}$ ein Körper ist, ist es auch $k[y_1, \ldots, y_r]$, also $k[y_1, \ldots, y_r] = k$. Damit ist $R/\mathfrak{m}$ endlich über k, d.h. eine endliche Körpererweiterung von k. Also $k \subseteq R/\mathfrak{m} \subseteq \overline{k}$.
2. Ist k algebraisch abgeschlossen, so folgt $R/\mathfrak{m} = k$. Schreibt man $\phi : R \to k$ für die Abbildung $R \to R/\mathfrak{m} \to k$ und $a_i = \phi(x_i)$, so ist $\phi(x_i - a_i) = 0$, also $x_i - a_i \in kern(\phi) = \mathfrak{m}$. Aus $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}$ folgt aber wegen $R/(x_1 - a_1, \ldots, x_n - a_n) \simeq k$ sofort
$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n).$$

Damit haben wir bewiesen:

SATZ. *Ist k ein algebraisch abgeschlossener Körper, so haben alle maximalen Ideale des Polynomrings $k[x_1, \ldots, x_n]$ die Gestalt $(x_1 - a_1, \ldots, x_n - a_n)$, mit $a_1, \ldots, a_n \in k$.*

Sei jetzt k algebraisch abgeschlossen und $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. Geometrisch ist die Nullstellenmenge
$$X = N(f_1, \ldots, f_r) = \{(a_1, \ldots, a_n) \in k^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\}$$
interessant. Sei $\mathfrak{a} = (f_1, \ldots, f_r)$ das von den f_i's erzeugte Ideal. Klar ist $N(\mathfrak{a}) = N(f_1, \ldots, f_r)$.

- Ist $\mathfrak{a} = k[x_1, \ldots, x_n]$, so gibt es Polynome g_i mit $1 = g_1 f_1 + \cdots + g_r f_r$ und es folgt $X = \emptyset$.
- Ist $\mathfrak{a} \neq k[x_1, \ldots, x_n]$, so gibt es ein maximales Ideal $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ mit $\mathfrak{a} \subseteq \mathfrak{m}$ und man sieht sofort $(a_1, \ldots, a_n) \in X$, insbesondere $X \neq 0$.

Wir formulieren dies:

FOLGERUNG. *Ist k algebraisch abgeschlossen und sind $f_1, \ldots, f_r$ Polynome mit $(f_1, \ldots, f_r) \neq k[x_1, \ldots, x_n]$, so haben $f_1, \ldots, f_r$ eine gemeinsame Nullstelle in k^n.*

Teilmengen von k^n der Gestalt $N(f_1, \ldots, f_r)$ nennt man auch algebraische Teilmengen von k^n. Ist $Y \subseteq k^n$ irgendeine Teilmenge, so sei
$$I(Y) = \{f \in k[x_1, \ldots, x_n] : f(P) = 0 \text{ für alle } P \in Y\}$$
das Ideal der Funktionen, die auf ganz Y verschwinden.
Nun fragen wir: Welche Polynome verschwinden auf $X = N(f_1, \ldots, f_r)$, d.h. was ist $I(X)$? Sei $\mathfrak{a} = (f_1, \ldots, f_r)$. Natürlich verschwinden alle Polynome aus $\mathfrak{a}$ auf X. Genauso klar ist: Alle Polynome aus $\sqrt{\mathfrak{a}}$ verschwinden auf X, denn ist $f \in \sqrt{\mathfrak{a}}$, so gibt es ein $n \geq 1$ mit $f^n \in \mathfrak{a}$, also verschwindet f^n auf X, also auch f. Dies ist nun auch die einzige Möglichkeit:

SATZ (Hilbertscher Nullstellensatz). *Ist k algebraisch abgeschlossen und sind $f_1, \ldots, f_r$ Polynome in $k[x_1, \ldots, x_n]$, so gilt:*
$$I(N(f_1, \ldots, f_r)) = \sqrt{(f_1, \ldots, f_r)}.$$

Beweis: Die Inklusion $\supseteq$ ist klar. Sei $f \in k[x_1, \ldots, x_n] = 0$ mit $f(P) = 0$, falls $f_1(P) = \cdots = f_r(P) = 0$ ist. Wir nehmen zu $x_1, \ldots, x_n$ noch eine weitere Unbestimmte y hinzu. Die Polynome $f_1, \ldots, f_r, 1 - zf$ können keine gemeinsame Nullstelle haben, also gibt es nach obiger Überlegung $g_1, \ldots, g_r, g \in k[x_1, \ldots, x_n, y]$ mit
$$1 = g_1 f_1 + \cdots + g_r f_r + g(1 - yf).$$
Setzt man nun $y = \frac{1}{f}$ ein und multipliziert mit einer genügend hohen Potenz von f durch, so erhält man in $k[x_1, \ldots, x_n]$: $f^n \in (f_1, \ldots, f_r)$, was wir zeigen wollten. ■

Die Voraussetzung, daß k algebraisch abgeschlossen ist, ist wichtig für den Satz, wie folgendes Beispiel zeigt:

Beispiel: Sei $k = \mathbf{R}$ und $f = x^2 + y^2 \in \mathbf{R}[x, y]$. Dann ist $N(f) = \{(0, 0)\}$ und $I(N(f)) = (x, y)$, also $(f) = \sqrt{(f)} \neq I(N(f))$.

Eine nichtleere algebraische Teilmenge von k^n heißt irreduzibel, wenn sie sich nicht als echte Vereinigung zweier algebraischer Teilmengen von k^n schreiben läßt. Als Übung zeige man für eine algebraische Menge $X \subseteq k^n$:

$$X \text{ irreduzibel} \iff I(X) \text{ Primideal.}$$

Eine irreduzible algebraische Teilmenge von k^n heißt auch Untervarietät. Ist $\mathfrak{p}$ ein Primideal, so ist also $I(N(\mathfrak{p})) = \mathfrak{p}$, d.h. $\mathfrak{p}$ ist durch $N(\mathfrak{p}) \subseteq k^n$ bestimmt. (Hilbertscher Nullstellensatz)

Geometrische Interpretation von $Spec(k[x_1, \ldots, x_n]/\mathfrak{a})$**:** Sei k algebraisch abgeschlossener Körper und $\mathfrak{a} = (f_1, \ldots, f_r)$ ein Ideal in $k[x_1, \ldots, x_n]$. Wir wissen bereits, daß wir $A = k[x_1, \ldots, x_n]/\mathfrak{a}$ als Ring von Funktionen auf $N(\mathfrak{a})$ auffassen können. Wie können wir $Spec(A)$ deuten?
Ein Punkt $P \in Spec(A)$ kann als Primideal $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ angesehen werden mit $\mathfrak{a} \subseteq \mathfrak{p}$. Dann ist $N(\mathfrak{p}) \subseteq N(\mathfrak{a})$ also eine Untervarietät von $N(\mathfrak{a})$.
Ist umgekehrt X eine Untervarietät von $N(\mathfrak{a})$, so gibt es ein Primideal $\mathfrak{p}$ mit $X = N(\mathfrak{p})$. Wegen $N(\mathfrak{p}) \subseteq N(\mathfrak{a})$ folgt $I(N(\mathfrak{a})) \subseteq I(N(\mathfrak{p}))$, was mit dem Hilbertschen Nullstellensatz $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \subseteq \mathfrak{p}$ ergibt. $\mathfrak{p}$ liefert wieder einen Punkt in $Spec(k[x_1, \ldots, x_n]/\mathfrak{a})$.
Ergebnis:

$$Spec(A) \simeq \{\text{Untervarietäten von } N(\mathfrak{a})\}.$$

KAPITEL 8

Assoziierte Primideale und Primärzerlegung

DEFINITION. Sei A ein noetherscher Ring und M ein A-Modul. Ein $\mathfrak{p} \in Spec(A)$ heißt assoziiertes Primideal zu M, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

1. Es gibt ein $x \in M$ mit $ann(x) = \mathfrak{p}$.
2. M enthält einen zu $A/\mathfrak{p}$ isomorphen Untermodul.

Die Menge der assoziierten Primideale von M wird mit $Ass(M) = Ass_A(M)$ bezeichnet.

(Zur Äquivalenz: Gibt es $x \in M$ mit $ann(x) = \mathfrak{p}$, so induziert $A \to M, a \mapsto ax$ eine Injektion $A/\mathfrak{p} \hookrightarrow M$. Ist umgekehrt $\phi : A/\mathfrak{p} \hookrightarrow M$ injektiv, so ist $ann(\phi(\overline{1})) = \mathfrak{p}$.)
Wir setzen in diesem Abschnitt voraus, daß alle Ringe noethersch sind.

Beispiele:

1. Ist A ein Integritätsring, $M = A$, so ist $ann(0) = A$ und $ann(a) = (0)$ für $a \neq 0$. Also $Ass(A) = \{(0)\}$. Insbesondere $Ass_{\mathbf{Z}}(\mathbf{Z}) = \{0\}$.
2. Ist A ein Ring, $\mathfrak{p} \in Spec(A)$ und $M = A/\mathfrak{p}$, so gilt für $a \in \mathfrak{p}$: $ann(\overline{a}) = A$, für $a \notin \mathfrak{p}$: $ann(a) = \mathfrak{p}$. Also $Ass_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$. Insbesondere $Ass_{\mathbf{Z}}(\mathbf{Z}/(p)) = \{(p)\}$. Man beachte auch, daß für $x \in M, x \neq 0$ gilt: $ann(x) = \mathfrak{p}$.
3. Sei A faktoriell und $\{p_i : i \in I\}$ ein Repräsentantensystem der irreduziblen Elemente. Sei $f = \prod p_i^{f_i}$ und $M = A/(f)$. Was ist $Ass_A(M)$? Wir berechnen zunächst $ann_A(\overline{a})$ für $a = u\prod p_i^{a_i}$. Sei $b = v\prod p_i^{b_i}$. Dann gilt:
$$b \in ann_A(\overline{a}) \iff f|ab \iff f_i \leq a_i + b_i \iff b_i \geq \max(f_i - a_i, 0) \iff$$
$$\iff b \in (\prod p_i^{\max(f_i - a_i, 0)}).$$
Damit:
$$ann(\overline{a}) = (\prod p_i^{\max(f_i - a_i, 0)}),$$
woraus schnell folgt:
$$Ass_A(A/(\prod p_i^{f_i})) = \{(p_i) : f_i > 0\} \text{ oder } Ass_A(A/(f)) = \{(p) : p|f\}.$$
4. Insbesondere hat man also
$$Ass_{\mathbf{Z}}(\mathbf{Z}/(12)) = \{(2), (3)\}.$$
5. Ebenso erhält man
$$Ass_{k[x,y]}(k[x,y]/(x^2y)) = \{(x), (y)\}.$$
Geometrische Interpretation: Ass besteht aus den irreduziblen Komponenten des Spektrums.

Bemerkung: Sei A noetherscher Ring und M ein A-Modul.

1. Für $x \in M$ gilt: $ann(x) = A \iff x = 0$.
2. Für $b \in A$ und $x \in M$ gilt: $ann(x) \subseteq ann(bx)$.

SATZ. *Sei M ein A-Modul. Ist $\mathfrak{p} \in \{ann(x) : x \in M, x \neq 0\}$ maximal, dann ist $\mathfrak{p} \in Ass(M)$.*

Beweis: Sei $\mathfrak{p} = ann(x)$ maximal wie im Satz. Wir müssen nur noch zeigen, daß $\mathfrak{p}$ Primideal ist. Nach Voraussetzung ist $\mathfrak{p} \neq A$. Sei $ab \in \mathfrak{p}$. Dann ist $abx = 0$. Ist $bx = 0$, so $b \in \mathfrak{p}$. Ist $bx \neq 0$, so ist $ann(x) \subseteq ann(bx) \neq A$, also $ann(x) = ann(bx)$ und wegen $abx = 0$ folgt $a \in ann(bx) = ann(x) = \mathfrak{p}$, woraus folgt, daß $\mathfrak{p}$ ein Primideal ist. ■

FOLGERUNG. *Für einen A-Modul M gilt: $M \neq 0 \iff Ass_A(M) \neq \emptyset$.*

Bemerkung: Es gibt nicht noethersche Ringe und Moduln $M \neq 0$ mit $Ass(M) = \emptyset$.

$a \in A$ heißt Nullteiler von M, wenn es ein $x \in M$, $x \neq 0$ gibt mit $ax = 0$, d.h. $a \in ann(x)$. Damit gilt:

$$\{\text{Nullteiler von } M\} = \cup_{x \in M, x \neq 0} ann(x) = \cup_{\mathfrak{p} \in Ass(M)} \mathfrak{p}.$$

Damit haben wir:

FOLGERUNG. *Die Menge der Nullteiler von M ist die Vereinigung der assoziierten Primideale für M.*

SATZ. *Ist S eine multiplikative Teilmenge von A und M ein A-Modul, so gilt*

$$Ass_A(S^{-1}M) = Ass_{S^{-1}A}(S^{-1}M) = Ass_A(M) \cap \{\mathfrak{p} \in Spec(A) : S \cap \mathfrak{p} = \emptyset\}.$$

Dabei interpretieren wir $Spec(S^{-1}A) = \{\mathfrak{p} \in Spec(A) : \mathfrak{p} \cap S = \emptyset\}$.

Beweis:

1. $Ass_A(S^{-1}M) = Ass_{S^{-1}A}(S^{-1}M)$:
   $\subseteq$: Ist $\mathfrak{p} = ann(\frac{x}{1})$, so gilt
   $$\frac{a}{1} \in ann(\frac{x}{1}) \iff \frac{ax}{1} = 0 \iff a \in \mathfrak{p},$$
   also $S^{-1}\mathfrak{p} \in Ass_{S^{-1}A}(S^{-1}M)$.
   $\supseteq$: Sei $S^{-1}\mathfrak{p} = ann(\frac{x}{1})$, insbesondere also $\mathfrak{p} \cap S = \emptyset$. Dann gilt:
   $$a \in ann(\frac{x}{1}) \iff \frac{ax}{1} = 0 \iff \frac{a}{1} \in S^{-1}\mathfrak{p},$$
   also $\mathfrak{p} = ann(\frac{x}{1})$.
2. $Ass_{S^{-1}A}(S^{-1}M) \simeq Ass_A(M) \cap \{\mathfrak{p} \in Spec(A) : \mathfrak{p} \cap S = \emptyset\}$.
   $\supseteq$: Sei $\mathfrak{p} \cap S = \emptyset$ und $\mathfrak{p} = ann(x)$. Dann gilt
   $$\frac{a}{1} \in ann(\frac{x}{1}) \iff \frac{ax}{1} = 0 \iff sax = 0$$
   für ein $s \in S$, was mit $sa \in \mathfrak{p}$ für ein $s \in S$ gleichwertig ist, d.h. $a \in \mathfrak{p}$. Also $ann(\frac{x}{1}) = S^{-1}\mathfrak{p}$.
   $\subseteq$: Sei $S^{-1}\mathfrak{p} = ann(\frac{x}{1})$, insbesondere $\mathfrak{p} \cap S = \emptyset$. Ist $p \in \mathfrak{p}$, so gilt $\frac{px}{1} = 0$, also gibt es ein $s \in S$ mit $spx = 0$. Nun ist $\mathfrak{p}$ endlich erzeugt: $\mathfrak{p} = (p_1, \ldots, p_r)$. Daher gibt es $s_i \in S$ mit $s_i p_i x = 0$. Wählt man $s = s_1 \ldots s_r \in S$, so ist $sp_i x = 0$, also $\mathfrak{p} \subseteq ann(sx)$.
   Ist $a \in ann(sx)$, so gilt $asx = 0$, also $\frac{as}{1} \in S^{-1}\mathfrak{p}$, also $\frac{a}{1} \in S^{-1}\mathfrak{p}$, also $a \in \mathfrak{p}$. Damit haben wir $\mathfrak{p} = ann(sx)$, woraus die Behauptung folgt. (Nur bei diesem Schritt haben wir benutzt, daß A noethersch ist.) ■

FOLGERUNG. *Sei M ein A-Modul. Dann gilt für $\mathfrak{p} \in Spec(A)$:*

$$\mathfrak{p} \in Ass_A(M) \iff \mathfrak{p}A_{\mathfrak{p}} \in Ass_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}).$$

Dies erhält man sofort, wenn man im Satz $S = A \setminus \mathfrak{p}$ wählt.

