Kommutative Algebra

Vorlesung von
Prof. Dr. Niko Naumann
im Sommersemester 2012
Überarbeitung und Textsatz in LyX von
Andreas Völklein

Stand: 10. Juli 2012

ACHTUNG

Diese Mitschrift ersetzt *nicht* die Vorlesung.
Es wird daher *dringend* empfohlen, die Vorlesung zu besuchen.

Copyright Notice

Disclaimer of Warranty

Limitation of Liability

Links

Der Text der „GNU Free Documentation License" kann auch auf der Seite

`https://www.gnu.org/licenses/fdl-1.3.de.html`

nachgelesen werden.
Eine transparente Kopie der aktuellen Version dieses Dokuments kann von

`https://github.com/andiv/KomAlg`

heruntergeladen werden.

Literatur

- Michael Francis Atiyah, Ian G. Macdonald: *Introduction to commutative algebra*, Westview Press, 1994; ISBN: 0-201-40751-5
- David Eisenbud: *Commutative algebra with a view toward algebraic geometry*, Springer, 2004; ISBN: 3-540-94269-6
- Hideyuki Matsumura: *Commutative ring theory*, Cambridge University Press, 2005 ISBN: 0-521-36764-6
- Nicolas Bourbaki: *Commutative algebra*, Springer, 1991 ISBN: 3-540-64239-0

Inhaltsverzeichnis

1 Ringe und Ideale

1.1 **Definition** (Ring, Ringhomomorphismus)

i) Ein (*unitärer*, *kommutativer*) *Ring* ist ein Tupel $(A, +, \cdot, 0, 1)$ mit den Eigenschaften:

a) $(A, +, 0)$ ist eine abelsche Gruppe.

b) Für alle $x,y,z \in A$ gelten:

$$\begin{aligned} (xy)\,z &= x\,(yz) && \text{(Assoziativität)} \\ x\,(y+z) &= xy + xz && \text{(Distributivität)} \\ xy &= yx && \text{(Kommutativität)} \\ x \cdot 1 &= x && \text{(neutrales Element)} \end{aligned}$$

ii) Sind A und B Ringe, so ist ein *Ringhomomorphismus* (*von A nach B*) (Abkürzung: Ringhom.) eine Abbildung $f : A \to B$, sodass für alle $x,y \in A$ gilt:

a) $f(x+y) = f(x) + f(y)$

b) $f(xy) = f(x)\,f(y)$

c) $f(1) = 1$

Aus a) folgt direkt $f(0) = 0$, da Ringe additive Gruppen sind.

Aus b) folgt aber nicht c), da Ringe im Allgemeinen keine multiplikativen Gruppen sind.

1.2 Beispiel

i) Bekannte Ringe sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\mathbf{i}] = \left\{a + b\mathbf{i} \middle| a,b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$, der Polynomring $A[X]$ eines Rings A und der Produktring $A \times B$ der Ringe A und B.

ii) Für jeden Ring A existiert genau ein Ringhomomorphismus $\mathbb{Z} \to A$.

Für jeden Ring A ist die Abbildung von Mengen

$$\begin{aligned} \left\{f : \mathbb{Z}[X] \to A \middle| f \text{ ist Ringhom.}\right\} &\xrightarrow{\sim} A \\ f &\mapsto f(X) \end{aligned}$$

bijektiv. (Die Ringhomomorphismen f sind die Einsetzungshomomorphismen.)

1.3 Definition (Unterring)

Sei A ein Ring.
Eine Teilmengen $B \subseteq A$ heißt *Unterring* (*von* A), wenn für alle x,$y \in B$ gilt:

i) $x - y \in B$, $x \cdot y \in B$

ii) $1 \in B$

In diesem Fall ist $\left(B, + \big|_{B\times B}, \cdot \big|_{B\times B}, 0, 1\right)$ wieder ein Ring.

1.4 Beispiel

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind Unterringe, nicht aber $\mathbb{N} \subseteq \mathbb{Z}$.

1.5 Definition und Bemerkung (Ideal, Quotientenring)

Sei A ein Ring.

i) Eine Teilmenge $I \subseteq A$ heißt *Ideal* (*von* A), falls folgende Eigenschaften gelten:

   a) $I \subseteq (A, +, 0)$ ist eine Untergruppe.
   b) Für alle $x \in A$ und $y \in I$ gilt $xy \in I$.

ii) Ist $I \subseteq A$ ein Ideal, so ist die für alle x,$y \in A$ durch

$$x \equiv y \mod I \qquad :\Leftrightarrow \qquad x - y \in I$$

   (lies: „*x ist kongruent zu y modulo I*“) auf A definierte Relation eine Äquivalenzrelation und es existiert genau eine Ringstruktur ${}^{A}\!/_{I}$, sodass die kanonische Abbildung

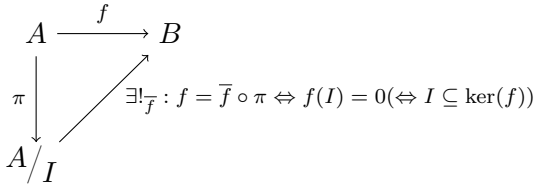
$$\begin{aligned} \pi : A &\to {}^{A}\!/_{I} \\ x &\mapsto \pi(x) := [x] := (x \mod I) \end{aligned}$$

   ein Ringhomomorphismus ist.
   Es gilt $\ker(\pi) = I$. Der Ring ${}^{A}\!/_{I}$ heißt *Quotientenring* (*von* A *bezüglich* I).

iii) Sind $I \subseteq A$ ein Ideal und B ein Ring, so ist die Abbildung

$$\begin{aligned} \left\{\overline{f} : {}^{A}\!/_{I} \to B \middle| \overline{f} \text{ ist Ringhom.}\right\} &\xrightarrow{\sim} \left\{f : A \to B \middle| f \text{ ist Ringhom.}, f(I) = 0\right\} \\ \overline{f} &\mapsto \overline{f} \circ \pi \end{aligned}$$

   bijektiv.
   Skizze:



   (universelle Eigenschaft des Quotientenrings)

1.6 **Beispiel** (Kern, Bild)

i) Ist $f : A \to B$ ein Ringhomomorphismus, so ist der *Kern*

$$\ker(f) := \{x \in A | f(x) = 0\} \subseteq A$$

ein Ideal und das *Bild*

$$\mathrm{im}(f) := \{f(x) | x \in A\} \subseteq B$$

ein Unterring.
(Ist $B \subseteq A$ ein Unterring, so ist $\iota : B \hookrightarrow A$ ein Ringhomomorphismus mit $\mathrm{im}(\iota) = B$.)

ii) Sind A ein Ring und $n \in \mathbb{N}_{>0}$, so gilt:

$$\left|\left\{f : {}^{\mathbb{Z}}/_{n\mathbb{Z}} \to A \text{ ist Ringhom.}\right\}\right| = \begin{cases} 1 & \text{falls } \underbrace{1 + \ldots + 1}_{n\text{-mal}} = 0 \text{ in } A \\ 0 & \text{sonst} \end{cases}$$

(Verwende 1.2 ii) und 1.5 iii) mit $I = n\mathbb{Z} \subseteq A = \mathbb{Z}$.)

1.7 **Proposition** (Ideale des Quotientenrings)

Seien A ein Ring, $I \subseteq A$ ein Ideal und $\pi : A \to {}^{A}/_{I}$ der kanonische Ringhomomorphismus. Dann ist die Abbildung

$$\begin{aligned} \Phi : M := \{J | J \subseteq A \text{ Ideal mit } I \subseteq J\} &\xrightarrow{\sim} N := \left\{\overline{J} | \overline{J} \subseteq {}^{A}/_{I} \text{ Ideal}\right\} \\ J &\mapsto \Phi(J) := \pi(J) \end{aligned}$$

wohldefiniert und bijektiv und erfüllt:
Für alle Ideale J_1,$J_2 \subseteq A$ mit $I \subseteq J_1$,J_2 gilt:

$$J_1 \subseteq J_2 \Leftrightarrow \Phi(J_1) \subseteq \Phi(J_2)$$

Man sagt, die Bijektion Φ ist ordnungserhaltend.

Beweis

Ist $J \in M$, so ist $\Phi(J) = \pi(J) \subseteq {}^{A}/_{I}$ als Bild des Ringhomomorphismus π ein Unterring von ${}^{A}/_{I}$ und somit ist insbesondere $(\pi(J), +, 0)$ eine Untergruppe.
Seien $\overline{x} \in {}^{A}/_{I}$ und $\overline{y} \in \Phi(J)$ gegeben. Wegen $\Phi(J) = \pi(J)$ und ${}^{A}/_{I} = \pi(A)$ gibt es ein $x \in A$ und ein $y \in J$ mit $\overline{x} = \pi(x)$ und $\overline{y} = \pi(y)$.

$$\overline{x} \cdot \overline{y} = \pi(x)\pi(y) = \pi(xy)$$

Da J ein Ideal ist, folgt aus $y \in J$ und $x \in A$ schon $xy \in J$. Daher ist $\overline{x} \cdot \overline{y} = \pi(xy) \in \pi(J)$, weswegen $\pi(J)$ ein Ideal ist. Also ist Φ wohldefiniert.

