2 Noethersche Ringe und Moduln

§1 Der Hilbertsche Basissatz

Definition 2.1
Sei R ein (kommutativer) Ring (mit Eins), M ein R-Modul.

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

(b) M heißt ***noethersch***, wenn M (ACC) erfüllt.

(c) R heißt ***noethersch***, wenn er als R-Modul noethersch ist.

Beispiele

1.) k Körper. Ein k-Vektorraum V ist noethersch $\Leftrightarrow \dim_k(V) < \infty$.
[k hat nur die Ideale $\{0\}, k$.]

2.) $R = \mathbb{Z}$
[alle Untermodule: $n\mathbb{Z}$, mit $\operatorname{ggT}(n, m)$ zusammenbauen]

3.) $R = k[X]$
[Ideale von einem Polynom erzeugt, um größer zu machen: ggT der Polynome nehmen.]

Bemerkung 2.2
Sei $0 \to M' \overset{\alpha}{\to} M \overset{\beta}{\to} M'' \to 0$ kurze exakte Sequenz von R-Moduln. Dann gilt:

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

Beweis
“$\Rightarrow$“:

(i) $M'_0 \subseteq M'_1 \subseteq \dots \subseteq M'_i \subseteq \dots$ Kette von Untermoduln von $M' \Rightarrow \alpha(M'_0) \subseteq \alpha(M'_1) \subseteq \dots$ wird stationär $\overset{\alpha \text{ injektiv}}{\Longrightarrow} M'_0 \subseteq M'_1 \subseteq \dots$ wird stationär.

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

“$\Leftarrow$“:
Sei $M_0 \subseteq M_1 \subseteq \dots \subseteq M_i \subseteq \dots$ Kette von Untermoduln von M. Sei $M'_i := \alpha^{-1}(M_i), M''_i := \beta(M_i)$.
Nach Voraussetzung gibt es $n \in \mathbb{N}$, so dass für $i \geq n$ gilt: $M'_i = M'_n, M''_i = M''_n$. Weiter gilt:

$$\begin{tikzcd}
 & 0 \arrow[r] & M'_n \arrow[r, "\alpha"] \arrow[d, equal] & M_n \arrow[r, "\beta"] \arrow[d, "\gamma"] & M''_n \arrow[r] \arrow[d, equal] & 0 & \text{ist exakt} \\
\text{für ein } i \geq n & 0 \arrow[r] & M'_i \arrow[r, "\alpha"] & M_i \arrow[r, "\beta"] & M''_i \arrow[r] & 0 & \text{ist exakt}
\end{tikzcd}$$

γ injektiv (Einbettung).
Zu zeigen: γ surjektiv.
Sei $x \in M_i$, dazu gibt es ein $y \in M_n$ mit $\beta(y) = \beta(x) \Rightarrow z := y - x \in \mathrm{Kern}(\beta) = \mathrm{Bild}(\alpha) = \alpha(M_i') = \alpha(M_n') \Rightarrow x = \gamma(y - z)$ und $y - z \in M_n$.

Folgerung 2.3
Jeder endlich erzeugbare Modul über einem noetherschen Ring ist noethersch.

Beweis
1. Fall: F freier Modul vom Rang n.
Induktion über n.
$n = 1$: Dann ist $F \cong R$ als R-Modul, also noethersch nach Voraussetzung.
$n \geq 1$: Sei $e_1, \ldots, e_n$ Basis von F. Dann ist $F \cong \bigoplus_{i=1}^{n} R \cdot e_i$. Dann ist $0 \to \bigoplus_{i=1}^{n-1} R \cdot e_i \to F \to R \cdot e_n \to 0$ exakt. Nach Induktionsvoraussetzung ist $\bigoplus_{i=1}^{n-1} R \cdot e_i$ noethersch, $R \cdot e_n$ ist nach Voraussetzung noethersch $\overset{2.2}{\Longrightarrow} F$ noethersch.
2. Fall: M werde erzeugt von $x_1, \ldots, x_n$. Dann gibt es (genau) einen surjektiven R-Modulhomomorphismus $\beta : \bigoplus_{i=1}^{n} R \cdot e_i \to M$ mit $\beta(e_i) = x_i \overset{2.2}{\Longrightarrow} M$ noethersch.

Proposition 2.4
Sei R ein Ring.

(a) Für einen R-Modul M sind äquivalent:
  (i) M ist noethersch
  (ii) jede nichtleere Teilmenge von Untermoduln von M hat ein (bzgl. $\subseteq$) maximales Element.
  (iii) jeder Untermodul von M ist endlich erzeugt.

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

Beweis

(a) **(i) $\Rightarrow$ (ii):** Sei $\emptyset \neq \mathcal{M}$ eine Familie von Untermoduln von M. Sei $M_0 \in \mathcal{M}$. Ist M_0 nicht maximal, so gibt es ein $M_1 \in \mathcal{M}$ mit $M_0 \subsetneq M_1$. Ist M_1 nicht maximal, so gibt es ein $M_2 \in \mathcal{M}$ mit $M_1 \subsetneq M_2$. ...
Die Kette $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots$ muss stationär werden, d.h. $\exists n$ mit M_n ist maximal in $\mathcal{M}$.

(ii) $\Rightarrow$ (iii): Sei $N \subseteq M$ ein Untermodul, $\mathcal{M}$ Familie der endlich erzeugbaren Untermoduln von N. $\mathcal{M} \neq \emptyset$, da $\{0\} \in \mathcal{M}$. Nach Voraussetzung enthält $\mathcal{M}$ ein maximales Element N_0. Wäre $N_0 \neq N$ so gäbe es ein $x \in N \setminus N_0$. Dann wäre der von N_0 und x erzeugte Untermodul $N_1 \subset N$ endlich erzeugt und $N_0 \subsetneq N_1$. Widerspruch zu N_0 maximal.

(iii) $\Rightarrow$ (i): Seien $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_i \subseteq \cdots$ Untermoduln von M. Sei $N := \bigcup_{i \geq 0} M_i$. N ist Untermodul $\checkmark$.
N ist nach Voraussetzung endlich erzeugt, z.B. von $x_1, \ldots, x_n$. Jedes x_k liegt in einem $M_{i(k)}$, also liegen alle in M_m mit $m = \max\{i(k) : k = 1, \ldots, n\} \Rightarrow N = M_m \Rightarrow M_i = M_m$ für $i \geq m$.

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

Satz 4 (Hilbert'scher Basissatz)
Ist R noetherscher Ring, so ist auch $R[X]$ noethersch.

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

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

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

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

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

Folgerung 2.5
Sei R noetherscher Ring. Dann gilt:

(a) $R[X_1,\dots,X_n]$ ist noethersch für jedes $n\in\mathbb{N}$

(b) Jede endlich erzeugte R-Algebra A ist noethersch (als Ring)

Beweis

(a) $n=1$: Satz 4
$n>1$: $R[X_1,\dots,X_n] = R[X_1,\dots,X_{n-1}][X_n]$

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

§2 Ganze Ringerweiterungen

Definition 2.6
Sei S/R eine Ringerweiterung (d.h. $R\subseteq S$).

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

(b) S heißt ***ganz*** über R, wenn jedes $b\in S$ ganz über R ist.

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

Proposition 2.7
Sei S/R Ringerweiterung. Für $b\in S$ sind äquivalent:

(i) b ist ganz über R.

(ii) $R[b]$ ist endlich erzeugbarer R-Modul.

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

Beweis
(i) $\Rightarrow$ (ii): Nach Voraussetzung gibt es $a_0,\dots,a_{n-1}\in R$, sodass $b^n = a_{n-1}b^{n-1}+\dots+a_0$
$\Rightarrow b^n$ ist in dem von $1,b,\dots,b^{n-1}$ erzeugtem R-Untermodul von S enthalten. Sei M dieser Untermodul.
$\Rightarrow b^{n+1} = a_{n-1}b^n+\dots+a_0 b = a_{n-1}(\sum_{i=0}^{n-1}a_i b^i)+\dots+a_0 b \in M$

$\overset{\text{Induktion}}{\Rightarrow} b^k \in M$ für alle $k \geq 0 \Rightarrow M = R[b]$. Daraus folgt, dass $R[b]$ ein endlich erzeugbarer R-Modul ist.

(ii) $\Rightarrow$ (iii): Trivial (setze $S' = R[b]$).

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

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

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

Bew.: Cramersche Regel:

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

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

$\det(A_k^i) = 0$: in der k-ten Zeile steht $a_{i1}, \ldots, a_{in} \Rightarrow i$-te und k-te Zeile sind gleich.

$\Rightarrow A \cdot A^{\#} = \det(A) \cdot E_n = A^{\#} \cdot A \Rightarrow 0 = A^{\#} \cdot A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \det(A) \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \Rightarrow \det(A) \cdot s_i = 0$ für $i = 1, \ldots, n$. Da $1 \in S'$, gibt es $\lambda_i \in R$ mit $1 = \sum_{i=1}^n \lambda_i s_i \Rightarrow \det(A) \cdot 1 = \sum_{i=1}^n \lambda_i \cdot \det(A) \cdot s_i = 0 \Rightarrow \det(A) = 0$.

Proposition 2.8

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

Beweis

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

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

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

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

Definition 2.9

Sei S/R Ringerweiterung.

(a) $\bar{R}$ (wie in 2.8) heißt der ***ganze Abschluss*** von R in S.

(b) Ist $R = \bar{R}$, so heißt R ***ganz abgeschlossen*** in S.

(c) Ein nullteilerfreier Ring R heißt ***normal***, wenn er ganz abgeschlossen in $\mathrm{Quot}(R)$ ist.

(d) Ist R nullteilerfrei, so heißt der ganze Abschluss $\bar{R}$ von R in $\mathrm{Quot}(R)$ die ***Normalisierung*** von R.

Bemerkung 2.10

Jeder faktorielle Ring ist normal.

Beweis
Sei R ein faktorieller Ring.
Sei $K = \mathrm{Quot}(R)$. Sei $x = \frac{a}{b} \in K^\times$ mit $a, b \in R$ teilerfremd. Sei x ganz über R. Dann gibt es $\alpha_0, \dots, \alpha_{n-1} \in R$ mit $x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_0 = 0 \overset{\cdot b^n}{\Rightarrow} a^n + \alpha_{n-1}ba^{n-1} + \dots + \alpha_1 b^{n-1}a + \alpha_0 b^n = 0 \Rightarrow b \mid a^n$. Da a und b teilerfremd sind, kann dies nur gelten, wenn b invertierbar ist. Also ist $x \in R$. Daher ist R normal.

§3 Der Hilbert'sche Nullstellensatz

Satz 5 (Hilbert'scher Nullstellensatz)
Sei K ein Körper und $\mathfrak{m}$ ein maximales Ideal in $K[X_1, \dots, X_n]$.
Dann ist $L := K[X_1, \dots, X_n]/\mathfrak{m}$ eine algebraische Körpererweiterung von K.

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

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

Da L Körper, liegt $K' := K(x_1)$ in L, so dass $L \subset K'[X_2, \dots, X_n]$ ein Faktorring von $K'[X_2, \dots, X_n]$ nach einem maximalen Ideal ist.

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

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

Definition 2.11
Sei $I \trianglelefteq K[X_1, \dots, X_n]$ ein Ideal. Dann heißt die Teilmenge $V(I) \subseteq K^n$, die durch

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

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

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

Bemerkung + Definition 2.12
(a) Für 2 Ideale $I_1 \subseteq I_2$ gilt $V(I_1) \supseteq V(I_2)$.

(b) Definiert man für eine beliebige Teilmenge $V \subseteq K^n$ das ***Verschwindungsideal*** von V durch
$$I(V) := \{f \in K[X_1, \dots, X_n] : f(x_1, \dots, x_n) = 0 \; \forall (x_1, \dots, x_n) \in V\},$$
so gilt $V \subseteq V(I(V))$;
ist V bereits Nullstellenmenge $V(I)$ eines Ideals I von $K[X_1, \dots, X_n]$, so gilt sogar $V = V(I(V))$.