SATZ. *Sei M ein A-Modul. Dann gilt:*

1. *$Ass(M) \subseteq supp(M)$.*
2. *Jedes minimale Primideal in $supp(M)$ liegt in $Ass(M)$. D.h. Die minimalen Elemente von $supp(M)$ und $Ass(M)$ stimmen überein.*

Beweis:

1. Sei $\mathfrak{p} \in Ass(M)$. Dann ist $\mathfrak{p}A_{\mathfrak{p}} \in Ass_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$, also $M_{\mathfrak{p}} \neq 0$, also $\mathfrak{p} \in supp(M)$.
2. Sei $\mathfrak{p}$ minimal in $supp(M)$. Dann gilt
   $$\emptyset \neq Ass_A(M_{\mathfrak{p}}) = Ass(M) \cap \{\mathfrak{q} : \mathfrak{q} \subseteq \mathfrak{p}\} \subseteq supp(M) \cap \{\mathfrak{q} : \mathfrak{q} \subseteq \mathfrak{p}\} = \{\mathfrak{p}\},$$
   also $\mathfrak{p} \in Ass(M)$. ■

DEFINITION. Für einen A-Modul M heißen die minimalen Elemente von $Ass(M)$ die isolierten assoziierten Primideale von M, die anderen heißen eingebettete Primideale.

Beispiel: Sei $\mathfrak{a}$ ein Ideal in A. Wir wissen: $supp(A/\mathfrak{a}) = V(\mathfrak{a})$. Nun ist $V(\mathfrak{a}) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r)$. Die $\mathfrak{p}_i$'s sind dann genau die minimalen Primoberideale von $\mathfrak{a}$ und genau die isolierten assoziierten Primideale zu $A/\mathfrak{a}$.

Beispiel: Sei $A = k[x,y]$ und $M = A/(x^2, xy)$. Dann ist $ann(x) = (x,y)$ und $ann(y) = (x)$. Man überlegt sich: $Ass(M) = \{(y), (x,y)\}$. Also ist (x,y) eingebettetes Primideal.

LEMMA. *Ist $0 \to M' \to M \to M'' \to 0$ eine exakte Sequenz von A-Moduln, so gilt $Ass(M') \subseteq Ass(M) \subseteq Ass(M') \cup Ass(M'')$.*

Beweis: Die erste Inklusion ist klar, denn $\mathfrak{p} \in Ass(M')$ liefert $A/\mathfrak{p} \subseteq M' \subseteq M$, also $\mathfrak{p} \in Ass(M)$. Sei $\mathfrak{p} \in Ass(M)$. Dann gibt es einen Untermodul N in M mit $N \simeq A/\mathfrak{p}$. Beachte, daß für $x \in N, x \neq 0$ gilt $ann(x) = \mathfrak{p}$. Ist $M' \cap N \neq 0$, dann gibt es ein $x \in M' \cap N$, $x \neq 0$, also ist $\mathfrak{p} = ann(x) \in Ass(M')$. Ist $N \cap M' = 0$, so ist N isomorph zu seinem Bild in M'', also hat M'' einen zu $A/\mathfrak{p}$ isomorphen Untermodul, d.h. $\mathfrak{p} \in Ass(M'')$. ■

FOLGERUNG. *Es gilt*

$$Ass_A(M_1 \oplus \cdots \oplus M_n) = Ass(M_1) \cup \cdots \cup Ass(M_n).$$

Beweis: Es genügt den Fall $n = 2$ zu zeigen. Wegen $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ folgt

$$Ass(M_1) \subseteq Ass(M_1 \oplus M_2) \subseteq Ass(M_1) \cup Ass(M_2)$$

und durch Vertauschen von M_1 und M_2

$$Ass(M_2) \subseteq Ass(M_1 \oplus M_2) \subseteq Ass(M_1) \cup Ass(M_2),$$

woraus die Behauptung folgt. ■

Beispiel: Ein endlich erzeugter $\mathbf{Z}$-Modul hat die Gestalt

$$M = \mathbf{Z}^r \oplus \mathbf{Z}/(p_1^{n_1}) \oplus \ldots \mathbf{Z}/(p_s^{n_s}),$$

mit $n_i > 0$, wo aber die p_i nicht verschieden sein müssen. Dann ist $Ass(M) = \{(0), (p_1), \ldots, (p_s)\}$, falls $r > 0$ und $Ass(M) = \{(p_1), \ldots, (p_s)\}$, falls $r = 0$ ist.

LEMMA. *Sei M ein endlich erzeugter A-Modul und $M \neq 0$. Dann gibt es Untermoduln M_i mit*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M,$$

so daß $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ für ein $\mathfrak{p}_i \in Spec(A)$ gilt.

Beweis: Da $M \neq 0$ ist $Ass(M) \neq \emptyset$, d.h. es gibt einen Untermodul $M_1 \subseteq M$ mit $M_1 \simeq A/\mathfrak{p}_1$ für $\mathfrak{p}_1 \in Ass(M)$. Ist $M \neq M_1$, so betrachten wir M/M_1 und erhalten M_2 mit $M_1 \subseteq M_2 \subseteq M$ mit $M_2/M_1 \simeq A/\mathfrak{p}_2$ mit $\mathfrak{p}_2 \in Ass(M/M_1)$. So fährt man fort und erhält eine Kette von Untermoduln

$$0 \subset M_1 \subset M_2 \subset M_3 \cdots \subset M$$

mit $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ mit $\mathfrak{p}_i \in Spec(A)$. Da A noethersch ist und M endlich erzeugt, ist auch M noethersch, d.h. es gibt ein n mit $M_n = M$, woraus die Behauptung folgt. ■

SATZ. *Ist M ein endlich erzeugter A-Modul, so ist $Ass(M)$ endlich.*

Beweis: Es gibt eine Kette

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

mit $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, $\mathfrak{p}_i \in Spec(A)$. Nun ist

$$0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0,$$

also nach dem letzten Satz:

$$Ass(M_i) \subseteq Ass(M_{i-1}) \cup \{\mathfrak{p}_i\},$$

woraus durch Induktion folgt:

$$Ass(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$■

Wir kommen nun zu Primärzerlegungen. Ziel ist es, die Ideale eines Rings strukturell besser verstehen.

Vorbemerkungen und Beispiele:

1. Sei $\mathfrak{a} \in \mathbf{Z}$ ein Ideal, $\mathfrak{a} \neq 0, \mathbf{Z}$. Dann gibt es verschiedenen Primzahlen $p_1, \ldots, p_r$ und natürlichen Zahlen $n_1, \ldots, n_r \geq 1$ mit $\mathfrak{a} = (p_1^{n_1} \ldots p_r^{n_r})$. Wir können dies auch anders schreiben:
$$\mathfrak{a} = (p_1)^{n_1} \cap \cdots \cap (p_r)^{n_r} = (p_1^{n_1}) \cap \cdots \cap (p_r^{n_r}).$$
2. Kann man die Zerlegung von eben auf allgemeine noethersche Ringe verallgemeinern? $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ mit speziellen bzw. geeigneten Idealen $\mathfrak{q}_i$?
3. Die Durchschnittsdarstellung hat folgenden Vorteil:
$$f \in \mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \quad \Longleftrightarrow \quad f \in \mathfrak{q}_i \text{ für alle } i.$$
Bei einer Produktdarstellung ist dies i.a. nicht der Fall.
4. Daß sich nicht jedes Ideal als Durchschnitt von Primidealen darstellen läßt, zeigt schon obiges Beispiel $A = \mathbf{Z}$.
5. Für das Ideal $\mathfrak{a} = (x^2, y)$ in $A = k[x, y]$ gilt: $\mathfrak{m} = (x, y)$ ist das einzige Primideal, das $\mathfrak{a}$ enthält, aber $\mathfrak{m}^2 \subset \mathfrak{a}$. Das Ideal ist also nicht Durchschnitt von Potenzen von Primidealen. D.h. man kann i.a. nicht hoffen, daß ein Ideal Durchschnitt von Potenzen von Primidealen ist wie in $\mathbf{Z}$.
6. Im Fall $A = \mathbf{Z}$ und $\mathfrak{a} = (p_1^{n_1}) \cap \cdots \cap (p_r^{n_r})$ hatten die einfachen Bausteine die Form $(p_i^{n_i})$. Für diese gilt $Ass_{\mathbf{Z}}(\mathbf{Z}/(p_i^{n_i})) = \{(p_i)\}$. Dies wird verallgemeinert.

Statt für Ideale in A entwickeln wir die Theorie gleich für Untermoduln eines (endlich erzeugten) Moduls M.

DEFINITION. Ein Untermodul N eines A-Moduls M heißt $\mathfrak{p}$-primär, wenn $Ass(M/N) = \{\mathfrak{p}\}$. Im Fall $M = A$ und $N = \mathfrak{q}$, $\mathfrak{q}$ ein Ideal in A, nennt man $\mathfrak{q}$ auch ein Primärideal und $\mathfrak{p}$ zu $\mathfrak{q}$ assoziiert.

Wir wollen jetzt überlegen, wann ein Ideal $\mathfrak{q} \subseteq A$ ein $\mathfrak{p}$-primäres Ideal ist. Sei zunächst $\mathfrak{q}$ ein $\mathfrak{p}$-primäres Ideal. Da die minimalen Primideale von $Ass(A/\mathfrak{q})$ und $supp(A/\mathfrak{q}) = V(\mathfrak{q})$ übereinstimmen, ist $V(\mathfrak{q}) = V(\mathfrak{p})$, also $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Da jedes Annullatorideal $\neq A$ in einem assoziierten Primideal enthalten ist, gilt weiter für $x \in A, x \notin \mathfrak{q}$: $ann(\overline{x}) \subseteq \mathfrak{p}$. Anders ausgedrückt: Sind $x, y \in A$ mit $xy \in \mathfrak{q}$ und $x \notin \mathfrak{q}$, so ist $y \in \mathfrak{p} = \sqrt{\mathfrak{q}}$, d.h. es gibt $n \geq 1$ mit $y^n \in \mathfrak{q}$. Damit haben wir die erste Hälfte des folgenden Satzes bewiesen:

SATZ. *Ein Ideal $\mathfrak{q} \subseteq A, \mathfrak{q} \neq A$ ist genau dann $\mathfrak{p}$-primär, wenn gilt:*
$$xy \in \mathfrak{q}, x \notin \mathfrak{q} \Rightarrow y^n \in \mathfrak{q} \text{ für ein } n \geq 1.$$
In diesem Fall ist $\mathfrak{p} = \sqrt{\mathfrak{q}}$.

Obige Charakterisierung dient auch oft zur Definition von primären Idealen.

Beweis: Der eine Richtung wurde bereits gezeigt. Sei umgekehrt obige Charakterisierung für $\mathfrak{q}$ gültig. Sei $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Dann ist nach Voraussetzung $\mathfrak{p} \neq A$. Sei $xy \in \mathfrak{p}$, also für ein n: $x^n y^n \in \mathfrak{q}$. Ist $x^n \in \mathfrak{q}$, so $x \in \mathfrak{p}$, andernfalls gibt es ein m mit $y^{nm} \in \mathfrak{q}$, d.h. $y \in \mathfrak{p}$. Also ist $\mathfrak{p}$ ein Primideal. Nun folgt aus
$$\emptyset \neq Ass(A/\mathfrak{q}) \subseteq supp(A/\mathfrak{q}) = V(\mathfrak{q}) = V(\sqrt{\mathfrak{q}}) = V(\mathfrak{p})$$
und der Tatsache, daß die minimalen Ideale in $supp$ und Ass übereinstimmen: $\mathfrak{p} \in Ass(\mathfrak{q})$. Nach Definition liegen aber nun alle Annulatoren $\neq A$ von $A/\mathfrak{q}$ in $\mathfrak{p}$, also folgt $Ass(A/\mathfrak{q}) = \mathfrak{p}$, da $\mathfrak{p}$ das einzige Primideal zwischen $\mathfrak{q}$ und $\mathfrak{p}$ ist. ■

Beispiele:

1. Ist $\mathfrak{m}$ ein maximales Ideal und $\mathfrak{q}$ ein Ideal mit $\sqrt{\mathfrak{q}} = \mathfrak{m}$, so gilt $\emptyset \neq Ass(A/\mathfrak{q}) \subseteq supp(A/\mathfrak{q}) = V(\mathfrak{q}) = V(\mathfrak{m}) = \{\mathfrak{m}\}$, also ist $\mathfrak{q}$ primär mit $\mathfrak{m}$ als assoziiertem Primideal.
2. Speziell sind alle Potenzen $\mathfrak{m}^n$, $n \geq 1$ eines maximalen Ideals $\mathfrak{m}$-primär. Aber nicht alle $\mathfrak{m}$-primären Ideale sind Potenzen von $\mathfrak{m}$, z.B. in $A = k[x, y]$ gilt für $\mathfrak{m} = (x, y)$:
$$\mathfrak{m}^2 \subset (x^2, y) \subset \mathfrak{m}.$$
Also ist (x^2, y) primär, aber keine Potenz von $\mathfrak{m}$.

3. Im allgemeinen folgt aber aus $\sqrt{\mathfrak{a}} = \mathfrak{p} \in Spec(A)$ noch nicht, daß $\mathfrak{a}$ primär ist. Selbst Potenzen von $\mathfrak{p}$ müssen nicht primär sein. Beide Aussagen zeigt folgendes Beispiel:
Sei $A = k[x,y,z]/(xy - z^2)$ und $\mathfrak{p} = (x,z)$. Wegen $A/\mathfrak{p} \simeq k[y]$ ist $\mathfrak{p} \in Spec(A)$. Wir betrachten $\mathfrak{a} = \mathfrak{p}^2$. Es ist $xy \in \mathfrak{a}$, $x \notin \mathfrak{a}$, aber auch $y \notin \mathfrak{p}$, also ist $\mathfrak{p}^2$ nicht primär. Natürlich kann man dies auch anders sehen:
$$A/\mathfrak{p}^2 = k[x,y,z]/(x^2, xy, xz, z^2).$$
Dann gilt in $A/\mathfrak{p}^2$: $ann(\overline{x}) = (x,y,z)$, d.h. $(x,y,z) \in Ass(A/\mathfrak{p}^2)$.

SATZ. *Sind N_1 und N_2 $\mathfrak{p}$-primäre Untermoduln von M, so auch $N_1 \cap N_2$.*

Beweis: Wir haben die exakte Sequenz
$$0 \to M/N(N_1 \cap N_2) \to M/N_1 \oplus M/N_2,$$
also gilt
$$\emptyset \neq Ass(M/N) \subseteq Ass(M/N_1 \oplus M/N_2) = Ass(M/N_1) \cup Ass(M/N_2) = \{\mathfrak{p}\},$$
wie behauptet. ■

Unser Ziel ist es jetzt einen Untermodul N von M als Durchschnitt primären Untermoduln zu schreiben. Um die Existenz zu sichern, gehen wir einen kleinen Umweg.

Ein Untermodul $N \subseteq M, N \neq M$ heißt irreduzibel, wenn aus $N = N_1 \cap N_2$ folgt $N_1 = N$ oder $N_2 = N$. Andernfalls heißt N reduzibel.

SATZ. *Jeder Untermodul N eines endlich erzeugten Moduls M ist Durchschnitt von endlich vielen irreduziblen Untermoduln N_i:*
$$N = N_1 \cap \cdots \cap N_r.$$
Im Fall $N = M$ ist $r = 0$.

Beweis: Sei S die Menge der Untermoduln von M, die sich nicht als endlicher Durchschnitt von irreduziblen Untermoduln schreiben lassen. Ist $S = \emptyset$, so sind wir fertig. Ist $S \neq \emptyset$, so enthält S ein maximales Element N, da M noethersch ist. Natürlich ist $N \neq M$. Wegen $N \in S$ ist N insbesondere reduzibel, d.h. $N = N_1 \cap N_2$ mit $N \subset N_1$ und $N \subset N_2$. Also $N_1, N_2 \notin S$, d.h. N_1 und N_2 sind endliche Durchschnitte von irreduziblen Untermoduln, und damit auch N: ein Widerspruch. Also tritt der Fall $S \neq \emptyset$ nicht ein. ■

Beispiel: Sei k ein Körper und V ein endlich dimensionaler k-Vektorraum der Dimension $n \geq 1$. Die irreduziblen Untervektoräume sind genau die der Dimension $n-1$. Jeder Untervektorraum ist Durchschnitt von endlich vielen Unterräumen der Dimension $n-1$, die Darstellung ist aber i.a. nicht eindeutig. Andererseits ist jeder Unterraum $U \neq V$ primär, da $Spec(k)$ einelementig ist.