Betrachte die Abbildung:

$$\begin{aligned}\Psi : N &\to M\\ \overline{J} &\mapsto \pi^{-1}\left(\overline{J}\right)\end{aligned}$$

Seien $\overline{J} \subseteq {}^{A}\!/_{I}$ ein Ideal und $a,b \in \Psi\left(\overline{J}\right) = \pi^{-1}\left(\overline{J}\right)$, das heißt $\pi(a), \pi(b) \in \overline{J}$. Dann gilt:

$$\pi(a-b) = \underbrace{\pi(a)}_{\in \overline{J}} - \underbrace{\pi(b)}_{\in \overline{J}} \overset{\overline{J} \text{ Ideal}}{\in} \overline{J}$$

Also ist $a - b \in \pi^{-1}\left(\overline{J}\right)$ und somit $\left(\Psi\left(\overline{J}\right), +, 0\right)$ eine Untergruppe von A.
Seien $x \in A$ und $y \in \Psi\left(\overline{J}\right)$, das heißt $\pi(y) \in \overline{J}$, so gilt:

$$\pi(x \cdot y) = \pi(x)\underbrace{\pi(y)}_{\in \overline{J}} \overset{\overline{J} \text{ Ideal}}{\in} \overline{J}$$

Also ist $xy \in \Psi\left(\overline{J}\right)$ und daher $\Psi\left(\overline{J}\right) \subseteq A$ ein Ideal.
Da für alle Ideale $\overline{J} \in {}^{A}\!/_{I}$ schon $0 \in \overline{J}$ gilt, folgt $\pi^{-1}\left(\overline{J}\right) \supseteq \pi^{-1}(0) = \ker(\pi) = I$. Daher ist Ψ wohldefiniert. Nun gilt:

$$\begin{aligned}(\Phi \circ \Psi)\left(\overline{J}\right) &= \left(\pi \circ \pi^{-1}\right)\left(\overline{J}\right) \overset{\pi \text{ surjektiv}}{=} \overline{J}\\ (\Psi \circ \Phi)(J) &= \left(\pi^{-1} \circ \pi\right)(J) = \left\{a + b \middle| a \in J, b \in I\right\} \overset{I \subseteq J}{=} J\end{aligned}$$

Somit ist Ψ die Umkehrabbildung zu Φ, weswegen Φ bijektiv ist.
Zeige nun $J_1 \subseteq J_2 \Leftrightarrow \Phi(J_1) \subseteq \Phi(J_2)$:
„$\Rightarrow$“: Seien $J_1 \subseteq J_2$, und $\overline{x} \in \Phi(J_1) = \pi(J_1)$. Dann gibt es ein $x \in J_1$ mit $\overline{x} = \pi(x)$ und wegen $J_1 \subseteq J_2$ gilt $x \in J_2$. Daher ist $\overline{x} = \pi(x) \in \pi(J_2) = \Phi(J_2)$. Also gilt $\Phi(J_1) \subseteq \Phi(J_2)$.
„$\Leftarrow$“: Seien $\Phi(J_1) \subseteq \Phi(J_2)$ und $x \in J_1$. Dann ist $\overline{x} \in \pi(J_1) = \Phi(J_1) \subseteq \Phi(J_2)$ und daher gibt es ein $\tilde{x} \in J_2$ mit $\pi(\tilde{x}) = \overline{x}$. Also ist $x - \tilde{x} = a \in I$. Wegen $I \subseteq J_2$ folgt somit $x = \tilde{x} + a \in J_2$. Also gilt $J_1 \subseteq J_2$. $\square_{1.7}$

1.8 Beispiel

Die Ideale des Ringes ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \ldots, \overline{5}\right\}$ sind genau die Hauptideale:

$$\left(\overline{0}\right), \left(\overline{3}\right), \left(\overline{2}\right), \left(\overline{1}\right) \subseteq {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$$

1.9 **Definition** (Nullteiler, Integritätsring)

i) Sei A ein Ring. Ein Element $x \in A$ heißt genau dann *Nullteiler*, wenn es ein $x \in A \setminus \{0\}$ mit $xy = 0$ gibt.

ii) Ein *Integritätsring* (Abkürzung: IR) ist ein Ring $A \neq \{0\}$, in dem $0 \in A$ der einzige Nullteiler ist.

1.10 Beispiel

i) $\mathbb{Z}$ ist ein Integritätsring.

ii) Ist A ein Integritätsring, so ist auch $A[X]$ ein Integritätsring. (Gradformel!)

iii) Der Ring $A := {}^{\mathbb{Z}[X]}\!/_{\left(X^2\right)}$ ist kein Integritätsring, denn für $\overline{X} := \left(X \mod \left(X^2\right)\right)$ gilt $\overline{X} \neq 0$, aber auch $\overline{X} \cdot \overline{X} = 0$, weswegen $\overline{X} \in A$ ein Nullteiler ist.
Auch ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$ ist kein Integritätsring, denn $\underbrace{\overline{2}}_{\neq\overline{0}} \cdot \underbrace{\overline{3}}_{\neq\overline{0}} = \overline{0}$.

1.11 Definition (nilpotent)

Sei A ein Ring. Ein $x \in A$ heißt genau dann *nilpotent*, wenn es ein $n \in \mathbb{N}_{>0}$ gibt mit $x^n = 0$.

1.12 Beispiel

i) Ist $0 \neq x \in A \neq \{0\}$ nilpotent, so ist x ein Nullteiler, denn für $N := \min\left\{n \in \mathbb{N}_{>0} \middle| x^n = 0\right\}$ gilt $N \geq 1$ und wegen der Minimalität von N ist $x^{N-1} \neq 0$. Also folgt aus

$$0 = x^N = \underbrace{x}_{\neq 0} \cdot \underbrace{x^{N-1}}_{\neq 0}$$

schon, dass x ein Nullteiler ist.

ii) In dem Produktring $A := \mathbb{Z} \times \mathbb{Z}$ ist $x := (1,0)$ ein Nullteiler, da $x \cdot (0,1) = (0,0) = 0$ gilt, aber nicht nilpotent, denn für alle $n \in \mathbb{N}_{>0}$ gilt:

$$x^n = (1,0)^n = (1^n,0^n) = (1,0) = x \neq 0$$

1.13 Definition und Bemerkung (Einheit, Einheitengruppe)

Sei A ein Ring. Ein $x \in A$ heißt genau dann *Einheit* (*in* A), wenn es ein $y \in A$ mit $xy = 1$ gibt. Die Menge $A^* = \left\{x \in A \middle| x \text{ ist Einheit}\right\}$ der Einheiten ist eine kommutative Gruppe bezüglich der Multiplikation und heißt *die Einheitengruppe von* A.
(Beachte: $\{0\}^* = \{0 = 1\}$)

1.14 Beispiel

i) $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

ii) $\mathbb{Z}[\mathbf{i}]^* = \{\pm 1, \pm \mathbf{i}\}$

iii) Ist A ein Integritätsring, dann ist $(A[X])^* = A^*$. (Folgt aus der Gradformel.)

1.15 Beispiel und Definition (Hauptideal(-ring))

Sei A ein Ring.

i) Für jedes $x \in A$ ist $(x) := \{xy | y \in A\} \subseteq A$ ein Ideal. Es heißt *das von x erzeugte Hauptideal* (Abkürzung: HI).

ii) Ist A ein Integritätsring, so gilt für alle $x,y \in A$:

$$(x) = (y) \quad \Leftrightarrow \quad \exists_{u \in A^*} : x = uy$$

Insbesondere gilt:

$$(x) = 1 = A \quad \Leftrightarrow \quad x \in A^* \tag{1.1}$$

(Beachte: (1.1) gilt für jeden Ring A.)

iii) A heißt genau dann *Hauptidealring* (Abkürzung: HIR), wenn A ein Integritätsring ist, in dem jedes Ideal $I \subseteq A$ ein Hauptideal ist.

iv) A heißt genau dann *Körper*, wenn $A^* = A \setminus \{0\}$ und $A \neq \{0\}$ ist.

1.16 Beispiel

Die Ringe $\mathbb{Z}, \mathbb{Z}[\mathbf{i}]$ und $k[X]$ für einen Körper k, nicht aber $\mathbb{Z}[X]$ oder $k[X,Y]$ sind Hauptidealringe.
Die Ringe $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ und $\mathbb{F}_p := {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ für eine Primzahl p sind Körper, nicht aber $\mathbb{Z}$.

1.17 Proposition (Ideale eines Körpers)

Für einen Ring $A \neq \{0\}$ sind folgende Aussagen äquivalent:

i) A ist ein Körper.

ii) $(0), (1) \subseteq A$ sind die einzigen Ideale.

iii) Jeder Ringhomomorphismus $f : A \to B \neq \{0\}$ ist injektiv.

Beweis

„i) ⇒ ii)“: Sei $(0) \neq I \subseteq A$ ein Ideal. Also gibt es ein Element $0 \neq x \in I$. Da A ein Körper ist, ist $A^* = A \setminus \{0\} \ni x$. Also folgt $(1) = (x) \subseteq I$. Daher ist $A = I = (1)$.

„ii) ⇒ iii)“: Wegen $f(1) = 1 \neq 0$ in B ist $(1) \neq \ker(f) \subseteq A$. Da der Kern aber ein Ideal ist, bleibt für den Kern nur das einzige andere Ideal $\ker(f) = (0)$, was äquivalent zur Injektivität von f ist.

„iii) ⇒ i)“: Nach Voraussetzung gilt $A \neq \{0\}$, weswegen nach der Definition 1.15 iv) ist nur noch $A \setminus \{0\} \subseteq A^*$ zu zeigen ist. Sei $x \in A \setminus A^*$, dann ist $(x) \subsetneq A$. Wende iii) auf den Quotientenhomomorphismus

$$\pi : A \to B := {}^{A}\!/_{(x)} \neq (0)$$

an und erhalte, dass π injektiv ist. Daher gilt $(0) = \ker(\pi) = (x)$ und somit $x = 0$. $\square_{1.17}$

1.18 Proposition und Definition (Primideal, maximales Ideal)

Sei $I \subsetneq A$ ein Ideal.

i) Äquivalent sind:

   a) $\forall_{a,b \in A} : ab \in I \Rightarrow (a \in I \vee b \in I)$
   b) A/I ist ein Integritätsring.