Beweis

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

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

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

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

Nach Satz 5 ist $K[X_1, \dots, X_n]/\mathfrak{m}$ eine algebraische Körpererweiterung von K.
Da K algebraisch abgeschlossen $\Rightarrow K[X_1, \dots, X_n]/\mathfrak{m} \cong K$.
Seien nun x_i die Restklasse von X_i in $K[X_1, \dots, X_n]/\mathfrak{m}$ und $x = (x_1, \dots, x_n)$.
Für $f \in K[X_1, \dots, X_n]$ ist $f(x) = f(\bar{X}_1, \dots, \bar{X}_n) = \bar{f} \mod I \Rightarrow f(x) = 0 \forall\; f \in I \Rightarrow x \in V(I)$.

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

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

Beweis (Rabinovitsch-Trick)
Sei $g \in I(V(I))$ und $f_1, \dots, f_m$ Idealerzeuger von $I \trianglelefteq K[X_1, \dots, X_n]$.
Zu zeigen: $\exists d \geq 1$ mit $g^d = \sum_{i=1}^m a_i f_i$ für irgendwelche a_i.

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

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

Nach Wahl von $g \in I(V(I))$ ist also $g(x') = 0$
$\Rightarrow (gX_{n+1} - 1)(x) = g(x')x_{n+1} - 1 = -1 \neq 0. \Rightarrow V(J) = \emptyset$.

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

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

"$\supseteq$": klar.

§4 Graduierte Ringe und Moduln

Definition + Bemerkung 2.13

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

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

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

(c) Ist $S = \bigoplus_{i \geq 0} S_i$ graduierter Ring, so ist S_0 Unterring mit $1 \in S_0$.

Beweis

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

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

Definition + Bemerkung 2.14

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

(a) Ein Ideal $I \subseteq S$ heißt ***homogen***, wenn es von homogenen Elementen erzeugt wird.

(b) Ein Ideal $I \subseteq S$ ist genau dann homogen, wenn für jedes $f \in I$, $f = \sum_{i \geq 0} f_i$ ($f_i \in S_i$) gilt: $f_i \in I$.

(c) Sei $I \subseteq S$ homogenes Ideal, erzeugt von homogenen Elementen $(h_\nu)_{\nu \in J}$. Dann hat jedes homogene $f \in I$ eine Darstellung $f = \sum_\nu g_\nu h_\nu$ mit g_ν homogen.

(d) Ist I homogenes Ideal in S, so ist ${}^{S}\!/\!_{I}$ graduierter Ring mit $\left({}^{S}\!/\!_{I}\right)_i = {}^{S_i}\!/\!_{(I \cap S_i)}$

Beweis

(b) "$\Leftarrow$": ✓

"$\Rightarrow$": Sei $(h_\nu)_{\nu \in J}$ homogenes Erzeugendensystem von I.

Sei $f \in I$. Dann gibt es $g_\nu \in S$ mit $f = \sum_\nu g_\nu h_\nu$. Sei $g_\nu = \sum_{i \geq 0} g_{\nu,i}$ Zerlegung in homogene Komponenten.

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

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

Beispiele

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

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

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

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

Definition + Bemerkung 2.15

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

(i) S noethersch.

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

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

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

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

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

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

Beweis der Behauptung durch Induktion über i:

$i = 0$: ✓

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

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

Definition + Bemerkung 2.16
Sei $S = \bigoplus_{i \geq 0} S_i$ graduierter Ring.

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

(b) Eine S-lineare Abbildung $\varphi : M \to M'$ zwischen graduierten S-Moduln heißt ***graderhaltend***, wenn $\varphi(M_i) \subseteq M'_i$ für alle $i \in \mathbb{Z}$

(c) Ein Ideal $I \subseteq S$ ist homogen ⇔ I ist als S-Modul graduiert (mit der geerbten Graduierung)

(d) Eine Abbildung $\varphi : M \to M'$ heißt *vom Grad d*, wenn $\varphi(M_i) \subseteq M'_{i+d}$ für alle i gilt.
In diesem Fall ist Kern(φ) ein graduierter Untermodul.
Graderhaltende Abbildungen sind genau die Abbildungen vom Grad 0.

(e) Ist $I \subseteq S$ homogenes Ideal, so ist $\varphi : S \to S/I = \bigoplus_{i \geq 0} S_i/(I \cap S_i)$ graderhaltend.

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

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

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

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

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

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

Proposition 2.17
Sei $S = k[X_1, \dots, X_n], k$ ein Körper, $S = \bigoplus_{d=0}^{\infty} S_d$.

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

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

Beweis
Induktion über n:

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

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

$n > 2$: Induktion über d:

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

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

$d > 1$: $\dim S_d^{(n)}$ ist die Anzahl der Monome vom Grad d in $X_1, \dots, X_n$.
In $S_d^{(n)}$ gibt es $\dim S_d^{(n-1)}$ Monome in denen X_n nicht vorkommt und $\dim S_{d-1}^{(n)}$ Monome in denen X_n vorkommt
$\overset{\text{I.V.}}{\Longrightarrow} \dim S_d^{(n)} = \binom{n+d-2}{d} + \binom{n+d-2}{d-1} = \frac{(n+d-2)!}{(d-1)!(n-2)!}(\frac{1}{d} + \frac{1}{n-1}) = \frac{(n+d-2)!}{(d-1)!(n-2)!} \frac{n+d-1}{d(n-1)} = \frac{(n+d-1)!}{d!(n-1)!} = \binom{n+d-1}{d}$

Satz 6 (Hilbert-Polynom)
Sei k ein Körper, $S = k[X_1, \dots, X_n]$. Sei M ein endlich erzeugbarer graduierter S-Modul.

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

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

Beweis
Induktion über n:

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

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

Dann ist

$$0 \to \underbrace{K}_{=\mathrm{Kern}(\varphi)} \to M(-1) \xrightarrow{\varphi} M \to {}^{M}\!/_{X_nM} \to 0$$

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

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

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

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

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

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

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

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

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

Definition 2.18
Sei S endlich erzeugte graduierte k-Algebra, $S_0 = k$, M endlich erzeugbarer graduierter S-Modul. Dann heißt die formale Potenzreihe

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

Hilbert-Reihe zu M.

Beispiele

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

2.) $M = S = k[X_1,\dots,X_n]$
Beh.: $H_M(t) = \frac{1}{(1-t)^n}$
Bew.: $\frac{1}{(1-t)^n} = \left(\sum_{i=0}^{\infty} t^i\right)^n = \sum_{i=0}^{\infty} c_i t^i$ mit $c_i =$ (Anzahl aller n-Tupel $(k_1,k_2,\dots,k_n)$ nichtnegativer ganzer Zahlen mit $k_1 + k_2 + \dots + k_n = i$) $=$ (Anzahl der Monome vom Grad i in $X_1,\dots,X_n$).

3.) $M = S = k[Y](\cong k[X^d]), \deg Y = d > 0 \Rightarrow H_M(t) = \sum_{i=0}^{\infty} t^{d\cdot i} = \frac{1}{1-t^d}$
$$\dim M_i = \begin{cases} 1: & d \mid i \\ 0: & \text{sonst} \end{cases}$$

Satz (6′)
Wie in Definition 2.18 seien S endlich erzeugbare graduierte k-Algebra, M endlich erzeugbarer graduierter S-Modul.
$f_1,\dots,f_r$ homogene Erzeuger von S als k-Algebra, $d_i := \deg f_i$.
Dann gibt es ein Polynom $F(t) \in \mathbb{Z}[t]$, sodass gilt:

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

Beweis
Induktion über r:

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

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

$$0 \to K \to M \xrightarrow{\cdot f_r} M(d_r) \to (M/f_rM)(d_r) \to 0$$

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

$$-\dim M_i + \dim M_{i+d_r} = \dim Q_{i+d_r} - \dim K_i$$

$$\Rightarrow \sum_{i=0}^{\infty} \dim M_{i+d_r} t^{i+d_r} - t^{d_r} \sum_{i=0}^{\infty} \dim M_i t^i = \sum_{i=0}^{\infty} \dim Q_{i+d_r} t^{i+d_r} - t^{d_r} \sum_{i=0}^{\infty} \dim K_i t^i$$

$$\Rightarrow H_M(t) - \sum_{i=0}^{d_r-1} \dim M_i t^i - t^{d_r} H_M(t) = H_Q(t) - \sum_{i=0}^{d_r-1} \dim Q_i t^i - t^{d_r} H_K(t)$$

$$(1 - t^{d_r}) H_M(t) = H_Q(t) - t^{d_r} H_K(t) + \sum_{i=0}^{d_r-1} \dim M_i t^i - \sum_{i=0}^{d_r-1} \dim Q_i t^i$$

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

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

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

§5 Invarianten endlicher Gruppen

Definition + Bemerkung 2.19
Sei k ein Körper, $n \geq 0$, $k[\mathfrak{X}] := k[X_1, \dots, X_n]$.

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

(a) $k[\mathfrak{X}]^G := \{f \in k[\mathfrak{X}] : \sigma(f) = f$ für alle $\sigma \in G\}$ heißt ***Invariantenring*** von $k[\mathfrak{X}]$ bezüglich G.

(b) $k[\mathfrak{X}]^G$ ist k-Algebra.

(c) G heißt ***linear***, wenn jedes $\sigma \in G$ graderhaltend ist. Dann ist $\sigma|_{k[\mathfrak{X}]_1}$ ein k-Vektorraum-Automorphismus und $\sigma \mapsto \sigma|_{k[\mathfrak{X}]_1}$ ist ein Gruppenhomomorphismus $G \to \mathrm{GL}_n(k)$.

Beispiele

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

2.) $n = 2$, $G = \{id, \varphi\}$ mit $\varphi(X) = -X$, $\varphi(Y) = -Y$ (wobei char $k \neq 2$).
$k[X,Y]^G$ wird erzeugt von X^2, Y^2, XY.

Satz 7 (Endliche Erzeugbarkeit des Invariantenrings)
Seien k, G, $k[\mathfrak{X}]$ wie in Def. 2.19, G linear und endlich.

(a) (Hilbert) Angenommen, char k sei kein Teiler von $|G|$. Dann ist $k[\mathfrak{X}]^G$ eine endlich erzeugbare k-Algebra.

(b) (E. Noether) Angenommen, char k sei kein Teiler von $|G|!$. Ist $m = |G|$, so wird $k[\mathfrak{X}]^G$ von Elementen vom Grad $\leq m$ erzeugt.

Beweis

(a) Sei $S := k[\mathfrak{X}]^G$ (graduierte Unteralgebra von $k[\mathfrak{X}]$).
$S_+ = \bigoplus_{i>0} S_i$, $I := S_+ k[\mathfrak{X}]$ (Ideal in $k[\mathfrak{X}]$) $\Rightarrow I$ ist endlich erzeugt (da $k[\mathfrak{X}]$ noethersch ist).
Somit enthält auch das Erzeugendensystem $\{s \in S_+ \mid s \text{ ist homogen}\}$ von I eine endliche Teilmenge, die I erzeugt (denn wannimmer ein Ideal J eines Ringes R endlich erzeugt ist, enthält jedes Erzeugendensystem von J eine endliche Teilmenge, die J erzeugt).
Seien also $f_1, \ldots, f_r \in S_+$ homogene Erzeuger von I. Sei $S' := k[f_1, \ldots, f_r] \subseteq S$.

Beh.: $S = S'$.

Bew.: Zeige mit Induktion: $S_d \subset S'$ für jedes $d \geq 0$.

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

$d \geq 1$: Sei $f \in S_d$. Dann ist $f \in S_+ \subseteq I \Rightarrow f = \sum_{i=1}^r g_i f_i$ mit $g_i \in k[\mathfrak{X}]_{d-d_i}$, $d_i = \deg(f_i)$ $\Rightarrow \deg(g_i) < d$.
Jetzt definieren wir die „Mittelung“: Die Abbildung $\varphi : k[\mathfrak{X}] \to S$, $h \mapsto \frac{1}{|G|} \sum_{\sigma \in G} \sigma(h)$ ist eine S-lineare, graderhaltende Projektion.
$\Rightarrow$ Wegen $f \in S_+ \subset S$ ist $f = \varphi(f) = \sum_{i=1}^r \varphi(g_i) f_i$ (da $f = \sum_{i=1}^r g_i f_i$) mit $\varphi(g_i) \in S$, $\deg(\varphi(g_i)) < d$.
Also nach Induktionsvoraussetzung $\varphi(g_i) \in S' \Rightarrow f \in S'$.
Damit ist induktiv gezeigt, daß $S_d \subset S'$ für jedes $d \geq 0$ ist. Somit ist $S = \sum_{d \geq 0} S_d \subset \sum_{d \geq 0} S' = S'$. $\Rightarrow k[f_1, \ldots, f_r] = S' = S = k[\mathfrak{X}]^G$, was zu zeigen war.