Wir müssen jetzt die irreduziblen Untermoduln von M untersuchen.

LEMMA. *Ist N ein irreduzibler Untermodul von M, so besteht $Ass(M/N)$ aus genau einem Primideal, d.h. N ist primär.*

Beweis: Wegen $M/N \neq 0$ ist $Ass(M/N) \neq \emptyset$. Angenommen, es gibt zwei Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \in Ass(M/N)$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Dann gibt es Untermoduln $U_1, U_2 \subseteq M/N$ mit $U_i \simeq A/\mathfrak{p}_i$, insbesondere $U_i \neq 0$. Für $x \in U_i, x \neq 0$ ist $ass(x) = \mathfrak{p}_i$. Damit folgt sofort $U_1 \cap U_2 = 0$. Ist V_i das Urbild von U_i unter der Abbildung $M \to M/N$, so gilt $V_1 \cap V_2 = N$, $V_1, V_2 \neq N$, also ist N reduzibel, ein Widerspruch zur Voraussetzung. Also ist $Ass(M/N)$ einelementig. ■

Bemerkung: Daß nicht jeder primäre Untermodul irreduzibel sein muß, haben wir bereits gesehen im Fall, daß $A = k$ ein Körper ist und M ein endlich dimensionaler k-Vektorraum. Ein weiterer Hinweis ist das Lemma: Q_1, Q_2 $\mathfrak{p}$-primär impliziert $Q_1 \cap Q_2$ $\mathfrak{p}$-primär.

DEFINITION. Sei jetzt M ein endlich erzeugter Modul eines noetherschen Rings A und N ein Untermodul. Eine Darstellung
$$N = Q_1 \cap \cdots \cap Q_r$$
mit primären Moduln Q_i heißt Primärzerlegung von N.

Sei N Untermodul eines endlich erzeugten Moduls M. Dann können wir schreiben

$$N = N_1 \cap \cdots \cap N_r$$

mit irreduziblen Untermoduln N_i. Wir haben gesehen, daß die N_i primär sind.

Folglich: Jeder Untermodul eines endlich erzeugten A-Moduls besitzt eine Primärzerlegung.

Sei nun $N = Q_1 \cap \cdots \cap Q_r$ eine Primärzerlegung von N mit $Ass(M/Q_i) = \{\mathfrak{p}_i\}$. Indem wir Q_i's zusammenfassen bzw. zusammenschneiden, die zum gleichen Primideal assoziiert sind, können wir annehmen $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i \neq j$. Weiter können wir auf überflüssige Q_i's verzichten, die nichts an der Zerlegung ändern, d.h. wir können annehmen $N \neq Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_r$ für alle i.

DEFINITION. Eine Primärzerlegung $N = Q_1 \cap \cdots \cap Q_r$ mit $Ass(M/Q_i) = \{\mathfrak{p}_i\}$ heißt irredundant, wenn alle assoziierten Primideale verschieden sind und auf keines der Q_i verzichtet werden kann. Q_i heißt $\mathfrak{p}_i$-primäre Komponente von N.

Wir haben bereits überlegt:

FOLGERUNG. *In einem endlich erzeugten A-Modul besitzt jeder Untermodul eine irredundante Primärzerlegung.*

Beispiel: Wir betrachten das Ideal $\mathfrak{a} = (x^2, xy)$ in $k[x, y]$. Wir haben bereits gesehen, daß $A/\mathfrak{a}$ zwei assoziierte Primideale besitzt, nämlich (x) und (x, y). Man rechnet nach, daß gilt

$$(x^2, xy) = (x) \cap (x^2, y).$$

Also hat man eine irredundante Primärzerlegung. Allerdings ist $(x^2, xy) = (x) \cap (x^2, xy, y^2)$ auch eine irredundante Primärzerlegung. Also ist die Primärzerlegung nicht eindeutig.

Wir wollen aber doch noch sehen, welche Eindeutigkeitsaussagen man bei der Primärzerlegung machen kann.

SATZ. *Sei M ein endlich erzeugter A-Modul, N ein Untermodul und*

$$N = Q_1 \cap \cdots \cap Q_r$$

eine irredundante Primärzerlegung von N mit $Ass(M/Q_i) = \{\mathfrak{p}_i\}$. Dann gilt:

$$Ass(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\},$$

d.h. die $\mathfrak{p}_i$'s sind eindeutig bestimmt durch N.

Beweis: Zunächst induziert $M \to M/Q_1 \oplus \cdots \oplus M/Q_r$ eine Injektion $M/(Q_1 \cap \cdots \cap Q_r) \hookrightarrow M/Q_1 \oplus \cdots \oplus M/Q_r$, woraus folgt

$$Ass(M/N) \subseteq Ass(M/Q_1) \cup \cdots \cup Ass(M/Q_r) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

Wir betrachten nun $\phi : Q_2 \cap \cdots \cap Q_r \to M/Q_1$. Dann ist $kern(\phi) = Q_1 \cap Q_2 \cap \cdots \cap Q_r = N$, also haben wir

$$Q_2 \cap \cdots \cap Q_r/N \hookrightarrow M/Q_1,$$

also $Ass(Q_2 \cap \cdots \cap Q_r/N) \subseteq Ass(M/Q_1) = \{\mathfrak{p}_1\}$, also $Ass(Q_2 \cap \cdots \cap Q_r/N) = \{\mathfrak{p}_1\}$. Nun ist $Q_2 \cap \cdots \cap Q_r/N \hookrightarrow M/N$, also folgt $\mathfrak{p}_1 \in Ass(M/N)$. Durch Permutieren der Indizes erhält man auch $\mathfrak{p}_i \in Ass(M/N)$, woraus dann die Behauptung folgt. ■

LEMMA. *Sei M ein endlich erzeugter A-Modul, Q ein $\mathfrak{p}$-primärer Untermodul, $\mathfrak{q} \in Spec(A)$ und $\phi : M \to M_\mathfrak{q}$ die natürliche Abbildung, insbesondere $N_\mathfrak{q} = \phi(N)$. Dann gilt:*

1. *Ist $\mathfrak{p} \not\subseteq \mathfrak{q}$, so ist $M_\mathfrak{q} = Q_\mathfrak{q}$.*
2. *Ist $\mathfrak{p} \subseteq \mathfrak{q}$, so ist $Q = \phi^{-1}(Q_\mathfrak{q})$.*

Beweis: Zunächst ist $(M/Q)_{\tilde{\mathfrak{p}}} \simeq M_{\tilde{\mathfrak{p}}}/Q_{\tilde{\mathfrak{p}}}$, also

$$\begin{aligned} Ass_{A_{\tilde{\mathfrak{p}}}}(M_{\tilde{\mathfrak{p}}}/Q_{\tilde{\mathfrak{p}}}) &= Ass_{A_{\tilde{\mathfrak{p}}}}((M/Q)_{\tilde{\mathfrak{p}}}) = Ass_A(M/Q) \cap \{\tilde{\mathfrak{p}}' \in Spec(A) : \tilde{\mathfrak{p}}' \subseteq \tilde{\mathfrak{p}}\} = \\ &= \{\mathfrak{p}\} \cap \{\tilde{\mathfrak{p}}' \subseteq \tilde{\mathfrak{p}}\} \end{aligned}$$

Ist $\mathfrak{p} \not\subseteq \tilde{\mathfrak{p}}$, so ist also $Ass_{A_{\tilde{\mathfrak{p}}}}(M_{\tilde{\mathfrak{p}}}/Q_{\tilde{\mathfrak{p}}}) = \emptyset$, also $M_{\tilde{\mathfrak{p}}} = Q_{\tilde{\mathfrak{p}}}$.
Sei nun $\mathfrak{p} \subseteq \tilde{\mathfrak{p}}$. Wir betrachten $\mu : M/Q \to (M/Q)_{\tilde{\mathfrak{p}}}$. Angenommen, μ ist nicht injektiv; dann gibt es $x \in M/Q, x \neq 0$ mit $\mu(x) = 0$, d.h. es gibt ein $s \notin \tilde{\mathfrak{p}}$ mit $sx = 0$. Dann ist s aber ein Nullteiler von M/Q, also $s \in \mathfrak{p} \subseteq \tilde{\mathfrak{p}}$, was einen Widerspruch liefert. Also ist μ injektiv. Wegen $Q \subseteq \phi^{-1}Q_{\tilde{\mathfrak{p}}}$ und $\mu(\phi^{-1}Q_{\tilde{\mathfrak{p}}}/Q) = 0$ folgt damit sofort $Q = \phi^{-1}(Q_{\tilde{\mathfrak{p}}})$. ■

Wir wollen das Lemma jetzt anwenden: Sei

$$N = Q_1 \cap \cdots \cap Q_r$$

eine irredundante Primärzerlegung von N mit $Ass(M/Q_i) = \{\mathfrak{p}_i\}$. Sei $\mathfrak{p} \in Ass(M/Q)$. Wir lokalisieren in $\mathfrak{p}$:

$$N_{\mathfrak{p}} = \cap\{(Q_i)_{\mathfrak{p}} : \mathfrak{p}_i \subseteq \mathfrak{p}\}.$$

Ist $\mathfrak{p}$ minimales Primideal in $Ass(M/N)$ und $\mathfrak{p}_j = \mathfrak{p}$, so wird

$$N_{\mathfrak{p}} = (Q_j)_{\mathfrak{p}},$$

also

$$\phi_{\mathfrak{p}_j}^{-1}(N_{\mathfrak{p}}) = \phi_{\mathfrak{p}_j}^{-1}((Q_j)_{\mathfrak{p}}) = Q_j.$$

Damit haben wir folgenden Satz bewiesen:

SATZ. *Sei $N = Q_1 \cap \cdots \cap Q_r$ eine irredundante Primärzerlegung von N, $Ass(M/Q_i) = \{\mathfrak{p}_i\}$. Die zu den isolierten zu M/Q assoziierten Primidealen gehörigen Primärkomponenten sind eindeutig bestimmt. Geauer: Ist $\mathfrak{p}_i$ isoliert und $\phi_i : M \to M_{\mathfrak{p}_i}$ die kanonische Abbildung, so ist $Q_i = \phi_i^{-1}(N_{\mathfrak{p}_i}) = \phi_i^{-1}(\phi_i(N))$.*

Beispiel: Wir betrachten nochmals $A = k[x, y]$ und $\mathfrak{a} = (x^2, xy)$. Wir kennen die assoziierten Primideale, nämlich (x) und (x, y). Wählt man $\mathfrak{m} = (x, y - 1)$ und lokalisiert in $\mathfrak{m}$: $\phi : A \to A_{\mathfrak{m}}$, so ist $\phi^{-1}(\mathfrak{a}A_{\mathfrak{m}})$ die (x)-primäre Komponente von $\mathfrak{a}$. Nun ist y Einheit in $A_{\mathfrak{m}}$, also:

$$(x^2, xy)A_{\mathfrak{m}} = xA_{\mathfrak{m}}, \text{ also } \phi^{-1}(\mathfrak{a}A_{\mathfrak{m}}) = (x),$$

da sowohl (x) als auch $\phi^{-1}(\mathfrak{a}A_{\mathfrak{m}})$ (x)-primär sind. Dies kannten wir natürlich schon: $(x^2, xy) = (x) \cap (x^2, xy, y^2)$ ist eine Primärzerlegung von (x^2, xy).

Problem: Wie findet man konstruktiv die Primärzerlegung eines Ideals?

Wir wollen kurz zeigen, wie man mit Hilfe von Gröbner-Basen den Durchschnitt zweier Ideale in einem Polynomring berechnen kann. Eigentlich gehört dies zum Paragraphen über Gröbner-Basen.

SATZ. *Sei $A = k[x_1, \ldots, x_n]$ Polynomring über einem Körper und $\mathfrak{a} = (f_1, \ldots, f_r)$ und $\mathfrak{b} = (g_1, \ldots, g_s)$ zwei Ideale in A. Dann gilt:*

$$\mathfrak{a} \cap \mathfrak{b} = (tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s) \cap k[x_1, \ldots, x_n],$$

wo t eine weitere Unbestimmte ist.

Beweis: Sei $\mathfrak{c}$ die rechte Seite der behaupteten Gleichung.
$\subseteq$: Sei $h = \sum a_i f_i = \sum b_j g_j \in \mathfrak{a} \cap \mathfrak{b}$, mit $a_i, b_j \in A$. Dann gilt

$$h = th + (1-t)h = \sum A_i(tf_i) + \sum B_j((1-t)g_j) \in \mathfrak{c}.$$

$\supseteq$: Sei $h \in \mathfrak{c}$, d.h.

$$h = \sum A_i t f_i + \sum B_j (1-t) g_j$$

mit $A_i, B_j \in k[x_1, \ldots, x_n, t]$. Setzt man jetzt $t = 0$ ein, so folgt $h \in \mathfrak{b}$, setzt man $t = 1$ ein, so folgt $h \in \mathfrak{a}$, also $h \in \mathfrak{a} \cap \mathfrak{b}$. ■

Bemerkung: Berechnet man die Gröbner-Basis von $[tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s]$ bzgl. der lexikographischen Ordnung $t > x_1 > \cdots > x_n$, so erhalten wir sofort eine Gröbner-Basis für $\mathfrak{a} \cap \mathfrak{b}$, indem wir alle Polynome der Basis nehmen, die kein t enthalten.

Beispiel: Sei $A = \mathbf{C}[x,y,z]$ und $\mathfrak{p}_1 = (x,y), \mathfrak{p}_2 = (x,z)$. Geometrisch entsprechen den Primidealen $\mathfrak{p}_1$ und $\mathfrak{p}_2$ zwei Geraden. Wir wollen die Primärzerlegung von $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$ finden.

1. Die Nullstellenmenge $N(\mathfrak{p}_1\mathfrak{p}_2)$ ist die Vereinigung der beiden Geraden $N(\mathfrak{p}_1)$ und $N(\mathfrak{p}_2)$. Es gilt: $\mathfrak{p}_1\mathfrak{p}_2 = (x^2, xy, xz, yz)$.
2. Wegen $supp(A/\mathfrak{a}) = V(\mathfrak{a}) = V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2)$ sind $\mathfrak{p}_1$ und $\mathfrak{p}_2$ assoziierte Primideale zu $A/\mathfrak{a}$.
3. $\mathfrak{p}_1 \cap \mathfrak{p}_2 = (x, yz)$ ist leicht zu überlegen. (Eine Gröbner-Basis von $[tx, ty, (1-t)x, (1-t)y]$ bzgl. lexikographischer Ordnung mit $t > x > y > z$ ist $[ty, tz - z, x, yz]$.)
4. Es ist $\mathfrak{p}_1\mathfrak{p}_2 \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \subset \mathfrak{m}$, wo $\mathfrak{m} = (x,y,z)$. Mit $\mathfrak{m}^2 = (x^2, xy, xz, y^2, yz, z^2)$ sieht man $\mathfrak{p}_1\mathfrak{p}_2 \subset \mathfrak{m}^2$. Wir berechnen $\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$: Eine Gröbner-Basis von $[tx, tyz, (1-t)x^2, (1-t)xy, (1-t)xz, (1-t)y^2, (1-t)yz, (1-t)z^2]$ ist $[tx, ty^2 - y^2, tz^2 - z^2, x^2, xy, xz, yz]$, also haben wir die Primärzerlegung von $\mathfrak{p}_1\mathfrak{p}_2$:
$$\mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2.$$

Wir geben noch ein Beispiel um zu zeigen, wie eingebettete Punkte natürlich auftreten:

Beispiel: Sei $\mathfrak{a}_t = (x) \cap (x-t, y) \subseteq \mathbf{C}[x,y]$. Dann ist $X_t = N(\mathfrak{a}_t) = \{x = 0\} \cup \{(t,0)\}$, d.h. X_t ist mengentheoretisch die y-Achse und ein Punkt. Für $t = 0$ bleibt nur die y-Achse übrig. Was passiert algebraisch?
$$\mathfrak{a}_t = (x) \cap (x-t, y) = (x(x-t), xy) = (x^2 - tx, xy).$$
Setzt man jetzt $t = 0$ ein, so hat man (x^2, xy), also die y-Achse und einen eingebetteten Punkt.

Zum Schluß wollen wir noch zwei Anwendungen von Primärzerlegungen geben.