   In diesem Fall heißt I *Primideal* (Abkürzung: PI).

ii) Äquivalent sind:

   a) Für alle Ideale $J \subseteq A$ mit $I \subsetneq J$ gilt $J = A$.
   b) A/I ist ein Körper.

   In diesem Fall heißt I *maximales Ideal*.

Beweis

i) „a) $\Rightarrow$ b)“: $A/I \neq \{0\}$, da $I \subsetneq A$ ein echtes Ideal ist. Sind $a,b \in A$ mit $\overline{a} \cdot \overline{b} = \overline{0}$ in A/I, so folgt $ab \in I$. Aus a) ergibt sich $(a \in I \vee b \in I)$ und im Quotientenring bedeutet dies $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$. Daher ist $\overline{0} \in A/I$ der einzige Nullteiler.

   „b) $\Rightarrow$ a)“: Folgt analog:
   Sind $a,b \in A$ mit $ab \in I$, so folgt $\overline{a} \cdot \overline{b} = \overline{0}$ in A/I. Da nach b) A/I ein Integritätsring ist, ist $\overline{0} \in A/I$ der einzige Nullteiler und somit $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$. Im Ring A bedeutet das $(a \in I \vee b \in I)$, womit a) gezeigt ist. $\square_{\text{i)}}$

ii) Da nach 1.17 i) $\Leftrightarrow$ ii) ein Körper genau die Ideale (0) und (1) hat und nach 1.7 die Ideale des Quotientenrings A/I den Idealen $J \subseteq A$ mit $I \subseteq J$ entsprechen, von denen es aufgrund der Maximalität von I nur die zwei Möglichkeiten $J = I$ und $J = A$ gibt, beziehungsweise andersherum nur diese zwei geben kann, wenn A/I ein Körper ist, ist die Äquivalenz gezeigt. $\square_{\text{ii)}}$

1.19 Beispiel

i) Jedes maximale Ideal ist ein Primideal, da jeder Körper ein Integritätsring ist.

ii) Das Nullideal $(0) \subseteq \mathbb{Z}$ ist ein Primideal, aber nicht maximal, da $\mathbb{Z}/(0) = \mathbb{Z}$ ein Integritätsring, aber kein Körper, ist.

iii) Die maximalen Ideal in $\mathbb{Z}$ sind genau die Hauptideale $(p) \subseteq \mathbb{Z}$ mit einer Primzahl p. Das einzige Primideal, welches nicht maximal ist, ist das Nullideal $(0) \subseteq \mathbb{Z}$.

1.20 Proposition (Urbild eines Primideals ist ein Primideal)

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

Beweis

Wegen $f^{-1}(\mathfrak{p}) = \ker\left(A \xrightarrow{f} B \xrightarrow{\pi} {}^{B}\!/_{\mathfrak{p}} \neq \{0\}\right) \subsetneq A$ ist $f^{-1}(\mathfrak{p})$ ein Ideal und

$$\{0\} \neq {}^{A}\!/_{f^{-1}(\mathfrak{p})} \hookrightarrow {}^{B}\!/_{\mathfrak{p}}$$

ein Unterring des Integritätsrings ${}^{B}\!/_{\mathfrak{p}}$, weshalb ${}^{A}\!/_{f^{-1}(\mathfrak{p})}$ ebenfalls ein Integritätsring ist. Dann ist nach der Definition 1.18 i) auch $f^{-1}(\mathfrak{p})$ ein Primideal. $\square_{1.20}$

1.21 Beispiel

Für den eindeutigen Ringhomomorphismus $f : \mathbb{Z} =: A \hookrightarrow B := \mathbb{Q}$ ist $\mathfrak{p} := (0) \subseteq B$ ein maximales Ideal, da B ein Körper ist, aber $f^{-1}(\mathfrak{p}) = (0) \subseteq A = \mathbb{Z}$ ist kein maximales Ideal.

1.22 Satz (Existenz eines maximalen Ideals)

In jedem Ring $A \neq \{0\}$ existiert mindestens ein maximales Ideal.

Beweis

Dies ist eine bekannte Anwendung des Lemmas von Zorn:

> „Jede halbgeordnete Menge, in der jede Kette (d.h. jede total geordnete Teilmenge) eine obere Schranke hat, enthält mindestens ein maximales Element."

Die Teilmengenrelation auf der Menge M der echten Ideale des Rings A erzeugt eine Halbordnung. Diese Menge ist nicht leer, da sie immer das triviale Ideal (0) enthält.
Außerdem ist für eine Kette K in M die Vereinigung $I := \bigcup_{k \in K} k$ aller Elemente eine obere Schranke für K, denn I ist nicht leer und ein Ideal von A.
Nach dem Lemma von Zorn gibt es also mindestens ein maximales Element von M, also ein maximales Ideal von A. $\square_{1.22}$

1.23 Korollar

Ist A ein Ring und $I \subsetneq A$ ein Ideal, so existiert ein maximales Ideal $\mathfrak{m} \subseteq A$ mit $I \subseteq \mathfrak{m}$.

Beweis

Sei $\mathfrak{n} \subseteq {}^{A}\!/_{I}$ ein maximales Ideal, das nach 1.22 existiert, und $\pi : A \to {}^{A}\!/_{I}$ der kanonische Ringhomomorphismus. Nach 1.7 ist $\mathfrak{m} := \pi^{-1}(\mathfrak{n}) \subseteq A$ ein maximales Ideal mit $I \subseteq \mathfrak{m}$. $\square_{1.23}$

1.24 Korollar

Sei A ein Ring. Für ein beliebiges Element $x \in A$ sind äquivalent:

i) $x \in A^*$

ii) x ist in keinem maximalen Ideal von A enthalten.

Beweis

„i) ⇒ ii)“: Dies ist klar, da $(x) = A$ ist und für jedes Ideal $I \subseteq A$ aus $x \in I$ schon $(x) \subseteq I$ folgt.

„ii) ⇒ i)“: Zeige äquivalent, dass wenn i) nicht gilt, auch ii) nicht gilt:

Sei $x \notin A^*$, so folgt aus 1.15 ii), dass $(x) \subsetneq A$ ein echtes Ideal ist und nach 1.23 gibt es ein maximales Ideal $\mathfrak{m} \subseteq A$ mit $x \in (x) \subseteq \mathfrak{m}$. $\square_{1.24}$

1.25 Ausblick

Seien X ein kompakter Hausdorffraum und $A = C(X,\mathbb{R})$ die $\mathbb{R}$-Algebra der stetigen $\mathbb{R}$-wertigen Funktionen auf X.

Für jedes $f \in A$ gilt:

$$\begin{aligned} f \in A^* &\Leftrightarrow \underset{x \in X}{\forall} : f(x) \neq 0 \\ f \in A^* &\Rightarrow \underset{x \in X}{\forall} : f^{-1}(x) = f(x)^{-1} \end{aligned} \tag{1.2}$$

Ein Vergleich mit 1.24 lässt einen Zusammenhang zwischen den Punkten $x \in X$ und den maximalen Idealen von A vermuten.

Für alle $x \in X$ ist die Auswertungsabbildung

$$\begin{aligned} \mathrm{ev}_x : A &\twoheadrightarrow \mathbb{R} \\ f &\mapsto \mathrm{ev}_x(f) := f(x) \end{aligned}$$

ein surjektiver $\mathbb{R}$-Algebrenhomomorphismus, dessen Kern

$$\mathfrak{m}_x := \ker(\mathrm{ev}_x) = \left\{ f \in C(X,\mathbb{R}) \,\middle|\, f(x) = 0 \right\} \subseteq A \tag{1.3}$$

ein maximales Ideal ist, da ${}^{A}\!/_{\mathfrak{m}_x} \overset{\sim}{=} \mathbb{R}$ ein Körper ist.

Genauer kann man auf der Menge

$$\mathrm{MaxSpec}(A) := \{\mathfrak{m} \subseteq A \text{ maximales Ideal}\}$$

eine Topologie nur mit Hilfe des kommutativen Ringes A definieren, so dass die Abbildung $X \to \mathrm{MaxSpec}(A), x \mapsto \mathfrak{m}_x$ ein Homöomorphismus, also insbesondere bijektiv ist. (vergleiche [Atiyah, Macdonald], chapter 1, exercise 26)

Insbesondere bestimmt der kommutative Ring A den topologischen Raum X.