Bevor wir den Beweis mit Teil (b) fortsetzen, fügen wir ein Beispiel ein:

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

Beh.1:
$k[X_1, \ldots, X_n]^{S_n}$ wird (als k-Algebra) erzeugt von den „elementarsymmetrischen“ Polynomen:
$s_1 := X_1 + \cdots + X_n$
$s_2 := X_1 X_2 + X_1 X_3 + \cdots + X_{n-1} X_n = \sum_{1 \leq i < j \leq n} X_i X_j$
$s_3 := \sum_{1 \leq i < j < k \leq n} X_i X_j X_k$
$\vdots$
$s_n := X_1 \cdot \ldots \cdot X_n$
(dies gilt für Körper jeglicher Charakteristik, und sogar allgemeiner für kommutative Ringe).

Beh.2: $k[X_1, \ldots, X_n]^{S_n}$ wird erzeugt von den Potenzsummen
$f_k := \sum_{i=1}^n X_i^k$, $k = 1, \ldots, n$ wenn char k kein Teiler von n ist. (Man bemerke, dass $f_1 = s_1 = \sum X_i$.)

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

Beweis

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

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

Wir definieren Hilfspolynome in $2n$ Variablen: Für jedes $d \geq 0$ sei $F_d := \sum_{\sigma\in G}(\underbrace{\sum_{i=1}^{n} \sigma(X_i)Y_i}_{=:Z_\sigma})^d \in$

$k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$.

Für jedes $\sigma \in G$ sei $Z_\sigma = \sum_{i=1}^n \sigma(X_i)\, Y_i$. Dann ist also $F_d = \sum_{\sigma\in G} Z_\sigma^d$. Schreiben wir G in der Form $G = \{\sigma_1, \ldots, \sigma_m\}$, mit $|G| = m$, so wird hieraus $F_d = \sum_{i=1}^m Z_i^d$, wobei $Z_j := Z_{\sigma_j}$.

Umformungen: Sei $\gamma_\nu = \frac{d!}{\nu_1! \cdot \ldots \cdot \nu_n!}$ für jedes $\nu \in \mathbb{N}^n$ mit $|\nu| = d$. Jedes $\sigma \in G$ erfüllt dann $Z_\sigma^d = \left(\sum_{i=1}^n \sigma(X_i)\, Y_i\right)^d = \sum_{|\nu|=d} \gamma_\nu \sigma(X^\nu) Y^\nu$. Aus $F_d = \sum_{\sigma\in G} Z_\sigma^d$ wird mithin

(1) $F_d = \sum_{\sigma\in G} \sum_{|\nu|=d} \gamma_\nu \sigma(X^\nu) Y^\nu = \sum_{|\nu|=d} \gamma_\nu (\sum_{\sigma\in G} \sigma(X^\nu) Y^\nu) = \sum_{|\nu|=d} \gamma_\nu m \varphi(X^\nu) Y^\nu$.

Sei nun $d \geq 0$ beliebig. Doch nach Beh.2 wird der Polynomring $k\left[W_1, \ldots, W_m\right]^{S_m}$ (wobei die W_i neue Variablen sind) erzeugt von den m Potenzsummen $p_j := \sum_{i=1}^m W_i^j$ für $j = 1, 2, \ldots, m$. Also muß das Polynom $\sum_{i=1}^m W_i^d$ ein Polynom in diesen m Potenzsummen p_j sein (da es in $k\left[W_1, \ldots, W_m\right]^{S_m}$ liegt). Es gibt also für jedes $\mu \in \mathbb{N}^m$ mit $\sum_{i=1}^m i\mu_i = d$ ein Skalar $a_\mu \in k$, so daß die Gleichung $\sum_{i=1}^m W_i^d = \sum_{\mu\in\mathbb{N}^m} a_\mu p_1^{\mu_1} \cdot \cdots \cdot p_m^{\mu_m}$ gilt, wobei die Summe (aus Homogeneitätsgründen) sich nur über alle $\mu \in \mathbb{N}^m$ mit $\sum_{i=1}^m i\mu_i = d$ erstreckt. Setzen wir in dieser Gleichung die m Terme $Z_1, \ldots, Z_m$ für die m Variablen $W_1, \ldots, W_m$ ein, so erhalten wir

$F_d = \sum_{\mu\in\mathbb{N}^m} a_\mu F_1^{\mu_1} \cdot \cdots \cdot F_m^{\mu_m}$

(denn durch die Einsetzung wird $\sum_{i=1}^m W_i^d$ zu $\sum_{i=1}^m Z_i^d = F_d$ ausgewertet, und $p_j = \sum_{i=1}^m W_i^j$ zu $\sum_{i=1}^m Z_i^j = F_j$ für jedes j). Mit anderen Worten:

(2) $F_d = \sum_{\mu\in\mathbb{N}^m} a_\mu \prod_{j=1}^m F_j^{\mu_j} \overset{(1)}{=} \sum_{\mu\in\mathbb{N}^m} a_\mu \prod_{j=1}^m (\sum_{|\nu|=j} \gamma_\nu m \varphi(X^\nu) Y^\nu)^{\mu_j} \underset{\text{Potenzen von } Y}{\overset{\text{sortieren nach}}{=}} \sum_{\lambda\in\mathbb{N}^m} P_\lambda(X) Y^\lambda$ mit $P_\lambda \in \tilde{S}$.

Für jedes $\lambda \in \mathbb{N}^m$ können wir nun zwischen (1) und (2) die Koeffizienten vor Y^λ vergleichen (wobei wir $X_1, \ldots, X_n$ als Konstanten betrachten), und erhalten hierdurch:

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

Hieraus folgt $\varphi(X^\lambda) \in \tilde{S}$ für alle $\lambda \in \mathbb{N}^m$, die $|\lambda| = d$ erfüllen. Da d beliebig gewählt war, ist also $\varphi(X^\lambda) \in \tilde{S}$ für alle $\lambda \in \mathbb{N}^m$. Das gesamte Bild von φ ist also in $\tilde{S}$ enthalten. Da das Bild von φ aber $k\left[\mathfrak{X}\right]^G$ ist, heißt dies, dass $k\left[\mathfrak{X}\right]^G$ in $\tilde{S}$ enthalten, d. h., von Elementen vom Grad $\leq m$ erzeugt ist.

Beispiele

Sei $n = 2$; der Kürze halber bezeichnen wir dann die beiden Variablen X_1 und X_2 mit X und Y. Sei nun $G = \langle\sigma\rangle$, wobei σ durch $\sigma(X) = Y$ und $\sigma(Y) = -X$ definiert ist. Dann ist $G \cong \mathbb{Z}/4\mathbb{Z}$ Durchrechnen aller Monome mit Grad $\leq |G|$:

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

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

§6 Nakayama, Krull und Artin-Rees

Definition + Bemerkung 2.20
Sei R ein Ring.

(a)
$$\mathcal{J}(R) := \bigcap_{\mathfrak{m} \text{ maximales Ideal in } R} \mathfrak{m}$$
heißt ***Jacobson-Radikal*** von R.

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

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

Beweis

(b) Sei $x \in R,\ x^n \in \mathcal{J}(R)$; zu zeigen: $x \in \mathcal{J}(R)$.
Sei $\mathfrak{m}$ maximales Ideal von R, dann ist $x^n \in \mathfrak{m} \overset{\mathfrak{m}\text{ prim}}{\Rightarrow} x \in \mathfrak{m} \Rightarrow x \in \mathcal{J}(R)$

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

Beispiele
$\mathcal{J}(\mathbb{Z}) = 0, \quad \mathcal{J}(k[X]) = 0$
R lokaler Ring $\Rightarrow \mathcal{J}(R) = \mathfrak{m}$ (es gibt nur ein maximales Ideal in R)

Satz 8 (Lemma von Nakayama)
Sei R ein Ring, $I \subseteq \mathcal{J}(R)$ ein Ideal, M ein endlich erzeugbarer R-Modul, $N \subseteq M$ ein Untermodul.
Dann gilt:
$$\text{Ist } M = I \cdot M + N, \text{ so ist } N = M$$
Speziell: Ist $M = I \cdot M \Rightarrow M = 0$.

Beweis
Sei $M = I \cdot M + N \Rightarrow M/N = (I\cdot M)/N = I \cdot M/N$, also ohne Einschränkung $N = 0$.
Annahme: $M \neq 0$
Dann sei $x_1, \dots, x_n$ ein minimales Erzeugendensystem von M, also $M' := \langle x_2, \dots, x_n\rangle \subsetneq M$.

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

Folgerung 2.21
R, I, M wie in Satz 8.
Dann gilt für $x_1, \ldots, x_n \in M$:

$$x_1, \ldots, x_n \text{ erzeugt } M \Leftrightarrow \overline{x_1}, \ldots, \overline{x_n} \text{ erzeugen } \overline{M} = M/_{IM}$$

Beweis
„$\Rightarrow$“: klar.

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

Beispiele
R lokaler Ring mit maximalem Ideal $\mathfrak{m}$. $M = \mathfrak{m}$, $I = \mathfrak{m}$.
Falls $\mathfrak{m}$ endlich erzeugt (dies gilt z.B. falls R noethersch ist): $\mathfrak{m}^2 = \mathfrak{m} \Rightarrow \mathfrak{m} = 0$, also R Körper.

Satz 9 (Durchschnittssatz von Krull)
Sei R noethersch, M endlich erzeugbarer R-Modul, $I \subseteq R$ Ideal.
Dann gilt für

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

Folgerung 2.22
(a) Ist in Satz 9 $I \subseteq \mathcal{J}(R)$, so ist $N = 0$.
(b) Ist R nullteilerfrei, so ist $\bigcap_{n \geq 0} I^n = 0$, falls $I \neq R$.

Beweis
(a) klar.
(b) Sei $\mathfrak{m}$ ein maximales Ideal mit $I \subseteq \mathfrak{m}$. $R_\mathfrak{m}$ die Lokalisierung von R nach $\mathfrak{m}$.
$R_\mathfrak{m}$ ist noethersch, lokal, also $\mathcal{J}(R_\mathfrak{m}) = \mathfrak{m} R_\mathfrak{m}$.
$i : R \to R_\mathfrak{m}$, $a \mapsto \frac{a}{1}$ ist injektiv, da R nullteilerfrei.

Dann ist $i(\bigcap_{n \geq 0} I^n) \subseteq \bigcap_{n \geq 0} i(I^n) \subseteq \bigcap_{n \geq 0} (\mathfrak{m} R_\mathfrak{m})^n \overset{\text{(a)}}{=} 0$.
Da i injektiv ist, folgt $\bigcap_{n \geq 0} I^n = 0$.

Proposition 2.23 (Artin-Rees)
Sei R noethersch, $I \subseteq R$ Ideal, M endlich erzeugbarer R-Modul, $N \subseteq M$ Untermodul.
Dann gibt es ein $n_0 \in \mathbb{N}$, sodass für alle $n \geq n_0$ gilt:

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

Beweis (Satz 9)
Setze in Prop. 2.23 (Artin-Rees) $N = \bigcap_{n \geq 0} I^n M$. Betrachte das n_0 aus Prop. 2.23 (Artin-Rees).

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

Beweis (Prop. 2.23)
Führe Hilfsgrößen ein:
$R' := \bigoplus_{n\geq 0} I^n$ ist graduierter Ring, $R'_0 = R$ ist noethersch, I ist endlich erzeugt,
$\Rightarrow R'$ ist noethersch (als endlich erzeugte R-Algebra),
$M' := \bigoplus_{n\geq 0} I^n M$ ist graduierter, endlich erzeugter R'-Modul,
$N' := \bigoplus_{n\geq 0} \underbrace{I^n M \cap N}_{=:N'_n}$ ist graduierter R'-Modul, Untermodul von M', also auch endlich erzeugbar. N' werde erzeugt von den homogenen Elementen $x_1, \ldots, x_r$ mit $x_i \in N'_{n_i}$.
Für $n \geq n_0 := \max\{n_1, \ldots, n_r\}$ ist dann $N'_{n+1} = \{\sum_{i=1}^r a_i x_i : \ a_i \in R'_{n+1-n_i} = I^{n+1-n_i}\}$.
$I \cdot N'_n = I \cdot \{\sum_{i=1}^r a_i x_i : \ a_i \in R'_{n-n_i} = I^{n-n_i}\} = \{\sum_{i=1}^r \tilde{a}_i x_i : \ \tilde{a}_i \in I \cdot I^{n-n_i} = I^{n+1-n_i}\} = N'_{n+1}$.
Mit Induktion folgt die Behauptung.

