Kommutative Algebra

Matthias Künzer

Universität Stuttgart

8. Juli 2020

Inhalt

Verzeichnis der Sätze und einiger sonstiger Aussagen

Vorwort

Polynomringe

Wir betrachten den Polynomring $\mathbf{C}[X,Y]$ in den zwei Variablen X und Y. Genauer gesagt, ist dies eine $\mathbf{C}$-Algebra. Darin ist ein *Ideal* eine Teilmenge, die die Null enthält und unter $\mathbf{C}[X,Y]$-Linearkombinationen abgeschlossen ist. Für Polynome $u_1(X,Y)$, $\ldots$, $u_n(X,Y)$ in $\mathbf{C}[X,Y]$ haben wir das Idealerzeugnis

$$\begin{array}{l} (u_1(X,Y),\ldots,u_n(X,Y)) \\ := \; \{\, s_1(X,Y)\cdot u_1(X,Y)+\cdots+s_n(X,Y)\cdot u_n(X,Y) :\; s_1(X,Y),\,\ldots,\, s_n(X,Y) \,\in\, \mathbf{C}[X,Y]\,\} \\ \subseteq\; \mathbf{C}[X,Y] \end{array}$$

als kleinstes Ideal, das diese vorgegebenen Polynome enthält.

Als maximales Ideal in $\mathbf{C}[X,Y]$ bezeichnet man eines, das eine echte Teilmenge von $\mathbf{C}[X,Y]$ ist und das zwischen sich und $\mathbf{C}[X,Y]$ kein weiteres Ideal liegen hat.

Die maximalen Ideale in $\mathbf{C}[X,Y]$ sind alle von der Form $(X-a, Y-b)$ für einen gewissen Punkt $(a,b)\in\mathbf{C}^2$. Man kann so jedem Punkt der komplexen Ebene in bijektiver Weise ein maximales Ideal zuordnen.

Sei nun $f(X,Y)\in\mathbf{C}[X,Y]$ ein Polynom in zwei Variablen.

Man denke etwa an $Y-X^2$, welches als Nullstellenmenge eine Parabel hat. Oder aber an Y^2-X^3, wessen Nullstellenmenge eine Spitze, also eine Singularität, im Ursprung hat.

Wann liegt der Punkt (a,b) in der Nullstellenmenge von $f(X,Y)$? Genau dann, wenn das Ideal $(f(X,Y))$ im Ideal $(X-a,Y-b)$ enthalten ist. Bijektiv ersetzt kann man also die Nullstellenmenge von $f(X,Y)$ ansehen als Menge aller maximalen Ideale, die $(f(X,Y))$ enthalten. Diese stehen dann wieder in Bijektion zu den maximalen Idealen der Faktoralgebra

$$\mathbf{C}[X,Y]/(f(X,Y)) \;=\; \{\, g(X,Y)+(f(X,Y)) :\; g(X,Y)\in\mathbf{C}[X,Y]\,\}\,.$$

Um die Nullstellenmenge von $f(X,Y)$ zu studieren, kann man also die maximalen Ideale von $\mathbf{C}[X,Y]/(f(X,Y))$ untersuchen.

Läßt sich dieser $\mathbf{C}$-Algebra entnehmen, ob die Nullstellenmenge eine Singularität hat? Ja, das geht. So etwa ist die Lokalisierung von $\mathbf{C}[X,Y]/(Y^2-X^3)$ an $(X-0,Y-0)$ keine regulärer lokaler $\mathbf{C}$-Algebra mehr.

Daß (a,b) in der Nullstellenmenge von $f(X,Y)$ liegt, läßt sich auch so ausdrücken, daß es den surjektiven $\mathbf{C}$-Algebrenmorphismus

$$\begin{array}{rcl} \mathbf{C}[X,Y]/(f(X,Y)) & \to & \mathbf{C}[X,Y]/(X-a,X-b) \\ g(X,Y)+(f(X,Y)) & \mapsto & g(X,Y)+(X-a,X-b) \end{array}$$

gibt. Allgemeiner, sind $\mathfrak{c}$ und $\mathfrak{d}$ Ideale von $\mathbf{C}[X,Y]$, dann liegt die Nullstellenmenge von $\mathfrak{c}$ in der Nullstellenmenge von $\mathfrak{d}$, falls es den surjektiven $\mathbf{C}$-Algebrenmorphismus

$$\begin{array}{rcl} \mathbf{C}[X,Y]/\mathfrak{d} & \to & \mathbf{C}[X,Y]/\mathfrak{c} \\ g(X,Y)+\mathfrak{d} & \mapsto & g(X,Y)+\mathfrak{c} \end{array}$$

gibt. Will man also das Verhalten von Nullstellenmengen von Polynomen untereinander studieren, so hat man $\mathbf{C}$-Algebrenmorphismen zu studieren.

Kommutative Algebren

Sei C ein kommutativer Ring.

Seien R und S kommutative C-Algebren. Sei $S \xrightarrow{f} R$ ein C-Algebrenmorphismus. Ist $\mathfrak{m} \subseteq R$ ein maximales Ideal, dann ist $f^{-1}(\mathfrak{m}) \subseteq S$ im allgemeinen kein maximales Ideal mehr, sondern nur noch ein Primideal. In anderen Worten, auch wenn $R/\mathfrak{m}$ ein Körper ist, ist $S/f^{-1}(\mathfrak{m})$ zu einer Teilalgebra von $R/\mathfrak{m}$ isomorph und damit i.a. nur nullteilerfrei, i.e. ein Integritätsbereich.

Daher betrachtet man Primideale, i.e. Ideale $\mathfrak{p} \subseteq R$ mit $R/\mathfrak{p}$ Integritätsbereich. Für ein Primideal $\mathfrak{p} \subseteq R$ ist auch $f^{-1}(\mathfrak{p}) \subseteq S$ ein Primideal. Dieser Begriff hat also die erforderliche Stabilität.

Die Menge der Primideale von R heißt auch das Spektrum $\mathrm{Spec}(R)$ und ist eine verallgemeinerte Version des Begriffs der Nullstellenmenge eines Polynoms; verallgemeinert auch in der Hinsicht, daß nicht notwendig maximale Primideale als neu hinzugekommene Punkte akzeptiert werden.

Der C-Algebrenmorphismus

$$S \xrightarrow{f} R$$

induziert einen Morphismus

$$\begin{array}{rcl} \mathrm{Spec}(S) & \xleftarrow{\mathrm{Spec}(f)} & \mathrm{Spec}(R) \\ f^{-1}(\mathfrak{p}) & \leftarrow\!\shortmid & \mathfrak{p} \end{array}$$

Ist f surjektiv, wie im obigen Beispiel, dann ist $\mathrm{Spec}(f)$ injektiv.

Nun kann man die Dimension von $\mathrm{Spec}(R)$ definieren als maximale Zahl der Inklusionen in einer echten Kette von Primidealen von R.

So etwa gibt die echte Kette von Primidealen $(0) \subset (X) \subset (X,Y)$, daß $\mathrm{Spec}(\mathbf{C}[X,Y])$ die Dimension 2 hat, was dem entspricht, daß die zu dieser $\mathbf{C}$-Algebra gehörige komplexe Ebene $\mathbf{C}^2$ zweidimensional ist.

Aus der Geometrie stammen eine Reihe weiterer Fragen. So etwa kann man die Nullstellenmenge des Polynoms $(Y - X^2)^3 \cdot (Y^2 + X^2 - 1)$ in ihre Bestandteile zerlegen, namentlich die Nullstellenmengen von $Y - X^2$ und von $Y^2 + X^2 - 1$, und das Zusammenfügen der Bestandteile geschieht durch eine nicht disjunkte Vereinigung von Parabel und Kreis. Allgemeiner führt diese Zerlegungsfrage zur Primärzerlegung eines Ideale in einer kommutativen $\mathbf{C}$-Algebra.

Organisatorisches

Inhaltlich orientieren wir uns an bekannten Darstellungen der Materie wie [**6**], [**2**], [**5**], wobei ich auch aus [**3**], [**4**], [**8**], [**1**] vieles lernen konnte. Die Verantwortung für Fehler und Unklarheiten im vorliegenden Skript trage ich natürlich selbst. Für diesbezügliche Hinweise bin ich dankbar.

Vorausgesetzt werden elementare Kenntnisse über Lineare Algebra, insbesondere der Begriff der abelschen Gruppe.

Auf Übungen und Lösungen wird im Skript manchmal Bezug genommen, sie sind daher als Bestandteil des Skripts anzusehen.

Wegen laufender Änderungen wird empfohlen, sich während des Semesters nur die Datei regelmäßig zu erneuern und erst am Ende einen Ausdruck zu erstellen.

Dank geht an Andrey Kharitenko für Vereinfachungen und Korrekturen. Dank geht an Jonas Dallendörfer, Svea Döring, Joachim Fuchs und Alexander Marroquin Nisch für Korrekturen.

Stuttgart, im Wintersemester 2017/18

Matthias Künzer

Konventionen. Seien X, Y, Z Mengen. Sei R ein kommutativer Ring.

- Es ist $\mathbf{N} = \{0, 1, 2, 3, \dots\}$.
- Ist $a \in \mathbf{Z}$, so schreiben wir $\mathbf{Z}_{\geqslant a} := \{\, z \in \mathbf{Z} :\ a \leqslant z \,\}$.
- Sind $a,\, b \in \mathbf{Z}$, so schreiben wir $[a, b] := \{\, z \in \mathbf{Z} :\ a \leqslant z \leqslant b \,\}$ für das ganzzahlige Intervall.
- Für $x,\, x' \in X$ sei $\partial_{x,y} := 1$ falls $x = y$ und $\partial_{x,y} := 0$ falls $x \neq y$.
- Es stehe "für $x \in X$" kurz für "für alle $x \in X$".
- Es bedeutet $Y \subset X$, daß $Y \subseteq X$ und $Y \neq X$ ist.
- Es bezeichnet $\mathrm{id} = \mathrm{id}_X$ die identische Abbildung von X nach X.
- Sei $f\colon X \longrightarrow Y$ eine Abbildung. Sei $X' \subseteq X$, $Y' \subseteq Y$ und $f(X') \subseteq Y'$. Wir schreiben $f|_{X'}^{Y'}\colon X' \longrightarrow Y'$, $x' \longmapsto f(x')$ für die Einschränkung. Ist $Y' = Y$, so schreiben wir auch $f|_{X'} := f|_{X'}^{Y}$. Ist $X' = X$, so schreiben wir auch $f|^{Y'} := f|_X^{Y'}$.
- Ist $f\colon X \longrightarrow Y$ bijektiv, so bezeichnet häufig $f^- := f^{-1}\colon Y \longrightarrow X$ ihre Umkehrabbildung, i.e. $f^- \circ f = \mathrm{id}_X$ und $f \circ f^- = \mathrm{id}_Y$.

  Ist $f\colon X \to Y$ eine Abbildung und ist $Y' \subseteq Y$, so schreiben wir $f^{-1}(Y') := \{\, x \in X :\ f(x) \in Y' \,\}$ für das Urbild von Y' unter f.
- Sei $(X, \leqslant)$ ein Poset, i.e. eine teilgeordnete Menge (partially ordered set).

  Es heißt $x \in X$ *minimal*, falls es kein $y \in X$ mit $y < x$ gibt. Es heißt $x \in X$ *initial*, falls $x \leqslant z$ für alle $z \in X$ gilt. Es heißt $x \in X$ *maximal*, falls es kein $y \in X$ mit $x < y$ gibt. Es heißt $x \in X$ *terminal*, falls $z \leqslant x$ für alle $z \in X$ gilt. Es existieren höchstens ein initiales und höchstens ein terminales Element in X. Für $a \in X$ schreiben wir $X_{>a} := \{\, x \in X :\ x > a \,\}$, etc.
- Sei A eine additiv geschriebene abelsche Gruppe; i.e. die Addition $(+) : A \times A \to A$ sei assoziativ, kommutativ und habe ein neutrales Element $0 = 0_A$; ferner habe jedes Element $a \in A$ ein additiv inverses Element $-a$ mit $a + (-a) = 0$. Wir schreiben oft kurz $0 := \{0\}$.
- Sei I eine Menge. Sei X_i eine Menge für $i \in I$. Schreiben wir $\bigsqcup_{i \in I} X_i$ für $\bigcup_{i \in I} X_i$, so bringen wir dadurch zum Ausdruck, daß $X_i \cap X_j = \emptyset$ ist für $i,\, j \in I$ mit $i \neq j$.

  Ist $n \in \mathbf{Z}_{\geqslant 1}$ und ist $I = [1, n]$, so schreiben wir auch $X_1 \sqcup \ldots \sqcup X_n := \bigsqcup_{i \in [1,n]} X_i$.
- Sind $a,\, b,\, x \in R$, so bedeute $a \equiv_x b$, daß es ein $r \in R$ mit $a - b = rx$ gibt.
- Für $r \in R$ und $d,\, i \in \mathbf{Z}_{\geqslant 0}$ schreiben wir $r^{d^i} := r^{(d^i)}$.
- In R ist $\sum_{i \in \emptyset} r_i := 0$ und $\prod_{i \in \emptyset} r_i := 1$.

Kapitel 1

Grundlagen

1.1 Kommutative Ringe und Ideale

1.1.1 Kommutative Ringe

Definition 1 Ein *kommutativer Ring* ist eine Menge R, zusammen mit einer Abbildung

$$(+)\colon R \times R \to R\colon (a,b) \mapsto a+b\ ,$$

und einer Abbildung

$$(\cdot)\colon R \times R \to R\colon (a,b) \mapsto a \cdot b\ ,$$

derart, daß die Eigenschaften $(1,2,3,4,5)$ gelten.

(1) Es ist $(R,+)$ eine abelsche Gruppe.

(2) Es ist $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für $a,\ b,\ c\ \in\ R$.

(3) Es ist $a \cdot b = b \cdot a$ für $a,\ b\ \in\ R$.

(4) Es gibt ein Element $1_R \in R$ mit $1_R \cdot a = a$ für $a \in R$.

(5) Es ist $(a + a') \cdot b = a \cdot b + a' \cdot b$ für $a,\ a',\ b \in R$.

Die Abbildung $(+)$ wird *Addition* genannt. Die Abbildung $(\cdot)$ wird *Multiplikation* genannt.

Das additiv neutrale Element schreiben wir $0 = 0_R$.

Oft schreiben wir $1 := 1_R$. Es ist das Element 1 durch die Eigenschaft (4) festgelegt, da ein weiteres Element $1'$ mit dieser Eigenschaft $1' = 1 \cdot 1' = 1' \cdot 1 = 1$ erfüllt.

Es ist $0 \cdot a = 0 \cdot a + 0 \cdot a - 0 \cdot a = (0+0) \cdot a - 0 \cdot a = 0 \cdot a - 0 \cdot a = 0$ für $a \in R$.

Oft schreiben wir $ab := a \cdot b$ für $a,\ b\ \in\ R$.

Sei $R^\times := R \smallsetminus \{0\} \subseteq R$.

Sei $\mathrm{U}(R) := \{\, x \in R :\ \text{es gibt ein } y \in R \text{ mit } xy = 1 \,\} \subseteq R$.

Ist $xy = 1 = xy'$ für gewisse $y,\, y' \in R$, dann ist $y = yxy' = y'$. Wir schreiben auch $x^- = x^{-1} := y$.

Es ist $\mathrm{U}(R)$, zusammen mit $(\cdot)|_{\mathrm{U}(R)\times\mathrm{U}(R)}^{\mathrm{U}(R)}$, eine abelsche Gruppe, die *Einheitengruppe* von R. Cf. Aufgabe 1.

Bemerkung 2 (und Definition) Es gibt den *Nullring* 0, welcher nur ein einziges Element $0_0 = 1_0$ enthält.

Ist umgekehrt in einem kommutativen Ring R die Gleichheit $0_R = 1_R$ erfüllt, dann ist für $x \in R$ auch $x = 1_R \cdot x = 0_R \cdot x = 0_R$, so daß der Nullring vorliegt.

Definition 3 Ein kommutativer Ring R heißt *Integritätsbereich* oder *integrer* Ring, falls $0_R \neq 1_R$ ist und falls für $a,\, b \in R$ aus $a \cdot b = 0$ folgt, daß $a = 0$ oder $b = 0$ ist.

Bemerkung 4 *Ein kommutativer Ring R, in welchem $0_R \neq 1_R$ gilt, ist ein Integritätsbereich genau dann, wenn die Abbildung*

$$\begin{array}{ccc} R & \xrightarrow{\lambda_a} & R \\ x & \mapsto & ax \end{array}$$

injektiv ist für alle $a \in R^\times$.

Beweis. Es ist λ_a ein Gruppenmorphismus auf der additiven abelschen Gruppen R. Also ist für $a \in R^\times$ die Abbildung λ_a injektiv genau dann, wenn ihr Kern gleich 0 ist, i.e. wenn für $b \in R$ aus $ab = 0$ auch $b = 0$ folgt. $\square$

Definition 5 Ein kommutativer Ring R heißt *Körper*, falls $0_R \neq 1_R$ ist und falls die Abbildung

$$\begin{array}{ccc} R & \xrightarrow{\lambda_a} & R \\ x & \mapsto & ax \end{array}$$

bijektiv ist für alle $a \in R^\times$.

Mit anderen Worten, ein kommutativer Ring R ist ein Körper, falls $\emptyset \neq R^\times = \mathrm{U}(R)$ ist.

Beispiel 6

(1) Es ist $\mathbf{Z}$ ein Integritätsbereich.

(2) Es sind $\mathbf{Q}$, $\mathbf{R}$ und $\mathbf{C}$ Körper.

Definition 7 Seien R, S und T kommutative Ringe.

Eine Abbildung $R \xrightarrow{f} S$ heißt *Ringmorphismus*, falls $(1, 2, 3)$ gelten.

(1) Es ist $f(x + y) = f(x) + f(y)$ für $x,\, y \,\in\, R$.

(2) Es ist $f(x \cdot y) = f(x) \cdot f(y)$ für $x,\, y \,\in\, R$.

(3) Es ist $f(1_R) = 1_S$.

Ist $R \xrightarrow{f} S$ ein Ringmorphismus, so ist $f(0) = f(0) + f(0) - f(0) = f(0 + 0) - f(0) = f(0) - f(0) = 0$.

Ist $R \xrightarrow{f} S$ ein Ringmorphismus und $x \in \mathrm{U}(R)$, so ist $f(x) \cdot f(x^-) = f(x \cdot x^-) = f(1) = 1$, mithin $f(x) \in \mathrm{U}(S)$ und $f(x^-) = f(x)^-$.

Es ist $R \xrightarrow{\mathrm{id}} R$ ein Ringmorphismus.

Sind $R \xrightarrow{f} S \xrightarrow{g} T$ gegebene Ringmorphismen, dann ist auch $R \xrightarrow{g \circ f} T$ ein Ringmorphimus.

Ist f ein bijektiver Ringmorphismus, dann ist auch f^- ein Ringmorphismus; cf. Aufgabe 5.(1). Ein bijektiver Ringmorphismus heißt *Ringisomorphismus*. Gibt es einen Ringisomorphismus von R nach S, so heißen R und S *isomorph*, geschrieben $R \simeq S$.

Definition 8 Sei R ein kommutativer Ring.

Eine abelsche Untergruppe $R' \subseteq R$ heißt *Teilring* von R, falls $1 \in R'$ liegt und falls für $x',\, y' \,\in\, R'$ auch $x'y' \in R'$ liegt.

Diesenfalls ist R' mit der auf R' eingeschränkten Addition und der auf R' eingeschränkten Multiplikation ein Ring.

Die Inklusionsabbildung $R' \hookrightarrow R \colon x' \mapsto x'$ ist ein Ringmorphismus.

Bemerkung 9 Seien R und S kommutative Ringe. Sei $R \xrightarrow{f} S$ ein Ringmorphismus.

Dann ist $f(R) \subseteq S$ ein Teilring.

Beweis. Es ist $1_S = f(1_R) \in f(R)$.

Seien $x',\, y' \,\in\, f(R)$. Schreibe $x' = f(x)$ und $y' = f(y)$ für gewisse Elemente $x,\, y \,\in\, R$. Dann wird $x' + y' = f(x) + f(y) = f(x + y) \in f(R)$. Ferner wird $x' \cdot y' = f(x) \cdot f(y) = f(x \cdot y) \in f(R)$. $\square$

Definition 10 Sei I eine Menge. Sei R_i ein kommutativer Ring für $i \in I$.

Wir betrachten das cartesische Produkt $R := \prod_{i \in I} R_i = \{\, (r_i)_{i \in I} :\ r_i \in R \text{ für } i \in I \,\}$.

Oft schreiben wir kurz $(r_i)_i := (r_i)_{i \in I}$.

Seien Addition und Multiplikation auf R erklärt durch

$$\begin{array}{rcl} (r_i)_i + (r'_i)_i & := & (r_i + r'_i)_i \\ (r_i)_i \cdot (r'_i)_i & := & (r_i \cdot r'_i)_i \end{array}$$

für $(r_i)_i\,,\ (r'_i)_i\ \in\ R$.

Sei ferner

$$1_R \ := \ (1_{R_i})_i \ .$$

Mit dieser Addition, dieser Multiplikation und diesem Element 1_R wird R ein kommutativer Ring, *direktes Produkt* von $(R_i)_{i\in I}$ genannt.

Für $j \in I$ ist die Projektionsabbildung

$$\begin{array}{rcl} R & \xrightarrow{\pi_j} & R_j \\ (r_i)_i & \mapsto & r_j \end{array}$$

ein Ringmorphismus.

Ist $I = [1, n]$ für ein $n \in \mathbf{Z}_{\geqslant 1}$, so schreiben wir auch $R_1 \times R_2 \times \cdots \times R_n := \prod_{i\in[1,n]} R_i$ für das direkte Produkt.

Beispiel. Es ist $\mathbf{Q}\times\mathbf{Q}$ kein Integritätsbereich. In der Tat ist $(1,0)\cdot(0,1) = (0,0) = 0_{\mathbf{Q}\times\mathbf{Q}}$, aber $(1,0) \neq 0_{\mathbf{Q}\times\mathbf{Q}} \neq (0,1)$.

Bemerkung 11 (Universelle Eigenschaft des direkten Produkts)

Sei I eine Menge. Sei R_i ein kommutativer Ring für $i \in I$. Schreibe $R := \prod_{i\in I} R_i$; cf. Definition 10*.*

Sei T ein kommutativer Ring. Sei $T \xrightarrow{t_i} R_i$ ein Ringmorphismus für $i \in I$.

Dann gibt es genau einen Ringmorphismus $T \xrightarrow{t} R$ mit $\pi_i \circ t = t_i$ für $i \in I$, namentlich

$$\begin{array}{rcl} T & \xrightarrow{t} & R \\ x & \mapsto & (t_i(x))_i \ . \end{array}$$

Beweis. Nach Konstruktion ist t die einzige Abbildung von T nach R mit $\pi_i \circ t = t_i$ für $i \in I$.

Es bleibt zu zeigen, daß t ein Ringmorphismus ist.

Es ist $t(1_T) = (t_i(1))_i = (1_{R_i})_i = 1_R$.

Für $x,\ y\ \in\ T$ ist

$$t(x+y) \ = \ (t_i(x+y))_i \ = \ (t_i(x)+t_i(y))_i \ = \ (t_i(x))_i + (t_i(y))_i \ = \ t(x)+t(y)$$

und

$$t(x\cdot y) \ = \ (t_i(x\cdot y))_i \ = \ (t_i(x)\cdot t_i(y))_i \ = \ (t_i(x))_i\cdot(t_i(y))_i \ = \ t(x)\cdot t(y) \ .$$

$\square$

1.1.2 Kommutative Algebren über einem kommutativen Grundring

Sei R ein kommutativer Ring.

Es wird R die Rolle des Grundrings spielen.

Definition 12 Eine *kommutative R-Algebra* ist ein Ring S, zusammen mit einem Ringmorphismus $R \xrightarrow{\alpha} S$. Oft schreiben wir kurz $S := (S, \alpha)$.

Man nennt eine kommutative R-Algebra auch eine *kommutative Algebra über R*.

Der Ringmorphismus α heißt auch *Strukturmorphismus* der R-Algebra $S = (S, \alpha)$.

Oft schreiben wir kurz $r := \alpha(r)$ für $r \in R$.

Für einige der im folgenden einzuführenden Begriffe und Sachverhalte wird der Strukturmorphismus nicht benötigt, wir könnten also für diese ebensogut bloße kommutative Ringe betrachten. Ich ziehe es aber vor, nicht allzuhäufig den Kontext zu wechseln. Kommutative Ringe können als $\mathbf{Z}$-Algebren aufgefaßt werden; genauer, der Vergißfunktor von den $\mathbf{Z}$-Algebren in die kommutativen Ringe, der den Strukturmorphismus vergißt, ist eine Äquivalenz. Cf. Aufgabe 5.

Definition 13 Seien kommutative R-Algebren $S = (S, \alpha)$, $T = (T, \beta)$ und $U = (U, \gamma)$ gegeben.

Ein *R-Algebrenmorphismus* von S nach T ist ein Ringmorphismus $S \xrightarrow{f} T$ mit $f \circ \alpha = \beta$.

$$\begin{tikzcd} S \arrow[rr, "f"] & & T \\ & R \arrow[ul, "\alpha"] \arrow[ur, "\beta"'] & \end{tikzcd}$$

Es ist $S \xrightarrow{\mathrm{id}} S$ ein R-Algebrenmorphismus.

Sind $S \xrightarrow{f} T \xrightarrow{g} U$ gegebene R-Algebrenmorphismen, dann ist auch $S \xrightarrow{g \circ f} U$ ein R-Algebrenmorphismus.

Ist f ein bijektiver R-Algebrenmorphismus, dann ist auch f^- ein R-Algebrenmorphismus; cf. Aufgabe 5.(2). Ein bijektiver R-Algebrenmorphismus heißt *R-Algebrenisomorphismus*. Gibt es einen R-Algebrenisomorphismus von S nach T, so heißen S und T *isomorph*, geschrieben $S \simeq T$.

Definition 14 Sei $S = (S, \alpha)$ eine kommutative R-Algebra.

Eine abelsche Untergruppe $S' \subseteq S$ heißt *R-Teilalgebra* von S, falls $S' \subseteq S$ ein Teilring ist, für welchen $\alpha(R) \subseteq S'$ liegt.

Diesenfalls ist S' zusammen mit $\alpha|^{S'}$ eine R-Algebra.

Die Inklusionsabbildung $S' \hookrightarrow S \colon x' \mapsto x'$ ist ein R-Algebrenmorphismus.

Bemerkung 15 Seien $S = (S, \alpha)$ und $T = (T, \beta)$ kommutative R-Algebren. Sei $S \xrightarrow{f} T$ ein R-Algebrenmorphismus.

Dann ist $f(S) \subseteq T$ eine R-Teilalgebra.

Beweis. Dank Bemerkung 9 ist $f(S)$ ein Teilring von T.

Ferner ist $\beta(R) = (f \circ \alpha)(R) \subseteq f(S)$. ▫

Definition 16 Sei I eine Menge. Sei $S_i = (S_i, \alpha_i)$ eine kommutative R-Algebra für $i \in I$.

Wir betrachten das direkte Produkt $S := \prod_{i \in I} S_i$. Dies ist ein Ring; cf. Definition 10.

Sei $R \xrightarrow{\alpha} S \colon r \mapsto (\alpha_i(r))_i$. Es ist α ein Ringmorphismus; cf. Bemerkung 11.

So wird $S = (S, \alpha)$ eine R-Algebra, *direktes Produkt* von $(S_i)_{i \in I}$ genannt.

Für $j \in I$ ist die Projektionsabbildung

$$\begin{array}{rcl} S & \xrightarrow{\pi_j} & S_j \\ (s_i)_i & \mapsto & s_j \end{array}$$

ein R-Algebrenmorphismus.

Ist $I = [1, n]$ für ein $n \in \mathbf{Z}_{\geqslant 1}$, so schreiben wir auch $S_1 \times S_2 \times \cdots \times S_n := \prod_{i \in [1,n]} S_i$ für das direkte Produkt.

Bemerkung 17 (Universelle Eigenschaft des direkten Produktes)

Sei I eine Menge. Sei $S_i = (S_i, \alpha_i)$ eine R-Algebra für $i \in I$. Schreibe $S := \prod_{i \in I} S_i$; cf. Definition 16*.*

Sei $T = (T, \beta)$ eine R-Algebra. Sei $T \xrightarrow{t_i} S_i$ ein R-Algebrenmorphismus für $i \in I$.

Dann gibt es genau einen R-Algebrenmorphismus $T \xrightarrow{t} S$ mit $\pi_i \circ t = t_i$ für $i \in I$, namentlich

$$\begin{array}{rcl} T & \xrightarrow{t} & S \\ x & \mapsto & (t_i(x))_i \ . \end{array}$$

Beweis. Nach Konstruktion ist t die einzige Abbildung von T nach R mit $\pi_i \circ t = t_i$ für $i \in I$.

Es bleibt zu zeigen, daß t ein R-Algebrenmorphismus ist.

Dank Bemerkung 11 ist t ein Ringmorphismus.

Für $r \in R$ ist

$$(t \circ \beta)(r) \ = \ (t_i(\beta(r)))_i \ = \ (\alpha_i(r))_i \ = \ \alpha(r) \ .$$

Mithin ist $t \circ \beta = \alpha$. ▫

Definition 18 Sei I eine Menge.

Sei $X = \{\, X_i :\ i \in I \,\}$ eine Menge, wobei die Abbildung $I \to X : i \mapsto X_i$ bijektiv sei.

Schreibe

$$E_I \ :=\ \Big\{\, (e_i)_{i\in I} \in \prod_{i\in I} \mathbf{Z}_{\geqslant 0} :\ \text{die Menge } \{\, i \in I :\ e_i \neq 0 \,\} \text{ ist endlich} \,\Big\}\ .$$

Wir schreiben oft $(e_i)_i := (e_i)_{i\in I}$.

Für $e' = (e'_i)_i$, $e'' = (e''_i)_i \ \in\ E_I$ ist auch $e' + e'' := (e'_i + e''_i)_i \in E_I$.

Sei

$$R[X] \ :=\ \{\, (r_e)_{e\in E_I} \in \prod_{e\in E_I} R :\ \text{die Menge } \{\, e \in E_I :\ r_e \neq 0 \,\} \text{ ist endlich} \,\}\ .$$

Wir schreiben oft $(r_e)_e := (r_e)_{e\in E_I}$.

Für $(r'_e)_e$, $(r''_e)_e \ \in\ R[X]$ sei

$$(r'_e)_e + (r''_e)_e \ :=\ (r'_e + r''_e)_e \ \in\ R[X]$$

und

$$(r'_e)_e \cdot (r''_e)_e \ :=\ \Big(\sum_{\substack{(e',\,e'')\,\in\, E_I\times E_I \\ e'+e''\,=\,e}} r'_{e'}\, r'_{e''} \Big)_e \ \in\ R[X]\ .$$

Sei ferner

$$\begin{array}{ccc} R & \xrightarrow{\alpha_{R,X}} & R[X] \\ r & \mapsto & (r\partial_{(0)_i,\,e})_e\ . \end{array}$$

Es ist $R[X]$, zusammen mit $(+)$, $(\cdot)$ und $\alpha_{R,X}$, eine kommutative R-Algebra, genannt die *Polynomalgebra* in $X = (X_i)_{i\in I}$ über R; cf. XXXUeXXX.

Schreiben wir für $j \in I$ etwas mißbräuchlich $d[j] := (\partial_{j,i})_i$ und $X_j := (\partial_{d[j],e})_e$, so erhalten wir für $(r_e)_e \in R[X]$ die Gleichheit

$$(r_e)_{e\in E_I} \ =\ \sum_{e\,=\,(e_i)_i\,\in\, E_I} r_e \prod_{i\in I} X_i^{e_i}\ ;$$

cf. XXXUeXXX. Man kann auch abkürzen zu $X^e := \prod_{i\in I} X_i^{e_i}$ für $e \in E_I$ und zu

$$\sum_{e\,\in\, E_I} r_e X^e \ :=\ \sum_{e\,=\,(e_i)_i\,\in\, E_I} r_e \prod_{i\in I} X_i^{e_i}\ .$$

Man sagt, $r_e X^e$ sei ein *Monom* des *Polynoms* $\sum_{e\,\in\, E_I} r_e X^e$.

Damit ergibt sich die Summe zweier Polynome $\sum_{e\,\in\, E_I} r'_e X^e$, $\sum_{e\,\in\, E_I} r''_e X^e \ \in\ R[X]$ zu

$$\Big(\sum_{e\,\in\, E_I} r'_e X^e \Big) + \Big(\sum_{e\,\in\, E_I} r''_e X^e \Big) \ =\ \Big(\sum_{e\,\in\, E_I} (r'_e + r''_e) X^e \Big)$$

und ihr Produkt zu

$$\Big(\sum_{e'\,\in\,E_I} r'_e X^e\Big)\cdot\Big(\sum_{e\,\in\,E_I} r''_e X^e\Big) \;=\; \sum_{e\,\in\,E_I}\Big(\sum_{(e',e'')\in E_I\times E_I,\; e'+e''=e} r'_{e'} r''_{e''}\Big) X^e\;,$$

Der Strukturmorphismus ist gegeben durch

$$\begin{array}{ccc} R & \xrightarrow{\alpha_{R,X}} & R[X] \\ r & \mapsto & r\;, \end{array}$$

unter Verwendung der Schreibweise $r = r\prod_{i\in I} X_i^0$.

Oft schreiben wir $R[X_i\colon i\in I] := R[X]$.

Ist $n\in\mathbf{Z}_{\geqslant 1}$ und ist $I = [1,n]$, so schreiben wir auch $R[X_1,X_2,\dots,X_n] := R[X]$.

Auch nicht eigens indizierte Mengen sind zugelassen, um eine Polynomalgebra zu bilden, wie etwa $R[X,Y,Z]$. Dies ist dann nur eine Umbezeichnung.

Beispiel 19 Sei $R = \mathbf{Z}$. Sei $I = \{1,2\}$.

In $\mathbf{Z}[X_1\,,X_2]$ gehört zu $(r_e)_e$ mit $r_{(2,1)} = 7$, mit $r_{(3,0)} = 5$ und $r_e = 0$ für $e\in E_{\{1,2\}}\smallsetminus\{(2,1),(3,0)\}$ Polynom

$$7X^{(2,1)} + 5X^{(3,0)} \;=\; 7X_1^2X_2 + 5X_1^3\;.$$

Lemma 20 (Universelle Eigenschaft der Polynomalgebra) *Sei I eine Menge. Sei $X = \{\, X_i\,:\; i\in I\,\}$ eine Menge mit $I\to X : i\mapsto X_i$ bijektiv.*

Sei $T = (T,\beta)$ eine kommutative R-Algebra. Sei $u\colon X\to T$ eine Abbildung.

Dann gibt es genau einen R-Algebrenmorphismus $f\colon R[X]\to T$, für welchen $f(X_i) = u(X_i)$ ist für $i\in I$.

Dieser Morphismus ist gegeben durch

$$\begin{array}{ccc} R[X] & \xrightarrow{f} & T \\ \sum\limits_{e\,=\,(e_i)_i\,\in\,E_I} r_e\;\prod_{i\in I} X_i^{e_i} & \mapsto & \sum\limits_{e\,=\,(e_i)_i\,\in\,E_I} \beta(r_e)\;\prod_{i\in I} u(X_i)^{e_i}\;. \end{array}$$

Beweis.

Eindeutigkeit. Sei $f\colon R[X]\to T$ ein R-Algebrenmorphismus mit $f(X_i) = u(X_i)$ ist für $i\in I$. Dann ist

$$\begin{aligned} f\Big(\sum_{e\,=\,(e_i)_i\,\in\,E_I} r_e\;\prod_{i\in I} X_i^{e_i}\Big) \;&=\; \sum_{e\,=\,(e_i)_i\,\in\,E_I} f\Big(r_e\;\prod_{i\in I} X_i^{e_i}\Big) \;=\; \sum_{e\,=\,(e_i)_i\,\in\,E_I} f\Big(\alpha(r_e)\;\prod_{i\in I} X_i^{e_i}\Big) \\ &=\; \sum_{e\,=\,(e_i)_i\,\in\,E_I} f(\alpha(r_e))\;\prod_{i\in I} f(X_i)^{e_i} \;=\; \sum_{e\,=\,(e_i)_i\,\in\,E_I} \beta(r_e)\;\prod_{i\in I} u(X_i)^{e_i}\;. \end{aligned}$$

für $\sum_{e=(e_i)_i\in E_I} r_e \ \prod_{i\in I} X_i^{e_i} \in R[X]$, unabhängig von f.

Existenz. Setze

$$f\Big(\sum_{e=(e_i)_i\in E_I} r_e \prod_{i\in I} X_i^{e_i}\Big) \ := \sum_{e=(e_i)_i\in E_I} \beta(r_e) \prod_{i\in I} u(X_i)^{e_i} \ .$$

Dann ist $f(X_i) = u(X_i)$. Ferner ist $f(\alpha(r)) = \beta(r)$ für $r \in R$, i.e. $f \circ \alpha = \beta$.

Es bleibt zu zeigen, daß f ein Ringmorphismus ist.

Es ist $f(1) = \beta(1) = 1$.

Für $\displaystyle\sum_{e=(e_i)_i\in E_I} r'_e \ \prod_{i\in I} X_i^{e_i}$ und $\displaystyle\sum_{e=(e_i)_i\in E_I} r''_e \ \prod_{i\in I} X_i^{e_i}$ aus $R[X]$ ist

$$\begin{aligned}
& f\Big(\Big(\sum_{e=(e_i)_i\in E_I} r'_e \ \prod_{i\in I} X_i^{e_i}\Big) + \Big(\sum_{e=(e_i)_i\in E_I} r''_e \ \prod_{i\in I} X_i^{e_i}\Big)\Big) \\
= \ & f\Big(\sum_{e=(e_i)_i\in E_I} (r'_e + r''_e) \ \prod_{i\in I} X_i^{e_i}\Big) \\
= \ & \sum_{e=(e_i)_i\in E_I} \beta(r'_e + r''_e) \ \prod_{i\in I} u(X_i)^{e_i} \\
= \ & \sum_{e=(e_i)_i\in E_I} (\beta(r'_e) + \beta(r''_e)) \ \prod_{i\in I} u(X_i)^{e_i} \\
= \ & \Big(\sum_{e=(e_i)_i\in E_I} \beta(r'_e) \ \prod_{i\in I} u(X_i)^{e_i}\Big) + \Big(\sum_{e=(e_i)_i\in E_I} \beta(r''_e) \ \prod_{i\in I} u(X_i)^{e_i}\Big) \\
= \ & f\Big(\sum_{e=(e_i)_i\in E_I} r'_e \ \prod_{i\in I} X_i^{e_i}\Big) + f\Big(\sum_{e=(e_i)_i\in E_I} r''_e \ \prod_{i\in I} X_i^{e_i}\Big)
\end{aligned}$$

und

$$\begin{aligned}
& f\Big(\Big(\sum_{e'=(e'_i)_i\in E_I} r'_{e'} \ \prod_{i\in I} X_i^{e'_i}\Big) \cdot \Big(\sum_{e''=(e''_i)_i\in E_I} r''_{e''} \ \prod_{i\in I} X_i^{e''_i}\Big)\Big) \\
= \ & f\Big(\sum_{e\in E_I}\Big(\sum_{(e',e'')\in E_I\times E_I,\, e'+e''=e} r'_{e'} r''_{e''}\Big) \prod_{i\in I} X_i^{e_i}\Big) \\
= \ & \sum_{e\in E_I}\beta\Big(\sum_{(e',e'')\in E_I\times E_I,\, e'+e''=e} r'_{e'} r''_{e''}\Big) \prod_{i\in I} u(X_i)^{e_i}\Big) \\
= \ & \sum_{e\in E_I}\Big(\sum_{(e',e'')\in E_I\times E_I,\, e'+e''=e} \beta(r'_{e'})\cdot\beta(r''_{e''})\Big) \prod_{i\in I} u(X_i)^{e_i}\Big) \\
= \ & \sum_{(e',e'')\in E_I\times E_I} \beta(r'_{e'})\cdot\beta(r''_{e''}) \prod_{i\in I} u(X_i)^{e'_i+e''_i} \\
= \ & \Big(\sum_{e'=(e'_i)_i\in E_I} \beta(r'_{e'}) \ \prod_{i\in I} u(X_i)^{e'_i}\Big) \cdot \Big(\sum_{e''=(e''_i)_i\in E_I} \beta(r''_{e''}) \ \prod_{i\in I} u(X_i)^{e''_i}\Big) \\
= \ & f\Big(\sum_{e'=(e'_i)_i\in E_I} r'_{e'} \ \prod_{i\in I} X_i^{e'_i}\Big) \cdot f\Big(\sum_{e''=(e''_i)_i\in E_I} r''_{e''} \ \prod_{i\in I} X_i^{e''_i}\Big)
\end{aligned}$$

□

Bemerkung 21 *Seien I und J disjunkte Mengen.*

Sei $X = \{ X_i : i \in I \}$ eine Menge mit $I \to X : i \mapsto X_i$ bijektiv.

Sei $Y = \{ Y_j : j \in J \}$ eine Menge mit $J \to Y : j \mapsto Y_j$ bijektiv.

Seien X und Y disjunkt.

Wir haben die Bijektion $I \sqcup J \to X \sqcup Y$, $i \mapsto X_i$ für $i \in I$, $j \mapsto Y_j$ für $j \in J$.

Es ist $(R[X])[Y]$ eine R-Algebra via $\alpha_{R[X],Y} \circ \alpha_{R,X} : R \mapsto (R[X])[Y]$.

Wir erhalten die sich invertierenden R-Algebrenisomorphismen

$$
\begin{array}{rcll}
(R[X])[Y] & \xrightarrow{f} & R[X \sqcup Y] & \\
X_i & \mapsto & X_i & \text{für } i \in I \\
Y_j & \mapsto & Y_j & \text{für } j \in J
\end{array}
$$

$$
\begin{array}{rcll}
(R[X])[Y] & \xleftarrow{g} & R[X \sqcup Y] & \\
X_i & \leftarrow\!\shortmid & X_i & \text{für } i \in I \\
Y_j & \leftarrow\!\shortmid & Y_j & \text{für } j \in J
\end{array}
$$

Wir identifizieren die beiden R-Algebren entlang diesem Isomorphismus.

Folgender Beweis soll mit Lemma 20 auskommen.

Beweis. Dank Lemma 20 gibt es den R-Algebrenmorphismus

$$u : R[X] \to R[X \sqcup Y] : X_i \mapsto X_i \qquad \text{für } i \in I\ .$$

Dank Lemma 20 gibt es den $R[X]$-Algebrenmorphismus

$$f : R[X][Y] \to R[X][Y] : R[X \sqcup Y] : Y_j \mapsto Y_j \qquad \text{für } j \in J\ .$$

Es ist f ein R-Algebrenmorphismus wegen $f \circ (\alpha_{R[X],Y} \circ \alpha_{R,X}) = u \circ \alpha_{R,X} = \alpha_{R,X \sqcup Y}$.

Dank Lemma 20 gibt es den R-Algebrenmorphismus $g : R[X \sqcup Y] \to (R[X])[Y]$, der X_i nach X_i schickt für $i \in I$ und Y_j nach Y_j für $j \in J$.

Es schicken die R-Algebrenmorphismen $f \circ g$ und $\mathrm{id}_{R[X \sqcup Y]}$ beide X_i nach X_i für $i \in I$ und Y_j nach Y_j für $j \in J$. Dank Lemma 20 ist also $f \circ g = \mathrm{id}_{R[X \sqcup Y]}$.

Es ist $\alpha_{R[X],Y}$ ein R-Algebrenmorphismus nach Konstruktion: es ist $\alpha_{R[X],Y} \circ \alpha_{R,X} = (\alpha_{R[X],Y} \circ \alpha_{R,X})$.

Es schickt $g \circ f$ ebenfalls X_i nach X_i für $i \in I$ und Y_j nach Y_j für $j \in J$. Es sind $g \circ f \circ \alpha_{R[X],Y}$ und $\alpha_{R[X],Y}$ zwei R-Algebrenmorphismen, die X_i nach X_i schicken für $i \in I$. Also ist $g \circ f \circ \alpha_{R[X],Y} = \alpha_{R[X],Y}$ dank Lemma 20. I.e. es ist $g \circ f$ ein $R[X]$-Algebrenmorphismus.

Somit sind $g \circ f$ und $\mathrm{id}_{(R[X])[Y]}$ zwei $R[X]$-Algebrenmorphismen, die Y_j nach Y_j schicken für $j \in J$. Also ist $g \circ f = \mathrm{id}_{(R[X])[Y]}$. □

Bemerkung 22 *Sei I eine Menge.*

Sei $X = \{ X_i : i \in I \}$ eine Menge mit $I \to X : i \mapsto X_i$ bijektiv.

Ist R integer, dann ist auch $R[X]$ integer.

Beweis. Seien $a := \sum_{e \in E_I} r'_e X^e$ und $b := \sum_{e \in E_I} r''_e X^e$ in $R[X]$ gegeben mit $ab = 0$. Sei $a \neq 0$. Wir haben $b \overset{!}{=} 0$ zu zeigen.

Sei $\tilde{E}_I := \{ e \in E_I : r'_e \neq 0 \text{ oder } r''_e \neq 0 \}$. Es ist $\tilde{E}_I$ eine endliche Menge als Vereinigung zweier endlicher Mengen.

Sei $\tilde{I} := \{ i \in I : \text{ es gibt ein } e \in \tilde{E}_I \text{ mit } e_i \neq 0 \}$. Es ist $\tilde{I}$ eine endliche Menge als Vereinigung endlich vieler endlicher Mengen.

Es ist $a, b \in R[X_i : i \in \tilde{I}] \subseteq R[X_i : i \in I] = R[X]$.

Somit können wir I als endlich annehmen. O.E. $X = \{ X_i : i \in [1, n] \}$ für ein $n \geqslant \mathbf{Z}_{\geqslant 0}$.

Mit Induktion genügt es zu zeigen, daß aus $R[X_1, \ldots, X_{m-1}]$ integer folgt, daß $R[X_1, \ldots, X_m]$ integer ist für $m \in [1, n]$.

Dank Bemerkung 21 genügt es also zu zeigen, daß für eine gegebene integre R-Algebra S auch $S[Y]$ integer ist, wobei Y eine einzelne Variable sei.

Sei also wieder $a, b \in S[Y]$, $a \neq 0$, aber $ab = 0$. *Annahme,* es ist $b \neq 0$. Schreibe $a = \sum_{i \in [0,k]} s'_i Y^i$ und $b = \sum_{j \in [0,\ell]} s''_j Y^j$, wobei $s'_k \neq 0$ und $s''_\ell \neq 0$. Da ab gleich 0 ist, ist auch der Koeffizient dieses Produktes bei $Y^{k+\ell}$ gleich 0. I.e. es ist $s'_k s''_\ell = 0$. Dies steht aber im *Widerspruch* zu S integer. ▫

Bemerkung 23 Sei S eine kommutative R-Algebra.

Wähle $X = \{ X_s : s \in S \}$ mit $S \to X : s \mapsto X_s$ bijektiv.

Nach Lemma 20 haben wir den R-Algebrenmorphismus

$$\begin{array}{rcll} R[X] & \to & S & \\ X_s & \mapsto & s & \text{für } s \in S \end{array}$$

Nach Konstruktion ist dieser surjektiv.

Man kann also R-Algebren studieren, indem man Polynomalgebren über R studiert und surjektive R-Algebrenmorphismen, die von diesen ausgehen.

Bemerkung. Sei S eine kommutative R-Algebra. Sei $M \subseteq S$ eine Teilmenge.

Seien I und $X = \{ X_i : i \in I \}$ Mengen derart, daß $i \mapsto X_i$ bijektiv ist und derart, daß wir eine Bijektion $I \mapsto M$, $i \mapsto m_i$ wählen können.

Dann gibt es genau einen R-Algebrenmorphismus $f : R[X] \to S$ mit $X_i \mapsto m_i$ für $i \in I$; cf. Lemma 20.

Sein Bild wird auch $R[m_i : i \in I] := f(R[X])$ geschrieben, ist eine R-Teilalgebra von S, die M enthält. Es heißt $R[m_i : i \in I]$ auch *R-Algebrenerzeugnis* von M in S. Ist $n \in \mathbf{Z}_{\geqslant 1}$ und ist $I = [1, n]$, so schreiben wir auch $R[m_1, \ldots, m_n] := R[m_i : i \in [1, n]]$.

Ist $T \subseteq S$ eine R-Teilalgebra, die M enthält, dann gibt es genau einen R-Algebrenmorphismus $g\colon R[X] \to T$ mit $X_i \mapsto m_i$ für $i \in I$; cf. Lemma 20. Ist $j\colon T \to S\colon t \mapsto t$ die Inklusionsabbildung, dann bildet auch $j \circ g$ für alle $i \in I$ das Element X_i auf m_i ab, ist also gleich f. Insbesondere ist

$$R[m_i : i \in I] \;=\; f(R[X]) \;=\; (j \circ g)(R[X]) \;\subseteq\; T\ .$$

Also ist $R[m_i : i \in I]$ die initiale R-Teilalgebra von S, die M enthält.

1.1.3 Ideale

Sei R ein kommutativer Ring. Seien kommutative R-Algebren $S = (S, \alpha)$ und $T = (T, \beta)$ gegeben.

Definition 24 Eine abelsche Untergruppe $\mathfrak{a} \subseteq S$ heißt *Ideal* in S, falls aus $s \in S$ und $a \in \mathfrak{a}$ auch $sa \in \mathfrak{a}$ folgt.

Mit anderen Worten, $\mathfrak{a}$ ist ein Ideal in S genau dann, wenn $0 \in \mathfrak{a}$ liegt und wenn für $s,\ s' \in S$ und $a,\ a' \in \mathfrak{a}$ auch $sa + s'a' \in \mathfrak{a}$ liegt.

Wir schreiben auch $\mathfrak{a}^\times := \mathfrak{a} \smallsetminus \{0\}$.

Definition 25 Sei $\mathfrak{a} \subseteq S$ ein Ideal.

Auf der Faktorgruppe $S/\mathfrak{a}$ definieren wir die Multiplikation durch

$$(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) := x \cdot y + \mathfrak{a}\ ,$$

wobei $x,\ y \in S$. Dann ist $S/\mathfrak{a}$ ein Ring, wobei $1_{S/\mathfrak{a}} = 1_S + \mathfrak{a}$ ist; cf. XXXUeXXX.

Wir haben den Ringmorphismus

$$\begin{array}{ccc} S & \xrightarrow{\rho_{S,\mathfrak{a}}} & S/\mathfrak{a} \\ s & \mapsto & s + \mathfrak{a}\ , \end{array}$$

genannt *Restklassenmorphismus* und oft auch nur $\rho := \rho_{S,\mathfrak{a}}$ geschrieben.

Es ist $S/\mathfrak{a} = (S/\mathfrak{a}, \rho_{S,\mathfrak{a}} \circ \alpha)$ eine kommutative R-Algebra, genannt *R-Faktoralgebra* von S modulo $\mathfrak{a}$.

Es ist $\rho_{S,\mathfrak{a}}$ wegen $\rho_{S,\mathfrak{a}} \circ \alpha = (\rho_{S,\mathfrak{a}} \circ \alpha)$ nach Konstruktion ein R-Algebrenmorphismus.

Bemerkung 26 (Universelle Eigenschaft der Faktoralgebra)

Sei $\mathfrak{a} \subseteq S$ *ein Ideal.*

Sei $S \xrightarrow{f} T$ *ein* R*-Algebrenmorphismus mit* $f(\mathfrak{a}) = 0$.

Dann gibt es genau einen R*-Algebrenmorphismus* $\bar{f}\colon S/\mathfrak{a} \to T$ *mit* $\bar{f} \circ \rho_{S,\mathfrak{a}} = f$.

Namentlich, es ist $\bar{f}(s + \mathfrak{a}) = f(s)$ *für* $s \in S$.

Beweis. Die Eindeutigkeit von $\bar{f}$ mit $\bar{f} \circ \rho_{S,\mathfrak{a}} = f$ folgt aus der Surjektivität von $\rho_{S,\mathfrak{a}}$.

Die Existenz von $\bar{f}$ mit $\bar{f} \circ \rho_{S,\mathfrak{a}} = f$ fordert gerade, daß $\bar{f}(s+\mathfrak{a}) = f(s)$ sein soll für $s \in S$.

Es ist bekannt, daß $\bar{f}$ als Gruppenmorphismus zwischen abelschen Gruppen existiert. In der Tat sind $s,\, s' \in S$ mit $s + \mathfrak{a} = s' + \mathfrak{a}$ gegeben, dann ist $s' = s + a$ für ein $a \in \mathfrak{a}$ und also $f(s') = f(s + a) = f(s) + s(a) = f(s)$; da f mit Addition verträglich ist, gilt dies dann auch für $\bar{f}$.

Es ist $\bar{f}$ ein Ringmorphismus, da $\bar{f}(1_{S/\mathfrak{a}}) = \bar{f}(1_S + \mathfrak{a}) = f(1_S) = 1_T$ ist und da

$$\bar{f}((s + \mathfrak{a}) \cdot (s' + \mathfrak{a})) \;=\; \bar{f}(s \cdot s' + \mathfrak{a}) \;=\; f(s \cdot s') \;=\; f(s) \cdot f(s') \;=\; \bar{f}(s + \mathfrak{a}) \cdot \bar{f}(s' + \mathfrak{a})$$

ist für $s,\, s' \in S$. □

Definition 27 Sei $S \xrightarrow{f} T$ ein R-Algebrenmorphismus.

Sei $\mathrm{Kern}(f) := f^{-1}(\{0\}) \subseteq S$.

Es ist $\mathrm{Kern}(f) \subseteq S$ ein Ideal; cf. Aufgabe 8.(1).

Wir haben den injektiven R-Algebrenmorphismus

$$\begin{array}{rcl} S/\,\mathrm{Kern}(f) & \xrightarrow{\bar{f}} & T \\ s + \mathrm{Kern}(f) & \mapsto & f(s)\,; \end{array}$$

cf. Aufgabe 8.(3).

Es ist also $\bar{f}|^{f(S)} : S/\,\mathrm{Kern}(f) \to f(S)$ ein R-Algebrenisomorphismus; cf. Bemerkung 15.

Falls f surjektiv ist, ist also $\bar{f}$ ein Isomorphismus.

Bemerkung 28 Für jede kommutative R-Algebra T existiert ein surjektiver R-Algebrenmorphismus $R[X] \xrightarrow{f} T$ von einer Polynomalgebra $R[X]$; cf. Bemerkung 23. Folglich ist $T \simeq R[X]/\,\mathrm{Kern}(f)$.

Bis auf Isomorphie ist also jede R-Algebra von der Form $R[X]/\mathfrak{a}$ für eine geeignete Menge X und ein geeignetes Ideal $\mathfrak{a} \subseteq R[X]$.

Bemerkung 29 *Sei* I *eine Menge. Sei* $\mathfrak{a}_i \subseteq S$ *ein Ideal für* $i \in I$.

(1) *Es ist*

$$\sum_{i\in I} \mathfrak{a}_i \;:=\; \Big\{\, \sum_{i\in I} a_i : \; a_i \in \mathfrak{a}_i \textit{ für } i \in I, \textit{ wobei } \{\, i\in I : \; a_i \neq 0 \,\} \textit{ endlich ist} \Big\} \;\subseteq\; S\,.$$

ein Ideal in S*.*

(2) *Es ist* $\bigcap_{i\in I} \mathfrak{a}_i$ *ein Ideal in* S*.*

(3) *Sei* $I = [1,n]$ *für ein* $n \in \mathbf{Z}_{\geqslant 1}$.

Sei

$$M \;:=\; \{\, a_1 \cdot a_2 \cdots a_n : \; a_i \in \mathfrak{a}_i \textit{ für } i \in [1,n] \,\}\,.$$

Es ist

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n \;:=\; \Big\{ \sum_{j\in[1,k]} m_j : \; k \in \mathbf{Z}_{\geqslant 0}\,,\; s_j \in S \textit{ und } m_j \in M \textit{ für } j \in [1,k] \Big\} \;\subseteq\; S$$

ein Ideal.

Das Produkt aus null Idealfaktoren sei gleich S*.*

Es ist $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \cdots \cdot \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n$.

Beweis.

Ad (1). Es ist $\sum_{i\in I} \mathfrak{a}_i$ eine abelsche Untegruppe von S. Denn zum einen ist $0 \in \sum_{i\in I} \mathfrak{a}_i$. Sind zum anderen $\sum_{i\in I} a_i$ und $\sum_{i\in I} a'_i$ gegeben mit $a_i,\, a'_i \in \mathfrak{a}_i$ für $i \in I$ mit $\{\, i \in I : \; a_i \neq 0 \,\}$ und $\{\, i \in I : \; a'_i \neq 0 \,\}$ endlich gegeben, dann ist wegen $-1 \in S$ auch $1 \cdot a_i + (-1) \cdot a'_i = -a'_i \in \mathfrak{a}_i$ für $i \in I$ und $\{\, i \in I : \; a_i - a'_i \neq 0 \,\}$ endlich und somit

$$\Big(\sum_{i\in I} a_i\Big) - \Big(\sum_{i\in I} a'_i\Big) \;=\; \sum_{i\in I} (a_i - a'_i) \;\in\; \sum_{i\in I} \mathfrak{a}_i\,.$$

Es ist die abelsche Untegruppe $\sum_{i\in I} \mathfrak{a}_i$ ein Ideal in S. Denn ist $s \in S$ gegeben und $\sum_{i\in I} a_i$ gegeben mit $a_i \in \mathfrak{a}_i$ für $i \in I$ mit $\{\, i \in I : \; a_i \neq 0 \,\}$ endlich, dann ist auch $sa_i \in \mathfrak{a}_i$ für $i \in I$ und $\{\, i \in I : \; sa_i \neq 0 \,\}$ als Teilmenge von $\{\, i \in I : \; a_i \neq 0 \,\}$ endlich und somit

$$s\Big(\sum_{i\in I} a_i\Big) \;=\; \sum_{i\in I} sa_i \;\in\; \sum_{i\in I} \mathfrak{a}_i\,.$$

Ist $I = [1,n]$ für ein $n \in \mathbf{Z}_{\geqslant 1}$, so schreiben wir auch $\mathfrak{a}_1 + \mathfrak{a}_2 + \cdots + \mathfrak{a}_n := \sum_{i\in[1,n]} \mathfrak{a}_i$.

Ad (2). Es ist $\bigcap_{i\in I} \mathfrak{a}_i \subseteq R$ eine abelsche Untergruppe.

Ist $s \in S$ und $x \in \bigcap_{i\in I} \mathfrak{a}_i$, dann ist $x \in \mathfrak{a}_i$ für $i \in I$, also $sx \in \mathfrak{a}_i$ für $i \in I$ und somit $sx \in \bigcap_{i\in I} \mathfrak{a}_i$.

Ad (3). Ist $s \in S$ und $m \in M$, dann ist $m = a_1 \cdot a_2 \cdots a_n$ mit $a_i \in \mathfrak{a}_i$ für $i \in [1,n]$ und also $sm = (sa_1) \cdot a_2 \cdots a_n \in M$.

Es ist $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n$ eine abelsche Untegruppe von S. Denn es ist $0 \in \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n$. Sind ferner $s,\, s' \in S$ und $\sum_{j\in[1,k]} m_j$ mit $m_j \in M$ für $j \in [1,k]$ und $\sum_{j\in[1,\ell]} m'_j$ gegeben mit $m'_j \in M$ für $j \in [1,\ell]$ gegeben, dann ist auch

$$s \cdot \Big(\sum_{j\in[1,k]} m_j\Big) + s' \cdot \Big(\sum_{j\in[1,k]} m'_j\Big) \;=\; \Big(\sum_{j\in[1,k]} sm_j\Big) + s' \cdot \Big(\sum_{j\in[1,k]} s'm'_j\Big) \;\in\; \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n\ .$$

□

Bemerkung 30 *Sei* $\mathfrak{a} \subseteq S$ *ein Ideal.*

Es ist genau dann $\mathfrak{a} = S$*, wenn* $\mathfrak{a} \cap \mathrm{U}(S) \neq \emptyset$ *ist.*

Beweis. Ist $\mathfrak{a} = S$, dann ist $1 \in \mathfrak{a} \cap \mathrm{U}(S)$.

Ist umgekehrt $\mathfrak{a} \cap \mathrm{U}(S) \neq \emptyset$, dann wählen wir $u \in \mathfrak{a} \cap \mathrm{U}(S)$. Ist $s \in S$ gegeben, dann haben wir $s \overset{!}{\in} \mathfrak{a}$ zu zeigen.

In der Tat ist $s = (su^{-})u \in \mathfrak{a}$ wegen $u \in \mathfrak{a}$. □

Definition 31 Sei $n \in \mathbf{Z}_{\geqslant 0}$. Sei $a_i \in S$ für $i \in [1,n]$. Sei

$$(a_i\colon i \in [1,n]) \;=\; \Big\{ \sum_{i\in[1,n]} s_i a_i \,:\; s_i \in S \text{ für } i \in [1,n] \Big\}$$

das *Idealerzeugnis* der Elemente $a_1\,, a_2\,, \ldots\,, a_n$.

Wir schreiben auch $(\, a_1\,,\; a_2\,,\; \ldots\; a_n\,) := (\, a_i\colon i \in [1,n])$.

Es ist $(a_i\colon i \in [1,n])$ ein Ideal, das $\{\, a_i :\; i \in [1,n]\,\}$ als Teilmenge enthält.

Ist $\mathfrak{a} \subseteq S$ ein Ideal, das $\{\, a_i :\; i \in [1,n]\,\}$ als Teilmenge enthält, dann ist $(a_i\colon i \in [1,n]) \subseteq \mathfrak{a}$.

Insbesondere ist $() = (0)$.

Definition 32

(1) Ein Element $t \in T$ heißt *nilpotent*, falls es ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $t^n = 0$ gibt.