Symbolische Potenzen: Sei A ein noetherscher Ring und $\mathfrak{p} \in Spec(A)$. Wir haben bereits ein Beispiel gesehen, wo $\mathfrak{p}^2$ nicht primär war. Sei $n \geq 1$. Es ist
$$\emptyset \neq Ass_A(A/\mathfrak{p}^n) \subseteq supp(A/\mathfrak{p}^n) = V(\mathfrak{p}^n) = V(\mathfrak{p}),$$
also ist $\mathfrak{p}$ minimales assoziiertes Primideal zu $\mathfrak{p}^n$, d.h. die $\mathfrak{p}$-primäre Komponente von $\mathfrak{p}^n$ ist eindeutig bestimmt. Wir nennen sie $\mathfrak{p}^{(n)}$ (symbolische Potenz):
$$\mathfrak{p}^n = \mathfrak{p}^{(n)} \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r,$$
wo $\mathfrak{q}_i$ zu Primidealen $\mathfrak{p}_i \supset \mathfrak{p}$ assoziiert sind. Ist $\phi : A \to A_\mathfrak{p}$ die Lokalisierung in $\mathfrak{p}$, so haben wir gesehen
$$\mathfrak{p}^{(n)} = \phi^{-1}(\mathfrak{p}^n A_\mathfrak{p}),$$
was man auch $\mathfrak{p}^{(n)} = A \cap \mathfrak{p}^n A_\mathfrak{p}$ schreibt und richtig zu verstehen ist. Genauso gilt natürlich: Ist $\mathfrak{m}$ ein (maximales) Primideal, das $\mathfrak{p}$ als einziges assoziiertes Primideal enthält, so ist $\mathfrak{p}^{(n)} = \phi_\mathfrak{m}^{-1}(\mathfrak{p}^n A_\mathfrak{m})$.

Geometrische Interpretation der symbolischen Potenzen:

SATZ. *Sei k algebraisch abgeschlossen, $\mathfrak{p}$ ein Primideal in $A = k[x_1, \ldots, x_n]$. Dann gilt:*
$$\mathfrak{p}^{(N)} = \{f \in A : \frac{\partial^{i_1 + \cdots + i_n} f}{\partial x_1^{i_1} \ldots \partial x_n^{i_n}} \in \mathfrak{p} \text{ für alle } i_1 + \cdots + i_n \leq N-1\}.$$

Mit anderen Worten: Ist $X = N(\mathfrak{p}) \subseteq k^n$ die durch die Polynome aus $\mathfrak{p}$ definierte Varietät, so besteht $\mathfrak{p}^{(N)}$ aus den Polynomen, deren Ableitungen bis zur Ordnung $N-1$ auf X verschwinden.

Beweisanfang: (Beweis bei Eisenbud.) Wir skizzieren nur den Fall $N = 2$. Sei
$$\mathfrak{q} = \{f \in \mathfrak{p} : \frac{\partial f}{\partial x_i} \in \mathfrak{p} \text{ für alle } i\}.$$

- Man sieht sofort: $\mathfrak{p}^2 \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. Insbesondere ist $\sqrt{\mathfrak{q}} = \mathfrak{p}$.
- Wir wollen zeigen, daß $\mathfrak{q}$ ein Primärideal ist. Sei $fg \in \mathfrak{q}$ aber $f \notin \mathfrak{q}$. Ist $f \notin \mathfrak{p}$, so gilt natürlich $g \in \mathfrak{p}$, was zu zeigen ist. Ist $f \in \mathfrak{p}$, so gibt es ein i mit $f_i \notin \mathfrak{p}$, wo f_i die partielle Ableitung nach x_i bezeichnet. Nun ist $(fg)_i \in \mathfrak{p}$, also $(fg)_i = fg_i + f_i g \in \mathfrak{p}$, also $g \in \mathfrak{p}$, was zu zeigen war.
- Damit sind $\mathfrak{q}$ und $\mathfrak{p}^{(2)}$ $\mathfrak{p}$-primäre Ideale. Können wir ein maximales Ideal $\mathfrak{m}$ finden, das $\mathfrak{p}$ als einziges assoziiertes Primideal enthält, mit $\mathfrak{q}_\mathfrak{m} = \mathfrak{p}_\mathfrak{m}^2$, so folgt schon $\mathfrak{q} = \mathfrak{p}^{(2)}$ und wir sind fertig. Für die weitere lokale Untersuchung fehlen uns noch die Hilfsmittel. ■

Anhang: Dedekindringe

DEFINITION. Ein Dedekindring ist ein ganz abgeschlossener noetherscher Integritätsring der Dimension 1.

Typische Beispiele:

1. (Zahlentheorie) Ist K eine endliche Körpererweiterung von $\mathbf{Q}$ und A der ganze Abschluß von $\mathbf{Z}$ in K, so ist A ein Dedekindring. (Nur daß A noethersch ist, muß man sich noch überlegen.) A ist der Ring der ganzen Zahlen von K.
2. (Algebraische Geometrie) Sind $a_1, \ldots, a_n \in \mathbf{C}$ alle verschieden, so ist der Ring $A = \mathbf{C}[x, \sqrt{(x-a_1)\ldots(x-a_n)}]$ ein Dedekindring. $Spec(A)$ ist der affine Teil einer elliptischen ($n = 3, 4$) bzw. hyperelliptischen ($n \geq 4$) Kurve.

Sei A ein Dedekindring.

1. Ist $\mathfrak{p}$ ein maximales Ideal in A, so ist $A_\mathfrak{p}$ lokaler noetherscher ganz abgeschlossener Integritätsring, also ein diskreter Bewertungsring, wie wir schon gesehen haben. Jedes Ideal $\neq 0$ in $A_\mathfrak{p}$ hat die Gestalt $\pi^n A_\mathfrak{p} = \mathfrak{p}^n A_\mathfrak{p}$, wo π das Ideal $\mathfrak{p}A_\mathfrak{p}$ erzeugt.
2. Sei $\mathfrak{q}$ ein $\mathfrak{p}$-primäres Ideal. Dann gibt es ein $n \geq 1$, so daß gilt:
$$(\mathfrak{q})_\mathfrak{p} = (\mathfrak{p})_\mathfrak{p}^n.$$
Da auch $\mathfrak{p}^n$ $\mathfrak{p}$-primär ist, folgt nach einem Lemma sofort $\mathfrak{q} = \mathfrak{p}^n$, d.h. die $\mathfrak{p}$-primären Ideale in A sind genau die Potenzen von $\mathfrak{p}$.
3. Sei jetzt $\mathfrak{a} \subseteq A$ ein Ideal, o.E. $\mathfrak{a} \neq 0, A$. Dann lautet die Primärzerlegung also (unter Benutzung des chinesischen Restsatzes)
$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \cdots \cap \mathfrak{p}_r^{e_r} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r},$$
wo alle $\mathfrak{p}_i$ verschieden sind. Die Primärzerlegung ist eindeutig, da es aus Dimensionsgründen keine eingebetteten Komponenten geben kann.

Damit haben wir folgenden Satz bewiesen:

SATZ. *In einem Dedekindring ist jedes von* 0 *verschiedene Ideal ein Produkt von Primidealen. Die Darstellung ist eindeutig.*

Eine wichtige Rolle spielt dieser Satz in der Zahlentheorie: In den Ganzheitsringen von Zahlkörpern hat man i.a. nicht mehr eindeutige Primfaktorzerlegung, aber immerhin noch eindeutige Primidealzerlegung.

Beispiel: Der Ring $A = \mathbf{Z}[\sqrt{-5}]$ ist Dedekindring, aber nicht faktoriell. Man hat z.B. $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Wie erklärt man das? Kummer versucht dies durch Einführung idealer Zahlen zu erklären: Hätte man
$$2 \cdot 3 = (P_2 Q_3)(P_3 Q_3) = (P_2 P_3)(Q_2 Q_3) = (1+\sqrt{-5})(1-\sqrt{-5}),$$
so wäre die obige Beziehung verständlich. Dedekind führt Ideale ein:
$$\mathfrak{p}_2 = (2, 1+\sqrt{-5}), \quad \mathfrak{q}_2 = (2, 1-\sqrt{-5}), \quad \mathfrak{p}_3 = (3, 1+\sqrt{-5}), \quad \mathfrak{q}_3 = (3, 1-\sqrt{-5}).$$
Man zeigt schnell, daß dies Primideale sind. (Z.B.
$$\mathbf{Z}[\sqrt{-5}]/\mathfrak{p}_3 \simeq \mathbf{Z}[x]/(x^2+5, 3, 1+x) = \mathbf{Z}[x]/(x^2-1, 3, x+1) = \mathbf{Z}[x]/(x+1, 3) \simeq \mathbf{F}_3.)$$
Nun gilt
$$\mathfrak{p}_2\mathfrak{q}_2 = (4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6) = (2),$$
analog $\mathfrak{p}_3\mathfrak{q}_3 = (3)$, und
$$\mathfrak{p}_2\mathfrak{p}_3 = (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, (1+\sqrt{-5})^2) = (1+\sqrt{-5}),$$
analog $\mathfrak{q}_2\mathfrak{q}_3 = (1-\sqrt{-5})$. Damit lautet obige Beziehung für Ideale:
$$(2 \cdot 3) = \mathfrak{p}_2\mathfrak{q}_2 \cdot \mathfrak{p}_3\mathfrak{q}_3 = \mathfrak{p}_2\mathfrak{p}_3 \cdot \mathfrak{q}_2\mathfrak{q}_3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

KAPITEL 9

Artinsche Moduln und Ringe

Sei nun wieder A ein beliebiger kommutativer Ring. Wir wollen zunächst die Länge eines A-Moduls definieren. Dazu brauchen wir ein paar Vorbereitungen.

DEFINITION. Ein Modul $M \neq 0$ heißt einfach, wenn 0 und M die einzigen Untermoduls von M sind.

Ist M einfacher A-Modul und $x \in M, x \neq 0$, so ist $M = Ax \simeq A/ann(x)$. Damit folgt sofort:

LEMMA. *Ein Ring A ist genau dann einfach, wenn A ein Körper ist. Ein A-Modul M ist einfach, wenn $M \simeq A/\mathfrak{m}$ für ein maximales Ideal von A gilt.*

Sei $M \neq 0$ ein A-Modul. Eine Folge von Untermoduln

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0,$$

wo alle M_i/M_{i+1} einfach sind, heißt Kompositionsreihe von M. Die Zahl n heißt die Länge der Kompositionsreihe. Die Einfachkeit der Quotienten M_i/M_{i+1} bedeutet, daß es keine Moduln zwischen M_i und M_{i+1} gibt, d.h. die Kompositionsreihe läßt sich nicht mehr verfeinern. Wir definieren nun für einen A-Modul M:

$$\ell_A(M) = \inf\{n : M \text{ besitzt eine Kompositionsreihe der Länge } n\}.$$

Ist $\ell_A(M) < \infty$, so sagt man, M hat endliche Länge. $\ell_A(M) = \infty$ bedeutet, daß es keine Kompositionsreihe gibt.

LEMMA. *Sei M von endlicher Länge. Ist dann $N \subset M$, so gilt $\ell_A(N) < \ell_A(M)$.*

Beweis: Wir wählen eine Kompositionsreihe $M = M_0 \supset \cdots \supset M_n = 0$ von M mit $n = \ell(M)$. Sei $N_i = N \cap M_i$. Dann gilt $N_i/N_{i+1} \hookrightarrow M_i/M_{i+1}$. Da M_i/M_{i+1} einfach ist, gibt es nur zwei Fälle: $N_i = N_{i+1}$ oder N_i/N_{i+1} ist ebenfalls einfach. Durch Herausstreichen mehrfacher N_i's können wir also die Folge $N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = 0$ zu einer Kompositionsreihe verkürzen. Dann folgt sofort $\ell(N) \leq \ell(M)$. Würde gelten $\ell(N) = \ell(M)$, so gilt auch $N_i/N_{i+1} = M_i/M_{i+1}$ woraus zunächst $N_{n-1} = M_{n-1}$ und dann durch Induktion $N_i = M_i$ für alle i folgt, also $N = M$, ein Widerspruch zur Voraussetzung. Also gilt $\ell(N) < \ell(M)$. ■

FOLGERUNG. *Sei M von endlicher Länge. Dann sind alle Kompositionsreihen von M gleich lang.*

Beweis: Ist $M = M_0' \supset M_1' \supset \cdots \supset M_k' = 0$ irgendeine Kompositionsreihe von M, so folgt mit dem Lemma

$$\ell(M) = \ell(M_0') > \ell(M_1') > \cdots > \ell(M_{k-1}') \geq 1,$$

also $\ell(M) \geq k$. Da aber $\ell(M)$ die Länge einer minimalen Kompositionsreihe war, folgt daraus sofort $k = \ell(M)$ und damit die Behauptung. ■

Beispiel: Sei V ein k-Vektorraum. V hat genau dann endliche Länge, wenn V endlich dimensional ist. Offensichtlich gilt $\dim(V) = \ell_k(V)$.

Bemerkung: Ist $\mathfrak{m}$ ein maximales Ideal in A und M ein A-Modul mit $\mathfrak{m}M = 0$, so ist M in natürlicher Weise auch ein $A/\mathfrak{m}$-Vektorraum. Die A-Untermoduln und die $A/\mathfrak{m}$-Untervektorräume von M sind gleich. Daher ist $\ell_A(M) = \ell_{A/\mathfrak{m}}(M) = dim_{A/\mathfrak{m}}(M)$. Wir werden dies später ein paar mal anwenden.

FOLGERUNG. *Sei* $0 \to M' \to M \to M'' \to 0$ *eine exakte Folge von* A*-Moduln. Dann gilt*

$$\ell_A(M) = \ell_A(M') + \ell_A(M'').$$

Anders ausgedrückt: Ist N *Untermodul von* M*, so gilt*

$$\ell_A(M) = \ell_A(N) + \ell_A(M/N).$$

Insbesondere folgt damit: M *hat genau dann endliche Länge, wenn sowohl* N *als auch* M/N *von endlicher Länge sind.*

Beweis: Wir beweisen den Satz in der zweiten Formulierung. Wir können annehmen, daß N und M/N von endlicher Länge sind. Wähle eine Kompositionsreihe von N:

$$N = N_0 \supset N_1 \supset \cdots \supset N_n = 0.$$

Lifte eine Kompositionsreihe von M/N nach M:

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = N.$$

Dann ist

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = N_0 \supset N_1 \supset \cdots \supset N_n = 0$$

eine Kompositionsreihe für M der Länge $m+n$, woraus mit der letzten Folgerung die Behauptung folgt. ■

Wir geben noch eine Variante an:

FOLGERUNG. *Ist* M *ein* A*-Modul und*

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$$

eine Folge von Untermoduln, so gilt:

$$\ell(M) = \sum_{i=0}^{n-1} \ell(M_i/M_{i+1}).$$

Wir kommen nun zu artinschen Moduln. Sie werden analog zu noetherschen Moduln definiert.

DEFINITION. Ein A-Modul M heißt artinsch, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

1. Jede absteigende Folge von Untermoduln wird stationär, d.h. ist
$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots,$$
so gibt es ein n mit $M_n = M_{n+1} = M_{n+2} = \ldots$.
2. Jede nichtleere Menge von Untermoduln von M besitzt ein minimales Element.

Ein Ring A heißt artinsch, wenn A als A-Modul artinsch ist.

Die Äquivalenz in der Definition zeigt man wie bei noetherschen Moduln.

Beispiele:

1. Sei k ein Körper und V ein k-Vektorraum. Dann ist V genau dann artinisch, wenn V endlich dimensional ist.
Beweis: Ist V endlich dimensional und sind $U_1 \supset U_2$ Unterräume, so gilt $\dim(U_1) > \dim(U_2)$, woraus schnell die Behauptung folgt. Ist V unendlich dimensional, so wähle man linear unabhängige e_n für $n \in \mathbf{N}$ und definiere U_N als das Erzeugnis von $\{e_n : n \geq N\}$. Dann gilt $U_N \supset U_{N+1}$ und man erhält eine unendlich absteigende Kette von Untervektorräumen.
2. $\mathbf{Z}$ ist kein artinscher Ring, denn
$$(2) \supset (4) \supset (8) \supset (16) \supset \ldots.$$
3. Für $n \geq 1$ ist der $\mathbf{Z}$-Modul $\mathbf{Z}/(n)$ endlich, trivialerweise also artinsch.