Beispiele

1) $R = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ ist noethersch, aber nicht nullteilerfrei.
   Sei I das von $e_1 = (1,0)$ erzeugte Ideal, $I^2 = (e_1^2) = (e_1) = I$ (e_1 ist „idempotent“)
   $e \in R$ heißt idempotent, wenn $e^2 = e$ ist. Dann ist $(e-1)e = 0$.
   Frage: was ist $\mathbb{Z}^2$ lokalisiert nach I?
   Antwort: $(\mathbb{Z} \oplus \mathbb{Z})_I = \mathbb{Q}$.
2) $R = \mathcal{C}^\infty(-1,1)$, $I = \{f \in R : \ f(0) = 0\}$. $R/I = \mathbb{C}$ (oder $\mathbb{R}$).
   I ist Hauptideal, erzeugt von $f(x) = x$.
   $\bigcap I^n = ?$ z.B. $f(x) = e^{-\frac{1}{x^2}} \in \bigcap I^n$.
   R ist nicht noethersch!
3) $R = k[X,Y]$, $I = (X,Y)$, k algebraisch abgeschlossen.
   $R' = R \oplus I \oplus I^2 \oplus \cdots = \bigoplus_{n\geq 0} I^n = R[u,v]/(Xv - Yu)$.
   Was sind die maximalen homogenen Ideale in R', die nicht ganz R'_+ enthalten?
   Typ 1: maximale Ideale in $R, \neq (X,Y)$: $(X-a, Y-b)$ mit $(a,b) \neq (0,0)$
   Typ 2: $(X, Y, \alpha u + \beta v)$, $(\alpha,\beta) \neq (0,0)$

§7 Krull-Dimension

Definition 2.24
Sei R ein Ring.

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

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

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

die ***Höhe*** von $\mathfrak{p}$.

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

Beispiele

(a) $R = k$ Körper: $\dim\ k = 0$
(b) $R = \mathbb{Z}$: $\dim\ \mathbb{Z} = 1$
(c) $R = k[X]$: $\dim\ k[X] = 1$

(d) $R = k[X,Y]$: dim $k[X,Y] = 2$
≥ 2 ist klar, da $(0) \subsetneq (X) \subsetneq (X,Y)$. Aber warum $= 2$?

Bemerkung 2.25
Sei R ein nullteilerfreier Ring. Dann gilt:

(a) Sind p, q Primelemente, $p \neq 0 \neq q$ mit $(p) \subseteq (q)$, so ist $(p) = (q)$.

(b) Ist R Hauptidealring, so ist R Körper oder $\dim(R) = 1$

Beweis

(a) $(p) \subseteq (q) \Rightarrow p \in (q)$, d.h. $p = q \cdot r$ für ein $r \in R$.
Da R nullteilerfrei, ist p irreduzibel, also $r \in R^\times \Rightarrow (p) = (q)$

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

Satz 10
Sei S/R eine ganze Ringerweiterung. Dann gilt:

(a) Zu jedem Primideal $\mathfrak{p}$ in R gibt es ein Primideal $\mathfrak{P}$ in S mit $\mathfrak{P} \cap R = \mathfrak{p}$

(b) Zu jeder Primidealkette $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ in R gibt es eine Primidealkette $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_n$ in S mit $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ $(i = 0, \ldots, n)$

(c) dim R = dim S

Beweis

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

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

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

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

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

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

Es folgt: b ist Nullstelle eines Polynoms vom Grad n mit Koeffizienten in $\mathfrak{p}$:
$b^n + \underbrace{\sum_{i=0}^{n-1} \alpha_i b^i = 0}_{\in \mathfrak{p}}, \alpha_i \in \mathfrak{p}$

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

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

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

Sei $S' := S/\mathfrak{P}_{n-1}$, $R' := R/\mathfrak{p}_{n-1}$. Dann ist S'/R' ganze Ringerweiterung.
Nach (a) gibt es in S' ein Primideal $\mathfrak{P}'_n$ mit $\mathfrak{P}'_n \cap R' = \mathfrak{p}'_n := \mathfrak{p}_n/\mathfrak{p}_{n-1}$.
Dann gilt für $\mathfrak{P}_n := \mathrm{pr}^{-1}(\mathfrak{P}'_n)$ $(\mathrm{pr} : S \to S'$ kanonische Projektion):
$\mathfrak{P}_n \cap R = \mathfrak{p}_n$ und $\mathfrak{P}_\mathfrak{n} \neq \mathfrak{P}_{n-1}$.

(c) Aus (b) folgt: $\dim\ S \geq \dim\ R$. Es bleibt zu zeigen: $\dim\ S \leq \dim\ R$.
Sei $\mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_n$ Kette in S, $\mathfrak{p}_i := \mathfrak{P}_i \cap R$, $i = 0, \ldots, n$.
klar: $\mathfrak{p}_i$ ist Primideal in R, $\mathfrak{p}_{i-1} \subseteq \mathfrak{p}_i$. Noch zu zeigen: $\mathfrak{p}_{i-1} \neq \mathfrak{p}_i$ für alle i.
Gehe über zu $R/\mathfrak{p}_{i-1}$ und $S/\mathfrak{P}_{i-1}$, also ohne Einschränkung $\mathfrak{p}_{i-1} = (0)$ und $\mathfrak{P}_{i-1} = (0)$.
Annahme: $\mathfrak{p}_i = (0)$
Sei $b \in \mathfrak{P}_i \setminus \{0\}$. b ist ganz über R: $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$.
Sei n der minimale Grad einer solchen Gleichung.
Es ist $a_0 = -b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in R \cap \mathfrak{P}_i = \mathfrak{p}_i = (0)$.
$\Rightarrow 0 = -b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$
Da S nullteilerfrei ist, muss gelten: $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 = 0$.
Widerspruch zur Wahl von n.

Folgerung 2.26
Sei S/R ganze Ringerweiterung, $\mathfrak{p}$ bzw. $\mathfrak{P}$ Primideale in R bzw. S. Ist $\mathfrak{p} = \mathfrak{P} \cap R$, so gilt:

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

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

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

Satz 11
Sei k Körper, A endlich erzeugbare k-Algebra.

(a) In A gibt es algebraisch unabhängige Elemente $x_1, \ldots, x_d$ (für ein $d \geq 0$), sodass A ganz ist über $k[x_1, \ldots, x_d]$. [Die Algebra $k[x_1, \ldots, x_d]$ ist dann isomorph zur Polynomalgebra $k[X_1, \ldots, X_d]$, da $x_1, \ldots, x_d$ algebraisch unabhängig sind. Ferner ist dann A als $k[x_1, \ldots, x_d]$-Modul endlich erzeugbar, da als Algebra endlich erzeugbar und ganz.]

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

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

Beweis

(c) „$\geq$“: klar.
„$\leq$“: Sei $0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ Primidealkette in A. Ohne Einschränkung (Satz 10) sei $A = k[x_1, \ldots, x_n]$.
Nach (b) existiert eine Einbettung $B := k[y_1, \ldots, y_d] \hookrightarrow A$ mit $\mathfrak{p}_1 \cap k[y_1, \ldots, y_d] = (y_{\delta+1}, \ldots, y_d)$.
Beh.: $\delta \leq d - 1$ (d.h. $\mathfrak{p}_1 \cap k[y_1, \ldots, y_d] \neq \{0\}$)
Denn: Sonst A ganz über $B \Rightarrow \mathfrak{p}_1 = 0$ (Satz 10, Beweis Teil (c)).
Sei nun $A_1 := A/\mathfrak{p}_1$, $B_1 := B/(\mathfrak{p}_1 \cap B) \cong k[y_1, \ldots, y_\delta]$. A_1 ist ganz über B_1, also ist nach Satz 10 (c) $\dim\ A_1 = \dim\ B_1 \overset{\text{I.V.}}{=} \delta$
Weiter ist $0 = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1$ Primidealkette in A_1.
$\Rightarrow m - 1 \leq \delta \leq d - 1 \Rightarrow m \leq d$

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

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

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

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

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

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

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

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

$\Rightarrow F_m(a_1, \dots, a_n) = F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \cdot a_n^m + \text{Terme niedriger Ordnung in } a_n$
$\Rightarrow F(a_1, \dots, a_n) = F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \cdot a_n^m + \text{Terme niedriger Ordnung in } a_n$
Ist $F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$, so weiter wie in Fall 1.
Ist k unendlich, so kann man immer $\lambda_1, \dots, \lambda_n$ finden, sodass $F_m(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$.
Ist k endlich, so hilft es, a_i durch $b_i = a_i - a_n^{\mu_i}$ zu ersetzen.

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

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

Setze $y_d := f$, $y_i = x_i - \lambda_i x_d$ für geeignete $\lambda_i \in k$.
Dann ist $f - y_d = 0$ normiertes Polynom in x_d über $k[y_1, \dots, y_d]$ (vgl. (a))

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

Denn: Sei $g \in I \cap k[y_1, \dots, y_d]$, d.h. $g = h \cdot f$ für ein $h \in k[x_1, \dots, x_d]$. h ist ganz über $k[y_2, \dots, y_d]$ $\Rightarrow$ $h^m + b_{m-1} h^{m-1} + \dots + b_1 h + b_0 = 0$ ($m \geq 1$, $b_i \in h[y_1, \dots, y_d]$) $\Rightarrow$ $g^m + \underbrace{b_{m-1} f g^{m-1} + \dots + b_1 f^{m-1} g + b_0 f^m}_{= y_d \cdot \dots} = 0$

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

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

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

$d > 1$: Sei $f \in I$, $f \neq 0$.
Dann gibt es nach Fall 1 eine Einbettung $k[y_1, \dots y_d] \hookrightarrow A$ mit $f = y_d$.
$I' := I \cap k[y_1, \dots y_{d-1}]$

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

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

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

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

Dabei bezeichnet $\operatorname{trdeg}(K)$ (der ***Transzendenzgrad*** von K über k) die Maximalzahl über k algebraisch unabhängiger Elemente in K, wenn K eine Körpererweiterung von k ist.

§8 Das Spektrum eines Rings

Definition + Bemerkung 2.27
Sei R ein Ring.

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

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

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

Beispiele
$R = \mathbb{Z}$: $\operatorname{Spec}(\mathbb{Z}) = \{(0)\} \cup \{(p) : p \text{ Primzahl}\}$
$V((p)) = (p) \Rightarrow (p)$ ist abgeschlossen in $\operatorname{Spec}(R)$ für jede Primzahl p.
$V((0)) = \operatorname{Spec}(\mathbb{Z})$.
$I = n\mathbb{Z} \Rightarrow V(I) = \{(p_1), \dots (p_k)\}$, wenn $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$ die Primfaktorzerlegung von n ist.
$\overline{\{(0)\}} = \operatorname{Spec}(\mathbb{Z})$

$R = k[X]$: $\overline{\{(0)\}} = \operatorname{Spec}(R)$.
$f \in k[X]$ irreduzibel $\Rightarrow (f)$ ist abgeschlossener Punkt.
$k := \mathbb{C}$: f irreduzibel $\Leftrightarrow f(X) = X - c$ für ein $c \in \mathbb{C}$. $\Rightarrow \operatorname{Spec}(\mathbb{C}[X]) = \mathbb{C} \cup \{(0)\}$

Beweis
c) Sei $U \subseteq \operatorname{Spec}(R)$ offen $:\Leftrightarrow \operatorname{Spec}(R) \setminus U$ abgeschlossen.
Zu zeigen:

(i) $\emptyset$ ist abgeschlossen: $\emptyset = V(R)$.
Spec(R) ist abgeschlossen: $\operatorname{Spec}(R) = V((0))$.
(ii) endliche Vereinigung von abgeschlossenen Mengen ist abgeschlossen.
Zeige dazu: $V(I_1) \cup \dots \cup V(I_n) = V(I_1 \cap \dots \cap I_n) = V(I_1 \cdot \dots \cdot I_n)$
denn: Ohne Einschränkung sei $n = 2$:
„$\subseteq$" Sei $\mathfrak{p} \in V(I_1) \Rightarrow I_1 \subseteq \mathfrak{p} \Rightarrow I_1 \cap I_2 \subseteq \mathfrak{p} \Rightarrow \mathfrak{p} \in V(I_1 \cap I_2)$.
„$\supseteq$" Sei $\mathfrak{p} \in V(I_1 \cap I_2)$, $\mathfrak{p} \notin V(I_1)$.
Dann gibt es ein $a \in I_1 \setminus \mathfrak{p}$. Sei $b \in I_2$.
Dann ist $a \cdot b \in I_1 \cap I_2 \underset{\text{Vor.}}{\subset} \mathfrak{p}. \overset{\mathfrak{p}\text{ prim}}{\underset{a \notin \mathfrak{p}}{\Longrightarrow}} b \in \mathfrak{p} \Rightarrow I_2 \subseteq \mathfrak{p}$, d.h. $\mathfrak{p} \in V(I_2)$.
(iii) beliebiger Durchschnitt von abgeschlossenen Mengen ist abgeschlossen. Zeige dazu:

$$\bigcap_\nu V(I_\nu) = V\Big(\sum_\nu I_\nu\Big)$$

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

Bemerkung 2.28

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

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

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

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

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

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

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

Sei also $U = \mathrm{Spec}(R) - V(I)$ mit $I \nsubseteq \sqrt{(0)}$. Für $f \in I \setminus \sqrt{(0)}$ ist $(f) \subseteq I$, also $V(f) \supseteq V(I)$
$\Rightarrow U(f) \subseteq U$.