(2) Ein Element $t \in T^\times$ heißt ein *Nullteiler* in T, falls es ein $t' \in T^\times$ mit $tt' = 0$ gibt.

(3) Wir erinnern daran, daß T integer heißt, falls $0_T \neq 1_T$ ist und falls T keine Nullteiler enthält.

(4) Es heiße T *fast integer*, falls $0_T \neq 1_T$ ist und falls jeder Nullteiler in T nilpotent ist.

Definition 33

(1) Ein Ideal $\mathfrak{m} \subseteq S$ heißt *maximal*, falls $S/\mathfrak{m}$ ein Körper ist.

(2) Ein Ideal $\mathfrak{p} \subseteq S$ heißt *prim* oder ein *Primideal*, falls $S/\mathfrak{p}$ integer ist.

(3) Ein Ideal $\mathfrak{p} \subseteq S$ heißt *primär* oder ein *Primärideal*, falls $S/\mathfrak{p}$ fast integer ist.

Wir haben für ein Ideal in S also die folgenden Implikationen.

$$\text{maximal} \quad \Longrightarrow \quad \text{prim} \quad \Longrightarrow \quad \text{primär}$$

Bemerkung 34 *Ein Ideal $\mathfrak{m} \subseteq S$ ist maximal im Sinne von Definition* 33.(1) *genau dann, wenn $\mathfrak{m} \subset S$ ist und wenn es kein Ideal $\mathfrak{a} \subseteq S$ gibt mit $\mathfrak{m} \subset \mathfrak{a} \subset S$.*

Insbesondere ist S genau dann ein Körper, wenn S zwei Ideale enthält.

Beweis. Sei zum einen $\mathfrak{m}$ ein maximales Ideal von S. Da Da $S/\mathfrak{m}$ ein Körper ist, ist $0_{S/\mathfrak{m}} \neq 1_{S/\mathfrak{m}}$ und also $\mathfrak{m} \subset S$. Sei $\mathfrak{a} \subseteq S$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a} \subseteq S$. Wir haben $\mathfrak{a} \overset{!}{=} S$ zu zeigen. Sei $a \in \mathfrak{a} \setminus \mathfrak{m}$. Dann ist $a + \mathfrak{m} \neq 0$ und somit eine Einheit in $S/\mathfrak{m}$. Es gibt also ein $x \in S$ mit

$$ax + \mathfrak{m} \;=\; (a + \mathfrak{m})(x + \mathfrak{m}) \;=\; 1_{S/\mathfrak{m}} \;=\; 1_S + \mathfrak{m}\;,$$

weswegen es ein $m \in \mathfrak{m}$ mit $ax + m = 1_S$ gibt. Da nun aber $m \in \mathfrak{m} \subseteq \mathfrak{a}$ liegt, folgt hieraus $1_S \in \mathfrak{a}$, also $\mathfrak{a} = S$.

Sei zum anderen $\mathfrak{m} \subset S$ und gebe es kein Ideal $\mathfrak{a} \subseteq S$ gibt mit $\mathfrak{m} \subset \mathfrak{a} \subset S$. Da $S/\mathfrak{m}$ aus mehr als einem Element besteht, ist $0_{S/\mathfrak{m}} \neq 1_{S/\mathfrak{m}}$. Sei $x \in S$ mit $x + \mathfrak{m} \in (S/\mathfrak{m})^{\times}$ gegeben. Wir haben $x + \mathfrak{m} \overset{!}{\in} \mathrm{U}(S/\mathfrak{m})$ zu zeigen. Nun ist $\mathfrak{m} \subset \mathfrak{m} + (x) \subseteq S$ und also $\mathfrak{m} + (x) = S$. Folglich gibt es ein $m \in \mathfrak{m}$, und ein $y \in S$ mit $m + xy = 1_S$. Folglich ist

$$(x + \mathfrak{m})(y + \mathfrak{m}) \;=\; xy + \mathfrak{m} \;=\; (1_S - m) + \mathfrak{m} \;=\; 1_S + \mathfrak{m} \;=\; 1_{S/\mathfrak{m}}$$

und also $x + \mathfrak{m} \in \mathrm{U}(S/\mathfrak{m})$.

Schließlich ist S ein Körper genau dann, wenn $(0) \subseteq S$ maximal ist, i.e. wenn $(0) \subset S$ ist und es außer (0) und S keine weiteren Ideale in S gibt, i.e. wenn S zwei Ideale enthält. ▫

Definition 35 Ein Element $x \in S$ heißt *prim*, wenn (x) ein Primideal von S ist.

Beispiel 36

(1) Ist S integer, dann ist $(0) \subseteq S$ prim und also 0 prim.

(2) Es ist 0 ein primes Element der $\mathbf{Z}$-Algebra $\mathbf{Z}$, da $\mathbf{Z} \simeq \mathbf{Z}/(0)$ integer ist. Es ist aber (0) nicht maximal, da $\mathbf{Z} \simeq \mathbf{Z}/(0)$ kein Körper ist.

    Primzahlen sind positive prime Elemente von $\mathbf{Z}$.

    Es hat $\mathbf{Z}$ die Primideale (0) und (p) für $p > 0$ prim. Es ist $\mathbf{Z}/(p) =: \mathbf{F}_p$ ein Körper für $p > 0$ prim. Also ist diesenfalls (p) maximal.

(3) Es ist die $\mathbf{Z}$-Algebra $\mathbf{Z}/(4)$ fast integer. Denn dieser Ring enthält die Null $0 + (4)$, die Einheiten $1+(4)$ und $-1+(4)$ und den einzigen Nichtnullteiler $2+(4)$. Letzterer ist aber nilpotent.

Also ist $(4) \subseteq \mathbf{Z}$ primär. Es ist (4) aber nicht prim.

(4) Es ist die $\mathbf{Z}$-Algebra $\mathbf{Z}/(6)$ nicht fast integer. Denn wegen $(2+(6))\cdot(3+(6)) = 0+(6)$ ist $2 + (6)$ ein Nichtnullteiler. Wegen $(2 + (6))^3 = 8 + (6) = 2 + (6)$ ist $2 + (6)$ aber nicht nilpotent.

Also ist $(6) \subseteq \mathbf{Z}$ nicht primär.

Beispiel 37 Seien $a_1\,,\ a_2 \,\in\, R$.

Wir haben den R-Algebrenmorphismus $u_{a_1,a_2}\colon R[X_1, X_2] \to R$, der $X_1 \mapsto a_1$ und $X_2 \mapsto a_2$ abbildet; cf. Lemma 20.

Es ist u_{a_1,a_2} surjektiv, da er $r \mapsto r$ schickt für $r \in R$.

Es ist $\mathrm{Kern}(u_{a_1,a_2}) = (X_1 - a_1\,, X_2 - a_2) \subseteq R[X_1, X_2]$, wie wir nun verifizieren wollen.

Die Inklusion $\supseteq$ folgt aus $u_{a_1,a_2}(X_1 - a_1) = a_1 - a_1 = 0$ und $u_{a_1,a_2}(X_2 - a_2) = a_2 - a_2 = 0$.

Zur Inklusion $\overset{!}{\subseteq}$. Sei $f(X_1, X_2) \in R[X_1, X_2]$ mit $0 = u_{a_1,a_2}(f(X_1, X_2)) = f(a_1, a_2)$ gegeben.

Polynomdivision bezüglich X_2 liefert $f(X_1, X_2) = (X_2 - a_2) \cdot g(X_1, X_2) + r(X_1)$ mit $r(X_1) \in R[X_1] \subseteq R[X_1, X_2]$. Somit ist

$$0 \;=\; f(a_1, a_2) \;=\; (a_2 - a_2) \cdot g(a_1, a_2) + r(a_1) \;=\; r(a_1)\;.$$

Polynomdivision bezüglich X_1 liefert $r(X_1) = (X_1 - a_1) \cdot \tilde{g}(X_1) + \tilde{r}$ mit $\tilde{r} \in R \subseteq R[X_1]$. Somit ist

$$0 \;=\; r(a_1) \;=\; (a_1 - a_1) \cdot \tilde{g}(a_1) + \tilde{r} \;=\; \tilde{r}\;.$$

Zusammen hat sich also

$$\begin{array}{rcl} f(X_1\,, X_2) & = & (X_2 - a_2) \cdot g(X_1, X_2) + r(X_1) \\ & = & (X_2 - a_2) \cdot g(X_1, X_2) + (X_1 - a_1) \cdot \tilde{g}(X_1) \\ & \in & (X_1 - a_1\,, X_2 - a_2) \end{array}$$

ergeben.

Dies beschließt unsere Verifikation.

Insbesondere ist die R-Faktoralgebra $R[X_1, X_2]/(X_1 - a_1\,, X_2 - a_2)$ isomorph zu R.

Ist R ein Integritätsbereich, so ist daher $(X_1 - a_1\,, X_2 - a_2) \subseteq R[X_1, X_2]$ ein Primideal.

Ist R ein Körper, so ist daher $(X_1 - a_1\,, X_2 - a_2) \subseteq R[X_1, X_2]$ ein maximales Ideal.

Definition 38 Die Menge der Primideale in S wird mit $\mathrm{Spec}(S)$ bezeichnet und heißt das *Spektrum* von S.

Mittels $(\subseteq)$ ist $\mathrm{Spec}(S)$ ein Poset.

Bemerkung 39 *Ein Ideal $\mathfrak{p} \subseteq S$ ist prim genau dann, wenn $\mathfrak{p} \subset S$ ist und wenn für $x,\, y \in S$ aus $xy \in \mathfrak{p}$ folgt, daß $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$ ist.*

Beweis. Ist $\mathfrak{p}$ prim, dann ist zunächst $\mathfrak{p} \subset S$. Sind ferner $x,\, y \in S$ mit $xy \in \mathfrak{p}$ gegeben, dann ist $(x+\mathfrak{p})(y+\mathfrak{p}) = 0_{S/\mathfrak{p}}$, wegen $S/\mathfrak{p}$ integer also $x+\mathfrak{p} = 0_{S/\mathfrak{p}}$ oder $y+\mathfrak{p} = 0_{S/\mathfrak{p}}$, i.e. $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.

Gilt umgekehrt die genannte Eigenschaft, dann ist zunächst $0_{S/\mathfrak{p}} \neq 1_{S/\mathfrak{p}}$. Sind ferner $x,\, y \in S$ mit $(x+\mathfrak{p})(y+\mathfrak{p}) = 0_{S/\mathfrak{p}}$ gegeben, dann ist $xy \in \mathfrak{p}$, wegen der genannten Eigenschaft also $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$, i.e. $x+\mathfrak{p} = 0_{S/\mathfrak{p}}$ oder $y+\mathfrak{p} = 0_{S/\mathfrak{p}}$. Somit ist $S/\mathfrak{p}$ integer, i.e. $\mathfrak{p} \subseteq S$ prim. ▫

Bemerkung 40 *Ein Ideal $\mathfrak{p} \subseteq S$ ist primär genau dann, wenn $\mathfrak{p} \subset S$ ist und wenn für $x,\, y \in S$ aus $xy \in \mathfrak{p}$ und $y \notin \mathfrak{p}$ folgt, daß $x^n \in \mathfrak{p}$ liegt für ein $n \in \mathbf{Z}_{\geqslant 0}$.*

Beweis. Ist $\mathfrak{p}$ primär, dann ist zunächst $\mathfrak{p} \subset S$. Sind ferner $x,\, y \in S$ mit $xy \in \mathfrak{p}$ und $y \notin \mathfrak{p}$ gegeben, dann ist $(x+\mathfrak{p})(y+\mathfrak{p}) = 0_{S/\mathfrak{p}}$, wegen $S/\mathfrak{p}$ fast integer also $(x+\mathfrak{p})^n = 0_{S/\mathfrak{p}}$ für ein $n \in \mathbf{Z}_{\geqslant 0}$, $x^n \in \mathfrak{p}$ für ein $n \in \mathbf{Z}_{\geqslant 0}$.

Gilt umgekehrt die genannte Eigenschaft, dann ist zunächst $0_{S/\mathfrak{p}} \neq 1_{S/\mathfrak{p}}$. Sind ferner $x,\, y \in S$ mit $(x+\mathfrak{p})(y+\mathfrak{p}) = 0_{S/\mathfrak{p}}$ und $y+\mathfrak{p} \neq 0_{S/\mathfrak{p}}$ gegeben, dann ist $xy \in \mathfrak{p}$, aber $y \notin \mathfrak{p}$, wegen der genannten Eigenschaft also $x^n \in \mathfrak{p}$ für ein $n \in \mathbf{Z}_{\geqslant 0}$, i.e. $x^n + \mathfrak{p} = 0_{S/\mathfrak{p}}$ für ein $n \in \mathbf{Z}_{\geqslant 0}$. Somit ist $S/\mathfrak{p}$ fast integer, i.e. $\mathfrak{p} \subseteq S$ primär. ▫

Bemerkung 41 (und Definition) *Sei*

$$S \xrightarrow{f} T$$

ein R-Algebrenmorphismus.

Ist $\mathfrak{q} \subseteq T$ ein Primideal, dann ist auch $f^{-1}(\mathfrak{q}) \subseteq S$ ein Primideal.

Dies liefert die Abbildung

$$\begin{array}{rcl} \operatorname{Spec}(S) & \xleftarrow{\operatorname{Spec}(f)} & \operatorname{Spec}(T) \\ f^{-1}(\mathfrak{q}) =: (\operatorname{Spec}(f))(\mathfrak{q}) & \leftarrow\!\shortmid & \mathfrak{q}\,. \end{array}$$

Beweis. Dank Aufgabe 8.(1) ist $f^{-1}(\mathfrak{q}) \subseteq S$ ein Ideal.

Dank Aufgabe 8.(2) haben wir einen injektiven R-Algebrenmorphismus

$$S/f^{-1}(\mathfrak{q}) \;\to\; T/\mathfrak{q}\,.$$

Also ist $S/f^{-1}(\mathfrak{q})$ isomorph zu ihrem Bild, was eine R-Teilalgebra von $T/\mathfrak{q}$ ist. Da $T/\mathfrak{q}$ integer ist, gilt dies auch für dieses Bild und damit für $S/f^{-1}(\mathfrak{q})$.

Alternativ kann man auch direkt argumentieren. Zum einen ist $f(1_S) = 1_T \notin \mathfrak{q}$, also $1_S \notin f^{-1}(\mathfrak{q})$, also $f^{-1}(\mathfrak{q}) \subset S$. Sind ferner $x,\, y \in S$ mit $xy \in f^{-1}(\mathfrak{q})$ gegeben, aber $y \notin f^{-1}(\mathfrak{q})$, dann ist $f(x)\cdot f(y) = f(xy) \in \mathfrak{q}$, aber $f(y) \notin \mathfrak{q}$, woraus wir wegen $\mathfrak{q}$ prim $f(x) \in \mathfrak{q}$ entnehmen, i.e. $x \in f^{-1}(\mathfrak{q})$. ▫

Bemerkung 42 (und Definition) *Sei* $\mathfrak{a} \subseteq S$ *ein Ideal.*

Sei $\sqrt{\mathfrak{a}} := \{\, x \in S :$ *es gibt ein* $n \in \mathbf{Z}_{\geqslant 0}$ *mit* $x^n \in \mathfrak{a} \,\}$ *das Radikal von* $\mathfrak{a}$ *in* S.

Es ist $\sqrt{\mathfrak{a}}$ *ein Ideal in* S, *das* $\mathfrak{a}$ *enthält.*

Insbesondere ist das Nilradikal $\sqrt{(0)} = \{\, x \in S :\, x$ *ist nilpotent*$\}$ *ein Ideal in* S.

Beweis. Es ist $0 \in \sqrt{\mathfrak{a}}$.

Seien $s,\, s' \in S$ und $x,\, x' \in \sqrt{\mathfrak{a}}$. Dann gibt es $n,\, n' \in \mathbf{Z}_{\geqslant 0}$ mit $x^n \in \mathfrak{a}$ und $x'^{n'} \in \mathfrak{a}$. Es ist

$$(sx + s'x')^{n+n'} \;=\; \sum_{i \in [0,n+n']} \binom{n+n'}{i} s^{n+n'-i} x^{n+n'-i} s'^{\,i} x'^{\,i} \,.$$

Da nicht sowohl $n+n'-i < n$ als auch $i < n'$ sein kann, da dies $n+n' = (n+n'-i)+i < n+n'$ nach sich zöge, liegt $(sx + s'x')^{n+n'}$ in $\mathfrak{a}$ und also $sx + s'x' \in \sqrt{\mathfrak{a}}$. ▫

Bemerkung 43

(1) *Ist* $\mathfrak{a} \subseteq S$ *ein Ideal, dann ist* $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.

(2) *Ist* $\mathfrak{p} \subseteq S$ *ein Primideal, dann ist* $\sqrt{\mathfrak{p}} = \mathfrak{p}$.

(3) *Ist* $\mathfrak{q} \subseteq S$ *ein Primärideal, dann ist* $\sqrt{\mathfrak{q}}$ *ein Primideal.*

Beweis.

Ad (1). Zu zeigen ist nur $\sqrt{\sqrt{\mathfrak{a}}} \overset{!}{\subseteq} \sqrt{\mathfrak{a}}$. Ist $x \in \sqrt{\sqrt{\mathfrak{a}}}$, so gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $x^n \in \sqrt{\mathfrak{a}}$, weswegen es ein $m \in \mathbf{Z}_{\geqslant 0}$ gibt mit $x^{nm} = (x^n)^m \in \mathfrak{a}$, was $x \in \sqrt{\mathfrak{a}}$ nach sich zieht.

Ad (2). Zu zeigen ist nur $\sqrt{\mathfrak{p}} \overset{!}{\subseteq} \mathfrak{p}$. Ist $x \in \sqrt{\mathfrak{p}}$, dann gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $x^n \in \mathfrak{p}$. Da $\mathfrak{p} \subset S$, ist $n \geqslant 1$. Da $(x+\mathfrak{p})^n = 0$ ist und da $S/\mathfrak{p}$ ein Integritätsbereich ist, folgt $x+\mathfrak{p} = 0$, i.e. $x \in \mathfrak{p}$.

Ad (3). Zum einen ist $1 \notin \sqrt{\mathfrak{p}}$, da $1 \notin \mathfrak{p}$. Also ist $\sqrt{\mathfrak{p}} \subset S$. Seien ferner $x,\, y \in S$ mit $xy \in \sqrt{\mathfrak{p}}$, aber mit $y \notin \sqrt{\mathfrak{p}}$ gegeben. Wir haben $x \overset{!}{\in} \sqrt{\mathfrak{p}}$ zu zeigen. Es gibt ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $x^n y^n \in \mathfrak{p}$. Da $\mathfrak{p} \subset S$, ist $n \geqslant 1$. Da $y \notin \sqrt{\mathfrak{p}}$, ist $y^n + \mathfrak{p} \neq 0$. Folglich ist $x^n + \mathfrak{p}$ gleich 0 oder ein Nullteiler. Wegen $S/\mathfrak{p}$ fast integer, ist also $x^n + \mathfrak{p}$ nilpotent. Also ist auch $x + \mathfrak{p}$ nilpotent, i.e. $x \in \sqrt{\mathfrak{p}}$. ▫

Bemerkung 44 *Sei* $\mathfrak{m}$ *ein maximales Ideal in* S.

Sei $n \in \mathbf{Z}_{\geqslant 1}$. *Sei* $\mathfrak{q} \subseteq S$ *ein Ideal, für welches* $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ *gilt.*

Dann ist $\mathfrak{q}$ *primär. Es ist* $\sqrt{\mathfrak{q}} = \mathfrak{m}$.

Beweis. Es ist
$$\mathfrak{m} \;\subseteq\; \sqrt{\mathfrak{m}^n} \;\subseteq\; \sqrt{\mathfrak{q}} \;\subseteq\; \sqrt{\mathfrak{m}} \;\overset{\text{B. 43.(2)}}{=}\; \mathfrak{m}$$
und also $\sqrt{\mathfrak{q}} = \mathfrak{m}$.

Es ist $\mathfrak{q} \subseteq \mathfrak{m} \subset S$ und also $\mathfrak{q} \subset S$.

Seien x, $y \in S$ gegeben mit $xy \in \mathfrak{q}$, aber $y \notin \mathfrak{q}$. Wir haben zu zeigen, daß es ein $m \in \mathbf{Z}_{\geqslant 0}$ gibt mit $x^m \in \mathfrak{q}$; cf. Bemerkung 40. I.e. wir haben $x \overset{!}{\in} \sqrt{\mathfrak{q}} = \mathfrak{m}$ zu zeigen.

Sei $\mathfrak{b} := \{\, s \in S :\; sy \in \mathfrak{q} \,\}$. Es ist $\mathfrak{b}$ ein Ideal in S mit $x \in \mathfrak{b}$.

Es ist $\mathfrak{q} \subseteq \mathfrak{b}$. Da $y \notin \mathfrak{q}$, ist $1 \notin \mathfrak{b}$ und also auch $1 \notin \sqrt{\mathfrak{b}}$. Somit ist $\sqrt{\mathfrak{b}} \subset S$. Es wird
$$\mathfrak{m} \;=\; \sqrt{\mathfrak{q}} \;\subseteq\; \sqrt{\mathfrak{b}} \;\subset\; S\,,$$
wegen der Maximalität von $\mathfrak{m}$ also $\mathfrak{m} = \sqrt{\mathfrak{b}}$. Es wird also
$$x \;\in\; \mathfrak{b} \;\subseteq\; \sqrt{\mathfrak{b}} \;=\; \mathfrak{m}\,.$$

□

Beispiel 45 Sei K ein Körper.

Wir haben das maximale Ideal $\mathfrak{m} := (X_1\,, X_2) \subseteq K[X_1, X_2]$, da $K[X_1, X_2]/(X_1\,, X_2) \simeq K$ ein Körper ist; cf. Beispiel 37.

Das Ideal $\mathfrak{q} := (X_1^2, X_2) \subseteq K[X_1, X_2]$ ist primär, da
$$\mathfrak{m}^2 \;=\; (X_1, X_2)^2 \;=\; (X_1^2, X_1X_2\,, X_2^2) \;\subseteq\; \mathfrak{q} = (X_1^2, X_2) \;\subseteq\; (X_1, X_2) \;=\; \mathfrak{m}$$
ist.

Das Ideal (X_1^2, X_2) ist aber nicht prim, da $X_1^2 \in \mathfrak{q}$, aber $X_1 \notin \mathfrak{q}$ liegt.

Wir wiederholen und ergänzen.

Bemerkung 46 *Sei* $\mathfrak{q}$ *ein Ideal in* S*.*

Wir betrachten die folgenden Aussagen $(1, 2, 3)$.

(1) *Es ist* $\sqrt{\mathfrak{q}}$ *maximal.*

(2) *Es ist* $\mathfrak{q}$ *primär.*

(3) *Es ist* $\sqrt{\mathfrak{q}}$ *prim.*

Es gelten folgende Implikationen.
$$(1) \implies (2) \implies (3)$$

> Vorsicht, in Aufgabe 13 wird gezeigt, daß im allgemeinen aus (3) nicht (2) folgt – nicht einmal, wenn $\mathfrak{q}$ das Quadrat eines Primideals ist.
>
> Aus (2) folgt im allgemeinen nicht (1), wie $\mathfrak{q} = (0)$ in $\mathbf{Z}$ zeigt.
>
> Der Beweis zu (1) $\Rightarrow$ (2) wird eine Variante des Beweises zu Bemerkung 44 sein.

Beweis.

Ad (2) $\Rightarrow$ (3). Dies folgt aus Bemerkung 43.(3).

Ad (1) $\Rightarrow$ (2). Seien $x, y \in S$ gegeben mit $xy \in \mathfrak{q}$, aber $y \notin \mathfrak{q}$. Wir haben $x \overset{!}{\in} \sqrt{\mathfrak{q}}$ zu zeigen; cf. Bemerkung 40.

Sei $\mathfrak{b} := \{ s \in S : \; sy \in \mathfrak{q} \}$. Es ist $x \in \mathfrak{b}$ und $\mathfrak{q} \subseteq \mathfrak{b}$, aber $1 \notin \mathfrak{b}$. Also ist auch $1 \notin \sqrt{\mathfrak{b}}$, i.e. $\sqrt{\mathfrak{b}} \subset S$. Also ist $\sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{b}} \subset S$, wegen der Maximalität von $\sqrt{\mathfrak{q}}$ also $\sqrt{\mathfrak{q}} = \sqrt{\mathfrak{b}}$. Mithin wird $x \in \mathfrak{b} \subseteq \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{q}}$. ▫

Lemma 47 (Existenz maximaler Ideale) *Sei $\mathfrak{a} \subset S$ ein Ideal.*

Dann gibt es ein maximales Ideal $\mathfrak{m}$ in S mit $\mathfrak{a} \subseteq \mathfrak{m} \subset S$.

Beweis. Sei

$$M \;:=\; \{ \mathfrak{b} : \; \mathfrak{b} \text{ ist ein Ideal in } S \text{ mit } \mathfrak{b} \subset S \}$$

die Menge der Ideale von S. Mittels $(\subseteq)$ teilgeordnet ist M ein Poset.

Wir haben zu zeigen, daß es in M ein maximales Element gibt, das $\mathfrak{a}$ enthält; cf. Bemerkung 34. Gemäß Lemma von Zorn genügt es zu zeigen, daß jede Kette in M eine obere Schranke enthält; cf. LemAppXXX.

Sei $K \subseteq M$ eine Kette. O.E. ist $K \neq \emptyset$. Sei $\mathfrak{c} := \bigcup K = \bigcup_{\mathfrak{b} \in K} \mathfrak{b}$. Wir *behaupten*, daß $\mathfrak{c}$ eine obere Schranke von K in M ist.

Es ist $\mathfrak{c} \subset S$, da $1 \notin \mathfrak{c}$. Denn *wäre* $1 \in \mathfrak{c}$, dann gäbe es ein $\mathfrak{b} \in K$ mit $1 \in \mathfrak{b}$, was aber $\mathfrak{b} = S$ nach sich zöge, was *nicht* der Fall ist; cf. Bemerkung 30.

Bleibt zu zeigen, daß $\mathfrak{c}$ ein Ideal in S ist. Verwenden wir ein $\mathfrak{b} \in K$, so sehen wir $0 \in \mathfrak{b} \subseteq \mathfrak{c}$.

Seien zum anderen $s, s' \in S$ und $c, c' \in \mathfrak{c}$ gegeben. Wir haben $sc + s'c' \overset{!}{\in} \mathfrak{c}$ zu zeigen.

Es gibt $\mathfrak{b}, \mathfrak{b}' \in K$ mit $c \in \mathfrak{b}$ und $c' \in \mathfrak{b}'$. Da K eine Kette ist, ist $\mathfrak{b} \subseteq \mathfrak{b}'$ oder $\mathfrak{b}' \subseteq \mathfrak{b}$.

O.E. ist $\mathfrak{b} \subseteq \mathfrak{b}'$. Da nun $c, c' \in \mathfrak{b}'$ und da $\mathfrak{b}'$ ein Ideal in S ist, folgt auch $sc + s'c' \in \mathfrak{b}' \subseteq \mathfrak{c}$.

Dies zeigt die *Behauptung*. ▫

Korollar 48 *Sei $0_S \neq 1_S$.*

Dann gibt es in S ein maximales Ideal.

Beweis. Wir haben das Ideal $(0) \subset S$, auf welches wir Lemma 47 anwenden können. ▫

Bemerkung 49 (und Definition)

Ein maximales Element von $\operatorname{Spec}(S)$ *ist dasselbe wie ein maximales Ideal in* S*.*

Ein minimales Element von $\operatorname{Spec}(S)$ *heiße ein* minimales Primideal *von* S*.*

Beweis. Wir verwenden Bemerkung 34.

Ist $\mathfrak{m}$ ein maximales Ideal in S, dann ist $\mathfrak{m}$ prim. Ist $\mathfrak{p} \in \operatorname{Spec}(S)$ mit $\mathfrak{m} \subseteq \mathfrak{p} \subset S$ gegeben, dann ist $\mathfrak{m} = \mathfrak{p}$. Also ist $\mathfrak{m}$ maximal in $\operatorname{Spec}(S)$.

Sei umgekehrt $\mathfrak{p}$ ein maximales Element von $\operatorname{Spec}(S)$. Wir wollen zeigen, daß $\mathfrak{p}$ ein maximales Ideal in S ist. Wir wählen ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{p} \subseteq \mathfrak{m} \subset S$; cf. Lemma 47. Da $\mathfrak{m}$ prim und $\mathfrak{p}$ maximal in $\operatorname{Spec}(S)$ ist, folgt $\mathfrak{p} = \mathfrak{m}$. Also ist $\mathfrak{p}$ ein maximales Ideal in S. □

Lemma 50 *Sei* $\mathfrak{a} \subset S$ *ein Ideal.*

Dann gibt es in der Menge $\{\, \mathfrak{q} \in \operatorname{Spec}(S) : \ \mathfrak{a} \subseteq \mathfrak{q} \,\}$ *ein minimales Element.*

Beweis. Ausgestattet mit $(\supseteq)$ ist $M := \{\, \mathfrak{q} \in \operatorname{Spec}(S) : \ \mathfrak{a} \subseteq \mathfrak{q} \,\}$ ein Poset.

Dank Lemma Lem25 ist $M \neq \emptyset$; cf. Definition 33.

Wir haben zu zeigen, daß M ein maximales Element $\mathfrak{q}$ enthält. Gemäß Lemma von Zorn genügt es zu zeigen, daß jede Kette in M eine obere Schranke enthält; cf. LemAppXXX.

Sei $K \subseteq M$ eine Kette. O.E. ist $K \neq \emptyset$.

Sei $\mathfrak{s} := \bigcap K = \bigcap_{\mathfrak{r} \in K} \mathfrak{r}$. Wir *behaupten*, daß $\mathfrak{s}$ eine obere Schranke von K in M ist.

Es ist $\mathfrak{s}$ ein Ideal, das $\mathfrak{a}$ enthält. Zu zeigen ist, daß $\mathfrak{s}$ prim ist.

Seien $x, y \in S$ gegeben mit $xy \in \mathfrak{s}$, aber $x \notin \mathfrak{s}$. Zu zeigen ist, daß $y \overset{!}{\in} \mathfrak{s}$ liegt. Sei $\mathfrak{r} \in K$ gegeben. Zu zeigen ist, daß $y \overset{!}{\in} \mathfrak{r}$ liegt.

Da $x \notin \mathfrak{s}$ liegt, gibt es ein $\mathfrak{t} \in K$ mit $x \notin \mathfrak{t}$.

Da K eine Kette ist, ist $\mathfrak{t} \subseteq \mathfrak{r}$ oder $\mathfrak{r} \subseteq \mathfrak{t}$.

Falls $\mathfrak{t} \subseteq \mathfrak{r}$ ist, dann folgt aus $\mathfrak{t}$ prim, aus $xy \in \mathfrak{s} \subseteq \mathfrak{t}$ und aus $x \notin \mathfrak{t}$, daß $y \in \mathfrak{t} \subseteq \mathfrak{r}$ liegt.

Falls $\mathfrak{r} \subseteq \mathfrak{t}$ ist, dann folgt aus $x \notin \mathfrak{t}$, daß $x \notin \mathfrak{r}$ liegt, weswegen aus $xy \in \mathfrak{s} \subseteq \mathfrak{r}$ und aus $\mathfrak{r}$ prim folgt, daß $y \in \mathfrak{r}$ liegt. □

1.1.4 Noetherzität

Sei R ein kommutativer Ring. Sei S eine kommutative R-Algebra.

Definition 51 Sei S eine kommutative R-Algebra.

(1) Sei $\mathfrak{a} \subseteq S$ ein Ideal. Es heißt $\mathfrak{a}$ *endlich erzeugt*, falls es $n \in \mathbf{Z}_{\geqslant 0}$ und $a_i \in S$ für $i \in [1, n]$ so gibt, daß

$$\mathfrak{a} \;=\; (\, a_i \colon i \in [1, n]\,)$$

ist.

(2) Es heiße S *noethersch*, falls jedes Ideal in S endlich erzeugt ist.

(3) Sei $\mathfrak{a} \subseteq S$ ein Ideal. Es heißt $\mathfrak{a}$ ein *Hauptideal*, wenn es ein $a \in S$ mit $\mathfrak{a} = (a)$ gibt.

(4) Es heiße S eine *Hauptidealalgebra*, falls jedes Ideal in S ein Hauptideal ist.

Insbesondere sind Hauptidealalgebren noethersch.

Beispiel 52

(1) Sei K ein Körper. Es ist K eine Hauptidealalgebra über K und insbesondere noethersch.

(2) Es ist $\mathbf{Z}$ eine Hauptidealalgebra über $\mathbf{Z}$ und also noethersch. Cf. auch XXXUeXXX.

Lemma 53 *Es ist S noethersch genau dann, wenn für jede aufsteigende abzählbare Kette von Idealen*

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

in S ein $k \in \mathbf{Z}_{\geqslant 1}$ existiert mit $\mathfrak{a}_k = \mathfrak{a}_i$ für $i \in \mathbf{Z}_{\geqslant k}$.

Beweis.

Sei zum einen S noethersch. Sei eine aufsteigende abzählbare Kette von Idealen

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

in S gegeben. Sei $\mathfrak{b} := \bigcup_{i \geqslant 1} \mathfrak{a}_i$. Es ist $\mathfrak{b}$ ein Ideal. Denn zum einen ist $0 \in \mathfrak{b}$. Zum anderen haben wir für gegebene $s,\, s' \in S$ und $b,\, b' \in \mathfrak{b}$ Elemente $i,\, i' \in \mathbf{Z}_{\geqslant 1}$ mit $b \in \mathfrak{a}_i$ und $b' \in \mathfrak{a}_{i'}$. O.E. ist $i \leqslant i'$. Also ist mit $b,\, b' \in \mathfrak{a}_{i'}$ auch $sb + s'b' \in \mathfrak{a}_{i'} \subseteq \mathfrak{b}$.

Da S noethersch ist, gibt es $k \in \mathbf{Z}_{\geqslant 1}$ und $b_1\,,\, \ldots,\, b_k \in S$ mit $\mathfrak{b} = (b_1, \ldots, b_k)$. Für $i \in [1, k]$ liegt $b_i \in \mathfrak{b}$, weswegen es ein $\ell_i \in \mathbf{Z}_{\geqslant 1}$ gibt mit $b_i \in \mathfrak{a}_{\ell_i}$. Sei $\ell := \max\{\, \ell_i :\ i \in [1, k]\,\}$. Dann ist $b_i \in \mathfrak{a}_{\ell_i} \subseteq \mathfrak{a}_\ell$ für $i \in [1, k]$ und also

$$\mathfrak{b} \;=\; (b_1, \ldots, b_k) \;\subseteq\; \mathfrak{a}_\ell \;\subseteq\; \mathfrak{a}_j \;\subseteq\; \mathfrak{b}$$

für $j \in \mathbf{Z}_{\geqslant \ell}$. Somit ist die obengenannte Kettenbedingung erfüllt.

Sei zum anderen die obengenannte Kettenbedingung erfüllt. Sei $\mathfrak{a}$ ein Ideal in S.

Annahme, es ist $\mathfrak{a}$ nicht endlich erzeugt.

Wähle ein Element $a_1 \in \mathfrak{a}$. Es ist $(a_1) \subset \mathfrak{a}$, da $\mathfrak{a}$ nicht endlich erzeugt ist.

Wähle ein Element $a_2 \in \mathfrak{a} \smallsetminus (a_1)$. Es ist $(\,a_1\,,a_2\,) \subset \mathfrak{a}$, da $\mathfrak{a}$ nicht endlich erzeugt ist.

Wähle ein Element $a_3 \in \mathfrak{a} \smallsetminus (\,a_1\,,a_2\,)$. Es ist $(\,a_1\,,a_2\,,a_3\,) \subset \mathfrak{a}$, da $\mathfrak{a}$ nicht endlich erzeugt ist.

Und so fort.

Dies gibt eine echt aufsteigende abzählbare Kette von Idealen

$$(a_1) \;\subset\; (\,a_1\,,a_2\,) \;\subset\; (\,a_1\,,a_2\,,a_3\,) \;\subset\; \ldots\;,$$

im *Widerspruch* zur obengenannten Kettenbedingung. $\square$

Bemerkung 54 *Sei S noethersch. Sei $\mathfrak{a} \in \mathrm{Ideale}(S)$ gegeben.*

Dann gibt es ein $n \in \mathbf{Z}_{\geqslant 1}$ mit $(\sqrt{\mathfrak{a}})^n \subseteq \mathfrak{a}$.

Beweis. Da S noethersch ist, können wir ein $k \in \mathbf{Z}_{\geqslant 0}$ und Elemente $x_1\,,\ldots,\,x_k \in S$ finden mit $\sqrt{\mathfrak{a}} = (x_1, x_2, \ldots, x_k)$. Für $i \in [1,k]$ gibt es also $m_i \in \mathbf{Z}_{\geqslant 0}$ mit $x_i^{m_i} \in \mathfrak{a}$. Wir wählen $m := \max\{\, m_i :\; i \in [1,k]\,\}$. Dann ist $x_i^m \in \mathfrak{a}$ für $i \in [1,k]$.

Wir *behaupten,* daß $(\sqrt{\mathfrak{a}})^{mk} \subseteq \mathfrak{a}$ liegt. Sei $s_{j,i} \in S$ für $i \in [1,k]$ und $j \in [1,mk]$ gegeben. Jedes Element von $(\sqrt{\mathfrak{a}})^{mk}$ ist eine Summe von Elementen der Form

$$\prod_{j\in[1,k]} \Big(\sum_{i\in[1,k]} s_{j,i}\, x_i\Big)$$

und also von der Form

$$\sum_{\substack{\ell\,=\,(\ell_1\,,\ldots,\,\ell_k)\in\mathbf{Z}_{\geqslant 0}^{\times k}\\ \ell_1+\ell_2+\cdots+\ell_k\,=\,mk}} s_\ell\, x_1^{\ell_1} x_2^{\ell_2}\cdots x_k^{\ell_k}$$

für gewisse $s_\ell \in S$. Es genügt also zu zeigen, daß stets $x_1^{\ell_1} x_2^{\ell_2}\cdots x_k^{\ell_k} \in \mathfrak{a}$ liegt. Dazu genügt es zu zeigen, daß stets ein $i \in [1,k]$ existiert mit $\ell_i \geqslant m$.

Wäre dem nicht so, dann folgte aus $\ell_i < m$ für $i \in [1,k]$, daß $mk = \ell_1 + \ell_2 + \cdots + \ell_k < mk$ ist, was aber *nicht* zutrifft. $\square$

Definition 55 Sei X ein einzelnes Element.

Sei

$$\begin{array}{rcl} S[X]^\times & \xrightarrow{\deg} & \mathbf{Z}_{\geqslant 0} \\ f(X) = \sum_{i\geqslant 0} s_i X^i & \mapsto & \deg(f) = \deg(f(X)) \;:=\; \max\{\, i \in \mathbf{Z}_{\geqslant 0} :\; s_i \neq 0\,\}\;. \end{array}$$

Es heißt $\deg(f)$ der *Grad* von $f(X)$ in X.

Satz 56 (Hilberts Basissatz) *Sei X ein einzelnes Element.*

Ist S noethersch, dann auch $S[X]$.

Beweis. Sei $\mathfrak{a} \subseteq S[X]$ ein Ideal. *Annahme*, es ist $\mathfrak{a}$ nicht endlich erzeugt.

Es ist $(0) \subset \mathfrak{a}$, da $\mathfrak{a}$ nicht endlich erzeugt ist. Wähle $f_1(X)$ in $\mathfrak{a} \smallsetminus (0)$ von minimalem Grad n_1.

Es ist $(f_1(X)) \subset \mathfrak{a}$, da $\mathfrak{a}$ nicht endlich erzeugt ist. Wähle $f_2(X)$ in $\mathfrak{a} \smallsetminus (f_1(X))$ von minimalem Grad n_2.

Es ist $(f_1(X), f_2(X)) \subset \mathfrak{a}$, da $\mathfrak{a}$ nicht endlich erzeugt ist. Wähle $f_3(X)$ in $\mathfrak{a} \smallsetminus (f_1(X), f_2(X))$ von minimalem Grad n_3.

Usf.

Es ist $n_1 \leqslant n_2 \leqslant n_3 \leqslant \dots$, da $\mathfrak{a} \smallsetminus (0) \supseteq \mathfrak{a} \smallsetminus (f_1(X)) \supseteq \mathfrak{a} \smallsetminus (f_1(X), f_2(X)) \dots$ gilt.

Schreibe $f_i(X) =: \sum_{j \in [0,n_i]} s_{i,j} X^j$ und sodann $z_i := s_{i,n_i}$ für $i \in \mathbf{Z}_{\geqslant 1}$.

Wir *behaupten*, es ist

$$(z_1) \subset (z_1, z_2) \subset (z_1, z_2, z_3) \subset \dots ,$$

gebildet in S.

Wäre für ein $k \in \mathbf{Z}_{\geqslant 2}$ das Element z_k enthalten in $(z_1, z_2, \dots, z_{k-1})$, dann gäbe es $t_1, t_2, \dots, t_{k-1} \in S$ mit $z_k = t_1 z_1 + t_2 z_2 + \dots + t_{k-1} z_{k-1}$.

Dann wäre aber wegen $f_k(X) \in \mathfrak{a} \smallsetminus (f_1(X), f_2(X), \dots, f_{k-1}(X))$ und wegen $f_1(X), f_2(X), \dots, f_k(X) \in \mathfrak{a}$ auch

$$\begin{array}{rcl} g(X) & := & f_k(X) - t_1 X^{n_k - n_1} f_1(X) - t_2 X^{n_k - n_2} f_2(X) - \dots - t_{k-1} X^{n_k - n_{k-1}} f_{k-1}(X) \\ & \in & \mathfrak{a} \smallsetminus (f_1(X), f_2(X), \dots, f_{k-1}(X)) , \end{array}$$

denn alle Summanden der rechten Seite liegen in $\mathfrak{a}$, aber nur $f_k(X)$ liegt nicht in $(f_1(X), f_2(X), \dots, f_{k-1}(X))$.

Es ist $\deg(g) \leqslant n_k$, da alle Summanden der rechten Seite einen Grad $\leqslant n_k$ haben.

Der Koeffizient von $g(X)$ bei X^{n_k} ergibt sich zu

$$z_k - t_1 z_1 - t_2 z_2 - \dots - t_{k-1} z_{k-1} = 0 .$$

Also ist $\deg(g(X)) < \deg(f_k(X))$, im Widerspruch zur Wahl von $f_k(X)$.

Dies zeigt die *Behauptung*, welche ihrerseits im *Widerspruch* zur Noetherzität von S steht; cf. Lemma 53. □

Korollar 57 *Sei $n \in \mathbf{Z}_{\geqslant 1}$. Sei S noethersch.*

Sei $X = \{ X_i : i \in [1,n] \}$ eine Menge, mit $[1,n] \to X : i \mapsto X_i$ bijektiv.

Sei $\mathfrak{a} \subseteq S[X_1, X_2, \dots, X_n]$ ein Ideal.

Es ist $S[X_1, X_2, \dots, X_n]/\mathfrak{a}$ noethersch.

Beweis. Mit Iteration von Satz 56 ist $S[X_1, X_2, \ldots, X_n]$ als noethersch zu erkennen; cf. Bemerkung 21. Dank XXXUeXXX ist dann auch $S[X_1, X_2, \ldots, X_n]/\mathfrak{a}$ noethersch. ▫

Satz 58 (Endlich viele minimale Primideale)

Sei S noethersch.

Die Menge der minimalen Primideale von S ist endlich.

Beweis. Sei $\mathfrak{a}$ ein Ideal in S. Wir *behaupten*, daß die Menge der minimalen Elemente von $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{a} \subseteq \mathfrak{p} \,\}$ endlich ist.

Sei M die Menge der Ideale von S, für welche die Menge der minimalen Elemente von $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{a} \subseteq \mathfrak{p} \,\}$ nicht endlich ist. Es ist M mittels $(\subseteq)$ teilgeordnet.

Annahme, es ist $M \neq \emptyset$. Da S noethersch ist, gibt es in M ein maximales Element $\mathfrak{b}$; cf. Aufgabe 12. Es ist $\mathfrak{b}$ nicht prim, da die Menge $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b} \subseteq \mathfrak{p} \,\}$ sonst nur ein einziges minimales Element enthielte, nämlich $\mathfrak{b}$.

Also gibt es $x, y \in S$ mit $xy \in \mathfrak{b}$, aber $x \notin \mathfrak{b}$ und $y \notin \mathfrak{b}$; cf. Bemerkung 39.

Schreibe $\mathfrak{b}' := \mathfrak{b} + (x)$ und $\mathfrak{b}'' := \mathfrak{b} + (y)$. Es ist $\mathfrak{b} \subset \mathfrak{b}'$ und $\mathfrak{b} \subset \mathfrak{b}''$. Also liegen $\mathfrak{b}'$ und $\mathfrak{b}''$ nicht in M.

Sei $\mathfrak{q}$ minimal in $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b} \subseteq \mathfrak{p} \,\}$. Dann ist $xy \in \mathfrak{b} \subseteq \mathfrak{q}$, also $x \in \mathfrak{q}$ oder $y \in \mathfrak{q}$, i.e. $\mathfrak{b}' \subseteq \mathfrak{q}$ oder $\mathfrak{b}'' \subseteq \mathfrak{q}$.

Ist $\mathfrak{b}' \subseteq \mathfrak{q}$, dann ist $\mathfrak{q}$ minimal in $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b}' \subseteq \mathfrak{p} \,\}$, da ein Primideal, das echt in $\mathfrak{q}$ läge und $\mathfrak{b}'$ enthielte, auch $\mathfrak{b}$ enthielte, was wegen der Minimalität von $\mathfrak{q}$ in $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b} \subseteq \mathfrak{p} \,\}$ nicht sein kann.

Ist $\mathfrak{b}'' \subseteq \mathfrak{q}$, dann ist $\mathfrak{q}$ minimal in $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b}'' \subseteq \mathfrak{p} \,\}$. Dies folgt genauso.

Somit ist die Menge der minimalen Elemente in $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b} \subseteq \mathfrak{p} \,\}$ enthalten in der Vereinigung der Menge der minimalen Elemente von $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b}' \subseteq \mathfrak{p} \,\}$ und der Menge der minimalen Elemente von $\{\, \mathfrak{p} \in \mathrm{Spec}(S) : \mathfrak{b}'' \subseteq \mathfrak{p} \,\}$.

Da die erstere Menge unendlich ist, die letzteren beiden aber endlich, haben wir einen *Widerspruch*. Dies zeigt die *Behauptung*.

Die Aussage folgt nun aus der Behauptung als Spezialfall $\mathfrak{a} = (0)$. ▫

1.1.5 Primärzerlegung

Sei R ein kommutativer Ring. Sei S eine kommutative R-Algebra.

Bemerkung 59 (und Definition) *Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in S. Sei*

$$(\mathfrak{a} : \mathfrak{b}) \;:=\; \{\, x \in S : x\mathfrak{b} \subseteq \mathfrak{a} \,\}\,.$$

Es ist $(\mathfrak{a} : \mathfrak{b})$ ein Ideal in S.

Beweis. Es ist $0 \in (\mathfrak{a} : \mathfrak{b})$.

Seien $x,\, x' \in (\mathfrak{a} : \mathfrak{b})$. Seien $s,\, s' \in S$. Wir haben $sx + s'x' \overset{!}{\in} (\mathfrak{a} : \mathfrak{b})$ zu zeigen. Sei $b \in \mathfrak{b}$. Wir haben $(sx + s'x')b \overset{!}{\in} \mathfrak{a}$ zu zeigen.

Aber es ist $(sx + s'x')b = s(xb) + s'(x'b) \in \mathfrak{a}$, da $xb,\, x'b \in \mathfrak{a}$ liegen. ▫

Beispiel 60 In $\mathbf{Z}$ ist $((6) : (3)) = (2)$, da für $z \in \mathbf{Z}$ genau dann $z(3) \subseteq (6)$ ist, wenn $z \in (2)$ liegt.

Definition 61 Sei $\mathfrak{a}$ ein Ideal in S.

Es heißt $\mathfrak{a}$ *unzerlegbar*, wenn für Ideale $\mathfrak{b}$ und $\mathfrak{c}$ in S aus $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ folgt, daß $\mathfrak{a} = \mathfrak{b}$ oder $\mathfrak{a} = \mathfrak{c}$ ist.

Lemma 62 *Sei $\mathfrak{a}$ ein Ideal in S.*

Folgende Aussagen $(1, 2)$ *gelten.*

(1) *Ist $\mathfrak{a}$ prim, dann ist $\mathfrak{a}$ unzerlegbar.*

(2) *Ist S noethersch und $\mathfrak{a}$ unzerlegbar, dann ist $\mathfrak{a}$ primär.*

Beweis. Wir verwenden die Bemerkungen 39 und 40.

Ad (1). Sei $\mathfrak{a}$ prim. Seien $\mathfrak{b}$ und $\mathfrak{c}$ Ideale in S mit $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. Es ist also $\mathfrak{a} \subseteq \mathfrak{b}$ und $\mathfrak{a} \subseteq \mathfrak{c}$. Zu zeigen ist, daß $\mathfrak{a} = \mathfrak{b}$ oder $\mathfrak{a} = \mathfrak{c}$ ist.

Annahme, es ist $\mathfrak{a} \subset \mathfrak{b}$ und $\mathfrak{a} \subset \mathfrak{c}$. Dann gibt es ein $b \in \mathfrak{b} \smallsetminus \mathfrak{a}$ und ein $c \in \mathfrak{c} \smallsetminus \mathfrak{a}$. Es ist $bc \in \mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}$. Also ist $b \in \mathfrak{a}$ oder $c \in \mathfrak{a}$. Wir haben einen *Widerspruch*.

Ad (2). Seien $x,\, y \in S$ mit $xy \in \mathfrak{a}$, aber $y \notin \mathfrak{a}$. Wir haben zu zeigen, daß es ein $n \in \mathbf{Z}_{\geqslant 0}$ gibt mit $x^n \in \mathfrak{a}$.

Es ist
$$\mathfrak{a} \;=\; (\mathfrak{a} : (x^0)) \;\subseteq\; (\mathfrak{a} : (x^1)) \;\subseteq\; (\mathfrak{a} : (x^2)) \;\subseteq\; \dots$$
Da S noethersch ist, gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $(\mathfrak{a} : (x^n)) = (\mathfrak{a} : (x^{n+1}))$; cf. Lemma 53.

Wir *behaupten* $\mathfrak{a} = (\mathfrak{a} + (x^n)) \cap (\mathfrak{a} + (y))$.

Sei $z \in (\mathfrak{a} + (x^n)) \cap (\mathfrak{a} + (y))$. Es ist $z \overset{!}{\in} \mathfrak{a}$ zu zeigen.

Schreibe $z = a + sx^n$ mit $a \in \mathfrak{a}$ und $s \in S$. Schreibe $z = a' + s'y$ mit $a' \in \mathfrak{a}$ und $s' \in S$.

Es wird
$$sx^{n+1} \;=\; x(a + sx^n) - xa \;=\; xz - xa \;=\; x(a' + s'y) - xa \;=\; x(a' - a) + s'(xy) \;\in\; \mathfrak{a}\,.$$
Also ist $s \in (\mathfrak{a} : (x^{n+1})) = (\mathfrak{a} : (x^n))$. Folglich ist $z = a + sx^n \in \mathfrak{a}$.

Da $\mathfrak{a}$ unzerlegbar ist, da $\mathfrak{a} = (\mathfrak{a} + (x^n)) \cap (\mathfrak{a} + (y))$ ist und da $\mathfrak{a} \subset \mathfrak{a} + (y)$ ist, folgt $\mathfrak{a} = \mathfrak{a} + (x^n)$, i.e. $x^n \in \mathfrak{a}$. ▫

Satz 63 (Existenz einer Primärzerlegung)

Sei S noethersch. Sei $\mathfrak{a}$ ein Ideal von S.

Dann gibt es ein $k \in \mathbf{Z}_{\geqslant 0}$ und Primärideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ in S mit

$$\mathfrak{a} \;=\; \bigcap_{i\in[1,k]} \mathfrak{q}_i \;.$$

Ist $k = 0$, so ist hierbei die rechte Seite als gleich S zu verstehen.

Beweis. Sei M die Menge der Ideale von S, welche nicht als Schnitt endlich vieler Primärideale in S geschrieben werden können. Es ist M teilgeordnet mittels $(\subseteq)$.

Annahme, es ist $M \neq \emptyset$. Da S noethersch ist, gibt es in M ein maximales Element $\mathfrak{b}$; cf. Aufgabe 12. Dieses ist nicht primär. Da S noethersch ist, ist $\mathfrak{b}$ nicht unzerlegbar; cf. Lemma 62.(2). Also können wir $\mathfrak{b} = \mathfrak{c} \cap \mathfrak{d}$ schreiben mit $\mathfrak{b} \subset \mathfrak{c}$ und $\mathfrak{b} \subset \mathfrak{d}$. Es sind $\mathfrak{c}$ und $\mathfrak{d}$ nicht in M. Also gibt es $k,\, \ell \in \mathbf{Z}_{\geqslant 0}$ und Primärideale $\mathfrak{q}'_i$ für $i \in [1,k]$ und $\mathfrak{q}''_j$ für $j \in [1,\ell]$ derart, daß

$$\mathfrak{c} \;=\; \bigcap_{i\in[1,k]} \mathfrak{q}'_i \qquad \text{und} \qquad \mathfrak{d} \;=\; \bigcap_{j\in[1,\ell]} \mathfrak{q}''_j$$

sind. Es folgt

$$\mathfrak{b} \;=\; \mathfrak{c} \cap \mathfrak{d} \;=\; \Big(\bigcap_{i\in[1,k]} \mathfrak{q}'_i\Big) \cap \Big(\bigcap_{j\in[1,\ell]} \mathfrak{q}''_j\Big)\;.$$

Wir haben einen *Widerspruch*. □

1.2 Konstruktionen

1.2.1 Lokalisierung

Sei R ein kommutativer Ring. Sei $S = (S, \alpha)$ eine kommutative R-Algebra.

Definition 64 Sei $N \subseteq S$ eine Teilmenge.

Es heißt N eine *multiplikative* Teilmenge, wenn $1 \in N$ liegt und wenn für alle $x,\, y \in N$ auch $xy \in N$ liegt.

> Es sollen mittels einer Konstruktion von Brüchen die Elemente von N "invertierbar gemacht" werden.

Beispiel 65

(1) Es ist $\mathrm{U}(S)$ eine multiplikative Teilmenge von S.

(2) Ist $s \in S$, so ist $\{ s^k : k \in \mathbf{Z}_{\geqslant 0} \}$ eine multiplikative Teilmenge von S.

(3) Ist $\mathfrak{p} \in \operatorname{Spec}(S)$, dann ist $S \smallsetminus \mathfrak{p}$ eine multiplikative Teilmenge von S. In der Tat ist $1 \in S \smallsetminus \mathfrak{p}$. Ferner folgt aus $x,\, y \in S \smallsetminus \mathfrak{p}$, daß auch $xy \in S \smallsetminus \mathfrak{p}$ liegt, da $\mathfrak{p}$ prim ist.

(4) Ist S integer, so erhalten wir als Spezialfall von (3), daß $S \smallsetminus (0) = S^\times$ eine multiplikative Teilmenge von S ist.

Bemerkung 66 (und Definition) *Sei $N \subseteq S$ eine multiplikative Teilmenge.*

Sei auf $S \times N$ folgende Relation $(\sim)$ erklärt. Es sei $(s,n) \sim (s',n')$ genau dann, wenn es ein $x \in N$ mit $xn's = xns'$ gibt, wobei $(s,n),\, (s',n') \in S \times N$.

Es ist $(\sim)$ eine Äquivalenzrelation. Die Äquivalenzklasse von (s,n) bezüglich $(\sim)$ werde mit $\frac{s}{n}$ oder mit s/n bezeichnet.

Sei

$$S /\!\!/ N \;:=\; \{ \frac{s}{n} : s \in S,\; n \in N \}$$

die Quotientenalgebra *von S durch N.*

Für $\frac{s}{n} \in S/\!\!/N$ ist $\frac{s}{n} = \frac{sy}{ny}$ für $y \in N$, da $1 \cdot s(ny) = 1 \cdot n(sy)$.

Auf $S/\!\!/N$ können wir eine Addition $(+)$ erklären durch

$$\frac{s}{n} + \frac{s'}{n'} \;:=\; \frac{sn' + ns'}{nn'}$$

und eine Multiplikation $(\cdot)$ durch

$$\frac{s}{n} \cdot \frac{s'}{n'} \;:=\; \frac{ss'}{nn'}\,,$$

wobei $\frac{s}{n}\,,\,\frac{s'}{n'} \in S/\!\!/N$.

Mittels dieser Addition und dieser Multiplikation wird $S/\!\!/N$ ein kommutativer Ring.

Hierbei ist $0_{S/\!\!/N} = \frac{0_S}{1}$ und $1_{S/\!\!/N} = \frac{1_S}{1}$.

Wir haben den Ringmorphismus

$$\begin{array}{ccc} S & \xrightarrow{\lambda_{S,N}} & S/\!\!/N \\ s & \mapsto & \frac{s}{1}\,. \end{array}$$

Somit wird $S/\!\!/N = (S/\!\!/N, \lambda_{S,N} \circ \alpha)$ zu einer kommutativen R-Algebra und $\lambda_{S,N}$ zu einem R-Algebrenmorphismus.

Es ist $\lambda_{S,N}(N) \subseteq \mathrm{U}(S/\!\!/N)$.

Oft schreiben wir auch $\lambda = \lambda_{S,N}$. Oft schreiben wir mißbräuchlich $s := \frac{s}{1}$ für $s \in S$.

Beweis.

Zur Äquivalenzrelation $(\sim)$. Es ist $(s,n) \sim (s,n)$ für $(s,n) \in S \times N$. Ist $(s,n) \sim (s',n')$, dann ist $(s',n') \sim (s,n)$ für (s,n), $(s',n') \in S \times N$.

Seien nun (s,n), (s',n'), $(s'',n'') \in S \times N$ mit $(s,n) \sim (s',n')$ und $(s',n') \sim (s'',n'')$ gegeben. Wir wählen $x \in N$ mit $xsn' = xs'n$. Wir wählen $x' \in N$ mit $x's'n'' = x's''n'$. Dann ist $xx'n' \in N$ und

$$(xx'n')sn'' = x'n''(xsn') = x'n''(xs'n) = xn(x's'n'') = xn(x's''n') = (xx'n')s''n \,.$$

Also ist $(s,n) \sim (s'',n'')$.

Zur Wohldefiniertheit der Addition. Es genügt zu zeigen, daß für (s,n), $(\tilde{s},\tilde{n})$, $(s',n') \in S \times N$ aus $(s,n) \sim (\tilde{s},\tilde{n})$ folgt, daß $\frac{sn'+ns'}{nn'} \overset{!}{=} \frac{\tilde{s}n'+\tilde{n}s'}{\tilde{n}n'}$ ist. Wähle $x \in N$ mit $xs\tilde{n} = x\tilde{s}n$. Dann wird in der Tat

$$x(sn'+ns')(\tilde{n}n') = xsn'\tilde{n}n' + xns'\tilde{n}n' = x\tilde{s}n'nn' + xns'\tilde{n}n' = x(\tilde{s}n'+\tilde{n}s')(nn') \,.$$

Zur Wohldefiniertheit der Multiplikation. Es genügt zu zeigen, daß für (s,n), $(\tilde{s},\tilde{n})$, $(s',n') \in S \times N$ aus $(s,n) \sim (\tilde{s},\tilde{n})$ folgt, daß $\frac{ss'}{nn'} \overset{!}{=} \frac{\tilde{s}s'}{\tilde{n}n'}$ ist. Wähle $x \in N$ mit $xs\tilde{n} = x\tilde{s}n$. Dann wird in der Tat

$$x(ss')(\tilde{n}n') = x(\tilde{s}s')(nn') \,.$$

Zur abelschen Gruppe $(S /\!\!/ N, +)$. Seien $\frac{s}{n}$, $\frac{s'}{n'}$, $\frac{s''}{n''} \in S /\!\!/ N$ gegeben.

Es ist $\frac{0}{1} + \frac{s}{n} = \frac{0 \cdot n + 1 \cdot s}{1 \cdot n} = \frac{s}{n}$. Also ist $0_{S /\!\!/ N} = \frac{0}{1}$.

Es ist $\frac{s}{n} + \frac{s'}{n'} = \frac{sn'+ns'}{nn'} = \frac{s'n+n's}{nn'} = \frac{s'}{n'} + \frac{s}{n}$.

Es ist $(\frac{s}{n} + \frac{s'}{n'}) + \frac{s''}{n''} = \frac{sn'+ns'}{nn'} + \frac{s''}{n''} = \frac{(sn'+ns')n''+(nn')s''}{(nn')n''} = \frac{sn'n''+ns'n''+nn's''}{nn'n''}$. Auf der anderen Seite ist $\frac{s}{n} + (\frac{s'}{n'} + \frac{s''}{n''}) = \frac{s}{n} + \frac{s'n''+n's''}{n'n''} = \frac{s(n'n'')+n(s'n''+n's'')}{n(n'n'')} = \frac{sn'n''+ns'n''+nn's''}{nn'n''}$. Das ist dasselbe.

Es ist $\frac{s}{n} + \frac{-s}{n} = \frac{sn+n(-s)}{n^2} = \frac{0}{n^2} = \frac{0}{1}$.

Zum kommutativen Ring $(S /\!\!/ N, +, \cdot)$. Seien $\frac{s}{n}$, $\frac{s'}{n'}$, $\frac{s''}{n''} \in S /\!\!/ N$ gegeben.

Es ist $\frac{s}{n} \cdot \frac{1}{1} = \frac{s \cdot 1}{n \cdot 1} = \frac{s}{n}$. Also ist $1_{S /\!\!/ N} = \frac{1}{1}$.

Es ist $\frac{s}{n} \cdot \frac{s'}{n'} = \frac{ss'}{nn'} = \frac{s's}{n'n} = \frac{s'}{n'} \cdot \frac{s}{n}$.