Wie für noethersche Moduln zeigt man folgenden Satz mit Folgerungen:

SATZ. *Sei $0 \to M' \to M \to M'' \to 0$ eine exakte Sequenz von A-Moduln. Dann ist M genau dann artinsch, wenn M' und M'' artinsch sind.*

FOLGERUNG. *Sind $M_1, \ldots, M_n$ artinsche Moduln, so auch $M_1 \oplus \cdots \oplus M_n$.*

FOLGERUNG. *Ist A artinsch und M ein endlich erzeugter A-Modul, so ist auch M artinsch.*

FOLGERUNG. *Ist A artinsch und $\mathfrak{a}$ ein Ideal in A, so ist auch $A/\mathfrak{a}$ artinsch.*

SATZ. *Für einen A-Modul M gilt:*

$$\ell_A(M) < \infty \quad \Longleftrightarrow \quad M \text{ ist noethersch und artinsch.}$$

Beweis: $\Rightarrow$: Klar!
$\Leftarrow$: Wir definieren induktiv eine absteigende Folge $M = M_0 \supset M_1 \supset \ldots$ wie folgt: $M_0 = M$. Ist $M_i \neq 0$ bereits konstruiert, so enthält M_i einen maximalen Untermodul $M_{i+1} \neq M_i$, da M_i noethersch ist, d.h. M_i/M_{i+1} ist einfach. Da M artinsch ist, bricht die Folge ab und wir erhalten eine Kompositionsreihe. ■

Beispiel: Für einen k-Vektorraum V gilt also offensichtlich:

$$V \text{ noethersch} \iff V \text{ artinsch} \iff \ell_k(V) = \dim_k(V) < \infty.$$

Beispiele: Wir betrachten $\mathbf{Z}$-Moduln.

1. $M = \mathbf{Z}$ ist noethersch, aber nicht artinsch.
2. Sei $M = \mathbf{Z}_2/\mathbf{Z}$, wobei $\mathbf{Z}_2 = \{\frac{a}{2^n} : n \geq 1, a \in \mathbf{Z}\}$. Wir wollen zeigen, daß M artinsch, aber nicht noethersch ist.
   (a) Für jedes $n \geq 0$ ist $M_n = \frac{1}{2^n}\mathbf{Z}/\mathbf{Z}$ ein Untermodul von M. Offensichtlich gilt
   $$0 = M_0 \subset M_1 \subset M_2 \subset M_3 \subset \ldots,$$
   insbesondere ist M nicht noethersch.
   (b) Jedes $x \in M$, $x \neq 0$ hat die Form $x = \frac{a}{2^n}$ mit $n \geq 1$ und $a \in \mathbf{Z}$, a ungerade. Dann ist $\frac{a}{2^n}\mathbf{Z} = M_n$.
   Beweis: $\subseteq$: klar. $\supseteq$: Da a ungerade ist, gibt es $r, s \in \mathbf{Z}$ mit $2^n r + as = 1$, also gilt in M:
   $$s\frac{a}{2^n} = \frac{1 - 2^n}{2^n} = \frac{1}{2^n},$$
   woraus die Behauptung folgt.
   (c) Damit folgt sofort, daß die nichttrivialen Untermoduln von M genau die M_n's sind mit $n \geq 1$.
   (d) Dies impliziert, daß M artinsch ist.

Wir wollen jetzt artinsche Ringe untersuchen.

LEMMA. *Sei A ein Integritätsring. Genau dann ist A artinsch, wenn A ein Körper ist.*

Beweis: Ein Körper ist natürlich trivialerweise artinsch, da er keine trivialen Untermoduln hat. Sei umgekehrt A als artinsch vorausgesetzt. Sei $f \in A, f \neq 0$. Dann gilt

$$(f) \supseteq (f^2) \supseteq (f^3) \supseteq \ldots,$$

also gibt es ein n mit $(f^n) = (f^{n+1})$. Erzeugen nun in einem Integritätsring Elemente das gleiche Hauptideal, so unterscheiden sie sich nur um eine Einheit, also ist f eine Einheit. Da $f \neq 0$ beliebig war, folgt, daß A ein Körper ist. ■

LEMMA. *Sei A artinsch. Dann ist jedes $\mathfrak{p} \in Spec(A)$ maximales Ideal. Insbesondere hat A Dimension 0.*

Beweis: Sei $\mathfrak{p} \in Spec(A)$. Dann ist $A/\mathfrak{p}$ artinscher Integritätsring, also Körper. ■

LEMMA. *Ist A artinsch, so enthält A nur endlich viele maximale Ideale.*

Beweis: Sind $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_i$ verschiedene maximale Ideale, so gilt

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supset \ldots,$$

denn wäre $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_j = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{j-1}$, so $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{j-1} \subseteq \mathfrak{m}_j$, also für ein $k < j$: $\mathfrak{m}_k \subseteq \mathfrak{m}_j$, was nicht sein kann. Da A artinsch ist, bricht obige Folge ab, es folgt die Behauptung. ■

LEMMA. *Sei A artinsch mit $Spec(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. Dann ist das Nilradikal $\mathfrak{n} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ nilpotent, d.h. es gibt ein n mit $\mathfrak{n}^n = 0$.*

Beweis: Da A artinsch ist, gibt es ein $n \geq 1$ mit $\mathfrak{n}^n = \mathfrak{n}^{n+1} = \ldots$. Ist $\mathfrak{n}^n = 0$, sind wir fertig. Wir nehmen also an, daß $\mathfrak{n}^n \neq 0$ ist. Sei $J = \{\mathfrak{a} : \mathfrak{a}\mathfrak{n}^n \neq 0\}$. Wegen $\mathfrak{n} \in J$, ist J nicht leer, also gibt es ein minimales Element. Sei $\mathfrak{c}$ ein solches. Wähle $x \in \mathfrak{c}$ mit $x\mathfrak{n}^n \neq 0$. Wegen $(x) \subseteq \mathfrak{c}$ gilt dann bereits $(x) = \mathfrak{c}$. Nun ist $(x\mathfrak{n})\mathfrak{n}^n = x\mathfrak{n}^n \neq 0$, also folgt auch $x\mathfrak{n} = (x)$. D.h. es gibt ein $y \in \mathfrak{n}$ mit $x = xy$. Nun ist y nilpotent und

$$x = xy = (xy)y = xy^2 = (xy)y^2 = xy^3 = \cdots = 0,$$

was ein Widerspruch zu $x \neq 0$ ist. Also ist doch $\mathfrak{n}^n = 0$. ■

SATZ. *Ein Ring A ist genau dann artinsch, wenn $\ell_A(A) < \infty$ gilt. Insbesondere ist jeder artinsche Ring auch noethersch.*

Beweis: Gilt $\ell(A) < \infty$, so haben wir gesehen, daß A artinsch (und noethersch) ist. Sei umgekehrt vorausgesetzt, daß A artinsch ist. Sei $Spec(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ und $\mathfrak{n} = \mathfrak{m}_1 \ldots \mathfrak{m}_r$. Nach dem letzten Lemma gibt es ein n mit $\mathfrak{n}^n = 0$. Wir betrachten nun die Folge

$$\begin{array}{ccl} A & \supseteq & \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \ldots \mathfrak{m}_{r-1} \supseteq \\ \mathfrak{n} & \supseteq & \mathfrak{n}\mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{n}\mathfrak{m}_1 \ldots \mathfrak{m}_{r-1} \supseteq \\ & \cdots & \\ \mathfrak{n}^{n-1} & \supseteq & \mathfrak{n}^{n-1}\mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{n}^n = 0. \end{array}$$

Je zwei aufeinanderfolgende Folgenglieder haben die Form $M \supseteq M\mathfrak{m}_i$. Nun ist $M/M\mathfrak{m}_i$ ein $A/\mathfrak{m}_i$-Vektorraum, der artinsch ist, also endlich dimensional. Also $\ell(M/M\mathfrak{m}_i) < \infty$. Damit folgt aber sofort $\ell(A) < \infty$, also die Behauptung. ■

FOLGERUNG. *Ein Ring A ist genau dann artinsch, wenn A ein 0-dimensionaler noetherscher Ring ist.*

Beweis: Daß ein artinscher Ring noethersch ist und Dimension 0 hat, haben wir bereits gesehen. Sei nun umgekehrt vorausgesetzt, daß A noethersch ist mit Dimension 0. Dann ist $Spec(A)$ endlich, also $Spec(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. Das Nilradikal $\mathfrak{n} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \mathfrak{m}_1 \ldots \mathfrak{m}_r$ ist nilpotent, da A noethersch ist, d.h. es gibt ein $n \geq 1$ mit $\mathfrak{n}^n = 0$. Nun kann man obige Folge von Untermoduln von A anschreiben. Zwei aufeinanderfolgende Untermoduln haben wieder die Gestalt $M \supseteq M\mathfrak{m}_i$. Also ist $M/M\mathfrak{m}_i$ ein $A/\mathfrak{m}_i$-Vektorraum, und zwar ein endlich dimensionaler, da M noethersch ist. Also $\ell(M/M\mathfrak{m}_i) < \infty$ und damit $\ell(A) < \infty$, was mit dem Satz die Behauptung liefert. ■

Beispiel: Sei k algebraisch abgeschlossen, $f, g \in K[x, y]$ nicht konstante Polynome ohne gemeinsamen Faktor. Dann ist $A = k[x, y]/(f, g)$ ein artinscher Ring. Ist $Spec(A) = \{(x - a_i, y - b_i) : i = 1, \ldots, r\}$, so gilt

$$\{f = g = 0\} = \{(a_i, b_i) : i = 1, \ldots, r\}.$$

Beweis: Der Ring A ist noethersch, also bleibt zu zeigen, daß A Dimension 0 hat. Wäre $dim(A) \geq 1$, so gäbe es eine Primidealkette in $k[x, y]$ mit $(f, g) \subseteq \mathfrak{p} \subset \mathfrak{m}$, wobei $\mathfrak{m} = (x - a, y - b)$ und $\mathfrak{p} = (h)$ mit einem irreduziblen Polynom h. Dann folgte aber $h|f$ und $h|g$, ein Widerspruch. Also gilt $dim(A) = 0$ und damit ist A artinsch. Die maximalen Ideale in A entsprechen den maximalen Idealen $(x - a, y - b) \in k[x, y]$ mit $(f, g) \subseteq (x - a, y - b)$, was aber gleichwertig mit $f(a, b) = g(a, b) = 0$ ist. ■

Wir wollen nun noch etwas genauer artinsche Ringe anschauen.

1. Sei A ein artinscher Ring mit $Spec(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. Dann gilt auch $supp(A) = Spec(A)$, und da hierin alle Ideale minimal sind, folgt
$$Ass(A/(0)) = Ass(A) = Spec(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}.$$
2. Da A noethersch ist, hat 0 eine irredundante Primärzerlegung
$$0 = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r,$$
wo $\mathfrak{q}_i$ $\mathfrak{m}_i$-primär ist. Insbesondere gilt $\sqrt{\mathfrak{q}_i} = \mathfrak{m}_i$.
3. Die $\mathfrak{q}_i$'s sind paarweise teilerfremd, also liefert der chinesische Restsatz
$$A \simeq A/\mathfrak{q}_1 \times \cdots \times A/\mathfrak{q}_r.$$
$A/\mathfrak{q}_i$ enthält als einziges Primideal $\mathfrak{m}_i/\mathfrak{q}_i$, also ist $A/\mathfrak{q}_i$ ein lokaler artinscher Ring.
4. Da A noethersch ist folgt aus $\sqrt{\mathfrak{q}_i} = \mathfrak{m}_i$, daß es ein n gibt mit $\mathfrak{m}_i^n \subseteq \mathfrak{q}_i$.
Behauptung: Gilt $\mathfrak{m}_i^n \subseteq \mathfrak{q}_i$, so gilt schon $\mathfrak{m}_i^n = \mathfrak{q}_i$, (und damit $\mathfrak{q}_i = \mathfrak{m}_i^n = \mathfrak{m}_i^{n+1} = \ldots.$)
Beweis: Natürlich sind auch $\mathfrak{m}_i^n, \mathfrak{q}_1, \ldots, \mathfrak{q}_{i-1}, \mathfrak{q}_{i+1}, \ldots, \mathfrak{q}_r$ paarweise teilerfremd. Also gibt es nach dem chinesischen Restsatz ein $s \in A$ mit
$$s \equiv 1 \bmod \mathfrak{m}_i^n, \quad s \equiv 0 \bmod \mathfrak{q}_j \text{ für alle } j \neq i.$$
Ist $x \in \mathfrak{q}_i$, so ist $sx \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = 0$, also $sx = 0$, aber $x \equiv sx = 0 \bmod \mathfrak{m}_i^n$, d.h. $x \in \mathfrak{m}_i^n$, woraus die Behauptung folgt. ■

5. *Behauptung:* $A_{\mathfrak{m}_i} \simeq A/\mathfrak{q}_i$.
Beweis: Wir zeigen zunächst, daß die natürliche Abbildung $A \to A_{\mathfrak{m}_i}$ surjektiv ist. Dazu genügt es zu zeigen, daß für $t \in A, t \notin \mathfrak{m}_i$ der Bruch $\frac{1}{t}$ im Bild liegt. Da $A/\mathfrak{q}_i$ lokal mit maximalem Ideal $\mathfrak{m}_i/\mathfrak{q}_i$ ist, gibt es ein $u \in A$ mit $tu \equiv 1 \bmod \mathfrak{q}_i$. Wähle $s \in A$ mit $s \equiv 1 \bmod \mathfrak{q}_i$ und $s \equiv 0 \bmod \mathfrak{q}_j$ für $j \neq i$. Dann ist
$$s(tu - 1) \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = 0,$$
also in $A_{\mathfrak{m}_i}$: $\frac{1}{t} = \frac{u}{1}$.
Wir zeigen noch $\mathfrak{q}_i = Kern(A \to A_{\mathfrak{m}_i})$, woraus dann unsere Behauptung folgt:
$\subseteq$: Ist $x \in \mathfrak{q}_i$ und s wie eben, so ist $sx \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = 0$, also $sx = 0$. D.h. $\frac{x}{1} = 0$ in $A_{\mathfrak{m}_i}$.
$\supseteq$: Ist $x \in A$ mit $\frac{x}{1} = 0$, so existiert ein $v \in A$, $v \notin \mathfrak{m}_i$ mit $vx = 0$. Nun ist $vx \in \mathfrak{q}_i$. Da $v \notin \mathfrak{m}_i = \sqrt{\mathfrak{q}_i}$ muß gelten $x \in \mathfrak{q}_i$, was zu zeigen war.

Wir fassen nochmals zusammen:

SATZ. *Ein artinscher Ring ist isomorph zu einem endlichen Produkt lokaler artinscher Ringe. Genauer: Ist $Spec(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$, so gilt*
$$A \simeq A_{\mathfrak{m}_1} \times \cdots \times A_{\mathfrak{m}_r}.$$
Außerdem gilt für alle hinreichend großen n: $A_{\mathfrak{m}_i} \simeq A/\mathfrak{m}_i^n$.

Bemerkungen:

1. Natürlich ist umgekehrt ein endliches Produkt von artinschen Ringen wieder artinsch.
2. Ist A ein lokaler artinscher Ring mit maximalem Ideal $\mathfrak{m}$, so gilt $Spec(A) = \{\mathfrak{m}\}$. Das maximale Ideal ist dann gleichzeitig das Nilradikal.

Beispiele:

1. $\mathbf{Z}/(p^n)$ ist ein lokaler artinscher Ring.
2. $k[x,y]/(x^m, y^n)$ ist ein lokaler artinscher Ring.

Bemerkung: Sei wieder k algebraisch abgeschlossen und f, g zwei nichtkonstante Polynome aus $k[x,y]$ ohne gemeinsamen Teiler. Sei $A = k[x,y]/(f,g)$. Die einfachen A-Moduln sind $A/\mathfrak{m} \simeq k$. Ist $\mathfrak{m} \in Spec(A)$, so heißt $\ell_A(A_{\mathfrak{m}}) = \dim_k A_{\mathfrak{m}}$ die Schnittmultiplizität von f und g im Punkt $\mathfrak{m}$. Man kann auch zeigen, daß $\ell_A(A) = \dim_k A \leq grad(f) \cdot grad(g)$. (Gleichheit gilt, wenn sich f und g im Unendlichen nicht mehr schneiden.) Die Beziehung
$$\ell(A) = \ell(A_{\mathfrak{m}_1}) + \cdots + \ell(A_{\mathfrak{m}_r})$$
ist dann eine erste Version des Satzes von Bézout.