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

Definition + Proposition 2.29

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

Beispiele
$R = \mathbb{C}[X, Y]$,
$V((X)) = \{(X)\} \cup \{(X, Y - c), c \in \mathbb{C}\}$
$V((Y)) = \{(Y)\} \cup \{(X - a, Y), a \in \mathbb{C}\}$.

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

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

Beweis
„$\Rightarrow$“ Seien $f_1, f_2 \in R$, $f_1 \cdot f_2 \in I$ und $f_1 \notin I$. Dann ist $V(f_1) \nsupseteq V := V(I)$.
Andererseits: $V \subseteq V(f_1 \cdot f_2) = V(f_1) \cup V(f_2)$
$\Rightarrow V = (V \cap V(f_1)) \cup (V \cap V(f_2))$
$\underset{V\text{ irreduz.}}{\Longrightarrow} V \subseteq V(f_2) \Rightarrow f_2 \in I$.
„$\Leftarrow$“ Sei $V(I) = V = V(I_1) \cup V(I_2)$ und $V(I_1) \neq V$
d.h. $I_1 \nsubseteq I$. Sei $f_1 \in I_1 \setminus I$

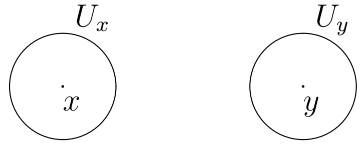
Andererseits ist $V(I_1 \cdot I_2) = V(I_1) \cup V(I_2) = V \Rightarrow I_1 \cdot I_2 \subseteq \sqrt{I} = I$

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

Folgerung 2.30
Ist $\mathrm{Spec}(R)$ hausdorffsch, so ist $\dim R = 0$

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

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



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

Definition + Bemerkung 2.31

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

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

das ***Verschwindungsideal*** von V.

b) Für jedes Ideal I von R gilt:

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

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

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

Definition + Proposition 2.32

a) Sei X ein topologischer Raum. Eine irreduzible Teilmenge $V \subseteq X$ heißt ***irreduzible Komponente***, wenn V maximale irreduzible Teilmenge ist bzgl. $\subseteq$.

b) Jeder topologischer Raum ist Vereinigung seiner irreduziblen Komponenten.

c) Ist R noethersch, so ist jede abgeschlossene Teilmenge von V von $\mathrm{Spec}(R)$ endliche Vereinigung von irreduziblen Komponenten von V; diese sind eindeutig bestimmt.

Beweis

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

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

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

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

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

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

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

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

$\Rightarrow U$ irreduzibel.

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

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

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

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

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

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

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

V_0 ist nicht irreduzibel.

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

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

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

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

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

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

Noch zu zeigen:

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

denn:

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

Sei W irreduzible Komponente von V.

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

$\underset{W \text{ Komponente}}{\Rightarrow} W = \widetilde{V_i}$

Folgerung 2.33
Ein noetherscher Ring hat nur endlich viele minimale Primideale.

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

Proposition 2.34
Sei $\alpha : R \to S$ Ringhomomorphismus.

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

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

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

Beweis

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

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

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

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

b) Seien $\mathfrak{p}, \mathfrak{p}' \in \mathrm{Spec}(S)$ mit $\varphi_\alpha(\mathfrak{p}) = \varphi_\alpha(\mathfrak{p}')$
$\Rightarrow \alpha^{-1}(\mathfrak{p}) = \alpha^{-1}(\mathfrak{p}') \Rightarrow \alpha(\alpha^{-1}(\mathfrak{p})) = \alpha(\alpha^{-1}(\mathfrak{p}')) \underset{\alpha \text{ surj.}}{\Rightarrow} \mathfrak{p} = \mathfrak{p}'$

§9 Diskrete Bewertungsringe

Definition 2.35
Sei K ein Körper.
Ein surjektiver Gruppenhomomorphismus $v : K^\times \to \mathbb{Z}$ heißt ***diskrete Bewertung***, wenn für alle $x, y \in K^\times$ mit $x + y \in K^\times$ gilt:

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

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

Beispiele

1.) $K = \mathbb{Q},\ p \in \mathbb{Z}$ Primzahl.
Für $\frac{a}{b} \in \mathbb{Q} \setminus \{0\},\ a, b \in \mathbb{Z}$ schreibe $a = p^n \cdot a',\ b = p^m \cdot b'$ mit $p \nmid a',\ p \nmid b'$.
Setze $v_p(\frac{a}{b}) := n - m$. Und es gilt: $a + b \overset{\text{Œ: } n \leq m}{=} p^n \cdot (a' + p^{m-n} b')$.
v_p heißt ***p-adische Bewertung*** auf $\mathbb{Q}$. Es gilt:
   - $v_p(a) \geq 0\ \forall a \in \mathbb{Z}$. $v_3(\frac{7}{2}) = 0,\ v_3(\frac{9}{2}) = 2$.
   - $v_p(a+b) = \min\{v_p(a), v_p(b)\}$, falls $v_p(a) \neq v_p(b)$.

2.) $K = k(X) = \mathrm{Quot}(k[X])$ (k Körper).
Für $f = \frac{f_1}{f_2}$ sei $v(f) = v(f_1) - v(f_2)$.
   a) $v(f_1) = \mathrm{ord}_a(f_1)$ für festes $a \in k$ (Nullstellenordnung).
   Es gilt $v_a(f_1 \cdot f_2) = v_a(f_1) + v_a(f_2)$
   $v_a(f_1 + f_2) = v_a((X-a)^{n_1} \cdot g_1 + (X-a)^{n_2} \cdot g_2)$
   $\overset{\text{Œ: } n_1 \leq n_2}{=} v_a((X-a)^{n_1}(g_1 + (X-a)^{n_2 - n_1} \cdot g_2))$
   b) Für $f \in k[X]$ sei $v(f) = -\deg(f)$.

Bemerkung 2.36
Sei $v : K^\times \to \mathbb{Z}$ diskrete Bewertung. Sei $\rho \in \mathbb{R}$ mit $0 < \rho < 1$. Dann ist die Abbildung

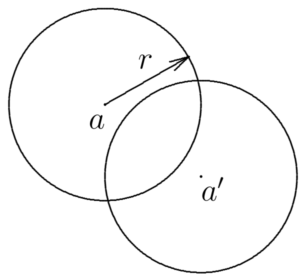
$$|\ |_v : K \to \mathbb{R},\ |x|_v = \begin{cases} 0 & : x = 0 \\ \rho^{v(x)} & : x \in K^\times \end{cases}$$

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

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

In unserer Situation gilt sogar:
$|x+y|_v \leq \max\{|x|_v, |y|_v\} \leq |x|_v + |y|_v \Rightarrow$ „nichtarchimedischer Betrag“
Weiter ist $d(x,y) := |x-y|_v$ eine Metrik auf K.

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



Jeder Kreis hat mehrere Mittelpunkte:
Beh.: Für jedes $a' \in K_r$ ist $K_r(a') = K_r(a)$
Bew.: Sei $b \in K_r(a)$, also $d(b,a) \leq r$.
Dreiecksungleichung:
$d(b,a') \leq \max\{\underbrace{d(b,a)}_{\leq r}, \underbrace{d(a,a')}_{\leq r}\} \leq r \Rightarrow b \in K_r(a')$

Es gibt kein allgemeines Dreieck:
Ist $d(a,b) < d(a,c)$, also $|a-b| < |c-a|$, so ist $|c-b| = |a-b+c-a| = \max\{|a-b|, |c-a|\} = |c-a|$
$\Rightarrow$ jedes Dreieck ist gleichschenklig.

Erinnerung
$\mathbb{R}$ entsteht aus $\mathbb{Q}$ durch „Vervollständigung“:
$C :=$ Ring der Cauchy-Folgen von $\mathbb{Q}$ (bzgl. $|\ |$)
$N :=$ Ideal der Nullfolgen in C (maximales Ideal)
$\mathbb{R} := C/N$
Analog:
$C_p :=$ Ring der Cauchy-Folgen von $\mathbb{Q}$ (bzgl. $|\ |_p := |\ |_{v_p}$)
$N_p :=$ Ideal der Nullfolgen in C_p (maximales Ideal)
$\mathbb{Q}_p := C_p/N_p$ „***Körper der p-adischen Zahlen***“

Bemerkung 2.37
Ist v diskrete Bewertung auf $K^\times$, so ist $\mathcal{O}_v := \{x \in K^\times : v(x) \geq 0\} \cup \{0\}$ ein Ring, genauer: ein lokaler Ring mit maximalem Ideal $\mathfrak{m}_v := \{x \in K^\times : v(x) > 0\} \cup \{0\}$.

Beweis
$\mathcal{O}_v$ ist Ring, da $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$ für alle $x, y \in \mathcal{O}_v$.
$\mathfrak{m}_v$ ist Ideal: Ist $x \in \mathfrak{m}_v$, $r \in \mathcal{O}_v$, so ist $v(x \cdot r) = v(x) + v(r) > 0$.
Für $x \in \mathcal{O}_v \setminus \mathfrak{m}_v = \{x \in K : v(x) = 0\}$ ist $v(\frac{1}{x}) = -v(x) = 0 \Rightarrow \frac{1}{x} \in \mathcal{O}_v(\setminus \mathfrak{m}_v) \Rightarrow x \in \mathcal{O}_v^\times$.

Definition + Proposition 2.38
(a) Ein nullteilerfreier Ring R heißt ***diskreter Bewertungsring***, wenn es eine diskrete Bewertung v von $K = \mathrm{Quot}(R)$ gibt mit $R = \mathcal{O}_v$.
(b) Jeder diskrete Bewertungsring ist noethersch, lokal und eindimensional.

Beweis
Zeige mehr: R ist Hauptidealring.
R ist lokal ✓, sei $\mathfrak{m}$ das maximale Ideal in R.
Beh.1: $\mathfrak{m}$ ist Hauptideal.
Bew.1: Sei $t \in R$ mit $v(t) = 1 \Rightarrow t \in \mathfrak{m}$. Sei $x \in \mathfrak{m} \setminus \{0\}$, $y = \frac{x}{t^{v(x)}} \Rightarrow v(y) = v(x) - v(t^{v(x)}) = 0$
$\Rightarrow y \in R^\times \Rightarrow x = t^{v(x)} \cdot y \in (t)$.
Beh.2: Jedes Ideal $\neq 0$ in R ist von der Form $\mathfrak{m}^n$ für ein $n \geq 0$.