Es ist $(\frac{s}{n} \cdot \frac{s'}{n'}) \cdot \frac{s''}{n''} = \frac{ss's''}{nn'''} = \frac{s}{n} \cdot (\frac{s'}{n'} \cdot \frac{s''}{n''})$.

Es ist $\frac{s}{n} \cdot (\frac{s'}{n'} + \frac{s''}{n''}) = \frac{s}{n} \cdot \frac{s'n''+n's''}{n'n''} = \frac{ss'n''+sn's''}{nn'n''}$ und $\frac{s}{n} \cdot \frac{s'}{n'} + \frac{s}{n} \cdot \frac{s''}{n''} = \frac{ss'}{nn'} + \frac{ss''}{nn''} = \frac{ss'nn''+nn'ss''}{nn'nn''} = \frac{ss'n''+sn's''}{nn'n''}$, was dasselbe ist.

Zum Ringmorphismus $\lambda_{S,N}$. Seien s, $s' \in S$ gegeben.

Es ist $\lambda_{S,N}(1_S) = \frac{1}{1} = 1_{S /\!\!/ N}$.

Es ist $\lambda_{S,N}(s) + \lambda_{S,N}(s') = \frac{s}{1} + \frac{s'}{1} = \frac{s\cdot 1 + 1\cdot s'}{1\cdot 1} = \frac{s+s'}{1} = \lambda_{S,N}(s+s')$.

Es ist $\lambda_{S,N}(s) \cdot \lambda_{S,N}(s') = \frac{s}{1} \cdot \frac{s'}{1} = \frac{s\cdot s'}{1} = \lambda_{S,N}(s \cdot s')$.

Zu $\lambda_{S,N}(N) \overset{!}{\subseteq} \mathrm{U}(S/\!\!/N)$. Für $n \in N$ ist $\lambda_{S,N}(n) \cdot \frac{1}{n} = \frac{n}{1} \cdot \frac{1}{n} = \frac{n}{n} = \frac{1}{1} = 1_{S/\!\!/N}$. ▫

Lemma 67 (Universelle Eigenschaft der Quotientenalgebra) *Sei $N \subseteq S$ eine multiplikative Teilmenge.*

Sei $T = (T, \beta)$ eine kommutative R-Algebra. Sei $S \xrightarrow{f} T$ ein R-Algebrenmorphismus mit $f(N) \subseteq \mathrm{U}(T)$.

Dann gibt es genau einen R-Algebrenmorphismus $S/\!\!/N \xrightarrow{f'} T$ mit $f' \circ \lambda_{S,N} = f$.

Dieser erfüllt dann $f'(\frac{s}{n}) = f(s) \cdot f(n)^-$ für $\frac{s}{n} \in S/\!\!/N$.

Beweis.

Zur Eindeutigkeit. Sei $S/\!\!/N \xrightarrow{g} T$ ein R-Algebrenmorphismus mit $g \circ \lambda_{S,N} = f$. Sei $\frac{s}{n} \in S/\!\!/N$. Wir wollen zeigen, daß $g(\frac{s}{n})$ durch die Vorgabe von f festliegt.

In der Tat ist $g(\frac{s}{n}) = g(\frac{s}{1} \cdot \frac{1}{n}) = g(\frac{s}{1}) \cdot g(\frac{1}{n}) = g(\frac{s}{1}) \cdot g((\frac{n}{1})^-) = g(\frac{s}{1}) \cdot (g(\frac{n}{1}))^- = (g \circ \lambda_{S,N})(s) \cdot ((g \circ \lambda_{S,N})(n))^- = f(s) \cdot f(n)^-$.

Zur Existenz. Wir wollen $f'(\frac{s}{n}) := f(s) \cdot f(n)^-$ setzen für $\frac{s}{n} \in S/\!\!/N$.

Zur Wohldefiniertheit von f'. Seien $s, \tilde{s} \in S$ und $n, \tilde{n} \in N$ gegeben, sowie $x \in N$ mit $xs\tilde{n} = x\tilde{s}n$. Dann wird in der Tat

$$\begin{aligned} f(s) \cdot f(n)^- &= f(x)^- \cdot f(\tilde{n})^- \cdot f(x) \cdot f(\tilde{n}) \cdot f(s) \cdot f(n)^- \\ &= f(x)^- \cdot f(\tilde{n})^- \cdot f(x\tilde{n}s) \cdot f(n)^- \\ &= f(x)^- \cdot f(\tilde{n})^- \cdot f(xn\tilde{s}) \cdot f(n)^- \\ &= f(x)^- \cdot f(\tilde{n})^- \cdot f(x) \cdot f(n) \cdot f(\tilde{s}) \cdot f(n)^- \\ &= f(\tilde{s}) \cdot f(\tilde{n})^- . \end{aligned}$$

Zu $f' \circ \lambda_{S,N} \overset{!}{=} f$. Für $s \in S$ wird $(f' \circ \lambda_{S,N})(s) = f'(\frac{s}{1}) = f(s) \cdot f(1)^- = f(s)$.

Zum Ringmorphismus f'. Seien $\frac{s}{n}, \frac{s'}{n'} \in S/\!\!/N$ gegeben.

Es wird $f'(1_{S/\!\!/N}) = f'(\frac{1}{1}) = f(1) \cdot f(1)^- = 1$.

Es wird $f'(\frac{s}{n} + \frac{s'}{n'}) = f'(\frac{s'n+n's}{nn'}) = f(s'n + n's) \cdot f(nn')^- = (f(s') \cdot f(n) + f(n') \cdot f(s)) \cdot f(n)^- \cdot f(n')^- = f(s') \cdot f(n')^- + f(s) \cdot f(n)^- = f'(\frac{s}{n}) + f'(\frac{s'}{n'})$.

Es wird $f'(\frac{s}{n} \cdot \frac{s'}{n'}) = f'(\frac{ss'}{nn'}) = f(ss') \cdot f(nn')^- = f(s) \cdot f(s') \cdot f(n)^- \cdot f(n')^- = (f(s) \cdot f(n)^-) \cdot (f(s') \cdot f(n')^-) = f'(\frac{s}{n}) \cdot f'(\frac{s'}{n'})$.

Zum R-Algebrenmorphismus f'. Zu zeigen ist $f' \circ (\lambda_{S,N} \circ \alpha) \overset{!}{=} \beta$. Für $r \in R$ wird

$$(f' \circ (\lambda_{S,N} \circ \alpha))(r) \;=\; f'(\frac{\alpha(r)}{1}) \;=\; f(\alpha(r)) \cdot f(1)^- \;=\; \beta(r) .$$

□

Bemerkung 68 (und Definition) *Sei $N \subseteq S$ eine multiplikative Teilmenge.*

Sei $\mathfrak{a}$ ein Ideal in S. Wir schreiben

$$\mathfrak{a}/\!\!/N \;:=\; \{\,\frac{a}{n} :\; a \in \mathfrak{a},\; n \in N\,\} \;\subseteq\; S/\!\!/N\,.$$

Es ist $\mathfrak{a}/\!\!/N$ ein Ideal in $S/\!\!/N$, das $\lambda_{S,N}(\mathfrak{a})$ enthält.

Es ist $\mathfrak{a}/\!\!/N$ in jedem Ideal von $S/\!\!/N$ enthalten, das $\lambda_{S,N}(\mathfrak{a})$ enthält.

Beweis. Es ist $0_{S/\!\!/N} = \frac{0}{1} \in \mathfrak{a}/\!\!/N$. Sind $\frac{s}{\tilde{n}}\,,\ \frac{s'}{\tilde{n}'} \in S/\!\!/N$ und $\frac{a}{n}\,,\ \frac{a'}{n'} \in \mathfrak{a}/\!\!/N$, dann ist

$$\frac{s}{\tilde{n}}\cdot\frac{a}{n} + \frac{s'}{\tilde{n}'}\cdot\frac{a'}{n'} \;=\; \frac{sa\tilde{n}'n' + \tilde{n}ns'a'}{\tilde{n}n\tilde{n}'n'} \;\in\; \mathfrak{a}/\!\!/N\,.$$

Ist $a \in \mathfrak{a}$, dann ist $\lambda_{S,N}(a) = \frac{a}{1} \in \mathfrak{a}/\!\!/N$. Also ist $\lambda_{S,N}(\mathfrak{a}) \subseteq \mathfrak{a}/\!\!/N$.

Ist umgekehrt $\mathfrak{b}$ ein Ideal in $S/\!\!/N$ mit $\lambda_{S,N}(\mathfrak{a}) \subseteq \mathfrak{b}$, dann ist für $a \in \mathfrak{a}$ und $n \in N$ auch $\frac{a}{n} = \frac{a}{1}\cdot\frac{1}{n} \in \mathfrak{b}$ und somit $\mathfrak{a}/\!\!/N \subseteq \mathfrak{b}$. □

Bemerkung 69

(1) *Sei $N \subseteq S$ eine multiplikative Teilmenge. Wir haben folgende Bijektion.*

$$\begin{array}{rcl} \{\,\mathfrak{p} \in \operatorname{Spec}(S) :\; \mathfrak{p} \subseteq S \smallsetminus N\,\} & \leftrightarrow & \operatorname{Spec}(S/\!\!/N) \\ \mathfrak{p} & \mapsto & \mathfrak{p}/\!\!/N \\ \lambda_{S,N}^{-1}(\mathfrak{q}) & \leftarrow\!\shortmid & \mathfrak{q} \end{array}$$

Ist ferner $\mathfrak{p} \in \operatorname{Spec}(S)$ mit $\mathfrak{p} \subseteq S \smallsetminus N$ gegeben, und ist $s \in S$ und $n \in N$, dann ist genau dann $\frac{s}{n} \in \mathfrak{p}/\!\!/N$, wenn $s \in \mathfrak{p}$ liegt.

(2) *Sei $\mathfrak{a} \subseteq S$ ein Ideal. Wir haben folgende Bijektion.*

$$\begin{array}{rcl} \{\,\mathfrak{p} \in \operatorname{Spec}(S) :\; \mathfrak{p} \supseteq \mathfrak{a}\,\} & \leftrightarrow & \operatorname{Spec}(S/\mathfrak{a}) \\ \mathfrak{p} & \mapsto & \rho_{S,\mathfrak{a}}(\mathfrak{p}) \\ \rho_{S,\mathfrak{a}}^{-1}(\mathfrak{q}) & \leftarrow\!\shortmid & \mathfrak{q} \end{array}$$

Beweis.

Ad (1). Zeigen wir zuerst die zweite *Behauptung.* Sei $s \in S$ und $n \in N$. Zu zeigen ist nur, daß aus $\frac{s}{n} \in \mathfrak{p}/\!\!/N$ folgt, daß $s \in \mathfrak{p}$ liegt. Sei also $\frac{s}{n} = \frac{p}{m}$ mit $p \in \mathfrak{p}$ und $m \in N$. Dann gibt es ein $x \in N$ mit $xsm = xpn \in \mathfrak{p}$. Da $x,\ m \in N \subseteq S \smallsetminus \mathfrak{p}$ liegen, folgt wegen $\mathfrak{p}$ prim hieraus $s \in \mathfrak{p}$. Dies zeigt die *Behauptung.*

Für die Wohldefiniertheit von $\mapsto$ müssen wir nachweisen, daß für $\mathfrak{p} \in \operatorname{Spec}(S)$ mit $\mathfrak{p} \subseteq S \smallsetminus N$ auch $\mathfrak{p}/\!\!/N$ ein Primideal von $S/\!\!/N$ ist. Es ist $\frac{1}{1} \notin \mathfrak{p}/\!\!/N$, da $1 \notin \mathfrak{p}$; cf. Behauptung.

Also ist $\mathfrak{p}/\!\!/N \subset S/\!\!/N$. Seien $\frac{s}{n}\,,\ \frac{s'}{n'} \in S/\!\!/N$ gegeben mit $\frac{s}{n}\cdot\frac{s'}{n'} \in \mathfrak{p}/\!\!/N$. Dank Behauptung ist dann $ss' \in \mathfrak{p}$, wegen $\mathfrak{p}$ prim also $s \in \mathfrak{p}$ oder $s' \in \mathfrak{p}$, woraus dann wieder $\frac{s}{n} \in \mathfrak{p}/\!\!/N$ oder $\frac{s'}{n'} \in \mathfrak{p}$ folgt.

Für die Wohldefiniertheit von $\leftarrow\!\!\shortmid$ merken wir zunächst an, daß $\lambda_{S,N}^{-1}(\mathfrak{q}) \in \operatorname{Spec}(S)$ liegt; cf. Bemerkung 44. Bleibt $N \cap \lambda_{S,N}^{-1}(\mathfrak{q}) \overset{!}{=} \emptyset$ zu zeigen. *Annahme*, es gibt ein $n \in N \cap \lambda_{S,N}^{-1}(\mathfrak{q})$. Dann ist $\lambda_{S,N}(n) \in \mathrm{U}(S/\!\!/N) \cap \mathfrak{q}$ dank Bemerkung 66 und also $\mathfrak{q} = S/\!\!/N$; cf. Bemerkung 30. Wir haben einen *Widerspruch* zu $\mathfrak{q} \subset S/\!\!/N$.

Sei $\mathfrak{p} \in \operatorname{Spec}(S)$ mit $\mathfrak{p} \cap N = \emptyset$ gegeben. Es ist $\lambda_{S,N}^{-1}(\mathfrak{p}/\!\!/N) = \{\, s \in S :\ \frac{s}{1} \in \mathfrak{p}\,\} = \mathfrak{p}$; cf. Behauptung.

Sei $\mathfrak{q} \in \operatorname{Spec}(S/\!\!/N)$. Es ist $\lambda_{S,N}^{-1}(\mathfrak{q})/\!\!/N \overset{!}{=} \mathfrak{q}$ zu zeigen. Sei $\frac{s}{n} \in \lambda_{S,N}^{-1}(\mathfrak{q})/\!\!/N$. Dann ist $s \in \lambda_{S,N}^{-1}(\mathfrak{q})$ gemäß Behauptung, i.e. $\frac{s}{1} \in \mathfrak{q}$. Also ist $\frac{s}{n} = \frac{s}{1}\cdot\frac{1}{n} \in \mathfrak{q}$. Sei umgekehrt $\frac{s}{n} \in \mathfrak{q}$. Dann ist $\frac{s}{1} = \frac{s}{n}\cdot\frac{n}{1} \in \mathfrak{q}$, i.e. $s \in \lambda_{S,N}^{-1}(\mathfrak{q})$. Also ist $\frac{s}{n} \in \lambda_{S,N}^{-1}(\mathfrak{q})/\!\!/N$.

Ad (2). Dies folgt aus den Aufgaben 10 und **??**.(4). ▫

Bemerkung 69.(2) wurde zwecks besserer Vergleichsmöglichkeit mit Bemerkung 69.(1) hier mit angeführt.

Bemerkung 70 *Sei $0_S \neq 1_S$. Sei $N \subseteq S$ eine multiplikative Teilmenge.*

Genau dann ist $S \xrightarrow{\lambda_{S,N}} S/\!\!/N$ injektiv, wenn N keinen Nullteiler von S und nicht 0_S enthält.

Insbesondere ist $\lambda_{S,N}$ injektiv, falls S integer und $0 \notin N$ ist.

Beweis. Wir wollen $\operatorname{Kern}(\lambda_{S,N})$ berechnen. Sei $s \in S$. Genau dann ist $s \in \operatorname{Kern}(\lambda_{S,N})$, wenn $\frac{s}{1} = \frac{0}{1}$ ist, i.e. wenn es ein $x \in N$ gibt mit $xs = 0$.

Genau dann zieht dies $s = 0$ nach sich, wenn N keinen Nullteiler von S und nicht 0_S enthält. ▫

Definition 71 Es heißt S *lokal*, wenn es in S genau ein maximales Ideal gibt.

Beispiel 72

(1) Ist S ein Körper, so ist S lokal, mit maximalem Ideal (0).

(2) Es ist $\mathbf{Z}/(4)$ eine lokale $\mathbf{Z}$-Algebra. Denn darin ist das von $2 + (4)$ erzeugte Ideal das eindeutige maximale Ideal.

Bemerkung 73 *Es ist S genau dann lokal, wenn $S \smallsetminus \mathrm{U}(S)$ ein Ideal in S ist.*

Diesenfalls ist $S \smallsetminus \mathrm{U}(S)$ das eindeutige maximale Ideal in S.

Beweis. Wir machen Gebrauch von Bemerkung 30.

Sei zum einen S lokal. Sei $\mathfrak{m} \subseteq S$ das eindeutige maximale Ideal. Wir behaupten $\mathfrak{m} = S \smallsetminus \mathrm{U}(S)$. Ist $x \in \mathfrak{m}$, dann ist $(x) \subseteq \mathfrak{m} \subset S$ und also $x \in S \smallsetminus \mathrm{U}(S)$. Ist umgekehrt $x \in S \smallsetminus \mathrm{U}(S)$, dann ist auch $xy \notin \mathrm{U}(S)$ für $y \in S$ und also $(x) \subset S$. Somit gibt es ein maximales Ideal $\mathfrak{n}$ in S mit $(x) \subseteq \mathfrak{n} \subset S$; cf. Lemma 47. Da es in S nur das maximale Ideal $\mathfrak{m}$ gibt, folgt $x \in (x) \subseteq \mathfrak{n} = \mathfrak{m}$.

Sei zum anderen $S \smallsetminus \mathrm{U}(S)$ ein Ideal in S. Sei $\mathfrak{m}$ ein maximales Ideal in S. Es genügt, $\mathfrak{m} \overset{!}{=} S \smallsetminus \mathrm{U}(S)$ zu zeigen. Da $\mathfrak{m} \subset S$ und $1 \in \mathrm{U}(S)$ ist, ist $\mathfrak{m} \subseteq S \smallsetminus \mathrm{U}(S) \subset S$. Dank Maximalität von $\mathfrak{m}$ ist also $\mathfrak{m} = S \smallsetminus \mathrm{U}(S)$. ▫

Bemerkung 74 (und Definition) *Sei* $\mathfrak{p} \in \mathrm{Spec}(S)$.

Wir betrachten die multiplikative Teilmenge $N := S \smallsetminus \mathfrak{p}$ *von* S*; cf. Beispiel* 65.(3).

Wir schreiben auch $S_\mathfrak{p} := S /\!\!/ N$ *für die* Lokalisierung von S an $\mathfrak{p}$.

Für ein Ideal $\mathfrak{a} \subseteq S$ *schreiben wir auch* $\mathfrak{a}_\mathfrak{p} := \mathfrak{a} /\!\!/ N$.

Es ist $S_\mathfrak{p}$ *lokal, mit maximalem Ideal* $\mathfrak{p}_\mathfrak{p}$.

Beweis.

Es genügt zu zeigen, daß $\mathfrak{p}_\mathfrak{p} = S_\mathfrak{p} \smallsetminus \mathrm{U}(S_\mathfrak{p})$ ist; cf. Bemerkung 73.

Um $\overset{!}{\subseteq}$ zu zeigen, genügt es $\frac{1}{1} \overset{!}{\notin} \mathfrak{p}_\mathfrak{p}$ zu zeigen; cf. Bemerkung 30. Dies aber folgt, da $1 \notin \mathfrak{p}$; cf. Bemerkung 69.(1).

Zeigen wir $\overset{!}{\supseteq}$. Sei $\frac{s}{n} \in S_\mathfrak{p} \smallsetminus \mathrm{U}(S_\mathfrak{p})$. Dann ist $s \notin N$, da *sonst* $\frac{s}{n} \cdot \frac{n}{s} = \frac{1}{1}$ auch $\frac{s}{n} \in \mathrm{U}(S_\mathfrak{p})$ nach sich zöge, was *nicht* so ist. Also ist $s \in \mathfrak{p}$ und somit $\frac{s}{n} \in \mathfrak{p}_\mathfrak{p}$. ▫

Bemerkung 75 (und Definition) *Sei* S *integer.*

Wir schreiben auch $\mathrm{Quot}(S) := S_{(0)} = S /\!\!/ S^\times$ *für den* Quotientenkörper *von* S.

Es ist in der Tat $\mathrm{Quot}(S)$ *ein Körper. Es ist* $S \xrightarrow{\lambda_{S,S^\times}} \mathrm{Quot}(S)$ *injektiv.*

Beweis. Es ist $(0)_{(0)} = (0)$ ein maximales Ideal in $\mathrm{Quot}(S)$; cf. Bemerkung 74. Also ist $\mathrm{Quot}(S) \simeq \mathrm{Quot}(S)/(0)$ ein Körper.

Da $S^\times$ keinen Nullteiler und nicht 0_S enthält, ist $\lambda_{S,S^\times}$ injektiv; cf. Bemerkung 70. ▫

Definition 76 Sei $x \in S$.

Schreibe $N := \{\, x^k : \ k \in \mathbf{Z}_{\geqslant 0} \,\}$.

Wir schreiben $S_x := S /\!\!/ N$.

Lemma 77 *Sei $\mathfrak{a}$ ein Ideal in S.*

Es ist $\sqrt{\mathfrak{a}} = \bigcap\{\, \mathfrak{p} \in \operatorname{Spec}(S) :\ \mathfrak{p} \supseteq \mathfrak{a} \,\}$.

Hierbei ist der Schnitt über eine leere Menge von Teilmengen von S als S definiert.

Beweis.

Ad $(\subseteq)$. Sei $\mathfrak{p} \in \operatorname{Spec}(S)$ mit $\mathfrak{p} \supseteq \mathfrak{a}$ gegeben. Es folgt $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$; cf. Bemerkung 43.(2).

Ad $(\supseteq)$. Sei $x \in S \smallsetminus \sqrt{\mathfrak{a}}$ gegeben. Wir haben zu zeigen, daß es ein $\mathfrak{p} \in \operatorname{Spec}(S)$ gibt mit $\mathfrak{p} \supseteq \mathfrak{a}$ und $x \notin \mathfrak{p}$.

Sei $N = \{\, x^k :\ k \in \mathbf{Z}_{\geqslant 0} \,\}$. Wir betrachten $S/\!\!/N = S_x$. Es ist $\mathfrak{a}/\!\!/N \subset S/\!\!/N$, da $\frac{1}{1} \notin \mathfrak{a}/\!\!/N$, da *ansonsten* aus $\frac{1}{1} = \frac{a}{x^k}$ für ein $a \in \mathfrak{a}$ und ein $k \in \mathbf{Z}_{\geqslant 0}$ folgen würde, daß $x^\ell \cdot x^k \cdot 1 = x^\ell \cdot 1 \cdot a \in \mathfrak{a}$ ist für ein $\ell \in \mathbf{Z}_{\geqslant 0}$, was *nicht* zutrifft. Somit gibt es ein maximales Ideal $\mathfrak{m}$ in $S/\!\!/N$ mit $\mathfrak{a}/\!\!/N \subseteq \mathfrak{m} \subset S/\!\!/N$; cf. Lemma 47. Folglich ist $\mathfrak{a} \subseteq \lambda_{S,N}^{-1}(\mathfrak{m}) =: \mathfrak{p} \in \operatorname{Spec}(S)$. Aber es ist $x \notin \mathfrak{p}$, da *ansonsten* $\frac{x}{1} \in \operatorname{U}(S/\!\!/N) \cap \mathfrak{m}$ läge, was gemäß Bemerkung 30 auch $\mathfrak{m} = S/\!\!/N$ nach sich zöge, was *nicht* so ist. $\square$

1.2.2 Limiten

Sei R ein kommutativer Ring.

1.2.2.1 Diagramme auf Quasiposets

Definition 78

(1) Sei I eine Menge. Eine Relation $(\leqslant)$ auf I heißt *Quasiteilordnung*, falls sie reflexiv und transitiv ist. Eine Menge I, ausgestattet mit einer Quasiteilordnung $(\leqslant)$, heißt auch *Quasiposet*.

(2) Ist $I = (I, \leqslant)$ ein Quasiposet und $J \subseteq I$, so ist $J = (J, (\leqslant) \cap (J \times J))$ ein Quasiposet, genannt *Teilquasiposet* von I.

(3) Sei $I = (I, \leqslant)$ ein Quasiposet. Ein *Diagramm* von kommutativen R-Algebren auf I besteht aus einem Tupel $(S_i)_{i \in I}$ aus kommutativen R-Algebren S_i und aus einem Tupel $(S_j \xleftarrow{u_{j,i}} S_i)_{j,\, i \in I,\, j \geqslant i}$ von R-Algebrenmorphismen derart, daß $u_{i,i} = \mathrm{id}_{S_i}$ ist für $i \in I$ und daß $u_{k,j} \circ u_{j,i} = u_{k,i}$ ist für alle $k,\ j,\ i\ \in\ I$ mit $k \geqslant j \geqslant i$.

(4) Sei $I = (I, \leqslant)$ ein Quasiposet. Es heißt I *gerichtet*, wenn es zu jedem $(i, j) \in I \times I$ ein $k \in I$ gibt mit $i \leqslant k$ und $j \leqslant k$.

1.2.2.2 Direkte Limiten und Halme

Sei $I = (I, \leqslant)$ ein nichtleeres gerichtetes Quasiposet.

Bemerkung 79 (und Definition) *Sei*

$$\mathcal{S} \;:=\; \big((S_i)_{i\in I}\,,\; (S_j \xleftarrow{u_{j,i}} S_i)_{j,\,i\,\in\, I,\, j\geqslant i}\big)$$

ein Diagramm von kommutativen R-Algebren. Sei dabei S_i mit dem Strukturmorphismus $R \xrightarrow{\alpha_i} S_i$ ausgestattet für $i \in I$.

Sei $M := \{\,(i, s_i) :\; i \in I,\; s_i \in S_i\,\}$.

Auf M sei die Relation $(\sim)$ folgendermaßen gegeben. Für $(i, s_i'),\ (j, s_j'') \in M$ sei

$$(i, s_i') \;\sim\; (j, s_j'')$$

genau dann, wenn es ein $k \in I$ gibt mit $k \geqslant i$ und $k \geqslant j$ und $u_{k,i}(s_i') = u_{k,\,j}(s_j'')$.

Es ist $(\sim)$ eine Äquivalenzrelation.

Für $(i, s_i) \in M$ schreiben wir $[i, s_i]$ für seine Äquivalenzklasse bezüglich $(\sim)$. Sei

$$\varinjlim_{i\in I} S_i \;:=\; \varinjlim \mathcal{S} \;:=\; \{\,[i, s_i] :\; (i, s_i) \in M\,\}$$

die Menge der Äquivalenzklassen von Elementen aus M.

Sei die Addition $(+)$ und die Multiplikation $(\cdot)$ auf $\varinjlim \mathcal{S}$ erklärt durch

$$[i, s_i'] + [j, s_j''] \;:=\; [k, u_{k,i}(s_i') + u_{k,j}(s_j'')]$$

resp. durch

$$[i, s_i'] \cdot [j, s_j''] \;:=\; [k, u_{k,i}(s_i') \cdot u_{k,j}(s_j'')]\;,$$

wobei $k \in I$ mit $k \geqslant i$ und $k \geqslant j$ gewählt sei.

Dann ist $\varinjlim \mathcal{S} = (\varinjlim \mathcal{S}, +, \cdot)$ ein kommutativer Ring.

Dabei ist $0_{\varinjlim \mathcal{S}} = [i, 0_{S_i}]$ und $1_{\varinjlim \mathcal{S}} = [i, 1_{S_i}]$ für jedes $i \in I$.

Wir haben den Ringmorphismus

$$\begin{array}{ccc} S_k & \xrightarrow{\omega_k^{\mathcal{S}}} & \varinjlim \mathcal{S} \\ s_k & \mapsto & [k, s_k] \end{array}$$

für $k \in I$. Es ist $\omega_\ell^{\mathcal{S}} \circ u_{\ell,k} = \omega_k^{\mathcal{S}}$ für $\ell,\ k \in I$ mit $\ell \geqslant k$.

Sei $\alpha := \omega_k^{\mathcal{S}} \circ \alpha_k$ für ein $k \in I$. Der Ringmorphismus α hängt nicht von der Wahl von $k \in I$ ab. Es ist $\varinjlim \mathcal{S} = (\varinjlim \mathcal{S}, \alpha)$ eine kommutative R-Algebra. Es ist $S_k \xrightarrow{\omega_k^{\mathcal{S}}} \varinjlim \mathcal{S}$ ein R-Algebrenmorphismus für $k \in I$.

Es heißt die R-Algebra $\varinjlim_{i\in I} S_i = \varinjlim \mathcal{S} = (\varinjlim \mathcal{S}, \alpha)$ der direkte Limes *des Diagramms $\mathcal{S}$.*

Oft schreiben wir auch $\omega_k := \omega_k^{\mathcal{S}}$ für $k \in I$.

Beweis.

Zur Äquivalenzrelation $(\sim)$. Es ist $(\sim)$ reflexiv und symmetrisch. Zeigen wir, daß $(\sim)$ transitiv ist. Seien (i, s_i'), (j, s_j''), (k, s_k''') in M gegeben mit $(i, s_i') \sim (j, s_j'')$ und $(j, s_j'') \sim (k, s_k''')$. Dann gibt es $\ell \in I$ mit $\ell \geqslant i$ und $\ell \geqslant j$ und $u_{\ell,i}(s_i') = u_{\ell,j}(s_j'')$. Ferner gibt es ein $m \in I$ mit $m \geqslant j$ und $m \geqslant k$ und $u_{m,j}(s_j'') = u_{m,k}(s_k''')$. Wähle $n \in I$ mit $n \geqslant \ell$ und $n \geqslant m$, möglich, da I gerichtet ist. Dann wird

$$\begin{array}{rcl} u_{n,i}(s_i') & = & u_{n,\ell}(u_{\ell,i}(s_i')) \;=\; u_{n,\ell}(u_{\ell,j}(s_j'')) \\ & = & u_{n,j}(s_j'') \;=\; u_{n,m}(u_{m,j}(s_j'')) \;=\; u_{n,m}(u_{m,k}(s_k''')) \;=\; u_{n,k}(s_k''') \end{array}$$

und also $(i, s_i') \sim (k, s_k''')$.

Beachte, daß für $(i, s_i) \in M$ und $j \in I$ mit $j \geqslant i$ stets $[i, s_i] = [j, u_{j,i}(s_i)]$ gilt, da $j \geqslant i$ und $j \geqslant j$ sowie $u_{j,i}(s_i) = u_{j,j}(u_{j,i}(s_i))$ gilt.

Zu $(+)$ *und* $(\cdot)$. Zeigen wir in der Situation der Definition der Addition, daß $[k, u_{k,i}(s_i') + u_{k,j}(s_j'')]$ nicht von der Wahl von k mit $k \geqslant i$ und $k \geqslant j$ abhängt. Sei $\ell \in I$ mit $\ell \geqslant i$ und $\ell \geqslant j$ gegeben. Wir haben $[k, u_{k,i}(s_i') + u_{k,j}(s_j'')] \overset{!}{=} [\ell, u_{\ell,i}(s_i') + u_{\ell,j}(s_j'')]$ zu zeigen. Wähle $m \in I$ mit $m \geqslant k$ und $m \geqslant \ell$. Dann wird

$$\begin{array}{rcl} [k, u_{k,i}(s_i') + u_{k,j}(s_j'')] & = & [m, u_{m,k}(u_{k,i}(s_i') + u_{k,j}(s_j''))] \\ & = & [m, u_{m,k}(u_{k,i}(s_i')) + u_{m,k}(u_{k,j}(s_j''))] \\ & = & [m, u_{m,i}(s_i') + u_{m,i}(s_j'')] \\ & = & [m, u_{m,\ell}(u_{\ell,i}(s_i')) + u_{m,\ell}(u_{\ell,j}(s_j''))] \\ & = & [m, u_{m,\ell}(u_{\ell,i}(s_i') + u_{\ell,j}(s_j''))] \\ & = & [\ell, u_{\ell,i}(s_i') + u_{\ell,j}(s_j'')] \;. \end{array}$$

Genauso hängt in der Situtation der Definition der Multiplikation $[k, u_{k,i}(s_i') \cdot u_{k,j}(s_j'')]$ nicht von der Wahl von k mit $k \geqslant i$ und $k \geqslant j$ ab.

Zeigen wir, daß $[k, u_{k,i}(s_i') + u_{k,j}(s_j'')]$ nicht von der Wahl der Repräsentanten (i, s_i') und (j, s_j'') abhängt. Es genügt zu zeigen, daß es nicht von der Wahl des Repräsentanten (i, s_i') abhängt. Sei $(h, \tilde{s}_h')$ mit $[i, s_i'] = [h, \tilde{s}_h']$ gegeben. Dann gibt es ein $\ell \in I$ mit $\ell \geqslant i$ und $\ell \geqslant h$ und $u_{\ell,i}(s_i') = u_{\ell,h}(\tilde{s}_h')$. Wähle ein $m \in I$ mit $m \geqslant k$ und $m \geqslant \ell$. Unter Beachtung der vorangegangenen Unabhängigkeit wird nun

$$\begin{array}{rcl} [m, u_{m,i}(s_i') + u_{m,j}(s_j'')] & = & [m, u_{m,\ell}(u_{\ell,i}(s_i')) + u_{m,j}(s_j'')] \\ & = & [m, u_{m,\ell}(u_{\ell,h}(\tilde{s}_h')) + u_{m,j}(s_j'')] \\ & = & [m, u_{m,h}(\tilde{s}_h') + u_{m,j}(s_j'')] \;. \end{array}$$

Genauso hängt $[k, u_{k,i}(s_i') \cdot u_{k,j}(s_j'')]$ nicht von der Wahl der Repräsentanten (i, s_i') und (j, s_j'') abhängt.

Zum kommutativen Ring $\varinjlim \mathcal{S}$.

Sei $i \in I$. Sei $[j, s_j] \in M$. Es ist

$$[i, 0_{S_i}] + [j, s_j] \;=\; [k, u_{k,i}(0_{S_i}) + u_{k,j}(s_j)] \;=\; [k, 0_{S_k} + u_{k,j}(s_j)] \;=\; [k, u_{k,j}(s_j)] \;=\; [j, s_j] \;,$$

wobei $k \in I$ mit $k \geqslant i$ und $k \geqslant j$. Folglich ist $0_{\varinjlim \mathcal{S}} := [i, 0_{S_i}]$ neutral bezüglich $(+)$. Diese Definition von $0_{\varinjlim \mathcal{S}}$ ist unabhängig von der Wahl von i.

Sei $i \in I$. Sei $[j, s_j] \in M$. Es ist

$$[i, 1_{S_i}] \cdot [j, s_j] \;=\; [k, u_{k,i}(1_{S_i}) \cdot u_{k,j}(s_j)] \;=\; [k, 1_{S_k} \cdot u_{k,j}(s_j)] \;=\; [k, u_{k,j}(s_j)] \;=\; [j, s_j]\;,$$

wobei $k \in I$ mit $k \geqslant i$ und $k \geqslant j$. Folglich ist $1_{\varinjlim \mathcal{S}} := [i, 1_{S_i}]$ neutral bezüglich $(\cdot)$. Diese Definition von $1_{\varinjlim \mathcal{S}}$ ist unabhängig von i.

Seien $[i, s'_i]$, $[j, s''_j]$, $[k, s'''_k] \in S$ gegeben. Wähle $m \in I$ mit $m \geqslant i$, $m \geqslant j$ und $m \geqslant k$, auffindbar durch zweifache Anwendung der Gerichtetheit von I. Es wird

$$\begin{array}{rcl}
[i, s'_i] + [j, s''_j] & = & [m, u_{m,i}(s'_i) + u_{m,j}(s''_j)] \\
& = & [m, u_{m,j}(s''_j) + u_{m,i}(s'_i)] \\
& = & [j, s''_j] + [i, s'_i] \\
([i, s'_i] + [j, s''_j]) + [k, s''_k] & = & ([m, u_{m,i}(s'_i) + u_{m,j}(s''_j)]) + [k, s''_k] \\
& = & [m, u_{m,i}(s'_i) + u_{m,j}(s''_j) + u_{m,k}(s''_k)] \\
& = & [i, s'_i] + [m, u_{m,j}(s''_j) + u_{m,k}(s''_k)] \\
& = & [i, s'_i] + ([j, s''_j] + [k, s''_k]) \\
[i, s'_i] + [i, -s'_j] & = & [i, s'_i - s'_j] \\
& = & [i, 0] \\
& = & 0_{\varinjlim \mathcal{S}}\;.
\end{array}$$

Entsprechend wird

$$\begin{array}{rcl}
[i, s'_i] \cdot [j, s''_j] & = & [m, u_{m,i}(s'_i) \cdot u_{m,j}(s''_j)] \\
& = & [m, u_{m,j}(s''_j) \cdot u_{m,i}(s'_i)] \\
& = & [j, s''_j] \cdot [i, s'_i] \\
([i, s'_i] \cdot [j, s''_j]) \cdot [k, s''_k] & = & ([m, u_{m,i}(s'_i) \cdot u_{m,j}(s''_j)]) \cdot [k, s''_k] \\
& = & [m, u_{m,i}(s'_i) \cdot u_{m,j}(s''_j) \cdot u_{m,k}(s''_k)] \\
& = & [i, s'_i] \cdot [m, u_{m,j}(s''_j) \cdot u_{m,k}(s''_k)] \\
& = & [i, s'_i] \cdot ([j, s''_j] \cdot [k, s''_k])\;.
\end{array}$$

Desweiteren wird

$$\begin{array}{rcl}
([i, s'_i] + [j, s''_j]) \cdot [k, s'''_k] & = & ([m, u_{m,i}(s'_i)] + [m, u_{m,j}(s''_j)]) \cdot [m, u_{m,k}(s'''_k)] \\
& = & ([m, u_{m,i}(s'_i) + u_{m,j}(s''_j)]) \cdot [m, u_{m,k}(s'''_k)] \\
& = & [m, (u_{m,i}(s'_i) + u_{m,j}(s''_j)) \cdot u_{m,k}(s'''_k)] \\
& = & [m, (u_{m,i}(s'_i) \cdot u_{m,k}(s'''_k) + u_{m,j}(s''_j) \cdot u_{m,k}(s'''_k)] \\
& = & [m, (u_{m,i}(s'_i) \cdot u_{m,k}(s'''_k)] + [m, u_{m,j}(s''_j) \cdot u_{m,k}(s'''_k)] \\
& = & [m, (u_{m,i}(s'_i)] \cdot [m, u_{m,k}(s'''_k)] + [m, u_{m,j}(s''_j)] \cdot [m, u_{m,k}(s'''_k)] \\
& = & [i, s'_i] \cdot [k, s'''_k] + [j, s''_j] \cdot [k, s'''_k]\;.
\end{array}$$

Also ist $\varinjlim \mathcal{S} = (\varinjlim \mathcal{S}, +, \cdot)$ ein kommutativer Ring.

Zum Ringmorphismus $\omega_k^{\mathcal{S}}$. Sei $k \in I$. Wir haben die Abbildung

$$\begin{array}{rcl} S_k & \xrightarrow{\omega_k^{\mathcal{S}}} & \varinjlim \mathcal{S} \\ s_k & \mapsto & [k, s_k] \end{array}$$

für $k \in I$. Seien s_k, $s'_k \in S_k$ gegeben. Es wird

$$\begin{array}{l} \omega_k^{\mathcal{S}}(s_k + s'_k) \;=\; [k, s_k + s'_k] \;=\; [k, s_k] + [k, s'_k] \;=\; \omega_k^{\mathcal{S}}(s_k) + \omega_k^{\mathcal{S}}(s'_k) \\ \omega_k^{\mathcal{S}}(1_{S_k}) \;=\; [k, 1_{S_k}] \;=\; 1_S \\ \omega_k^{\mathcal{S}}(s_k \cdot s'_k) \;=\; [k, s_k \cdot s'_k] \;=\; [k, s_k] \cdot [k, s'_k] \;=\; \omega_k^{\mathcal{S}}(s_k) \cdot \omega_k^{\mathcal{S}}(s'_k) \end{array}$$

Also ist $\omega_k^{\mathcal{S}}$ ein Ringmorphismus.

Für ℓ, $k \in I$ mit $\ell \geqslant k$ wird

$$(\omega_\ell^{\mathcal{S}} \circ u_{\ell,k})(s_k) \;=\; [\ell, u_{\ell,k}(s_k)] \;=\; [k, s_k] \;=\; \omega_k^{\mathcal{S}}(s_k)$$

für $s_k \in S_k$, woraus

$$\omega_\ell^{\mathcal{S}} \circ u_{\ell,k} \;=\; \omega_k^{\mathcal{S}}$$

folgt.

Zur kommutativen R-Algebra $\varinjlim \mathcal{S}$ und zum R-Algebrenmorphismus $\omega_k^{\mathcal{S}}$.

Zeigen wir, daß $\omega_k^{\mathcal{S}} \circ \alpha_k$ nicht von der Wahl von $k \in I$ abhängt. Sei $\ell \in I$. Wir haben $\omega_k^{\mathcal{S}} \circ \alpha_k \overset{!}{=} \omega_\ell^{\mathcal{S}} \circ \alpha_\ell$ zu zeigen. Wähle $m \in I$ mit $m \geqslant k$ und $m \geqslant \ell$. Es wird

$$\omega_k^{\mathcal{S}} \circ \alpha_k \;=\; \omega_m^{\mathcal{S}} \circ u_{m,k} \circ \alpha_k \;=\; \omega_m^{\mathcal{S}} \circ u_{m,\ell} \circ \alpha_\ell \;=\; \omega_\ell^{\mathcal{S}} \circ \alpha_\ell \,.$$

Somit können wir für beliebig gewähltes $k \in I$ setzen, es sei $\alpha := \omega_k^{\mathcal{S}} \circ \alpha_k$; dies ist unabhängig von der Wahl von k.

Es folgt, daß $\varinjlim \mathcal{S} = (\varinjlim \mathcal{S}, \alpha)$ eine kommutative R-Algebra ist.

Ferner ist wegen $\omega_k^{\mathcal{S}} \circ \alpha_k = \alpha$ in der Tat $S_k \xrightarrow{\omega_k^{\mathcal{S}}} S$ ein R-Algebrenmorphismus für $k \in I$. □

Lemma 80 (Universelle Eigenschaft des direkten Limes)

Sei

$$\mathcal{S} \;=\; \big((S_i)_{i \in I} \,,\; (S_j \xleftarrow{u_{j,i}} S_i)_{j,\, i \,\in\, I,\; j \geqslant i} \big)$$

ein Diagramm von kommutativen R-Algebren. Sei dabei S_i mit dem Strukturmorphismus $R \xrightarrow{\alpha_i} S_i$ ausgestattet für $i \in I$.

Sei $T = (T, \beta)$ eine kommutative R-Algebra. Sei $S_k \xrightarrow{\eta_k} T$ ein R-Algebrenmorphismus für $k \in I$, und sei dabei $\eta_\ell \circ u_{\ell,k} = \eta_k$ für ℓ, $k \in I$ mit $\ell \geqslant k$.

Dann gibt es genau einen R-Algebrenmorphismus $\varinjlim_{i \in I} S_i \xrightarrow{\eta} T$ mit $\eta \circ \omega_k^{\mathcal{S}} = \eta_k$ für $k \in I$. Es ist $\eta([i, s_i]) = \eta_i(s_i)$ für $[i, s_i] \in \varinjlim \mathcal{S}$.

Beweis. Schreibe $S := \varinjlim_{i\in I} S_i$ und α für den Strukturmorphismus von S.

Zur Eindeutigkeit. Ist $S \xrightarrow{\eta} T$ ein R-Algebrenmorphismus mit $\eta \circ \omega_k^{\mathcal{S}} = \eta_k$ für $i \in I$, dann ist für $s_k \in S_k$ auch $\eta([k, s_k]) = (\eta \circ \omega_k^{\mathcal{S}})(s_k) = \eta_k(s_k)$ festgelegt.

Zur Existenz. Wir wollen $\eta([k, s_k]) := \eta_k(s_k)$ setzen für $[k, s_k] \in S$. Dies ist unabhängig von der Repräsentantenwahl, denn ist $\ell \in I$ und $\tilde{s}_\ell \in S_\ell$ gegeben mit $(k, s_k) = (\ell, \tilde{s}_\ell)$, dann gibt es ein $m \in I$ mit $m \geqslant i$ und $m \geqslant j$ sowie $u_{m,k}(s_k) = u_{m,\ell}(\tilde{s}_\ell)$. Es folgt

$$\eta_k(s_k) \;=\; \eta_m(u_{m,k}(s_k)) \;=\; \eta_m(u_{m,\ell}(\tilde{s}_\ell)) \;=\; \eta_\ell(\tilde{s}_\ell)\ .$$

Also ist η eine wohldefinierte Abbildung.

Es ist $\eta \circ \omega_k^{\mathcal{S}} = \eta_k$ für $k \in I$, da für $s_k \in S_k$ sich $(\eta \circ \omega_k^{\mathcal{S}})(s_k) = \eta([k, s_k]) = \eta_k(s_k)$ ergibt.

Wir wollen zeigen, daß η ein Ringmorphismus ist. Es ist $\eta(1_S) = \eta([k, 1_{S_k}]) = \eta_k(1_{S_k}) = 1_T$, wozu $k \in I$ gewählt wurde.

Seien $[k, s'_k]$, $[\ell, s''_\ell] \in S$. Wähle $m \in I$ mit $m \geqslant k$ und $m \geqslant \ell$. Dann wird

$$\begin{array}{rcl}
\eta([k, s'_k] + [\ell, s''_\ell]) & = & \eta([m, u_{m,k}(s'_m) + u_{m,\ell}(s''_\ell)]) \\
& = & \eta_k(u_{m,k}(s'_k) + u_{m,\ell}(s''_\ell)]) \\
& = & \eta_k(u_{m,k}(s'_k)) + \eta_m(u_{m,\ell}(s''_\ell)]) \\
& = & \eta_k(s'_k) + \eta_\ell(s''_\ell) \\
& = & \\
et([k, s'_k]) + \eta([\ell, s''_\ell])\ . & &
\end{array}$$

Genauso wird

$$\eta([k, s'_k] \cdot [\ell, s''_\ell]) \;=\; \eta([k, s'_k]) \cdot \eta([\ell, s''_\ell])\ .$$

Bleibt zu zeigen, daß η ein R-Algebrenmorphismus ist, i.e. daß $\eta \circ \alpha = \beta$ ist. Für ein gewähltes $k \in I$ wird in der Tat

$$\eta \circ \alpha \;=\; \eta \circ \omega_k^{\mathcal{S}} \circ \alpha_k \;=\; \eta_k \circ \alpha_k \;=\; \beta\ .$$

□

Bemerkung 81 (und Definition) *Sei S eine kommutative R-Algebra.*

Für $x \in S$ sei $\mathrm{D}_x = \mathrm{D}_{S,x} := \{\, \mathfrak{p} \in \mathrm{Spec}(S) :\ x \notin \mathfrak{p} \,\}$.

Für y, $x \in S$ sei $y \geqslant x$, falls $\mathrm{D}_y \subseteq \mathrm{D}_x$ ist.

Wir schreiben $N_x := \{\, x^k :\ k \in \mathbf{Z}_{\geqslant 0} \,\}$ für $x \in S$.

Es gelten $(1, 2, 3)$.

(1) *Es ist $(S, \leqslant)$ ein Quasiposet. Ist $N \subseteq S$ eine multiplikative Teilmenge, dann ist N ein nichtleeres gerichtetes Teilquasiposet von S.*

(2) *Seien* $y, x \in S$ *gegeben. Genau dann ist* $y \geqslant x$, *wenn* $\sqrt{(y)} \subseteq \sqrt{(x)}$ *liegt.*

(3) *Seien* $y, x \in S$ *mit* $y \geqslant x$ *gegeben. Dann gibt es den R-Algebrenmorphismus*

$$\begin{array}{ccc} S_y & \xleftarrow{v_{y,x}} & S_x \\ \frac{s}{1} \cdot (\frac{x^k}{1})^- & \leftarrow\!\shortmid & \frac{s}{x^k} \end{array}$$

wobei $k \in \mathbf{Z}_{\geqslant 0}$. *Es ist* $v_{y,x} \circ \lambda_{S,N_x} = \lambda_{S,N_y}$.

(4) *Seien* $z, y, x \in S$ *mit* $z \geqslant y \geqslant x$ *gegeben. Dann ist* $v_{x,x} = \mathrm{id}_{S_x}$ *und* $v_{z,y} \circ v_{y,x} = v_{z,x}$.

Beweis.

Ad (1). Da $(\subseteq)$ auf den Teilmengen von S reflexiv und transitiv ist, ist auch $(\leqslant)$ reflexiv und transitiv. Somit ist S ein Quasiposet.

Betrachten wir das Teilquasiposet N. Da $1 \in N$, ist $N \neq \emptyset$. Bleibt zu zeigen, daß N gerichtet ist. Seien $x, y \in N$. Es ist $xy \in N$. Wegen Symmetrie genügt es, $\mathrm{D}_{xy} \overset{!}{\subseteq} \mathrm{D}_x$ zu zeigen. Sei $\mathfrak{p} \in \mathrm{D}_{xy}$. Dann ist $xy \notin \mathfrak{p}$. Also ist $x \notin \mathfrak{p}$.

Ad (2). Sei zum einen $y \geqslant x$, i.e. $\mathrm{D}_y \subseteq \mathrm{D}_x$. Dann ist $\{\, \mathfrak{p} : \mathfrak{p} \supseteq (y) \,\} \supseteq \{\, \mathfrak{p} : \mathfrak{p} \supseteq (x) \,\}$. Also ist $\bigcap\{\, \mathfrak{p} : y \in \mathfrak{p} \,\} \subseteq \bigcap\{\, \mathfrak{p} : x \in \mathfrak{p} \,\}$. Dank Lemma 77 bedeutet dies $\sqrt{(y)} \subseteq \sqrt{(x)}$.

Sei zum anderen $\sqrt{(y)} \subseteq \sqrt{(x)}$. Wir haben $y \overset{!}{\geqslant} x$ zu zeigen, i.e. $\mathrm{D}_y \overset{!}{\subseteq} \mathrm{D}_x$. Sei $\mathfrak{p} \in \mathrm{Spec}(S) \smallsetminus \mathrm{D}_x$. Wir haben $\mathfrak{p} \overset{!}{\in} \mathrm{Spec}(S) \smallsetminus \mathrm{D}_y$ zu zeigen, i.e. $y \overset{!}{\in} \mathfrak{p}$.

Es ist $x \in \mathfrak{p}$, also $(x) \subseteq \mathfrak{p}$ und somit in der Tat

$$y \;\in\; \sqrt{(y)} \;\subseteq\; \sqrt{(x)} \;\subseteq\; \sqrt{\mathfrak{p}} \;=\; \mathfrak{p}\,;$$

cf. Bemerkung 43.(2).

Ad (3). Gemäß Lemma 67 ist zu zeigen, daß $\lambda_{S,N_y}(N_x) \overset{!}{\subseteq} \mathrm{U}(S_y)$ liegt. Es genügt zu zeigen, daß $\lambda_{S,N_y}(x) = \frac{x}{1} \overset{!}{\in} \mathrm{U}(S_y)$ liegt. Dank (2) ist $y \in \sqrt{(y)} \subseteq \sqrt{(x)}$. Folglich gibt es ein $z \in S$ und ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $y^n = xz$. Wir erhalten $\frac{x}{1}\frac{z}{y^n} = \frac{1}{1}$ und also $\frac{x}{1} \in \mathrm{U}(S_y)$.

Für $s \in S$ ist $(v_{y,x} \circ \lambda_{S,N_x})(s) = \frac{s}{1} \cdot (\frac{x^0}{1})^- = \frac{s}{1} = \lambda_{S,N_y}(s)$. Also ist $v_{y,x} \circ \lambda_{S,N_x} = \lambda_{S,N_y}$.

Ad (4). Es ist $v_{x,x} \circ \lambda_{S,N_x} = \lambda_{S,N_x} = \mathrm{id}_{S_x} \circ \lambda_{S,N_x}$ und also $v_{x,x} = \mathrm{id}_{S_x}$; cf. Lemma 67.

Es ist $v_{z,y} \circ v_{y,x} \circ \lambda_{S,N_x} = v_{z,y} \circ \lambda_{S,N_y} = \lambda_{S,N_z} = v_{z,x} \circ \lambda_{S,N_x}$ und also $v_{z,y} \circ v_{y,x} = v_{z,x}$; cf. Lemma 67. □

Lemma 82 (Halme) *Sei* S *eine kommutative R-Algebra.*

Sei $N \subseteq S$ *eine multiplikative Teilmenge.*

Es ist $N = (N, \leqslant)$ *ein nichtleeres gerichtetes Teilquasiposet von* S *; cf. Bemerkung* 81.(1).

Es ist

$$\mathcal{S}_{S,N} \;:=\; \Big((S_x)_{x\in N}\,,\;(S_y \xleftarrow{v_{y,x}} S_x)_{y,\,x\,\in\,N,\;y\geqslant x}\Big)$$

ein Diagramm von kommutativen R-Algebren auf N; cf. Bemerkung 81.(3, 4).

Es gibt den R-Algebrenisomorphismus

$$\begin{array}{rcl} \varinjlim_{x\in N} S_x & \xrightarrow[\sim]{\eta} & S/\!\!/N \\ [x, \frac{s}{x^k}] & \mapsto & \frac{s}{x^k}\;. \end{array}$$

Für $\mathfrak{p} \in \mathrm{Spec}(S)$ *können wir insbesondere* $N = S \smallsetminus \mathfrak{p}$ *wählen. Wir erhalten so den R-Algebrenisomorphismus*

$$\begin{array}{rcl} \varinjlim_{\substack{x\in S \\ \text{with } \mathfrak{p}\,\in\, \mathrm{D}_x}} S_x & \xrightarrow[\sim]{\eta} & S_{\mathfrak{p}} \\ [x, \frac{s}{x^k}] & \mapsto & \frac{s}{x^k}\;. \end{array}$$

In den Begriffen der Algebraischen Geometrie, welche wir nicht einführen, haben wir so den Halm der Strukturgarbe auf dem affinen Schema $\mathrm{Spec}(S)$ im Punkt $\mathfrak{p}$ berechnet.

Beweis. Wir schreiben kurz $\omega_x := \boldsymbol{\omega}_x^{\mathcal{S}_{S,N}} : S_x \to \varinjlim_{x\in N} S_x \colon \frac{s}{x^k} \mapsto [x, \frac{s}{x^k}]$ für $x \in N$.

Wir haben den R-Algebrenmorphismus $\eta_x \colon S_x \xrightarrow{\eta_x} S/\!\!/N \colon \frac{s}{x^k} \mapsto \frac{s}{1}\cdot(\frac{x^k}{1})^- = \frac{s}{x^k}$; cf. Lemma 67.

Für $y,\, x \in N$ mit $y \geqslant x$ ist $\eta_y \circ v_{y,x} = \eta_x$. Denn für $\frac{s}{x^k} \in S_x$ wird

$$(\eta_y \circ v_{y,x})(\tfrac{s}{x^k}) \;=\; \eta_y(\tfrac{s}{1}\cdot(\tfrac{x^k}{1})^-) \;=\; \tfrac{s}{1}\cdot(\tfrac{x^k}{1})^- \;=\; \tfrac{s}{x^k} \;=\; \eta_x(\tfrac{s}{x^k})\;.$$

Also gibt es einen eindeutigen R-Algebrenmorphismus $\varinjlim_{x\in N} S_x \xrightarrow{\eta} S/\!\!/N$ mit $\eta\circ\omega_x = \eta_x$ für $x \in N$; cf. Lemma 80. Mithin ist

$$\eta([x, \tfrac{s}{x^k}]) \;=\; \eta(\omega_x(\tfrac{s}{x^k})) \;=\; \eta_x(\tfrac{s}{x^k}) \;=\; \tfrac{s}{x^k}\;.$$

Es bleibt zu zeigen, daß η bijektiv ist.

Zur Surjektivität. Sei $\frac{s}{x} \in S/\!\!/N$ gegeben. Dann ist $\frac{s}{x} = \eta([x, \frac{s}{x^1}])$.

Zur Injektivität. Wir haben zu zeigen, daß $\mathrm{Kern}(\eta) \overset{!}{=} (0)$ ist; cf. Aufgabe 8.(3). Sei $[y, \frac{s}{y^k}] \in \mathrm{Kern}(\eta)$. Dann ist $\frac{s}{y^k} = \frac{0}{1}$ in $S/\!\!/N$. Somit gibt es ein $n \in N$ mit $ns = 0$. Beachte, daß $yn \geqslant y$ ist; cf. e.g. Bemerkung 81.(2). Folglich wird

$$[y, \tfrac{s}{y^n}] \;=\; [yn, v_{yn,y}(\tfrac{s}{y^n})] \;=\; [yn, \tfrac{s}{1}\cdot(\tfrac{y^n}{1})^-] \;=\; [yn, \tfrac{syn}{yn}\cdot(\tfrac{y^n}{1})^-] \;=\; [yn, \tfrac{0}{yn}\cdot(\tfrac{y^n}{1})^-] \;=\; 0_{\varinjlim_{x\in N} S_x}\;.$$

□

1.2.2.3 Inverse Limiten und Komplettierung

Sei I ein Quasiposet.

Bemerkung 83 (und Definition) *Sei*

$$\mathcal{S} \; := \; \big((S_i)_{i\in I}\, ,\; (S_j \xleftarrow{u_{j,i}} S_i)_{j,\,i\,\in\, I,\, j\geqslant i}\big)$$

ein Diagramm von kommutativen R-Algebren. Sei dabei S_i mit dem Strukturmorphismus $R \xrightarrow{\alpha_i} S_i$ ausgestattet für $i \in I$.

Sei

$$\varprojlim_{i\in I} S_i \;=\; \varprojlim \mathcal{S} \;:=\; \{\,(s_i)_{i\in I} \in \prod_{i\in I} S_i :\; u_{\ell,k}(s_k) = s_\ell \text{ für } \ell,\, k \,\in\, I \text{ mit } \ell \geqslant k\,\}\;.$$

Es ist $\varprojlim \mathcal{S}$ eine R-Teilalgebra von $\prod_{i\in I} S_i$; cf. Bemerkung 17. Bezeichnen wir den Strukturmorphismus von $\varprojlim \mathcal{S}$ mit β, so ist $\beta(r) = (\alpha_i(r))_i$ für $r \in R$.

Für ein Element von $\varprojlim \mathcal{S}$ schreiben wir oft $(s_i)_i = (s_i)_{i\in I}$.

Für $k \in I$ haben wir den R-Algebrenmorphismus

$$\begin{array}{ccc} \varprojlim \mathcal{S} & \xrightarrow{\omega^k_{\mathcal{S}}} & S_k \\ (s_i)_i & \mapsto & s_k\;. \end{array}$$

Es ist $u_{\ell,k} \circ \omega^k_{\mathcal{S}} = \omega^\ell_{\mathcal{S}}$ für $\ell,\, k \,\in\, I$ mit $\ell \geqslant k$.

Oft schreiben wir auch $\omega^k := \omega^k_{\mathcal{S}}$ für $k \in I$.

Beweis. Es ist $(0_{S_i})_i \in \varprojlim \mathcal{S}$ und $(1_{S_i})_i \in \varprojlim \mathcal{S}$, da $u_{k,i}$ sowohl Null als auch Eins respektieren.

Seien $(s_i)_i\, ,\, (\tilde{s}_i)_i \,\in\, \varprojlim \mathcal{S}$. Seien $j,\, i \,\in\, I$ mit $j \geqslant i$ gegeben. Dann wird

$$\begin{array}{rcl} u_{j,i}(s_i - \tilde{s}_i) & = & u_{j,i}(s_i) - u_{j,i}(\tilde{s}_i) \\ & = & s_j - \tilde{s}_j \\ u_{j,i}(s_i \cdot \tilde{s}_i) & = & u_{j,i}(s_i) \cdot u_{j,i}(\tilde{s}_i) \\ & = & s_j \cdot \tilde{s}_j\;. \end{array}$$

Folglich sind auch $(s_i)_i - (\tilde{s}_i)_i$ und $(s_i)_i \cdot (\tilde{s}_i)_i \in \varprojlim \mathcal{S}$.

Bleibt zu zeigen, daß $\varprojlim \mathcal{S}$ eine R-Teilalgebra von $\prod_{i\in I} S_i$ ist. Sei $r \in R$. Der Strukturmorphismus α von $\prod_{i\in I} S_i$ schickt r auf $\alpha(r) = (\alpha_i(r))_i$; cf. Definition 16. Seien $j,\, i \,\in\, I$ mit $j \geqslant i$ gegeben. Es ist $u_{j,i}(\alpha_i(r)) = (u_{j,i} \circ \alpha_i)(r) = \alpha_j(r)$, da $u_{j,i}$ ein R-Algebrenmorphismus ist. Folglich ist $\alpha(r) \in \varprojlim \mathcal{S}$.

Dies zeigt, daß $\varprojlim \mathcal{S}$ eine R-Teilalgebra von $\prod_{i\in I} S_i$ ist, mit Strukturmorphismus $\beta := \alpha|^{\varprojlim \mathcal{S}}$, i.e. $\beta(r) = (\alpha_i(r))_i$ für $r \in R$.

Für $j \in J$ haben wir den R-Algebrenmorphismus $\pi_j\colon \prod_{i\in I} S_i \to S_i\colon (s_i)_i \mapsto s_j$; cf. Definition 16. Also ist auch $\omega^j_{\mathcal{S}} = \pi_j|_{\varprojlim \mathcal{S}}$ ein R-Algebrenmorphismus.

Für $\ell,\, k \in I$ mit $\ell \geqslant k$ ist $u_{\ell,k} \circ \omega^k_{\mathcal{S}} = \omega^\ell_{\mathcal{S}}$, da für $(s_i)_i \in \varprojlim \mathcal{S}$ sich

$$(u_{\ell,k} \circ \omega^k_{\mathcal{S}})\big((s_i)_i\big) \;=\; u_{\ell,k}(s_k) \;=\; s_\ell \;=\; \omega^\ell_{\mathcal{S}}\big((s_i)_i\big)$$

ergibt. ▫

Lemma 84 (Universelle Eigenschaft des inversen Limes)

Sei

$$\mathcal{S} \;:=\; \big((S_i)_{i\in I}\,,\; (S_j \xleftarrow{u_{j,i}} S_i)_{j,\,i\,\in\, I,\; j\geqslant i}\big)$$

ein Diagramm von kommutativen R-Algebren. Sei dabei S_i mit dem Strukturmorphismus $R \xrightarrow{\alpha_i} S_i$ ausgestattet für $i \in I$.