Bemerkung: Aus $\#Spec(A) = 1$ folgt noch nicht, daß A artinsch ist.

Beispiel: Sei $A = k[x_1, x_2, x_3, \dots]/(x_1, x_2^2, x_3^3, \dots)$. Offensichtlich hat A nur das Primideal $\mathfrak{m} = (x_1, x_2, x_3, \dots)$, das aber nicht endlich erzeugt ist. $\mathfrak{m}$ besteht aus lauter nilpotenten Elementen, ist aber selbst nicht nilpotent. Also ist A nicht noethersch, also auch nicht artinsch. Aber $Spec(A)$ ist einpunktig.

KAPITEL 10

Dimensionstheorie I

Erinnerung: Ist A und Ring und $\mathfrak{p} \in Spec(A)$, so ist die Höhe von $\mathfrak{p}$ definiert durch

$$h(\mathfrak{p}) = \sup\{n : \text{es gibt eine Primidealkette } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}\}.$$

Die Dimension von A ist

$$dim(A) = \sup\{h(\mathfrak{p}) : \mathfrak{p} \in Spec(A)\}.$$

Beispiel: Ist A ein Hauptidealring, so ist

$$Spec(A) = \{0\} \cup \{(p) : p \text{ irreduzibel}\}.$$

Also ist $h(0) = 0$ und $h((p)) = 1$. Insbesondere $dim(A) = 1$.

Bemerkung: Sei $\mathfrak{p} \in Spec(A)$ ein Primideal der Höhe n. Dann gibt es eine Primidealkette

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p},$$

woraus man in $Spec(A)$ erhält

$$Spec(A) \supseteq V(\mathfrak{p}_0) \supset V(\mathfrak{p}_1) \supset \cdots \supset V(\mathfrak{p}_n) = V(\mathfrak{p}).$$

Hier ist $V(\mathfrak{p}_0)$ eine irreduzible Komponente von $Spec(A)$, die $V(\mathfrak{p}_i)$'s eine Folge abgeschlossener irreduzibler Teilmengen. Man nennt daher $n = h(\mathfrak{p})$ auch Kodimension von $\mathfrak{p}$: $codim(\mathfrak{p}) = h(\mathfrak{p})$.

Beispiel: Wir betrachten in k^3 die Vereinigung der x,y-Ebene mit der z-Achse, d.h. die Nullstellenmenge von $(x,y) \cap (z) = (xz, yz)$. Algebraisch: Sei $A = k[x,y,z]/(xz,yz)$. Es gilt

$$Spec(A) = V((z)) \cup V((x,y)).$$

Wir betrachten die beiden Punkte $\mathfrak{m}_1 = (x-1, y-1, z)$ und $\mathfrak{m}_2 = (x, y, z-1)$. Wir finden die Primidealketten

$$(z) \subset (x-1, z) \subset \mathfrak{m}_1 \text{ und } (x,y) \subset (x,y,z-1)$$

und zugehörig

$$V((z)) \supset V((x-1,z)) \supset V(x-1, y-1, z)), \quad V((x,y)) \supset V((x,y,z-1)).$$

Man überlege sich zur Übung, daß die Primidealketten maximal sind. Dann ist also $h(\mathfrak{m}_1) = codim(\mathfrak{m}_1) = 2$ und $h(\mathfrak{m}_2) = codim(\mathfrak{m}_2) = 1$, wie auch die geometrische Vorstellung nahelegt.

Wir bestimmen nun zunächst die Dimension des Polynomrings über einem Körper.

SATZ. $dim(k[x_1, \ldots, x_n]) = n$.

Beweis: durch Induktion nach n. Die Fälle $n = 0$ und $n = 1$ kennen wir bereits. Sei nun $n \geq 2$ und $m = dim(k[x_1, \ldots, x_n])$. Es ist naheliegend, die Primidealkette

$$0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n)$$

zu betrachten. Sie hat Länge n, also gilt $m \geq n$.

1. Es gibt eine Primidealkette in $k[x_1, \ldots, x_n]$:

$$0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m.$$

Da die Kette maximal ist, ist $\mathfrak{p}_1$ ein minimales Primideal $\neq 0$. Wir haben bereits früher gesehen, daß in einem faktoriellen Ring diese Ideale Hauptideale sind: $\mathfrak{p}_1 = (f)$. f ist also ein irreduzibles Polynom.

2. Wie man Beweis des Noetherschen Normalisierungssatzes können wir einen linearen Koordinatenwechsel $(x_1 = x_1', x_2 = x_2' - c_2x_1', \ldots, x_n = x_n' - c_nx_1')$ durchführen und dann o.E. annehmen, daß f folgende Gestalt hat:
$$f = x_1^d + a_1(x_2, \ldots, x_n)x_1^{d-1} + \cdots + a_n(x_2, \ldots, x_n).$$
3. Der Ring $k[x_1, \ldots, x_n]$ ist also ganz über dem Ring $A = k[f, x_2, \ldots, x_n]$. Wir wissen daher $dim(A) = dim(k[x_1, \ldots, x_n])$, außerdem
$$0 \subset A \cap \mathfrak{p}_1 \subset \ldots A \cap \mathfrak{p}_m.$$
4. Die letzte Primidealkette reduzieren wir modulo (f) und erhalten in $A/(f) \simeq k[x_2, \ldots, x_n]$:
$$0 = 0 \subset \overline{A \cap \mathfrak{p}_2} \subset \cdots \subset \overline{A \cap \mathfrak{p}_m}.$$
Nach Induktionsannahme folgt $m - 1 \leq n - 1 = dim(A/(f)) = dim(k[x_2, \ldots, x_n])$, also $m \leq n$, was wir zeigen wollten. ■

Wir kommen nun zu einem wichtigen Satz, dem Krullschen Hauptidealsatz.

SATZ. *Sei A ein noetherscher Ring und $f \in A$. Dann hat jedes minimale Primoberideal $\mathfrak{p}$ von (f) Höhe ≤ 1. Ist f kein Nullteiler, so gilt $h(\mathfrak{p}) = 1$.*

Beweis: Sei also $\mathfrak{p}$ minimales Primoberideal von (f). Durch Lokalisieren können wir o.E. annehmen, daß A lokal ist mit maximalem Ideal $\mathfrak{p}$. Dann gibt es in $A/(f)$ nur ein Primideal, nämlich das Bild von $\mathfrak{p}$, also hat $A/(f)$ Dimension 0 und damit ist $A/(f)$ artinsch. Wir können annehmen, daß es ein Primideal $\mathfrak{q} \subset \mathfrak{p}$ gibt. Dann ist $f \notin \mathfrak{q}$. Wir betrachten die symbolischen Potenzen $\mathfrak{q}^{(n)} = \phi_{\mathfrak{q}}^{-1}(\mathfrak{q}^n A_{\mathfrak{q}})$. Die Folge
$$\mathfrak{q}^{(1)} + (f) \supseteq \mathfrak{q}^{(2)} + (f) \supseteq \mathfrak{q}^{(3)} + (f) \supseteq \ldots$$
wird modulo (f) stationär, da $A/(f)$ artinsch ist, und damit auch die Folge selbst (, da die Untermoduln von $A/(f)$ in Bijektion stehen zu den Untermoduln von A, die (f) enthalten), d.h. es gibt ein n mit
$$\mathfrak{q}^{(n)} + (f) = \mathfrak{q}^{(n+1)} + (f) = \ldots.$$
Für $a \in \mathfrak{q}^{(n)}$ gibt es also ein $b \in \mathfrak{q}^{(n+1)}$ und ein $c \in A$ mit $a = b + cf$. Dann ist $cf \in \mathfrak{q}^{(n)}$. Nun ist $\mathfrak{q}^{(n)}$ $\mathfrak{q}$-primär und $f \notin \mathfrak{q}$. Also folgt $c \in \mathfrak{q}^{(n)}$. Damit haben wir $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + f\mathfrak{q}^{(n)}$ und daher
$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + f\mathfrak{q}^{(n)}.$$
Da $f \in \mathfrak{p}$ können wir das Lemma von Nakayama anwenden und erhalten
$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}.$$
Jetzt lokalisieren wir in $\mathfrak{q}$ und erhalten
$$\mathfrak{q}^n A_{\mathfrak{q}} = \mathfrak{q}^{n+1} A_{\mathfrak{q}}.$$
Das Lemma von Nakayama liefert nun in diesem Ring $\mathfrak{q}^n A_{\mathfrak{q}} = 0$. Daher sind alle Elemente aus $\mathfrak{q}A_{\mathfrak{q}}$ nilpotent, also hat $A_{\mathfrak{q}}$ Dimension 0. Und damit folgt $h(\mathfrak{p}) = 1$. ■

Bemerkungen:

1. Läßt man noethersch in der Voraussetzung des Krullschen Hauptidealsatzes weg, so stimmt die Folgerung im allgemeinen nicht mehr. (Siehe Übungsaufgabe 49.)
2. Wir geben eine geometrische Interpretation des Satzes im Fall, daß A ein Integritätsring ist. Sei $f \in A, f \neq 0, f \notin A^\times$. Dann hat man in $Spec(A)$ eine Zerlegung in irreduzible Komponenten:
$$V(f) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r).$$
Die $\mathfrak{p}_i$'s sind dabei genau die minimalen Primoberideale von (f). Der Krullsche Hauptidealsatz besagt nun, daß $codim(\mathfrak{p}_i) = h(\mathfrak{p}_i) = 1$ ist, d.h. die $V(\mathfrak{p}_i)$ sind abgeschlossene irreduzible Teilmengen der Kodimension 1, man nennt so etwas auch Hyperflächen.
3. Umgekehrt gilt natürlich nicht, daß jedes Primideal der Höhe ≤ 1 von einem Element erzeugt wird.

Beispiel: Der Ring $A = \mathbf{Z}[\sqrt{-5}]$ ist ein Dedekindring, hat Dimension 1, $\mathfrak{p} = (2, 1+\sqrt{-5})$ ist ein Primideal der Höhe 1, aber kein Hauptideal.

Wir können aber die Ringe charakterisieren, in denen jedes Primideal der Höhe 1 ein Hauptideal ist:

SATZ. *Ein noetherscher Integritätsring A ist genau dann faktoriell, wenn jedes Primideal der Höhe 1 ein Hauptideal ist.*

Beweis: Zunächst ist 0 das einzige Primideal der Höhe 0.
$\Rightarrow$: Sei A faktoriell und $\{p_i : i \in I\}$ ein Repräsentantensystem der irreduziblen Elemente. Jedes (p_i) ist Primideal. Ist $\mathfrak{p} \neq 0$ ein Primideal der Höhe 1, so gibt es ein Element $\prod p_i^{n_i} \in \mathfrak{p}$, also gibt es ein j mit $p_j \in \mathfrak{p}$, d.h. $0 \subset (p_j) \subseteq \mathfrak{p}$. Daraus folgt $\mathfrak{p} = (p_j)$.
$\Leftarrow$: Jedes Primideal der Höhe 1 sei jetzt Hauptideal. Es genügt zu zeigen: Jedes irreduzible Element a erzeugt ein Primideal. Sei $\mathfrak{p}$ ein minimales Primoberideal von (a). Nach dem Krullschen Hauptidealsatz hat $\mathfrak{p}$ Höhe 1. Also ist $\mathfrak{p}$ Hauptideal: $\mathfrak{p} = (p)$. Es folgt $(a) \subseteq (p)$, d.h. $a = bp$ mit $b \in A$. Da a irreduzibel ist, p keine Einheit, muß b Einheit sein, d.h. $(a) = (p) = \mathfrak{p}$, was wir zeigen wollten. ■

Wir geben jetzt eine Verallgemeinerung des Krullschen Hauptidealsatzes an:

SATZ. *Ist A ein noetherscher Ring, $f_1, \ldots, f_n \in A$ und $\mathfrak{p}$ ein minimales Primoberideal von $(f_1, \ldots, f_n)$, so gilt $h(\mathfrak{p}) \leq n$.*

Beweis:

1. Sei $\mathfrak{p}$ ein minimales Primoberideal von $(f_1, \ldots, f_n)$. Nach Lokalisieren können wir annehmen, daß A lokaler Ring mit maximalem Ideal $\mathfrak{p}$ ist.
2. Da $\sqrt{(f_1, \ldots, f_n)}$ der Durchschnitt aller Primoberideale ist, folgt
$$\sqrt{(f_1, \ldots, f_n)} = \mathfrak{p}.$$
3. Sei $\mathfrak{p}_1$ ein maximales Primideal $\mathfrak{p}_1 \subset \mathfrak{p}$. Nicht alle f_i's liegen in $\mathfrak{p}_1$, da sonst $\mathfrak{p}$ nicht mehr minimal über $(f_1, \ldots, f_n)$ wäre. O.E. $f_1 \notin \mathfrak{p}_1$.
4. Also ist $\mathfrak{p}$ minimales Primoberideal von $(f_1) + \mathfrak{p}_1$. Also folgt wie eben $\sqrt{(f_1) + \mathfrak{p}_1} = \mathfrak{p}$.
5. Wegen $f_1, \ldots, f_n \in \mathfrak{p}$ gibt es ein $n_i \geq 1$ mit $f_i^{n_i} \in (f_1) + \mathfrak{p}_1$, d.h. es gibt $a_i \in A$ und $g_i \in \mathfrak{p}_1$ mit
$$f_i^{n_i} = a_i f_1 + g_i.$$
6. Wegen $(f_1, \ldots, f_n) \subseteq \sqrt{(f_1, g_2, \ldots, g_n)}$ folgt mit $\sqrt{(f_1, \ldots, f_n)} = \mathfrak{p}$ sofort
$$\sqrt{(f_1, g_2, \ldots, g_n)} = \mathfrak{p}.$$
Hieraus folgt sofort, daß $\mathfrak{p}$ minimales Primoberideal von $(f_1, g_2, \ldots, g_n)$ ist.
7. Das Ideal $(g_2, \ldots, g_n)$ ist in den Idealen $(f_1, \ldots, f_n)$, $\mathfrak{p}_1$, $\mathfrak{p}$ enthalten. Wir betrachten jetzt alles in $\overline{A} = A/(g_2, \ldots, g_n)$. Das Ideal $\overline{\mathfrak{p}}$ ist minimales Primoberideal von $(\overline{f_1})$, also folgt nach dem Krullschen Hauptidealsatz, daß $h(\overline{\mathfrak{p}}) \leq 1$ gilt. Dann gilt aber wegen $\overline{\mathfrak{p}_1} \subset \overline{\mathfrak{p}}$ die Gleichheit $h(\overline{\mathfrak{p}_1}) = 0$, d.h. $\overline{\mathfrak{p}_1}$ ist minimales Primideal in $\overline{A}$.
8. Im Ring A heißt dies: $\mathfrak{p}_1$ ist minimales Primoberideal von $(g_2, \ldots, g_n)$, also nach Induktionsvoraussetzung $h(\mathfrak{p}_1) \leq n - 1$.
9. Nun war $\mathfrak{p}_1 \subset \mathfrak{p}$ beliebig, woraus mit der letzten Ungleichung sofort $h(\mathfrak{p}) \leq n$ folgt. ■

Bemerkungen:

1. In einem noetherschen Ring ist jedes Primideal endlich erzeugt, hat also endliche Höhe. Daher gilt die absteigende Kettenbedingung für Primideale.
2. Ein noetherscher lokaler Ring hat also endliche Dimension.
3. Es gibt noethersche Ringe unendlicher Dimension. (Vgl. Aufgabe 50.)
4. Gilt für ein Primideal $\mathfrak{p}$ in einem noetherschen Ring $h(\mathfrak{p}) = n$ und $\mathfrak{p} = (f_1, \ldots, f_m)$, so folgt $m \geq n$.