Nicht jeder kommutative Ring ist von der Form $C(X,\mathbb{R})$. Aber eine Grundidee der topologischen Geometrie ist, dass jeder Ring A der Ring von „stetigen Funktionen“ auf einem „Raum“ sein soll, zum Beispiel:

Betrachte $\mathrm{MaxSpec}(A) := \left\{\mathfrak{m} \subseteq A \middle| \mathfrak{m} \text{ maximales Ideal}\right\}$. Jedes $a \in A$ bestimmt eine Abbildung

$$\begin{aligned} \mathrm{MaxSpec}(A) &\to \dot{\bigcup_{\mathfrak{m} \in \mathrm{MaxSpec}(A)}} \left({}^{A}\!/_{\mathfrak{m}} \right) =: M \\ \mathfrak{m}_0 &\mapsto \underbrace{(a \mod \mathfrak{m}_0)}_{\in {}^{A}\!/_{\mathfrak{m}_0} \subseteq M} =: a(\mathfrak{m}_0) \end{aligned}$$

und es gilt:

i) Für alle $\mathfrak{m} \in \operatorname{MaxSpec}(A)$ gilt nach Definition $\mathfrak{m} = \{a \in A \mid a(\mathfrak{m}) = 0\}$. (vergleiche (1.3))

ii) Für alle $a \in A$ gilt

$$a \in A^* \Leftrightarrow \left(\underset{\mathfrak{m} \in \operatorname{MaxSpec}(A)}{\forall} : a(\mathfrak{m}) \neq 0 \right)$$

da $a(\mathfrak{m}) \neq 0 \Leftrightarrow a \notin \mathfrak{m}$ ist und nach 1.24 eine Einheit in keinem maximalen Ideal enthalten ist. (vergleiche (1.2))

$\square_{1.25}$

Zum Beispiel für $A = \mathbb{Z}$ ist $A/\mathbb{Z} = \mathbb{F}_p$ für eine Primzahl p.

1.26 **Definition** (lokaler Ring, Restklassenkörper)

Ein *lokaler Ring* ist ein Ring A mit genau einem maximalem Ideal $\mathfrak{m}$.
(Jeder Körper ist ein lokaler Ring mit $\mathfrak{m} = (0)$.)
Der Körper $A/\mathfrak{m}$ heißt der *Restklassenkörper* (*von* A).
Schreibe (A,$\mathfrak{m}$) für einen lokalen Ring mit maximalem Ideal $\mathfrak{m}$, und definiere $\kappa(\mathfrak{m}) := A/\mathfrak{m}$.

1.27 **Proposition** (Kriterium für lokalen Ring)

Seien A ein Ring und $\mathfrak{m} \subsetneq A$ ein Ideal.

i) $A \setminus \mathfrak{m} \subseteq A^*$ gilt genau dann, wenn (A,$\mathfrak{m}$) ein lokaler Ring ist.
In diesem Fall ist $A \setminus \mathfrak{m} = A^*$.

ii) Ist $\mathfrak{m}$ maximal und gilt $1 + \mathfrak{m} := \{1 + x \mid x \in \mathfrak{m}\} \subseteq A^*$, so ist ($A$,$\mathfrak{m}$) ein lokaler Ring.

Beweis

i) Da $\mathfrak{m}$ ein echtes Ideal ist, gilt für alle $u \in A^*$ schon $u \in A \setminus \mathfrak{m}$, denn sonst wäre mit $u \in \mathfrak{m}$ auch:

$$u^{-1} \cdot u = 1 \in \mathfrak{m}$$

Das hieße $\mathfrak{m} = (1)$ im Widerspruch zu $\mathfrak{m} \subsetneq A$. Daher gilt $A^* \subseteq A \setminus \mathfrak{m}$.

„⇒“: Ist $I \subseteq A$ ein Ideal mit $\mathfrak{m} \subseteq I$, so existiert ein $u \in I \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{m} \subseteq A^*$, weswegen $I = (1)$ ist. Also ist $\mathfrak{m} \subseteq A$ ein maximales Ideal.

Sei $\mathfrak{n} \subseteq A$ ein (weiteres) maximales Ideal. Zeige $\mathfrak{n} \subseteq \mathfrak{m}$, denn dann folgt, weil beides maximale Ideale sind, schon $\mathfrak{m} = \mathfrak{n}$, das heißt $\mathfrak{m} \subseteq A$ ist das einzige maximale Ideal.

Angenommen es gilt $\mathfrak{n} \subsetneq \mathfrak{m}$, dann existiert ein $x \in \mathfrak{n} \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{m} \subseteq A^*$. Deswegen ist $\mathfrak{n} = (1)$ im Widerspruch zur Maximalität von $\mathfrak{n}$.

„⇐“: Ist (A,$\mathfrak{m}$) ein lokaler Ring, und sei $u \in A \setminus \mathfrak{m}$. Dann ist $(u) \subseteq A$ mit $(u) \nsubseteq \mathfrak{m}$.

Wäre $(u) \neq (1)$, so gäbe es nach 1.23 ein maximales Ideal $\mathfrak{n} \subseteq A$ mit $(u) \subseteq \mathfrak{n}$. Da $\mathfrak{m}$ das einzige maximale Ideal ist, folgt $\mathfrak{m} = \mathfrak{n}$ und somit der Widerspruch $(u) \subseteq \mathfrak{m}$. Also ist $(u) = (1)$ und somit gibt es ein $a \in A$ mit $au = 1$, das heißt $u \in A^*$. $\square_{\text{i)}}$

ii) Wegen i) ist nur $A \setminus \mathfrak{m} \subseteq A^*$ zu zeigen.

Sei $x \in A \setminus \mathfrak{m}$, so ist $\mathfrak{m} \subsetneq \mathfrak{m} + (x) = \{y + ax | y \in \mathfrak{m}, a \in A\}$ ein Ideal, aber $\mathfrak{m}$ ist ein maximales Ideal, weswegen $\mathfrak{m} + (x) = (1)$ gelten muss. Daher gibt es ein $y \in \mathfrak{m}$ und ein $a \in A$ mit $1 = y + ax$ und somit $ax = 1 + (-y) \in 1 + \mathfrak{m} \subseteq A^*$. Deswegen existiert ein $b \in A$ mit $1 = b(ax) = (ba)x$ und daher ist x invertierbar und somit $x \in A^*$. $\square_{\text{ii)}}$

1.28 Beispiel

Sei $p \in \mathbb{Z}$ eine Primzahl, insbesondere $(p) \neq 0$. Dann ist $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \middle| a \in \mathbb{Z}, p \nmid b \in \mathbb{Z} \right\} \subsetneq \mathbb{Q}$ ein Unterring von $\mathbb{Q}$ und $\left(\mathbb{Z}_{(p)}, (p)\right)$ ist ein lokaler Ring mit $\kappa(\mathfrak{p}) \cong \mathbb{F}_p$.

Beweis

Nach Beispiel 2.6 aus Algebra ist die Lokalisierung $\mathbb{Z}_{(p)} = (\mathbb{Z} \setminus (p))^{-1}\mathbb{Z}$ von $\mathbb{Z}$ bei (p) ein Unterring von $\mathbb{Z}_{(0)} = \mathbb{Q}$ mit der Einheitengruppe $\mathbb{Z}_{(p)}^* = \mathbb{Z}_{(p)} \setminus (p)$.

Nach 1.27 i) ist also $\left(\mathbb{Z}_{(p)}, (p)\right)$ ein lokaler Ring. $\square_{1.28}$

1.29 Proposition und Definition (Nilradikal)

Sei A ein Ring. Dann ist $\mathfrak{N}(A) := \{x \in A | x \text{ nilpotent}\} \subseteq A$ ein Ideal und es gilt:

$$\mathfrak{N}\left(A/\mathfrak{N}(A)\right) = (\overline{0})$$

Das Ideal $\mathfrak{N}(A) \subseteq A$ heißt *das Nilradikal von A*.

Beweis

Überprüfe 1.5 i) a) und b):

$$x,y \in \mathfrak{N}(A) \quad \Rightarrow \quad \underset{N \in \mathbb{N}_{\geq 1}}{\exists} : x^N = y^N = 0 \quad \Rightarrow \quad (x-y)^{2N} = \sum_{i=0}^{2N} \binom{2N}{i} x^i \cdot (-1)^{2N-i} \cdot y^{2N-i}$$

Da für alle $0 \leq i \leq 2N$ gilt $(i \geq N \vee 2N - i \geq N)$ ist in jedem Produkt $x^i \cdot y^{2N-i}$ mindestens einer der Faktoren Null und es folgt $(x-y)^{2N} = (0)$, also $x - y \in \mathfrak{N}(A)$. $\square_{\text{a)}}$

Zu b): Seien $x \in \mathfrak{N}(A)$ und $a \in A$. Dann gibt es ein $N \in \mathbb{N}_{\geq 1}$ mit $x^N = 0$ und somit gilt:

$$(ax)^N = a^N x^N = a^N \cdot 0 = 0$$

Daher ist $ax \in \mathfrak{N}(A)$. $\square_{\text{b)}}$

Sei nun $x \in A$ mit $\overline{x} := (x \mod \mathfrak{N}(A)) \in \mathfrak{N}\left(A/\mathfrak{N}(A)\right)$. Daher gibt es ein $N \in \mathbb{N}_{\geq 1}$ mit $0 = (\overline{x})^N = \overline{(x^N)}$ in $A/\mathfrak{N}(A)$, weswegen $x^N \in \mathfrak{N}(A)$ ist. Also gibt es ein $M \in \mathbb{N}_{\geq 1}$ mit $0 = \left(X^N\right)^M = x^{N \cdot M}$ in A, weshalb $x \in \mathfrak{N}(A)$ ist, also $\overline{x} = 0$ ist. $\square_{1.29}$

1.30 **Satz** (Nilradikal ist Schnitt aller Primideale)

Sei A ein Ring. Dann gilt:

$$\mathfrak{N}(A) = \bigcap_{\mathfrak{p} \subseteq A \text{ Primideal}} \mathfrak{p}$$

(Es folgt nochmal, dass $\mathfrak{N}(A) \subseteq A$ ein Ideal ist.)