Sei $T = (T,\gamma)$ eine kommutative R-Algebra. Sei $T \xrightarrow{\xi^k} S_k$ ein R-Algebrenmorphismus für $k \in I$, und sei dabei $u_{\ell,k} \circ \xi^k = \xi^\ell$ für $\ell,\, k \in I$ mit $\ell \geqslant k$.

Dann gibt es genau einen R-Algebrenmorphismus $T \xrightarrow{\xi} \varprojlim_{i\in I} S_i$ mit $\omega^k_{\mathcal{S}} \circ \xi = \xi^k$ für $k \in I$. Es ist $\xi(t) = (\xi^i(t))_i$ für $t \in T$.

Beweis. Wir schreiben $\iota\colon \varprojlim_{i\in I} S_i \to \prod_{i\in I} S_i\colon (s_i)_i \mapsto (s_i)_i$ für den Einbettungsmorphismus. Wir schreiben $\pi_k\colon \prod_{i\in I} S_i \to S_k\colon (s_i)_i \mapsto s_k$.

Eindeutigkeit. Seien R-Algebrenmorphismen ξ und $\tilde{\xi}$ von T nach $\varprojlim_{i\in I} S_i$ gegeben mit $\omega^k_{\mathcal{S}} \circ \xi = \xi^k$ für $k \in I$. Dann ist auch $\pi_k \circ \iota \circ \xi = \omega^k_{\mathcal{S}} \circ \xi = \omega^k_{\mathcal{S}} \circ \tilde{\xi} = \pi_k \circ \iota \circ \tilde{\xi}$ und somit $\iota \circ \xi = \iota \circ \tilde{\xi}$; cf. Bemerkung 17. Wegen ι injektiv folgt $\xi = \tilde{\xi}$.

Existenz. Es gibt den R-Algebrenmorphismus $T \xrightarrow{\hat{\xi}} \prod_{i\in I} S_i\colon t \mapsto (\xi^i(t))_i$; cf. Bemerkung 17. Zu zeigen ist $\hat{\xi}(T) \overset{!}{\subseteq} \varprojlim \mathcal{S}$, da es dann einen R-Algebrenmorphismus $T \xrightarrow{\xi} \varprojlim \mathcal{S}$ mit $\iota \circ \xi = \hat{\xi}$ gibt.

Sei $t \in T$. Wir haben $\hat{\xi}(t) = (\xi^i(t))_i \overset{!}{\in} \varprojlim \mathcal{S}$ zu zeigen. Seien $\ell,\, k \in I$ mit $\ell \geqslant k$ gegeben. Es wird

$$u_{\ell,k}(\xi^k(t)) \;=\; (u_{\ell,k} \circ \xi^k)(t) \;=\; \xi^\ell(t)\;.$$

▫

Definition 85 Eine *diskrete Bewertungsalgebra* über R ist eine lokale, integre Hauptidealalgebra über R, welche kein Körper ist.

Bemerkung 86 *Sei S eine diskrete Bewertungsalgebra. Dann ist* $\operatorname{Spec}(S) = \{\,(0),\,(p)\,\}$ *für ein $p \in S^\times$ prim. Hierbei ist (p) maximal.*

Beweis. In einer integren Hauptidealalgebra sind alle Primideale ungleich (0) maximal. Denn aus $(p) \subseteq (q)$ mit $p,\, q \in S^\times$ prim folgt $p = qu$ für ein $u \in S$, wegen p prim also $q \in (p)$ oder $u \in (p)$. Ersterenfalls folgt $(p) = (q)$, wie gewünscht. Zweiterenfalls folgt $u = pv$ für ein $v \in S$, also $p = qu = pqv$, also $1 = qv$, also $q \in \mathrm{U}(S)$, was nicht eintritt.

Da S lokal ist, gibt es genau ein maximales Ideal in S. Da S kein Körper ist, ist dieses ungleich (0). Weitere Primideale gibt es nach vorstehender Anmerkung nicht. ▫

Bemerkung 87 *Sei S eine integre Hauptidealalgebra über R. Sei $p \in S^\times$ prim.*

Dann ist $S_{(p)}$ eine diskrete Bewertungsalgebra über R; cf. Bemerkung 74.

Beweis. Es ist $S_{(p)}$ lokal dank Bemerkung 74.

Zeigen wir, daß $S_{(p)}$ integer ist. Seien $\frac{s}{n}$, $\frac{s'}{n'} \in (S_{(p)})^\times$ gegeben. Wir haben $\frac{ss'}{nn'} \overset{!}{\neq} \frac{0}{1}$ zu zeigen. Da S integer ist, ergibt sich für $x \in S \smallsetminus (p)$ aus $s,\, s' \in S^\times$ auch $xss' \neq 0$.

Zeigen wir, daß $S_{(p)}$ ein Hauptidealbereich ist. Wir erinnern an den R-Algebrenmorphismus $\lambda\colon S \to S_{(p)} : s \mapsto \frac{s}{1}$. Sei $\mathfrak{a} \subseteq S_{(p)}$ ein Ideal. Es ist $\lambda^{-1}(\mathfrak{a}) = (a)$ für ein $a \in S$. Es ist $\frac{a}{1} \in \mathfrak{a}$. Folglich ist $(\frac{a}{1}) \subseteq \mathfrak{a}$. Wir wollen Gleichheit zeigen. Sei $\frac{s}{n} \in \mathfrak{a}$. Es wird $\frac{s}{1} = \frac{s}{n} \cdot \frac{n}{1} \in \mathfrak{a}$ und also $s \in \lambda^{-1}(\mathfrak{a}) = (a)$. Schreibe $s = at$ für ein $t \in S$. Es wird $\frac{s}{n} = \frac{a}{1} \cdot \frac{t}{n} \in (\frac{a}{1})$.

Zeigen wir, daß $S_{(p)}$ kein Körper ist. Es ist $(p)_{(p)}$ ein maximales Ideal in $S_{(p)}$. Es ist $(p)_{(p)} \ni \frac{p}{1} \neq \frac{0}{1}$, da S integer ist. ▫

Beispiel 88

(1) Sei $p \in \mathbf{Z}^\times$ prim. Es ist

$$\mathbf{Z}_{(p)} \;=\; \{\, \tfrac{z}{n} :\; z \in \mathbf{Z} \text{ und } n \in \mathbf{Z} \smallsetminus (p)\,\}$$

eine diskrete Bewertungsalgebra über $\mathbf{Z}$.

(2) Sei $a \in \mathbf{C}$. Sei X ein einzelnes Element. Es ist

$$\mathbf{C}[X]_{(X-a)} \;=\; \Big\{\, \tfrac{f(X)}{n(X)} :\; f(X),\, n(X) \,\in\, \mathbf{C}[X] \text{ und } n(a) \neq 0 \,\Big\}$$

eine diskrete Bewertungsalgebra über $\mathbf{C}$.

Bemerkung 89 (und Definition) *Sei S eine diskrete Bewertungsalgebra über R mit maximalem Ideal (p). Die folgenden Aussagen $(1,2,3)$ gelten.*

(1) *Sei $q \in S^\times$ prim. Dann gibt es ein $u \in \mathrm{U}(S)$ mit $q = pu$.*

(2) *Sei $\mathfrak{a} \subseteq S$ ein Ideal mit $\mathfrak{a} \neq (0)$. Dann gibt es genau ein $k \in \mathbf{Z}_{\geqslant 0}$ mit $\mathfrak{a} = (p^k)$.*

(3) *Sei* $s \in S^\times$. *Dann gibt es genau ein* $k \in \mathbf{Z}_{\geqslant 0}$ *und genau ein* $u \in \mathrm{U}(S)$ *mit* $s = p^k u$. *Wir schreiben auch* $\mathrm{v}_p(s) := k$ *(engl.* v*aluation, deutsch Bewertung).*

Beweis.

Ad (1). Es ist $(q) = (p)$; cf. Bemerkung 86. Also gibt es ein $u,\, v \in S$ mit $q = pu$ und $p = qv$. Wegen S integer folgt aus $q = pu = quv$, daß $1 = uv$ ist, mithin $u \in \mathrm{U}(S)$.

Ad (2). Da S eine Hauptidealalgebra ist, gibt es ein $a \in S$ mit $\mathfrak{a} = (a)$. Da $\mathfrak{a} \neq (0)$, ist $a \neq 0$.

Fall $a \in \mathrm{U}(S)$. Es ist $\mathfrak{a} = (a) = S = (p^0)$. Für $k \in \mathbf{Z}_{\geqslant 1}$ ist $(p^k) \subseteq (p) \subset S$ und also $\mathfrak{a} \neq (p^k)$.

Fall $a \in S \smallsetminus \mathrm{U}(S)$. Wir können a als Produkt von Primelementen aus $S^\times$ schreiben, cf. Aufgabe **??**.(2). Dank (1) folgt $a = p^k u$ für ein $k \in \mathbf{Z}_{\geqslant 1}$ und ein $u \in \mathrm{U}(S)$. Also ist $\mathfrak{a} = (p^k)$.

Bleibt die Eindeutigkeit zu zeigen. Sei $(p^k) = (p^\ell)$ mit $k,\, \ell \in \mathbf{Z}_{\geqslant 1}$. Zu zeigen ist $k \overset{!}{=} \ell$. O.E. $k \leqslant \ell$. Es ist $p^k = p^\ell b$ für ein $b \in S$. Wegen S integer folgt $1 = p^{\ell - k} b$ und somit $p^{\ell-k} \in \mathrm{U}(S)$, mithin $\ell - k = 0$.

Ad (3). Sei $s \in S^\times$. Dann gibt es genau ein $k \in \mathbf{Z}_{\geqslant 0}$ mit $(s) = (p^k)$; cf. (2). Also ist $s = p^k u$ und $p^k = sv$ für gewisse $u,\, v \in S$. Dank S integer folgt aus $p^k uv = sv = p^k$, daß $uv = 1$ und also $u \in \mathrm{U}(S)$ ist.

Bleibt die Eindeutigkeit von $k \in \mathbf{Z}_{\geqslant 0}$ und von $u \in \mathrm{U}(S)$ zu zeigen. Wegen S integer genügt es, die Eindeutigkeit von k zu zeigen. Diese folgt aber aus (2). $\square$

Definition 90 Sei S eine diskrete Bewertungsalgebra über R, mit maximalem Ideal (p).

Betrachten wir das linear geordnete Poset $\mathbf{Z}_{\geqslant 1}$ mit der linearen Ordnung $(\succeq)$ definiert durch $j \succeq i$ genau dann, wenn $j \leqslant i$, wobei $j,\, i \in \mathbf{Z}_{\geqslant 1}$.

Für $i \in \mathbf{Z}_{\geqslant 1}$ sei $S_i := S/(p^i)$. Für $j,\, i \in \mathbf{Z}_{\geqslant 1}$ mit $j \succeq i$, i.e. $j \leqslant i$, sei

$$\begin{array}{ccc} S_j & \xleftarrow{u_{j,i}} & S_i \\ s + (p^j) & \leftarrow\!\shortmid & s + (p^i) \end{array}$$

Dann ist $\mathcal{S} := \big((S_i)_{i \in \mathbf{Z}_{\geqslant 1}}\,,\ (S_j \xleftarrow{u_{j,i}} S_i)_{j,\,i \in I,\, j \succeq i}\big)$ ein Diagramm auf I ; cf. Definition 78.(3). Wir schreiben

$$\widehat{S} \;:=\; \varprojlim \mathcal{S} \;=\; \varprojlim_{i \geqslant 1} S/(p^i) \;=\; \{\, (s_i + (p^i))_{i \geqslant 1} :\ s_i \equiv_{p^j} s_j \text{ für } j,\, i \,\in\, \mathbf{Z}_{\geqslant 1} \text{ mit } j \leqslant i \,\}$$

für die *Komplettierung* von S. Wir haben den R-Algebrenmorphismus

$$\begin{array}{ccc} \widehat{S} & \xrightarrow{\omega^i} & S/(p^i) \\ (s_i + (p^i))_{i \geqslant 1} & \mapsto & s_i + (p^i) \end{array}$$

für $i \in \mathbf{Z}_{\geqslant 1}$.

Wir haben auch den R-Algebrenmorphismus

$$\begin{array}{ccc} S & \xrightarrow{\rho_{S,(p^i)}} & S/(p^i) \\ s & \mapsto & s + (p^i) \end{array}$$

für $i \in \mathbf{Z}_{\geqslant 1}$, und es ist $u_{j,i} \circ \rho_{S,(p^i)} = \rho_{S,(p^j)}$ für $j,\, i \in \mathbf{Z}_{\geqslant 1}$ mit $j \succeq i$, i.e. $j \leqslant i$.

Gemäß Lemma 84 liefert dies den R-Algebrenmorphismus

$$\begin{array}{ccc} S & \xrightarrow{\kappa_S} & \widehat{S} \\ s & \mapsto & (s + (p^i))_{i \geqslant 1} \,. \end{array}$$

Es heißt S *komplett*, wenn κ_S ein Isomorphismus von R-Algebren ist.

Lemma 91 *Sei S eine diskrete Bewertungsalgebra über R, mit maximalem Ideal (p). Die Aussagen $(1, 2, 3, 4)$ treffen zu.*

(1) *Es ist κ_S injektiv. Wir schreiben oft mißbräuchlich $s := \kappa_S(s)$ für $s \in S$.*

(2) *Es ist $\kappa_S^{-1}(\,(p^k)\,) = (p^k)$ für $k \in \mathbf{Z}_{\geqslant 0}$.*

(3) *Es ist $\widehat{S}$ eine diskrete Bewertungsalgebra, mit maximalem Ideal (p).*

(4) *Sei $k \in \mathbf{Z}_{\geqslant 1}$. Wir haben den R-Algebrenisomorphismus*

$$\begin{array}{rcl} S/(p^k) & \to & \widehat{S}/(p^k) \\ s + (p^k) & \mapsto & s + (p^k) \,. \end{array}$$

(5) *Es ist $\widehat{S}$ komplett.*

Beweis. Da S integer ist, dürfen wir S als R-Teilalgebra von $\operatorname{Quot}(S)$ ansehen und darin p^{-1} verwenden.

Ad (1). Sei $s \in \operatorname{Kern}(\kappa_S)$. Dann ist $s \in (p^i)$ für alle $i \in \mathbf{Z}_{\geqslant 0}$.

Annahme, es ist $s \in S^\times$. Wir können $s = p^k u$ schreiben für ein $k \in \mathbf{Z}_{\geqslant 0}$; cf. Bemerkung 89.(3). Da aber $s = p^k u \in (p^{k+1})$ liegt, gibt es ein $t \in S$ mit $p^k u = p^{k+1} t$, wegen S integer also $u = pt$, also $1 = p(tu^-)$. Es folgt $p \in \mathrm{U}(S)$. Wir haben einen *Widerspruch* zu $(p) \subset S$. Also ist $s = 0$.

Folglich ist $\operatorname{Kern}(\kappa_S) = 0$, i.e. κ_S ist injektiv.

Ad (2). Es ist $p^k \in \kappa_S^{-1}(\,(p^k)\,)$, da $\kappa_S(p^k) = \kappa_S(p)^k = p^k$. Also ist $\kappa_S^{-1}(\,(p^k)\,) \supseteq (p^k)$.

Zeigen wir $\kappa_S^{-1}(\,(p^k)\,) \overset{!}{\subseteq} (p^k)$. Sei $\kappa_S(s) \in (p^k)$. Also gibt es ein $(t_i + (p^i))_i \in \widehat{S}$ mit $(s + (p^i))_i = (t_i + (p^i))_i \cdot (p^k + (p^i))_i = (t_i p^k + (p^i))_i$. Es folgt $s + (p^k) = t_k p^k + (p^k) = 0 + (p^k)$ und also $s \in (p^k)$.

Ad (3). Wir beobachten, daß für $a,\, b\, \in\, \mathrm{U}(S)$ und $m \in \mathbf{Z}_{\geqslant 0}$ aus $a+(p^m) = b+(p^m)$ auch

$$a^- + (p^m) \;=\; (a^- b^- + (p^m))(b+(p^m)) \;=\; (a^- b^- + (p^m))(a+(p^m)) \;=\; b^- + (p^m)$$

folgt.

Wir *behaupten*, daß jedes Element $(s_i + (p^i))_i \in \widehat{S}^\times$ von der Form $p^k u$ ist für ein $k \in \mathbf{Z}_{\geqslant 0}$ und ein $u \in \mathrm{U}(\widehat{S})$, wobei $k \in \mathbf{Z}_{\geqslant 0}$ minimal ist mit $s_{k+1} \not\in (p^{k+1})$, was wegen $(s_i + (p^i))_i \neq (0 + (p^i))_i$ existiert. Da $s_\ell + (p^k) = s_k + (p^k) = 0 + (p^k)$ ist für $\ell \in \mathbf{Z}_{\geqslant k}$, können wir $u_i := p^{-k} s_{i+k}$ setzen für $i \in \mathbf{Z}_{\geqslant 1}$. Für $j,\, i\, \in\, \mathbf{Z}_{\geqslant 1}$ mit $j \geqslant i$ wird dann $s_{j+k} + (p^{i+k}) = s_{i+k} + (p^{i+k})$ und also

$$u_j + (p^i) \;=\; p^{-k} s_{j+k} + (p^i) \;=\; p^{-k} s_{i+k} + (p^i) \;=\; u_i + (p^i)\;.$$

Somit ist $(u_i + (p^i)) \in \widehat{S}$. Für $\ell \geqslant 1$ ist ferner $u_\ell + (p) = u_1 + (p) = p^{-k} s_{k+1} + (p) \neq 0 + (p)$, i.e. $u_\ell \in S \smallsetminus \mathfrak{p} = \mathrm{U}(S)$. Für $j,\, i\, \in\, \mathbf{Z}_{\geqslant 1}$ mit $j \geqslant i$ wird dann

$$u_j^- + (p^i) \;=\; u_i^- + (p^i)$$

dank vorstehender Beobachtung. Somit ist auch $(u_i^- + (p^i))_i \in \widehat{S}$. Da nun $(u_i^- + (p^i))_i \cdot (u_i + (p^i))_i = (1 + (p^i))_i$ ist, folgt $u := (u_i + (p^i))_i \in \mathrm{U}(\widehat{S})$.

Es bleibt zu zeigen, daß $p^k u = (p^k u_i + (p^i))_i \overset{!}{=} (s_i + (p^i))_i$ ist. In der Tat wird für $i \in \mathbf{Z}_{\geqslant 1}$

$$p^k u_i + (p^i) \;=\; s_{i+k} + (p^i) \;=\; s_i + (p^i)\;.$$

Dies zeigt die *Behauptung*.

Seien nun Elemente $p^k u$ und $p^\ell v$ aus $\widehat{S}^\times$ gegeben, wobei $k,\, \ell\, \in\, \mathbf{Z}_{\geqslant 0}$ und $u,\, v\, \in\, \mathrm{U}(\tilde{S})$. Dann ist ihr Produkt $p^{k+\ell} uv$ ungleich 0, da der R-Algebrenmorphismus $\omega_S^{k+\ell+1}$ die Einheit uv auf eine Einheit in $S/(p^{k+\ell+1})$ schickt und das Element $p^{k+\ell}$ auf $p^{k+\ell} + (p^{k+\ell+1})$, also nicht auf 0. Somit ist $\widehat{S}$ integer.

Ferner ist p wegen $\omega_S^1(p) = 0$ keine Einheit, aber wegen $\omega_S^2(p) \neq 0$ auch ungleich 0. Insbesondere ist $\widehat{S}$ kein Körper.

Sei nun $\mathfrak{a}$ ein Ideal in $\widehat{S}$. Sei $\mathfrak{a} \neq (0)$. Sei $p^k u$ ein Element mit minimalem Exponenten k in $\mathfrak{a} \smallsetminus (0)$, wobei $u \in \mathrm{U}(\widehat{S})$. Dann ist $(p^k) \subseteq \mathfrak{a}$. Ist umgekehrt $p^\ell v \in \mathfrak{a}$, wobei $\ell \in \mathbf{Z}_{\geqslant 0}$ und $v \in \mathrm{U}(\widehat{S})$, dann ist $\ell \geqslant k$ und also $p^\ell v = p^k \cdot p^{\ell-k} v \in (p^k)$. Also ist $(p^k) = \mathfrak{a}$. Folglich ist (p) das einzige maximale Ideal von $\widehat{S}$.

Somit ist $\widehat{S}$ eine integre, lokale Hauptidealalgebra, aber kein Körper. I.e. es ist $\widehat{S}$ ein diskreter Bewertungsring. Das maximale Ideal ist (p).

Ad (4). Dank (2) ist der fragliche R-Algebrenmorphismus wohldefiniert und injektiv; cf. Aufgabe 8.(2). Zu zeigen bleibt, daß er surjektiv ist. Sei $(s_i + (p^i))_i \in \widehat{S}$ gegeben. Es wird $s_k + (p^k)$ abgebildet auf $s_k + (p^k) = (s_k + (p^i))_i + (p^k)$. Wir wollen zeigen, daß

$$(s_k + (p^i))_i + (p^k) \;\overset{!}{=}\; (s_i + (p^i))_i + (p^k)$$

ist. In der Tat wird die Differenz zu $(s_k - s_i + (p^i))_i$. Ihr Tupeleintrag bei $i \in [1, k-1]$ ist gleich 0. Folglich ist sie durch p^k teilbar; cf. Behauptung.

Ad (5). Zu zeigen ist, daß $\kappa_{\widehat{S}}$ ein R-Algebrenisomorphismus ist. Es genügt zu zeigen, daß $\kappa_{\widehat{S}}$ surjektiv ist; cf. (1).

Sei $((s_{j,i} + (p^i))_i + (p^j))_j \in \widehat{\widehat{S}}$ gegeben. Wir *behaupten*

$$\kappa_{\widehat{S}}(s_{i,i} + (p^i)) \overset{!}{=} ((s_{i,i} + (p^i))_i + (p^j))_j \overset{!}{=} ((s_{j,i} + (p^i))_i + (p^j))_j \; .$$

Zu zeigen ist hierfür zunächst einmal, daß $(s_{i,i}+(p^i))_i$ ein Element von $\widehat{S}$ ist, i.e. daß wir für $\ell,\, k \in I$ mit $\ell \geqslant k$ auch $s_{\ell,\ell} \equiv_{p^k} s_{k,k}$ haben. Da $(s_{\ell,i} + (p^i))_i \in \widehat{S}$ liegt, ist $s_{\ell,\ell} \equiv_{p^k} s_{\ell,k}$. Da $((s_{j,i}+(p^i))_i+(p^j))_j \in \widehat{\widehat{S}}$ liegt, ist $(s_{\ell,i}+(p^i))_i \equiv_{p^k} (s_{k,i}+(p^i))_i$, insbesondere $s_{\ell,k} \equiv_{p^k} s_{k,k}$. Zusammen ist

$$s_{\ell,\ell} \equiv_{p^k} s_{\ell,k} \equiv_{p^k} s_{k,k} \; .$$

Zu zeigen ist hierfür ferner, daß $(s_{j,i} + (p^i))_i \equiv_{p^j} (s_{i,i} + (p^i))_i$ ist für $j \in \mathbf{Z}_{\geqslant 0}$, i.e. daß $(s_{j,i} - s_{i,i} + (p^i))_i \overset{!}{\in} (p^j)$ liegt. Gemäß Behauptung aus (4) genügt es zu zeigen, daß $s_{j,i} - s_{i,i} \equiv_{p^i} 0$ ist für $i \in [1, j]$. Das aber folgt wie eben aus $((s_{j,i} + (p^i))_i + (p^j))_j \in \widehat{\widehat{S}}$. Dies zeigt die *Behauptung*. ▫

Beispiel 92 Sei $p \in \mathbf{Z}$ eine Primzahl. Wir betrachten die Komplettierung $\widehat{\mathbf{Z}_{(p)}}$ der diskreten Bewertungsalgebra $\mathbf{Z}_{(p)}$ über $\mathbf{Z}$; cf. Bemerkung 87.

Es ist $\mathbf{Z}/(p^k) \to \mathbf{Z}_{(p)}/(p^k) \colon z + (p^k) \mapsto z + (p^k)$ ein Isomorphismus von $\mathbf{Z}$-Algebren; cf. Aufgabe **??**.(3).

Jedes Element von $\widehat{\mathbf{Z}_{(p)}}$ ist also von der Form $(w_i + (p^i))_i$ mit $w_i \in \mathbf{Z}$ und mit $w_{i+1} \equiv_{p^i} w_i$ für $i \in \mathbf{Z}_{\geqslant 1}$. Somit ist es von der Form

$$(z_0\, p^0 + (p^1),\; z_0\, p^0 + z_1\, p^1 + (p^1),\; z_0\, p^0 + z_1\, p^1 + z_2\, p^2 + (p^3),\; \ldots) \;=:\; \lfloor z_0 | z_1 | z_2 | z_3 | \ldots \rfloor \; ,$$

mit eindeutig festgelegten Elementen $z_i \in [0, p-1]$ für $i \in \mathbf{Z}_{\geqslant 0}$. Dies ist die *p-adische* Darstellung dieses Elements. Dementsprechend wird $\widehat{\mathbf{Z}_{(p)}}$ auch der *Ring der p-adischen Zahlen* genannt.

Es ist $\mathbf{Z}_{(p)}$ abzählbar.

Es ist $\widehat{\mathbf{Z}_{(p)}}$ überabzählbar. Denn für jede Abbildung $\mathbf{Z}_{\geqslant 0} \to \widehat{\mathbf{Z}_{(p)}} \colon n \mapsto \xi_n$ können wir $\xi_n =: \lfloor z_{n,0} | z_{n,1} | z_{n,2} | z_{n,3} | \ldots \rfloor$ schreiben mit $z_{n,i} \in [0, p-1]$ stets. Wir wählen nun ein $v_i \in [0, p-1] \smallsetminus \{z_{i,i}\}$ für $i \in \mathbf{Z}_{\geqslant 0}$. Für jedes $n \in \mathbf{Z}_{\geqslant 0}$ ist

$$\lfloor z_{n,0} | z_{n,1} | z_{n,2} | z_{n,3} | \ldots \rfloor \neq \lfloor v_0 | v_1 | v_2 | v_3 | \ldots \rfloor \; ,$$

da jedenfalls in Position n sich $z_{n,n} \neq v_n$ einstellt. Also ist $n \mapsto \xi_n$ nicht surjektiv.

1.3 Weitere Anwendungen der Konstruktionen

1.3.1 Mehr zur Primärzerlegung

Sei R ein kommutativer Ring. Sei S eine noethersche kommutative R-Algebra.

Beispiel 93 Sei K ein Körper. Seien X und Y Elemente.

Sei $\mathfrak{a} := (X^2, XY)$.

Es ist $\mathfrak{a}$ nicht primär. Denn es ist $XY \in \mathfrak{a}$ und $X \in \mathfrak{a}$, aber $Y^n \notin \mathfrak{a}$ für alle $n \in \mathbf{Z}_{\geqslant 0}$.

(1) *Es ist* $\mathfrak{a} = (X) \cap (X,Y)^2$ *eine Primärzerlegung.*
Dabei ist $\sqrt{(X)} = (X)$ *und* $\sqrt{(X,Y)^2} = (X,Y)$.

Es ist (X) prim wegen des Isomorphismus $K[X,Y]/(X) \to K[Y] \colon X \mapsto 0,\ Y \mapsto Y$, invertiert von $K[Y] \to K[X,Y]/(X) \colon Y \mapsto Y$.

Es ist (X,Y) maximal, insbesondere prim; cf. Beispiel 37. Also ist $(X,Y)^2$ primär und $\sqrt{(X,Y)^2} = (X,Y)$; cf. Bemerkung 44.

Es ist $\mathfrak{a} \subseteq (X) \cap (X,Y)^2$.

Sei umgekehrt $f(X,Y) \in (X) \cap (X,Y)^2$ gegeben. Dann ist

$$f(X,Y) \;=\; b(X,Y)X^2 + c(X,Y)XY + d(X,Y)Y^2$$

für gewisse $b(X,Y)$, $c(X,Y)$, $d(X,Y) \in K[X,Y]$. Da X ein Teiler von $f(X,Y)$ ist, teilt X auch $d(X,Y)$. Folglich ist $f(X,Y) \in (X^2, XY) = \mathfrak{a}$.

(2) *Sei* $s \in K$. *Es ist* $\mathfrak{a} = (X) \cap (X^2, Y + sX)$ *eine Primärzerlegung.*
Dabei ist $\sqrt{(X)} = (X)$ *und* $\sqrt{(X^2, Y + sX)} = (X,Y)$.

Es ist (X) prim; cf. (1).

Es ist $(X,Y)^2 \subseteq (X^2, Y + sX) \subseteq (X,Y)$, ersteres wegen $XY = X(Y + sX) - sX^2$ und dann wegen $Y^2 = Y(Y + sX) - sXY$. Da (X,Y) maximal ist, ist mithin $(X^2, Y + sX)$ primär; cf. (1) und Bemerkung 44.

Es ist

$$(X,Y) \;\subseteq\; \sqrt{(X^2, Y + sX)} \;\subseteq\; \sqrt{(X,Y)} \;=\; (X,Y)\;,$$

ersteres wegen $(X,Y)^2 \subseteq (X^2, Y + sX)$, letzteres wegen Bemerkung 43.(2).

Also ist $\sqrt{(X^2, Y + sX)} = (X,Y)$.

Es ist

$$\mathfrak{a} \;\subseteq\; (X) \cap (X,Y)^2 \;\subseteq\; (X) \cap (X^2, Y + sX)\;;$$

cf. (1). Sei umgekehrt $f(X,Y) \in (X) \cap (X^2, Y + sX)$. Dann ist

$$f(X,Y) \;=\; b(X,Y)X^2 + c(X,Y)(Y + sX)$$

für gewisse $b(X,Y)$, $c(X,Y) \in K[X,Y]$. Da X ein Teiler von $f(X,Y)$ ist, teilt X auch $c(X,Y)$. Folglich ist $f(X,Y) \in (X^2, XY) = \mathfrak{a}$.

(3) Es fällt auf, daß die Menge der Radikale der Teilnehmer der Primärzerlegung sowohl in (1) als auch in (2) gleich $\{(X),\ (X,Y)\}$ ist.

Ferner fällt auf, daß (X) minimal ist in dieser Menge und daß das zu (X) gehörige Primärideal in (1) und in (2) beidemale gleich (X) ist.

Dahingegen ist das Primärideal $(X,Y)^2$ aus (1) echt im Primärideal $(X^2, Y+sX)$ aus (2) enthalten, da $Y+sX$ nicht in $(X,Y)^2$ liegt, da jedes Monom eines Polynoms in $(X,Y)^2$ durch X^2, durch XY oder durch Y^2 teilbar ist, was für Y nicht zutrifft. Somit unterscheidet sich die Primärzerlegung in (1) von allen Primärzerlegungen, die in (2) auftreten.

Ferner sind für $s,\ \tilde{s} \in K$ mit $s \neq \tilde{s}$ die Primärzerlegungen $\mathfrak{a} = (X) \cap (X^2, Y+sX)$ und $\mathfrak{a} = (X) \cap (X^2, Y+\tilde{s}X)$ aus (2) verschieden:

Jedenfalls ist $(X) \neq (X^2, Y+\tilde{s}X)$, da sonst $\mathfrak{a} = (X)$ folgte, was wegen $\mathfrak{a}$ nicht primär und (X) prim nicht geht.

Annahme $(X^2, Y+sX) = (X^2, Y+\tilde{s}X)$. Dann liegt $Y+sX \in (X^2, Y+\tilde{s}X)$. Es ist also $Y+sX = a(X,Y)X^2 + b(X,Y)(Y+\tilde{s}X)$ für gewisse $a(X,Y)$, $b(X,Y) \in K[X,Y]$. Koeffizientenvergleich bei Y liefert $b(X,Y) = 1+\tilde{b}(X,Y)$ für ein $\tilde{b}(X,Y) \in K[X,Y]$ mit $\tilde{b}(0,0) = 0$. Also wird $(s-\tilde{s})X = a(X,Y)X^2 + \tilde{b}(X,Y)(Y+\tilde{s}X)$. Koeffizientenvergleich bei X liefert $s = \tilde{s}$, was *nicht* zutrifft.

Definition 94 Sei $\mathfrak{a} \subset S$ ein Ideal. Sei

$$\mathrm{Ass}(S,\mathfrak{a}) \;:=\; \{\,\mathfrak{p} \in \mathrm{Spec}(S) :\ \text{es gibt ein } s \in S \smallsetminus \mathfrak{a} \text{ mit } \mathfrak{p} = (\mathfrak{a} : (s))\,\} \;\subseteq\; \mathrm{Spec}(S)$$

die Menge der *zu* $\mathfrak{a}$ *assoziierten* Primideale in S.

Zu (0) assoziierte Primideale heißen auch kurz *assoziiert*. Wir schreiben dann auch $\mathrm{Ass}(S) := \mathrm{Ass}(S,(0))$.

Bemerkung 95 *Sei* $\mathfrak{a} \subset S$ *ein Ideal.*

Ist $\mathfrak{p} \in \mathrm{Ass}(S,\mathfrak{a})$*, dann ist* $\mathfrak{p} \supseteq \mathfrak{a}$.

Beweis. Es gibt ein $s \in S \smallsetminus \mathfrak{a}$ mit $\mathfrak{p} = (\mathfrak{a} : (s))$. Also ist $\mathfrak{a} \subseteq (\mathfrak{a} : (s)) = \mathfrak{p}$. ▫

Beispiel 96

(1) Ist $\mathfrak{p} \in \mathrm{Spec}(S)$, dann ist $(\mathfrak{p} : (s)) = \mathfrak{p}$ für alle $s \in S \smallsetminus \mathfrak{p}$. Somit ist $\mathrm{Ass}(S,\mathfrak{p}) = \{\mathfrak{p}\}$.

(2) Wir betrachten die $\mathbf{Z}$-Algebra $\mathbf{Z}$ und darin das Ideal (12).

Sei $s \in \mathbf{Z} \smallsetminus (12)$. Es ist $((12) : (s)) \in \{\,(2),\ (4),\ (3),\ (6),\ (12)\,\}$.

Also ist $\mathrm{Ass}(\mathbf{Z},(12)) = \{\,(2),\ (3)\,\}$.

Bemerkung 97 *Sei* $\mathfrak{a} \subset S$ *ein Ideal.*

Es ist $\operatorname{Ass}(S, \mathfrak{a}) \neq \emptyset$.

Beweis. Wir betrachten die Menge $M := \{\, (\mathfrak{a} : (s)) : \; s \in S \smallsetminus \mathfrak{a} \,\}$, teilgeordnet mittels $(\subseteq)$. Es ist $\mathfrak{a} = (\mathfrak{a} : (1)) \in M$.

Da S noethersch ist, gibt es in M ein maximales Element $(\mathfrak{a} : (x))$, wobei $x \in S \smallsetminus \mathfrak{a}$; cf. Aufgabe 12.

Wir *behaupten*, daß $(\mathfrak{a} : (x))$ prim ist.

Es ist $(\mathfrak{a} : (x)) \subset S$ wegen $x \not\in \mathfrak{a}$ und also $1 \not\in (\mathfrak{a} : (x))$.

Seien $y,\, z \in S$ mit $yz \in (\mathfrak{a} : (x))$, aber $z \not\in (\mathfrak{a} : (x))$ gegeben. Wir haben $y \overset{!}{\in} (\mathfrak{a} : (x))$ zu zeigen.

Es ist $xyz \in \mathfrak{a}$, aber es ist $xz \not\in \mathfrak{a}$. Wir haben $xy \overset{!}{\in} \mathfrak{a}$ zu zeigen.

Da $(\mathfrak{a} : (x)) \subseteq (\mathfrak{a} : (xz))$ ist und da $xz \in S \smallsetminus \mathfrak{a}$ liegt, gibt die Maximalität von $(\mathfrak{a} : (x))$ in M die Gleichheit $(\mathfrak{a} : (x)) = (\mathfrak{a} : (xz))$. Wegen $xyz \in \mathfrak{a}$ ist $y \in (\mathfrak{a} : (xz)) = (\mathfrak{a} : (x))$. Also ist $xy \in \mathfrak{a}$. Dies zeigt die *Behauptung.* ▫

Lemma 98 *Sei* $\mathfrak{a} \subset S$ *ein Ideal. Sei* $y \in S \smallsetminus \mathfrak{a}$. *Sei* $\mathfrak{b} := (\mathfrak{a} : (y))$.

(1) *Es existiert in* $\{\, \mathfrak{q} \in \operatorname{Spec}(S) : \; \mathfrak{b} \subseteq \mathfrak{q} \,\}$ *ein minimales Element.*

(2) *Jedes minimale Element* $\mathfrak{p}$ *in* $\{\, \mathfrak{q} \in \operatorname{Spec}(S) : \; \mathfrak{b} \subseteq \mathfrak{q} \,\}$ *ist assoziiert zu* $\mathfrak{a}$.

Beweis.

Ad (1). Es ist $\mathfrak{b} \subset S$ wegen $y \not\in \mathfrak{a}$. Folglich ist $\{\, \mathfrak{q} \in \operatorname{Spec}(S) : \; \mathfrak{b} \subseteq \mathfrak{q} \,\} \neq \emptyset$; cf. Lemma 47, Definition 33. Dank Lemma 50 existiert in dieser Menge ein minimales Element.

Ad (2). Es ist $S_\mathfrak{p}$ noethersch; cf. Aufgabe **??**.

Wäre $\frac{1}{1} \in \mathfrak{b}_\mathfrak{p}$, dann wäre $\frac{1}{1} = \frac{b}{n}$ mit $b \in \mathfrak{b}$ und $n \in S \smallsetminus \mathfrak{p}$, also gäbe es ein $x \in S \smallsetminus \mathfrak{p}$ mit $xn = xb$, aber $xn \in S \smallsetminus \mathfrak{p}$ und $xb \in \mathfrak{b} \subseteq \mathfrak{p}$, was *nicht* geht. Also ist $\mathfrak{b}_\mathfrak{p} \subset S_\mathfrak{p}$.

Dank Bemerkung 97 ist also $\operatorname{Ass}(S_\mathfrak{p}, \mathfrak{b}_\mathfrak{p}) \neq \emptyset$.

Wir *behaupten* $\operatorname{Ass}(S_\mathfrak{p}, \mathfrak{b}_\mathfrak{p}) \overset{!}{=} \{\mathfrak{p}_\mathfrak{p}\}$. Sei $\mathfrak{q} \in \operatorname{Spec}(S)$ mit $\mathfrak{q} \subset \mathfrak{p}$. Es genügt, $\mathfrak{q}_\mathfrak{p} \overset{!}{\not\in} \operatorname{Ass}(S_\mathfrak{p}, \mathfrak{b}_\mathfrak{p})$ zu zeigen; cf. Bemerkungen 69.(1) und 74.

Annahme, es ist $\mathfrak{q}_\mathfrak{p} \in \operatorname{Ass}(S_\mathfrak{p}, \mathfrak{b}_\mathfrak{p})$. Es ist $\mathfrak{b}_\mathfrak{p} \subseteq \mathfrak{q}_\mathfrak{p}$; cf. Bemerkung 95. Also ist

$$\mathfrak{b} \;\subseteq\; \lambda^{-1}(\mathfrak{b}_\mathfrak{p}) \;\subseteq\; \lambda^{-1}(\mathfrak{q}_\mathfrak{p}) \;=\; \mathfrak{q}\;;$$

cf. Bemerkung 69.(1). Aber wegen der Minimalität von $\mathfrak{p}$ und wegen $\mathfrak{q} \subset \mathfrak{p}$ muß $\mathfrak{b} \not\subseteq \mathfrak{q}$ sein. Dieser *Widerspruch* zeigt die *Behauptung.*

Also gibt es ein $\frac{s}{n} \in S_\mathfrak{p} \smallsetminus \mathfrak{b}_\mathfrak{p}$ mit $\mathfrak{p}_\mathfrak{p} = (\mathfrak{b}_\mathfrak{p} : (\frac{s}{n}))$. Da S noethersch ist, können wir $\mathfrak{p} = (p_1, \dots, p_k)$ schreiben für ein $k \in \mathbf{Z}_{\geqslant 0}$ und gewisse $p_i \in S$ für $i \in [1,k]$. Dann ist $\frac{s}{n} \cdot \frac{p_i}{1} \in \mathfrak{b}_\mathfrak{p}$ für $i \in [1,k]$. Folglich gibt es ein $t_i \in S \smallsetminus \mathfrak{p}$ mit $t_i s p_i \in \mathfrak{b}$ für $i \in [1,k]$. Mit $t = \prod_{i \in [1,k]} t_i \in S \smallsetminus \mathfrak{p}$ ist also $tsp_i \in \mathfrak{b}$ für $i \in [1,k]$.

Wir *behaupten* $\mathfrak{p} \overset{!}{=} (\mathfrak{b} : (st))$. Es gilt $\mathfrak{p} \subseteq (\mathfrak{b} : (st))$, da $tsp_i \in \mathfrak{b}$ ist für $i \in [1,k]$. Sei umgekehrt $x \in (\mathfrak{b} : (st))$ gegeben. Wir haben $x \overset{!}{\in} \mathfrak{p}$ zu zeigen. Es ist $stx \in \mathfrak{b}$.

Wäre $x \in S \smallsetminus \mathfrak{p}$, dann wäre $\frac{tx}{1} \in \mathrm{U}(S_\mathfrak{p})$. Da aber $\frac{s}{n} \cdot \frac{tx}{1} \in \mathfrak{b}_\mathfrak{p}$ liegt, folgte $\frac{s}{n} \in \mathfrak{b}_\mathfrak{p}$, was *nicht* zutrifft. Dies zeigt die *Behauptung*. Insbesondere ist $st \notin \mathfrak{b}$.

Wir wollen $\mathfrak{p} \overset{!}{=} (\mathfrak{a} : (sty))$ zeigen. Für $z \in S$ ist genau dann $z \in (\mathfrak{a} : (sty))$, wenn $stzy \in \mathfrak{a}$ liegt, i.e. wenn $stz \in \mathfrak{b}$ liegt, i.e. wenn $z \in (\mathfrak{b} : (st)) = \mathfrak{p}$ liegt. Dies zeigt die fragliche Gleichheit. Insbesondere ist $sty \notin \mathfrak{a}$.

Infolgedessen ist $\mathfrak{p} \in \mathrm{Ass}(S, \mathfrak{a})$. ▫

Lemma 99 *Sei* $\mathfrak{q} \subset S$ *ein Ideal.*

Die Aussagen $(1,2)$ *sind äquivalent.*

(1) *Es ist* $\mathfrak{q}$ *primär.*

(2) *Es ist* $\mathrm{Ass}(S, \mathfrak{q}) = \{\sqrt{\mathfrak{q}}\}$.

Beweis.

Ad (1) $\Rightarrow$ (2). Da $\mathfrak{q}$ primär ist, ist $\sqrt{\mathfrak{q}}$ prim; cf. Bemerkung 43.(2).

Es ist $\mathfrak{q} \subset S$. Also ist $\mathrm{Ass}(S, \mathfrak{q}) \neq \emptyset$; cf. Bemerkung 97.

Sei nun $\mathfrak{p} \in \mathrm{Ass}(S, \mathfrak{q})$ gegeben. Wir haben $\mathfrak{p} \overset{!}{=} \sqrt{\mathfrak{q}}$ zu zeigen.

Aus $\mathfrak{q} \subseteq \mathfrak{p}$ folgt $\sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$; cf. Bemerkungen 95 und 43.(2).

Bleibt $\sqrt{\mathfrak{q}} \overset{!}{\supseteq} \mathfrak{p}$ zu zeigen. Schreibe $\mathfrak{p} = (\mathfrak{q} : (x))$ für ein $x \in S \smallsetminus \mathfrak{q}$. Sei $y \in \mathfrak{p} = (\mathfrak{q} : (x))$ gegeben. Aus $yx \in \mathfrak{q}$ und $x \notin \mathfrak{q}$ folgt wegen $\mathfrak{q}$ primär, daß $y \in \sqrt{\mathfrak{q}}$ liegt.

Ad (2) $\Rightarrow$ (1). Es ist $\mathfrak{p} := \sqrt{\mathfrak{q}}$ prim.

Seien $z \in S$ und $y \in S \smallsetminus \mathfrak{q}$ mit $zy \in \mathfrak{q}$ gegeben. Wir haben $z \overset{!}{\in} \mathfrak{p}$ zu zeigen.

Es ist $z \in (\mathfrak{q} : (y)) =: \mathfrak{t} \subset S$. Somit genügt es, $\sqrt{\mathfrak{t}} \overset{!}{=} \mathfrak{p}$ zu zeigen.

Sei M die Menge der minimalen Elemente von $\{\, \mathfrak{u} \in \mathrm{Spec}(S) : \ \mathfrak{t} \subseteq \mathfrak{u} \,\}$.

Die Menge M ist endlich, da sie in Bijektion steht zur Menge der minimalen Primideale von $S/\mathfrak{q}$; cf. Bemerkung 69.(2), Aufgabe **??**.(2), Satz 58. Das brauchen wir aber nicht.

In der nichtleeren Menge $\{\,\mathfrak{u}\in\operatorname{Spec}(S):\ \mathfrak{t}\subseteq\mathfrak{u}\,\}$ liegt jedes Element über einem Element von M ; cf. Lemmata 47 und 50. Also ist $M\neq\emptyset$ und es ist

$$\sqrt{\mathfrak{t}} \overset{\text{Lemma 77}}{=} \bigcap\{\,\mathfrak{u}\in\operatorname{Spec}(S):\ \mathfrak{t}\subseteq\mathfrak{u}\,\} \;=\; \bigcap M\;.$$

Es genügt also, $M\overset{!}{\subseteq}\{\mathfrak{p}\}$ zu zeigen.

Aber ist $\mathfrak{v}\in M$, dann ist $\mathfrak{v}\in\operatorname{Ass}(S,\mathfrak{q})$ gemäß Lemma 98. Und es ist $\operatorname{Ass}(S,\mathfrak{q})=\{\mathfrak{p}\}$ nach Voraussetzung. Also ist $\mathfrak{v}=\mathfrak{p}$. ▫

Definition 100 Sei $\mathfrak{a}\subset S$ ein Ideal.

Wir betrachten eine Primärzerlegung $\mathfrak{a}=\bigcap_{i\in[1,k]}\mathfrak{q}_i$, wobei $k\in\mathbf{Z}_{\geqslant 0}$ und wobei $\mathfrak{q}_i$ ein Primärideal in S ist für $i\in[1,k]$. Cf. Satz 63.

Es heißt eine solche Primärzerlegung *reduziert*, wenn $\mathfrak{a}\subset\bigcap_{i\in[1,k]\smallsetminus\{j\}}\mathfrak{q}_i$ ist für $j\in[1,k]$ und wenn $\sqrt{\mathfrak{q}_i}\neq\sqrt{\mathfrak{q}_j}$ ist für $i,\,j\in[1,k]$ mit $i\neq j$.

Beispiel 101 Die Primärzerlegungen in Beispiel 93.(1, 2) sind reduziert, da $\mathfrak{a}$ selbst nicht primär ist und da $(X)\neq(X,Y)$ ist.

Bemerkung 102 *Sei $\mathfrak{a}$ ein Ideal in S.*

Es besitzt $\mathfrak{a}$ eine reduzierte Primärzerlegung.

Beweis. Wir können eine Primärzerlegung $\mathfrak{a}=\bigcap_{i\in[1,k]}\mathfrak{q}_i$ wählen; cf. Satz 63.

Für $i,\,j\in[1,k]$ sei $i\sim j$, falls $\sqrt{\mathfrak{q}_i}=\sqrt{\mathfrak{q}_j}$ ist. Es ist $(\sim)$ eine Äquivalenzrelation. Wir wählen Repräsentanten h_j für $j\in[1,\ell]$ der ℓ Äquivalenzklassen.

Sei $\tilde{\mathfrak{q}}_j:=\bigcap_{i\in[1,k],\,i\sim h_j}\mathfrak{q}_h$ für $j\in[1,\ell]$. Dann ist $\tilde{\mathfrak{q}}_j$ ein Primärideal mit $\sqrt{\tilde{\mathfrak{q}}_j}=\sqrt{\mathfrak{q}_i}$ für $i\in[1,k]$ mit $i\sim h_j$; cf. Aufgabe **??**. Ferner ist

$$\mathfrak{a} \;=\; \bigcap_{i\in[1,k]}\mathfrak{q}_i \;=\; \bigcap_{j\in[1,\ell]}\left(\bigcap_{i\in[1,k],\,i\sim h_j}\mathfrak{q}_i\right) \;=\; \bigcap_{j\in[1,\ell]}\tilde{\mathfrak{q}}_j\;.$$

Für $j,\,j'\in[1,\ell]$ mit $j\neq j'$ ist $h_j\not\sim h_{j'}$ und also $\sqrt{\tilde{\mathfrak{q}}_j}=\sqrt{\mathfrak{q}_{h_j}}\neq\sqrt{\mathfrak{q}_{h_{j'}}}=\sqrt{\tilde{\mathfrak{q}}_{j'}}$.

Nun entferne man noch aus der Primärzerlegung $\mathfrak{a}=\bigcap_{j\in[1,\ell]}\tilde{\mathfrak{q}}_j$ schrittweise solche Primärideale, bei deren Entfernung sich die Schnittmenge nicht ändert. Dies setze man fort, bis kein solches Primärideal mehr an der Schnittmenge teilnimmt. So erhalten wir eine reduzierte Primärzerlegung von $\mathfrak{a}$. ▫

Lemma 103 *Sei $N\subseteq S$ eine multiplikative Teilmenge.*

Sei $\mathfrak{q}$ ein Primärideal in S mit $\sqrt{\mathfrak{q}}\cap N=\emptyset$.

Dann ist $\mathfrak{q}/\!\!/N$ ein Primärideal in $S/\!\!/N$ mit $\sqrt{\mathfrak{q}/\!\!/N}=\sqrt{\mathfrak{q}}/\!\!/N$ und mit $\mathfrak{q}=\lambda_{S,N}^{-1}(\mathfrak{q}/\!\!/N)$.

Beweis. Zeigen wir $\sqrt{\mathfrak{q}/\!\!/N} \overset{!}{=} \sqrt{\mathfrak{q}}/\!\!/N$.

Ad $\overset{!}{\supseteq}$. Ist $\frac{s}{n} \in S/\!\!/N$ gegeben mit $s^k \in \mathfrak{q}$ für ein $k \in \mathbf{Z}_{\geqslant 0}$, dann ist $(\frac{s}{n})^k = \frac{s^k}{n^k} \in \mathfrak{q}/\!\!/N$.

Ad $\overset{!}{\subseteq}$. Sei $\frac{s}{n} \in S/\!\!/N$ gegeben mit $(\frac{s}{n})^k \in \mathfrak{q}/\!\!/N$. Dann gibt es ein $x \in N$ mit $xs^k \in \mathfrak{q}$. Da $\mathfrak{q}$ primär ist und $x \in N \subseteq S \smallsetminus \sqrt{\mathfrak{q}}$ liegt, folgt $s^k \in \mathfrak{q}$. Also ist $\frac{s}{n} \in \sqrt{\mathfrak{q}}/\!\!/N$.

Zeigen wir $\mathfrak{q} \overset{!}{=} \lambda_{S,N}^{-1}(\mathfrak{q}/\!\!/N)$. Zu zeigen ist nur $\overset{!}{\supseteq}$. Sei $s \in S$ gegeben mit $\frac{s}{1} \in \mathfrak{q}/\!\!/N$. Dann gibt es ein $x \in N$ mit $xs \in \mathfrak{q}$. Da $x \in N \subseteq S \smallsetminus \sqrt{\mathfrak{q}}$ liegt, muß $s \in \mathfrak{q}$ liegen.

Zeigen wir, daß $\mathfrak{q}/\!\!/N$ ein Primärideal ist. Seien $\frac{s}{n}, \frac{t}{m} \in S/\!\!/N$ gegeben mit $\frac{s}{n} \cdot \frac{t}{m} \in \mathfrak{q}/\!\!/N$, aber $\frac{t}{m} \notin \mathfrak{q}/\!\!/N$. Dann ist $t \notin \mathfrak{q}$. Es gibt ein $x \in N$ mit $xst \in \mathfrak{q}$. Da $x \in N \subseteq S \smallsetminus \sqrt{\mathfrak{q}}$ liegt, muß $st \in \mathfrak{q}$ liegen. Da $t \notin \mathfrak{q}$ liegt, muß es ein $k \in \mathbf{Z}_{\geqslant 0}$ geben mit $s^k \in \mathfrak{q}$. Es folgt $(\frac{s}{n})^k \in \mathfrak{q}/\!\!/N$. $\square$

Bemerkung 104 *Sei $N \subseteq S$ eine multiplikative Teilmenge.*

Seien $\mathfrak{a}, \mathfrak{b} \subseteq S$ Ideale.

Es ist $(\mathfrak{a} \cap \mathfrak{b})/\!\!/N = (\mathfrak{a}/\!\!/N) \cap (\mathfrak{b}/\!\!/N)$.

Beweis. Zu zeigen ist nur $\overset{!}{\supseteq}$. Sei $\frac{s}{n} \in (\mathfrak{a}/\!\!/N) \cap (\mathfrak{b}/\!\!/N)$ gegeben. Zu zeigen ist $\frac{s}{n} \overset{!}{\in} (\mathfrak{a} \cap \mathfrak{b})/\!\!/N$.

Da $\frac{s}{n} \in \mathfrak{a}/\!\!/N$ liegt, gibt es ein $x \in N$ mit $xs \in \mathfrak{a}$. Da $\frac{s}{n} \in \mathfrak{b}/\!\!/N$ liegt, gibt es ein $y \in N$ mit $ys \in \mathfrak{b}$. Also ist $xys \in \mathfrak{a} \cap \mathfrak{b}$ und somit $\frac{s}{n} = \frac{xys}{xyn} \in (\mathfrak{a} \cap \mathfrak{b})/\!\!/N$. $\square$

Cf. auch Aufgabe **??**.(1).

Lemma 105 *Sei $N \subseteq S$ eine multiplikative Teilmenge.*

Sei $\mathfrak{a} \subset S$ ein Ideal. Sei $\mathfrak{a} = \bigcap_{i \in [1,\ell]} \mathfrak{q}_i$ eine reduzierte Primärzerlegung.

Schreibe $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ für $i \in [1,\ell]$. Sei $k \in [1,\ell]$ gegeben mit

$$\mathfrak{p}_i \cap N \left\{ \begin{array}{lll} = & \emptyset & \text{für } i \in [1,k] \\ \neq & \emptyset & \text{für } i \in [k+1,\ell] \,. \end{array} \right.$$

Dann ist $\mathfrak{a}/\!\!/N = \bigcap_{i \in [1,k]} (\mathfrak{q}_i/\!\!/N)$ eine reduzierte Primärzerlegung.

Ferner ist $\lambda_{S,N}^{-1}(\mathfrak{a}/\!\!/N) = \bigcap_{i \in [1,k]} \mathfrak{q}_i$.

Beweis. Für $i \in [k+1,\ell]$ ist $\mathfrak{q}_i/\!\!/N = S/\!\!/N$, da es ein $x \in \mathfrak{p}_i \cap N$ gibt und also ein $j \in \mathbf{Z}_{\geqslant 0}$ mit $x^j \in \mathfrak{q}_i$ existiert, weswegen $\frac{x^j}{1} \in \mathfrak{q}_i/\!\!/N$ von $\frac{1}{x^j} \in S/\!\!/N$ invertiert wird; cf. Bemerkung 30.

Dank Bemerkung 104 folgt also aus $\mathfrak{a} = \bigcap_{i \in [1,\ell]} \mathfrak{q}_i$, daß $\mathfrak{a}/\!\!/N = \bigcap_{i \in [1,k]} (\mathfrak{q}_i/\!\!/N)$ ist. Mittels Lemma 103 erkennen wir, daß eine Primärzerlegung vorliegt und daß $\sqrt{\mathfrak{q}_i/\!\!/N} = \sqrt{\mathfrak{q}_i}/\!\!/N = \mathfrak{p}_i/\!\!/N$ ist. Für $i, j \in [1,k]$ mit $i \neq j$ ist also $\sqrt{\mathfrak{q}_i/\!\!/N} \neq \sqrt{\mathfrak{q}_j/\!\!/N}$; cf. Bemerkung 69.(1).

Um zu zeigen, daß eine reduzierte Primärzerlegung vorliegt, bleibt uns also zu zeigen, daß für $j \in [1,k]$ nicht $\bigcap_{i\in[1,k]\smallsetminus\{j\}} (\mathfrak{q}_i /\!\!/ N) \subseteq \mathfrak{q}_j /\!\!/ N$ liegt.

Es ist $\bigcap_{i\in[1,k]\smallsetminus\{j\}} \mathfrak{q}_i \not\subseteq \mathfrak{q}_j$, da wir von einer reduzierten Primärzerlegung ausgegangen waren. Wähle $x \in \left(\bigcap_{i\in[1,k]\smallsetminus\{j\}} \mathfrak{q}_i\right) \smallsetminus \mathfrak{q}_j$. Dann ist $\frac{x}{1} \in \bigcap_{i\in[1,k]\smallsetminus\{j\}} (\mathfrak{q}_i /\!\!/ N)$. Es genügt zu zeigen, daß $\frac{x}{1} \overset{!}{\not\in} \mathfrak{q}_j /\!\!/ N$ liegt.

Annahme, es ist $\frac{x}{1} \in \mathfrak{q}_j /\!\!/ N$. Dann gibt es ein $y \in N$ mit $xy \in \mathfrak{q}_j$, was wegen $x \not\in \mathfrak{q}_j$ und $\mathfrak{q}_j$ primär aber $y \in \sqrt{\mathfrak{q}_j} = \mathfrak{p}_j$ nach sich zieht, im *Widerspruch* zu $\mathfrak{p}_j \cap N = \emptyset$.

Schließlich folgt

$$\lambda_{S,N}^{-1}(\mathfrak{a} /\!\!/ N) \;=\; \lambda_{S,N}^{-1}\Big(\bigcap_{i\in[1,k]} (\mathfrak{q}_i /\!\!/ N)\Big) \;=\; \bigcap_{i\in[1,k]} \lambda_{S,N}^{-1}(\mathfrak{q}_i /\!\!/ N) \;\overset{\text{L. 103}}{=}\; \bigcap_{i\in[1,k]} \mathfrak{q}_i \,.$$

□

Satz 106 (Vergleich zweier reduzierter Primärzerlegungen) *Sei $\mathfrak{a} \subset S$ ein Ideal. Seien $\mathfrak{a} = \bigcap_{i\in[1,\ell]} \mathfrak{q}_i$ und $\mathfrak{a} = \bigcap_{i\in[1,\tilde\ell]} \tilde{\mathfrak{q}}_i$ reduzierte Primärzerlegungen.*

(1) *Es ist $\ell = \tilde\ell$ und $\{\sqrt{\mathfrak{q}_i} : i \in [1,\ell]\} = \{\sqrt{\tilde{\mathfrak{q}}_i} : i \in [1,\tilde\ell]\}$.*

(2) *Sei $\mathfrak{p} \in \mathrm{Spec}(S)$ ein minimales Element von $\{\sqrt{\mathfrak{q}_i} : i \in [1,\ell]\} = \{\sqrt{\tilde{\mathfrak{q}}_i} : i \in [1,\tilde\ell]\}$; cf.* (1). *Sei dabei $\mathfrak{p} = \sqrt{\mathfrak{q}_j} = \sqrt{\tilde{\mathfrak{q}}_{\tilde\jmath}}$ mit $j \in [1,\ell]$ und $\tilde\jmath \in [1,\tilde\ell]$.*

Dann ist $\mathfrak{q}_j = \tilde{\mathfrak{q}}_{\tilde\jmath}$.

Beweis.

Ad (1). Es genügt, $\mathrm{Ass}(S,\mathfrak{a}) \overset{!}{=} \{\sqrt{\mathfrak{q}_i} : i \in [1,\ell]\}$ zu zeigen.

Da $\mathfrak{a} = \bigcap_{i\in[1,\ell]} \mathfrak{q}_i$ ist, folgt

$$\mathrm{Ass}(S,\mathfrak{a}) \subseteq \bigcup_{i\in[1,\ell]} \mathrm{Ass}(S,\mathfrak{q}_i) \;=\; \{\sqrt{\mathfrak{q}_i} : i \in [1,\ell]\}\,;$$

cf. Aufgabe **??**, Lemma 99.

Sei $j \in [1,\ell]$ gegeben. Wir haben $\sqrt{\mathfrak{q}_j} \overset{!}{\in} \mathrm{Ass}(A,\mathfrak{a})$ zu zeigen. Da $\mathfrak{a} = \bigcap_{i\in[1,\ell]} \mathfrak{q}_i$ eine reduzierte Primärzerlegung ist, gibt es ein $x \in \bigcap_{i\in[1,\ell]\smallsetminus\{j\}} \mathfrak{q}_i$ mit $x \not\in \mathfrak{a}$, i.e. mit $x \not\in \mathfrak{q}_j$.

Sei $\mathfrak{b} := (\mathfrak{a} : (x))$. Es ist $\mathfrak{b} \subset S$. Also ist $\mathrm{Ass}(S,\mathfrak{b}) \neq \emptyset$; cf. Bemerkung 97. Wähle $\mathfrak{p} \in \mathrm{Ass}(S,\mathfrak{b})$. Es gibt also ein $y \in S \smallsetminus \mathfrak{b}$ mit $\mathfrak{p} = (\mathfrak{b} : (y))$. Nun ist

$$\mathfrak{p} \;=\; (\mathfrak{b} : (y)) \;=\; ((\mathfrak{a} : (x)) : (y)) \;=\; (\mathfrak{a} : (xy))\,,$$

insbesondere $xy \not\in \mathfrak{a}$ und also $\mathfrak{p} \in \mathrm{Ass}(S,\mathfrak{a})$.