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

Satz 12 (Diskrete Bewertungsringe)
Sei R ein lokaler noetherscher Ring der Dimension 1 mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper $k = R/\mathfrak{m}$.
Dann sind äquivalent:

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

Beweis

$$\begin{tikzcd}
(i) \arrow[rr, Rightarrow] & & (ii) \arrow[dl, Rightarrow] \arrow[d, Rightarrow] \\
& (v) \arrow[dr, Rightarrow] & (vi) \arrow[d, Rightarrow] \\
(iv) \arrow[uu, Rightarrow] & & (iii) \arrow[ll, Rightarrow]
\end{tikzcd}$$

(i) $\Rightarrow$ (ii) Proposition 2.38

(iv) $\Rightarrow$ (i)

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

<u>Diskrete Bewertung:</u>
Für $a = u \cdot t^n \in R \setminus \{0\}$ setze $v(a) = n$. Für $x = \frac{a}{b} \in K = \mathrm{Quot}(R),\ a, b \in R \setminus \{0\}$ setze $v(x) = v(a) - v(b)$.

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

v ist diskrete Bewertung: $v(x \cdot y) = v(u \cdot t^n \cdot v \cdot t^m) = v(u \cdot v \cdot t^{n+m}) = n + m = v(x) + v(y)$.
$v(x + y) \overset{m \leq n}{=} v(t^m \cdot (v + u \cdot t^{n-m})) \geq m = \min\{v(x), v(y)\}$.

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

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

a in $R/\mathfrak{m} = k$.
Es ist $\mathfrak{m}^2 \neq \mathfrak{m}$, da $\dim R = 1$ (und R noethersch) $\Rightarrow \dim_k \mathfrak{m}/\mathfrak{m}^2 \geq 1$.
$\mathfrak{m}/\mathfrak{m}^2$ wird von $\bar{t}$ erzeugt (als R-Modul und damit auch als $R/\mathfrak{m}$-Modul) $\Rightarrow \dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$
$\Rightarrow \dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

(v) $\Rightarrow$ **(iii)** Sei $t \in \mathfrak{m}$, sodass $\bar{t} \in \mathfrak{m}/\mathfrak{m}^2$ Erzeuger ist.
Mit Nakayama (Folgerung 2.21) folgt: t erzeugt $\mathfrak{m}$.

(ii) $\Rightarrow$ **(vi)** Jeder (nullteilerfreie) Hauptidealring ist faktoriell
$\Rightarrow R$ ist normal. (Bemerkung 2.10)

(vi) $\Rightarrow$ **(iii)** Sei $K = \mathrm{Quot}(R)$.
Sei $\bar{\mathfrak{m}} := \{x \in K : x \cdot \mathfrak{m} \subseteq \mathfrak{m}\}$, $\mathfrak{m}^{-1} := \{x \in K : x \cdot \mathfrak{m} \subseteq R\}$
Offensichtlich: $R \subseteq \bar{\mathfrak{m}} \subseteq \mathfrak{m}^{-1}$

Beh. 1:

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

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

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

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

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

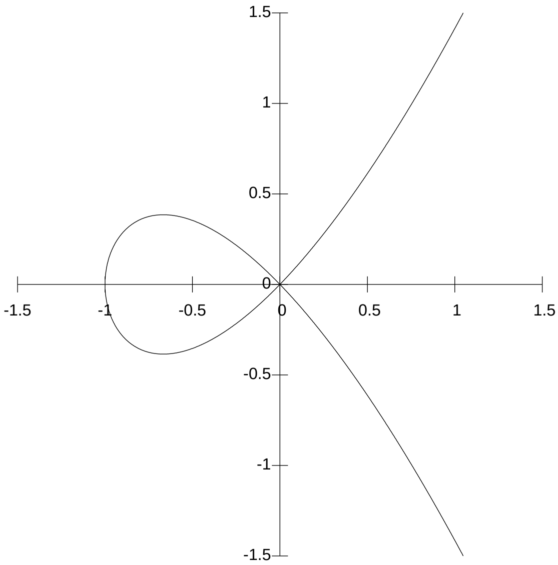
Bew. 1: $\bar{\mathfrak{m}}$ ist Unterring von K.
Zeige: $\bar{\mathfrak{m}}$ ist ganz über R (dann ist $\bar{\mathfrak{m}} = R$, da R normal).
Es genügt zu zeigen: $\bar{\mathfrak{m}}$ ist endlich erzeugter R-Modul.
Für $t \in \mathfrak{m} \setminus \{0\}$ ist $t \cdot \bar{\mathfrak{m}} \subseteq R$, also endlich erzeugt, da R noethersch. Als R-Modul sind $\bar{\mathfrak{m}}$ und $t \cdot \bar{\mathfrak{m}}$ isomorph.

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

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

Bew. 4: $\sqrt{(t)} = \bigcap_{\mathfrak{p} \subset R, t \in \mathfrak{p}} \mathfrak{p} = \mathfrak{m}$.
Seien $x_1, \ldots, x_r$ Erzeuger von $\mathfrak{m}$, $\nu_i \in \mathbb{N}$ $(i = 1, \ldots, r)$ mit $x_i^{\nu_i} \in (t)$.
Für $N = 1 + \sum_{i=1}^{r} (\nu_i - 1)$ ist dann $\mathfrak{m}^N \subseteq (t)$, da $\mathfrak{m}^N$ erzeugt wird von den $x_1^{\nu_1} \cdot \ldots \cdot x_r^{\nu_r}$ mit $\sum \nu_i = N \Rightarrow \exists\, \nu_i = 1$.

Beispiele
$R = \left(k[X,Y]/(Y^2 - X^3 - X^2)\right)_{(X,Y)}$ ist nullteilerfrei, eindimensional, lokal, noethersch aber *kein* diskreter Bewertungsring.
Denn: das maximale Ideal in R ist kein Hauptideal:
$\mathfrak{m} = (X,Y),\ f = Y^2 - X^2(X+1) \in \mathfrak{m}^2$.
Es gilt $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 2$, da X, Y linear unabhängig in $\mathfrak{m}/\mathfrak{m}^2$. Sei $\mathfrak{M}$ das von X und Y in $k[X,Y]$ erzeugte Ideal. $\mathfrak{m}/\mathfrak{m}^2 = (\mathfrak{M}/(f))/(\mathfrak{M}^2/(f)) \cong \mathfrak{M}/\mathfrak{M}^2$
Geometrisch:
$V(f) = \{(x,y) \in k^2 :\ f(x,y) = 0\} = \{(x,y) \in k^2 : y^2 = x^2(x+1)\}$
Singularität in $(0,0) = (X,Y) \Rightarrow$ "Newton-Knoten".



§10 Dedekindringe

Definition 2.39
Ein nullteilerfreier Ring heißt ***Dedekindring***, wenn er noethersch, normal und eindimensional ist.

Beispiele
1) $\mathbb{Z}$, $k[X]$ (k Körper)
2) diskrete Bewertungsringe
3) Hauptidealringe (nullteilerfrei)
4) der ganze Abschluss $\mathcal{O}_d$ von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ wobei $d \in \mathbb{Z}$ quadratfrei.

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \mod 4 \end{cases}$$

Beobachtung: Es gibt Dedekindringe, die nicht faktoriell sind: Beispiel: $\mathbb{Z}[\sqrt{-5}]$.
$(2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}))$.

Definition + Bemerkung 2.40
Sei R nullteilerfrei, $K = \operatorname{Quot}(R)$

a) Ein R-Untermodul $I \neq (0)$ von K heißt ***gebrochenes Ideal*** von R, wenn es ein $a \in R \setminus \{0\}$ gibt mit $a \cdot I \subseteq R$. (Beispiel: $(\frac{1}{n})$ ist gebrochenes Ideal von $\mathbb{Z}$, da $n \cdot (\frac{1}{n}) \subseteq \mathbb{Z}$ mit $R = \mathbb{Z}$.)
b) Für gebrochene Ideale I, J von R sei $I \cdot J$ der von allen $a \cdot b$, $a \in I, b \in J$, erzeugte R-Untermodul von K.
c) Die gebrochenen Ideale von R bilden mit der Multiplikation aus b) ein kommutatives Monoid mit neutralem Element R.
d) Die Einheiten in diesem Monoid heißen ***invertierbare*** (gebrochene) Ideale.
   d.h. I invertiertbar $\Leftrightarrow \exists I'$ mit $I \cdot I' = R$.

Beispiele
0) Jedes von 0 verschiedene Ideal in R ist gebrochenes Ideal.

1) Jeder von 0 verschiedene endlich erzeugbare R-Untermodul von K ist gebrochenes Ideal.
   denn: Seien $x_1 = \frac{a_1}{b_1}, \dots, x_n = \frac{a_n}{b_n}$ Erzeuger von M $(a_i, b_i \in R) \Rightarrow$ für $b = b_1 \cdot \ldots \cdot b_n$ ist $b \cdot M \subseteq R$.
2) Ist I gebrochenes Ideal, so ist $I^{-1} := \{x \in K : x \cdot I \subseteq R\}$ ebenfalls gebrochenes Ideal: für jedes $a \in I$ ist $a \cdot I^{-1} \subseteq R$.
   I ist invertierbar $\Leftrightarrow I \cdot I^{-1} = R$.
3) $R = k[X, Y]$, $I = (X, Y) \Rightarrow I^{-1} = R$.
   denn: für $a = \frac{f}{g} \in I^{-1}$ muss gelten: $a \cdot X \in R$, $a \cdot Y \in R$.
4) Jedes Hauptideal $\neq (0)$ ist invertierbar: $(a) \cdot (\frac{1}{a} \cdot R) = R$.

Bemerkung 2.41
Jedes invertierbare Ideal von einem Integritätsbereich ist endlich erzeugbar (als R-Modul).

Beweis
Sei I invertierbar, also $I \cdot I^{-1} = R$, dann gibt es $a_i \in I, b_i \in I^{-1}$ mit $1 = \sum_{i=1}^n a_i b_i$

Beh: $a_1, \dots a_n$ erzeugen I.

denn: Sei $a \in I \Rightarrow a = a \cdot 1 = a \cdot \sum_{i=1}^n a_i b_i = \sum_{i=1}^n a_i \underbrace{(ab_i)}_{\in R}$

Satz 13 (Dedekindringe)
Für einen nullteilerfreien Ring R sind äquivalent:

(i) R ist Dedekindring oder Körper.
(ii) R ist noethersch und $R_\mathfrak{p}$ ist diskreter Bewertungsring für jedes Primideal $\mathfrak{p} \neq (0)$ in R.
(iii) Jedes Ideal $I \neq (0)$ in R ist invertierbar.
(iv) Die gebrochenen Ideal in R bilden eine Gruppe.
(v) Jedes echte Ideal in R ist Produkt von endlich vielen Primidealen.
(vi) Jedes echte Ideal besitzt eine eindeutige Darstellung als Produkt von endlich vielen Primidealen.

Beweis
Beweisplan:

$$\begin{tikzcd}
& (ii) \arrow[dr, Rightarrow] & & (v) \arrow[dd, Leftrightarrow] \\
(i) \arrow[ur, Rightarrow] & & (iii) \arrow[ur, Leftrightarrow] \arrow[dl, Rightarrow] & \\
& (iv) \arrow[ul, Rightarrow] & & (vi)
\end{tikzcd}$$

(i) $\Rightarrow$ (ii) :

Sei $\mathfrak{p} \neq (0)$ Primideal im Dedekindring R. $\Rightarrow R_\mathfrak{p}$ noethersch, $\dim R_\mathfrak{p} = \operatorname{lat}(\mathfrak{p}) = 1$, da $\dim R = 1$.

$R_\mathfrak{p}$ normal: Sei $a \in K = \operatorname{Quot}(R) = \operatorname{Quot}(R_\mathfrak{p})$ ganz über $R_\mathfrak{p}$.

Dann gibt es eine Gleichung: $a^n + \sum_{i=0}^{n-1} \frac{b_i}{s_i} a^i = 0$ mit $b_i \in R, s_i \in R \setminus \mathfrak{p}$

$\Rightarrow (s \cdot a)^n + \sum_{i=0}^{n-1} \widetilde{b_i} (sa)^i = 0$ mit $\widetilde{b_i} \in R$, $s := \prod_{i=0}^{n-1} s_i$

$\underset{R \text{ normal}}{\Longrightarrow} s \cdot a \in R \Rightarrow a \underset{s \notin \mathfrak{p}}{=} \frac{s \cdot a}{s} \in R_\mathfrak{p}$

(iii) $\Rightarrow$ **(iv)** :

Sei $(0) \neq I \subset K$ gebrochenes Ideal, $a \in R \setminus \{0\}$ mit $a \cdot I \subseteq R$. $\underset{\text{(iii)}}{\Rightarrow}$ $a \cdot I$ invertierbar. $\Rightarrow$ $R = (a \cdot I) \cdot I' = I \cdot (a \cdot I') \Rightarrow I$ ist invertierbar.