Beweis

„$\subseteq$“: Seien $x \in \mathfrak{N}(A)$ und $\mathfrak{p} \subseteq A$ ein Primideal. Dann existiert ein $n \in \mathbb{N}_{\geq 1}$ mit $x^n = 0 \in \mathfrak{p}$.
Aus der Definition eines Primideals 1.18 i) a) folgt $x \in \mathfrak{p}$, da dies der einzige Faktor im Produkt x^n ist.
„$\supseteq$“: Sei $x \in A \setminus \mathfrak{N}(A)$. Zeige, dass ein Primideal $\mathfrak{p} \subseteq A$ mit $x \notin \mathfrak{p}$ existiert.

- 1. Beweis (direkt): Betrachte $\Sigma := \left\{\mathfrak{u} \middle| \mathfrak{u} \subseteq A \text{ Ideal mit } \left(\forall_{n \in \mathbb{N}_{\geq 1}} : x^n \notin \mathfrak{u}\right)\right\}$.
  Wegen $x \notin \mathfrak{N}(A)$ gilt $(0) \in \Sigma$, also $\Sigma \neq \emptyset$.
  Es ist klar, dass $(\Sigma, \subseteq)$ eine teilweise geordnete Menge ist.
  Ist $\Sigma' \subseteq \Sigma$ total geordnet, so gilt:

  $$\mathfrak{u}' := \bigcup_{\mathfrak{u} \in \Sigma'} \mathfrak{u} \in \Sigma$$

  Denn aus der totalen Ordnung von Σ' folgt, dass $\mathfrak{u}' \subseteq A$ ein Ideal ist und $x^n \notin \mathfrak{u}'$ für alle $n \in \mathbb{N}_{\geq 1}$ ist dann klar, denn sonst müsste es schon in einem $\mathfrak{u}$ sein.
  Aus dem Lemma von Zorn folgt daraus die Existenz eines maximalen Elementes $\mathfrak{p} \in \Sigma$.
  Wegen $x \notin \mathfrak{p}$ zeige noch, dass $\mathfrak{p}$ ein Primideal ist.
  Angenommen dies ist nicht der Fall, dann existieren a,$b \in A$ mit a,$b \notin \mathfrak{p}$ und $ab \in \mathfrak{p}$.
  Wegen $\mathfrak{p} \subsetneq \mathfrak{p}+(a)$,$\mathfrak{p}+(b)$ und der Maximalität von $\mathfrak{p}$ existieren n,$m \in \mathbb{N}_{\geq 1}$ mit $x^n \in \mathfrak{p}+(a)$ und $x^m \in \mathfrak{p} + (b)$. Dann folgt:

  $$x^{n+m} = x^n \cdot x^m \in \mathfrak{p} + (ab) \overset{ab \in \mathfrak{p}}{=} \mathfrak{p}$$

  Dies ist ein Widerspruch zu $\mathfrak{p} \in \Sigma$, also $x^{n+m} \notin \mathfrak{p}$. $\square_{\text{1. Beweis}}$
- 2. Beweis (mit Lokalisierung): $S := \left\{x^n \middle| n \geq 0\right\} \subseteq A$ ist multiplikativ abgeschlossen und wegen $x \notin \mathfrak{N}(A)$ gilt $0 \notin S$. Es folgt $S^{-1}A \neq \{0\}$.
  Nach 1.22 existiert ein maximales Ideal $\mathfrak{m} \subseteq S^{-1}A$ und nach 1.19 i) und 1.20 ist

  $$\mathfrak{p} := \left(\varphi : A \xrightarrow{\text{kanonisch}} S^{-1}A\right)^{-1}(\mathfrak{m}) \subseteq A$$

  ein Primideal. Wegen $\varphi(x) \in \left(S^{-1}A\right)^*$ folgt $\varphi(x) \notin \mathfrak{m}$ nach 1.24 und somit gilt also $x \notin \varphi^{-1}(\mathfrak{m}) = \mathfrak{p}$. $\square_{\text{2. Beweis}}$

1.31 **Korollar und Definition** (Radikal)

Seien A ein Ring und $I \subseteq A$ ein Ideal. Dann heißt $\sqrt{I} := \left\{x \in A \middle| \exists_{n \in \mathbb{N}_{\geq 1}} : x^n \in I\right\}$ *das Radikal von* I. Es gilt:

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \subseteq A \text{ PI} \\ \text{mit } I \subseteq \mathfrak{p}}} \mathfrak{p}$$

Beispiel: $\sqrt{(0)} = \mathfrak{N}(A)$

Beweis

Für den kanonischen Ringhomomorphismus $\pi : A \to {}^{A}/_{I}$ gilt $\sqrt{I} = \pi^{-1}\left(\pi\left(\sqrt{I}\right)\right)$, da π surjektiv ist. Zudem ist offenbar $\pi\left(\sqrt{I}\right) = \mathfrak{N}\left({}^{A}/_{I}\right)$. Nach der Definition von $\sqrt{I}$ folgt:

$$\sqrt{I} = \pi^{-1}\left(\pi\left(\sqrt{I}\right)\right) = \pi^{-1}\left(\mathfrak{N}\left({}^{A}/_{I}\right)\right) =$$
$$\overset{1.30}{=} \pi^{-1}\left(\bigcap_{\overline{\mathfrak{p}} \subseteq {}^{A}/_{I} \text{ PI}} \overline{\mathfrak{p}}\right) = \bigcap_{\overline{\mathfrak{p}} \subseteq {}^{A}/_{I} \text{ PI}} \pi^{-1}(\overline{\mathfrak{p}}) =$$
$$\overset{1.20}{\underset{1.7}{=}} \bigcap_{\substack{\mathfrak{p} \subseteq A \text{ PI} \\ I \subseteq \mathfrak{p}}} \mathfrak{p}$$

$\square_{1.31}$

1.32 **Proposition und Definition** (Summe, Schnitt und Produkt von Idealen)

Seien A ein Ring, K eine Menge und $\forall_{k \in K}$ sei $I_k \subseteq A$ ein Ideal.

i) Das kleinste Ideal, welches alle I_k enthält, ist:

$$\sum_{k \in K} I_k := \left\{ \sum_{k \in K'} x_k \,\middle|\, K' \subseteq K \text{ endlich}, x_k \in I_k \right\} \subseteq A$$

Es heißt *die Summe der* I_k über alle $k \in K$.

ii) $\bigcap_{k \in K} I_k \subseteq A$ ist das größte Ideal, dass in allen I_k enthalten ist.

iii) Sind I und J Ideale, so auch

$$IJ := \left\{ \sum_{i=0}^{n} x_i y_i \,\middle|\, n \in \mathbb{N}, x_i \in I, y_i \in J \right\} \subseteq A$$

das Produkt von X *und* Y.

Beweis

i) Ist $x \in I_k$, so ist nach Definition auch $x \in \sum_{k \in K} I_k$ und somit ist für alle $k \in K$ schon $I_k \subseteq \sum_{k \in K} I_k$.

Andererseits müssen mit alle I_k auch beliebige endliche Summen von Elementen aus den I_k in jedem Ideal liegen, dass die I_k enthält. Daher ist die Summe das kleinste solche Ideal. $\square_{\text{i)}}$

ii) Der Schnitt ist definitionsgemäß in allen I_k enthalten.
Sei J ein Ideal, dass in allen I_k enthalten ist. Dann gilt für jedes $x \in J$ schon $x \in I_k$ für alle $k \in K$ und somit $x \in \bigcap_{k \in K} I_k$. Also ist der Schnitt das größte solche Ideal. $\square_{\text{ii)}}$

iii) Nach Definition ist IJ eine Gruppe bezüglich der Addition. Für $a \in A$ und $x \in IJ$ gilt für ein $n \in \mathbb{N}$ und $1 \leq i \leq n$ mit $x_i \in I$ und $y_i \in J$:

$$x = \sum_{i=0}^{n} x_i y_i$$
$$ax = a\left(\sum_{i=0}^{n} x_i y_i\right) = \sum_{i=0}^{n} \underbrace{(ax_i)}_{\in I} y_i \in IJ$$

Also ist IJ ein Ideal. $\square_{\text{iii)}}$

1.33 Beispiel

i) Sind I und J Ideale, so gilt $IJ \subseteq I \cap J$. Denn ist $a \in IJ$, so gibt es ein $n \in \mathbb{N}$ und für $0 \leq i \leq n$ auch $x_i \in I$ und $y_i \in J$ mit:

$$a = \sum_{i=0}^{n} x_i y_i$$

Da I ein Ideal ist und $x_i \in I$ und $y_i \in A$ ist, folgt $x_i y_i \in I$ und somit auch die Summe aller dieser Faktoren, also $a \in I$. Analog folgt $a \in J$ und somit $a \in I \cap J$.

ii) Für $A = \mathbb{Z}$, $I = (a)$ und $J = (b)$ gilt:

$$(a) + (b) = (\text{ggT}\,(a,b))$$
$$(a) \cap (b) = (\text{kgV}\,(a,b))$$
$$(a)\,(b) = (ab)$$

Insbesondere folgt:

$$(a)\,(b) = (a) \cap (b) \quad \Leftrightarrow \quad \text{kgV}\,(a,b) = \pm ab \quad \Leftrightarrow \quad \text{ggT}\,(a,b) = 1$$

iii) Seien k ein Körper, $n \in \mathbb{N}_{\geq 1}$ und

$$A = k\,[X_1, \ldots, X_n] = \left\{ f = \sum_{i_1,\ldots,i_n \geq 0} a_{(i_1,\ldots,i_n)} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \,\middle|\, a_{(i_1,\ldots,i_n)} \in k \text{ fast alle Null} \right\}$$

der Polynomring über k in den Variablen $X_1, \ldots, X_n$. Dann ist

$$\mathfrak{m} := (X_1, \ldots, X_n) = \left\{ f \in A \,\middle|\, a_{(0,\ldots,0)} = 0 \right\} = \left\{ f \in A \,\middle|\, f\,(0,\ldots,0) = 0 \right\} \subseteq A$$

ein maximales Ideal mit ${}^{A}\!/_{\mathfrak{m}} \overset{\sim}{=} k$ vermöge $\overline{f} \mapsto f\,(0,\ldots,0) \in k$. Für alle $n \in \mathbb{N}_{\geq 1}$ gilt:

$$\mathfrak{m}^n = \left\{ f \in A \,\middle|\, \forall_{(i_1,\ldots,i_n) \in \mathbb{N}^n} : \left(\sum_{j=1}^{n} ij < n \Rightarrow a_{(i_1,\ldots,i_n)} = 0 \right) \right\}$$