Da $xy \in \bigcap_{i\in[1,\ell]\smallsetminus\{j\}} \mathfrak{q}_i$ liegt, folgt

$$\mathfrak{p} \;=\; (\mathfrak{a} : (xy)) \;=\; (\mathfrak{q}_j : (xy))$$

und also $\mathfrak{p} \in \operatorname{Ass}(S, \mathfrak{q}_j) = \{\mathfrak{q}_j\}$, i.e. $\mathfrak{p} = \sqrt{\mathfrak{q}_j}$; cf. Lemma 99.

Insgesamt ist $\sqrt{\mathfrak{q}_j} = \mathfrak{p} \in \operatorname{Ass}(S, \mathfrak{a})$.

Ad (2). Sei $N := S \smallsetminus \mathfrak{p}$. Es genügt, $\mathfrak{q}_j \overset{!}{=} \lambda^{-1}_{S,S\smallsetminus\mathfrak{p}}(\mathfrak{a}/\!\!/N)$ zu zeigen.

Sei $i \in [1,\ell]\smallsetminus\{j\}$. Da $\mathfrak{a} = \bigcap_{i\in[1,\ell]} \mathfrak{q}_i$ eine reduzierte Primärzerlegung ist, gibt es wegen der vorausgesetzten Minimalität von $\mathfrak{p} = \sqrt{\mathfrak{q}_j}$ ein $x \in \sqrt{\mathfrak{q}_i}$, das nicht in $\mathfrak{p}$ liegt. Mit anderen Worten, es ist $N \cap \sqrt{\mathfrak{q}_i} \neq \emptyset$.

Ferner ist $N \cap \sqrt{\mathfrak{q}_j} = \emptyset$.

Die Aussage folgt also mit Lemma 105 nach Umnumerierung. ▫

1.3.2 Mehr zur Komplettierung: Hensels Faktorisierungslemma

Sei R ein kommutativer Ring.

Sei S eine komplette diskrete Bewertungsalgebra mit maximalem Ideal (p).

Sei X ein Element.

> Wir wollen Hensels Lemma zum Faktorisieren von Polynomen behandeln; cf. Satz 110.
>
> Hensels Lemma zum Heben von Nullstellen kennen wir aus Aufgabe **??**.(5).

Bemerkung 107 *Seien $U = (U,\xi)$ und $V = (V,\eta)$ kommutative R-Algebren.*

Sei $f\colon U \to V$ ein Morphismus von R-Algebren.

Dann haben wir den R-Algebrenmorphismus

$$\begin{array}{rcl} U[X] & \xrightarrow{\tilde f} & V[X] \\ \sum_{i\geqslant 0} u_i X^i & \mapsto & \sum_{i\geqslant 0} f(u_i) X^i \end{array}$$

Beweis. Es sind auch $U = (U, \mathrm{id}_U)$ und $V = (V, f)$ U-Algebren. Wegen $f\circ\mathrm{id}_U = f$ ist f ein U-Algebrenmorphismus. Ferner ist $\alpha_{V,X} : V \to V[X]\colon v \mapsto v$ ein V-Algebrenmorphismus, mittels Einschränkung entlang f also auch ein U-Algebrenmorphismus. Zusammen haben wir den U-Algebrenmorphismus $\alpha_{V,X} \circ f\colon U \to V[X]\colon u \mapsto f(u)$, was zugleich der Strukturmorphismus von $V[X]$ ist.

Dank universeller Eigenschaft der Polynomalgebra gibt es also zur Abbildung $X \mapsto X$ genau einen U-Algebrenmorphismus von $U[X]$ nach $V[X]$, der X nach X abbildet, nämlich

$$\begin{array}{rcl} U[X] & \xrightarrow{\tilde f} & V[X] \\ \sum_{i\geqslant 0} u_i X^i & \mapsto & \sum_{i\geqslant 0} f(u_i) X^i \end{array}$$

cf. Lemma 20. Nach Einschränken entlang ξ wird $\tilde{f}$ auch zu einem R-Algebrenmorphismus, denn aus $\tilde{f} \circ \alpha_{U,X} = \alpha_{V,X} \circ f$ folgt $\tilde{f} \circ \alpha_{U,X} \circ \xi = \alpha_{V,X} \circ f \circ \xi = \alpha_{V,X} \circ \eta$. ▫

Definition 108 Ein Polynom $f(X) = \sum_{i \geqslant 0} a_i X^i \in S[X]^\times$ heißt *normiert*, falls für $j := \max\{\, i \in \mathbf{Z}_{\geqslant 0} : \; a_i \neq 0 \,\}$ dann $a_j = 1$ ist.

Bemerkung 109 *Gegeben sei $f(X) \in S[X]$ normiert.*

Gegeben seien $g_n(X)$, $h_n(X) \in S[X]$ normiert für $n \in \mathbf{Z}_{\geqslant 1}$.

Für $n \in \mathbf{Z}_{\geqslant 1}$ sei

$$\begin{array}{rcl} f(X) & \equiv_{p^n} & g_n(X) \cdot h_n(X) \\ g_{n+1}(X) & \equiv_{p^n} & g_n(X) \\ h_{n+1}(X) & \equiv_{p^n} & h_n(X) \end{array}$$

Insbesondere sind $\deg(g_n(X))$ und $\deg(h_n(X))$ konstant in n.

Wir schreiben $f_n(X) =: \sum_{i \geqslant 0} u_{n,i} X^i$ und $g_n(X) =: \sum_{i \geqslant 0} v_{n,i} X^i$ für $n \in \mathbf{Z}_{\geqslant 1}$.

Sei $i \in \mathbf{Z}_{\geqslant 1}$ gegeben. Es ist $u_{n+1,i} \equiv_{p^n} u_{n,i}$ und $v_{n+1,i} \equiv_{p^n} v_{n,i}$ für $n \in \mathbf{Z}_{\geqslant 1}$. Insbesondere sind $(u_{n,i})_n$ und $(v_{n,i})_n$ Cauchyfolgen; cf. Aufgabe **??**. *Sei u_i der Grenzwert von $(u_{n,i})_n$ und sei v_i der Grenzwert von $v_{n,i}$; cf. Aufgabe* **??**.(1). *Seien*

$$\begin{array}{rcl} g(X) & := & \sum_{i \geqslant 0} u_i X^i \\ h(X) & := & \sum_{i \geqslant 0} v_i X^i \end{array}$$

Es sind $g(X)$ und $h(X)$ normiert.

Es ist

$$f(X) \;=\; g(X) \cdot h(X)\,.$$

Ferner ist

$$\begin{array}{rcl} g(X) & \equiv_p & g_1(X) \\ h(X) & \equiv_p & h_1(X)\,. \end{array}$$

Beweis. Sei $(s_n)_n$ eine Folge in S mit $s_{n+1} \equiv_{p^n} s_n$ für $n \in \mathbf{Z}_{\geqslant 1}$. Es ist $(s_n)_n$ eine Cauchyfolge. Sei s ihr Grenzwert; cf. Aufgabe **??**.(1). Dann gibt es für ein gegebenes $m \in \mathbf{Z}_{\geqslant 1}$ ein $\tilde{m} \in \mathbf{Z}_{\geqslant m}$ mit $s \equiv_{p^m} s_{\tilde{m}}$. Daher ist $s \equiv_{p^m} s_{\tilde{n}} \equiv_{p^m} s_m$.

Es folgt

$$\begin{array}{rcl} g(X) & \equiv_{p^m} & g_m(X) \\ h(X) & \equiv_{p^m} & h_m(X) \end{array}$$

für $m \in \mathbf{Z}_{\geqslant 1}$.

Sei $n \in \mathbf{Z}_{\geqslant 1}$ gegeben. Wir betrachten den R-Algebrenmorphismus

$$\begin{array}{ccl} S & \xrightarrow{\rho_n} & S/(p^n) \\ s & \mapsto & s + (p^n) \;=:\; \bar{s}\,. \end{array}$$

Dieser induziert den R-Algebrenmorphismus

$$\begin{array}{rcl} S[X] & \xrightarrow{\tilde{\rho}_n} & (S/(p^n))[X] \\ \sum_{i\geqslant 0} a_i X^i & \mapsto & \sum_{i\geqslant 0} \bar{a}_i X^i \; ; \end{array}$$

cf. Bemerkung 107. Es folgt

$$\begin{array}{rcl} \tilde{\rho}_n\Big(f(X)\Big) \;=\; \tilde{\rho}_n\Big(g_n(X)\cdot h_n(X)\Big) & = & \tilde{\rho}_n\Big(g_n(X)\Big)\cdot\tilde{\rho}_n\Big(h_n(X)\Big) \\ & = & \tilde{\rho}_n\Big(g(X)\Big)\cdot\tilde{\rho}_n\Big(h(X)\Big) \;=\; \tilde{\rho}_n\Big(g(X)\cdot h(X)\Big)\;. \end{array}$$

Da dies für alle $n \in \mathbf{Z}_{\geqslant 1}$ gilt, folgt $f(X) = g(X)\cdot h(X)$. ▫

Satz 110 (Hensels Faktorisierungslemma) *Wir erinnern an die komplette diskrete Bewertungsalgebra S über R mit maximalem Ideal (p).*

Wir schreiben $\bar{S} := S/(p)$ und $\bar{s} := s + (p)$ für $s \in S$. Wir haben den R-Algebrenmorphismus

$$\begin{array}{rcl} S[X] & \xrightarrow{\tilde{\rho}_1} & \bar{S}[X] \\ f(X) \;=\; \sum_{i\geqslant 0} a_i X^i & \mapsto & \sum_{i\geqslant 0} \bar{a}_i X^i \;=:\; \bar{f}(X)\;; \end{array}$$

cf. Bemerkung 107.

Sei $f(X) \in S[X]$ normiert.

Seien $g_1(X)$, $h_1(X) \in S[X]$ normiert gegeben mit $\big(\bar{g}_1(X), \bar{h}_1(X)\big) = (1)$ und mit

$$\bar{f}(X) \;=\; \bar{g}_1(X)\cdot\bar{h}_1(X)\;.$$

Dann gibt es $g(X)$, $h(X) \in S[X]$ normiert mit $\bar{g}(X) = \bar{g}_1(X)$, mit $\bar{h}(X) = \bar{h}_1(X)$ und mit

$$f(X) \;=\; g(X)\cdot h(X)\;.$$

Beweis. Wir schreiben $a := \deg(g_1)$ und $b := \deg(h_1)$. Dann ist $\deg(f) = a + b$.

Sei ferner für das Nullpolynom vereinbart, daß $\deg(0) := -\infty$ gelte, sodaß jedenfalls $\deg(0) < k$ ist für $k \in \mathbf{Z}_{\geqslant 0}$.

Für $n \in \mathbf{Z}_{\geqslant 1}$ konstruieren wir rekursiv $g_n(X)$, $h_n(X) \in S[X]$ normiert mit

$$\begin{array}{rcl} g_{n+1}(X) & \equiv_{p^n} & g_n(X) \\ h_{n+1}(X) & \equiv_{p^n} & h_n(X) \\ f(X) & \equiv_{p^n} & g_n(X)\cdot h_n(X)\;. \end{array}$$

Die Aussage folgt dann hieraus mittels Bemerkung 109.

Um die Konstruktion durchzuführen seien $n \geqslant 1$ und $g_n(X)$, $h_n(X) \in S[X]$ normiert mit $f(X) \equiv_{p^n} g_n(X)\cdot h_n(X)$, mit $\deg(g_n) = a$ und mit $\deg(h_n) = b$ gegeben.

Beim Rekursionsanfang $n = 1$ trifft dies nach Voraussetzung zu.

Gesucht sind $g_{n+1}(X)$, $h_{n+1}(X) \in S[X]$ normiert mit $f(X) \equiv_{p^n} g_n(X) \cdot h_n(X)$ und mit

$$\begin{array}{rcl} g_{n+1}(X) & \equiv_{p^n} & g_n(X) \\ h_{n+1}(X) & \equiv_{p^n} & h_n(X) \\ f(X) & \equiv_{p^{n+1}} & g_{n+1}(X) \cdot h_{n+1}(X) \;. \end{array}$$

Wir suchen demgemäß $u(X)$, $v(X) \in S[X]$ mit $\deg(u) < a$, mit $\deg(v) < b$, und mit

$$f(X) \stackrel{!}{\equiv}_{p^{n+1}} (g_n(X) + p^n u(X))(h_n(X) + p^n v(X)) \;.$$

Denn dann können wir $g_{n+1}(X) := g_n(X) + p^n u(X)$ und $h_{n+1}(X) := h_n(X) + p^n v(X)$ setzen.

Schreibe $f(X) - g_n(X) \cdot h_n(X) =: p^n w(X)$ mit $w(X) \in S[X]$, was nach Rekursionsvoraussetzung möglich ist. Da $f(X)$ und $g_n(X)h_n(X)$ normierte Polynome vom gleichen Grad $a + b$ sind, ist $\deg(w) < \deg(f) = a + b$.

Wir haben

$$p^n w(X) \stackrel{!}{\equiv}_{p^{n+1}} p^n u(X) \cdot h_n(X) + g_n(X) \cdot p^n v(X)$$

zu erfüllen, i.e.

$$w(X) \stackrel{!}{\equiv}_p u(X) \cdot h_n(X) + g_n(X) \cdot v(X) \equiv_p u(X) \cdot h_1(X) + v(X) \cdot g_1(X) \;.$$

Da $\big(\bar{g}_1(X), \bar{h}_1(X)\big) = (1)$, gibt es $\tilde{u}(X)$, $\tilde{v}(X) \in S[X]$ mit

$$w(X) \equiv_p \tilde{u}(X) \cdot h_1(X) + \tilde{v}(X) \cdot g_1(X) \;.$$

Polynomdivision mit Rest gibt $\tilde{v}(X) = h_1(X) \cdot t(X) + v(X)$ mit $t(X)$, $v(X) \in S[X]$, wobei $\deg(t) < \deg(h_1) = b$ ist.

Sei noch $u(X)$ das Polynom, das aus dem Polynom $\tilde{u}(X) + t(X) \cdot g_1(X)$ durch Subtraktion all seiner durch p teilbarer Monome hervorgeht. Dann ist $\deg(u) = \deg(\bar{u})$. Es wird

$$w(X) \equiv_p (\tilde{u}(X) + t(X) \cdot g_1(X)) \cdot h_1(X) + v(X) \cdot g_1(X) \equiv_p u(X) \cdot h_1(X) + v(X) \cdot g_1(X) \;,$$

da $\tilde{\rho}_1$ mit Multiplikation verträglich ist. Mit anderen Worten, es ist

$$\bar{w}(X) = \bar{u}(X) \cdot \bar{h}_1(X) + \bar{v}(X) \cdot \bar{g}_1(X) \;.$$

Hierin ist $\deg(\bar{v}(X) \cdot \bar{g}_1(X)) \leqslant \deg(v(X) \cdot g_1(X)) < b + a$. Ebenso ist $\deg(\bar{w}) \leqslant \deg(w) < a+b$. Da nun $\deg(\bar{h}_1) = b$ ist, kann nicht $\deg(\bar{u}) \geqslant a$ sein. Folglich ist $\deg(u) = \deg(\bar{u}) < a$, wie verlangt. $\square$

Beispiel 111 Wir haben die komplette diskrete Bewertungsalgebra $\widehat{\mathbf{Z}_{(5)}}$; cf. Bemerkung 74, Lemma 91.(5).

Wir betrachten $X^2 + 1 \in \widehat{\mathbf{Z}_{(5)}}[X]$.

Wir haben die Isomorphismen $\mathbf{F}_5 = \mathbf{Z}/(5) \xrightarrow{\sim} \mathbf{Z}_{(5)}/(5) \xrightarrow{\sim} \widehat{\mathbf{Z}_{(5)}}/(5)$, entlang denen wir identifizieren; cf. Aufgabe **??**.(3), Lemma 91.(4).

Es ist $X^2 + 1 \equiv_5 (X - 2)(X + 2)$, und diese Faktoren $X - 2$ und $X + 2$ sind teilerfremd in $\mathbf{F}_5[X]$, i.e. $(X + 2, X - 2) = (1)$ in $\mathbf{F}_5[X]$.

Dank Satz 110 gibt es eine Zerlegung der Form $X^2 + 1 = (X - w_1)(X - w_2)$ in $\widehat{\mathbf{Z}_{(5)}}[X]$ mit $X - w_1 \equiv_5 X - 2$ und mit $X - w_2 \equiv_5 X + 2$, i.e. mit $w_1 \equiv_5 2$ und mit $w_2 \equiv_5 -2$.

Tatsächlich muß $w_2 = -w_1$ sein, wie der Koeffizientenvergleich bei X^1 liefert.

Cf. Aufgabe **??**.(6). Das dortige Element s muß das hiesige Element w_1 sein, da w_1 und w_2 die einzigen Nullstellen von $X^2 + 1$ bleiben und da $s \equiv_5 2$ ist.

Dahingegen ist $X^2 + 1$ in $\mathbf{Z}_{(5)}[X]$ irreduzibel, da wir $\mathbf{Z}_{(5)}$ als Teilalgebra von $\mathbf{Q}$ ansehen dürfen und $X^2 + 1$ in $\mathbf{Q}[X]$ irreduzibel ist.

Kapitel 2

In Richtung Geometrie

2.1 Moduln

Sei R ein kommutativer Ring.

Definition 112

(1) Ein R-*Modul* besteht aus einer abelschen Gruppe $(M,+)$ und einer Abbildung

$$\begin{array}{ccccc} R & \times & M & \xrightarrow{(\cdot)} & M \\ (r & , & m) & \mapsto & r\cdot m \ =: \ rm \end{array}$$

derart, daß die folgenden Eigenschaften (Mod 1–3) gelten.

(Mod 1) Es ist $1\cdot m = m$ für $m \in M$.

(Mod 2) Es ist $r\cdot(r'\cdot m) = (r\cdot r')\cdot m$ für $r,\, r' \in R$ und $m \in M$.

(Mod 3) Es ist $(r+r')\cdot(m+m') = r\cdot m + r'\cdot m + r\cdot m' + r'\cdot m'$ für $r,\, r' \in R$ und $m,\, m' \in M$.

Oft schreiben wir kurz $M = (M,+,\cdot)$.

Es ist $0\cdot m = 0\cdot m + 0\cdot m - 0\cdot m = (0+0)\cdot m - 0\cdot m = 0\cdot m - 0\cdot m = 0$ für $m \in M$.

Es ist $(-1)\cdot m = (-1)\cdot m + 1\cdot m - m = (-1+1)\cdot m - m = -m$ für $m \in M$.

(2) Seien R-Moduln M und N gegeben. Eine Abbildung $f : M \to N$ heißt R-linear, falls

$$f(r\cdot m + r'\cdot m') \ = \ r\cdot f(m) + r'\cdot f(m')$$

ist für $r,\, r' \in R$ und $m,\, m' \in M$.

Insbesondere ist f ein Morphismus abelscher Gruppen.

Ist f eine bijektive R-lineare Abbildung, dann auch f^- eine R-lineare Abbildung, denn $f^-(rn + r'n') = f^-(rf(f^-(n)) + r'f(f^-(n'))) = f^-(f(rf^-(n) + r'f^-(n'))) = rf^-(n) + r'f^-(n')$ für $r,\ r' \in R$ und $n,\ n' \in N$. Diesenfalls heißt f ein *Isomorphismus* von R-Moduln.

Beispiel 113

(1) Ist R ein Körper, so nennt man einen R-Modul auch einen R-Vektorraum.

(2) Es ist R vermöge der aus der kommutativen Ringstruktur stammenden Multiplikation

$$\begin{array}{ccccc} R & \times & R & \xrightarrow{(\cdot)} & R \\ (r & , & r') & \mapsto & rr' \end{array}$$

ein R-Modul.

(3) Sei $S = (S, \alpha)$ eine kommutative R-Algebra. Sei M ein S-Modul vermöge $(\cdot)\colon S \times M \to M$. Dann wird die abelsche Gruppe $(M, +)$ zu einem R-Modul vermöge

$$\begin{array}{ccccc} R & \times & M & \xrightarrow{(\cdot)} & M \\ (r & , & m) & \mapsto & r \cdot m \ := \ \alpha(r)m \end{array}$$

Wir sagen, der R-Modul M entsteht aus dem S-Modul M durch *Einschränken entlang* α.

Es gilt (Mod 1), da $1 \cdot m = \alpha(1)m = 1\,m = m$ ist für $m \in M$.

Es gilt (Mod 2), da

$$\begin{array}{rcl} r \cdot (r' \cdot m) & = & \alpha(r)(\alpha(r')m) \\ & = & (\alpha(r)\alpha(r'))m \\ & = & \alpha(rr')m \\ & = & (r \cdot r') \cdot m \end{array}$$

ist für $r,\ r' \in R$ und $m \in M$.

Es gilt (Mod 3), da

$$\begin{array}{rcl} (r + r') \cdot (m + m') & = & \alpha(r + r')(m + m') \\ & = & (\alpha(r) + \alpha(r'))(m + m') \\ & = & \alpha(r)m + \alpha(r')m + \alpha(r)m' + \alpha(r')m' \\ & = & r \cdot m + r' \cdot m + r \cdot m' + r' \cdot m' \end{array}$$

für $r,\ r' \in R$ und $m,\ m' \in M$.

(4) Sei $S = (S, \alpha)$ eine R-Algebra. Wir haben den S-Modul S aus (2). Schränken wir diesen gemäß (3) entlang α ein, so erhalten wir den R-Modul S via

$$\begin{array}{ccccc} R & \times & S & \xrightarrow{(\cdot)} & S \\ (r & , & s) & \mapsto & r \cdot s \ := \ \alpha(r)s\ . \end{array}$$

Definition 114 Sei M ein R-Modul.

(1) Eine Teilmenge $U \subseteq M$ heißt *R-Teilmodul* oder kurz *Teilmodul*, falls $0 \in U$ und falls für $r,\, r' \in R$ und $u,\, u' \in U$ auch $ru + r'u' \in U$ liegt.

Insbesondere ist ein Teilmodul eine abelsche Untergruppe.

Ist $U \subseteq M$ ein Teilmodul, so ist U mittels $(\cdot)|_{R\times U}^{U}$ ein R-Modul.

Diesenfalls ist die Einbettungsabbildung $U \to M : u \mapsto u$ eine R-lineare Abbildung.

(2) Sei $X \subseteq M$ eine Teilmenge. Es ist

$$ {}_R\langle X\rangle \;:=\; \Big\{ \sum_{x\in X} r_x x : \text{ es ist } r_x \in R \text{ für } x \in X \text{ mit } \{\, x \in X : \, r_x \neq 0 \,\} \text{ endlich} \Big\} \;\subseteq\; M $$

ein Teilmodul, genannt das *R-lineare Erzeugnis* von X in M.

Es ist $X \subseteq {}_R\langle X\rangle$.

Für einen Teilmodul $U \subseteq M$ ist genau dann $X \subseteq U$, wenn ${}_R\langle X\rangle \subseteq U$ ist.

Ist $X = \{\, m_i : \, i \in [1,k] \,\}$ für ein $k \in \mathbf{Z}_{\geqslant 0}$ und gewisse $m_i \in M$ für $i \in [1,k]$, so schreiben wir auch ${}_R\langle X\rangle =: {}_R\langle m_i : i \in [1,k]\rangle = {}_R\langle m_1, \ldots, m_k\rangle$.

(3) Seien U und V Teilmoduln von M. Dann sind auch $U \cap V$ und $U + V := \{\, u + v : \, u \in U,\; v \in V \,\}$ Teilmoduln von M.

(4) Sei $U \subseteq M$ ein Teilmodul. Wir können die abelsche Faktorgruppe

$$ M/U \;=\; \{\, m + U : \, m \in M \,\} $$

mittels $r \cdot (m + U) := (r \cdot m) + U$ für $r \in R$ und $m \in M$ zu einem R-Modul machen, dem *Faktormodul* von M modulo U.

Wir haben die R-lineare *Restklassenabbildung* $M \to M/U : m \mapsto m + U$.

Cf. Aufgabe **??**.(1).

(5) Eine Sequenz von R-Moduln und R-linearen Abbildungen

$$ M' \xrightarrow{i} M \xrightarrow{f} M'' $$

heißt *kurz exakt*, wenn i injektiv, f surjektiv und $i(M) = \mathrm{Kern}(f)$ ist.

Beispiel 115 Sei S eine kommutative R-Algebra.

(1) Eine Teilmenge $X \subseteq S$ ist genau dann ein Ideal, wenn sie ein S-Teilmodul ist.

(2) Sei $\mathfrak{a} \subseteq S$ ein Ideal. Sei M ein S-Modul. Es ist

$$\mathfrak{a}M \ := \ \Big\{ \sum_{i\in[1,k]} a_i m_i : \ k \in \mathbf{Z}_{\geqslant 0}\,,\ a_i \in \mathfrak{a} \text{ und } m_i \in M \text{ für } i \in [1,k] \Big\}$$

ein Teilmodul von M.

Beispiel 116

(1) Seien R-Moduln M und N gegeben. Sei $f\colon M \to N$ eine R-lineare Abbildung.

Sei $N' \subseteq N$ ein Teilmodul. Dann ist $f^{-1}(N') \subseteq M$ ein Teilmodul. Denn es ist $0 \in f^{-1}(N')$. Ferner ist für $r, \tilde{r} \in R$ und $m, \tilde{m} \in f^{-1}(N')$ auch $f(rm + r'm') = rf(m) + \tilde{r}f(\tilde{m}) \in N'$ und also $rm + r'm \in f^{-1}(N')$.

Insbesondere ist $\operatorname{Kern}(f) := f^{-1}(0) \subseteq M$ ein Teilmodul.

Sei $M' \subseteq M$ ein R-Teilmodul. Dann ist $f(M') \subseteq M$ ein Teilmodul. Denn es ist $0 \in f(M')$. Ferner liegt für $r, \tilde{r} \in R$ und $m', \tilde{m}' \in M'$ auch $rf(m') + \tilde{r}f(\tilde{m}') = f(rm' + \tilde{r}\tilde{m}') \in f(M')$.

Insbesondere ist $f(M)$ ein Teilmodul von N.

(2) Sei M ein R-Modul. Sei $M' \subseteq M$ ein Teilmodul. Wir haben die R-lineare Inklusionsabbildung $M' \xrightarrow{i} M\colon m' \mapsto m'$ und die R-lineare Restklassenabbildung $M \xrightarrow{r} M/M'\colon m \mapsto m + M'$. Dann ist die Sequenz

$$M' \xrightarrow{i} M \xrightarrow{r} M/M'$$

kurz exakt.

Definition 117 Sei I eine Menge. Sei M_i ein R-Modul für $i \in I$.

(1) Wir betrachten

$$\prod_{i\in I} M_i \ = \ \{\, (m_i)_i : \ m_i \in M_i \text{ für } i \in I \,\}\,.$$

Es ist $\prod_{i\in I} M_i$ eine abelsche Gruppe vermöge $(m_i)_i + (m'_i)_i := (m_i + m'_i)_i$ für $(m_i)_i\,,\ (m'_i)_i \in \prod_{i\in I} M_i$. Es ist $\prod_{i\in I} M_i$ ein R-Modul vermöge $r \cdot (m_i)_i := (rm_i)_i$ für $r \in R$ und $(m_i)_i \in \prod_{i\in I} M_i$.

(2) Wir haben den Teilmodul

$$\bigoplus_{i\in I} M_i \ = \ \{\, (m_i)_i \in \prod_{i\in I} M_i : \ \{\, i \in I : \ m_i \neq 0 \,\} \text{ ist endlich} \,\} \ \subseteq \ \prod_{i\in I} M_i\,.$$

Denn für $r, r' \in R$ und $(m_i)_i\,,\ (m'_i)_i \in \bigoplus_{i\in I} M_i$ ist

$$\{\, i \in I : \ rm_i + r'm'_i \neq 0 \,\} \ \subseteq \ \{\, i \in I : \ m_i \neq 0 \,\} \cup \{\, i \in I : \ m'_i \neq 0 \,\}$$

und letztere Menge ist endlich; mithin ist $r(m_i)_i + r'(m'_i)_i \in \bigoplus_{i\in I} M_i$.

(3) Sei X eine Menge. Wir schreiben $RX := \bigoplus_{x \in X} R$.

Wir schreiben auch $y := (\partial_{y,x})_x$ für $y \in X$.

Dann ist jedes Element von RX eindeutig schreibbar in der Form $\sum_{x \in X} r_x x = (r_x)_x$ mit $r_x \in R$ für $\in X$ und mit $\{ x \in X : r_x \neq 0 \}$ endlich.

(4) Ist $k \in \mathbf{Z}_{\geqslant 1}$ und $I = [1, k]$, dann schreiben wir auch $M_1 \oplus \ldots \oplus M_k := \bigoplus_{i \in [1,k]} M_i$.

Beispiel 118 Sei $k \in \mathbf{Z}_{\geqslant 0}$. Wir schreiben $R^{\oplus k} := \bigoplus_{i \in [1,k]} R = R[1, k]$.

Insbesondere ist $R^{\oplus 0} = \{(\ )\}$, und darin ist $(\ ) = 0$. Also ist $R^{\oplus 0} = 0$.

Sei M ein R-Modul. Seien $x_i \in M$ Elemente in M für $i \in [1, k]$. Wir schreiben $x := (x_i)_{i \in [1,k]}$ und erhalten die R-lineare Abbildung

$$\begin{array}{ccc} R^{\oplus k} & \xrightarrow{f_x} & M \\ (r_i)_i & \mapsto & \sum_{i \in [1,k]} r_i x_i \end{array}$$

Für jede R-lineare Abbildung g von $R^{\oplus k}$ nach M gibt es genau ein Tupel $x = (x_i)_{i \in [1,k]}$ von Elementen von M mit $g = f_x$, bestehend namentlich aus $x_j := g((\partial_{j,i})_i)$ für $j \in [1, k]$.

Die Eindeutigkeit folgt aus $f_x((\partial_{j,i})_i) = \sum_{i \in [1,k]} \partial_{j,i} x_i = x_j$ für $j \in [1, k]$, da so f_x das x festlegt.

Die Existenz folgt aus $g((r_i)_i) = g(\sum_{j \in [1,k]} r_j (\partial_{j,i})_i) = \sum_{j \in [1,k]} r_j g(\partial_{j,i})_i \ = \ \sum_{i \in [1,k]} r_i x_i = f_x((r_i)_i)$ für $(r_i)_i \in R^{\oplus k}$.

Definition 119 Sei M ein R-Modul. Sei S eine kommutative R-Algebra.

Sei $k \in \mathbf{Z}_{\geqslant 0}$ und seien $s_i \in S$ für $i \in [1, k]$. Wir erinnern daran, daß $R[s_1, \ldots, s_k]$ das Bild ist der R-Algebrenmorphismus von $R[X_1, \ldots, X_k]$ nach S, der X_i auf x_i abbildet für $i \in [1, k]$; cf. Lemma 20.

(1) Es heißt M *endlich erzeugt*, wenn es ein $k \in \mathbf{Z}_{\geqslant 0}$ und eine surjektive R-lineare Abbildung von $R^{\oplus k}$ nach M gibt.

(2) Es heißt M *endlich erzeugt frei*, wenn es ein $k \in \mathbf{Z}_{\geqslant 0}$ und eine bijektive R-lineare Abbildung von $R^{\oplus k}$ nach M gibt.

(3) Es heißt S *endlich über* R, wenn S als R-Modul endlich erzeugt ist.

(4) Es heißt S *endlich erzeugt als* R*-Algebra*, wenn es ein $k \in \mathbf{Z}_{\geqslant 0}$ und Elemente $x_i \in S$ für $i \in [1, k]$ gibt mit $S = R[x_1, \ldots, x_k]$.

(5) Es heißt $x \in S$ *ganz über* R, wenn $R[x]$ endlich ist über R.

Es heißt S *ganz über* R, wenn s ganz ist über R für $s \in S$.

(6) Es heißt $x \in S$ *algebraisch über* R, wenn es ein $r \in R^\times$ gibt mit $r \cdot x = \alpha(r)x$ ganz über R.

Es heißt S *algebraisch über* R, wenn s algebraisch ist über R für $s \in S$.

Vorsicht, wenn S endlich ist über R, dann ist i.a. nicht S als Menge endlich. So etwa ist $\mathbf{Z}$ endlich über $\mathbf{Z}$.

Bemerkung 120 Sei S eine kommutative R-Algebra.

Ist S endlich über R, dann ist S auch endlich erzeugt als R-Algebra.

Denn für $k \in \mathbf{Z}_{\geqslant 0}$ und Elemente $x_i \in S$ für $i \in [1, k]$ ist ${}_R\langle x_1, \ldots, x_k \rangle \subseteq R[x_1, \ldots, x_k]$, da $R[x_1, \ldots, x_k]$ ein R-Teilmodul von S ist, der x_i enthält für $i \in [1, k]$.

Ist also ${}_R\langle x_1, \ldots, x_k \rangle = S$, dann ist auch $R[x_1, \ldots, x_k] = S$.

2.2 Tensorprodukte

Sei R ein kommutativer Ring.

Definition 121 Seien R-Moduln M und N gegeben.

Sei

$$\begin{array}{rcl} X & := & \{ (rm + r'm', n) - r(m, n) - r'(m', n) : \ r,\, r' \in R,\ m,\, m' \in M,\ n \in N \} \\ & \cup & \{ (m, rn + r'n') - r(m, n) - r'(m, n') : \ r,\, r' \in R,\ m \in M,\ n,\, n' \in N \} \\ & \subseteq & R(M \times N)\ . \end{array}$$

Sei

$$M \underset{R}{\otimes} N \ := \ R(M \times N) / {}_R\langle X \rangle$$

das *Tensorprodukt* von M und N über R. Dies ist ein R-Modul nach Konstruktion.

Für $m \in M$ und $n \in N$ schreiben wir den *Elementartensor*

$$m \otimes n \ := \ (m, n) + {}_R\langle X \rangle\ .$$

Es ist $(rm + r'm') \otimes n = r(m \otimes n) + r'(m' \otimes n)$ für $r,\, r' \in R$, $m,\, m' \in M$, $n \in N$.

Es ist $m \otimes (rn + r'n') = r(m \otimes n) + r'(m \otimes n')$ für $r,\, r' \in R$, $m \in M$, $n,\, n' \in N$.

Jedes Element von $M \underset{R}{\otimes} N$ ist von der Form

$$\sum_{(m,n) \in W} m \otimes n$$

für eine endliche Teilmenge $W \subseteq M \times N$; cf. Aufgabe **??**.(1).

Lemma 122 (Universelle Eigenschaft des Tensorprodukts von Moduln)

Seien R-Moduln M und N gegeben.

Wir haben die Abbildung $\tau := \tau_{M,N} \colon M \times N \to M \underset{R}{\otimes} N \colon (m,n) \mapsto m \otimes n$. Diese erfüllt

$$\begin{array}{rcl} \tau(rm + r'm', n) & = & r\tau(m,n) + r'\tau(m',n) \\ \tau(m, rn + r'n') & = & r\tau(m,n) + r'\tau(m,n') \end{array}$$

für $r, r' \in R$, $m, m' \in M$, $n, n' \in N$; cf. Definition 121.

Sei T ein R-Modul. Sei $t \colon M \times N \to T$ eine Abbildung mit

$$\begin{array}{rcl} t(rm + r'm', n) & = & rt(m,n) + r't(m',n) \\ t(m, rn + r'n') & = & rt(m,n) + r't(m,n') \end{array}$$

für $r, r' \in R$, $m, m' \in M$, $n, n' \in N$.

Dann gibt es genau eine R-lineare Abbildung $\hat{t} \colon M \underset{R}{\otimes} N \to T$ mit $\hat{t} \circ \tau = t$.

Diese erfüllt also $\hat{t}(m \otimes n) = t(m,n)$ für $m \in M$ und $n \in N$.

Beweis. Siehe Aufgabe **??**.(2). ▫

Definition 123 (und Lemma)

Seien $A = (A, \alpha)$ und $B = (B, \beta)$ kommutative R-Algebren.

Es wird der R-Modul $A \underset{R}{\otimes} B$ zu einem kommutativen Ring vermittels

$$\Big(\sum_{i \in I} a_i \otimes b_i\Big) \cdot \Big(\sum_{j \in J} a'_j \otimes b'_j\Big) \;:=\; \sum_{i \in I,\, j \in J} a_i a'_j \otimes b_i b'_j \;,$$

wobei I und J endliche Mengen sind, wobei $a_i \in A$ und $b_i \in B$ liegen für $i \in I$ und wobei $a'_j \in A$ und $b'_j \in B$ liegen für $j \in J$.

Es wird $A \underset{R}{\otimes} B$ zu einer kommutativen R-Algebra vermittels des Strukturmorphismus $\gamma \colon R \to A \underset{R}{\otimes} B \colon r \mapsto \gamma(r) := \alpha(r) \otimes 1 = 1 \otimes \beta(r)$.

Man beachte hierbei, daß für $a \in A$, $b \in B$ und $r \in R$ stets $(\alpha(r)a) \otimes b = (r \cdot a) \otimes b = r \cdot (a \otimes b) = a \otimes (r \cdot b) = a \otimes (\beta(r)b)$ gilt.

Die R-Modulstruktur auf $A \underset{R}{\otimes} B$ aus Definition 121 stimmt mit der via Strukturmorphismus γ und Beispiel 113.(4) überein.

Siehe Aufgabe **??**.

Bemerkung 124 (Universelle Eigenschaft des Tensorprodukts von Algebren)

Seien $A = (A, \alpha)$ und $B = (B, \beta)$ kommutative R-Algebren.

Es sind $\kappa_1 \colon A \to A \underset{R}{\otimes} B \colon a \mapsto a \otimes 1$ und $\kappa_2 \colon B \to A \underset{R}{\otimes} B \colon b \mapsto 1 \otimes b$ Morphismen von R-Algebren.

Sei eine kommutative R-Algebra $T = (T, \delta)$ gegeben, zusammen mit R-Algebrenmorphismen $t_1 \colon A \to T$ und $t_2 \colon B \to T$.

Dann gibt es genau einen R-Algebrenmorphismus $t \colon A \underset{R}{\otimes} B \to T$ mit $t \circ \kappa_1 = t_1$ und $t \circ \kappa_2 = t_2$.

Dieser erfüllt $t(a \otimes b) = t_1(a) \cdot t_2(b)$ für $a \in A$ und $b \in B$.

Beweis. Siehe Aufgabe **??**.(2). ▫

> Die universelle Eigenschaft des direkten Produkts von R-Algebren aus Bemerkung 17 wird auch dadurch zum Ausdruck gebracht, dieses direkte Produkt als *Produkt* in der *Kategorie* der kommutativen R-Algebren anzusprechen.
>
> Die universelle Eigenschaft des Tensorprodukts von R-Algebren aus Bemerkung refXXXXX wird auch dadurch zum Ausdruck gebracht, dieses Tensorprodukt als *Coprodukt* in der *Kategorie* der kommutativen R-Algebren anzusprechen.
>
> Erstere universelle Eigenschaft heißt auch *dual* zu letzterer.

2.3 Jacobsonsche Algebren und der Nullstellensatz

Sei R ein kommutativer Ring. Sei X ein Element.

Seien $S = (S, \alpha)$ und $T = (T, \beta)$ kommutative R-Algebren.

Sei $f \colon S \to T$ ein R-Algebrenmorphismus.

Definition 125 Sei

$$\mathrm{Jac}(S) \;:=\; \bigcap \{\, \mathfrak{m} : \; \mathfrak{m} \subset S \text{ ist ein maximales Ideal} \,\}$$

das *Jacobsonradikal* von S.

Es ist $\mathrm{Jac}(S)$ ein Ideal in S.

Es ist das Nilradikal von S im Jacobsonradikal von S enthalten; i.e. $\sqrt{(0)} \subseteq \mathrm{Jac}(S)$; cf. Lemma 77, Definition 33.

Bemerkung 126 *Sei $s \in S$. Die folgenden Aussagen $(1, 2)$ sind äquivalent.*

(1) *Es ist $s \in \mathrm{Jac}(S)$.*

(2) *Es ist $1 + xs \in \mathrm{U}(S)$ für $x \in S$.*

Beweis.

Ad (1) $\Rightarrow$ (2). Wir haben $1 \overset{!}{\in} (1+xs)$, i.e. $(1+xs) \overset{!}{=} S$ zu zeigen; cf. Bemerkung 30.

Annahme, es ist $(1+xs) \subset S$. Dann gibt es ein maximales Ideal $\mathfrak{m} \subset S$ mit $(1+xs) \subseteq \mathfrak{m}$; cf. Lemma 47. Es ist dann $xs \in \mathrm{Jac}(S) \subseteq \mathfrak{m}$ und also $1 = 1+xs-xs \in \mathfrak{m}$, im *Widerspruch* zu $\mathfrak{m} \subset S$.

Ad (2) $\Rightarrow$ (1). Sei $\mathfrak{m} \subset S$ ein maximales Ideal. Wir haben $s \in \mathfrak{m}$ zu zeigen. *Annahme*, es ist $s \notin \mathfrak{m}$. Dann ist $\mathfrak{m} \subset \mathfrak{m} + (s) \subseteq S$, wegen der Maximalität von $\mathfrak{m}$ also $\mathfrak{m} + (s) = S$. Folglich gibt es ein $m \in \mathfrak{m}$ und ein $y \in S$ mit $m + ys = 1$. Dann aber ist die Einheit $1-ys$ in $\mathfrak{m}$ und also $\mathfrak{m} = S$; cf. Bemerkung 30. Wir haben einen *Widerspruch* zu $\mathfrak{m} \subset S$. ▫

Lemma 127 (Nakayama) *Sei M ein endlich erzeugter S-Modul. Sei $M \neq 0$.*

Dann ist $\mathrm{Jac}(S)M \subset M$.

Beweis. Sei $k \in \mathbf{Z}_{\geqslant 0}$ minimal derart, daß wir $m_i \in M$ für $i \in [1,k]$ so wählen können, daß $M = {}_S\langle m_i \colon i \in [1,k]\rangle$ ist. Da $M \neq 0$ ist, ist $k \geqslant 1$.

Annahme, es ist $\mathrm{Jac}(S)M = M$. Dann ist $m_k \in \mathrm{Jac}(S)M$. Daher können wir

$$m_k \;=\; \sum_{j\in[1,\ell]} a_j\,\tilde{m}_j$$

schreiben mit $\ell \in \mathbf{Z}_{\geqslant 0}$, mit $a_j \in \mathrm{Jac}(S)$ und $\tilde{m}_j \in M$ für $j \in [1,\ell]$. Für $j \in [1,t]$ können wir $\tilde{m}_j = \sum_{i\in[1,k]} s_{j,i}\,m_i$ schreiben mit $s_{j,i} \in S$ für $i \in [1,k]$. Einsetzen gibt

$$m_k \;=\; \textstyle\sum_{j\in[1,\ell]} a_j \left(\sum_{i\in[1,k]} s_{j,i}\,m_i\right) \;=\; \sum_{i\in[1,k]} \underbrace{\left(\sum_{j\in[1,\ell]} a_j\,s_{i,j}\right)}_{=:\,b_i} m_i\;,$$

wobei $b_i \in \mathrm{Jac}(S)$ liegt für $i \in [1,k]$. Es ist $1 - b_k \in \mathrm{U}(S)$; cf. Bemerkung 126. Umformen gibt

$$(1-b_k)m_k \;=\; \sum_{i\in[1,k-1]} b_i\,m_i$$

und also

$$m_k \;=\; \sum_{i\in[1,k-1]} (1-b_k)^{-}b_i\,m_i\;.$$

Somit ist $m_k \in {}_S\langle m_i \colon i \in [1,k-1]\rangle$. Folglich ist

$$M \;=\; {}_S\langle m_i \colon i \in [1,k]\rangle \;=\; {}_R\langle m_i \colon i \in [1,k-1]\rangle\;,$$

im *Widerspruch* zur Minimalität von k. ▫

Lemma 128 *Sei $x \in S$.*

(i) *Die Aussagen* (1, 2, 3) *sind äquivalent.*

(1) *Es gibt ein normiertes Polynom* $g(X) \in R[X]$ *mit* $g(x) = 0$.

(2) *Es ist* x *ganz über* R, *i.e. es ist* $R[x]$ *endlich über* R.

(3) *Es ist* x *enthalten in einer* R*-Teilalgebra* $T \subseteq S$, *welche endlich über* R *ist.*

(ii) *Sei* R *integer. Die Aussagen* (1, 2) *sind äquivalent.*

(1) *Es gibt ein Polynom* $g(X) \in R[X]^\times$ *mit* $g(x) = 0$.

(2) *Es ist* x *algebraisch über* S.

Beweis.

Ad (i).

Ad (1) $\Rightarrow$ (2). Sei $n \in \mathbf{Z}_{\geqslant 0}$ und $g(X) = \sum_{i\in[0,n]} a_i X^i \in R[X]$ mit $a_n = 1$ und $g(x) = 0$ gegeben. Für $j \in \mathbf{Z}_{\geqslant 0}$ ist $x^{n+j} = -\sum_{i\in[0,n-1]} a_i x^{i+j} \in {}_A\langle\, x^i \,:\, i \in [0, n+j-1]\,\rangle$ und also

$$ {}_R\langle\, x^i : i \in [0, n+j]\,\rangle \;\subseteq\; {}_R\langle\, x^i \,:\, i \in [0, n+j-1]\,\rangle\ . $$

Iteration gibt

$$ {}_R\langle\, x^i \,:\, i \in [0, n+j]\,\rangle \;\subseteq\; {}_R\langle\, x^i \,:\, i \in [0, n-1]\,\rangle $$

und also die Inklusion $\subseteq$ in

$$ R[x] \;=\; \bigcup_{j\geqslant 0} {}_R\langle\, x^i \,:\, i \in [0, n+j]\,\rangle \;=\; {}_R\langle\, x^i \,:\, i \in [0, n-1]\,\rangle\ . $$

Ad (2) $\Rightarrow$ (3). Wir können $T = R[x]$ verwenden.

Ad (3) $\Rightarrow$ (1). Wir schreiben $T = {}_R\langle\, t_i \,:\, i \in [1, k]\,\rangle$ für ein $k \in \mathbf{Z}_{\geqslant 0}$ und gewisse $t_i \in T$ für $i \in [1, k]$. Es ist $xt_i \in T$ für $i \in [1, k]$. Also gibt es eine Matrix $A = (r_{i,j})_{i,j} \in R^{k\times k}$ mit $xt_i = \sum_{j\in[1,k]} \alpha(r_{i,j})t_j$ für $i \in [1, k]$, i.e. mit $\sum_{j\in[1,k]}(x\partial_{i,j} - \alpha(r_{i,j}))t_j = 0$ für $i \in [1, k]$.

Wir schreiben $B = (b_{i,j})_{i,j} := x\mathrm{E}_k - (\alpha(r_{i,j}))_{i,j} \in S^{k\times k}$. Es ist also $\sum_{j\in[1,k]} b_{i,j}t_j = 0$ für $i \in [1, k]$.

Sei $B' = (b'_{i,j})_{i,j} \in S^{k\times k}$ die Adjunkte zu S, i.e. sei

$$ b'_{u,v} \;=\; (-1)^{u+v} \det((b_{i,j})_{i\in[1,k]\smallsetminus\{v\},\, j\in[1,k]\smallsetminus\{u\}}) $$

für $u,\, v \in [1, k]$. Dann gilt nach der Cramerschen Regel $B'B = \det(B)\mathrm{E}_k$; cf. XXXU-eXXX. I.e. es ist $\sum_{i\in[1,k]} b'_{\ell,i} b_{i,j} = \det(B)\partial_{\ell,j}$ für $j,\, \ell \in [1, k]$. Für $\ell \in [1, k]$ folgt

$$ \det(B)t_\ell \;=\; \textstyle\sum_{j\in[1,k]} \det(B)\partial_{\ell,j}\, t_j \;=\; \sum_{i,\,j\,\in[1,k]} b'_{\ell,i}\, b_{i,j}\, t_j \;=\; 0\ , $$

also, da $1 \in T = {}_R\langle\, t_i \,:\, i \in [1, k]\,\rangle$, auch $\det(B) = 0$.

Daher ist $g(X) := \det(X\mathrm{E}_k - A) \in R[X]$ nach der Leibnizformel ein normiertes Polynom, und es ist $g(x) = \det(x\mathrm{E}_k - (\alpha(r_{i,j}))_{i,j}) = \det(B) = 0$.

Ad (ii).

Ad (2) $\Rightarrow$ (1). Schreibe $g(X) = \sum_{i\in[0,k]} r_i X^i$ mit $k \in \mathbf{Z}_{\geqslant 0}$ und $r_k \neq 0$. Es ist $0 = r_k^{k-1} g(x) = (r_k x)^k + \sum_{i\in[0,k]} r_i r_k^{k-i-1} (r_k x)^i$. Also ist $r_k x$ ganz über R; cf. (i). Also ist x algebraisch über R.

Ad (1) $\Rightarrow$ (2). Wähle $y \in R^\times$ mit yx ganz über R. Dann gibt es ein Polynom $h(X) = \sum_{i\in[0,k]} \tilde{r}_i X^i$ mit $k \in \mathbf{Z}_{\geqslant 0}$ und $r_k \neq 0$ und $h(yx) = 0$; cf. (i). Also ist $0 = \sum_{i\in[0,k]} \tilde{r}_i y^i x^i$. Es ist $y^k \neq 0$. Also ist $g(X) := \sum_{i\in[0,k]} \tilde{r}_i y^i X^i$ ungleich 0. Es ist $g(x) = 0$. ▫

Bemerkung 129 *Sei* $\alpha\colon R \to S$ *injektiv. Sei* S *integer.*

Sei S *ganz über* R.

Die folgenden Aussagen $(1, 2)$ *sind äquivalent.*

(1) *Es ist* R *ein Körper.*

(2) *Es ist* S *ein Körper.*

Beweis.

Ad (2) $\Rightarrow$ (1). Sei $x \in R^\times$. Wir haben zu zeigen, daß $x \overset{!}{\in} \mathrm{U}(R)$ liegt.

Es ist $y := \alpha(x)^- \in \mathrm{U}(S) \subseteq S$ ganz über R.

Dank Lemma 128.(i) gibt es ein $k \in \mathbf{Z}_{\geqslant 0}$ und ein normiertes Polynom $g(X) = \sum_{i\in[0,k]} r_i X^i \in R[X]$ mit $g(y) = 0$. Mit anderen Worten, es ist $\sum_{i\in[0,k]} \alpha(r_i)\, y^i = 0$. Folglich ist

$$\begin{array}{rcl}
\alpha\left(x \cdot \left(-\sum_{i\in[0,k-1]} r_i\, x^{k-i-1}\right)\right) & = & -\sum_{i\in[0,k-1]} \alpha(r_i)\alpha(x)^{k-i} \\
& = & y^{-k} \cdot \left(-\sum_{i\in[0,k-1]} \alpha(r_i)\, y^i\right) \\
& = & y^{-k} \cdot y^k \\
& = & 1\,.
\end{array}$$

Da α injektiv ist, folgt $x \cdot \left(-\sum_{i\in[0,k-1]} r_i x^{k-i-1}\right) = 1$ und also $x \in \mathrm{U}(R)$.

Ad (1) $\Rightarrow$ (2). Sei $y \in S^\times$. Wir haben zu zeigen, daß $y \overset{!}{\in} \mathrm{U}(S)$ liegt.

Es ist y ganz über R. Dank Lemma 128.(i) gibt es ein $k \in \mathbf{Z}_{\geqslant 0}$ und ein normiertes Polynom $g(X) = \sum_{i\in[0,k]} r_i X^i \in R[X]$ mit $g(y) = 0$. Mit anderen Worten, es ist $\sum_{i\in[0,k]} \alpha(r_i)\, y^i = 0$.

Da S integer ist, dürfen wir nach Kürzen einer Potenz von y annehmen, daß $r_0 \neq 0$ ist. Da R ein Körper ist, ist $r_0 \in \mathrm{U}(R)$.

Es ist $y \cdot \left(\sum_{i\in[1,k]} \alpha(r_i)\, y^i\right) = -\alpha(r_0) \in \mathrm{U}(S)$. Folglich ist $y \in \mathrm{U}(S)$. ▫

Bemerkung 130 *Die folgenden Aussagen* $(1,2)$ *gelten.*

(1) *Es ist* $\{\, x \in S :\ x \text{ ist ganz über } R \,\}$ *eine* R*-Teilalgebra von* S*.*

(2) *Sei* R *integer. Es ist* $\{\, x \in S :\ x \text{ ist algebraisch über } R \,\}$ *eine* R*-Teilalgebra von* S*.*

Beweis.

Ad (1). Wir schreiben $T := \{\, x \in S :\ x \text{ ist ganz über } R \,\}$.

Es ist $\alpha(R) \subseteq T$, insbesondere sind $0,\ 1 \in T$.

Seien $x,\ y \in T$. Wir haben zu zeigen, daß $x - y$ und xy in T liegen.

Da y ganz über R ist, ist y auch ganz über $R[x]$; cf. Lemma 128.(i).

Dank Aufgabe **??**.(1) folgt aus $R[x,y]$ endlich über $R[x]$ und $R[x]$ endlich über R, daß $R[x,y]$ endlich ist über R. Da $x - y,\ xy \in R[x,y]$ liegen, folgt die Aussage nun mit Lemma 128.(i).

Ad (2). Wir schreiben $T' := \{\, x' \in S :\ x' \text{ ist algebraisch über } R \,\}$.

Es ist $\alpha(R) \subseteq T'$, insbesondere sind $0,\ 1 \in T'$.

Seien $x',\ y' \in T$. Wir haben zu zeigen, daß $x' - y'$ und $x'y'$ in T' liegen.

Wir wählen $a,\ b \in R^\times$ mit $a \cdot x'$ und $b \cdot y'$ ganz über R. Dank (1) sind dann auch $ab \cdot x'y'$ und $ba \cdot x' - ab \cdot y' = ab \cdot (x' - y')$ ganz über R.

Da R integer ist, ist $ab \in R^\times$. Folglich sind $x'y'$ und $x' - y'$ algebraisch über R, wie benötigt. ▫

Definition 131 Es heißt S *jacobsonsch*, wenn $\mathrm{Jac}(S/\mathfrak{p}) = (0)$ ist für $\mathfrak{p} \in \mathrm{Spec}(S)$.

Beispiel 132 Sei $R := \mathbf{C}$. Sei $S := \mathbf{C}[X]_{(X)}$.

Es ist $S = \mathbf{C}[X]_{(X)}$ integer; cf. Aufgabe **??**.(3). Also ist $(0) \subseteq S$ prim. Es ist $S \simeq S/(0)$. Es ist aber S lokal mit maximalem Ideal $(X)_{(X)} = (\frac{X}{1})$; cf. Bemerkung 74. Also ist $\mathrm{Jac}(S) = (X)_{(X)} \neq (0)$.

Folglich ist S nicht jacobsonsch.

Bemerkung 133 *Sei* S *jacobsonsch. Sei* $f\colon S \to T$ *surjektiv.*

Dann ist T *jacobsonsch.*

Beweis. Sei $\mathfrak{q} \in \mathrm{Spec}(T)$. Sei $\mathfrak{p} := f^{-1}(\mathfrak{q})$. Es ist $\mathfrak{p} \in \mathrm{Spec}(S)$; cf. Bemerkung 41.

Wir haben den R-Algebrenisomorphismus $\bar{f}\colon S/\mathfrak{p} \to T/\mathfrak{q}\colon s + \mathfrak{p} \mapsto f(s) + \mathfrak{q}$; cf. Aufgabe 8.(3).

Da $\mathrm{Jac}(S/\mathfrak{p}) = (0)$ ist, ist auch $\mathrm{Jac}(T/\mathfrak{q}) = (0)$. ▫

Bemerkung 134 *Sei S jacobsonsch.*

Sei $\mathfrak{a} \in \mathrm{Ideale}(S)$*. Es ist*

$$\sqrt{\mathfrak{a}} \;=\; \bigcap \{\, \mathfrak{m} : \text{ es ist } \mathfrak{m} \subset S \text{ ein maximales Ideal mit } \mathfrak{a} \subseteq \mathfrak{m} \,\} \;.$$

Hierbei ist der Schnitt über eine leere Menge von Teilmengen von S als S definiert. Insbesondere ist $\sqrt{(0)} = \mathrm{Jac}(S)$*.*

Beweis. Zu zeigen ist

$$\begin{array}{rcl} \sqrt{\mathfrak{a}} & = & \bigcap \{\, \mathfrak{p} : \text{ es ist } \mathfrak{p} \subset S \text{ ein Primideal mit } \mathfrak{a} \subseteq \mathfrak{m} \,\} \\ & \overset{!}{\supseteq} & \bigcap \{\, \mathfrak{m} : \text{ es ist } \mathfrak{m} \subset S \text{ ein maximales Ideal mit } \mathfrak{a} \subseteq \mathfrak{m} \,\} \;=:\; \mathfrak{b} \;; \end{array}$$

cf. Lemma 77.

Sei $x \in \mathfrak{b}$. Sei $\mathfrak{p} \in \mathrm{Spec}(S)$ mit $\mathfrak{a} \subseteq \mathfrak{p}$. Zu zeigen ist $x \overset{!}{\in} \mathfrak{p}$.

Da $\mathrm{Jac}(S/\mathfrak{p}) = (0)$ ist, ist

$$\bigcap \{\, \mathfrak{m} : \text{ es ist } \mathfrak{m} \subset S \text{ ein maximales Ideal mit } \mathfrak{p} \subseteq \mathfrak{m} \,\} \;=\; \mathfrak{p} \;;$$

cf. Aufgaben 10 und **??**.(5).

Es genügt also, $x \overset{!}{\in} \mathfrak{m}$ zu zeigen für jedes maximale Ideal $\mathfrak{m} \subset S$ mit $\mathfrak{p} \subseteq \mathfrak{m}$.

Dann aber ist $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$ und die Behauptung folgt aus $x \in \mathfrak{b}$. ▫

Lemma 135 *Die folgenden Aussagen* $(1, 2)$ *sind äquivalent.*

(1) *Es ist S jacobsonsch.*

(2) *Für* $\mathfrak{p} \in \mathrm{Spec}(S)$ *und* $x \in S \smallsetminus \mathfrak{p}$ *mit* $(S/\mathfrak{p})_{x+\mathfrak{p}}$ *Körper ist auch* $S/\mathfrak{p}$ *ein Körper.*

Beweis.

Ad $(1) \Rightarrow (2)$. Wir schreiben $\bar{S} := S/\mathfrak{p}$ und $\bar{x} := x + \mathfrak{p}$.

Sei $\bar{S}_{\bar{x}}$ ein Körper. Wir haben zu zeigen, daß $\bar{S}$ ein Körper ist.

Wir schreiben $N := \{\, \bar{x}^i : i \in \mathbf{Z}_{\geqslant 0} \,\}$. Es ist $\mathrm{Spec}(\bar{S}_{\bar{x}}) = \{\, \mathfrak{q}/\!\!/N : \mathfrak{q} \in \mathrm{Spec}(\bar{S}),\ \bar{x} \not\in \mathfrak{q} \,\}$; cf. Bemerkung 69.(1). Da $\bar{S}_{\bar{x}}$ ein Körper ist, ist $\mathrm{Spec}(\bar{S}_{\bar{x}}) = \{(0)\}$. Also ist für jedes $\mathfrak{q} \in \mathrm{Spec}(\bar{S})$ mit $\bar{x} \not\in \mathfrak{q}$ bereits $\mathfrak{q}/\!\!/N = (0)$, was wegen $\bar{S}$ integer gerade $\mathfrak{q} = (0)$ bedeutet. In anderen Worten, ist $\mathfrak{q} \in \mathrm{Spec}(\bar{S}) \smallsetminus \{(0)\}$, dann ist $\bar{x} \in \mathfrak{q}$.

Annahme, es ist $\bar{S}$ kein Körper. Dann ist das Ideal $(0) \subset \bar{S}$ nicht maximal. Folglich ist jedes maximale Ideal in $\bar{S}$ ungleich (0). Also ist $\bar{x}$ in jedem maximalen Ideal von $\bar{S}$ enthalten;

cf. Definition 33. Dann aber ist $\bar{x} \in \mathrm{Jac}(\bar{S}) = (0)$, und wir haben einen *Widerspruch* zu $\bar{x} \neq 0$.

Ad (2) $\Rightarrow$ (1). Sei $\mathfrak{p} \in \mathrm{Spec}(S)$. Wir schreiben $\bar{S} := S/\mathfrak{p}$ und $\bar{s} := s + \mathfrak{p}$ für $s \in S$. Wir haben $\mathrm{Jac}(\bar{S}) \overset{!}{=} (0)$ zu zeigen.

Sei $x \in S \smallsetminus \mathfrak{p}$, i.e. $\bar{x} \in \bar{S}^{\times}$. Wir müssen zeigen, daß $\bar{x} \overset{!}{\notin} \mathrm{Jac}(\bar{S})$ liegt, i.e. daß es ein maximales Ideal $\mathfrak{m} \subset \bar{S}$ mit $\bar{x} \overset{!}{\notin} \mathfrak{m}$ gibt.

Es ist $\bar{S}_{\bar{x}}$ nicht der Nullring, da $\bar{S}$ integer ist und $\bar{x} \in \bar{S}^{\times}$.

Sei $\mathfrak{n} \subset \bar{S}_{\bar{x}}$ ein maximales Ideal. Dann ist $\bar{S}_{\bar{x}}/\mathfrak{n}$ ein Körper. Sei $\mathfrak{q} := \rho_{S,\mathfrak{p}}^{-1}(\lambda_{S,N}^{-1}(\mathfrak{n})) \in \mathrm{Spec}(S)$; cf. Definition 33, Bemerkung 69. Es ist $\mathfrak{p} = \rho_{S,\mathfrak{p}}^{-1}((0)) \subseteq \rho_{S,\mathfrak{p}}^{-1}(\lambda_{S,N}^{-1}(\mathfrak{n})) = \mathfrak{q}$.