Da wir ab jetzt den Krullschen Hauptidealsatz anwenden, setzen wir voraus, daß die betrachteten Ringe noethersch sind.
Wir geben folgende partielle Umkehrung des letzten Satzes an:

SATZ. *Jedes Primideal $\mathfrak{p} \subset A$ der Höhe n ist minimales Primoberideal eines Ideals $(f_1, \ldots, f_n)$, das von n Elementen erzeugt wird.*

Beweis: Wir konstruieren rekursiv $f_1, \ldots, f_i \in \mathfrak{p}$, so daß die minimalen Primoberideale von $(f_1, \ldots, f_i)$ Höhe i haben. Der Induktionsanfang $i = 0$ ist trivial. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die minimalen Primoberideale von $(f_1, \ldots, f_i)$, die also Höhe i haben. Natürlich können wir $i < n$ annehmen.
Behauptung: $\mathfrak{p} \not\subseteq (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$.
Beweis: Andernfalls gibt es ein j mit $\mathfrak{p} \subseteq \mathfrak{p}_j$, ein Widerspruch zu $h(\mathfrak{p}) = n > i = h(\mathfrak{p}_j)$.
Also gibt es ein $f_{i+1} \in \mathfrak{p} \setminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. Dann haben alle minimalen Primoberideale von $(f_1, \ldots, f_i, f_{i+1})$ Höhe $i + 1$. ■

SATZ. *Ist A lokal mit maximalem Ideal $\mathfrak{m}$ und sind $f_1, \ldots, f_n \in \mathfrak{m}$, so gilt*

$$dim(A/(f_1, \ldots, f_n)) \geq dim(A) - n.$$

Beweis: Sei $m = dim(A/(f_1, \ldots, f_n))$. Dann hat $\overline{\mathfrak{m}}$ die Höhe m in $A/(f_1, \ldots, f_n)$, also gibt es nach dem letzten Satz $g_1, \ldots, g_m \in A$, so daß $\overline{\mathfrak{m}}$ minimales Primoberideal von $(\overline{g_1}, \ldots, \overline{g_m})$ ist. Also ist in A das maximale Ideal $\mathfrak{m}$ minimales Primoberideal von $(f_1, \ldots, f_n, g_1, \ldots, g_m)$, also folgt mit dem verallgemeinerten Krullschen Hauptidealsatz

$$dim(A) = h(\mathfrak{m}) \leq n + m = n + dim(A/(f_1, \ldots, f_n)),$$

woraus die Behauptung folgt. ■

Läßt man in der Voraussetzung lokal weg, so muß der Satz aus trivialen Gründen nicht mehr gelten, wie folgendes Beispiel zeigt:

Beispiel: Sei $A = k[x, y, z]/(xz, yz)$. $Spec(A)$ entspricht dann der Vereinigung der $x - y$-Ebene und der z-Achse. Nun ist

$$A/(z - 1) \simeq k[x, y, z]/(xz, yz, z - 1) \simeq k[x, y]/(x, y) \simeq k,$$

also $dim(A/(z - 1)) = 0$, während $dim(A) = 2$ gilt.

Sei A ein lokaler Ring der Dimension n mit maximalem Ideal $\mathfrak{m}$. Ist $\mathfrak{m} = (x_1, \ldots, x_m)$, so folgt aus dem verallgemeinerten Krullschen Hauptidealsatz $n \leq m$, d.h. um das maximale Ideal zu erzeugen, braucht man mindestens $dim(A)$ Elemente.

DEFINITION. Ein lokaler (noetherscher) Ring A mit maximalem Ideal $\mathfrak{m}$ heißt regulär, wenn sich $\mathfrak{m}$ von $dim(A)$ Elementen erzeugen läßt.

SATZ. *Für einen lokalen Ring A mit maximalem Ideal $\mathfrak{m}$ gelten die Aussagen:*

$$dim(A) \leq dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2).$$

$$dim(A) = dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \iff A \text{ ist regulär}$$

Beweis: Wähle $x_1, \ldots, x_m \in \mathfrak{m}$, so daß sie eine Basis des Vektorraums $\mathfrak{m}/\mathfrak{m}^2$ bilden. (Also $m = dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.) Dann gilt $\mathfrak{m} = Ax_1 + \cdots + Ax_m + \mathfrak{m}^2$, woraus nach Nakayama sofort

$$\mathfrak{m} = (x_1, \ldots, x_m)$$

folgt. Nach dem verallgemeinerten Krullschen Hauptidealsatz gilt

$$dim(A) = h(\mathfrak{m}) \leq m = dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2),$$

also die erste Aussage. Gilt Gleichheit, so haben wir ein Erzeugendensystem von $\mathfrak{m}$ aus $dim(A)$ Elementen, d.h. A ist regulär. Die Umkehrung ist dann trivial. ■

SATZ. *Ist A regulärer lokaler Ring, dann ist A Integritätsring.*

Zum Beweis benötigen wir ein Lemma, das wir etwas weniger allgemein schon bewiesen haben:

LEMMA. *Sind in einem Ring A Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ und Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ gegeben mit*

$$\mathfrak{a} \subseteq \mathfrak{b} \cup \mathfrak{c} \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r,$$

so gilt $\mathfrak{a} \subseteq \mathfrak{b}$ oder $\mathfrak{a} \subseteq \mathfrak{c}$ oder $\mathfrak{a} \subseteq \mathfrak{p}_i$ für ein $i = 1, \ldots, r$.

Beweis als Übung.

Beweis des Satzes: Wir machen Induktion nach $n = dim(A) = h(\mathfrak{m})$. Im Fall $n = 0$ ist $\mathfrak{m} = 0$, A also ein Körper. Sei nun $n \geq 1$ vorausgesetzt. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die minimalen Primideale von A. Wegen $\mathfrak{m} \neq 0$ gilt nach Nakayama auch $\mathfrak{m}^2 \subset \mathfrak{m}$. Mit dem letzten Lemma weiß man dann:

$$\mathfrak{m} \not\subseteq \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r.$$

Wähle $x \in \mathfrak{m}$, $x \notin \mathfrak{m}^2$, $x \notin \mathfrak{p}_i$ für $i = 1, \ldots, r$. Wir ergänzen jetzt x zu einer Basis modulo $\mathfrak{m}^2$: $x = x_1, \ldots, x_n$. Wir wissen dann $\mathfrak{m} = (x, x_2, \ldots, x_n)$. Wir betrachten jetzt den Ring $A/(x)$. Das maximale Ideal wird von $n-1$ Elementen erzeugt, außerdem gilt $dim(A/(x)) \geq n-1$, also gilt sogar $dim(A/(x)) = n-1$. Also ist $A/(x)$ regulär und nach Induktionsvoraussetzung demnach Integritätsring. D.h. (x) ist Primideal in A. Da x nicht in einem minimalen Primideal liegt, gibt es ein minimales Primideal mit $\mathfrak{p}_i \subset (x)$. Ist $y \in \mathfrak{p}_i$, so gibt es $a \in A$ mit $y = ax$. Nun ist $ax \in \mathfrak{p}_i, x \notin \mathfrak{p}_i$, also $a \in \mathfrak{p}_i$. Also $\mathfrak{p}_i \subseteq \mathfrak{p}_i(x) \subseteq \mathfrak{m}\mathfrak{p}_i$. Nach Nakayama folgt $\mathfrak{p}_i = 0$. Daher ist 0 Primideal, A also Integritätsring. ■

Damit erhalten wir in Dimension 0 und 1 folgenden Satz:

SATZ. *Sei A ein lokaler noetherscher Ring. Dann gilt:*

$dim(A) = 0$: A regulär $\iff$ A ist Körper.
$dim(A) = 1$: A regulär $\iff$ A ist diskreter Bewertungsring.

Beweis: Die Richtung $\Leftarrow$ ist jeweils sofort klar. Zur Umkehrung: Ist A regulär, so ist A Integritätsring. Bei $dim(A) = 0$ ist dann A ein Körper. Sei jetzt $dim(A) = 1$. Dann ist A ein lokaler noetherscher Integritätsring, dessen maximales Ideal von einem Element erzeugt wird. Wir haben bereits früher gesehen, daß dann A ein diskreter Bewertungsring ist. ■

Reguläre lokale Ringe treten ganz natürlich auf als die lokalen nichtsingulärer Punkte auf algebraischen Varietäten.

LEMMA. *Sei k algebraisch abgeschlossener Körper, $\mathfrak{a} = (f_1, \ldots, f_r) \subseteq k[x_1, \ldots, x_n]$. Wir betrachten $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. Sei $\mathfrak{m} = (x_1 - p_1, \ldots, x_n - p_n) \in Spec(A)$ ein maximales Ideal. Dann gilt:*

$$dim_k \mathfrak{m}/\mathfrak{m}^2 = n - Rang((\frac{\partial f_i}{\partial x_j}(P))_{i,j}).$$

Beweis: Nach Koordinatenwechsel können wir $p_1 = \cdots = p_n = 0$ annehmen. Wir haben einen Isomorphismus

$$\mathfrak{m}/\mathfrak{m}^2 \simeq (x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2 + (f_1, \ldots, f_r).$$

Gilt jetzt $f_i \equiv \sum_j a_{ij} x_j \bmod (x_1, \ldots, x_n)^2$, so gilt:

$$dim(\mathfrak{m}/\mathfrak{m}^2) = dim_k(kx_1 + \cdots + kx_n) - dim_k(k(a_{11}x_1 + \cdots + a_{1n}x_n) + \cdots + k(a_{r1}x_1 + \cdots + a_{rn}x_n)),$$

was offensichtlich genau die Formel ist. ■

Primideale der Höhe 2 in $k[x, y, z]$

Die folgenden Bemerkungen geben wir als eine Art Vorschau ohne Beweis an. Siehe [**Gey77, Kun80**].

Sei k ein algebraisch abgeschlossener Körper. Wir betrachten $A = k[x, y, z]$. Dies ist ein 3-dimensionaler noetherscher faktorieller Integritätsring. Für $\mathfrak{p} \in Spec(A)$ gilt:

$$\begin{aligned} h(\mathfrak{p}) = 0 &\iff \mathfrak{p} = (0), \\ h(\mathfrak{p}) = 1 &\iff \mathfrak{p} = (f), \text{ wo } f \text{ ein irreduzibles Polynom ist}, \\ h(\mathfrak{p}) = 3 &\iff \mathfrak{p} = (x-a, y-b, z-c) \text{ mit } a, b, c \in k. \end{aligned}$$

Wie sehen Primideale der Höhe 2 aus? $V(\mathfrak{p}) \subset Spec(A)$ definiert eine irreduzible Kurve. Nach dem verallgemeinerten Krullschen Hauptidealsatz muß $\mathfrak{p}$ von mindestens 2 Elementen erzeugt werden.

DEFINITION. Ein Primideal $\mathfrak{p}$ der Höhe 2 in $k[x, y, z]$ heißt

1. vollständiger Durchschnitt, falls es $f, g \in k[x, y, z]$ gibt mit
$$\mathfrak{p} = (f, g),$$
(dann ist $V(\mathfrak{p}) = V(f) \cap V(g)$)
2. mengentheoretisch vollständiger Durchschnitt, falls es $f, g \in k[x, y, z]$ gibt mit
$$\mathfrak{p} = \sqrt{(f, g)},$$
(dann ist $V(\mathfrak{p}) = V(f) \cap V(g)$)
3. lokal vollständiger Durchschnitt, falls für jedes maximale Ideal $\mathfrak{m} \subseteq k[x, y, z]$ mit $\mathfrak{p} \subseteq \mathfrak{m}$ Funktionen $f, g \in k[x, y, z]$ existieren mit
$$\mathfrak{p}k[x, y, z]_{\mathfrak{m}} = (f, g)k[x, y, z]_{\mathfrak{m}}.$$

Bemerkungen:

1. Ist $\mathfrak{p}$ vollständiger Durchschnitt, so auch mengentheoretisch und lokal vollständiger Durchschnitt.
2. Es gibt Beispiele, die nicht lokal vollständige Durchschnitte sind, aber mengentheoretisch schon. (Siehe Aufgabe 51.)
3. Szpiro hat gezeigt, daß lokal vollständige Durchschnitte auch mengentheoretisch vollständige Durchschnitte sind.
4. Es gibt die Vermutung, daß jedes Primideal der Höhe 2 mengentheoretisch vollständiger Durchschnitt ist.
5. Auf Macaulay geht ein Beispiel zurück, wo für gegebenes r ein Primideal $\mathfrak{p}$ der Höhe 2 angegeben wird, das sich nicht von r Elementen erzeugen läßt.
6. Definiert $\mathfrak{p}$ eine glatte Kurve, d.h. ist $A/\mathfrak{p}$ ein Dedekindring, so ist $\mathfrak{p}$ lokal vollständiger Durchschnitt. Ist das Geschlecht der Kurve ≤ 1, so ist $\mathfrak{p}$ sogar vollständiger Durchschnitt, bei Geschlecht ≥ 2 braucht man im allgemeinen 3 Polynome um $\mathfrak{p}$ zu beschreiben.

ANHANG A

Übungen

1. Jeder Ring R mit $\mathbf{Z} \subseteq R \subseteq \mathbf{Q}$ hat die Form
$$R = \mathbf{Z}[\frac{1}{p_i} : i \in I],$$
wo $\{p_i : i \in I\}$ eine Menge von Primzahlen ist.
2. Zeige, daß gilt
$$\mathbf{Z}[\sqrt{2}]^\times = \{\pm(1 \pm \sqrt{2})^n : n \geq 0\}.$$
3. Sei R ein kommutativer Ring. Zeige, daß $A \in M_n(R)$ genau dann eine Einheit ist, wenn $\det(A)$ eine Einheit in R ist.
4. Sei R ein kommutativer Ring. Zeige, daß ein Polynom $f = a_0 + a_1 x + a_2 x^2 + \ldots$ genau dann Einheit in $R[x]$ ist, wenn a_0 Einheit in R ist und alle a_i für $i \geq 1$ nilpotent sind, d.h. $a_i^{m_i} = 0$ erfüllen für eine natürliche Zahl m_i.
5. Charakterisiere die Nullteiler im Matrizenring $M_n(k)$ über einem Körper k.
6. Bestimme alle Ideale des Matrizenrings $M_n(k)$ über einem Körper k.
7. Der Ring $\mathbf{Z}[\sqrt{-2}]$ ist Hauptidealring.
8. Der Ring $\mathbf{Z}[\sqrt{-5}]$ ist kein Hauptidealring. ($(2, 1 + \sqrt{-5})$ ist kein Hauptideal.)
9. Gib ein Beispiel mit zwei Idealen $\mathfrak{a}$ und $\mathfrak{b}$ an, so daß
$$\mathfrak{ab} \neq \{ab : a \in \mathfrak{a}, b \in \mathfrak{b}\}.$$
10. Bestimme alle Ideale der Restklassenringe $\mathbf{Z}/(15)$, $\mathbf{Z}/(16)$ und $\mathbf{Z}/(17)$.
11. Sei X eine Menge, R ein Integritätsring und S ein Teilring von $\mathcal{F}(X, R)$. Ist $Y \subseteq X$ eine Teilmenge, so ist $I(Y) = \{f \in S : f(Y) = 0\}$ ein Ideal in S. Umgekehrt kann man die Nullstellenmengen von Funktionen betrachten: Ist $F \subseteq S$ eine Menge von Funktionen, so sei
$$N(F) = \{x \in X : f(x) = 0 \text{ für alle } f \in F\}.$$
   (a) Für eine Teilmenge $F \subseteq S$ gilt $N(F) = N((F))$.
   (b) Ist $F_i \subseteq S$ eine Familie von Teilmengen von S, so gilt
$$\cap N(F_i) = N(\cup F_i)$$
   (c) Es gilt auch
$$N(F_1) \cup N(F_2) = N((F_1)(F_2)).$$
   (d) Die Mengen $N(F)$ mit $F \subseteq S$ bilden die abgeschlossenen Teilmengen einer Topologie auf X.
   (e) Wie sieht diese Topologie im Fall $X = \mathbf{R}$ und $S = \mathbf{R}[x]$ bzw. $S = \mathcal{C}(\mathbf{R})$ aus?
12. Bestimme sämtliche Ideale in den Ringen $\mathbf{Q}[x]/(x^2 - 1)$, $\mathbf{Q}[x]/(x^2)$ und $\mathbf{Q}[x]/(x^2 + 1)$. Welche der Ideale sind prim, welche maximal?
13. In einem Hauptidealring ist jedes Primideal $\neq 0$ schon maximal.
14. (a) Bestimme $\{x \in M_2(\mathbf{Z}) : x^2 = 1\}$.
   (b) Für jede Zahl $n \geq 0$ gibt es einen kommutativen Ring R mit $\#\{x \in R : x^2 = 1\} = 2^n$.
15. (a) Der Ring $\mathbf{R}[x, y]/(x^2 + y^2 - 1)$ ist nicht faktoriell.
   (b) Der Ring $\mathbf{C}[x, y]/(x^2+y^2-1)$ ist faktoriell. Zeige dazu $\mathbf{C}[x, y]/(x^2+y^2-1) \simeq \mathbf{C}[x, y]/(xy-1)$.
16. Sei $\mathfrak{o}$ der Ring der auf ganz $\mathbf{C}$ holomorphen Funktionen.
   (a) $\mathfrak{o}$ ist nicht faktoriell.
   (b) $\mathfrak{o}$ ist nicht noethersch.