Für $n = 2$ gilt zum Beispiel:

$$k[X,Y] \supseteq (X,Y)^n = \left\{ \sum_{\substack{i,j\geq 0 \\ i+j\geq n}} a_{i,j} X^i Y^j \,\middle|\, a_{ij} \in k \text{ fast alle Null} \right\} =$$
$$= \left(X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n\right)$$

$\square_{1.33}$

1.34 **Bemerkung und Definition** (komaximal)

Zwei Ideale I und J heißen genau dann *komaximal*, wenn $I + J = (1)$ ist. Nach 1.31 i) ist dies äquivalent dazu, dass es ein $a \in I$ und ein $b \in J$ mit $a + b = 1$ gibt.
In diesem Fall gilt $IJ = I \cap J$.

Beweis

Wegen 1.32 i) ist nur noch $I \cap J \subseteq IJ$ zu zeigen.
Wähle $a \in I$ und $b \in J$ mit $a + b = 1$ und sei $x \in I \cap J$ beliebig. Dann folgt:

$$x = x \cdot 1 = \underbrace{xa}_{\in JI = IJ} + \underbrace{xb}_{\in IJ} \in IJ$$

$\square_{1.34}$

1.35 **Satz** (Chinesischer Restsatz)

Seien A ein Ring, $n \in \mathbb{N}_{\geq 1}$ und $I_1, \ldots, I_n \subseteq A$ Ideale. Dann ist die Abbildung

$$\varphi : A \to \prod_{i=1}^{n} \left({}^{A}/_{I_i} \right)$$
$$a \mapsto \varphi(a) := (a \mod I_i)_{i_1,\ldots,i_n}$$

ein Ringhomomorphismus und es gilt:

a) φ ist surjektiv $\overset{\text{ii)}}{\Leftrightarrow} \left(\underset{1\leq i,j\leq n, i\neq j}{\forall} I_i + I_j = (1) \right) \overset{\text{i)}}{\Rightarrow} \bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$

b) $\ker(\varphi) = \bigcap_{i=1}^{n} I_i$

Beweis

Dass φ ein Ringhomomorphismus ist, kann man leicht nachrechnen.

a) i) $n = 1$ ist klar. $n = 2$ wurde in 1.33 gezeigt.
Für $n > 2$ führe eine Induktion über n durch:
Induktionsvoraussetzung:

$$J := \bigcap_{i=1}^{n-1} I_i = \prod_{i=1}^{n-1} I_i$$

Für alle $1 \leq i \leq n-1$ gibt es wegen $I_i + I_n = (1)$ ein $x_i \in I_i$ und ein $y_i \in I_n$ mit:

$$1 = x_i + y_i \tag{1.4}$$

Es folgt:

$$J = \prod_{i=1}^{n-1} I_i \ni \prod_{i=1}^{n-1} x_i \overset{(1.4)}{=} \prod_{i=1}^{n-1} (1 - y_i) \overset{y_i \in I_n}{\equiv} 1 \mod I_n$$

Also gibt es ein $y \in I_n$ mit:

$$1 = \underbrace{\left(\prod_{i=1}^{n-1} x_i \right)}_{\in J} + y$$

$$\Rightarrow \quad J + I_n = (1) \tag{1.5}$$

Es folgt:

$$\prod_{i=1}^{n} I_i = J \cdot I_n \overset{1.5}{\underset{n=2}{=}} J \cap I_n \overset{\text{Induktions-}}{\underset{\text{voraussetzung}}{=}} \bigcap_{i=1}^{n-1} I_i \cap I_n = \bigcap_{i=1}^{n} I_i$$

$\square_{\text{a) i)}}$

ii) „$\Leftarrow$“: Da $\operatorname{im}(\varphi) \subseteq \prod_{i=1}^{n} \left(A/I_i \right)$ ein A-Untermodul ist, genügt es zu zeigen:

$$\underset{1 \leq i \leq n}{\forall} : e_i := (0, \ldots, 0, \underbrace{1}_{i\text{-te Stelle}}, 0, \ldots, 0) \in \operatorname{im}(\varphi)$$

Sei $i = 1$ (sonst analog), so ist zu zeigen, dass es ein $x \in A$ gibt, für das gilt:

$$x \equiv 1 \mod I_1$$
$$x \in \bigcap_{i=2}^{n} I_i$$

Nach Voraussetzung existieren für alle $2 \leq i \leq n$ schon $x_i \in I_1$ und $y_i \in I_i$ mit:

$$1 = x_i + y_i$$
$$\Rightarrow \quad x := \prod_{i=2}^{n} y_i \in \prod_{i=2}^{n} I_i \subseteq \bigcap_{i=2}^{n} I_i$$
$$x = \prod_{i=2}^{n} (1 - x_i) \overset{x_i \in I_1}{\equiv} 1 \mod I_1$$

„⇒“: Seine $1 \leq i,j \leq n$ mit $i \neq j$ gegeben. Da φ surjektiv ist, existiert ein $x \in A$ mit:

$$\varphi(x) = e_i$$

Nach der Definition von φ folgt für alle $1 \leq j \leq n$ mit $j \neq i$:

$$x \equiv 1 \mod I_i \qquad\qquad x \equiv 0 \mod I_j$$

Es folgt $1 = x + y$ mit einem geeigneten $y \in I_i$. Also gilt $I_i + I_j = (1)$. $\square_{\text{a) ii)}}$

b) Dies ist klar, da $\varphi(x) = 0$ bedeutet, dass $x \mod I_i = 0$ für allen $1 \leq i \leq n$ gilt, also x in alle I_i liegt, und somit im Schnitt liegt. $\square_{\text{b)}}$

1.36 **Definition und Bemerkung** (Bild und Urbild eines Ideals)

Sei $f : A \to B$ ein Ringhomomorphismus.

i) Ist $I \subseteq A$ ein Ideal, so ist

$$f_*(I) := \left\{ \sum_{i=1}^{n} b_i \cdot f(x_i) \,\middle|\, n \in \mathbb{N}, b_i \in B, x_i \in I \right\} \subseteq B$$

das kleinste Ideal von B, welches $f(I)$umfasst. Es heißt *das Bild von I unter f*.

ii) Ist $J \subseteq B$ ein Ideal, so ist $f^*(J) := f^{-1}(J) \subseteq A$ ein Ideal, *das Urbild von J unter f*.

iii) Ist $\mathfrak{p} \subseteq B$ ein Primideal, so auch $f^*(\mathfrak{p}) \subseteq A$, wie in 1.20 gezeigt wurde.

iv) Es ist $\mathfrak{p} := (5) \subseteq A := \mathbb{Z}$ ein Primideal, aber für den eindeutigen Ringhomomorphismus $f : \mathbb{Z} \to \mathbb{Q}$ ist $f_*(\mathfrak{p}) = (1) \subseteq \mathbb{Q}$ kein Primideal.

v) Für den eindeutigen Ringhomomorphismus $f : \mathbb{Z} \to \mathbb{Z}[\mathbf{i}]$ und eine Primzahl $p \in \mathbb{Z}$ gelten:

$$f_*((p)) = \begin{cases} \mathfrak{p}^2 & \text{mit } \mathfrak{p} = (1+\mathbf{i}) \subseteq \mathbb{Z}[\mathbf{i}] \text{ für } p = 2 \\ \mathfrak{p}_1 \cdot \mathfrak{p}_2 & \text{für Primideale } \mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_1 \neq \mathfrak{p}_2 \text{ für } p \equiv 1 \mod 4 \\ (p) & p \equiv 3 \mod 4 \end{cases}$$

Durch Betrachten der Norm ist dies äquivalent zu:

$$p \neq 2 \text{ Primzahl } \Rightarrow \left(\underset{x,y \in \mathbb{Z}}{\exists} p = x^2 + y^2 \Leftrightarrow p \equiv 1 \mod 4 \right)$$

(Der Beweis erfolgt später in der algebraischen Zahlentheorie.)

freiwillige Übung: Was aus Kapitel 1 gilt allgemein für nicht notwendig kommutative Ringe?

2 Moduln

2.1 Definition ((Unter-)Modul)

Sei A ein Ring.

i) Ein *A-Modul* ist eine abelsche Gruppe M zusammen mit einer Abbildung

$$\begin{aligned} A \times M &\to M \\ (a,m) &\mapsto am \end{aligned}$$

die *Skalarmultiplikation* heißt, und für die für alle $a,b \in A$ und $x,y \in M$ gilt:

a) $a(x+y) = ax + ay$
b) $(a+b)x = ax + bx$
c) $(ab)x = a(bx)$
d) $1 \cdot x = x$

(Äquivalent dazu ist, dass die Abbildung $A \to \mathrm{End}_{\mathbb{Z}}(M), a \mapsto (m \mapsto am)$ ein Ringhomomorphismus ist.)

ii) Sei M ein A-Modul. Ein *(A-)Untermodul (von M)* (Abkürzung: UM) ist eine abelsche Untergruppe $N \subseteq M$ mit $ax \in N$ für alle $a \in A$ und alle $x \in N$.