Es ist genau dann $\frac{\bar{a}}{\bar{x}^i} \in \mathfrak{n}$, wenn $a \in \mathfrak{q}$ ist; wobei $a \in S$ und $i \in \mathbf{Z}_{\geqslant 0}$ liegen. Insbesondere ist $\frac{\bar{x}}{1} \in \mathrm{U}(\bar{S}_{\bar{x}})$, also $\frac{\bar{x}}{1} \notin \mathfrak{n}$, i.e. $x \notin \mathfrak{q}$.

Wir schreiben $\tilde{S} := S/\mathfrak{q}$ und $\tilde{s} := s + \mathfrak{q}$ für $s \in S$. Wir haben die sich invertierenden R-Algebrenmorphismen

$$\begin{array}{ccc} \bar{S}_{\bar{x}}/\mathfrak{n} & \longleftrightarrow & \tilde{S}_{\tilde{x}} \\ \frac{\bar{a}}{\bar{x}^i} + \mathfrak{n} & \mapsto & \frac{\tilde{a}}{\tilde{x}^i} \\ \frac{\bar{a}}{\bar{x}^i} + \mathfrak{n} & \leftarrow\!\shortmid & \frac{\tilde{a}}{\tilde{x}^i} \,, \end{array}$$

cf. Bemerkung 26, Lemma 67. In der Tat haben wir den R-Algebrenmorphismus $S \to \tilde{S}_{\tilde{x}}\colon s \mapsto \frac{\tilde{s}}{1}$. Dieser schickt $\mathfrak{p}$ auf 0, was den R-Algebrenmorphismus $\bar{S} \to \tilde{S}_{\tilde{x}}\colon \bar{s} \mapsto \frac{\tilde{s}}{1}$ induziert. Dieser wiederum schickt $\bar{x}$ auf die Einheit $\frac{\tilde{x}}{1}$ mit Inversem $\frac{1}{\tilde{x}}$, was den R-Algebrenmorphismus $\bar{S}_{\bar{x}} \to \tilde{S}_{\tilde{x}}\colon \frac{\bar{s}}{\bar{x}^i} \mapsto \frac{\tilde{s}}{\tilde{x}^i}$ induziert. Dieser schließlich schickt $\mathfrak{n}$ auf 0, was den R-Algebrenmorphismus $\bar{S}_{\bar{x}}/\mathfrak{n} \to \tilde{S}_{\tilde{x}}\colon \frac{\bar{s}}{\bar{x}^i} + \mathfrak{n} \mapsto \frac{\tilde{s}}{\tilde{x}^i}$ induziert. In der Gegenrichtung haben wir den R-Algebrenmorphismus $S \to \bar{S}_{\bar{x}}/\mathfrak{n}\colon s \mapsto \frac{\bar{s}}{1} + \mathfrak{n}$. Dieser schickt $\mathfrak{q}$ auf 0, was den R-Algebrenmorphismus $\tilde{S} \to \bar{S}_{\bar{x}}/\mathfrak{n}\colon \tilde{s} \mapsto \frac{\bar{s}}{1} + \mathfrak{n}$ induziert. Dieser wiederum schickt $\tilde{x}$ auf das invertierbare Element $\frac{\bar{x}}{1} + \mathfrak{n}$ mit Inversem $\frac{1}{\bar{x}} + \mathfrak{n}$, was den R-Algebrenmorphismus $\tilde{S}_{\tilde{x}} \to \bar{S}_{\bar{x}}/\mathfrak{n}\colon \frac{\tilde{s}}{\tilde{x}^i} \mapsto \frac{\bar{s}}{x^i} + \mathfrak{n}$ induziert.

Also ist $\tilde{S}_{\tilde{x}}$ ein Körper. Da $\tilde{S} = S/\mathfrak{q}$ ist und da $\tilde{x} \neq 0$ ist, ist dank (2) auch $\tilde{S}$ ein Körper. Also ist $\mathfrak{q}$ maximal in S und daher auch $\mathfrak{m} := \rho_{S,\mathfrak{p}}(\mathfrak{q}) = \{\, \bar{s} : s \in \mathfrak{q} \,\}$ maximal in $\bar{S}$; cf. Aufgabe **??**.(5). Da $x \notin \mathfrak{q}$ liegt, liegt auch $\bar{x} \notin \mathfrak{m}$, wie verlangt. ▫

Bemerkung 136 *Sei R ein Körper.*

Dann ist $R[X]$ jacobsonsch.

Jedes Primideal in $R[X]$ ungleich (0) *ist maximal und von einem Primelement erzeugt.*

Beweis. Jedes Primideal in $R[X]$ ungleich (0) ist maximal und von einem Primelement erzeugt; cf. Aufgaben 11.(2) und **??**.(3), Bemerkung 74.

Sei $\mathfrak{p} \subseteq R[X]$ ein Primideal. Wir haben $\mathrm{Jac}(R[X]/\mathfrak{p}) \overset{!}{=} (0)$ zu zeigen.

Fall $\mathfrak{p} = (0)$.

Behauptung. Es gibt in $R[X]$ neben (X) noch unendlich viele weitere maximale Ideale.

Annahme nicht. Sei $k \in \mathbf{Z}_{\geqslant 1}$ und seien $\mathfrak{m}_i$ für $i \in [1,k]$ die verschiedenen maximalen Ideale. Sei $\mathfrak{m}_i = (m_i(X))$ mit $\deg(m_i) \geqslant 1$ für $i \in [1,k]$. Dann ist $u(X) := 1 + \prod_{i\in[1,k]} m_i(X)$ von Grad $\geqslant 1$. Also ist $(u(X)) \subset R[X]$, aber $(u(X)) \not\subseteq (m_i(X))$ für $i \in [1,k]$, im *Widerspruch* zu Lemma 47. Dies zeigt die *Behauptung.*

Sei nun $g(X) \in \mathrm{Jac}(R[X])$. Wir haben $g(X) \overset{!}{=} 0$ zu zeigen.

Annahme, es ist $g(X) \neq 0$. Es ist $g(X) \notin \mathrm{U}(R[X])$. Also können wir $g(X) = \prod_{i\in[1,\ell]} p_i(X)$ schreiben mit $\ell \in \mathbf{Z}_{\geqslant 1}$ und $p_i(X) \in R[X]^\times$ prim für $i \in [1,\ell]$; cf. Aufgabe **??**.(8). Sei $\mathfrak{m}$ ein maximales Ideal, welches nicht in $\{\, (p_i(X)) : \ i \in [1,\ell] \,\}$ liegt. Es ist $g(X) \in \mathrm{Jac}(R[X]) \subseteq \mathfrak{m}$. Also gibt es ein $j \in [1,\ell]$ mit $(p_i(X)) \subseteq \mathfrak{m}$. Wegen $(p_i(X))$ maximal folgt $(p_i(X)) = \mathfrak{m}$. Wir haben einen *Widerspruch.*

Fall $\mathfrak{p} \neq (0)$. Es ist $\mathfrak{p}$ maximal, also $R[X]/\mathfrak{p}$ ein Körper, worin (0) maximal ist, was $\mathrm{Jac}(R[X]/\mathfrak{p}) = (0)$ nach sich zieht. □

Lemma 137 *Sei S jacobsonsch. Sei $T = S[x]$ für ein $x \in T$.*

Die folgenden Aussagen $(1,2)$ gelten.

(1) *Es ist T jacobsonsch.*

(2) *Sei $\mathfrak{q} \subset T$ ein maximales Ideal. Dann ist auch $\mathfrak{p} := f^{-1}(\mathfrak{q}) \subset S$ ein maximales Ideal und $T/\mathfrak{q}$ endlich über $S/\mathfrak{p}$ via $\bar{f}\colon S/\mathfrak{p} \to T/\mathfrak{q}\colon s + \mathfrak{p} \mapsto f(s) + \mathfrak{q}$.*

Beweis.

Ad (1). Sei $\mathfrak{q} \in \mathrm{Spec}(T)$.

Wir schreiben $\mathfrak{p} := f^{-1}(\mathfrak{q}) \subset S$. Es sind $\bar{S} := S/\mathfrak{p}$ und $\bar{T} := T/\mathfrak{q}$ integer; cf. Bemerkung 41. Wir haben den injektiven R-Algebrenmorphismus $\bar{f}\colon \bar{S} \to \bar{T}\colon s + \mathfrak{p} \mapsto f(s) + \mathfrak{q}$; cf. Aufgabe 8.(3). Wir identifizieren entlang $\bar{f}$ und sehen $\bar{S}$ als Teilalgebra von $\bar{T}$ an.

Für $y \in T$ schreiben wir kurz $\bar{y} := y + \mathfrak{q} \in \bar{T}$. Es ist $\bar{T} = \bar{S}[\bar{x}]$.

Sei $\mathfrak{u} \subseteq \bar{S}[X]$ der Kern des surjektiven $\bar{S}$-Algebrenmorphismus $\bar{S}[X] \to \bar{S}[\bar{x}]\colon X \mapsto \bar{x}$; cf. Lemma 20. Dieser ist auch ein R-Algebrenmorphismus. Es ist $\bar{T} \simeq \bar{S}[X]/\mathfrak{u}$; cf. Aufgabe 8.(3). Insbesondere ist $\mathfrak{u}$ ein Primideal.

Sei $t \in T \smallsetminus \mathfrak{q}$. Sei $\bar{T}_{\bar{t}}$ ein Körper. Gemäß Lemma 135 ist zu zeigen, daß $\bar{T}$ ein Körper ist.

Fall $\mathfrak{u} = (0)$. Dann ist $\bar{T} \simeq \bar{S}[X]$. Folglich genügt es zu zeigen, daß für $a(X) \in \bar{S}[X]^\times$ der Ring $\bar{S}[X]_{a(X)}$ kein Körper ist.

Annahme, doch. Sei $K = \mathrm{Quot}(\bar{S})$. Wir identifizieren entlang $\lambda\colon \bar{S} \to K$. Wir wählen ein Primelement $b(X) \in K[X]^\times$ mit $a(X) \notin (b(X)) \subseteq K[X]$. Ein solches existiert, da sonst $a(X)$ in allen maximalen Idealen von $K[X]$ liegt, im Widerspruch zu $K[X]$ jacobsonsch; cf.

Bemerkung 136. Durch Multiplikation mit einem gemeinsamen Nenner der Koeffizienten können wir erreichen, daß $b(X) \in \bar{S}[X]$ liegt.

Da $\bar{S}[X]_{a(X)}$ ein Körper ist, gibt es ein Element $\frac{c(X)}{a(X)^k} \in \bar{S}[X]_{a(X)}$ mit $\frac{c(X)}{a(X)^k} \cdot \frac{b(X)}{1} = 1$. Dann ist aber $b(X) \cdot c(X) = a(X)^k$, also $a(X)^k \in (b(X))$, also, da $(b(X))$ prim ist, auch $a(X) \in (b(X))$. Wir haben einen *Widerspruch*.

Fall $\mathfrak{u} \neq (0)$. Wir wählen $u(X) \in \mathfrak{u}$ mit $u(X) \neq 0$. Es ist $u(\bar{x}) = 0$. Daher ist $\bar{x}$ algebraisch über $\bar{S}$; cf. Lemma 128.(ii). Infolgedessen ist $\bar{S}[\bar{x}]$ algebraisch über $\bar{S}$; cf. Bemerkung 130.(2). Insbesondere ist $\bar{t}$ algebraisch über $\bar{S}$. Es gibt also ein Polynom $\sum_{i\in[0,\ell]} \vartheta_i X^i \in \bar{S}[X]$ mit $\ell \in \mathbf{Z}_{\geqslant 1}$ und $\vartheta_\ell \neq 0$ und $\sum_{i\in[0,\ell]} \vartheta_i \bar{t}^i = 0$. Da $\bar{T}$ integer ist, können wir hierbei noch $\vartheta_0 \neq 0$ erreichen.

Da $\bar{T}_{\bar{t}}$ ein Körper ist, sind darin ϑ_0 und η_k invertierbar. Wir schreiben $\xi := \vartheta_0\eta_k \in \bar{S}^\times$. Wir haben den injektiven R-Algebrenmorphismus $\bar{S}_\xi \to \bar{T}_{\bar{t}}$: $\frac{\bar{y}}{\xi^k} \mapsto \bar{y}\xi^{-k}$, dementlang wir S_ξ mit einer R-Teilalgebra von $\bar{T}_{\bar{t}}$ identifizieren.

In $\bar{T}_{\bar{t}}$ ist $0 = \sum_{i\in[0,\ell]} \vartheta_{\ell-i}\vartheta_0^-(\frac{1}{\bar{t}})^i = (\frac{1}{\bar{t}})^\ell + \sum_{i\in[0,\ell-1]} \vartheta_{\ell-i}\vartheta_0^-(\frac{1}{\bar{t}})^i$. Also ist $\frac{1}{\bar{t}}$ ganz über $\bar{S}_\xi$; cf. Lemma 128.(i).

Es ist $\bar{x}^k + \sum_{i\in[0,k-1]} \eta_i\eta_k^{-1}\bar{x}^i = 0$. Also ist $\bar{x}$ ganz über $\bar{S}_\xi$.

Folglich ist $\bar{T}_{\bar{t}} = \bar{S}[\bar{x}, \frac{1}{\bar{t}}]$ ganz über $\bar{S}_\xi$; cf. Bemerkung 130.(1).

Da $\bar{T}_{\bar{t}}$ ein Körper ist, ist $\bar{S}_\xi$ ebenfalls ein Körper; cf. Bemerkung 129.

Da S jacobsonsch ist und da $\bar{S} = S/\mathfrak{p}$ ist, folgt aus $\bar{S}_\xi$ Körper, daß $\bar{S}$ ein Körper ist; cf. Lemma 135.

Daher ist $\mathfrak{u} \subset \bar{S}[X]$ maximal; cf. Bemerkung 136. Folglich ist $\bar{T} \simeq \bar{S}[X]/\mathfrak{u}$ ein Körper.

Ad (2). Um zu zeigen, daß $\mathfrak{p} \subset S$ maximal ist, haben wir zu zeigen, daß $\bar{S}$ ein Körper ist.

Nun ist $\bar{T}$ ein Körper. Also ist $\mathfrak{u} \subset \bar{S}[X]$ maximal. Da $\bar{S}[X]$ wegen $X \in \bar{S}[X]^\times \smallsetminus \mathrm{U}(\bar{S}[X])$ kein Körper ist, ist $\mathfrak{u} \neq (0)$. Wir wählen $u(X) \in \mathfrak{u}$ mit $u(X) \neq 0$. Wir schreiben $u(X) = \sum_{i\in[0,k]} \eta_i X^i$ mit $k \in \mathbf{Z}_{\geqslant 0}$ und $\eta_k \neq 0$.

Es ist $0 = u(\bar{x}) = \sum_{i\in[0,k]} \eta_i\bar{x}^i$. Es ist also $0 = \bar{x}^k + \sum_{i\in[0,k-1]} \eta_k^-\eta_i\bar{x}^i$. Folglich ist $\bar{x}$ ganz über $\bar{S}_{\eta_k}$; cf. Lemma 128.(i). Also ist $\bar{T} = \bar{S}[\bar{x}]$ ganz über $\bar{S}_{\eta_k}$; cf. Bemerkung 130.(1). Da $\bar{T}$ ein Körper ist, gilt das auch für $\bar{S}_{\eta_k}$; cf. Bemerkung 129. Da S jacobsonsch ist und da $\bar{S} = S/\mathfrak{p}$ ist, folgt aus $\bar{S}_{\eta_k}$ Körper, daß $\bar{S}$ ein Körper ist; cf. Lemma 135.

Insbesondere ist $\eta_k \in \mathrm{U}(\bar{S})$. Folglich ist $\bar{x}$ ganz über $\bar{S}$. Somit ist $\bar{T} = \bar{S}[\bar{x}]$ endlich über $\bar{S}$. ▫

Satz 138 (Rabinowitsch) *Sei S jacobsonsch.*

Sei $T = (T, f)$ endlich erzeugt als S-Algebra.

Die folgenden Aussagen $(1, 2)$ gelten.

(1) *Es ist T jacobsonsch.*

(2) *Sei* $\mathfrak{q} \subset T$ *ein maximales Ideal. Dann ist auch* $\mathfrak{p} := f^{-1}(\mathfrak{q}) \subset S$ *ein maximales Ideal und* $T/\mathfrak{q}$ *endlich über* $S/\mathfrak{p}$ *via* $\bar{f}\colon S/\mathfrak{p} \to T/\mathfrak{q}\colon s + \mathfrak{p} \mapsto f(s) + \mathfrak{q}$.

Beweis. Wir schreiben $T = S[x_1, \ldots, x_n]$ für $n \in \mathbf{Z}_{\geqslant 0}$ und $x_i \in T$ für $i \in [1, n]$ geeignet.

Ad (1). Iteriertes Anwenden von Lemma 137.(1) gibt

$$\begin{array}{rcl} S \text{ jacobsonsch} & \Longrightarrow & S[x_1] \text{ jacobsonsch} \\ & \Longrightarrow & S[x_1, x_2] \text{ jacobsonsch} \\ & \vdots & \\ & \Longrightarrow & S[x_1, x_2, \ldots, x_n] = T \text{ jacobsonsch} . \end{array}$$

Ad (2). Wir haben zu zeigen, daß $S/\mathfrak{p}$ ein Körper ist.

Wir schreiben $S_i := S[x_1, \ldots, x_i]$ für $i \in [1, n]$. Sei ferner $S_0 := S$.

Es läßt sich f schreiben als Kompositum von $f|^{S_1}$ mit den Inklusionsabbildungen $S_i \to S_{i+1}$ für $i \in [1, n-1]$.

Sei $\mathfrak{v}_i$ das Urbild von $\mathfrak{q}$ unter dem Kompositum $S_i \to S_n = T$ für $i \in [0, n]$. Insbesondere ist $\mathfrak{v}_0 = \mathfrak{p}$ und $\mathfrak{v}_n = \mathfrak{q}$.

Wir schreiben $\bar{S}_i := S_i/\mathfrak{v}_i$ für $i \in [0, n]$. Wir erhalten gemäß Aufgabe 8 injektive R-Algebrenmorphismen

$$\bar{S} \;=\; \bar{S}_0 \;\to\; \bar{S}_1 \;\to\; \bar{S}_2 \;\to\; \ldots \;\to\; \bar{S}_n \;=\; \bar{T} .$$

Iteriertes Anwenden von Lemma 137.(2) gibt

$$\begin{array}{rcl} \bar{T} = \bar{S}_n \text{ Körper} & \Longrightarrow & \bar{S}_{n-1} \text{ Körper} \\ & \Longrightarrow & \bar{S}_{n-2} \text{ Körper} \\ & \vdots & \\ & \Longrightarrow & \bar{S}_0 = \bar{S} \text{ Körper} . \end{array}$$

Ferner liefert Lemma 137.(2) zusammen mit Aufgabe **??**.(1), daß $\bar{T}$ endlich über $\bar{S}$ ist. ▫

Korollar 139 *Sei* K *ein Körper.*

Sei $n \in \mathbf{Z}_{\geqslant 0}$ *. Seien* $X_1, \ldots, X_n$ *paarweise verschiedene Elemente.*

Sei $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ *ein Ideal.*

Dann ist $K[X_1, \ldots, X_n]/\mathfrak{a}$ *jacobsonsch.*

Insbesondere ist $K[X_1, \ldots, X_n]$ *jacobsonsch.*

Beweis. Dies folgt aus Satz 138.(1) und aus K jacobsonsch. ▫

Lemma 140 *Sei K ein Körper.*

Sei $n \in \mathbf{Z}_{\geqslant 0}$. Seien X_1 , ..., X_n paarweise verschiedene Elemente.

(1) *Sei $(b_i)_{i\in[1,n]} \in K^{\oplus n}$ gegeben. Dann ist*

$$(X_1 - b_1, \dots, X_n - b_n) \ \subset \ K[X_1, \dots, X_n]$$

ein maximales Ideal.

Ist $g(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$, dann ist genau dann $g(b_1, \dots, b_n) = 0$, wenn $g(X_1, \dots, X_n) \in (X_1 - b_1, \dots, X_n - b_n)$ liegt.

(2) *Sei K algebraisch abgeschlossen.*

Sei $\mathfrak{m} \subset K[X_1, \dots, X_n]$ ein maximales Ideal.

Dann gibt es $(c_i)_{i\in[1,n]} \in K^{\oplus n}$ mit

$$\mathfrak{m} \ = \ (X_1 - c_1, \dots, X_n - c_n) \ .$$

Cf. auch Beispiel 37.

Beweis.

Ad (1). Wir haben den surjektiven K-Algebrenmorphismus $K[X_1, \dots, X_n] \to K$, der $X_i \mapsto b_i$ abbildet für $i \in [1, n]$; cf. Lemma 20. Er bildet also $g(X_1, \dots, X_n)$ nach $g(b_1, \dots, b_n)$ ab.

Sein Kern $\mathfrak{k}$ ist ein maximales Ideal.

Es ist $\tilde{\mathfrak{k}} := (X_1 - b_1, \dots, X_n - b_n) \subseteq \mathfrak{k}$. Wir haben $\supseteq$ zu zeigen.

Sei $g_1(X_1, \dots, X_n) \in \mathfrak{k}$ gegeben. Es ist $g_1(b_1, \dots, b_n) = 0$. Wir haben $g_1(X_1, \dots, X_n) \overset{!}{\in} \tilde{\mathfrak{k}}$ zu zeigen.

Polynomdivision gibt $g_1(X_1, \dots, X_n) = (X_1 - b_1) \cdot q_1(X_1, \dots, X_n) + g_2(X_2, \dots, X_n)$, mit $q_1(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ und mit $g_2(X_2, \dots, X_n) \in K[X_1, \dots, X_n]$ konstant in X_1 . Es ist

$$0 \ = \ g_1(b_1, \dots, b_n) = (b_1 - b_1) \cdot q_1(b_1, \dots, b_n) + g_2(b_2, \dots, b_n) \ = \ g_2(b_2, \dots, b_n) \ .$$

Wir haben $g_2(X_2, \dots, X_n) \overset{!}{\in} \tilde{\mathfrak{k}}$ zu zeigen.

Polynomdivision gibt $g_2(X_2, \dots, X_n) = (X_2 - b_2) \cdot q_2(X_2, \dots, X_n) + g_3(X_3, \dots, X_n)$, mit $q_2(X_2, \dots, X_n) \in K[X_1, \dots, X_n]$ konstant in X_1 und mit $g_3(X_3, \dots, X_n) \in K[X_1, \dots, X_n]$ konstant in X_1 und X_2 . Es ist

$$0 \ = \ g_2(b_2, \dots, b_n) = (b_2 - b_2) \cdot q_2(b_2, \dots, b_n) + g_3(b_3, \dots, b_n) \ = \ g_3(b_3, \dots, b_n) \ .$$

Wir haben $g_3(X_3, \dots, X_n) \overset{!}{\in} \tilde{\mathfrak{k}}$ zu zeigen.

Usf.

Am Ende muß $g_{n+1} \stackrel{!}{\in} \tilde{\mathfrak{k}}$ gezeigt werden, was aber aus $g_{n+1} = 0$ folgt.

Ad (2). Es ist $K[X_1, \ldots, X_n]/\mathfrak{m}$ endlich über $K/(\mathfrak{m} \cap K) = K/(0) \simeq K$; cf. Korollar 139, Satz 138.(2).

Da K algebraisch abgeschlossen ist, hat K keine endlichdimensionalen Körpererweiterungen von Dimension $\geqslant 2$. Denn *wäre* L eine solche Erweiterung, dann hätte ein Element aus L, das nicht aus K stammt, ein Minimalpolynom von Grad $\geqslant 2$. Da K algebraisch abgeschlossen ist, hat dieses Minimalpolynom eine Nullstelle aus K, deren zugehörigen Linearfaktor man abdividieren kann. Der verbleibende Faktor muß unser Element als Nullstelle haben, was wegen Minimalität aber *nicht* geht.

Es folgt, daß der Strukturmorphismus $K \to K[X_1, \ldots, X_n]/\mathfrak{m}$ ein Isomorphismus ist. Sei $u\colon K[X_1, \ldots, X_n]/\mathfrak{m} \to K$ sein Inverses.

Wir schreiben $c_i := u(X_i)$ für $i \in [1, n]$. Es ist $u(X_i - c_i + \mathfrak{m}) = c_i - c_i = 0$ für $i \in [1, n]$. Die Injektivität von u gibt dann $X_i - c_i + \mathfrak{m} = 0$ für $i \in [1, n]$. Also ist $(X_1 - c_1, \ldots, X_n - c_n) \subseteq \mathfrak{m}$. Dank (1) ist aber $(X_1 - c_1, \ldots, X_n - c_n)$ maximal. Also ist $(X_1 - c_1, \ldots, X_n - c_n) = \mathfrak{m}$. □

Satz 141 (Hilberts Nullstellensatz) *Sei K ein algebraisch abgeschlossener Körper.*

Sei $n \in \mathbf{Z}_{\geqslant 0}$. Seien X_1 , ..., X_n paarweise verschiedene Elemente.

Sei $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ ein Ideal.

Sei

$$V \;:=\; \{\, (v_i)_i \in K^{\oplus n} :\ \text{es ist } a(v_1, \ldots, v_n) = 0 \text{ für } a(X_1, \ldots, X_n) \in \mathfrak{a} \,\}\ .$$

Dann wird

$$\{\, g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n] :\ \text{es ist } g(v_1, \ldots, v_n) = 0 \text{ für } (v_i)_i \in V \,\} \;=\; \sqrt{\mathfrak{a}}\ .$$

Arbeitet man in der algebraischen Geometrie mit Varietäten wie etwa V, so erlaubt der Hilbertsche Nullstellensatz die Übersetzung zwischen Geometrie und Algebra.

Arbeitet man dort mit Schemata, also verallgemeinerten Varietäten, dann genügt einem dazu stattdessen das einfacher erhältliche Lemma 77.

Beweis.

Ad $\supseteq$. Sei $g(X_1, \ldots, X_n) \in \sqrt{\mathfrak{a}}$. Sei $v \in V$. Zu zeigen ist $g(v_1, \ldots, v_n) \stackrel{!}{=} 0$.

Es gibt ein $k \in \mathbf{Z}_{\geqslant 1}$ mit $g(X_1, \ldots, X_n)^k \in \mathfrak{a}$. Also ist $g(v_1, \ldots, v_n)^k = 0$. Mithin ist $g(v_1, \ldots, v_n) = 0$.

Ad $\subseteq$. Sei $\mathfrak{m} \subset K[X_1, \ldots, X_n]$ ein maximales Ideal. Wir schreiben

$$\mathfrak{m} \;=\; (X_1 - b_1, \ldots, X_n - b_n)$$

für ein $(b_i)_i \in K^{\oplus n}$; cf. Lemma 140.(2).

Es ist genau dann $\mathfrak{a} \subseteq \mathfrak{m}$, wenn $a(b_1, \ldots, b_n) = 0$ ist für alle $a(X_1, \ldots, X_n) \in \mathfrak{a}$; cf. Korollar 140.(1). I.e. genau dann, wenn $(b_i)_i \in V$ liegt.

Folglich ist

$$\begin{aligned}
\sqrt{\mathfrak{a}} &\overset{\text{K. 139, B. 134}}{=} \bigcap \{\, \mathfrak{m} : \text{ es ist } \mathfrak{m} \subset K[X_1, \ldots, X_n] \text{ ein maximales Ideal mit } \mathfrak{a} \subseteq \mathfrak{m} \,\} \\
&\overset{\text{K. 140}}{=} \bigcap\nolimits_{(v_i)_i \in V} (X_1 - v_1, \ldots, X_n - v_n) \\
&\overset{\text{K. 140.(1)}}{=} \bigcap\nolimits_{(v_i)_i \in V} \{\, g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n] : \ g(v_1, \ldots, v_n) = 0 \ \} .
\end{aligned}$$

□

2.4 Krulldimension

Sei R ein kommutativer Ring.

Seien $S = (S, \alpha)$ und $T = (T, \beta)$ kommutative R-Algebren. Sei $0_S \neq 1_S$. Sei $0_T \neq 1_T$.

Sei $f \colon S \to T$ ein R-Algebrenmorphismus.

Sei X, Y verschiedene Elemente. Seien X_i für $i \in \mathbf{Z}_{\geqslant 1}$ paarweise verschiedene Elemente.

2.4.1 Definition der Krulldimension

Definition 142

(1) Wir betrachten die Teilmenge

$$L \ := \ \{\, k \in \mathbf{Z}_{\geqslant 0} : \text{ es gibt } \mathfrak{p}_i \in \operatorname{Spec}(S) \text{ für } i \in [0, k] \text{ mit } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k \,\} \ \subseteq \ \mathbf{Z}_{\geqslant 0}$$

Ist L nach oben beschränkt, so sei $\operatorname{Krdim}(S) := \max(L)$ die *Krulldimension* von S.

Ist L nicht nach oben beschränkt, so schreiben wir $\operatorname{Krdim}(S) := \infty$.

(2) Sei $\mathfrak{q} \in \operatorname{Spec}(S)$. Sei $\operatorname{ht}(\mathfrak{q}) := \operatorname{Krdim}(S_{\mathfrak{q}})$ die *Höhe* von $\mathfrak{q}$ (engl. height).

Mit anderen Worten, ist die Menge

$$\{\, k \in \mathbf{Z}_{\geqslant 0} : \text{ es gibt } \mathfrak{p}_i \in \operatorname{Spec}(S) \text{ für } i \in [1, k] \text{ mit } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k \subseteq \mathfrak{q} \,\}$$

nach oben beschränkt, dann ist $\operatorname{ht}(\mathfrak{q})$ ihr Maximum, ansonsten ist $\operatorname{ht}(\mathfrak{q}) = \infty$; cf. Bemerkung 69.(1).

Beispiel 143

(1) Ist S ein Körper, dann ist $\operatorname{Krdim}(S) = 0$.

(2) Ist R ein Körper, dann ist $\operatorname{Krdim}(R[X]) = 1$; cf. Bemerkung 136.

(3) Ist R integer, dann ist $\operatorname{Krdim}(R[X,Y]) \geqslant 2$. Denn in $\operatorname{Spec}(R[X,Y])$ gibt es die Primidealkette $(0) \subset (X) \subset (X,Y)$.

(4) Ist R integer, dann ist $\operatorname{Krdim}(R[X_i \colon i \in \mathbf{Z}_{\geqslant 1}]) = \infty$. Denn in $\operatorname{Spec}(R[X_i \colon i \in \mathbf{Z}_{\geqslant 1}])$ gibt es die Primidealkette

$$(0) \;\subset\; (X_1) \;\subset\; (X_1, X_2) \;\subset\; (X_1, X_2, X_3) \;\subset\; \dots$$

2.4.2 Noether-Normalisierung

Wir wollen nun das Problem der Bestimmung der Krulldimension auf die Berechnung der Krulldimension eines Polynomrings zurückführen. Dazu suchen wir eine isomorphe Kopie eines Polynomrings zwischen R und S.

Definition 144 Sei $k \in \mathbf{Z}_{\geqslant 0}$. Sei $x_i \in S$ für $i \in [1,k]$.

Es heißt das Tupel $(x_i)_{i\in[1,k]}$ *algebraisch unabhängig* über R, wenn der R-Algebrenmorphismus $u\colon R[X_1,\dots,X_k] \to S$, der X_i auf x_i schickt für $i \in [1,k]$, injektiv ist. Cf. Lemma 20.

Mit anderen Worten, es ist $(x_i)_{i\in[1,k]}$ algebraisch unabhängig über R genau dann, wenn es ein Polynom $f(X_1,\dots,X_k) \in R[X_1,\dots,X_k]^\times$ gibt, welches im Kern von u liegt, i.e. für welches $f(x_1,\dots,x_k) = 0$ ist.

Ist $(x_i)_{i\in[1,k]}$ algebraisch unabhängig, dann ist u ein R-Algebrenisomorphismus.

Lemma 145 (Noether-Normalisierung)

Sei R ein Körper.

Sei S endlich erzeugt als Algebra über R.

Es gibt $k \in \mathbf{Z}_{\geqslant 0}$ und ein algebraisch unabhängiges Tupel $(x_i)_{i\in[1,k]}$ von Elementen von S derart, daß S ganz ist über $R[x_1,\dots,x_k]$.

Beweis. Wir bemerken zunächst, daß wegen R Körper und wegen $0_S \neq 1_S$ der Strukturmorphismus $\alpha\colon R \to S$ nicht Kern R hat, folglich Kern (0) hat, i.e. injektiv ist.

Wir führen eine Induktion über die Zahl der Erzeuger von S als Algebra über R.

Ist diese Zahl gleich 0, dann ist $\alpha : R \to S$ ein Isomorphismus.

Sei nun $S = R[y_1,\dots,y_\ell]$ für ein $\ell \in \mathbf{Z}_{\geqslant 1}$ und gewisse $y_i \in S$ für $i \in [1,\ell]$. Per Induktion dürfen wir die Aussage für $\ell - 1$ als bekannt voraussetzen.

Fall $(y_i)_{i\in[1,\ell]}$ algebraisch unabhängig über R. Wir können $(x_i)_{i\in[1,k]} := (y_i)_{i\in[1,\ell]}$ wählen.

Fall $(y_i)_{i\in[1,\ell]}$ nicht algebraisch unabhängig über R. Wir wählen uns ein Polynom $g(X_1,\dots,X_\ell) \in R[X_1,\dots,X_\ell]^\times$ mit $g(y_1,\dots,y_\ell) = 0$.

Wir schreiben $g(X_1,\dots,X_\ell) =: \sum_{e\,=\,(e_i)_i\in U} r_e \prod_{i\in[1,\ell]} X_i^{e_i}$ für eine endliche Teilmenge U von $\prod_{i\in[1,\ell]} \mathbf{Z}_{\geqslant 0}$, wobei $r_e \in R^\times$ sei für $e \in U$.

Wähle nun $d \in \mathbf{Z}_{\geqslant 0}$ mit $d > \max\{\, e_j :\ (e_i)_i \in U,\ j \in [1,\ell]\,\}$. Sei $z_i := y_i - y_\ell^{d^i} \in S$ für $i \in [1, \ell-1]$.

Es ist $y_i = z_i + y_\ell^{d^i}$ für $i \in [1,\ell-1]$. Folglich ist

$$0 \;=\; g(y_1,\dots,y_\ell) \;=\; g(z_1{+}y_\ell^{d^1}, z_2{+}y_\ell^{d^2},\dots,z_{\ell-1}{+}y_\ell^{d^{\ell-1}}, y_\ell) \;=\; \sum_{e\,=\,(e_i)_i\in U} r_e{\cdot}y_\ell^{e_\ell} \prod_{i\in[1,\ell-1]} (z_i{+}y_\ell^{d^i})^{e_i}\;.$$

Sei $\tilde S := R[z_1,\dots,z_{\ell-1}] \subseteq S$. Es ist $S = R[y_1,\dots,y_\ell] = R[z_1,\dots,z_{\ell-1},y_\ell] = \tilde S[y_\ell]$.

Es genügt zu zeigen, daß y_ℓ ganz ist über $\tilde S$. Denn dann ist S ganz über $\tilde S$; cf. Bemerkung 130.(1). Ferner gibt es dann nach Induktionsvoraussetzung ein $k \in \mathbf{Z}_{\geqslant 0}$ und ein über R algebraisch unabhängiges Tupel $(x_i)_{i\in[1,k]}$ von Elementen von $\tilde S$ mit $\tilde S$ ganz über $R[x_1,\dots,x_\ell]$. Dank Aufgabe **??**.(2) ist dann auch S ganz über $R[x_1,\dots,x_\ell]$.

Zeigen wir also, daß y_ℓ ganz ist über $\tilde S$. Sei

$$h(Y) := g(z_1{+}Y^{d^1}, z_2{+}Y^{d^2},\dots,z_{\ell-1}{+}Y^{d^{\ell-1}}, Y) \;=\; \sum_{e\,=\,(e_i)_i\in U} r_e{\cdot}Y^{e_\ell} \prod_{i\in[1,\ell-1]} (z_i{+}Y^{d^i})^{e_i} \in \tilde S[Y]\;.$$

Es ist $h(y_\ell) = 0$.

Wir schreiben $c_e := e_\ell + \sum_{i\in[1,\ell-1]} d^i e_i$ für $e = (e_i)_i \in U$.

Es ist $c_e = \deg(Y^{e_\ell} \prod_{i\in[1,\ell-1]} (z_i + Y^{d^i})^{e_i})$.

Gemäß Wahl von d ist $c_e \neq c_{\tilde e}$ für $e,\ \tilde e \in U$ mit $e \neq \tilde e$. Denn *wäre* $c_e = c_{\tilde e}$, so hätte man $e_\ell \equiv_d c_e \equiv_d c_{\tilde e} \equiv_d \tilde e_\ell$, wegen $e_\ell,\ \tilde e_\ell \in [0, d-1]$ also $e_\ell = \tilde e_\ell$. Es folgte $\sum_{i\in[1,\ell-1]} d^{i-1} e_i = \sum_{i\in[1,\ell-1]} d^{i-1} \tilde e_i$, also $e_1 \equiv_d \tilde e_1$, wegen $e_1,\ \tilde e_1 \in [0, d-1]$ mithin $e_1 = \tilde e_1$. Es folgte $\sum_{i\in[2,\ell-1]} d^{i-2} e_i = \sum_{i\in[2,\ell-2]} d^{i-2} \tilde e_i$, also $e_2 \equiv_d \tilde e_2$, wegen $e_2,\ \tilde e_2 \in [0, d-1]$ mithin $e_2 = \tilde e_2$. Usf. Insgesamt folgte $e = \tilde e$, was *nicht* zutrifft.

Sei nun $\hat e \in U$ derart, daß $c_{\hat e} := \max\{\, c_e :\ e \in U\,\}$ ist. Dann ist $\deg(h) = c_{\hat e}$. Der Koeffizient von $h(Y)$ bei $Y^{c_{\hat e}}$ ist $r_{\hat e}$.

Da R ein Körper ist, ist $r_{\hat e} \in \mathrm{U}(R)$.

Es ist $r_{\hat e}^{-}\, h(Y) \in \tilde S[Y]$ normiert mit $h(y_\ell) = 0$. Folglich ist y_ℓ ganz über $\tilde S$. ▫

2.4.3 Krulldimension und ganze Erweiterungen

Es ist $T = (T, f)$ eine kommutative S-Algebra. Sei T ganz über S.

Bemerkung 146

(1) *Sei $M \subseteq S$ eine multiplikative Teilmenge. Dann ist auch $N := f(M) \subseteq T$ eine multiplikative Teilmenge.*

Wir haben den R-Algebrenmorphismus $\tilde{f} \colon S/\!\!/M \to T/\!\!/N \colon \frac{s}{m} \mapsto \frac{f(s)}{f(m)}$; cf. Lemma 67.

Es ist $T/\!\!/N = (T/\!\!/N, \tilde{f})$ eine kommutative $S/\!\!/M$-Algebra. Es ist $T/\!\!/N$ ganz über $S/\!\!/M$.

(2) *Sei $\mathfrak{a} \in \mathrm{Ideale}(S)$. Wir schreiben $\bar{S} := S/\mathfrak{a}$ und $\bar{s} := s + \mathfrak{a}$ für $s \in S$.*

Sei $\mathfrak{b} \in \mathrm{Ideale}(T)$. Wir schreiben $\bar{T} := T/\mathfrak{b}$ und $\bar{t} := t + \mathfrak{b}$ für $t \in T$.

Sei $f(\mathfrak{a}) \subseteq \mathfrak{b}$. Wir haben den R-Algebrenmorphismus $\bar{f} \colon \bar{S} \to \bar{T} \colon \bar{s} \mapsto \overline{f(s)}$; cf. Bemerkung 26.

Es ist $\bar{T} = (\bar{T}, \bar{f})$ eine kommutative $\bar{S}$-Algebra. Es ist $\bar{T}$ ganz über $\bar{S}$.

Beweis. Wir verwenden Lemma 128.(i).

Ad (1). Sei $\frac{t}{n} \in T/\!\!/N$. Wir haben $\frac{t}{n}$ als ganz über $S/\!\!/M$ nachzuweisen.

Wir wählen ein $m \in M$ mit $f(m) = n$.

Es ist t ganz über S. Wir wählen $g(X) \in S[X]$ normiert mit $g(t) = 0$. Wir schreiben $g(X) =: \sum_{i \in [0,k]} a_i X^i$ mit $k \in \mathbf{Z}_{\geqslant 0}$ und $a_k = 1$.

Nun folgt aus

$$0 \;=\; g(t) \;=\; \sum_{i \in [0,k]} a_i t^i \;=\; \sum_{i \in [0,k]} f(a_i) t^i$$

auch

$$0 \;=\; \frac{1}{n^k} \sum_{i \in [0,k]} \frac{f(a_i)}{1} \left(\frac{t}{1}\right)^i \;=\; \sum_{i \in [0,k]} \tilde{f}\Big(\frac{a_i}{m^{k-i}}\Big) \left(\frac{t}{n}\right)^i .$$

Folglich ist $\tilde{g}(X) := \sum_{i \in [0,k]} \frac{a_i}{m^{k-i}} X^i \in (S/\!\!/M)[X]$ normiert mit $\tilde{g}(\frac{t}{n}) = 0$. Also ist $\frac{t}{n}$ ganz über $S/\!\!/M$.

Ad (2). Sei $t \in T$. Wir haben $\bar{t}$ als ganz über $\bar{S}$ nachzuweisen. Es ist t ganz über S. Wir wählen $g(X) \in S[X]$ normiert mit $g(t) = 0$. Wir schreiben $g(X) =: \sum_{i \in [0,k]} a_i X^i$ mit $k \in \mathbf{Z}_{\geqslant 0}$ und $a_k = 1$.

Nun folgt aus

$$0 \;=\; g(t) \;=\; \sum_{i \in [0,k]} a_i t^i \;=\; \sum_{i \in [0,k]} f(a_i) t^i$$

auch

$$0 \;=\; \sum_{i \in [0,k]} \overline{f(a_i)}\, \bar{t}^i \;=\; \sum_{i \in [0,k]} \bar{f}(\bar{a}_i) \bar{t}^i .$$

Folglich ist $\bar{g}(X) := \sum_{i \in [0,k]} \bar{a}_i X^i \in \bar{S}[X]$ ein normiertes Polynom mit $\bar{g}(\bar{t}) = 0$. Also ist $\bar{t}$ ganz über $\bar{S}$. ▫

Lemma 147 (Lying over) *Sei $f\colon S \to T$ injektiv. Sei $\mathfrak{p} \in \mathrm{Spec}(S)$ gegeben. Es gelten* $(1, 2)$.

(1) *Es gibt ein $\mathfrak{q} \in \mathrm{Spec}(T)$ mit $\mathfrak{p} = f^{-1}(\mathfrak{q})$.*

(2) *Seien $\mathfrak{q}$, $\mathfrak{q}' \in \mathrm{Spec}(T)$ mit $\mathfrak{p} = f^{-1}(\mathfrak{q}) = f^{-1}(\mathfrak{q}')$ und $\mathfrak{q} \subseteq \mathfrak{q}'$ gegeben.*

Dann ist auch $\mathfrak{q} = \mathfrak{q}'$.

Mit anderen Worten, die Abbildung $\mathrm{Spec}(S) \xleftarrow{\mathrm{Spec}(f)} \mathrm{Spec}(T)$ ist surjektiv und bewahrt echte Inklusionen.

Beweis. Sei $M := S \setminus \mathfrak{p}$. Es ist $M \subseteq S$ eine multiplikative Teilmenge. Daher ist auch $N := f(M) \subseteq T$ eine multiplikative Teilmenge. Es ist $0 \notin N$, da f injektiv ist und $0 \notin M$ liegt. Also ist $\frac{1}{0} \neq \frac{0}{0}$ in $T/\!\!/N$.

Wir haben den R-Algebrenmorphismus $\tilde{f}\colon S/\!\!/M \to T/\!\!/N\colon \frac{s}{m} \mapsto \frac{f(s)}{f(m)}$; cf. Lemma 67. Es ist $T/\!\!/N$ ganz über $S/\!\!/M$; cf. Bemerkung 146.(1).

Ad (1). Wir wählen ein maximales Ideal $\mathfrak{n} \subset T/\!\!/N$; cf. Korollar 48.

Sei $\mathfrak{m} := \tilde{f}^{-1}(\mathfrak{n}) \in \mathrm{Spec}(S/\!\!/M)$. Es ist $(T/\!\!/N)/\mathfrak{n}$ ganz über $(S/\!\!/M)/\mathfrak{m}$; cf. Bemerkung 146.(2). Da $(T/\!\!/N)/\mathfrak{n}$ ein Körper ist, ist auch $(S/\!\!/M)/\mathfrak{m}$ ein Körper; cf. Aufgabe 8.(3), Bemerkung 129. Also ist $\mathfrak{m} \subset S/\!\!/M$ maximal.

Es ist $S/\!\!/M = S_{\mathfrak{p}}$ lokal; cf. Bemerkung 74. Also ist $\mathfrak{m} = \mathfrak{p}_{\mathfrak{p}}$.

Sei $\mathfrak{q} := \lambda_{T,N}^{-1}(\mathfrak{n}) \in \mathrm{Spec}(T)$. Es ist

$$f^{-1}(\mathfrak{q}) \;=\; f^{-1}(\lambda_{T,N}^{-1}(\mathfrak{n})) \;=\; \lambda_{S,M}^{-1}(\tilde{f}^{-1}(\mathfrak{n})) \;=\; \lambda_{S,M}^{-1}(\mathfrak{m}) \;=\; \lambda_{S,M}^{-1}(\mathfrak{p}_{\mathfrak{p}}) \;=\; \mathfrak{p}\,.$$

Ad (2). Es ist $\mathfrak{m} := \mathfrak{p}_{\mathfrak{p}} \subset S/\!\!/M$ maximal; cf. Bemerkung 74. Da $\mathfrak{p} \cap M = \emptyset$, ist auch $\mathfrak{q} \cap N = \emptyset$. Es ist $\mathfrak{n} := \mathfrak{q}/\!\!/N \in \mathrm{Spec}(T/\!\!/N)$; cf. Bemerkung 69.(1). Es ist $\check{T} := (T/\!\!/N)/\mathfrak{n}$ integer und ganz über $\check{S} := (S/\!\!/M)/\mathfrak{m}$; cf. Bemerkung 146.(2). Es ist $\check{S}$ ein Körper. Es ist $0_{\check{T}} \neq 1_{\check{T}}$. Also hat $\check{f}\colon \check{S} \to \check{T}\colon \frac{s}{m} + \mathfrak{m} \mapsto \frac{f(s)}{f(m)} + \mathfrak{n}$ den Kern (0), ist also injektiv; cf. Bemerkung 26, Lemma 67, Bemerkung 34. Folglich ist $\check{T}$ ein Körper; cf. Bemerkung 129. Mithin ist $\mathfrak{n} \subset T/\!\!/N$ maximal.

Nun ist auch $\mathfrak{q}' \cap N = \emptyset$ und also $\mathfrak{n}' := \mathfrak{q}'/\!\!/N \in \mathrm{Spec}(T/\!\!/N)$; cf. Bemerkung 69.(1). Da $\mathfrak{n} \subseteq \mathfrak{n}' \subset T$, folgt aus der Maximalität von $\mathfrak{n}$, daß $\mathfrak{n} = \mathfrak{n}'$ ist. Somit ist auch $\mathfrak{q} = \lambda_{S,N}^{-1}(\mathfrak{n}) = \lambda_{S,N}^{-1}(\mathfrak{n}') = \mathfrak{q}'$; cf. Bemerkung 69.(1). □

Lemma 148 (Going up) *Sei $\mathfrak{q} \in \mathrm{Spec}(T)$. Sei $\mathfrak{p}' \in \mathrm{Spec}(S)$. Sei $\mathfrak{p} := f^{-1}(\mathfrak{q}) \subseteq \mathfrak{p}'$.*

Dann existiert ein $\mathfrak{q}' \in \mathrm{Spec}(T)$ mit $\mathfrak{q} \subseteq \mathfrak{q}'$ und $f^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Beweis. Wir haben den injektiven R-Algebrenmorphismus $\bar{f}\colon \bar{S} := S/\mathfrak{p} \to T/\mathfrak{q} =: \bar{T}$; cf. Aufgabe 8.(3). Es ist $\bar{T}$ ganz über $\bar{S}$; cf. Bemerkung 146.(2).

Es ist $\bar{\mathfrak{p}}' := \rho_{S,\mathfrak{p}}(\mathfrak{p}') \in \operatorname{Spec}(\bar{S})$; cf. Bemerkung 69.(2). Also gibt es $\mathfrak{r} \in \operatorname{Spec}(\bar{T})$ mit $\bar{f}^{-1}(\mathfrak{r}) = \bar{\mathfrak{p}}'$; cf. Lemma 147.(1).

Mit $\mathfrak{q}' := \rho_{T,\mathfrak{q}}^{-1}(\mathfrak{r}) \in \operatorname{Spec}(T)$ wird $\mathfrak{q} \subseteq \mathfrak{q}'$ und

$$f^{-1}(\mathfrak{q}') \;=\; f^{-1}(\rho_{T,\mathfrak{q}}^{-1}(\mathfrak{r})) \;=\; \rho_{S,\mathfrak{p}}^{-1}(\bar{f}^{-1}(\mathfrak{r})) \;=\; \rho_{S,\mathfrak{p}}^{-1}(\bar{\mathfrak{p}}'^{-1}) \;=\; \mathfrak{p}' \,;$$

cf. Bemerkung 69.(2) ▫

Korollar 149 (Konstanz der Krulldimension bei ganzen Erweiterungen)

Wir erinnern an die kommutativen R-Algebren S und T und an den R-Algebrenmorphismus $f\colon S \to T$, sowie daran, daß $T = (T, f)$ ganz über S ist.

Sei $f\colon S \to T$ injektiv.

Dann ist $\operatorname{Krdim}(S) = \operatorname{Krdim}(T)$.

Beweis.

Ad ($\leqslant$). Sei $k \in \mathbf{Z}_{\geqslant 0}$. Sei $\mathfrak{p}_i \in \operatorname{Spec}(S)$ für $i \in [0, k]$ mit $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k$. Wir haben $k \overset{!}{\leqslant} \operatorname{Krdim}(T)$ zu zeigen.

Dank Lemma 147.(1) gibt es ein $\mathfrak{q}_0 \in \operatorname{Spec}(T)$ mit $f^{-1}(\mathfrak{q}_0) = \mathfrak{p}_0$.

Dank Lemma 148 gibt es ein $\mathfrak{q}_1 \in \operatorname{Spec}(T)$ mit $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$ und $f^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$. Da $\mathfrak{p}_0 \neq \mathfrak{p}_1$, ist auch $\mathfrak{q}_0 \neq \mathfrak{q}_1$.

Dank Lemma 148 gibt es ein $\mathfrak{q}_2 \in \operatorname{Spec}(T)$ mit $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ und $f^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$. Da $\mathfrak{p}_0 \neq \mathfrak{p}_1$, ist auch $\mathfrak{q}_0 \neq \mathfrak{q}_1$.

Usf.

Insgesamt erhalten wir eine Kette $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_k$ in $\operatorname{Spec}(T)$ und also $k \leqslant \operatorname{Krdim}(T)$.

Ad ($\geqslant$). Sei $\ell \in \mathbf{Z}_{\geqslant 0}$. Sei $\mathfrak{q}_i \in \operatorname{Spec}(T)$ für $i \in [0, \ell]$ mit $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_\ell$. Wir haben $\ell \overset{!}{\leqslant} \operatorname{Krdim}(S)$ zu zeigen. Da aber $\operatorname{Spec}(f)$ gemäß Lemma 147.(2) strikte Inklusionen erhält, ist $f^{-1}(\mathfrak{q}_0) \subset f^{-1}(\mathfrak{q}_1) \subset \ldots \subset f^{-1}(\mathfrak{q}_\ell)$ und also $\ell \leqslant \operatorname{Krdim}(S)$. ▫

Korollar 149 gilt insbesondere im Falle $\operatorname{Krdim}(S) = \infty$ oder $\operatorname{Krdim}(T) = \infty$.

2.4.4 Krulldimension null

Definition 150 Sei M ein S-Modul.

Es heißt M *einfach*, falls die Anzahl der Teilmoduln von M gleich zwei ist.

Mit anderen Worten, M ist einfach, falls $M \neq 0$ ist und falls M nur die Teilmoduln 0 und M hat.

Ist M einfach, dann ist jede S-lineare Abbildung von einem S-Modul X nach M null oder surjektiv und jede S-lineare Abbildung von M zu einem S-Modul Y null oder injektiv. Denn Bild und Kern einer S-linearen Abbildung sind Teilmoduln.

Definition 151 Sei M ein S-Modul.

Eine *Teilmodulreihe* $(M_i)_{i\in[0,\ell]}$ von M besteht aus ihrer *Länge* $\ell \in \mathbf{Z}_{\geqslant 0}$ und aus S-Teilmoduln M_i von M für $i \in [0,\ell]$ mit $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots \subseteq M_\ell = M$.

Eine solche Teilmodulreihe heißt *echt*, wenn $0 = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_\ell = M$ ist.

Für $i \in [1,\ell]$ heißt der S-Modul M_i/M_{i-1} ein *Subfaktor* von $(M_i)_{i\in[0,\ell]}$.

Eine Teilmodulreihe $(M_i)_{i\in[0,\ell]}$ von M heißt *Kompositionsreihe*, falls alle ihre Subfaktoren einfach sind.

Falls für M eine Kompositionsreihe existiert, so sagen wir, *M hat eine Kompositionsreihe.*

Lemma 152 (und Definition) *Sei M ein S-Modul.*

Sei $(M_i)_{i\in[0,\ell]}$ eine Kompositionsreihe von M.

Sei $(\tilde{M}_i)_{i\in[0,k]}$ eine echte Teilmodulreihe von M.

Dann ist $k \leqslant \ell$.

Ist insbesondere $(\tilde{M}_i)_{i\in[0,k]}$ auch eine Kompositionsreihe von M, dann ist $k = \ell$.

Hat M eine Kompositionsreihe, dann bezeichnet $\ell(M)$ die Länge jeder Kompositionsreihe. Es heißt $\ell(M)$ die Länge *von M.*

Beweis. Siehe Aufgabe **??**.$(4, 5)$. ▫

Bemerkung 153 *Sei $M' \xrightarrow{i} M \xrightarrow{p} M''$ eine kurz exakte Sequenz von S-Moduln.*

Es gelten die Aussagen $(1, 2)$.

(1) *Es hat genau dann M eine Kompositionsreihe, wenn M' und M'' Kompositionsreihen haben.*

(2) *Hat M eine Kompositionsreihe, dann ist $\ell(M) = \ell(M') + \ell(M'')$.*

Beweis. Siehe Aufgabe **??**. ▫

Definition 154 Es heißt S *artinsch*, wenn der S-Modul S eine Kompositionsreihe hat.

Beispiel 155

(1) Ist R ein Körper und $S = R$, dann ist S artinsch.

(2) Ist R ein Körper und S endlichdimensional als R-Vektorraum, dann ist S artinsch. Denn dann kann man $\mathfrak{a}_0 := (0)$ nehmen, sodann ein Ideal $\mathfrak{a}_1$ minimaler Dimension gewählt werden mit $\mathfrak{a}_0 \subset \mathfrak{a}_1$, sodann ein Ideal $\mathfrak{a}_2$ minimaler Dimension gewählt werden mit $\mathfrak{a}_1 \subset \mathfrak{a}_2$, usf. Die Prozedur muß für ein $k \in \mathbf{Z}_{\geqslant 0}$ bei $\mathfrak{a}_k = S$ enden.

Ist e.g. $S = R \times R[X]/(X^2)$, dann ist S von Dimension 3 als R-Vektorraum und also artinsch.

Wir haben die Kompositionsreihe $0 \subset {}_S\langle (1,0) \rangle \subset {}_S\langle (1,0), (0, X + (X^2)) \rangle \subset S$, deren Subfaktoren sogar eindimensional sind über R.

(3) Ist $R = S = \mathbf{Z}$, dann ist S nicht artinsch. Denn $\mathbf{Z}$ hat eine echte Teilmodulreihen von Länge k für jedes $k \in \mathbf{Z}_{\geqslant 1}$, e.g. $0 \subset (2^{k-1}) \subset \ldots \subset (2^1) \subset (2^0)$; cf. Lemma 152.

Bemerkung 156 *Sei S noethersch.*

Es ist S artinsch genau dann, wenn für jede absteigende abzählbare Kette von Idealen

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

in S ein $k \in \mathbf{Z}_{\geqslant 1}$ existiert mit $\mathfrak{a}_k = \mathfrak{a}_i$ für $i \in \mathbf{Z}_{\geqslant k}$.

Beweis.

Sei *zum einen* S artinsch. *Annahme,* die genannte Kettenbedingung ist nicht erfüllt. Dann gibt es eine echte absteigende abzählbare Kette von Idealen

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

in S. O.E. ist $\mathfrak{a}_1 = S$. Sei $(\mathfrak{b}_i)_{i \in [1,k]}$ eine Kompositionsreihe in S. Dann ist

$$0 \subset \mathfrak{a}_{k+1} \subset \mathfrak{a}_k \subset \mathfrak{a}_{k-1} \subset \ldots \subset \mathfrak{a}_1 = S$$

eine echte Teilmodulreihe in S von Länge $k+1$. Aber es ist nicht $k+1 \leqslant k$, im *Widerspruch* zu Aufgabe **??**.(4).

Sei *zum anderen* die genannte Kettenbedingung erfüllt.

Sei $\mathfrak{b}_0 := S$.

Wir wählen in der Menge der echt in $\mathfrak{b}_0$ enthaltenen Ideale ein maximales Element $\mathfrak{b}_1 \subset \mathfrak{b}_0$, möglich, da S noethersch ist; cf. Aufgabe 12. Dann ist $\mathfrak{b}_0/\mathfrak{b}_1$ ein einfacher S-Modul.

Falls $\mathfrak{b}_1 \neq (0)$ ist, wählen wir in der Menge der echt in $\mathfrak{b}_1$ enthaltenen Ideale ein maximales Element $\mathfrak{b}_2 \subset \mathfrak{b}_1$, möglich, da S noethersch ist. Dann ist $\mathfrak{b}_1/\mathfrak{b}_2$ ein einfacher S-Modul.

Falls $\mathfrak{b}_2 \neq (0)$ ist, wählen wir in der Menge der echt in $\mathfrak{b}_2$ enthaltenen Ideale ein maximales Element $\mathfrak{b}_3 \subset \mathfrak{b}_2$, möglich, da S noethersch ist. Dann ist $\mathfrak{b}_2/\mathfrak{b}_3$ ein einfacher S-Modul.

Usf.

Wegen der genannten Kettenbedingung muß es ein $k \in \mathbf{Z}_{\geqslant 1}$ geben mit $\mathfrak{b}_k = 0$. Dann ist $\mathfrak{b}_k \subset \mathfrak{b}_{k-1} \subset \ldots \subset \mathfrak{b}_0$ eine Kompositionsreihe von S. Also ist S artinsch. ▫

Lemma 157 *Sei S noethersch. Sei* $\mathrm{Krdim}(S) = 0$. *Dann ist S artinsch.*

Beweis. Annahme, es ist S nicht artinsch. Dann ist die Menge

$$\{\, \mathfrak{a} \in \mathrm{Ideale}(S) :\ S/\mathfrak{a} \text{ ist nicht artinsch} \,\} \neq \emptyset\ .$$

Sei $\mathfrak{b}$ darin maximal; cf. Aufgabe 12.

Wir behaupten, daß $\mathfrak{b}$ ein Primideal ist. Annahme nicht. Dann können wir $s,\, t \in S \smallsetminus \mathfrak{b}$ wählen mit $st \in \mathfrak{b}$.

Wir haben die surjektive S-lineare Abbildung $h\colon S/\mathfrak{b} \to S/(\mathfrak{b}+(s))\colon x+\mathfrak{b} \mapsto x+(\mathfrak{b}+(s))$; cf. Aufgabe **??**.(2).

Die S-lineare Abbildung $g\colon S/(\mathfrak{b} : (s)) \to S/\mathfrak{b}\colon x + (\mathfrak{b} : (s)) \mapsto xs + \mathfrak{b}$ ist wohldefiniert und injektiv, denn für $x \in S$ ist genau dann $x + (\mathfrak{b} : (s)) = 0$, wenn $xs + \mathfrak{b} = 0$ ist; cf. Aufgabe **??**.(2).

Es ist der Kern von h gleich $(\mathfrak{b} + (s))/\mathfrak{b}$, also gleich dem Bild von g. Wir haben also die kurz exakte Sequenz

$$S/(\mathfrak{b} : (s)) \ \xrightarrow{g}\ S/\mathfrak{b} \ \xrightarrow{h}\ S/(\mathfrak{b} + (s))\ .$$

Es ist $t \in (\mathfrak{b} : (s)) \smallsetminus \mathfrak{b}$. Also ist $\mathfrak{b} \subset (\mathfrak{b} : (s))$ und somit $S/(\mathfrak{b} : (s))$ artinsch. Folglich hat $S/(\mathfrak{b} : (s))$ eine Kompositionsreihe, auch als S-Modul.

Es ist $s \in (\mathfrak{b} + (s)) \smallsetminus \mathfrak{b}$. Also ist $\mathfrak{b} \subset \mathfrak{b} + (s)$ und somit $S/(\mathfrak{b} + (s))$ artinsch. Folglich hat $S/(\mathfrak{b} + (s))$ eine Kompositionsreihe, auch als S-Modul.

Daher hat auch $S/\mathfrak{b}$ eine Kompositionsreihe als S-Modul und daher auch als $S/\mathfrak{b}$-Modul; cf. Bemerkung 153. I.e. es ist $S/\mathfrak{b}$ artinsch. Wir haben einen Widerspruch.

Also ist $\mathfrak{b}$ prim. Da $\mathrm{Krdim}(S) = 0$ ist, ist $\mathfrak{b}$ ein maximales Ideal. Folglich ist $S/\mathfrak{b}$ ein Körper und damit artinsch. Wir haben einen *Widerspruch.* ▫

2.4.5 Krulls Höhensatz

Sei S noethersch.

Wir erinnern daran, daß jede Faktoralgebra und jede Quotientenalgebra von S noethersch ist; cf. Aufgaben **??**.(2) und **??**.