17. (a) (Umgekehrte lexikographische Ordnung) Definiere auf der Menge der Monome in n Unbestimmten $x_1, \ldots, x_n$ eine Ordnung durch:

$$x^a > x^b \quad \Longleftrightarrow \quad \text{der letzte Eintrag in } a-b \text{ ist negativ.}$$

Zeige, daß dadurch eine multiplikative Totalordnung definiert wird, die die zusätzliche Eigenschaft erfüllt für $f \in k[x_0, \ldots, x_i]$:

$$x_i | f \quad \Longleftrightarrow \quad x_i | L(f).$$

(b) (Graduierte umgekehrte lexikographische Ordnung) Zeige, daß durch folgende Vorschrift eine multiplikative Totalordnung auf der Menge der Monome in n Unbestimmten definiert wird: Sei $x^a > x^b$, wenn gilt: entweder ist $a_1 + \cdots + a_n > b_1 + \cdots + b_n$ oder $a_1 + \cdots + a_n = b_1 + \cdots + b_n$ und gleichzeitig ist der letzte Eintrag in $a - b$ negativ.

18. Bestimme die Lösungen des Gleichungssystems

$$x^2 + y^2 + z^2 = 4, \quad x^2 + 2y^2 = 5, \quad xz = 1.$$

19. Berechne jeweils eine Gröbner-Basis bzgl. der lexikographischen Ordnung mit $x > y > z$ für folgende Ideale $\mathfrak{a}$ und $\mathfrak{b}$:

$$\mathfrak{a} = (x^5 + y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1) \qquad \mathfrak{b} = (x^5 + y^4 + z^3 - 1, x^3 + y^3 + z^2 - 1).$$

20. Betrachte die Polynome

$$f = x^{n+1} - yz^{n-1}, \quad g = xy^{n-1} - z^n, \quad h = x^n z - y^n.$$

Zeige, daß das Polynom $y^{n^2} - z^{n^2+1}$ in der reduzierten Gröbner-Basis von (f, g, h) bzgl. der lexikographischen Ordnung mit $x > y > z$ enthalten ist.

21. Gib ein Beispiel für einen kommutativen Ring A und eine multiplikative Teilmenge S an, so daß durch

$$(a_1, s_1) \sim (a_2, s_2) \quad \Longleftrightarrow \quad a_1 s_2 = a_2 s_1$$

keine Äquivalenzrelation auf $A \times S$ definiert wird.

22. Für einen Ring R sei Λ die Menge aller multiplikativen Teilmengen S von R mit $0 \notin S$. Zeige, daß Λ maximale Elemente hat. $S \in \Lambda$ ist genau dann maximal, wenn $R \setminus S$ ein minimales Primideal in R ist.

23. Eine multiplikative Teilmenge S eines Ringes R heißt saturiert, wenn gilt: $xy \in S \iff x \in S$ und $y \in S$. Zeige:
    (a) S ist genau dann saturiert, wenn $R \setminus S$ Vereinigung von Primidealen ist.
    (b) Zu einer multiplikativen Teilmenge S von R gibt es eine kleinste saturierte multiplikative Menge $\overline{S} \subseteq R$ mit $S \subseteq \overline{S}$. Es gilt:

$$\overline{S} = R \setminus \bigcup \{\mathfrak{p} : \mathfrak{p} \text{ Primideal mit } \mathfrak{p} \cap S = \emptyset\}.$$

24. Sei $R = \mathbf{Z}[\sqrt{-7}]$. Ist p eine Primzahl in $\mathbf{Z}$, so ist (p) nicht notwendig Primideal in R. Sei $\mathfrak{p}_p$ das kleinste Primideal in R, das p enthält.
    (a) Wann ist $\mathfrak{p}_p = (p)$?
    (b) Zeige, daß $R_{\mathfrak{p}_p}$ genau dann ein diskreter Bewertungsring ist, wenn $p \neq 2$ ist.

25. (a) Sei R ein lokaler Ring und seien M und N zwei endlich erzeugte R-Moduln. Ist dann $M \otimes_R N = 0$, so folgt $M = 0$ oder $N = 0$.
    (b) Ist R nicht lokal, so gibt es endlich erzeugte R-Moduln M und N mit $M \otimes_R N = 0$, aber $M \neq 0$ und $N \neq 0$.

26. Für einen R-Modul M sei

$$M_{tor} = \{m \in M : am = 0 \text{ für ein } a \in R, a \neq 0\}.$$

Zeige, daß für einen Integritätsring M_{tor} ein Untermodul von M ist. Gib ein Beispiel dafür, daß diese Ausage im allgemeinen nicht stimmt.

27. Sei $K \subseteq L$ eine Körpererweiterung und $f(x) \in K[x]$. Zeige, daß gilt:

$$K[x]/(f(x)) \otimes_K L \simeq L[x]/(f(x)).$$

Was ist $\mathbf{Q}(\sqrt{-5}) \otimes_{\mathbf{Q}} \mathbf{R}$ bzw. $\mathbf{Q}(\sqrt{-5}) \otimes_{\mathbf{Q}} \mathbf{C}$?

28. Sei $a \in R, a \neq 0$ kein Nullteiler und M ein flacher R-Modul. Gilt $am = 0$ für ein $m \in M$, so ist $m = 0$.
29. Sei B eine A-Algebra, M ein A-Modul, N ein B-Modul. Beweise oder gib ein Gegenbeispiel für folgende Aussagen:
    (a) Ist M flacher bzw. freier A-Modul, so ist $M_B = B \otimes_A M$ flacher bzw. freier B-Modul.
    (b) Ist N flacher bzw. freier B-Modul, so ist N als A-Modul flach bzw. frei.
30. Sei $\mathbf{Z}_{(p)}$ die Lokalisierung von $\mathbf{Z}$ in (p). Zeige, daß $\mathbf{Q}$ ein flacher, aber kein freier $\mathbf{Z}_{(p)}$-Modul ist.
31. Sei R ein Hauptidealring. Zeige, daß ein endlich erzeugter R-Modul M genau dann flach ist, wenn M torsionsfrei ist.
32. Welche Dimension hat der Ring $\mathbf{Z}[\sqrt{-5}]$?
33. Beschreibe $Spec(\mathbf{R}[x])$.
34. Bestimme $Spec(\mathbf{Z}[i])$.
35. Sei $d \in \mathbf{Z}, d \neq 1$ quadratfrei und $K = \mathbf{Q}(\sqrt{d})$. Zeige, daß der ganze Abschluß von $\mathbf{Z}$ in K

$$\mathbf{Z}[\frac{1+\sqrt{d}}{2}] \text{ für } d \equiv 1 \bmod \text{ und } \mathbf{Z}[\sqrt{d}] \text{ für } d \equiv 2, 3 \bmod \text{ ist.}$$

36. Sei R faktoriell mit $2 \in R^\times$. Ist $f \in R$ quadratfrei, dann ist $R[\sqrt{f}]$ ein ganz abgeschlossener Integritätsring.
37. Bestimme den ganzen Abschluß von $A = k[x, y]/(y^2 - x^3)$ in $Quot(A)$.
38. Sei $B = k[t, z]$, $u = t(t-1), v = t^2(t-1)$ und $A = k[u, v, z] \subseteq B$. Zeige:
    (a) $A \simeq k[x, y, z]/(y^2 - xy - x^3)$.
    (b) Going-up gilt für $A \subseteq B$.
    (c) Sei $\mathfrak{q} = (t - z) \in Spec(B)$ und $\alpha : Spec(B) \to Spec(A)$ die kanonische Abbildung. Bestimme die irreduziblen Komponenten von $\alpha^{-1}V(\alpha\mathfrak{q})$ und folgere, daß Going-down nicht für $A \subseteq B$ gilt.
39. Ist A ganz abgeschlossener Integritätsring, so auch $A[x]$.
40. $Spec(\mathbf{C}[x, y]) \to Spec(\mathbf{C}[x])$ ist nicht abgeschlossen.
41. Gib ein Beispiel für einen Ring A und einen A-Modul M, so daß $M \neq 0$ aber $Ass_A(M) = \emptyset$ gilt.
42. Gib ein Beispiel für einen Ring A und einen A-Modul M, eine multiplikative Teilmenge S in A, so daß

$$S^{-1}\mathfrak{p} = ann(\frac{x}{1}), \text{ aber } \mathfrak{p} \subset ann(x).$$

43. Sei A ein noetherscher ganz abgeschlossener Integritätsring und $f \in A, f \notin A^\times$. Dann hat $A/(f)$ keine eingebetteten Primideale. (Hinweis: O.E. ist $f \neq 0$. Wähle $\mathfrak{p} \in Ass_A(A/(f))$. Lokalisiere in $\mathfrak{p}$. Zeige, daß $\mathfrak{p}A_\mathfrak{p}$ Hauptideal ist. Dann ist $A_\mathfrak{p}$ diskreter Bewertungsring, also $\mathfrak{p}A_\mathfrak{p}$ minimales Primoberideal von $fA_\mathfrak{p}$.)
44. Zeige, daß im Polynomring $k[x, y]$ gilt $(x^2, xy, y^2) = (x^2, y) \cap (x, y^2)$, daß alle drei Ideale (x, y)-primär sind, daß (x^2, y) und (x, y^2) irreduzibel sind.
45. Ist $\mathfrak{a}$ ein Radikalideal im noetherschen Ring A, so hat $A/\mathfrak{a}$ keine eingebetteten assoziierten Primideale.
46. Zeige, daß im Polynomring $k[x, y]$ für jedes $a \in k$

$$(x^2, xy) = (x) \cap (y - ax, x^2)$$

eine Primärzerlegung von (x^2, xy) liefert.
47. Sei $A = k[x, y, z]/(xy - z^2)$ und $\mathfrak{p} = (x, z)$. Bestimme die Primärzerlegung von $\mathfrak{p}^2$.
48. Sei A ein eindimensionaler noetherscher Ring.
    (a) Ist A ein Integritätsring, so sind die Primärkomponenten eines Ideals eindeutig bestimmt, d.h. die (irredundante) Primärzerlegung ist eindeutig.
    (b) Zeige, daß die Aussage in a. im eindimensionalen Ring $k[x, y]/(y^3)$ nicht gilt.
49. Betrachte den folgenden Unterring von $\mathbf{Z}[x]$:

$$A = \mathbf{Z}[2x, 2x^2, 2x^3, \dots] = \{a_0 + 2a_1x + 2a_2x^2 + 2a_3x^3 + \cdots + 2a_nx^n : a_0, \dots, a_n \in \mathbf{Z}\}.$$

    (a) Das Primideal $\mathfrak{p} = (2x, 2x^2, 2x^3, \dots)$ ist nicht endlich erzeugt, insbesondere ist A nicht noethersch.
    (b) $\mathfrak{m} = (2, 2x, 2x^2, 2x^3, \dots)$ ist maximales Ideal der Höhe 2.

(c) $\mathfrak{m}$ ist minimales Primoberideal von (2), also kann der Krullsche Hauptidealsatz nicht ganz allgemein gelten.

50. Sei k ein Körper, $A = k[x_{11}, x_{21}, x_{22}, \ldots, x_{n1}, x_{n2}, \ldots, x_{nn}, \ldots]$ und $\mathfrak{p}_n = (x_{n1}, \ldots, x_{nn})$. Sei S das Komplement von $\mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \ldots$ in A und $A_0 = A_S$.
    (a) A_0 ist noethersch.
    (b) Die Primideale $\mathfrak{p}_n A_0$ sind maximal, und dies sind die einzigen maximalen Ideale von A_0.
    (c) $h(\mathfrak{p}_n A_0) = n$.
    (d) $dim(A_0) = \infty$.
51. Sei $\mathfrak{p}$ der Kern der Abbildung
$$k[x, y, z] \to k[t], x \mapsto t^3, y \mapsto t^4, z \mapsto t^5.$$
    (a) $\mathfrak{p}$ ist Primideal der Höhe 2 und
$$\mathfrak{p} = (x^3 - yz, x^2y - z^2, xz - y^2).$$
    (b) Sei $\mathfrak{m} = (x, y, z)$. Zeige, daß $dim_k(\mathfrak{p}/\mathfrak{m}\mathfrak{p}) = 3$ ist, und folgere daraus, daß $\mathfrak{p}$ im Punkt $\mathfrak{m}$ nicht vollständiger Durchschnitt ist.
    (c) Zeige, daß gilt
$$\mathfrak{p} = \sqrt{(x^2y - z^2, x^4 + y^3 - 2xyz)},$$
    d.h. $\mathfrak{p}$ ist mengentheoretisch vollständiger Durchschnitt.

ANHANG B

Vorlesungsankündigung

MATHEMATISCHES INSTITUT
UNIVERSITÄT ERLANGEN-NÜRNBERG
Priv.-Doz. Dr. W. Ruppert

Bismarckstraße $1\frac{1}{2}$, 15. Juli 1994
D-91054 Erlangen
Tel. 09131/852466

Vorlesungsankündigung
für das Wintersemester 1994/95

Kommutative Algebra

Die kommutative Algebra ist ein eigenständiges Teilgebiet der Algebra, das sich dem Studium der kommutativen Ringe widmet. Die historischen Wurzeln der kommutativen Algebra liegen in der Zahlentheorie und der algebraischen Geometrie:

Der Grundbereich der Zahlentheorie ist zunächst der Ring $\mathbf{Z}$ der ganzen Zahlen. Doch schon bei einfachen Fragestellungen mit ganzen Zahlen ist es oft hilfreich, den Bereich der ganzen Zahlen etwas zu erweitern. So hat zum Beispiel Euler zur Untersuchung der diophantischen Gleichung $x^3 + y^3 = z^3$ Zahlen der Bauart $a+b\sqrt{-3}$ herangezogen und Eigenschaften benutzt, die der Ring $\{a+b\sqrt{-3} : a, b \in \mathbf{Z}\}$ aber nicht besitzt. Dies und ähnliche Fragestellungen in der Zahlentheorie führten im Weiteren zur Untersuchung von allgemeinen kommutativen Ringen.

Der zweite Ursprung der kommutativen Algebra liegt in der algebraischen Geometrie, wo man sich mit algebraischen Varietäten beschäftigt, also Mengen, die sich durch Polynomgleichungen beschreiben lassen. Geometrische Fragestellungen führten zu einer intensiven Entwicklung in der Algebra - ausgehend vom Studium der Polynomringe. Heute ist die kommutative Algebra wesentliche Grundlage der algebraischen Geometrie.

Die 4-stündige Vorlesung will an Hand konkreter Fragestellungen und Beispiele die abstrakten algebraischen Begriffe motivieren und entwickeln. Dabei soll auch auf konstuktive Verfahren im Umgang mit Polynomidealen eingegangen werden.

Die Vorlesung wendet sich an Hörer, die etwas tiefer in die Algebra eindringen wollen, oder die sich die algebraischen Grundlagen für die algebraische Geometrie aneignen wollen.

Zeit und Ort: Di, Do 8-10, Seminarraum
Beginn: 3. November 1994
Nummer im Vorlesungsverzeichnis: 06220

gez. W. Ruppert

Literaturverzeichnis

[AM69] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Company, 1969.

[Bou89] N. Bourbaki, Commutative Algebra, Chapters 1-7, Springer-Verlag, 1989.

[CLO92] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[Eis] D. Eisenbud, Commutative Algebra, vorläufige Version.

[Gey77] W.-D. Geyer, On the number of equations which are necessary to describe an algebraic set in n-space, Separata das Atas da 3^a Escola de Algebra, Vol. 9, 1977.

[Hut81] H. C. Hutchins, Examples of Commutative Rings, Polygonal Publishing House, Passaic NJ, 1981.

[Kun80] E. Kunz, Einführung in die kommutative Algebra und algebraische Geometrie, Vieweg, 1980.

[Lan84] S. Lang, Algebra, second edition, Addison-Wesley Publishing Company, 1984.

[Mat80] H. Matsumura, Commutative Algebra, Benjamin/Cummings, 1980.

[Mat86] H. Matsumura, Commutative ring theory, Cambridge University Press, 1986.