2.2 Bemerkung und Beispiel

Sei A ein Ring.

i) Die Ringmultiplikation $A \times A \to A$ definiert auf $(A, +, 0)$ die Struktur eines A-Moduls, und die A-Untermoduln sind genau die Ideale von A.

ii) Ist $A = k$ ein Körper, so ist ein A-Modul dasselbe wie ein k-Vektorraum.

iii) Jede abelsche Gruppe M besitzt genau eine $\mathbb{Z}$-Modulstruktur, nämlich:

$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (n,x) &\mapsto \begin{cases} \sum_{k=1}^{n} x & n \geq 0 \\ -\sum_{k=1}^{-n} x & n < 0 \end{cases} \end{aligned}$$

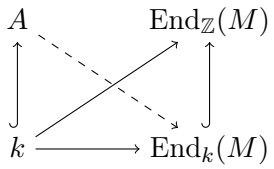
iv) Seien k ein Körper, $A = k[X_1, \ldots, X_n]$ für $n \in \mathbb{N}_{\geq 1}$ und M eine abelsche Gruppe.

Die Angabe eines Ringhomomorphismus $\varphi : A \to \mathrm{End}_{\mathbb{Z}}(M)$ ist äquivalent zur Angabe

a) von einem Ringhomomorphismus $k \to \mathrm{End}_{\mathbb{Z}}(M)$, also ein k-Vektorraumstruktur auf M und

b) von $\varphi_1 = \varphi(X_1), \ldots, \varphi_n = \varphi(X_n) \in \mathrm{End}_k(M)$ mit $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ für alle $1 \leq i,j \leq n$.

Beachte die universelle Eigenschaft der k-Algebra A:



Die Abbildung $A \to \mathrm{End}_k(M)$ ist dabei durch die φ_i bestimmt.

2.3 Definition und Bemerkung (lineare Abbildung)

Seien A ein Ring und M und N zwei A-Moduln.

i) Eine *(A-)lineare Abbildung (von M nach N)* ist ein Homomorphismus abelscher Gruppen $f : M \to N$ mit $f(ax) = af(x)$ für alle $a \in A$ und alle $x \in M$.

ii) Die Menge $\mathrm{Hom}_A(M,N) := \{f : M \to N \mid g \text{ ist } A\text{-linear}\}$ ist ein A-Modul vermöge

$$(f+g)(x) := f(x) + g(x)$$
$$(af)(x) := a(f(x))$$

für alle $f,g \in \mathrm{Hom}_A(M,N)$, alle $x \in A$ und alle $a \in A$.

iii) Sind $\alpha : M' \to M$ und $\beta : N \to N'$ A-linear, so auch

$$\alpha^* : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M',N)$$
$$f \mapsto \alpha^*(f) := f \circ \alpha$$

und:

$$\beta_* : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N')$$
$$f \mapsto \beta^*(f) := \beta \circ f$$

iv) Die Abbildung

$$\varepsilon_M : \mathrm{Hom}_A(A,M) \xrightarrow{\sim} M$$
$$f \mapsto f(1)$$

ist ein A-Modul-Isomorphismus, der *natürlich* in M ist, das heißt, ist $f : M \to N$ A-linear, so ist folgendes Diagramm kommutativ:

$$\begin{array}{ccc} \mathrm{Hom}_A(A,M) & \xrightarrow[\varepsilon_M]{\sim} & M \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f} \\ \mathrm{Hom}_A(A,N) & \xrightarrow[\varepsilon_N]{\sim} & N \end{array}$$

v) Sind wie in 2.2 iv) M_1 und M_2 zwei $A = k[X_1, \ldots, X_n]$-Moduln, bestimmt durch Abbildungen $\varphi_i^{(j)} \in \mathrm{End}_k(M_j)$ für alle $1 \leq i \leq n$, $1 \leq j \leq 2$, so sind die A-linearen Abbildungen $f : M_1 \to M_2$ genau die k-linearen Abbildungen mit $f \circ \varphi_i^{(1)} = \varphi_i^{(2)} \circ f$ für alle $1 \leq i \leq n$.

Beweis

iv): Man sieht leicht, dass ε_M eine A-lineare Abbildung und $\varepsilon_M^{-1}(x)(a) = ax$ ist.
Also ist ε_M ein A-linearer Isomorphismus.
Sei $\varphi \in \mathrm{Hom}_A(A,M)$, so rechne einerseits

$$f(\varepsilon_M(\varphi)) = f(\varphi(1))$$

und andererseits:

$$\varepsilon_N(f_*(\varphi)) = \varepsilon_N(f \circ \varphi) = (f \circ \varphi)(1) = f(\varphi(1))$$

$\square_{\text{iv)}}$

2.4 **Bemerkung und Definition** (Quotientenmodul)

Seien A ein Ring, M ein A-Modul und $N \subseteq M$ ein A-Untermodul.

i) Auf der abelschen Gruppe M/N existiert genau eine A-Modulstruktur so, dass die kanonische Abbildung $\pi : M \to M/N$ A-linear ist, nämlich $a[x] = [ax]$ für alle $a \in A$ und alle $x \in M$.
Der A-Modul M/N heißt *der Quotientenmodul (von M nach N).*

ii) Die Abbildung von Mengen

$$\begin{array}{ccc} \{U \,|\, N \subseteq U \subseteq M \text{ ist } A\text{-Untermodul}\} & \tilde{\to} & \left\{\overline{U} \,|\, \overline{U} \subseteq M/N \text{ ist } A\text{-Untermodul}\right\} \\ U & \mapsto & \pi(U) \end{array}$$

ist bijektiv und inklusionserhaltend. (vergleiche 1.7 für den Spezialfall $M = A$)

iii) Ist L ein weiterer A-Modul, so ist

$$\begin{array}{ccc} \mathrm{Hom}_A\left(M/N, L\right) & \xrightarrow{\sim} & \{f \in \mathrm{Hom}_A(M,L) \,|\, f(N) = 0\} \\ & {\scriptstyle \pi^*} \searrow & \downarrow \\ & & \mathrm{Hom}_A(M,L) \end{array}$$

ein A-linearer Isomorphismus. (vergleiche 1.5 iii))

2.5 Beispiel und Definition (Kokern)

Sei $f : M \to N$ A-linear, so gilt:

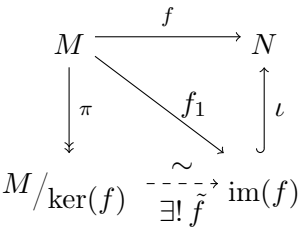
i) $\ker(f) := \{x \in M \mid f(x) = 0\} \subseteq M$ ein A-Untermodul.

ii) Es heißt $\operatorname{koker}(f) := {}^{N}\!/_{\operatorname{im}(f)}$ *der Kokern von* f.

$$\ker(f) \hookrightarrow M \xrightarrow{f} N \twoheadrightarrow \operatorname{koker}(f)$$

2.6 Proposition (Homomorphiesatz)

Sei A ein Ring. Dann faktorisiert jede A-lineare Abbildung $f : M \to N$ wie folgt:



Das heißt es existiert genau eine Abbildung $\tilde{f} : {}^{M}\!/_{\ker(f)} \to \operatorname{im}(f)$ mit $f = \iota \circ \tilde{f} \circ \pi$.
Dieses $\tilde{f}$ ist ein A-linearer Isomorphismus

Beweis

Zunächst faktorisiert f als $f : M \overset{f_1}{\twoheadrightarrow} \operatorname{im}(f) \overset{\iota}{\hookrightarrow} N$, f_1 und ι sind A-linear, es gilt $\ker(f) = \ker(f_1)$ und f_1 ist surjektiv.
Nach 2.4 iii) faktorisiert dann f_1 eindeutig mit einer A-lineare Abbildung $\tilde{f}$

$$f_1 : M \xrightarrow{\pi} {}^{M}\!/_{\ker(f_1)} \xhookrightarrow{\tilde{f}} \operatorname{im}(f)$$

und $\tilde{f}$ ist injektiv und surjektiv, also ein A-linearer Isomorphismus. $\square_{2.6}$

2.7 Definition (Summe, Schnitt, endlich erzeugt)

Seien A ein Ring, M ein A-Modul, I eine Menge und für alle I sei $M_i \subseteq M$ ein A-Untermodul.

i) Der kleinste Untermodul von M, der alle M_i enthält ist:

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in J} x_i \,\middle|\, J \subseteq I \text{ ist endlich, } x_i \in M_i \right\} \subseteq M$$

Er heißt die *Summe der* M_i *(in* M*).*

ii) Der *Schnitt* $\bigcap_{i \in I} M_i \subseteq M$ ist der größte Untermodul von M, der in allen M_i enthalten ist.

iii) Ist für alle $i \in I$ nun $x_i \in M$ ein Element, so ist $Ax_i := \{ax_i | a \in A\} \subseteq M$ der kleinste A-Untermodul, der x_i enthält.

Nach i) ist also $\sum_{i \in I} Ax_i \subseteq M$ der kleinste A-Untermodul von M, der alle x_i enthält.

iv) M heißt genau dann *endlich erzeugt*, wenn es ein $n \in \mathbb{N}_{\geq 1}$ und $x_1, \ldots, x_n \in M$ gibt, mit:

$$M = \sum_{i=1}^{n} Ax_i$$

Beispiel: Für einen Körper k ist der k-Modul $k[X]$ nicht endlich erzeugt.