Lemma 158 *Sei S lokal. Sei $\mathfrak{m} \subset S$ das maximale Ideal.*

Es ist $\bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \mathfrak{m}^i = (0)$.

Beweis. Sei $\mathfrak{a} := \bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \mathfrak{m}^i$. Da S noethersch ist, ist $\mathfrak{a}$ ein endlich erzeugter S-Modul. Es genügt also, $\mathfrak{m}\mathfrak{a} \overset{!}{=} \mathfrak{a}$ zu zeigen; cf. Lemma 127.

Schreibe $\mathfrak{m}\mathfrak{a} = \mathfrak{q}_0 \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$ für ein $k \in \mathbf{Z}_{\geqslant 0}$ und Primärideale $\mathfrak{q}_i \subseteq S$ für $i \in [0, k]$; cf. Satz 63. Sei hierbei $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ für $i, j \in [0, k]$ mit $i \neq j$; cf. Aufgabe **??**. O.E. ist $\sqrt{\mathfrak{q}_0} = \mathfrak{m}$, denn taucht $\mathfrak{m}$ nicht unter den Radikalen der Teilnehmer des Schnitts auf, dann kann $\mathfrak{m}$ selbst als Teilnehmer hinzugefügt werden. Dann ist $\sqrt{\mathfrak{q}_i} \subset \mathfrak{m}$ für $i \in [1, k]$. Wähle $x_i \in \mathfrak{m} \smallsetminus \sqrt{\mathfrak{q}_i}$ für $i \in [1, k]$.

Es ist $\mathfrak{m} = \sqrt{\mathfrak{q}_0}$. Da S noethersch ist, ist $\mathfrak{m}$ endlich erzeugt. Also gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ mit $\mathfrak{m}^n \subseteq \mathfrak{q}_0$. Also ist $\mathfrak{a} \subseteq \mathfrak{m}^n \subseteq \mathfrak{q}_0$.

Sei $i \in [1, k]$. Sei $a \in \mathfrak{a}$. Es ist $a x_i \in \mathfrak{a}\mathfrak{m} \subseteq \mathfrak{q}_i$. Da $\mathfrak{q}_i$ primär ist und $x_i \notin \sqrt{\mathfrak{q}_i}$ liegt, folgt $a \in \mathfrak{q}_i$. Also ist $\mathfrak{a} \subseteq \mathfrak{q}_i$.

Es folgt $\mathfrak{a} \subseteq \mathfrak{q}_0 \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k = \mathfrak{m}\mathfrak{a}$. Also ist $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$. ▫

Bemerkung 159 *Sei $\mathfrak{q}$ ein Primärideal von T. Dann ist $f^{-1}(\mathfrak{q})$ ein Primärideal von S.*

Beweis. Es ist $S/f^{-1}(\mathfrak{q}) \to T/\mathfrak{q}\colon s + f^{-1}(\mathfrak{q}) \mapsto f(s) + \mathfrak{q}$ ein injektiver R-Algebrenmorphismus; cf. Aufgabe 8.(3).

Da $\mathfrak{q}$ primär ist, ist $T/\mathfrak{q}$ fast integer. Folglich ist auch $S/f^{-1}(\mathfrak{q})$, isomorph zu einer Teilalgebra von $T/\mathfrak{q}$, fast integer. Also ist $f^{-1}(\mathfrak{q})$ primär.

Cf. Definitionen 32.(4) und 33.(3). ▫

Bemerkung 160 (und Definition) *Sei $\mathfrak{p} \in \operatorname{Spec}(S)$. Sei $k \in \mathbf{Z}_{\geqslant 1}$.*

Wir schreiben $N := S \smallsetminus \mathfrak{p}$. Sei $\mathfrak{p}^{(k)} := \lambda_{S,N}^{-1}(\mathfrak{p}_{\mathfrak{p}}^k) \subseteq S$.

Die folgenden Aussagen $(1, 2, 3, 4)$ gelten.

(1) *Es ist $\mathfrak{p}^{(k)}$ primär.*

(2) *Es ist $\mathfrak{p}^k \subseteq \mathfrak{p}^{(k)}$.*

(3) *Es ist $\mathfrak{p}^{(k)} \supseteq \mathfrak{p}^{(k+1)}$.*

(4) *Es ist $\sqrt{\mathfrak{p}^{(k)}} = \mathfrak{p}$.*

Beweis.

Ad (1). Dank Bemerkung 159 genügt es zu zeigen, daß $\mathfrak{p}_{\mathfrak{p}}^k$ primär ist. Es ist $\mathfrak{p}_{\mathfrak{p}} \subset S_{\mathfrak{p}}$ maximal; cf. Bemerkung 74. Also ist $\mathfrak{p}_{\mathfrak{p}}^k$ in der Tat primär; cf. Bemerkung 44.

Ad $(2,3)$. Dies ist nach Konstruktion gegeben.

Ad (4). Es ist $\mathfrak{p}^{(1)} = \lambda_{S,N}^{-1}(\mathfrak{p}_{\mathfrak{p}}) = \mathfrak{p}$; cf. Bemerkung 69.(1). Also ist

$$\sqrt{\mathfrak{p}^{(k)}} \overset{(3)}{\subseteq} \sqrt{\mathfrak{p}^{(1)}} = \sqrt{\mathfrak{p}} = \mathfrak{p} \; ;$$

cf. Bemerkung 43.(2).

Sei umgekehrt $x \in \mathfrak{p}$. Wir haben $x \overset{!}{\in} \sqrt{\mathfrak{p}^{(k)}}$ zu zeigen. Es genügt also zu zeigen, daß $x^k \overset{!}{\in} \mathfrak{p}^{(k)}$ liegt. Aber in der Tat ist $x^k \in \mathfrak{p}^k \overset{(2)}{\subseteq} \mathfrak{p}^{(k)}$. ▫

Definition 161 Sei $\mathfrak{p} \in \operatorname{Spec}(S)$. Sei $\mathfrak{a} \in \operatorname{Ideale}(S)$.

Wir sagen, es ist $\mathfrak{p}$ *minimal über* $\mathfrak{a}$, wenn $\mathfrak{p}$ ein minimales Element ist von

$$\{\, \mathfrak{q} \in \operatorname{Spec}(S) : \; \mathfrak{a} \subseteq \mathfrak{q} \,\} \; .$$

Lemma 162 *Sei* $x \in S$. *Sei* $\mathfrak{p} \in \operatorname{Spec}(S)$ *minimal über* (x).

Dann ist $\operatorname{ht}(\mathfrak{p}) \leqslant 1$.

Beweis. Annahme, es ist $\operatorname{ht}(\mathfrak{p}) \geqslant 2$. Dann gibt es $\mathfrak{p}'' \subset \mathfrak{p}' \subset \mathfrak{p}$ in $\operatorname{Spec}(S)$.

Dann haben wir die Primideale $(0) \subset \rho_{S,\mathfrak{p}''}(\mathfrak{p}') \subset \rho_{S,\mathfrak{p}''}(\mathfrak{p})$ in $S/\mathfrak{p}''$, wobei $\rho_{S,\mathfrak{p}''}(\mathfrak{p})$ minimal ist über $(x + \mathfrak{p}'')$; cf. Aufgabe 10, Bemerkung 69.(2). Also ist o.E. $\mathfrak{p}'' = (0)$ und S integer.

Wir schreiben $N := S \smallsetminus \mathfrak{p}$. Dann gibt es Primideale $(0) \subset \mathfrak{p}'/\!\!/N \subset \mathfrak{p}/\!\!/N$ in $S/\!\!/N$, wobei $\mathfrak{p}/\!\!/N$ minimal ist über $(\frac{x}{1})$ zu enthalten; cf. Bemerkung 69.(1). Also ist o.E. S lokal und darin $\mathfrak{p}$ maximal; cf. Bemerkung 74.

Alles in allem dürfen wir o.E. annehmen, es ist S integer und lokal mit maximalem Ideal $\mathfrak{p}$, es ist $\mathfrak{p}$ minimal über (x), es ist $\mathfrak{p}'' = (0)$ und es ist $\mathfrak{p}' \in \operatorname{Spec}(S)$ mit $(0) \subset \mathfrak{p}' \subset \mathfrak{p}$ gegeben.

Sei $\mathfrak{q} \in \operatorname{Spec}(S)$ mit $x \in \mathfrak{q}$. Wegen S lokal ist $\mathfrak{q} \subseteq \mathfrak{p}$. Wegen der Minimalität von $\mathfrak{p}$ über (x) folgt $\mathfrak{q} = \mathfrak{p}$. Insbesondere ist $x \not\in \mathfrak{p}'$.

Es ist $\operatorname{Spec}(S/(x)) = \{\rho_{S,(x)}(\mathfrak{p})\}$; cf. Bemerkung 69.(2). Insbesondere ist $\operatorname{Krdim}(S/(x)) = 0$. Also ist $S/(x)$ artinsch; cf. Lemma 157. Somit können wir ein $n_0 \in \mathbf{Z}_{\geqslant 1}$ wählen mit $\rho_{S,(x)}(\mathfrak{p}'^{(n)} + (x)) = \rho_{S,(x)}(\mathfrak{p}'^{(n+1)} + (x))$ für $n \in \mathbf{Z}_{\geqslant n_0}$; cf. Bemerkung 156.

Daher ist $\mathfrak{p}'^{(n)} + (x) = \mathfrak{p}'^{(n+1)} + (x)$; cf. Bemerkung 69.(2). I.e. $\mathfrak{p}'^{(n)} \subseteq \mathfrak{p}'^{(n+1)} + (x)$.

Sei $y \in \mathfrak{p}'^{(n)}$ gegeben. Wir können $y = z + sx$ schreiben mit $z \in \mathfrak{p}'^{(n+1)}$ und $s \in S$. Also ist $sx = y - z \in \mathfrak{p}'^{(n)}$; cf. Bemerkung 160.(3). Nun ist aber $x \not\in \mathfrak{p}' = \sqrt{\mathfrak{p}'^{(n)}}$; cf. Bemerkung 160.(4). Da $\mathfrak{p}'^{(n)}$ primär ist gemäß Bemerkung 160.(1), folgt $s \in \mathfrak{p}'^{(n)}$. Also ist $y = z + sx \in \mathfrak{p}'^{(n+1)} + \mathfrak{p}'^{(n)}(x)$.

Daher ist $\mathfrak{p}'^{(n)} \subseteq \mathfrak{p}'^{(n+1)} + \mathfrak{p}'^{(n)}(x)$ und also $\mathfrak{p}'^{(n)} = \mathfrak{p}'^{(n+1)} + \mathfrak{p}'^{(n)}(x)$.

Für den endlich erzeugten S-Modul $M := \mathfrak{p}'^{(n)}/\mathfrak{p}'^{(n+1)}$ heißt dies, es ist $xM = M$. Da $x \in \mathrm{Jac}(S) = \mathfrak{p}$, folgt $\mathrm{Jac}(S)M = M$. Also ist $M = 0$; cf. Lemma 127.

Mit anderen Worten, es ist $\mathfrak{p}'^{(n)} = \mathfrak{p}'^{(n+1)}$ für $n \in \mathbf{Z}_{\geqslant n_0}$. Also ist $\bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \mathfrak{p}'^{(i)} = \mathfrak{p}'^{(n_0)}$.

Sei $N' := S \smallsetminus \mathfrak{p}'$. Da S integer ist, ist $\lambda_{S,N'} \colon S \to S/\!\!/N' = S_{\mathfrak{p}'}$ injektiv. Es ist

$$\lambda_{S,N'}\left(\bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \mathfrak{p}'^{(i)}\right) \subseteq \bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \lambda_{S,N'}(\mathfrak{p}'^{(i)}) \subseteq \bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \mathfrak{p}'^{\,i}_{\mathfrak{p}'} = (0)$$

dank Lemma 158; cf. Bemerkung 74. Also ist auch $\mathfrak{p}'^{(n_0)} = \bigcap_{i \in \mathbf{Z}_{\geqslant 1}} \mathfrak{p}'^{(i)} = (0)$.

Wähle $p' \in \mathfrak{p}'^{\times}$. Da S integer ist, ist $0 \neq p'^{n_0} \in \mathfrak{p}'^{n_0} \subseteq \mathfrak{p}'^{(n_0)} = (0)$; cf. Bemerkung 160.(2). Wir haben einen *Widerspruch.* ▫

Lemma 163 *Seien* $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \in \mathrm{Spec}(S)$ *mit* $\mathfrak{p}'' \subset \mathfrak{p}' \subset \mathfrak{p}$ *gegeben.*

Sei $x \in \mathfrak{p} \smallsetminus \mathfrak{p}'$ *gegeben.*

Dann gibt es ein $\tilde{\mathfrak{p}}' \in \mathrm{Spec}(S)$ *mit* $x \in \tilde{\mathfrak{p}}'$ *und* $\mathfrak{p}'' \subset \tilde{\mathfrak{p}}' \subset \mathfrak{p}$.

Beweis. O.E. ist S lokal und integer mit $\mathfrak{p}'' = (0)$ und mit maximalem Ideal $\mathfrak{p}$; cf. Bemerkung 69.

Es ist $(0) \subset (x) \subseteq \mathfrak{p} \subset S$. Also gibt es in ein $\tilde{\mathfrak{p}}' \in \mathrm{Spec}(S)$ minimal über (x); cf. Lemma 50. Es ist $(0) \subset \tilde{\mathfrak{p}}' \subseteq \mathfrak{p}$.

Es ist $\mathrm{ht}(\tilde{\mathfrak{p}}') \leqslant 1$; cf. Lemma 162. Es ist $\mathrm{ht}(\tilde{\mathfrak{p}}') \geqslant 2$ nach Voraussetzung. Daher ist $(0) \subset \tilde{\mathfrak{p}}' \subset \mathfrak{p}$. ▫

Lemma 164 *Sei* $\mathfrak{a} \in \mathrm{Ideale}(S)$. *Sei* $\ell \in \mathbf{Z}_{\geqslant 1}$. *Sei* $\mathfrak{p}_i \in \mathrm{Spec}(S)$ *für* $i \in [1, \ell]$.

Sei $\mathfrak{a} \subseteq \bigcup_{i \in [1,\ell]} \mathfrak{p}_i$.

Dann gibt es ein $j \in [1, \ell]$ *mit* $\mathfrak{a} \subseteq \mathfrak{p}_j$.

Beweis. O.E. können wir $\mathfrak{a} \not\subseteq \bigcup_{i \in [1,\ell] \smallsetminus \{k\}} \mathfrak{p}_i$ annehmen für $k \in [1, \ell]$.

Zu zeigen ist $\ell \overset{!}{=} 1$.

Annahme, $\ell \geqslant 2$. Wir wählen $a_j \in (\mathfrak{p}_j \cap \mathfrak{a}) \smallsetminus (\bigcup_{i \in [1,\ell] \smallsetminus \{j\}} \mathfrak{p}_i)$, was möglich ist, denn ansonsten *wäre* $\mathfrak{a} \subseteq \bigcup_{i \in [1,\ell] \smallsetminus \{j\}} \mathfrak{p}_i$, was *nicht* zutrifft.

Sei $I := \{\, i \in [3, \ell] : \ a_1 + a_2 \notin \mathfrak{p}_i \,\}$. Wir setzen

$$a \ := \ a_1 + a_2 + a_1 \cdot a_2 \cdot \prod_{i \in I} a_i \ .$$

Es ist $a \in \mathfrak{a}$.

Es ist $a \notin \mathfrak{p}_1$, da alle Summanden außer a_2 in $\mathfrak{p}_1$ liegen.

Es ist $a \notin \mathfrak{p}_2$, da alle Summanden außer a_1 in $\mathfrak{p}_2$ liegen.

Für $j \in I$ ist $a \notin \mathfrak{p}_j$, da der dritte Summand in $\mathfrak{p}_j$ liegt, nicht aber $a_1 + a_2$.

Für $j \in [3, \ell]$ ist zunächst kein Faktor des Produkts $a_1 \cdot a_2 \cdot \prod_{i \in I} a_i$ in $\mathfrak{p}_j$ enthalten. Da $\mathfrak{p}_j$ aber ein Primideal ist, folgt, daß auch $a_1 \cdot a_2 \cdot \prod_{i \in I} a_i \notin \mathfrak{p}_j$ liegt. Wohl aber liegt $a_1 + a_2 \in \mathfrak{p}_j$. Also ist $a \notin \mathfrak{p}_j$.

Insgesamt ist $a \in \mathfrak{a} \smallsetminus (\bigcup_{i \in [1,\ell]} \mathfrak{p}_i)$ und wir haben einen *Widerspruch.* ▫

Satz 165 (Krulls Höhensatz)

Wir erinnern daran, daß S eine noethersche kommutative R-Algebra ist mit $0_S \neq 1_S$.

Sei $\mathfrak{p} \in \operatorname{Spec}(S)$. *Es ist*

$\operatorname{ht}(\mathfrak{p}) \ =$

$\min\{ k \in \mathbf{Z}_{\geqslant 0} :$ es gibt ein von k Elementen erzeugtes Ideal $\mathfrak{a}$ in S mit $\mathfrak{p}$ minimal über $\mathfrak{a} \}$.

Beweis.

Ad ($\leqslant$). Sei $\mathfrak{a} = (x_1, \ldots, x_k)$, wobei $k \in \mathbf{Z}_{\geqslant 0}$ und $x_i \in S$ für $i \in [1, k]$. Sei $\mathfrak{p} \in \operatorname{Spec}(S)$ minimal über $\mathfrak{a}$. Zu zeigen ist $\operatorname{ht}(\mathfrak{p}) \overset{!}{\leqslant} k$.

Wir führen eine Induktion über k.

Ist $k = 0$, dann ist $\mathfrak{p}$ ein minimales Primideal von S und also von Höhe 0.

Sei $k \geqslant 1$. *Annahme,* es ist $\operatorname{ht}(\mathfrak{p}) \geqslant k + 1$.

Behauptung. Wir können $\mathfrak{p}_i \in \operatorname{Spec}(S)$ wählen für $i \in [0, k+1]$ mit

$$\mathfrak{p}_0 \ \subset \ \mathfrak{p}_1 \ \subset \ \ldots \ \subset \ \mathfrak{p}_{k+1} \ \subseteq \ \mathfrak{p}$$

und mit $x_1 \in \mathfrak{p}_1$.

Wegen $\operatorname{ht}(\mathfrak{p}) \geqslant k + 1$ gibt es $\mathfrak{p}_i \in \operatorname{Spec}(S)$ für $i \in [0, k+1]$ mit

$$\mathfrak{p}_0 \ \subset \ \mathfrak{p}_1 \ \subset \ \ldots \ \subset \ \mathfrak{p}_{k+1} \ \subseteq \ \mathfrak{p} \ .$$

Sei $j \in [1, k]$ minimal mit $x_1 \in \mathfrak{p}_j$.

Wir wählen nun $\mathfrak{p}_i \in \operatorname{Spec}(S)$ für $i \in [0, k+1]$ derart, daß j minimal wird.

Annahme, die Behauptung trifft nicht zu. Es ist $j \geqslant 2$. Es ist $x_1 \notin \mathfrak{p}_{j-1}$.

Dank Lemma 163, angewandt auf $\mathfrak{p}_{j-2} \subset \mathfrak{p}_{j-1} \subset \mathfrak{p}_j$, erhalten wir ein $\tilde{\mathfrak{p}}_{j-1} \in \operatorname{Spec}(S)$ mit $\mathfrak{p}_{j-2} \subset \tilde{\mathfrak{p}}_{j-1} \subset \mathfrak{p}_j$ und $x_1 \in \tilde{\mathfrak{p}}_{j-1}$. Dann steht aber

$$\mathfrak{p}_0 \ \subset \ \mathfrak{p}_1 \ \subset \ \ldots \ \subset \ \mathfrak{p}_{j-2} \ \subset \ \tilde{\mathfrak{p}}_{j-1} \ \subset \ \mathfrak{p}_j \ \subset \ \ldots \ \subset \ \mathfrak{p}_{k+1} \ \subseteq \ \mathfrak{p}$$

im Widerspruch zur Minimalität von j. Dies zeigt die *Behauptung*.

Wir schreiben $\bar{x} := s + \mathfrak{p}_1$ für $s \in S$. Wir schreiben $\bar{S} := S/\mathfrak{p}_1$. Wir schreiben $\bar{\mathfrak{a}} := \rho_{S,\mathfrak{p}_1}(\mathfrak{a})$ für $\mathfrak{a} \in \mathrm{Ideale}(S)$ mit $\mathfrak{p}_1 \subseteq \mathfrak{a}$.

Es ist $\mathfrak{b} := \mathfrak{p}_1 + \mathfrak{a} \subseteq \mathfrak{p}$, wobei $\mathfrak{p}$ dann auch minimal über $\mathfrak{b}$ ist.

Wegen $x_1 \in \mathfrak{p}_1$ ist $\bar{x}_1 = 0$. Also ist $\bar{\mathfrak{b}} = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_k) = (\bar{x}_2, \ldots, \bar{x}_k)$.

Ferner ist

$$(0) \;=\; \bar{\mathfrak{p}}_1 \;\subset\; \bar{\mathfrak{p}}_2 \;\subset\; \ldots \;\subset\; \bar{\mathfrak{p}}_{k+1} \;=\; \bar{\mathfrak{p}}$$

in $\mathrm{Spec}(\bar{S})$ und also $\mathrm{ht}(\bar{\mathfrak{p}}) \geqslant k$.

Aber es ist $\bar{\mathfrak{p}}$ minimal über $\bar{\mathfrak{b}}$; cf. Aufgabe 10, Bemerkung 69.(2). Dank Induktionsvoraussetzung folgt hieraus $\mathrm{ht}(\bar{\mathfrak{p}}) \leqslant k-1$.

Wir haben einen *Widerspruch.*

Ad ($\geqslant$). Sei $\mathfrak{p} \in \mathrm{Spec}(S)$ gegeben. Wir schreieben $k := \mathrm{ht}(\mathfrak{p})$. Wir haben zu zeigen, daß es Elemente $x_i \in \mathfrak{p}$ für $i \in [1,k]$ derart gibt, daß $\mathfrak{p}$ minimal über $(x_1, \ldots, x_k)$ ist.

Wir zeigen diese Behauptung mit Induktion über k.

Für $k = 0$ folgt aus $\mathrm{ht}(\mathfrak{p}) = 0$, daß $\mathfrak{p}$ ein minimales Primideal von S ist, i.e. es ist minimal über $(\,) = (0)$.

Sei $k \geqslant 1$. Seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell \in \mathrm{Spec}(S)$ die minimalen Primideale von S, die in $\mathfrak{p}$ enthalten sind, wobei $\ell \in \mathbf{Z}_{\geqslant 1}$; cf. Bemerkung 69.(1), Lemma 50, Satz 58.

Sei $i \in [1,\ell]$. Da $\mathrm{ht}(\mathfrak{p}) \geqslant 1$ und $\mathrm{ht}(\mathfrak{q}_i) = 0$, ist $\mathfrak{p} \not\subseteq \mathfrak{q}_i$.

Also ist $\mathfrak{p} \not\subseteq \bigcup_{i\in[1,\ell]} \mathfrak{q}_i$; cf. Lemma 164. Wir wählen $x_1 \in \mathfrak{p} \smallsetminus (\bigcup_{i\in[1,\ell]} \mathfrak{q}_i)$.

Wir schreibe $\bar{S} := S/(x_1)$. Für $s \in S$ schreiben wir $\bar{s} := \rho_{S,(x_1)}(s) = s + (x_1) \in \bar{S}$. Für $\mathfrak{b} \in \mathrm{Ideale}(S)$ mit $x_1 \in \mathfrak{b}$ schreiben wir $\bar{\mathfrak{b}} := \rho_{S,(x_1)}(\mathfrak{b}) \in \mathrm{Ideale}(\bar{S})$.

Es ist $\mathrm{ht}(\bar{\mathfrak{p}}) \leqslant \mathrm{ht}(\mathfrak{p}) = k$; cf. Bemerkung 69.(2).

Wir *behaupten* $\mathrm{ht}(\bar{\mathfrak{p}}) \overset{!}{\leqslant} k-1$. *Annahme,* es ist $\mathrm{ht}(\bar{\mathfrak{p}}) = k$. Dann gibt es Primideale $\mathfrak{p}_i \in \mathrm{Spec}(S)$ mit $x_1 \in \mathfrak{p}_i$ für $i \in [0,k]$ und mit $\bar{\mathfrak{p}}_0 \subset \bar{\mathfrak{p}}_1 \subset \ldots \subset \bar{\mathfrak{p}}_k \subseteq \bar{\mathfrak{p}}$. Mit anderen Worten, es ist $(x_1) \subseteq \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k \subseteq \mathfrak{p}$. Cf. Bemerkung 69.(2). Da $k = \mathrm{ht}(\mathfrak{p})$, ist $\mathfrak{p}_0$ ein minimales Primideal in S. Dann aber ist $x_1 \notin \mathfrak{p}_0$ nach Wahl von x_1. Wir haben einen *Widerspruch.*

Nach Induktion finden wir Elemente $x_i \in S$ für $i \in [2,k]$ mit $\bar{\mathfrak{p}}$ minimal über $(\bar{x}_2, \ldots, \bar{x}_k)$. Also ist $\rho^{-1}_{S,(x_1)}(\bar{\mathfrak{p}}) = \mathfrak{p}$ minimal über $\rho^{-1}_{S,(x_1)}(\,(\bar{x}_2, \ldots, \bar{x}_k)\,) = (x_1, x_2, \ldots, x_k)$; cf. Aufgabe 10, Bemerkung 69.(2). ▫

Korollar 166 *Wir erinnern an S noethersch.*

Sei $\mathfrak{p} \in \mathrm{Spec}(S)$. *Es ist* $\mathrm{ht}(\mathfrak{p}) = \mathrm{Krdim}(S_\mathfrak{p})$ *endlich.*

Beweis. Dies folgt aus Satz 165 wegen $\mathfrak{p}$ minimal über $\mathfrak{p}$ selbst und wegen $\mathfrak{p}$ endlich erzeugt. $\square$

2.4.6 Krulldimension und Polynomalgebra

Sei S noethersch.

Dagegen ist T nicht als noethersch vorausgesetzt.

Bemerkung 167 (und Definition) Für $\mathfrak{a} \in \mathrm{Ideale}(T)$ schreiben wir

$$\mathfrak{a}[X] \;:=\; \{\, g(X) = \sum_{i \geqslant 0} t_i X^i : \text{ es ist } t_i \in \mathfrak{a} \text{ für } i \in \mathbf{Z}_{\geqslant 0} \,\} \,.$$

(1) Wir haben den T-Algebrenisomorphismus

$$\begin{array}{rcl} T[X]/\mathfrak{a}[X] & \overset{\sim}{\longleftrightarrow} & (T/\mathfrak{a})[X] \\ (\sum_{i\geqslant 0} t_i X^i) + \mathfrak{a}[X] & \mapsto & \sum_{i\geqslant 0}(t_i + \mathfrak{a})X^i \\ (\sum_{i\geqslant 0} t_i X^i) + \mathfrak{a}[X] & \leftarrow\!\shortmid & \sum_{i\geqslant 0}(t_i + \mathfrak{a})X^i \;; \end{array}$$

cf. Lemma 20, Bemerkung 26. Insbesondere folgt aus $\mathfrak{a}$ prim, daß $\mathfrak{a}[X]$ prim ist; cf. Bemerkung 22.

(2) Wir haben den T-Algebrenisomorphismus

$$\begin{array}{rcl} T[X]/(\mathfrak{a}[X] + (X)) & \overset{\sim}{\longleftrightarrow} & T/\mathfrak{a} \\ (\sum_{i\geqslant 0} t_i X^i) + (\mathfrak{a}[X] + (X)) & \mapsto & t_0 + \mathfrak{a} \\ t + (\mathfrak{a}[X] + (X)) & \leftarrow\!\shortmid & t + \mathfrak{a} \;; \end{array}$$

cf. Lemma 20, Bemerkung 26. Insbesondere folgt aus $\mathfrak{a}$ prim, daß $\mathfrak{a}[X] + (X)$ prim ist.

Lemma 168 *Seien* $\mathfrak{q}$, $\mathfrak{q}' \in \mathrm{Spec}(T[X])$ *gegeben mit* $\mathfrak{q}' \subset \mathfrak{q}$ *und* $\mathfrak{q}' \cap T = \mathfrak{q} \cap T =: \mathfrak{p}$.

Dann ist $\mathfrak{q}' = \mathfrak{p}[X]$.

Beweis. Wir schreiben $\bar{T} := T/\mathfrak{p}$. Wir schreiben $\bar{t} := t + \mathfrak{p}$ für $t \in T$.

Sei $\varphi\colon T[X]/\mathfrak{p}[X] \xrightarrow{\sim} \bar{T}[X]\colon X + \mathfrak{p}[X] \mapsto X$; cf. Bemerkung 167.(1).

Wir schreiben $\bar{\mathfrak{a}} := \varphi(\rho_{T[X],\mathfrak{p}[X]}(\mathfrak{a}))$ für $\mathfrak{a} \in \mathrm{Ideale}(T[X])$ mit $\mathfrak{p}[X] \subseteq \mathfrak{a}$.

Es ist $\mathfrak{p}[X] \subseteq \mathfrak{q}' \subset \mathfrak{q}$.

Annahme, es ist $\mathfrak{p}[X] \subset \mathfrak{q}' \subset \mathfrak{q}$. Dann ist $(0) \subset \bar{\mathfrak{q}}' \subset \bar{\mathfrak{q}}$ in $\mathrm{Spec}(\bar{T}[X])$; cf. Bemerkung 69.(2). Es ist $\bar{\mathfrak{q}}' \cap \bar{T} = \bar{\mathfrak{q}} \cap \bar{T} = (0)$, da in $\mathfrak{q}'$ wie in $\mathfrak{q}$ alle Polynome von Grad 0 bereits in $\mathfrak{p}$ liegen.

Es ist $\bar{N} := \bar{T}^\times \subseteq \bar{T} \subseteq \bar{T}[X]$ eine multiplikative Teilmenge. Es ist $\operatorname{Quot}(\bar{T}) = \bar{T}/\!\!/\bar{N}$. Wir haben den $\bar{T}$-Algebrenisomorphismus

$$\begin{array}{rcl} \bar{T}[X]/\!\!/\bar{N} & \overset{\sim}{\longleftrightarrow} & (\bar{T}/\!\!/\bar{N})[X] \\ \frac{\sum_{i\geqslant 0} \bar{t}_i X^i}{\bar{n}} & \mapsto & (\sum_{i\geqslant 0} \frac{\bar{t}_i}{1} X^i) \cdot \bar{n}^- \\ \sum_{i\geqslant 0} \bar{t}_i \cdot \bar{n}_i^- X^i & \leftarrow\!\shortmid & \sum_{i\geqslant 0} \frac{\bar{t}_i}{\bar{n}_i} X^i \ ; \end{array}$$

cf. Lemmata 20 und 67.

Es ist $\bar{\mathfrak{q}} \cap \bar{N} = \emptyset$. Also haben wir $(0) \subset \bar{\mathfrak{q}}'/\!\!/\bar{N} \subset \bar{\mathfrak{q}}/\!\!/\bar{N}$ in $\operatorname{Spec}(\bar{T}[X]/\!\!/\bar{N})$; cf. Bemerkung 69.(1).

Dies aber steht im *Widerspruch* zu $\operatorname{Krdim}(\bar{T}[X]/\!\!/\bar{N}) = \operatorname{Krdim}(\operatorname{Quot}(\bar{T})[X]) = 1$; cf. Beispiel 143.(2). ▫

Lemma 169 *Sei* $\mathfrak{p} \in \operatorname{Spec}(S)$. *Es ist* $\operatorname{ht}(\mathfrak{p}[X]) = \operatorname{ht}(\mathfrak{p})$.

Beweis. Wir schreiben $k := \operatorname{ht}(\mathfrak{p})$.

Ad ($\geqslant$). Seien $\mathfrak{p}_i \in \operatorname{Spec}(S)$ gewählt für $i \in [0,k]$ mit $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k \subseteq \mathfrak{p}$.

Zu zeigen ist $\operatorname{ht}(\mathfrak{p}[X]) \overset{!}{\geqslant} k$. In $\operatorname{Spec}(S[X])$ haben wir dank Bemerkung 167.(1) aber

$$\mathfrak{p}_0[X] \ \subset\ \mathfrak{p}_1[X] \ \subset\ \ldots\ \subset\ \mathfrak{p}_k[X] \ \subseteq\ \mathfrak{p}[X] \ .$$

Ad ($\leqslant$). Wir wählen $s_1, \ldots, s_k \in S$ mit $\mathfrak{p}$ in S minimal über $\mathfrak{a} := (s_1, \ldots, s_k)$; cf. Satz 165.

Es genügt zu zeigen, daß $\mathfrak{p}[X]$ in $S[X]$ minimal über $\mathfrak{a}[X] = (s_1, \ldots, s_k)$ ist; cf. Satz 165.

Annahme, es gibt $\mathfrak{q} \in \operatorname{Spec}(S[X])$ mit $\mathfrak{a}[X] \subseteq \mathfrak{q} \subset \mathfrak{p}[X]$.

Dann aber ist $\mathfrak{a} = \mathfrak{a}[X] \cap S \subseteq \mathfrak{q} \cap S \subseteq \mathfrak{p}[X] \cap S = \mathfrak{p}$, wegen der Minimalität von $\mathfrak{p}$ über $\mathfrak{a}$ also $\mathfrak{q} \cap S = \mathfrak{p}$. Dank Lemma 168 folgt hieraus $\mathfrak{q} = \mathfrak{p}[X]$. Wir haben einen *Widerspruch*. ▫

Lemma 170 *Sei* $\operatorname{Krdim}(S)$ *endlich.*

Dann ist $\operatorname{Krdim}(S[X]) = \operatorname{Krdim}(S) + 1$.

Beweis.

Ad ($\geqslant$). Wir schreiben $k := \operatorname{Krdim}(S)$. Zu zeigen ist $\operatorname{Krdim}(S[X]) \overset{!}{\geqslant} k + 1$.

Seien $\mathfrak{p}_i \in \operatorname{Spec}(S)$ gewählt für $i \in [0,k]$ mit $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k$.

In $\operatorname{Spec}(S[X])$ haben wir dank Bemerkung 167.(1, 2) aber

$$\mathfrak{p}_0[X] \ \subset\ \mathfrak{p}_1[X] \ \subset\ \ldots\ \subset\ \mathfrak{p}_k[X] \ \subset\ \mathfrak{p}_k[X] + (X) \ .$$

Ad ($\leqslant$). Sei $\ell \in \mathbf{Z}_{\geqslant 0}$ und sei $\mathfrak{q}_i \in \operatorname{Spec}(S[X])$ für $i \in [0, k]$ mit $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_\ell$.

Zu zeigen ist $\ell \overset{!}{\leqslant} \operatorname{Krdim}(S) + 1$, i.e. $\operatorname{Krdim}(S) \overset{!}{\geqslant} \ell - 1$.

Wir schreiben $\mathfrak{p}_i := \mathfrak{q}_i \cap S$ für $i \in [0, \ell]$. Es ist $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_\ell$.

Fall: Es ist $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_\ell$. Dann ist $\operatorname{Krdim}(S) \geqslant \ell \geqslant \ell - 1$.

Fall: Es gibt ein $j \in [1, \ell]$ *mit* $\mathfrak{p}_{j-1} = \mathfrak{p}_j$.

Wähle j damit maximal. Es ist also $\mathfrak{p}_j \subset \mathfrak{p}_{j+1} \subset \ldots \subset \mathfrak{p}_\ell$.

Dank Lemma 168 ist $\mathfrak{p}_{j-1}[X] = \mathfrak{q}_{j-1}$.

Nun ist

$$j - 1 \;\leqslant\; \operatorname{ht}(\mathfrak{q}_{j-1}) \;=\; \operatorname{ht}(\mathfrak{p}_{j-1}[X]) \;=\; \operatorname{ht}(\mathfrak{p}_{j-1})$$

gemäß Lemma 169.

Also gibt es $\mathfrak{p}'_i \in \operatorname{Spec}(S)$ für $i \in [0, j-1]$ mit $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_{j-1} \subseteq \mathfrak{p}_{j-1}$.

Insbesondere ist $\mathfrak{p}'_{j-1} \subseteq \mathfrak{p}_{j-1} = \mathfrak{p}_j \subset \mathfrak{p}_{j+1}$.

Insgesamt haben wir also

$$\mathfrak{p}'_0 \;\subset\; \mathfrak{p}'_1 \;\subset\; \ldots \;\subset\; \mathfrak{p}'_{j-1} \;\subset\; \mathfrak{p}_{j+1} \;\subset\; \mathfrak{p}_{j+2} \;\subset\; \ldots \;\subset \mathfrak{p}_\ell$$

in $\operatorname{Spec}(S)$. Somit ist $\operatorname{Krdim}(S) \geqslant \ell - 1$. □

Satz 171 (Krulldimension der Polynomalgebra)

Wir erinnern daran, daß S noethersch ist mit $0_S \neq 1_S$.

Sei $\operatorname{Krdim}(S)$ *endlich. Sei* $k \in \mathbf{Z}_{\geqslant 0}$.

Dann ist $\operatorname{Krdim}(S[X_1, \ldots, X_k]) = \operatorname{Krdim}(S) + k$.

Beweis. Dies folgt mit iterierter Anwendung von Lemma 170; cf. Satz 56.

Anhang A

Anhang

Wir folgen im wesentlichen [**7,** Ch. 1, §6].

A.1 Zorn

Erinnerung 172 Sei an folgende Begriffe erinnert.

(1) Das *Auswahlaxiom* besagt, daß es für jede surjektive Abbildung $U \xrightarrow{f} V$ zwischen Mengen U und V eine Abbildung $U \xleftarrow{s} V$ mit $f \circ s = \mathrm{id}_V$ gibt.

(2) In einem Poset X heißen Elemente $x,\ y \in X$ *vergleichbar*, wenn $x \leqslant y$ oder $y \leqslant x$ ist.

Ein Poset X heißt *linear* geordnet, wenn für $x,\ y \in X$ stets x vergleichber zu y ist.

(3) Eine Teilmenge K eines Posets X heißt *Kette*, wenn sie linear geordnet ist.

Die Menge aller Ketten in X werde mit $\mathrm{Chain}(X)$ bezeichnet. Es ist $\mathrm{Chain}(X)$, zusammen mit $(\subseteq)$, ein Poset.

(4) Eine Teilmenge Y eines Posets hat ein Element $s \in X$ als *obere Schranke*, wenn $y \leqslant s$ ist für $y \in Y$.

(5) Für ein Poset X und ein Element $x \in X$ schreiben wir $X_{<x} := \{\, y \in X :\ y < x \,\}$ und $X_{\leqslant x} := \{\, y \in X :\ y \leqslant x \,\}$.

(6) Ein $(\leqslant)$-*Abschnitt* eines Posets $X = (X, \leqslant)$ ist eine Teilmenge Y mit der Eigenschaft, daß für $y \in Y$ auch $X_{<y} \subseteq Y$ liegt.

(7) Ein linear geordnetes Poset X heißt *wohlgeordnet*, wenn jede nichtleere Teilmenge $Y \subseteq X$ ein minimales Element m besitzt. Dieses ist dann auch initial, denn ist $y \in Y$, dann ist nicht $y < m$, also $m \leqslant y$.

Insbesondere liegt es eindeutig fest, und wir können $m =: \min(Y)$ schreiben.

(8) Ist M eine Menge und $(\leqslant) \subseteq M \times M$ eine Teilmenge derart, daß $(M, \leqslant)$ ein wohlgeordnetes Poset ist, dann heißt $(\leqslant)$ eine *Wohlordnung* auf M.

Bemerkung 173

(1) Sei $\mathcal{X}$ eine Menge, die aus nichtleeren Mengen besteht.

Wir bilden
$$\hat{\mathcal{X}} := \{ (X, x) : X \in \mathcal{X} \text{ und } x \in X \} .$$
Wir haben die surjektive Abbildung
$$\begin{array}{rcl} \hat{\mathcal{X}} & \xrightarrow{f} & \mathcal{X} \\ (X, x) & \mapsto & X , \end{array}$$
wobei die Surjektivität aus $X \neq \emptyset$ für $X \in \mathcal{X}$ folgt.

Dank Auswahlaxiom gibt es eine Abbildung $\hat{\mathcal{X}} \xleftarrow{s} \mathcal{X}$ mit $f \circ s = \mathrm{id}_{\mathcal{X}}$. Mit anderen Worten, für $X \in \mathcal{X}$ ist $s(X) = (X, x)$ für ein $x \in X$.

(2) Besteht in der Situation von (1) nun $\mathcal{X}$ aus nichtleeren Teilmengen einer Menge M, so haben wir auch eine Abbildung
$$\begin{array}{rcl} \hat{\mathcal{X}} & \xrightarrow{t} & M \\ (X, x) & \mapsto & x . \end{array}$$
Somit ist $f := t \circ s$ eine Abbildung von $\mathcal{X}$ nach M, für welche $f(X) \in X$ liegt für $X \in \mathcal{X}$.

Bemerkung 174 (Induktionsprinzip)

Sei $X = (X, \leqslant)$ ein Poset. Habe jede nichtleere Teilmenge von X ein minimales Element.

Sei $f \colon X \to \{0, 1\}$ eine Abbildung.

Erfülle f die folgende Eigenschaft.

Ist $x \in X$ und $f(s) = 1$ für $s \in X_{<x}$, dann ist $f(x) = 1$.

Dann ist $f(x) = 1$ für alle $x \in X$.

Beweis. Annahme, es gibt ein $x \in X$ mit $f(x) = 0$. Sei $m \in X$ minimal mit $f(m) = 0$. Dann ist $f(s) = 1$ für $s \in X_{<m}$. Folglich ist $f(m) = 1$. Wir haben einen Widerspruch. ▫

Bemerkung 175 Sei $X = (X, \leqslant)$ ein wohlgeordnetes Poset.

Sei $Y \subset X$ ein $(\leqslant)$-Abschnitt. Dann ist $Y = X_{<\min(X \smallsetminus Y)}$.

Beweis. Schreibe $m := \min(X \smallsetminus Y)$.

Ad $(\supseteq)$. Sei $x \in X$ mit $x < m$ gegeben. *Annahme,* es ist $x \in X \smallsetminus Y$. Dann ist $m \leqslant x$, im *Widerspruch* zu $x < m$.

Ad $(\subseteq)$. Sei $y \in Y$. *Annahme*, es ist nicht $y < m$. Dann ist $y \geqslant m$. Da Y ein $(\leqslant)$-Abschnitt ist, folgt $m \in Y$, im *Widerspruch* zu $m \in X \smallsetminus Y$. ▫

Lemma 176 *Sei M eine Menge. Es gibt eine Wohlordnung $(\leqslant) \subseteq M \times M$ auf M.*

Beweis. Ohne Einschränkung ist $M \neq \emptyset$.

Sei $P := \{\, X \subseteq M : \; X \neq \emptyset \,\}$. Wähle eine Abbildung $f : P \to M$ mit $f(X) \in X$; cf. Bemerkung 173.(2).

Ist $X \in P$ und ist $W \subseteq X \times X$ eine Wohlordnung auf X, so schreiben wir

$$X_{W,<x} := \{\, y \in X : \; (y, x) \in W \text{ und } y \neq x \,\} \; .$$

Beachte $x \in M \smallsetminus X_{W,<x}$. Sei

$$\begin{aligned} E := \{(X, W) : \text{es ist } X \in P \text{ und } W \text{ eine Wohlordnung auf } X \text{ derart,} \\ \text{daß } f(M \smallsetminus X_{W,<x}) = x \text{ ist für alle } x \in X.\} \end{aligned}$$

Die Elemente von E werden als *erledigte* bezeichnet.

Behauptung 1. Seien (X, W), $(X', W') \in E$. Wir behaupten, daß

$$X \text{ ein } W'\text{-Abschnitt in } X' \text{ und } W = W' \cap (X \times X) \text{ ist}$$

oder

$$X' \text{ ein } W\text{-Abschnitt in } X \text{ und } W' = W \cap (X' \times X') \text{ ist.}$$

Sei

$$B := \bigcup \left\{ A \subseteq X \cap X' : \begin{array}{l} \text{es ist } A \text{ ein } W\text{-Abschnitt in } X \text{ und ein } W'\text{-Abschnitt in } X', \\ \text{und es ist } W \cap (A \times A) = W' \cap (A \times A) \end{array} \right\} .$$

Es ist $B \subseteq X \cap X'$.

Es ist B ein W-Abschnitt in X, denn ist $b \in B$ und $x \in X_{W,<b}$ gegeben, dann gibt es einen W-Abschnitt A in X mit $b \in A \subseteq B$, was $x \in A \subseteq B$ nach sich zieht.

Genauso ist B auch ein W'-Abschnitt in X'.

Vorbemerkung.

(1) Sei $(s,t) \in W$ mit $t \in B$. Dann gibt es ein $A \subseteq X \cap X'$ so, daß A ein W-Abschnitt in X ist, daß $W \cap (A \times A) = W' \cap (A \times A)$ gilt und daß $t \in A$. Da $(s,t) \in W$ liegt und da A ein W-Abschnitt in X ist, ist auch $s \in A$. Es folgt $(s,t) \in W \cap (A \times A) = W' \cap (A \times A) \subseteq W'$.

(2) Wegen Symmetrie folgt auch aus $(s,t) \in W'$ mit $t \in B$, daß $(s,t) \in W$ liegt.

Annahme, es ist $B \subset X$ und $B \subset X'$.

Sei $m_X := \min(X \smallsetminus B)$, gebildet bezüglich W. Es ist $B = X_{W,<m_X}$; cf. Bemerkung 175. Da (X, W) erledigt ist, ist $m_X = f(M \smallsetminus X_{W,<m_X}) = f(M \smallsetminus B)$.

Sei $m_{X'} := \min(X' \smallsetminus B)$, gebildet bezüglich W'. Genauso ist $m_{X'} = f(M \smallsetminus B)$.

Also ist $m = m_X = m_{X'} \in X \cap X'$, aber $m \notin B$. Beachte, daß $B = X_{W,<m}$ ist und daß genauso $B = X'_{W',<m}$ ist.

Sei $\tilde{B} := B \sqcup \{m\} \subseteq X \cap X'$.

Nun ist auch $\tilde{B}$ ein W-Abschnitt in X: Sei dazu $s \in \tilde{B}$. Falls $s \in B$ liegt, dann ist $X_{W,<s} \subseteq B \subseteq \tilde{B}$, da B ein W-Abschnitt in X ist. Falls $s = m$ ist, dann ist $X_{W,<s} = X_{W,<m} = B \subseteq \tilde{B}$.

Genauso ist $\tilde{B} \subseteq X \cap X'$ ein W'-Abschnitt in X'.

Wir behaupten, es ist $W \cap (\tilde{B} \times \tilde{B}) = W' \cap (\tilde{B} \times \tilde{B})$.

Dank Symmetrie genügt es, $\overset{!}{\subseteq}$ zu zeigen.

Seien $s,\, t \in \tilde{B}$ mit $(s,t) \in W$ gegeben. Wir haben $(s,t) \overset{!}{\in} W'$ zu zeigen.

Falls $t \in B$ ist, dann ist nach Vorbemerkung (1) auch $(s,t) \in W'$.

Falls $s \neq t = m$ ist, dann ist $s \in B = X'_{W',<m}$ und also $(s,m) \in W'$.

Falls $s = t = m$ ist, dann ist $(s,t) = (m,m) \in W'$.

Dies zeigt die Behauptung.

Dann aber liegt $\tilde{B}$ in der Menge, deren Vereinigung B definiert. Also ist $B \sqcup \{m\} = \tilde{B} \subseteq B$, was einen *Widerspruch* darstellt.

Also ist $X = B \subseteq X'$ oder $X' = B \subseteq X$.

Sei o.E. $X = B \subseteq X'$.

Wir behaupten $W \overset{!}{=} W' \cap (X \times X)$.

Zu $\overset{!}{\subseteq}$. Sei $(s,t) \in W$. Dann ist $t \in X = B$. Nach Vorbemerkung (1) ist $(s,t) \in W'$.

Zu $\overset{!}{\supseteq}$. Sei $(s,t) \in W' \cap (X \times X)$. Dann ist $t \in X = B$. Nach Vorbemerkung (2) ist $(s,t) \in W$.

Dies zeigt die Behauptung.

Dies zeigt *Behauptung* 1.

Sei für (X, W) und (X', W') erklärt, daß $(X, W) \leqslant (X', W')$ genau dann gelte, wenn X ein W'-Abschnitt in X' mit $W = W' \cap (X \times X)$ ist.

Es ist $(E, \leqslant)$ ein Poset. Denn es ist $(\leqslant)$ reflexiv, da für $(X, W) \in E$ sich X als W-Abschnitt in X und $W = (X \times X) \cap W$ ergibt. Es ist $(\leqslant)$ identitiv, da für (X, W), $(X', W') \in E$ mit $(X, W) \leqslant (X', W') \leqslant (X, W)$ folgt, daß $X \subseteq X' \subseteq X$, also $X = X'$ ist, und also auch $W = (X \times X) \cap W' = W'$ ist. Es ist $(\leqslant)$ transitiv, da für (X, W), (X', W'), $(X'', W'') \in E$ mit $(X, W) \leqslant (X', W') \leqslant (X'', W'')$ sich zunächst $X \subseteq X' \subseteq X''$, mithin

$$W \ = \ W' \cap (X \times X) \ = \ (W'' \cap (X' \times X')) \cap (X \times X) \ = \ W'' \cap (X \times X)$$

ergibt. Ferner ist X ein W'-Abschnitt in X' und X' ein W''-Abschnitt in X''. Wir müssen zeigen, daß X ein W''-Abschnitt in X'' ist. Ist $x \in X$ und $x'' \in X''$ mit $(x'', x) \in W''$ gegeben, dann ist $x \in X'$ und also $x'' \in X'$. Da nun $(x'', x) \in W'' \cap (X' \times X') = W'$ liegt, folgt $x'' \in X$.

Dank *Behauptung* 1 ist $(E, \leqslant)$ linear geordnet.

Sei $Y := \bigcup_{(X,W) \in E} X$. Sei $V := \bigcup_{(X,W) \in E} W \subseteq Y \times Y$.

Zunächst zeigen wir $W \overset{!}{=} V \cap (X \times X)$ für $(X, W) \in E$. Wir haben nur $\overset{!}{\supseteq}$ zu zeigen. Seien $s,\ t \in X$ mit $(s, t) \in V$ gegeben. Es existiert $(X', W') \in E$ mit $(s, t) \in W' \subseteq X' \times X'$. Da E linear geordnet ist, ist $(X', E') \leqslant (X, E)$ oder $(X, E) \leqslant (X', E')$. Falls $(X', W') \leqslant (X, W)$ ist, folgt $(s, t) \in W' = W \cap (X' \times X') \subseteq W$. Falls $(X, W) \leqslant (X', W')$ ist, folgt $(s, t) \in W' \cap (X \times X) = W$. Jedenfalls folgt $(s, t) \in W$.

Behauptung 2. Wir behaupten, daß V eine Wohlordnung auf Y ist.

Es ist V reflexiv, da für $s \in Y$ ein $(X, W) \in E$ mit $s \in X$ existiert und $(s, s) \in W \subseteq V$ ist.

Es ist V identitiv, da für $s,\ t \in Y$ mit (s, t), $(t, s) \in V$ wegen E linear geordnet ein (X, W) mit $s,\ t \in X$ existiert, daher (s, t), $(t, s) \in V \cap (X \times X) = W$ liegen, wegen W identitiv also $s = t$ gilt.

Es ist V transitiv, da für $s,\ t,\ u \in Y$ mit (s, t), $(t, u) \in V$ wegen E linear geordnet ein (X, W) mit $s,\ t,\ u \in X$ existiert, daher (s, t), $(t, u) \in V \cap (X \times X) = W$ liegen, wegen W transitiv also $(s, u) \in W \subseteq V$ gilt.

Es ist V linear geordnet, da für $s,\ t \in Y$ wegen E linear geordnet ein (X, W) mit $s,\ t \in X$ existiert und daher $(s, t) \in W \subseteq V$ oder $(t, s) \in W \subseteq V$ gilt.

Bleibt zu zeigen, daß jede nichtleere Teilmenge Z von Y ein bezüglich V minimales Element enthält. Wähle $z \in Z$. Wähle (X, W) mit $z \in X$. Sei m minimal in $X \cap Z$ bezüglich W, existent, da W eine Wohlordnung ist. Es ist m minimal in Z bezüglich V. Denn sei $z' \in Z$ mit $(z', m) \in V$ gegeben. Wir haben $z' \overset{!}{=} m$ zu zeigen. Wir wählen $(X', W') \in E$ mit $z' \in X'$. Falls $(X', W') \leqslant (X, W)$ ist, dann ist $z' \in X' \subseteq X$. Falls $(X, W) \leqslant (X', W')$ ist, dann ist X ein W'-Abschnitt in X', sodaß aus $(z', m) \in V \cap (X', X') = W'$ und

$m \in X$ folgt, daß $z' \in X$ liegt. In beiden Fällen ergibt sich also $z' \in X \cap Z$, mithin $(z', m) \in V \cap (X \times X) = W$ und folglich $z' = m$ wegen der Minimalität von m.

Dies zeigt *Behauptung* 2.

Es bleibt zu zeigen, daß $Y \overset{!}{=} M$ ist.

Zeigen wir zunächst, daß (Y, V) erledigt ist. Es ist V eine Wohlordnung auf Y.

Sei $s \in Y$ gegeben.

Wähle ein $(X, W) \in E$ mit $s \in X$. Es ist $Y_{V,<s} = X_{W,<s}$. Hierbei folgt $\supseteq$, denn ist $(t, s) \in W$ mit $t \neq s$, dann ist $(t, s) \in W \subseteq V$ und $t \in X \subseteq Y$. Ferner folgt $\subseteq$, denn ist $(t, s) \in V$ mit $t \neq s$, dann gibt es ein $(X', W') \in E$ mit $t \in X'$. Ist $(X', W') \leqslant (X, W)$, dann ist $t \in X' \subseteq X$. Ist $(X, W) \leqslant (X', W')$, dann ist $s \in X$, $t \in X'$ und $(t, s) \in V \cap (X' \times X') = W'$; da X ein W'-Abschnitt in X' ist, folgt $t \in X$. Beidenfalls ist $t \in X$ und somit $(t, s) \in V \cap (X \times X) = W$.

Folglich ist $f(M \smallsetminus Y_{V,<s}) = f(M \smallsetminus X_{W,<s}) = s$, letzteres, da (X, W) erledigt ist.

Somit ist (Y, V) erledigt.

Annahme, es ist $Y \subset M$.

Sei $y' := f(M \smallsetminus Y) \in M \smallsetminus Y$. Sei $Y' := Y \sqcup \{y'\}$. Sei $V' := V \sqcup \{\, (s, y') : \ s \in Y' \,\} \subseteq Y' \times Y'$.

Es ist V' reflexiv, da V reflexiv ist und zudem $(y', y') \in V'$ liegt.

Es ist V' identitiv, da V identitiv ist und da aus (s, y'), $(y', s) \in V'$ folgt, daß $s = y'$ ist.

Es ist V' transitiv, da für (s, t), $(t, u) \in V'$ entweder $u = y'$ und somit $(s, u) = (s, y') \in V'$ ist oder aber $u \neq y'$, also $t \neq y'$, also $s \neq y'$, also (s, t), $(t, u) \in V$ und somit $(s, u) \in V \subseteq V'$ ist.

Es ist V' linear geordnet, da für $(s, t) \in V'$ entweder $\{s, t\} \cap \{y'\} \neq \emptyset$ ist, wesfalls $(s, t) \in V'$ oder $(t, s) \in V'$ ist, oder $\{s, t\} \cap \{y'\} = \emptyset$ ist, wesfalls s, $t \in Y$ liegen und also $(s, t) \in V \subseteq V'$ oder $(t, s) \in V \subseteq V'$ ist.

Es ist V' wohlgeordnet. Sei dazu Z eine nichtleere Teilmenge von Y'. Ist $Z \cap Y \neq \emptyset$, dann ist das Minimum von $Z \cap Y$ in Y auch das Minimum von $Z \cap Y$ in Y'. Ist $Z \cap Y = \emptyset$, dann ist $Z = \{y'\}$ und hat y' als Minimum.

Wir zeigen, daß (Y', V') erledigt ist. Es ist, wie eben gesehen, V' eine Wohlordnung auf Y'.

Sei $s \in Y'$ gegeben.

Falls $s \in Y$ liegt, ist $Y'_{V',<s} = Y_{V,<s}$ und also $f(M \smallsetminus Y'_{V',<s}) = f(M \smallsetminus Y_{V,<s}) = s$, da (Y, V) erledigt ist. Falls $s = y'$ ist, ist $Y'_{V',<s} = Y$ und also $f(M \smallsetminus Y'_{V',<s}) = f(M \smallsetminus Y) = y'$. In beiden Fällen ist die erforderliche Gleichheit richtig. Also ist (Y', V') erledigt.

Da nun (Y', V') erledigt ist, ist $Y' = Y \sqcup \{y'\} \subseteq Y$ nach Definition von Y, und wir haben einen *Widerspruch.*

Also ist $Y = M$. Mithin ist $(\leqslant) := V$ eine Wohlordnung auf M. $\square$

Lemma 177 *Sei $X = (X, \leqslant)$ ein Poset.*

Sei $K \in \operatorname{Chain}(X)$. Es gibt ein maximales Element M in $\operatorname{Chain}(X)$ mit $K \subseteq M$.

Beweis. Wir wählen eine Wohlordnung $(\preceq)$ auf $X \smallsetminus K$, möglich dank Lemma 176.

> Dies geschehe völlig unabhängig von der gegebenen Ordnungsrelation $(\leqslant)$ auf X. Im allgemeinen haben $(\leqslant)$ und $(\preceq)$ nichts miteinander zu tun.

Für $s \in X \smallsetminus K$ sei $f(s) := 1$, falls es genau eine Abbildung $g_s \colon (X \smallsetminus K)_{\preceq s} \to \{0, 1\}$ mit folgender Eigenschaft (A_s) gibt.

(A_s) Es ist $g_s(t) = 1$ für $t \in (X \smallsetminus K)_{\preceq s}$ genau dann, wenn t vergleichbar ist mit allen Elementen von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec t} :\ g_s(u) = 1 \,\}$.

Ansonsten sei $f(s) := 0$.

Wir *behaupten*, daß $f(s) \stackrel{!}{=} 1$ ist für $s \in X \smallsetminus K$.

Gemäß Bemerkung 174 ist zu zeigen, daß für $s \in X \smallsetminus K$ aus $f((X \smallsetminus K)_{\prec s}) \subseteq \{1\}$ folgt, daß $f(s) \stackrel{!}{=} 1$ ist.

Zur Eindeutigkeit. Annahme, es gibt zwei solche Abbildungen g_s und $\tilde{g}_s$. Dann ist gibt es ein bezüglich $(\preceq)$ minimales Element $m \in X \smallsetminus K$ mit $g_s(m) \neq \tilde{g}_s(m)$.

Sei o.E. $g_s(m) = 1$ und $\tilde{g}_s(m) = 0$. Ersteres bedeutet, daß m vergleichbar ist mit allen Elementen von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec m} :\ g_s(u) = 1 \,\}$. Zweiteres bedeutet, daß m nicht mit allen Elementen von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec m} :\ \tilde{g}_s(u) = 1 \,\}$ vergleichbar ist. Da $g_s(u) = \tilde{g}_s(u)$ für $u \in (X \smallsetminus K)_{\prec m}$ und also

$$\{\, u \in (X \smallsetminus K)_{\prec m} :\ g_s(u) = 1 \,\} = \{\, u \in (X \smallsetminus K)_{\prec m} :\ \tilde{g}_s(u) = 1 \,\}$$

ist, stellt dies einen *Widerspruch* dar.

Zur Existenz. Es ist $f(t) = 1$ für $t \in (X \smallsetminus K)_{\prec s}$. Wir haben also die eindeutige Existenz von g_t mit der Eigenschaft (A_t) für $t \in (X \smallsetminus K)_{\prec s}$ zur Verfügung.

Da für $u, t \in (X \smallsetminus K)_{\prec s}$ mit $u \prec t$ auch $g_t|_{(X \smallsetminus K)_{\preceq u}}$ die Eigenschaft (A_u) hat, folgt $g_t|_{(X \smallsetminus K)_{\preceq u}} = g_u$.

Setze $g_s(t) := g_t(t)$ für $t \in (X \smallsetminus K)_{\prec s}$. Setze $g_s(s) := 1$, falls s vergleichbar ist mit allen Elementen von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec s} :\ g_u(u) = 1 \,\}$, ansonsten setze $g_s(s) := 0$.

Für $u, t \in (X \smallsetminus K)_{\prec s}$ mit $u \prec t$ ist dann

$$g_s|_{(X \smallsetminus K)_{\preceq t}}(u) \;=\; g_s(u) \;=\; g_u(u) \;=\; g_t(u)\ .$$

Für $t \in (X \smallsetminus K)_{\prec s}$ ist somit

$$g_s|_{(X \smallsetminus K)_{\preceq t}} \;=\; g_t\ .$$

Also ist $g_s(t) = 1$ für $t \in (X \smallsetminus K)_{\prec s}$ genau dann, wenn $g_t(t) = 1$ ist, i.e. wenn t vergleichbar ist mit allen Elementen von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec t} :\ g_t(u) = 1 \,\}$, i.e. mit allen Elementen von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec t} :\ g_s(u) = 1 \,\}$.

Ferner ist $g_s(s) = 1$ genau dann, wenn s vergleichbar ist mit allen Elementen von

$$K \sqcup \{\, u \in (X \smallsetminus K)_{\prec s} :\ g_u(u) = 1 \,\} \;=\; K \sqcup \{\, u \in (X \smallsetminus K)_{\prec s} :\ g_s(u) = 1 \,\} \,.$$

Somit ist $f(s) = 1$. Dies zeigt die *Behauptung.*

Da für $u,\ s \in X \smallsetminus K$ mit $u \preceq s$ zum einen $f(u) = 1$ ist und zum anderen auch $g_s|_{(X \smallsetminus K)_{\preceq u}}$ die Eigenschaft (A_u) hat, folgt $g_s|_{(X \smallsetminus K)_{\preceq u}} = g_u$.