(ii) $\Rightarrow$ **(iii)** :

Sei $I \neq (0)$ Ideal in R. $K = \mathrm{Quot}(R)$. $I^{-1} := \{x \in K : x \cdot I \subseteq R\}$

Zu zeigen: $I \cdot I^{-1} = R$.

Annahme: $I \cdot I^{-1} \subsetneqq R$:
Dann gibt es ein maximales Ideal $\mathfrak{m}$ von R mit $I \cdot I^{-1} \subseteq \mathfrak{m}$.
$\Rightarrow R_{\mathfrak{m}}$ ist diskreter Bewertungsring.
$\Rightarrow I \cdot R_{\mathfrak{m}}$ ist Hauptideal, d.h. $I \cdot R_{\mathfrak{m}} = \frac{a}{s} \cdot R_{\mathfrak{m}}$ für ein $a \in I, s \in R \setminus \mathfrak{m}$

Seien $b_1, \ldots, b_n \in I$ Erzeuger (R ist noethersch). $\Rightarrow \frac{b_i}{1} = \frac{a}{s} \cdot \frac{r_i}{s_i}$ für gewisse $r_i \in R, s_i \in R \backslash \mathfrak{m}$

Sei $t = s \cdot \prod_{i=1}^{n} s_i$. Es gilt: $t \in R \setminus \mathfrak{m}$.

Für jedes $i = 1, \ldots n$ ist $\frac{t}{a} \cdot b_i = r_i \cdot s_i \cdot \ldots \cdot \widehat{s_i} \cdot \ldots \cdot s_n \in R$.

$\Rightarrow \frac{t}{a} \in I^{-1} \Rightarrow t = a \cdot \frac{t}{a} \in I \cdot I^{-1} \subseteq \mathfrak{m}$. Widerspruch.

(iv) $\Rightarrow$ **(i)** :

<u>R noethersch</u>: Nach Bemerkung 2.41 ist jedes invertierbare Ideal endlich erzeugbar.

<u>R normal</u>: Sei $x \in K$ ganz über R. $\Rightarrow R[x]$ ist endlich erzeugbarer R-Modul, also gebrochenes Ideal (Beispiel 1). $\underset{\text{(iv)}}{\Rightarrow}$ $R[x]$ ist invertierbar.

Da $R[x]$ Ring ist, gilt $R[x] \cdot R[x] = R[x]$. $\underset{R[x] \text{ invertierbar}}{\Longrightarrow}$ $R[x] = R$ (neutrale Element).

$\Rightarrow x \in R$.

<u>$\dim R \leq 1$</u>: Sei $\mathfrak{p} \neq (0)$ Primideal in R, $\mathfrak{m} \subseteq R$ maximales Ideal mit $\mathfrak{p} \subseteq \mathfrak{m}$.

$\Rightarrow \mathfrak{m}^{-1} \cdot \mathfrak{p} \subseteq \mathfrak{m}^{-1}\mathfrak{m} \underset{\text{(iv)}}{=} R$ und $\mathfrak{m} \cdot (\mathfrak{m}^{-1}\mathfrak{p}) = \mathfrak{p}$.

$\underset{\mathfrak{p} \text{ Primideal}}{\Longrightarrow}$ $\mathfrak{m} = \mathfrak{p}$ oder $\mathfrak{m}^{-1}\mathfrak{p} \subseteq \mathfrak{p}$.

Falls $\mathfrak{m}^{-1}\mathfrak{p} \subseteq \mathfrak{p} \underset{\cdot \mathfrak{p}^{-1}}{\Rightarrow} \mathfrak{m}^{-1} \subseteq R$. Widerspruch (da sonst $\mathfrak{m}^{-1} \cdot \mathfrak{m} \subseteq \mathfrak{m}$)

(iii) $\Rightarrow$ **(v)** :

Sei $I \neq (0)$, $I \neq R$ Ideal in R.

Setze $I_0 := I$.

Definiere induktiv: I_n für $n \geq 1$:

Ist $I_{n-1} \neq R$, so sei $\mathfrak{m}_{n-1}$ maximales Ideal mit $I_{n-1} \subseteq \mathfrak{m}_{n-1}$ und $I_n := I_{n-1}\mathfrak{m}_{n-1}^{-1} \subseteq R$.

Es ist $I_{n-1} \subseteq I_n$

Wäre $I_n = I_{n-1}$, so wäre $\mathfrak{m}_{n-1}^{-1} = R$. Widerspruch zu $\mathfrak{m}_{n-1}^{-1} \cdot \mathfrak{m}_{n-1} = R$.

Da nach 2.41 R noethersch ist, wird die Kette $I_0 \subsetneqq I_1 \subsetneqq I_2 \subsetneqq \cdots$ stationär.

$\Rightarrow \exists n$ mit $R = I_n = I_{n-1}\mathfrak{m}_{n-1}^{-1} = I_{n-2}\mathfrak{m}_{n-2}^{-1}\mathfrak{m}_{n-1}^{-1} = \cdots = I_0 \cdot \prod_{i=0}^{n-1} \mathfrak{m}_i^{-1}$

$\Rightarrow I = I_0 = \prod_{i=0}^{n-1} \mathfrak{m}_i$

(v) $\Rightarrow$ **(vi)** :

Sei $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ mit Primidealen $\mathfrak{p}_i$, $\mathfrak{q}_i$. Zu zeigen: $n = m$ und $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ für eine Permutation $\sigma \in S_n$:

Induktion über n:

$n=1$: $\mathfrak{p}=\mathfrak{p}_1=\mathfrak{q}_1\cdots\mathfrak{q}_m \underset{\mathfrak{p}\text{ prim}}{\Rightarrow} \exists\, i_0$ mit $\mathfrak{q}_{i_0}\subseteq\mathfrak{p}$. Umgekehrt ist $\mathfrak{p}\subseteq\mathfrak{q}_i$ für jedes i. $\Rightarrow$ $\mathfrak{p}=\mathfrak{q}_{i_0}$

$n>1$: Ohne Einschränkung $\mathfrak{p}_1$ minimal bzgl. $\subseteq$ in $\{\mathfrak{p}_1,\dots\mathfrak{p}_n\}$.

Aus $\prod\mathfrak{q}_i \subseteq \prod\mathfrak{p}_j \subseteq \mathfrak{q}_{i_1} \Rightarrow \exists j_0$ mit $\mathfrak{p}_{j_0}\subseteq\mathfrak{q}_{i_0}\subseteq\mathfrak{p}_1 \underset{\mathfrak{p}_1\text{ minimal}}{\Rightarrow} \mathfrak{p}_1=\mathfrak{q}_{i_0} \underset{\text{(iii)}}{\Rightarrow} \mathfrak{p}_2\cdots\mathfrak{p}_n = \mathfrak{q}_1\dots\widehat{\mathfrak{q}_{i_0}}\dots\mathfrak{q}_m \Rightarrow$ Behauptung aus Induktionsvoraussetzung.

(v) $\Rightarrow$ **(iii)** :

Sei $I\neq(0)$, $I=\mathfrak{p}_1\cdots\mathfrak{p}_r$ mit Primidealen $\mathfrak{p}_i$. Ist jedes $\mathfrak{p}_i$ invertierbar, so ist $I^{-1}=\mathfrak{p}_1^{-1}\dots\mathfrak{p}_r^{-1}$ und $I\cdot I^{-1}=R$. Also ohne Einschränkung $I=\mathfrak{p}$ Primideal.

Sei $a\in\mathfrak{p}-\{0\}$, $(a)=\mathfrak{q}_1\dots\mathfrak{q}_n$ mit Primidealen $\mathfrak{q}_i \Rightarrow \mathfrak{q}_i\subseteq\mathfrak{p}$ für ein i.

$\mathfrak{q}_i$ ist invertierbar: $\mathfrak{q}_i^{-1}=\frac{1}{a}\cdot R\cdot\mathfrak{q}_1\cdots\widehat{\mathfrak{q}}_i\cdots\mathfrak{q}_n$

Es genügt also zu zeigen: $\mathfrak{q}_i=\mathfrak{p}$

Beh. 1: Jedes invertierbare Primideal $\mathfrak{q}$ in R ist maximal.

Bew. 1: Ist $\mathfrak{q}$ nicht maximal, so sei $x\in R\setminus\mathfrak{q}$ mit $\mathfrak{q}+(x)\neq R$.

Beh. 2: Dann ist $(\mathfrak{q}+(x))^2=\mathfrak{q}+(x^2)$

Dann ist $\mathfrak{q}\subseteq\mathfrak{q}+(x^2) \underset{\text{Beh. 2}}{=} (\mathfrak{q}+(x))^2\subseteq\mathfrak{q}^2+(x)$ $(*)$

Weiter ist $\mathfrak{q}\subseteq\mathfrak{q}^2+\mathfrak{q}\cdot(x)$

denn: Sei $b\in\mathfrak{q}$, schreibe nach $(*)$ $b=c+rx$ mit $c=\mathfrak{q}^2, r\in R$, dabei ist $r\in\mathfrak{q}$, da $r\cdot x\in\mathfrak{q}$ und $x\notin\mathfrak{q}$.

$\Rightarrow \mathfrak{q}=\mathfrak{q}^2+\mathfrak{q}\cdot(x)$ („$\supseteq$“ ist trivial)

$\Rightarrow \mathfrak{q}=\mathfrak{q}(\mathfrak{q}+(x)) \underset{\mathfrak{q}\text{ invertierbar}}{\Rightarrow} R=\mathfrak{q}+(x)$ Widerspruch.

Bew. 2: „$\subseteq$“ ✓, „$\supseteq$“

Schreibe beide Seiten als Produkt von Primidealen.

$\mathfrak{q}+(x)=\mathfrak{p}_1\cdots\mathfrak{q}_r$, $\mathfrak{q}+(x^2)=\mathfrak{q}_1\cdots\mathfrak{q}_s$.

In $R/\mathfrak{q}$ ist dann: $(\bar{x})=\bar{\mathfrak{p}}_1\cdots\bar{\mathfrak{p}}_r$, $(\bar{x})^2=\bar{\mathfrak{q}}_1\cdots\bar{\mathfrak{q}}_s=\bar{\mathfrak{p}}_1^2\cdots\bar{\mathfrak{q}}_r^2$

$(\bar{x}),(\bar{x}^2)$ invertierbar. $\Rightarrow \bar{\mathfrak{p}}_i,\bar{\mathfrak{q}}_j$ invertierbar.

$\underset{\text{„(iii) + (v) = (vi)“}}{\Rightarrow} \bar{\mathfrak{q}}_i=\bar{\mathfrak{p}}^2_{\sigma(i)} \Rightarrow$ ohne Einschränkung $\mathfrak{q}_i=\mathfrak{p}_i^2$.

Satz 14

Sei R ein Dedekindring, $K=\mathrm{Quot}(R)$, L/K endliche separable Körpererweiterung. S der ganze Abschluß von R in L.
Dann ist S ein Dedekindring.

Beweis

$\underline{\dim S=1:}$ Folgt aus Satz 10(c)

$\underline{S\text{ normal:}}$

Sei $x\in L$ ganz über S, also $x^n+\sum_{i=1}^{n-1}a_ix^i=0$ mit $a_i\in S$. Sei S' der von R und $a_1,\dots,a_{n-1}$ erzeugte Unterring von S. S' ist endlich erzeugbarer R-Modul, da die a_i ganz über R sind. $S[X]$ ist endlich erzeugter S'-Modul und damit endlich erzeugbarer R-Modul $\Rightarrow$ x ist ganz über $R\Rightarrow x\in S$.

$\underline{S\text{ noethersch:}}$

Beh. 1: Es gibt ein primitives Element α von L/K mit $\alpha\in S$.

Bew. 1: Sei $\tilde{\alpha}\in L$ primitives Element, also $1,\tilde{\alpha},\tilde{\alpha}^2,\dots,\tilde{\alpha}^{n-1}$ ist K-Basis von L ($n:=[L:K]$).

Sei $\tilde{\alpha} = \sum_{i=0}^{n-1} c_i \tilde{\alpha}^i$ für gewisse $c_i \in K,\ i = 0, \dots, n-1$. Schreibe $c_i = \frac{a_i}{b_i}$ mit $a_i, b_i \in R,\ b := \prod_{i=0}^{n-1} b_i$. Setze $\alpha := b \cdot \tilde{\alpha} \Rightarrow \alpha^n = b^n \cdot \sum_{i=0}^{n-1} c_i \tilde{\alpha}^i = \sum_{i=0}^{n-1} \underbrace{c_i b^{n-i}}_{\in R} \alpha^i \Rightarrow \alpha \in S$

$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ linear unabhängig:
Sei $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0 \Rightarrow \sum \lambda_i b^i \tilde{\alpha}^i = 0 \Rightarrow \lambda_i b^i = 0\ \forall i$
Sei nun $\bar{K}$ ein algebraischer Abschluss von K. Seien $\sigma_1, \dots, \sigma_n$ die verschiedenen Einbettungen von L in $\bar{K}$, also die Elemente von $\mathrm{Hom}(L, \bar{K})$.
$d := d(\alpha) := (\det(\sigma_i(\alpha^{j-1})_{i,j=1,\dots,n}))^2$ heißt die Diskriminante von L/K (bzgl. α).

Beh. 2:
(a) $d \neq 0$
(b) S ist in dem von $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}$ erzeugten R-Untermodul von L enthalten.

Dann ist S als Untermodul eines endlich erzeugbaren R-Modul selbst endlich erzeugbar und damit noethersch (weil R noethersch ist).

Bew. 2:

(a) $$d = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \dots & \sigma_n(\alpha) \\ \sigma_1(\alpha)^2 & \sigma_2(\alpha)^2 & \dots & \sigma_n(\alpha)^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha)^{n-1} & \sigma_2(\alpha)^{n-1} & \dots & \sigma_n(\alpha)^{n-1} \end{pmatrix} \overset{\text{Vandermonde}}{=} \prod_{i>j} (\sigma_i(\alpha) - \sigma_j(\alpha)) \neq 0$$

(b) Für $x \in L$ sei $\mathrm{Spur}(x) := \sum_{i=1}^n \sigma_i(x) \in \bar{K}$
$\mathrm{Spur}(x) \in K$: Für $\sigma \in \mathrm{Aut}_K(\bar{K})$ ist $\sigma \circ \sigma_i \in \mathrm{Hom}_K(L, \bar{K})$
$\sigma(\mathrm{Spur}(x)) = \sum_{i=1}^n (\sigma \circ \sigma_i)(x) = \mathrm{Spur}(x) \in \bar{K}^{\mathrm{Aut}_K(\bar{K})} = K$.
Sei $x \in S,\ x = \sum_{j=1}^n c_j \alpha^j$ mit $c_j \in K$.

Beh. 3: $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ ist Lösung eines LGS $A \cdot c = b$ mit $b \in R^n$ und $A \in R^{n \times n}$ mit $\det A = d$.

Nach der Cramerschen Regel ist dann $c_i = \frac{\det A_i}{\det A}$ wobei A_i aus A dadurch entsteht, dass die i-te Zeile durch b ersetzt wird. $\Rightarrow c_i \in \frac{1}{d} R \Rightarrow x$ liegt in dem von $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}$ erzeugten R-Modul.
Bew. 3: Für $i = 1, \dots, n$ ist $\mathrm{Spur}(\alpha^{i-1}x) = \sum_{j=1}^n \mathrm{Spur}((\alpha^{i-1}\alpha^{j-1})c_j) \in K \quad (*)$ ganz über R
$\Rightarrow \mathrm{Spur}(\alpha^{i-1}x) \in R \Rightarrow A := (\mathrm{Spur}(\alpha^{i-1}\alpha^{j-1})_{i,j=1,\dots,n}) \in R^{n \times n}$

$$b := \begin{pmatrix} \mathrm{Spur}(x) \\ \mathrm{Spur}(\alpha x) \\ \vdots \\ \mathrm{Spur}(\alpha^{n-1}x) \end{pmatrix} \in R^n\ (*) \text{ heißt } A \cdot c = b.$$

Noch zu zeigen: $\det A = d$.
Nach Definition ist $d = (\det B)^2$ mit $B = (\sigma_i(\alpha^{j-1})_{i,j})$
$\Rightarrow B^T \cdot B = (\beta_{ij})$ mit $\beta_{ij} = \sum_{k=1}^n \sigma(\alpha^{i-1})\sigma_k(\alpha^{j-1}) = \mathrm{Spur}(\alpha^{i-1}\alpha^{j-1})$
$\Rightarrow B^T \cdot B = A \Rightarrow \det A = (\det B)^2 = d$

Beispiele
$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$, D quadratfrei, $R = \mathbb{Z}$.
Was ist d? $\alpha = \sqrt{D}$, $\sigma_1 = \mathrm{id}$, $\sigma_2(a + b\sqrt{D}) = a - b\sqrt{D}$

$$B = \begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix}$$

$d = (\det B)^2 = (-2\sqrt{D})^2 = 4D$

§11 Primärzerlegung

Beispiele
$R = k[X,Y]$. $I = (X^2, Y)$ hat keine Darstellung als Produkt von Primidealen.

denn: Wäre $I = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$, so wäre $\sqrt{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = (X,Y) = \mathfrak{m}$. also $r = 1$, $\mathfrak{p}_1 = \mathfrak{m}$. Aber: $\mathfrak{m} \supsetneqq I \supsetneqq \mathfrak{m}^2$.

Definition + Bemerkung 2.42
Sei R Ring, $\mathfrak{q} \subseteq R$ echtes Ideal.

a) $\mathfrak{q}$ heißt ***Primärideal***, wenn für alle $a, b \in R$ mit $a \cdot b \in \mathfrak{q}$ und $a \notin \mathfrak{q}$ gilt: es gibt ein $n \geq 1$ mit $b^n \in \mathfrak{q}$.
b) Ist $\mathfrak{q}$ Primärideal, so ist $\mathfrak{p} = \sqrt{\mathfrak{q}}$ Primideal. $\mathfrak{p}$ heißt zu $\mathfrak{q}$ ***assoziiertes*** Primideal.

   Beweis
   Seien $a, b \in R$ mit $a \cdot b \in \sqrt{\mathfrak{q}} \Rightarrow a^n b^n \in \mathfrak{q}$ für ein $n \geq 1$.
   Ist $a \notin \sqrt{\mathfrak{q}}$, so ist $a^n \notin \mathfrak{q} \underset{\text{Def.}}{\Rightarrow} (b^n)^m \in \mathfrak{q} \Rightarrow b \in \sqrt{\mathfrak{q}}$

c) $\mathfrak{q}$ Primärideal $\Leftrightarrow$ jeder Nullteiler in $R/\mathfrak{q}$ ist nilpotent.

Beispiele
1) Ist $p \in R$ ein Primelement, so ist $(p^n) = (p)^n$ Primärideal für jedes $n \geq 1$.
   denn: Seien $a, b \in R$ mit $a \cdot b \in (p^n)$ und $a \notin (p^n)$ Ist $b \in (p)$, so ist $b^n \in (p^n)$.
   Anderenfalls ist $a \in (p)$. Dann gibt es $1 \leq d < n$ mit $a \in (p^d) \setminus (p^{d+1}) \Rightarrow a = p^d \cdot u$ mit $u \in R \setminus (p)$. Dann ist $u \cdot b \notin (p) \Rightarrow a \cdot b = p^d \cdot u \cdot b \notin (p^{d+1})$ Widerspruch.
2) Ist R Dedekindring, so sind die Primärideale genau die Potenzen von Primidealen.
   denn: Ist $\mathfrak{q}$ Primärideal, $\mathfrak{q} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ die Zerlegung von $\mathfrak{q}$ in Primidealen.
   $\Rightarrow \sqrt{\mathfrak{q}} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \underset{\sqrt{\mathfrak{q}}\text{ ist prim}}{\Rightarrow} r = 1$.
   Sei umgekehrt $\mathfrak{q} = \mathfrak{p}^n$ für ein Primideal $\mathfrak{p}$, $n \geq 1$. Seien $a, b \in R$, $a \cdot b \in \mathfrak{p}^n$, $a \notin \mathfrak{p}^n$. Nach Satz 13 ist $R_\mathfrak{p}$ Hauptidealring. D.h. $\mathfrak{p}R_\mathfrak{p}$ wird erzeugt von einem $\frac{p}{s}$, wobei $p \in \mathfrak{p}, s \in R \setminus \mathfrak{p}$ $\underset{\text{Bsp 1}}{\Rightarrow} \mathfrak{p}^n R_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^n$ ist Primideal.
   Ist $a \in \mathfrak{p}^n R_\mathfrak{p}$, so ist $a = \frac{p^n}{s^n} \cdot \frac{u}{t}$ mit $u \in R, t \in R \setminus \mathfrak{p} \Rightarrow t \cdot s^n \cdot a \in \mathfrak{p}^n \Rightarrow a \in \mathfrak{p}^n$. Widerspruch.
   Anderenfalls ist $b^m \in \mathfrak{p}^n R_\mathfrak{p}$ für ein m und damit $b \in \mathfrak{p}$ und $b^n \in \mathfrak{p}^n$.

Bemerkung 2.43
Sind $I_1, \ldots I_r$ $\mathfrak{p}$-primär (d.h. I_i primär und $\sqrt{I_i} = \mathfrak{p}$), so ist auch $I := \bigcap_{i=1}^{r} I_i$ $\mathfrak{p}$-primär.

Beweis
Seien $a, b \in R$ mit $a \cdot b \in I$, $a \notin I$. Dann gibt es i mit $a \notin I_i \Rightarrow b^{n_i} \in I_i$ für ein $n_i \geq 1 \Rightarrow b \in \sqrt{I_i} = \mathfrak{p} \Rightarrow$ Für $j = 1, \ldots r$ gibt es $n_j \geq 1$ mit $b^{n_j} \in I_j \Rightarrow b^n \in I$ für $n = \max_{j=1}^{n} n_j$.

Definition 2.44
Sei I Ideal in R.

a) Eine Darstellung $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ heißt ***Primärzerlegung*** von I, wenn alle $\mathfrak{q}_i$ primär sind.
b) Eine Primärzerlegung heißt ***reduziert***, wenn $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ für $i \neq j$ und kein $\mathfrak{q}_i$ weggelassen werden kann.
c) Besitzt $\mathfrak{q}$ eine Primärzerlegung, so auch eine reduzierte.

Satz 15 (Reduzierte Primärzerlegung)
Sei R noetherscher Ring.

Dann hat jedes echte Ideal in R eine reduzierte Primärzerlegung. Die assoziierten Primideale sind eindeutig. Die Primärideale, deren assoziierten Primideale minimal unter den in der Zerlegung vorkommenden sind, sind ebenfalls eindeutig.

Beweis
Sei $\mathcal{B} = \{I \subset R \text{ Ideal} : I \text{ besitzt keine Primärzerlegung}\}$. Ist $\mathcal{B} \neq \emptyset$, so besitzt $\mathcal{B}$ ein maximales Element I_0. Da I_0 nicht primär ist, gibt es $a, b \in R$ mit $a \cdot b \in I_0$ und $a \notin I_0$ und $b^n \notin I_0$ für alle $n \geq 1$.

Ziel: Konstruiere Ideale I und J mit $I_0 = I \cap J$ und $I \neq I_0 \neq J$. Dann haben I und J Primärzerlegungen, also I_0 auch. Widerspruch!

Für $n \geq 1$ sei $I_n := \{c \in R : c \cdot b^n \in I_0\}$. I_n ist Ideal mit $I_0 \subseteq I_n \subseteq I_{n+1}$. Da R noethersch ist, gibt es $k \in \mathbb{N}$ mit $I_n = I_k$ für alle $n \geq k$. Setze $I := I_n$. Beachte $a \in I_1 \setminus I_0 \subseteq I \setminus I_0$.

Sei $J := I_0 + (b^k) \supsetneqq I_0$, da $b^k \notin I_0$.

Beh: $I \cap J = I_0$

denn: „$\supseteq$“ ✓ „$\subseteq$“ Sei $y \in I \cap J$, also $y = x + b^k \cdot r$ (für ein $x \in I_0, r \in R$) und $y \cdot b^k \in I_0 \Rightarrow y \cdot b^k = b^{2k} \cdot r + x \cdot b^k \Rightarrow r \cdot b^{2k} = yb^k \cdot xb^k \Rightarrow r \in I_{2k} = I_k \Rightarrow r \cdot b^k \in I_0 \Rightarrow y \in I_0$.