Setze $g(s) := g_s(s)$ für $s \in X \smallsetminus K$. Für $u \in X \smallsetminus K$ mit $u \preceq s$ ist

$$g|_{(X \smallsetminus K)_{\preceq s}}(u) \;=\; g(u) \;=\; g_u(u) \;=\; g_s(u) \,.$$

Folglich ist

$$g|_{(X \smallsetminus K)_{\preceq s}} \;=\; g_s$$

für $s \in X \smallsetminus K$.

Daher ist $g\colon X \smallsetminus K \to \{0, 1\}$ eine Abbildung mit der Eigenschaft, daß für $s \in X \smallsetminus K$ genau dann $g(s) = 1$ gilt, wenn s vergleichbar ist mit allen Elementen von

$$K \sqcup \{\, u \in (X \smallsetminus K)_{\prec s} :\ g(u) = 1 \,\} \,.$$

Setze

$$M \;:=\; K \sqcup \{\, u \in X \smallsetminus K :\ g(u) = 1 \,\} \,.$$

Wir *behaupten,* daß M eine bezüglich $(\subseteq)$ maximale Kette ist, die K enthält.

Seien $t,\ s \in M$. Wir haben zu zeigen, daß t und s vergleichbar sind. Sind $t,\ s \in K$, so folgt dies aus K Kette. Ist $t \in K$ und $s \in M \smallsetminus K$, so folgt dies daraus, daß $g(s) = 1$ ist. Ist $t \in M \smallsetminus K$ und $s \in K$, so folgt dies daraus, daß $g(t) = 1$ ist. Sind $t,\ s \in M \smallsetminus K$, so ist o.E. $t \prec s$. Da $g(s) = 1$ ist und da $t \in (X \smallsetminus K)_{\prec s}$ liegt und $g(t) = 1$ ist, ist s vergleichbar mit t. Somit ist M eine Kette in X.

Annahme, es ist M keine maximale Kette in X. Sei $M \subset L \subseteq X$ und L eine Kette. Wähle $z \in L \smallsetminus M$. Dann ist $z \in X \smallsetminus K$ und $g(z) = 0$. Folglich gibt es ein Element von $K \sqcup \{\, u \in (X \smallsetminus K)_{\prec z} :\ g(u) = 1 \,\} \subseteq M$, das nicht mit z vergleichbar ist. Also ist L keine Kette. Wir haben einen *Widerspruch.* ▫

Lemma 178 (Zorn) *Sei $X = (X, \leqslant)$ ein Poset.*

Es habe in X jede Kette eine obere Schranke.

Sei $x \in X$. Dann gibt es ein maximales Element $m \in X$ mit $x \leqslant m$.

Beweis. Die Kette $\{x\}$ ist in einer maximalen Kette M enthalten. Diese hat eine obere Schranke m.

Dann ist $x \leqslant m$.

Annahme, es ist m nicht maximal in X. Dann gibt es ein $y \in X$ mit $m < y$.

Dann ist $M \subset M \sqcup \{y\} =: M'$.

Ferner ist M' eine Kette. Denn sind $s,\ t\ \in\ M'$, so haben wir folgende Fälle zu betrachten.

Falls $s,\ t\ \in\ M$ liegen, dann ist $s \leqslant t$ oder $t \leqslant s$, da M eine Kette ist.

Falls $s \in M$ liegt und $t = y$ ist, dann ist $s \leqslant m \leqslant y = t$.

Falls $t \in M$ liegt und $s = y$ ist, dann ist $t \leqslant m \leqslant y = s$.

Falls $t = y$ und $s = y$ ist, dann ist $s = t$.

Wir haben einen *Widerspruch* zur Maximalität der Kette M. $\square$

Anhang B

Aufgaben und Lösungen

B.1 Aufgaben

Aufgabe 1 (§1.1.1)

(1) Sei R ein kommutativer Ring. Zu zeigen ist, daß $\mathrm{U}(R)$, zusammen mit der auf $\mathrm{U}(R)$ eingeschränkten Multiplikation, eine abelsche Gruppe bildet.

(2) Seien R und S kommutative Ringe. Sei $R \xrightarrow{f} S$ ein Ringmorphismus.
Zu zeigen ist, daß $\mathrm{U}(f) := f|_{\mathrm{U}(R)}^{\mathrm{U}(S)} \colon \mathrm{U}(R) \to \mathrm{U}(S)$ ein Gruppenmorphismus ist.

Aufgabe 2 (§1.1.1) Sei R ein Integritätsbereich, welcher als Menge endlich ist.

Zu zeigen ist, daß R ein Körper ist.

Aufgabe 3 (§1.1.1) Sei R ein kommutativer Ring.

(1) Zu zeigen ist, daß es genau einen Ringmorphismus von $\mathbf{Z}$ nach R gibt.

(2) Zu zeigen ist, daß es genau einen Ringmorphismus von R nach 0 gibt.

Der Ringmorphismus aus (1) werde $\mathbf{Z} \xrightarrow{\varepsilon_R} R$ geschrieben.

Oft schreiben wir $z := \varepsilon_R(z) \in R$ für $z \in \mathbf{Z}$.

Der Ringmorphismus aus (2) werde $R \xrightarrow{\eta_R} 0$ geschrieben.

Aufgabe 4 (§1.1.1) Zu zeigen oder zu widerlegen.

(1) Sei R ein kommutativer Ring. Von R nach R ist id_R der einzige Ringisomorphismus.

(2) Von $\mathbf{Q}$ nach $\mathbf{Q}$ ist $\mathrm{id}_{\mathbf{Q}}$ der einzige Ringmorphismus.

(3) Es hat $\mathbf{Q}$ nur die Teilringe $\mathbf{Z}$ und $\mathbf{Q}$.

Aufgabe 5 (§1.1.2) Seien R und S kommutative Ringe. Zu zeigen ist folgendes.

(1) Es ist R auf eindeutige Weise eine $\mathbf{Z}$-Algebra.

(2) Es ist jeder Ringmorphismus $R \xrightarrow{f} S$ ein $\mathbf{Z}$-Algebrenmorphismus.

Aufgabe 6 (§1.1.1, §1.1.2) Zu zeigen ist folgendes.

(1) Seien S und T kommutative Ringe.

Ist $S \overset{f}{\to} T$ ein bijektiver Ringmorphismus, dann auch $S \xleftarrow{f^-} T$.

(2) Sei R ein kommutativer Ring. Seien $S = (S, \alpha)$ und $T = (T, \beta)$ kommutative R-Algebren.

Ist $S \overset{f}{\to} T$ ein bijektiver R-Algebrenmorphismus, dann auch $S \xleftarrow{f^-} T$.

Aufgabe 7 (§1.1.2) Sei R ein kommutativer Ring.

Sei I eine Menge. Sei $X = \{\, X_i : \ i \in I \,\}$ eine Menge, wobei $I \to X : i \mapsto X_i$ bijektiv sei.

Wir schreiben die Elemente von $R[X]$ zunächst als Koeffiziententupel $(r_e)_e = (r_e)_{e \in E_I}$ mit Einträgen aus R, wobei jeweils $\{\, e \in E_I : \ r_e \neq 0 \,\}$ endlich ist. Cf. auch (4).

Zu zeigen ist folgendes.

(1) Für $(r_e)_e\,,\ (r'_e)_e \ \in \ R[X]$ sind auch

$$(r'_e)_e + (r''_e)_e \ := \ (r'_e + r''_e)_e \ \in \ R[X]$$

und

$$(r'_e)_e \cdot (r''_e)_e \ := \ \Bigg(\sum_{\substack{(e',\, e'') \,\in\, E_I \times E_I \\ e' + e'' \,=\, e}} r'_{e'}\, r''_{e''} \Bigg)_e$$

wieder in $R[X]$.

(2) Es ist $R[X] = (R[X], +, \cdot)$ ein kommutativer Ring.

(3) Zusammen mit $R \xrightarrow{\alpha_{R,X}} R[X] \colon r \mapsto (r\partial_{(0)_i,\, e})_e$ ist $R[X]$ eine R-Algebra.

(4) Schreiben wir für $j \in I$ etwas mißbräuchlich $d[j] := (\partial_{j,i})_i$ und $X_j := (\partial_{d[j],e})_e$, sowie $r := \alpha_{R,X}(r)$ für $r \in R$, so erhalten wir für $(r_e)_e \in R[X]$ die Gleichheit

$$(r_e)_{e \in E_I} \ = \ \sum_{e \,=\, (e_i)_i \,\in\, E_I} r_e \prod_{i \in I} X_i^{e_i} \ .$$

Aufgabe 8 (§1.1.3) Sei R ein kommutativer Ring.

Seien R-Algebren $S = (S, \alpha)$ und $T = (T, \beta)$ gegeben.

Sei $S \xrightarrow{f} T$ ein R-Algebrenmorphismus.

Sei $\mathfrak{b} \subseteq T$ ein Ideal. Sei $\mathfrak{a} := f^{-1}(\mathfrak{b}) \subseteq S$. Zu zeigen ist folgendes.

(1) Es ist $\mathfrak{a} \subseteq S$ ein Ideal mit $f(\mathfrak{a}) \subseteq \mathfrak{b}$.

(2) Ist $\tilde{\mathfrak{a}} \subseteq S$ ein Ideal mit $f(\tilde{\mathfrak{a}}) \subseteq \mathfrak{b}$, dann ist die Abbildung

$$\begin{array}{rcl} S/\tilde{\mathfrak{a}} & \xrightarrow{\bar{f}} & T/\mathfrak{b} \\ s + \tilde{\mathfrak{a}} & \mapsto & f(s) + \mathfrak{b} \end{array}$$

wohldefiniert und ein R-Algebrenmorphismus.

(3) Die Abbildung

$$\begin{array}{rcl} S/\mathfrak{a} & \xrightarrow{\bar{f}} & T/\mathfrak{b} \\ s + \mathfrak{a} & \mapsto & f(s) + \mathfrak{b} \end{array}$$

ist wohldefiniert und ein injektiver R-Algebrenmorphismus.

Aufgabe 9 (§1.1.3) Sei R ein kommutativer Ring. Sei $\mathfrak{a}$ ein Ideal in R.

Zu zeigen ist, daß auf der abelschen Gruppe $R/\mathfrak{a}$ mittels $(r + \mathfrak{a}) \cdot (r' + \mathfrak{a}) := rr' + \mathfrak{a}$ für $r,\ r' \in R$ die Struktur eines kommutativen Rings definiert wird.

Aufgabe 10 (§1.1.3) Sei R ein kommutativer Ring.

Seien S und T kommutative R-Algebren.

Sei $S \xrightarrow{f} T$ ein surjektiver R-Algebrenmorphismus. Sei $\mathfrak{k} \subseteq S$ sein Kern.

Bezeichne Ideale(S) die Menge der Ideale von S.

Zu zeigen ist folgende Bijektion.

$$\begin{array}{rcl} \mathrm{Ideale}(T) & \leftrightarrow & \{\, \mathfrak{b} \in \mathrm{Ideale}(S) :\ \mathfrak{k} \subseteq \mathfrak{b} \subseteq S \,\} \\ \mathfrak{c} & \mapsto & f^{-1}(\mathfrak{c}) \\ f(\mathfrak{b}) & \leftarrow\!\shortmid & \mathfrak{b} \end{array}$$

Aufgabe 11 (§1.1.3) Zu zeigen oder zu widerlegen.

Sei R ein kommutativer Ring. Sei S eine kommutative R-Algebra. Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in S.

(1) Es ist $\mathbf{Z}$ eine Hauptidealalgebra über $\mathbf{Z}$.

(2) Ist K ein Körper und X ein Element, dann ist $K[X]$ eine Hauptidealalgebra über K.

(3) Ist R eine Hauptidealalgebra über R, dann ist $R[X]$ eine Hauptidealalgebra über R.

(4) Es ist $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a}}\sqrt{\mathfrak{b}}$.

(5) Es ist $\sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.

(6) Es ist $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$.

Aufgabe 12 (§1.1.4) Sei R ein kommutativer Ring. Sei S eine kommutative R-Algebra. Zu zeigen ist die Äquivalenz der Aussagen (1) und (2).

(1) Es ist S noethersch.

(2) Jede nichtleere Teilmenge der Menge der Ideale von S hat ein maximales Element.

Aufgabe 13 (§1.1.3) Sei K ein Körper. Seien X, Y, Z drei Elemente.

Sei $S := K[X,Y,Z]/(XY - Z^2)$. Wir schreiben $\bar{\xi} := \xi + (XY - Z^2) \in S$ für $\xi \in K[X,Y,Z]$.

Sei $\mathfrak{p} := (\bar{X}, \bar{Z}) \subseteq S$. Zu zeigen ist folgendes.

(1) Es ist $K[X,Y] \to S\colon X \mapsto \bar{X},\ Y \mapsto \bar{Y}$ ein injektiver K-Algebrenmorphismus.

(2) Für jedes $\eta \in S$ gibt es eindeutige Elemente $f(X,Y)$, $g(X,Y) \in K[X,Y]$ mit $\eta = f(\bar{X},\bar{Y}) + \bar{Z}\,g(\bar{X},\bar{Y})$.

(3) Es ist $\mathfrak{p} \subseteq S$ ein Primideal.

(4) Jedes Element von $\mathfrak{p}^2$ ist von der Form $a(\bar{X},\bar{Y})\bar{X}^2 + b(\bar{X},\bar{Y})\bar{X}\bar{Y} + c(\bar{X},\bar{Y})\bar{X}\bar{Z}$ für gewisse $a(X,Y)$, $b(X,Y)$, $c(X,Y) \in K[X,Y]$. Folglich ist jedes Element von $\mathfrak{p}^2$ von der Form $f(\bar{X},\bar{Y}) + \bar{Z}\,g(\bar{X},\bar{Y})$ mit $f(X,Y) \in (X^2, XY) \subseteq K[X,Y]$ und $g(X,Y) \in (X) \subseteq K[X,Y]$.

(5) Es ist $\bar{X}\bar{Y} \in \mathfrak{p}^2$, aber $\bar{X} \notin \mathfrak{p}^2$ und $\bar{Y}^n \notin \mathfrak{p}^2$ für alle $n \in \mathbf{Z}_{\geqslant 0}$.

(6) Es ist $\mathfrak{p}^2 \subseteq S$ nicht primär, obwohl $\sqrt{\mathfrak{p}^2} = \mathfrak{p}$ prim ist. ([1])

[1] Dieses Beispiel kenne ich von `en.wikipedia.org/wiki/Primary_ideal`

B.2 Lösungen

Aufgabe 1

Ad (1). Zunächst sollte die Multiplikation auf $\mathrm{U}(R)$ einschränken. Seien $x,\ y\ \in\ \mathrm{U}(R)$. Es ist $xyx^-y^- = 1$. Also ist $xy \in \mathrm{U}(R)$.

Nun sollten die Gesetze einer abelschen Gruppe gelten für $\mathrm{U}(R)$, ausgestattet mit dieser eingeschränkten Multiplikation.

Da die Multiplikation auf R assoziativ und kommutativ ist, gilt dies auch für ihre Einschränkung auf $\mathrm{U}(R)$.

Da $1 \cdot 1 = 1$ ist, ist auch $1 \in \mathrm{U}(R)$. Somit hat $\mathrm{U}(R)$ ein neutrales Element.

Ist $x \in \mathrm{U}(R)$, dann auch x^-, da $x^-x = 1$. Also hat jedes Element von $\mathrm{U}(R)$ ein Inverses.

Insgesamt ist nun $\mathrm{U}(R)$ als abelsche Gruppe nachgewiesen.

Ad (2). Wir haben bei Definition 7 gesehen, daß $f|_{\mathrm{U}(R)}^{\mathrm{U}(S)}$ existiert. Sind ferner $x,\ y\ \in\ \mathrm{U}(R)$, dann ist auch $\mathrm{U}(f)(x \cdot y) = f(x \cdot y) = f(x) \cdot f(y) = \mathrm{U}(f)(x) \cdot \mathrm{U}(f)(y)$. Folglich ist $\mathrm{U}(f)$ ein Gruppenmorphismus.

Aufgabe 2

Da R ein Integritätsbereich ist, ist $0_R \neq 1_R$.

Sei $a \in R^\times$. Zu zeigen ist, daß $\lambda_a \colon R \to R \colon x \mapsto ax$ bijektiv ist.

Da R ein Integritätsbereich ist, ist λ_a injektiv.

Da R endlich ist, ist die injektive Selbstabbildung λ_a von R auch surjektiv. Insgesamt ist λ_a also bijektiv.

Aufgabe 3

Ad (1).

Zeigen wir, daß es höchstens einen Ringmorphismus von $\mathbf{Z}$ *nach* R *gibt.*

Sei $f : \mathbf{Z} \to R$ ein Ringmorphismus. Es ist $f(0) = 0$ und $f(1) = 1$. Für $n \in \mathbf{Z}_{\geqslant 1}$ ist $f(n) = f(\sum_{i\in[1,n]} 1) = \sum_{i\in[1,n]} f(1) = \sum_{[1,n]} 1_R$. Desweiteren ist $f(-n) = -f(n) = -\sum_{[1,n]} 1$. Somit liegen alle Funktionswerte von f fest.

Zeigen wir, daß es mindestens einen Ringmorphismus von $\mathbf{Z}$ *nach* R *gibt.*

Wir erinnern daran, daß gemäß dem Aufbau des Zahlensystems eine ganze Zahl eine Äquivalenzklasse $[(a, b)]$ natürlicher Zahlen $a,\ b\ \in\ \mathbf{N}$ ist, wobei $[(a, b)] = [(c, d)]$ für $a,\ b,\ c,\ d\ \in\ \mathbf{N}$ genau dann gelte, wenn $a + d = c + b$ ist. Ferner ist $[(a, b)] + [(c, d)] = [(a + c, b + d)]$ und $[(a, b)] \cdot [(c, d)] = [(ac + bd, bc + ad)]$.

Wir haben die injektive Abbildung $\mathbf{N} \to \mathbf{Z} \colon n \mapsto (n, 0)$ und identifizieren $\mathbf{N}$ mit seinem Bild.

Wir betrachten zunächst die Abbildung $u : \mathbf{N} \to R,\ n \mapsto u(n) := \sum_{i\in[1,n]} 1_R$. [2]

Es ist $u(0) = 0$. Es ist $u(1) = 1$.

Für $n,\ m\ \in\ \mathbf{N}$ ist

$$u(n) + u(m) \;=\; (\sum_{i\in[1,n]} 1_R) + (\sum_{j\in[1,m]} 1_R) \;=\; \sum_{i\in[1,n+m]} 1_R \;=\; u(n+m)\ .$$

[2] Man kann sauberer auch u rekursiv definieren und die Eigenschaften von u dann per Induktion zeigen.

und

$$u(n) \cdot u(m) \;=\; (\sum_{i \in [1,n]} 1_R) \cdot (\sum_{j \in [1,m]} 1_R) \;=\; \sum_{(i,j) \in [1,n] \times [1,m]} 1_R \;=\; \sum_{k \in [1,nm]} 1_R \;=\; u(nm)\;.$$

Setze nun

$$\begin{array}{rcl} \mathbf{Z} & \xrightarrow{\varepsilon_R} & R \\ [(a,b)] & \mapsto & u(a) - u(b)\;. \end{array}$$

Dies ist wohldefiniert, denn für $a,\, b,\, c,\, d \in \mathbf{N}$ mit $a + d = c + b$ ist auch $u(a) + u(d) = u(a + d) = u(c + b) = u(c) + u(b)$ und also $u(a) - u(b) = u(c) - u(d)$.

Verifizieren wir, daß f ein Ringmorphismus ist.

Es ist $\varepsilon_R(1) = \varepsilon_R([(1, 0)]) = u(1) - u(0) = 1 - 0 = 1$.

Für $[(a, b)],\, [(c, d)] \in \mathbf{Z}$ ist

$$\varepsilon_R([(a,b)]+[(c,d)]) \;=\; \varepsilon_R([(a+c,b+d)]) \;=\; u(a+c)-u(b+d) \;=\; u(a)-u(b)+u(c)-u(d) \;=\; \varepsilon_R([(a,b)])+\varepsilon_R([(c,d)])\;.$$

Für $[(a, b)],\, [(c, d)] \in \mathbf{Z}$ ist

$$\begin{array}{rcl} \varepsilon_R([(a,b)] \cdot [(c,d)]) & = & f([(ac + bd, bc + ad)]) \\ & = & u(ac + bd) - u(bc + ad) \\ & = & u(a) \cdot u(c) + u(b) \cdot u(d) - u(b) \cdot u(c) - u(a) \cdot u(d) \\ & = & (u(a) - u(b)) \cdot (u(c) - u(d)) \\ & = & \varepsilon_R([(a,b)]) \cdot \varepsilon_R([(c,d)])\;. \end{array}$$

Ad (2). Von R nach 0 gibt es nur die Abbildung $\eta_R\colon R \to 0\colon r \mapsto 0$. Wir haben nur zu zeigen, daß η_R ein Ringmorphismus ist.

Für $x,\, y \in R$ ist $\eta_R(x + y) = 0 = 0 + 0 = \eta_R(x) + \eta_R(y)$ und $\eta_R(x \cdot y) = 0 = 0 \cdot 0 = \eta_R(x) \cdot \eta_R(y)$. Ferner ist $\eta_R(1) = 0 = 1$.

Aufgabe 4

Ad (1). Die Aussage ist falsch.

Sei etwa $R = \mathbf{C}$. Die komplexe Konjugation ist ein Ringisomorphismus von $\mathbf{C}$ nach $\mathbf{C}$, welcher nicht gleich $\mathrm{id}_{\mathbf{C}}$ ist.

Ad (2). Die Aussage ist richtig.

Sei hierzu ein Ringisomorphismus $\mathbf{Q} \xrightarrow{f} \mathbf{Q}$ gegeben. Dank Aufgabe 3.(1) ist $f \circ \varepsilon_{\mathbf{Q}} = \varepsilon_{\mathbf{Q}}$, i.e. es ist $f(z) = z$ für $z \in \mathbf{Z}$.

Folglich ist für $z \in \mathbf{Z}$ und $w \in \mathbf{Z}^\times$ auch

$$f(z \cdot w^-) \;=\; f(z) \cdot f(w^-) \;=\; f(z) \cdot f(w)^- \;=\; z \cdot w^-\;.$$

Mithin ist $f = \mathrm{id}_{\mathbf{Q}}$.

Ad (3). Die Aussage ist falsch.

Sei etwa $\mathbf{Z}_{(3)} := \{\, \frac{z}{w} :\ z \in \mathbf{Z},\ w \in \mathbf{Z} \smallsetminus 3\mathbf{Z}\,\}$. Es ist $1_{\mathbf{Q}} = 1/1 \in \mathbf{Z}_{(3)}$. Sind $z,\, z' \in \mathbf{Z}$ und $w,\, w' \in \mathbf{Z} \smallsetminus 3\mathbf{Z}$, dann ist $\frac{z}{w} - \frac{z'}{w'} = \frac{zw' - z'w}{ww'} \in \mathbf{Z}_{(3)}$ und $\frac{z}{w} \cdot \frac{z'}{w'} = \frac{zz'}{ww'} \in \mathbf{Z}_{(3)}$. Also ist $\mathbf{Z}_{(3)}$ ein Teilring von $\mathbf{Q}$.

Da $\frac{1}{3} \in \mathbf{Q} \smallsetminus \mathbf{Z}_{(3)}$ und $\frac{1}{2} \in \mathbf{Z}_{(3)} \smallsetminus \mathbf{Z}$ liegen, ist $\mathbf{Z} \subset \mathbf{Z}_{(3)} \subset \mathbf{Q}$.

Aufgabe 5

Ad (1). Gemäß Aufgabe 3.(1) gibt es genau einen Ringmorphismus von $\mathbf{Z}$ nach R, genannt ε_R, desbezüglich R dann eine $\mathbf{Z}$-Algebra ist.

Ad (2). Wir haben $f \circ \varepsilon_R \stackrel{!}{=} \varepsilon_S$ zu zeigen. Nun sind $f \circ \varepsilon_R$ und ε_S Ringmorphismen von $\mathbf{Z}$ nach S, sodaß wir dank Aufgabe 3.(1) also $f \circ \varepsilon_R = \varepsilon_S$ bekommen.

Aufgabe 6

Ad (1). Es ist $f^-(1_T) = f^-(f(1_S)) = 1_S$.

Für $x, y \in T$ ist $f^-(x+y) = f^-(f(f^-(x)) + f(f^-(y))) = f^-(f(f^-(x) + f^-(y))) = f^-(x) + f^-(y)$.

Für $x, y \in T$ ist $f^-(x \cdot y) = f^-(f(f^-(x)) \cdot f(f^-(y))) = f^-(f(f^-(x) \cdot f^-(y))) = f^-(x) \cdot f^-(y)$.

Ad (2). Seien augeschrieben $S = (S, \alpha)$ und $T = (T, \gamma)$.

Dank (1) ist f^- ein Ringmorphismus. Also genügt es zu zeigen, daß $f^- \circ \beta \stackrel{!}{=} \alpha$ ist. Aber es ist $f \circ \alpha = \beta$, und also $\alpha = f^- \circ f \circ \alpha = f^- \circ \beta$.

Aufgabe 7

Ad (1).

Zur Addition. Es ist $\{\, e \in E_I :\, r'_e + r''_e \neq 0 \,\} \subseteq \{\, e \in E_I :\, r'_e \neq 0 \,\} \cup \{\, e \in E_I :\, r''_e \neq 0 \,\}$ endlich. Also ist $(r'_e + r''_e)_e \;\in\; R[X]$.

Zur Multiplikation. Zeigen wir zunächst, daß für $e',\, e'' \in E_I$ auch $e' + e''$ wieder in E_I liegt. In der Tat ist $\{\, i \in I :\, e'_i + e''_i \neq 0 \,\} \subseteq \{\, i \in I :\, e'_i \neq 0 \,\} \cup \{\, i \in I :\, e''_i \neq 0 \,\}$ und also endlich.

Sei $e \in E_I$ gegeben. Es ist die Menge $\{\, (e', e'') \in E_I \times E_I :\, e' + e'' = e \,\}$ endlich, genauer gesagt, sie enthält $\prod_{i \in I} (e_i + 1)$ Elemente.

Nun zur Wohldefiniertheit der Multiplikation. O.E. sind dazu $(r'_e)_e$ und $(r''_e)_e$ ungleich 0.

Sei $\hat{e}'$ definiert durch $\hat{e}'_i := \max\{\, e_i :\, e \in E_I \text{ mit } r'_e \neq 0 \,\}$ für $i \in I$.

Sei $\hat{e}''$ definiert durch $\hat{e}''_i := \max\{\, e_i :\, e \in E_I \text{ mit } r''_e \neq 0 \,\}$ für $i \in I$.

Es ist $\hat{e}' \in E_I$, da

$$\{\, i \in I :\, \hat{e}'_i \neq 0 \,\} \;=\; \bigcup_{e \in E_I,\, r_e \neq 0} \{\, i \in I :\, e_i \neq 0 \,\}\,,$$

was als endliche Vereinigung endlicher Mengen endlich ist.

Sei nun $e \in E_I$ gegeben mit $\sum_{\substack{(e',\, e'') \,\in\, E_I \times E_I \\ e' + e'' \,=\, e}} r'_{e'}\, r''_{e''} \neq 0$.

Es genügt zu zeigen, daß e dann in der endlichen Menge $\{\, \tilde{e} \in E_I :\, \tilde{e}_i \leqslant \hat{e}'_i + \hat{e}''_i \,\}$ enthalten ist.

Annahme, nicht. Sei $j \in J$ gewählt mit $e_j > \hat{e}'_j + \hat{e}''_j$. Seien $e',\, e'' \in E_I$ mit $e = e' + e''$ und $r'_{e'} \neq 0$ und $r''_{e''} \neq 0$ gewählt. Es folgt $e'_j \leqslant \hat{e}'_j$ und $e''_j \leqslant \hat{e}''_j$. Also ist

$$e_j \;=\; e'_j + e''_j \;\leqslant\; \hat{e}'_j + \hat{e}''_j \;<\; e_j\,.$$

Wir haben einen *Widerspruch.*

Zeigen wir schließlich noch folgende *Behauptung.* Seien $d',\, d'' \in E_I$. Seien $r',\, r'' \in R$. Dann ist $(r' \partial_{d',e})_e \cdot (r'' \partial_{d'',e})_e = (r' r'' \partial_{d'+d'',e})_e$.

In der Tat wird

$$\begin{aligned}
(r'\partial_{d',e})_e \cdot (r''\partial_{d'',e})_e &= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} r'\partial_{d',e'}\, r''\partial_{d'',e''}\Big)_e \\
&= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e\\ e'=d'\,,\,e''=d''}} r'r''\Big)_e \\
&= (r'r''\partial_{d'+d'',e})_e\,.
\end{aligned}$$

Dies zeigt die *Behauptung*.

Ad (2).

Mit $0 = (0)_e$ und $-(r_e)_e = (-r_e)_e$ für $(r_e)_e \in R[X]$ erkennen wir, daß $R[X]$ eine abelsche Gruppe ist.

Die Multiplikation ist ersichtlich kommutativ.

Zeigen wir die Assoziativität. Seien $(r'_e)_e\,,\,(r''_e)_e\,,\,(r'''_e)_e \;\in\; R[X]$ gegeben.

Zum einen erhalten wir

$$\begin{aligned}
((r'_e)_e \cdot (r''_e)_e) \cdot (r'''_e)_e &= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} r'_{e'}\, r''_{e''}\Big)_e \cdot (r'''_e)_e \\
&= \Big(\sum\nolimits_{\substack{(\tilde e,\,e''')\,\in\,E_I\times E_I\\ \tilde e+e'''=\tilde e}}\ \sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=\tilde e}} r'_{e'}\, r''_{e''} r'''_{e'''}\Big)_e \\
&= \Big(\sum\nolimits_{\substack{(e',\,e'',\,e''')\,\in\,E_I\times E_I\times E_I\\ e'+e''+e'''=e}} r'_{e'}\, r''_{e''} r'''_{e'''}\Big)_e\,.
\end{aligned}$$

Zum anderen erhalten wir genauso

$$(r'_e)_e \cdot ((r''_e)_e \cdot (r'''_e)_e) = \Big(\sum_{\substack{(e',\,e'',\,e''')\,\in\,E_I\times E_I\times E_I\\ e'+e''+e'''=e}} r'_{e'}\, r''_{e''} r'''_{e'''}\Big)_e\,.$$

Zeigen wir, daß $1_{R[X]} := (\partial_{(0)_i,e})_e$ das neutrale Element der Multiplikation ist.

Für $(r_e)_e \in R[X]$ wird

$$\begin{aligned}
1_{R[X]} \cdot (r_e)_e &= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} \partial_{(0)_i,e'}\, r''_{e''}\Big)_e \\
&= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e\\ e'=(0)_i}} r''_{e''}\Big)_e \\
&= \Big(r''_e\Big)_e\,.
\end{aligned}$$

Zeigen wir die Distributivität. Seien $(r'_e)_e\,,\,(\tilde r'_e)_e\,,\,(r''_e)_e \;\in\; R[X]$ gegeben. Es wird

$$\begin{aligned}
((r'_e)_e + (\tilde r'_e)_e) \cdot (r''_e)_e &= (r'_e + \tilde r'_e)_e \cdot (r''_e)_e \\
&= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} (r'_{e'} + \tilde r'_{e'})\, r''_{e''}\Big)_e \\
&= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} r'_{e'}\, r''_e + \tilde r'_{e'}\, r''_{e''}\Big)_e \\
&= \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} r'_{e'}\, r''_e\Big)_e + \Big(\sum\nolimits_{\substack{(e',\,e'')\,\in\,E_I\times E_I\\ e'+e''=e}} \tilde r'_{e'}\, r''_{e''}\Big)_e \\
&= (r'_e)_e \cdot (r''_e)_e + (\tilde r'_e)_e \cdot (r''_e)_e\,.
\end{aligned}$$

Ad (3). Es ist zu zeigen, daß $\alpha_{R,X}$ ein Ringmorphismus ist.

Es ist $\alpha_{R,X}$ ersichtlich mit Addition verträglich.

Es ist $\alpha_{R,X}(1_R) = (\partial_{(0)_i,e})_e = 1_{R[X]}$; cf. (2).

Zeigen wir die Verträglichkeit mit der Multiplikation. Seien r', $r'' \in R$ gegeben. Es wird

$$\begin{array}{rcl} \alpha_{R,X}(r') \cdot \alpha_{R,X}(r'') & = & (r'\partial_{(0)_i,e})_e \cdot (r''\partial_{(0)_i,e})_e \\ & \overset{\text{Beh.}}{=} & (r'\partial_{(0)_i+(0)_i,e})_e \\ & = & (r'\partial_{(0)_i,e})_e \\ & = & \alpha_{R,X}(r'r'') \; . \end{array}$$

Ad (4). Sei $(r_e)_e \in R[X]$ gegeben. Nach Entfernung der mißbräuchlichen Bezeichnung ist

$$(r_e)_{e \in E_I} \overset{!}{=} \sum_{\tilde{e} \,=\, (\tilde{e}_i)_i \,\in\, E_I} (r_{\tilde{e}}\partial_{(0)_i,e})_e \prod_{i \in I} (\partial_{d[i],e})^{\tilde{e}_i}$$

zu zeigen.

Es ist $(r_e)_e = \sum_{\tilde{e} \in E_I} (r_{\tilde{e}}\partial_{\tilde{e},e})_e$. Somit bleibt

$$(r\partial_{\tilde{e},e})_e \overset{!}{=} (r\partial_{(0)_i,e})_e \prod_{i \in I} (\partial_{d[i],e})^{\tilde{e}_i}$$

zu zeigen für $r \in R$ und $\tilde{e} \in E_I$.

Es ist

$$\begin{array}{rcl} (r\partial_{(0)_i,e})_e \cdot (\partial_{\tilde{e},e})_e & = & \left(\sum_{\substack{(e',\, e'') \,\in\, E_I \times E_I \\ e' + e'' \,=\, e}} r_{\tilde{e}}\partial_{(0)_i,e'} r\partial_{(0)_i,e'}\, \partial_{\tilde{e},e''} \right)_e \\ & = & \left(\sum_{\substack{(e',\, e'') \,\in\, E_I \times E_I \\ e' + e'' \,=\, e \\ e' \,=\, (0)_i \,,\; e'' \,=\, \tilde{e}}} r \right)_e \\ & = & (r\partial_{\tilde{e},e})_e \; . \end{array}$$

Somit bleibt

$$(\partial_{\tilde{e},e})_e \overset{!}{=} \prod_{i \in I} (\partial_{d[i],e})^{\tilde{e}_i}$$

zu zeigen für $\tilde{e} \in E_I$.

Da $\tilde{e} = \sum_{i \in I} \tilde{e}_i \partial_{d[i],e}$ ist, folgt dies durch iterierte Anwendung der Behauptung.

Aufgabe 8

Ad (1). Es ist $0 \in \mathfrak{a}$. Für s, $s' \in S$ und a, $a' \in \mathfrak{a}$ wird

$$f(sa + s'a') \;=\; f(s) \cdot f(a) + f(s') \cdot f(a') \;\in\; \mathfrak{b}$$

und also

$$sa + s'a' \;\in\; \mathfrak{a} \; .$$

Ad (2). Sind s, $s' \in S$ mit $s + \tilde{\mathfrak{a}} = s' + \tilde{\mathfrak{a}}$ gegeben, dann ist $f(s) - f(s') = f(s - s') \in f(\tilde{\mathfrak{a}}) \subseteq \mathfrak{b}$ und also $f(s) + \mathfrak{b} = f(s') + \mathfrak{b}$. Somit ist $\bar{f}$ wohldefiniert.

Sind s, $s' \in S$ gegeben, so wird

$$\bar{f}(s + s') \;=\; f(s + s') + \mathfrak{b} \;=\; f(s) + f(s') + \mathfrak{b} \;=\; (f(s) + \mathfrak{b})(f(s') + \mathfrak{b}) \;=\; \bar{f}(s) + \bar{f}(s')$$

und

$$\bar{f}(s \cdot s') \;=\; f(s \cdot s') \cdot \mathfrak{b} \;=\; f(s) \cdot f(s') \cdot \mathfrak{b} \;=\; (f(s) \cdot \mathfrak{b})(f(s') \cdot \mathfrak{b}) \;=\; \bar{f}(s) \cdot \bar{f}(s') \,.$$

Ferner ist

$$\bar{f}(1_{S/\tilde{\mathfrak{a}}}) \;=\; \bar{f}(1_S + \tilde{\mathfrak{a}}) \;=\; f(1_S) + \mathfrak{b} \;=\; 1_T + \mathfrak{b} \;=\; 1_{T/\mathfrak{b}} \,.$$

Also ist $\bar{f}$ ein Ringmorphismus.

Für $r \in R$ ist

$$\big(\bar{f} \circ (\rho_{S,\tilde{\mathfrak{a}}} \circ \alpha)\big)(r) \;=\; \bar{f}(\alpha(r) + \tilde{\mathfrak{a}}) \;=\; f(\alpha(r)) + \mathfrak{b} \;=\; \beta(r) + \mathfrak{b} \;=\; \big(\rho_{T,\mathfrak{b}} \circ \beta\big)(r)$$

und also

$$\bar{f} \circ (\rho_{S,\tilde{\mathfrak{a}}} \circ \alpha \;=\; \rho_{T,\mathfrak{b}} \circ \beta \,.$$

Somit ist $\bar{f}$ ein R-Algebrenmorphismus.

Ad (3). Wir haben zu zeigen, daß $\bar{f}$ aus (2) diesenfalls injektiv ist. Sei $s \in S$ mit $\bar{f}(s+\mathfrak{a}) = 0_{T/\mathfrak{b}}$ gegeben. Wir haben zu zeigen, daß $s + \mathfrak{a} \overset{!}{=} 0_{S/\mathfrak{a}}$ ist.

Es ist $f(s) + \mathfrak{b} = \bar{f}(s + \mathfrak{a}) = 0_{T/\mathfrak{b}} = 0_T + \mathfrak{b}$, i.e. $f(s) \in \mathfrak{b}$, i.e. $s \in \mathfrak{a}$, i.e. $s + \mathfrak{a} = 0_{S/\mathfrak{a}}$.

Aufgabe 9

Es ist $R/\mathfrak{a}$ bekanntermaßen eine abelsche Gruppe, mit $0_{R/\mathfrak{a}} = 0_R + \mathfrak{a}$.

Wohldefiniertheit des Produkts. Seien r, $\tilde{r}$, r', $\tilde{r}'$ mit $r + \mathfrak{a} = \tilde{r} + \mathfrak{a}$ und $r' + \mathfrak{a} = \tilde{r}' + \mathfrak{a}$ gegeben. Zu zeigen ist $rr' + \mathfrak{a} \overset{!}{=} \tilde{r}\tilde{r}' + \mathfrak{a}$.

Schreibe $\tilde{r} = r + a$ und $\tilde{r}' = r' + a'$ mit a, $a' \in \mathfrak{a}$. Es wird

$$\tilde{r}\tilde{r}' - rr' \;=\; (r + a)(r' + a') - rr' \;=\; ar' + ra' + aa' \;\in\; \mathfrak{a}\,,$$

wie zu zeigen war.

Es ist

$$\begin{array}{rcl} (r + \mathfrak{a}) \cdot ((r' + \mathfrak{a}) \cdot (r'' + \mathfrak{a})) & = & (r + \mathfrak{a}) \cdot (r'r'' + \mathfrak{a}) \\ & = & rr'r'' + \mathfrak{a} \\ & = & (rr' + \mathfrak{a}) \cdot (r'' + \mathfrak{a}) \\ & = & ((r + \mathfrak{a}) \cdot (r' + \mathfrak{a})) \cdot (r'' + \mathfrak{a}) \end{array}$$

für r, r', $r'' \in R$.

Es ist $(r + \mathfrak{a}) \cdot (r' + \mathfrak{a}) = rr' + \mathfrak{a} = r'r + \mathfrak{a} = (r' + \mathfrak{a}) \cdot (r + \mathfrak{a})$ für r, $r' \in R$.

Es ist $(1_R + \mathfrak{a}) \cdot (r + \mathfrak{a}) = 1_R \cdot r + \mathfrak{a} = r + \mathfrak{a}$ für $r \in R$. Also ist $1_{R/\mathfrak{a}} := 1_R + \mathfrak{a}$ multiplikativ neutral.

Es ist

$$\begin{array}{rcl} (r + \mathfrak{a}) \cdot ((r' + \mathfrak{a}) + (r'' + \mathfrak{a})) & = & (r + \mathfrak{a}) \cdot (r' + r'' + \mathfrak{a}) \\ & = & r(r' + r'') + \mathfrak{a} \\ & = & rr' + rr'' + \mathfrak{a} \\ & = & (rr' + \mathfrak{a}) + (rr'' + \mathfrak{a}) \\ & = & (r + \mathfrak{a}) \cdot (r' + \mathfrak{a}) + (r + \mathfrak{a}) \cdot (r'' + \mathfrak{a}) \end{array}$$

für r, r', $r'' \in R$.

Aufgabe 10

Wohldefiniertheit $\mapsto$. Ist $\mathfrak{c}$ ein Ideal in T, so ist zu zeigen, daß $f^{-1}(\mathfrak{c})$ ein Ideal in S ist. Es ist $0 \in f^{-1}(\mathfrak{c})$, da $f(0) = 0 \in \mathfrak{c}$ liegt. Sind ferner a, $a' \in f^{-1}(\mathfrak{c})$ und s, $s' \in T$, dann ist $sa + s'a' \in f^{-1}(\mathfrak{c})$, da

$$f(sa + s'a') \;=\; f(s)f(a) + f(s')f(a') \;\in\; \mathfrak{c}$$

liegt.

Ferner ist $\mathfrak{k} \subseteq f^{-1}(\mathfrak{c})$, da $f(\mathfrak{k}) = 0 \subseteq \mathfrak{c}$ liegt.

Wohldefiniertheit $\hookleftarrow$. Ist $\mathfrak{b}$ ein Ideal in S, so ist zu zeigen, daß $f(\mathfrak{b})$ ein Ideal in T ist. Es ist $0 = f(0) \in f(\mathfrak{b})$. Sind ferner $b,\ b' \in \mathfrak{b}$ und $t,\ t' \in T$, dann gibt es $s,\ s' \in S$ mit $f(s) = t$ und $f(s') = t'$, weswegen wir

$$t \cdot f(b) + t' \cdot f(b') \ = \ f(s) \cdot f(b) + f(s') \cdot f(b') \ = \ f(sb + s'b') \ \in \ f(\mathfrak{b})$$

erhalten.

Inversion.

Sei zuerst $\mathfrak{c}$ ein Ideal in T. Es ist $f(f^{-1}(\mathfrak{c})) \subseteq \mathfrak{c}$. Sei umgekehrt $c \in \mathfrak{c}$ gegeben. Wir haben $c \overset{!}{\in} f(f^{-1}(\mathfrak{c}))$ zu zeigen. Da f surjektiv ist, gibt es ein $s \in S$ mit $f(s) = c$. Daher ist $s \in f^{-1}(\mathfrak{c})$. Also ist $c = f(s) \in f(f^{-1}(\mathfrak{c}))$.

Sei dann $\mathfrak{b}$ ein Ideal in S mit $\mathfrak{k} \subseteq \mathfrak{b}$. Es ist $\mathfrak{b} \subseteq f^{-1}(f(\mathfrak{b}))$. Sei umgekehrt $s \in f^{-1}(f(\mathfrak{b}))$ gegeben. Wir haben $s \overset{!}{\in} \mathfrak{b}$ zu zeigen. Es ist $f(s) = f(b)$ für ein $b \in \mathfrak{b}$. Also ist $f(s - b) = 0$, i.e. $s - b \in \mathfrak{k}$. Da $\mathfrak{k} \subseteq \mathfrak{b}$ liegt, folgt $s = b + (s - b) \in \mathfrak{b}$.

Aufgabe 11

Ad (1). Die Aussage ist richtig.

Sei $\mathfrak{a} \subseteq \mathbf{Z}$ ein Ideal. Wir müssen zeigen, daß $\mathfrak{a}$ ein Hauptideal ist. O.E. ist $\mathfrak{a} \neq (0)$.

Sei $z \in \mathfrak{a} \smallsetminus \{0\}$ mit $|z|$ minimal. O.E. ist $z > 0$.

Wir *behaupten*, es ist $\mathfrak{a} \overset{!}{=} (z)$. Zu zeigen ist nur $\subseteq$.

Sei $a \in \mathfrak{a}$. Zu zeigen ist $a \overset{!}{\in} (z)$.

Division mit Rest liefert $a = zs + r$ mit $r \in [0, z - 1]$. *Wäre* $r \neq 0$, dann wäre $r = a - zs \in \mathfrak{a} \smallsetminus \{0\}$, aber $|r| = r < z = |z|$, was nach Wahl von z *nicht* stimmt. Also ist $r = 0$ und also $a = zs$ *in*(z).

Ad (2). Die Aussage ist richtig.

Sei $\mathfrak{a} \subseteq K[X]$ ein Ideal. Wir müssen zeigen, daß $\mathfrak{a}$ ein Hauptideal ist. O.E. ist $\mathfrak{a} \neq (0)$.

Sei $f(x) \in \mathfrak{a} \smallsetminus \{0\}$ mit $\deg(f)$ minimal. O.E. ist $f(X)$ normiert.

Wir *behaupten*, es ist $\mathfrak{a} \overset{!}{=} (f(X))$. Zu zeigen ist nur $\subseteq$.

Sei $g(X) \in \mathfrak{a}$. Zu zeigen ist $g(X) \overset{!}{\in} (f(X))$.

Polynomdivision mit Rest liefert $g(X) = f(X) \cdot s(X) + r(X)$ mit $\deg(r) \in [0, \deg(f(X)) - 1]$. *Wäre* $r(X) \neq 0$, dann wäre $r(X) = g(X) - f(X) \cdot s(X) \in \mathfrak{a} \smallsetminus \{0\}$, aber $\deg(r(X)) < \deg(f(X))$, was nach Wahl von $f(X)$ *nicht* stimmt. Also ist $r(X) = 0$ und also $g(X) = f(X) \cdot s(X)$ *in*$(f(X))$.

Ad (3). Die Aussage ist falsch.

Seien X und Y zwei Elemente.

Nach (2) ist $K[X]$ eine Hauptidealalgebra über K.

Wir wollen zeigen, daß (X, Y) kein Hauptideal in $K[X, Y]$ ist.

Annahme, doch. Dann gibt es ein Polynom $f(X, Y) \in K[X, Y]^\times$ mit $(X, Y) = (f(X, Y))$.

Da $X = f(X, Y) \cdot u(X, Y)$ für ein $u(X, Y) \in K[X, Y]^\times$ sein muß, ist der Grad von $f(X, Y)$ in Y gleich 0.

Da $Y = f(X, Y) \cdot v(X, Y)$ für ein $v(X, Y) \in K[X, Y]^\times$ sein muß, ist der Grad von $f(X, Y)$ in X gleich 0.

Also ist $f(X,Y) = s$ für ein $s \in K^\times \subseteq \mathrm{U}(K[X,Y])$. Dann aber ist $(X,Y) = (s) = K[X,Y]$.

Aber es ist $1 \notin (X,Y)$, da aus $1 = X \cdot a(X,Y) + Y \cdot b(X,Y)$ mit $a(X,Y),\, b(X,Y) \in K[X,Y]$ durch Einsetzen von 0 für X und von 0 für Y folgte, daß $1 = 0$ ist, was in einem Körper nicht zutrifft. Wir haben einen *Widerspruch.*

Ad (4). Die Aussage ist falsch.

Sei etwa $\mathfrak{a} := (2) \subseteq \mathbf{Z}$ und $\mathfrak{b} := (2) \subseteq \mathbf{Z}$. Dann ist $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{(4)} = (2)$, wohingegen $\sqrt{\mathfrak{a}}\sqrt{\mathfrak{b}} = (2)(2) = (4)$ ist.

Ad (5). Die Aussage ist richtig.

Zum einen folgt aus $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$, daß $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subseteq \sqrt{\mathfrak{a}}$ liegt. Genauso folgt $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subseteq \sqrt{\mathfrak{b}}$. Somit haben wir $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subseteq \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.

Um $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \overset{!}{\supseteq} \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$ zu zeigen, sei $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$ gegeben. Wir haben $x \overset{!}{\in} \sqrt{\mathfrak{a} \cap \mathfrak{b}}$ zu zeigen.

Es gibt $k,\, \ell \in \mathbf{Z}_{\geqslant 0}$ mit $x^k \in \mathfrak{a}$ und $x^\ell \in \mathfrak{b}$. Sei $m := \max\{k, \ell\}$. Dann ist $x^m \in \mathfrak{a} \cap \mathfrak{b}$. Also ist $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

Ad (6). Die Aussage ist falsch.

Sei etwa $\mathfrak{a} := (X^2 + Y) \subseteq \mathbf{C}[X,Y]$ und $\mathfrak{b} := (Y) \subseteq \mathbf{C}[X,Y]$.

Zum einen ist $\mathfrak{a} + \mathfrak{b} = (X^2 + Y, Y) = (X^2, Y)$ und also $X \in \sqrt{(X^2, Y)}$.

Zum anderen wollen wir zeigen, daß $X \notin \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$ enthalten ist.

Dazu wollen wir zeigen, daß $\mathfrak{a} \overset{!}{=} \sqrt{\mathfrak{a}}$ und $\mathfrak{b} \overset{!}{=} \sqrt{\mathfrak{b}}$ ist. Denn dann ist $\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}} = \mathfrak{a} + \mathfrak{b} = (X^2, Y)$, sodaß es darin kein Polynom gibt, welches in X den Grad 1 hat.

Es genügt also zu zeigen, daß $\mathbf{C}[X,Y]/(Y)$ und $\mathbf{C}[X,Y]/(X^2+Y)$ integer sind; cf. Definition 33, Bemerkung 43.(2).

Die folgenden $\mathbf{C}$-Algebrenmorphismen werden mit Hilfe von Lemma 20 und Bemerkung 26 konstruiert.

Es wird der $\mathbf{C}$-Algebrenmorphimus $\mathbf{C}[X,Y]/(Y) \to \mathbf{C}[X]\colon Y \mapsto 0,\ X \mapsto X$ beidseitig invertiert durch $\mathbf{C}[X] \to \mathbf{C}[X,Y]/(Y)\colon X \mapsto X + (Y)$. Also ist $\mathbf{C}[X,Y]/(Y)$ isomorph zur integren $\mathbf{C}$-Algebra $\mathbf{C}[X]$ und damit selbst integer.

Es wird der $\mathbf{C}$-Algebrenmorphimus $\mathbf{C}[X,Y]/(X^2+Y) \to \mathbf{C}[X]\colon Y \mapsto -X^2,\ X \mapsto X$ beidseitig invertiert durch $\mathbf{C}[X] \to \mathbf{C}[X,Y]/(Y)\colon X \mapsto X + (X^2+Y)$. Also ist $\mathbf{C}[X,Y]/(X^2+Y)$ isomorph zur integren $\mathbf{C}$-Algebra $\mathbf{C}[X]$ und damit selbst integer.

Aufgabe 12

Ad (1) $\Rightarrow$ (2). Sei M eine nichtleere Teilmenge von $\mathrm{Ideale}(S)$. *Annahme,* es gibt in S kein maximales Element.

Da M nichtleer ist, können wir ein $\mathfrak{a}_1 \in M$ wählen.

Da $\mathfrak{a}_1$ in M nicht maximal ist, können wir ein $\mathfrak{a}_2 \in M$ wählen mit $\mathfrak{a}_1 \subset \mathfrak{a}_2$.

Da $\mathfrak{a}_2$ in M nicht maximal ist, können wir ein $\mathfrak{a}_3 \in M$ wählen mit $\mathfrak{a}_2 \subset \mathfrak{a}_3$.

Und so fort.

Dies liefert eine aufsteigende abzählbare Kette von Idealen

$$\mathfrak{a}_1 \ \subset\ \mathfrak{a}_2 \ \subset\ \mathfrak{a}_3 \ \subset\ \dots$$

Also ist S nicht noethersch; cf. Lemma 53. Wir haben einen *Widerspruch.*

Ad (2) $\Rightarrow$ (1). Sei

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

eine aufsteigende abzählbare Kette von Idealen in S. Wir haben zu zeigen, daß es ein $k \in \mathbf{Z}_{\geqslant 1}$ mit $\mathfrak{a}_k = \mathfrak{a}_i$ gibt für $i \in \mathbf{Z}_{\geqslant k}$; cf. Lemma 53.

Sei $M := \{\, \mathfrak{a}_i : i \in \mathbf{Z}_{\geqslant 1} \,\}$. Es ist M eine nichtleere Teilmenge von Ideale(S). Also können wir in M ein maximales Element $\mathfrak{a}_k$ wählen, wobei $k \in \mathbf{Z}_{\geqslant 1}$. Für $i \in \mathbf{Z}_{\geqslant k}$ ist also $\mathfrak{a}_k \subseteq \mathfrak{a}_i$ und nicht $\mathfrak{a}_k \subset \mathfrak{a}_i$, folglich also $\mathfrak{a}_k = \mathfrak{a}_i$.

Aufgabe 13

Ad (1). Wir sehen $K[X,Y]$ als Teilalgebra von $K[X,Y,Z]$ an.

Dank Lemma 20 ist $K[X,Y] \to S\colon X \mapsto \bar{X},\ Y \mapsto \bar{Y}$ ein wohldefinierter K-Algebrenmorphismus.

Sein Kern ist $(XY - Z^2) \cap K[X,Y]$. Ein Element darin ist von der Form $(XY - Z^2) \cdot u(X,Y,Z)$, wobei $u(X,Y,Z) \in K[X,Y,Z]$. *Wäre* $u(X,Y,Z) \neq 0$, dann wäre der Grad in Z von $(XY - Z^2) \cdot u(X,Y,Z)$ größer als 0, was aber $(XY - Z^2) \cdot u(X,Y,Z) \in K[X,Y]$ *widerspricht.*

Somit ist der Kern gleich 0 und unser K-Algebrenmorphismus injektiv.

Mit anderen Worten, für $f(X,Y) \in K[X,Y]$ ist genau dann $f(\bar{X},\bar{Y}) = 0$, wenn $f(X,Y) = 0$ ist.

Ad (2).

Existenz. Für $i,\ j,\ k \in \mathbf{Z}_{\geqslant 0}$ und $\ell \in \{0,1\}$ ist $\bar{X}^i \bar{Y}^j \bar{Z}^{2k+\ell} = \bar{X}^{i+k} \bar{Y}^{j+k} \bar{Z}^{\ell}$.

Eindeutigkeit. Seien $f(X,Y)$, $g(X,Y)$, $\tilde{f}(X,Y)$, $\tilde{g}(X,Y) \in K[X,Y]$ gegeben mit $\eta = f(\bar{X},\bar{Y}) + \bar{Z}\, g(\bar{X},\bar{Y}) = \tilde{f}(\bar{X},\bar{Y}) + \bar{Z}\, \tilde{g}(\bar{X},\bar{Y})$. Schreibe $u(X,Y) := f(X,Y) - \tilde{f}(X,Y)$ und $v(X,Y) := g(X,Y) - \tilde{g}(X,Y)$. Es ist $u(\bar{X},\bar{Y}) + \bar{Z}\, v(\bar{X},\bar{Y}) = 0$. Mit anderen Worten, es ist $u(X,Y) + Z\, v(X,Y) = w(X,Y)(XY - Z^2)$ für ein $w(X,Y) \in K[X,Y]$. Wir haben zu zeigen, daß $u(X,Y) \overset{!}{=} 0$ und $v(X,Y) \overset{!}{=} 0$.

Wäre $w(X,Y) \neq 0$, dann wäre der Grad von $u(X,Y) + Z\, v(X,Y)$ in Z größer oder gleich 2. Dies ist aber *nicht* der Fall. Also ist $w(X,Y) = 0$. Koeffizientenvergleich in Potenzen von Z gibt nun $u(X,Y) = 0$ und $v(X,Y) = 0$.

Ad (3). Wir haben zu zeigen, daß $S/\mathfrak{p}$ integer ist.

Die folgenden K-Algebrenmorphismen werden mit Hilfe von Lemma 20 und Bemerkung 26 konstruiert.

Da $0 \cdot Y - 0^2 = 0$ ist, haben wir den K-Algebrenmorphismus

$$\begin{array}{rcl} S & \to & K[Y] \\ \bar{X} & \mapsto & 0 \\ \bar{Y} & \mapsto & Y \\ \bar{Z} & \mapsto & 0\,. \end{array}$$

Also haben wir den K-Algebrenmorphismus

$$\begin{array}{rcl} S/\mathfrak{p} & \to & K[Y] \\ \bar{X} + \mathfrak{p} & \mapsto & 0 \\ \bar{Y} + \mathfrak{p} & \mapsto & Y \\ \bar{Z} + \mathfrak{p} & \mapsto & 0\,. \end{array}$$

Hierbei sind $\bar{X} + \mathfrak{p}$ und $\bar{Z} + \mathfrak{p}$ nur der Form halber aufgelistet; sie sind beide 0.

Dieser wird beidseitig invertiert vom K-Algebrenmorphismus

$$\begin{array}{rcl} S/\mathfrak{p} & \leftarrow & K[Y] \\ \bar{Y} + \mathfrak{p} & \leftarrow\!\shortmid & Y\,. \end{array}$$

Denn zum einen wird $Y \mapsto \bar{Y} + \mathfrak{p} \mapsto Y$ geschickt. Zum anderen werden $\bar{X} + \mathfrak{p} \mapsto 0 \mapsto 0 = \bar{X} + \mathfrak{p}$ und $\bar{Y} + \mathfrak{p} \mapsto Y \mapsto \bar{Y} + \mathfrak{p}$, schließlich $\bar{Z} + \mathfrak{p} \mapsto 0 \mapsto 0 = \bar{Z} + \mathfrak{p}$.

Folglich ist $S/\mathfrak{p}$ als K-Algebra isomorph zu $K[Y]$. Da letztere integer ist, gilt dies auch für erstere.

Ad (4). Da $\mathfrak{p} = (\bar{X}, \bar{Z})$, ist

$$\mathfrak{p}^2 \;=\; (\bar{X}^2, \bar{X}\bar{Z}, \bar{Z}^2)\;.$$

Dank (3) ist also jedes Element von $\mathfrak{p}^2$ eine $K[\bar{X}, \bar{Y}]$-Linearkombination der Elemente

$$\bar{X}^2,\ \bar{X}^2\bar{Z},\ \bar{X}\bar{Z},\ \bar{X}\bar{Z}^2,\ \bar{Z}^2,\ \bar{Z}^3$$

i.e. der Elemente

$$\bar{X}^2,\ \bar{X}^2\bar{Z},\ \bar{X}\bar{Z},\ \bar{X}^2\bar{Y},\ \bar{X}\bar{Y},\ \bar{X}\bar{Y}\bar{Z}\ ,$$

i.e. der Elemente

$$\bar{X}^2,\ \bar{X}\bar{Z},\ \bar{X}\bar{Y}\ ,$$

wie benötigt.

Mit anderen Worten, für $f(X,Y),\, g(X,Y) \in K[X]$ ist genau dann $f(\bar{X},\bar{Y}) + \bar{Z}\, g(\bar{X},\bar{Y}) \in \mathfrak{p}^2$, wenn $f(X,Y) \in (X^2, XY)$ und $g(X,Y) \in (X)$ liegen; cf. $(1,2)$.

Ad (5). Es ist $\bar{X}\bar{Y} \in \mathfrak{p}^2$; cf. (4).

Wäre $\bar{X} \in \mathfrak{p}^2$, dann wäre gemäß (4) auch $X \in (X^2, XY)$ und also $1 \in (X,Y)$, was aber *nicht* zutrifft, wie Einsetzen von 0 für X und von 0 für Y zeigt.

Also ist $\bar{X} \notin \mathfrak{p}^2$.

Sei $n \in \mathbf{Z}_{\geqslant 0}$. *Wäre* $\bar{Y}^n \in \mathfrak{p}^2$, dann wäre gemäß (4) auch $Y \in (X^2, XY)$, was aber *nicht* zutrifft, wie Einsetzen von 0 für Y zeigt.

Also ist $\bar{Y}^n \notin \mathfrak{p}^2$.

Ad (6). Es ist $\mathfrak{p}^2$ kein Primärideal von S, da gemäß (5) zwar $\bar{X}\bar{Y}$ in $\mathfrak{p}^2$ liegt, $\bar{X}$ nicht in $\mathfrak{p}^2$ liegt, aber für jedes $n \in \mathbf{Z}_{\geqslant 0}$ das Element $\bar{Y}^n$ auch nicht in $\mathfrak{p}^2$ liegt; cf. Bemerkung 40.

Schließlich ist $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}^2} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$; cf. Bemerkung 43.(2). Also ist $\sqrt{\mathfrak{p}^2} = \mathfrak{p}$ prim; cf. (3).

Literatur

[1] Altman, A.; Kleiman, S., *A Term of Commutative Algebra,* Vorlesungsskript, 2012.

[2] Atiyah, M.F., Macdonald, I.G., *Introduction to Commutative Algebra,* Addison-Wesley, 1969.

[3] Brüske, R.; Ischebeck, F.; Vogel F.;, *Kommutative Algebra*, B.I., 1989.

[4] Eisenbud, D., *Commutative algebra, with a view toward algebraic geometry*, Springer GTM 150, 1995.

[5] Hochster, M., *Dimension theory and systems of parameters*, draft, `www.math.lsa.umich.edu/~hochster/615W10/supDim.pdf`, 2010.

[6] Külshammer, B., *Kommutative Algebra*, Vorlesungsskript, 2016.

[7] Kurosch, *Lectures in general algebra*, Pergamon, 1965.

[8] Reimann, H., *Algebraische Geometrie 1,* Vorlesungsmitschrieb, Bielefeld, 2000.