2.8 **Proposition** (Isomorphiesätze)

Sei A ein Ring.

i) Sind L ein A-Modul und $M \subseteq N \subseteq L$ zwei A-Untermoduln, so existiert genau eine A-lineare Abbildung

$$\varphi : \left(L/M\right) / \left(N/M\right) \xrightarrow{\sim} L/N$$

für die für alle $x \in L$ schon

$$\varphi\left((x + M) + \left(N/M\right)\right) = x + N$$

gilt. Dieses φ ist ein A-linearer Isomorphismus.

ii) Sind M ein A-Modul und M_1,$M_2 \subseteq M$ zwei A-Untermoduln, so existiert genau eine A-lineare Abbildung

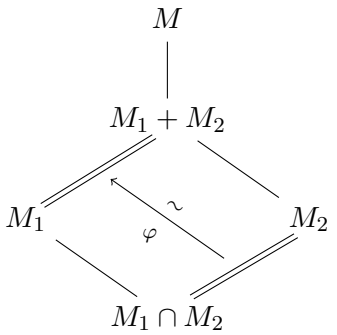
$$\varphi : M_2/(M_1 \cap M_2) \xrightarrow{\sim} M_1 + M_2/M_1$$

für die für alle $x \in M_2$ schon

$$\varphi(x + (M_1 \cap M_2)) = x + M_1$$

gilt. Dieses φ ist ein Isomorphismus.

Merkhilfe:



Beweis

i) Betrachte die Abbildung:

$$\begin{aligned} \psi : {}^{L}\!/_{M} &\to {}^{L}\!/_{N} \\ x + M &\mapsto x + N \end{aligned}$$

Diese ist wegen $M \subseteq N$ wohldefiniert und surjektiv, und offenbar A-linear. Außerdem gilt:

$$\ker \psi = \left\{ x + M \in {}^{L}\!/_{M} \,\middle|\, x + N = N \right\} = \left\{ x + M \in {}^{L}\!/_{M} \,\middle|\, x \in N \right\} = {}^{N}\!/_{M}$$

Damit folgt nach 2.6, dass es eine eindeutige A-lineare Abbildung

$$\varphi : \left({}^{L}\!/_{M} \right) / \left({}^{N}\!/_{M} \right) \xrightarrow{\sim} {}^{L}\!/_{N}$$

mit

$$\varphi \left((x + M) + \left({}^{N}\!/_{M} \right) \right) = x + N$$

gibt. $\square_{\text{i)}}$

ii) Betrachte die Abbildung:

$$\begin{aligned} \psi : M_2 \hookrightarrow M_1 + M_2 &\twoheadrightarrow {}^{M_1 + M_2}\!/_{M_1} \\ x &\mapsto x + M_1 \end{aligned}$$

Diese Komposition von Inklusions- und Projektionshomomorphismus ist A-linear. Außerdem gilt:

$$\ker \psi = \left\{ x \in M_2 \middle| x + M_1 = M_1 \right\} = \left\{ x \in M_2 \middle| x \in M_1 \right\} = M_1 \cap M_2$$

Damit folgt nach 2.6, dass es eine eindeutige A-lineare Abbildung

$$\varphi : {}^{M_2}\!/_{(M_1 \cap M_2)} \xrightarrow{\sim} {}^{M_1 + M_2}\!/_{M_1}$$

mit

$$\varphi \left(x + (M_1 \cap M_2) \right) = x + M_1$$

gibt. $\square_{\text{ii)}}$

2.9 **Bemerkung und Definition** (Produkt und direkte Summe)

Seien A ein Ring, I eine Menge und für alle $i \in I$ sei M_i ein A-Modul.

i) Das kartesische Produkt $\prod_{i \in I} M_i$ ist ein A-Modul vermöge komponentenweiser Addition und Skalarmultiplikation, *das Produkt der* M_i. Für alle $i_0 \in I$ ist die Abbildung

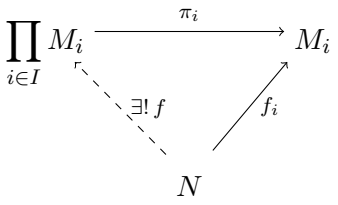
$$\pi_{i_0} : \prod_{i \in I} M_i \to M_{i_0}$$

A-linear und für jeden A-Modul N ist die Abbildung

$$\begin{aligned}\mathrm{Hom}_A\left(N, \prod_{i\in I} M_i\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A\left(N, M_i\right)\\ f &\mapsto \left(\pi_i^* f = \pi_i \circ f\right)_{i\in I}\end{aligned}$$

ein A-linearer Isomorphismus.

Skizze:



Die eindeutige Abbildung ist $f(x) = (f_i(x))_{i\in I}$ für alle $x \in N$.

Dies ist *die universelle Eigenschaft des Produkts.*

ii) Die Teilmenge

$$\bigoplus_{i\in I} M_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} M_i \,\middle|\, \left|\left\{i \in I \middle| x_i \neq 0\right\}\right| < \infty \right\} \subseteq \prod_{i\in I} M_i$$

ist ein A-Untermodul, *die direkte Summe der M_i.*

Die Abbildungen

$$\begin{aligned}\iota_i : M_i &\hookrightarrow \bigoplus_{i\in I} M_i\\ x &\mapsto \left(\iota_i(x)\right)_j := \delta_{ij} \cdot x\end{aligned}$$

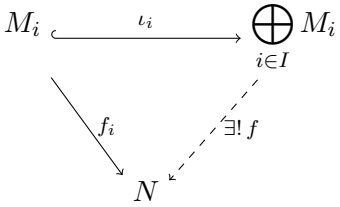
sind A-linear und für jeden A-Modul N ist die Abbildung

$$\begin{aligned}\mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A\left(M_i, N\right)\\ f &\mapsto \left(f \circ \iota_i = \iota_{i,*}(f)\right)\end{aligned}$$

ein A-linearer Isomorphismus.

Dies ist *die universelle Eigenschaft der direkten Summe.*

Skizze:



Beachte:
$\bigoplus_{i\in I} M_i$ ist nicht dasselbe wie $\sum_{i\in I} M_i$ aus 2.7 i).
Aber falls alle $M_i \subseteq M$ Untermoduln desselben Moduls M sind, gibt es genau eine A-lineare Abbildung

$$f : \bigoplus_{i\in I} M_i \to \sum_{i\in I} M_i$$

für die für alle $i \in I$ und $x_i \in M_i$ schon $f(x_i) = x_i$ gilt.

2.10 Beispiel

Seien A ein Ring und X eine Menge. Dann heißt

$$A^{(X)} := \bigoplus_{x\in X} A$$

der freie A-Modul mit Basis X.
Für jeden A-Modul N erhalte einen A-linearen Isomorphismus:

$$\mathrm{Hom}_A\left(A^{(X)},N\right) \underset{\text{2.9 ii)}}{\overset{\sim}{\to}} \prod_{x\in X} \mathrm{Hom}_A(A,N) \underset{\text{2.3 iv)}}{\overset{\prod \varepsilon_N}{\to}} \prod_{x\in X} N = \mathrm{Abb}(X,N)$$

Dies ist *die universelle Eigenschaft des freien A-Moduls.*

2.11 Satz (Cayley-Hamilton)

Seien A ein Ring, $I \subseteq A$ ein Ideal, M ein durch $n \in \mathbb{N}$ Elemente erzeugbarer A-Modul und

$$f \in \mathrm{End}_A(M) := \mathrm{Hom}_A(M,M)$$

erfülle:

$$f(M) \subseteq IM := \left\{ \sum_{i=1}^{m} \alpha_i x_i \,\middle|\, m \in \mathbb{N}, \alpha_i \in I, x_i \in M \right\} \subseteq M$$

Dann existiert ein

$$P(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$$

mit $a_i \in I^i \subseteq A$ für alle $1 \leq i \leq n$ und $P(f) = 0$ in $\mathrm{End}_k(M)$.

Beweis

Wähle Elemente $x_1,\ldots,x_n \in M$ mit $M = \sum_{i=1}^{n} Ax_i$. Schreibe für alle $1 \leq i \leq n$

$$f(x_i) = \sum_{j=1}^{n} a_{ij} \cdot x_j$$

mit geeigneten $a_{ij} \in I$.
Setze $Z := (\delta_{ij} X - a_{ij})_{1 \leq i,j \leq n} \in M_n(A[X])$. Dann gilt:

$$\underbrace{Z(f)}_{\in M_n(\mathrm{End}_A(M))} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Es folgt durch Linksmultiplikation mit der Adjunkten $Z^{\mathrm{ad}}(f)$ von $Z(f)$:

$$\left(Z^{\mathrm{ad}}(f) \cdot Z(f)\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Wegen $\left(Z^{\mathrm{ad}}(f) \cdot Z(f)\right) = \det(Z)(f) \cdot E_n$ gilt mit $P := \det(Z)$ für alle $1 \leq i \leq n$:

$$P(f)(x_i) = 0$$

Also folgt wegen $M = \sum_{i=1}^{n} Ax_i$, dass $P(f) = 0$ in $\mathrm{End}_A(M)$ gilt.
Bekannte Rechenregeln für die Determinante zeigen, dass P die behauptete Form besitzt. $\square_{2.11}$

2.12 Korollar

Seien A ein Ring, M ein endlich erzeugter A-Modul und $f : M \to M$ ein A-linearer Epimorphismus. Dann ist f ein Isomorphismus.

Beweis

Betrachte M als $A[X]$-Modul vermöge f, das heißt vermöge des Ringhomomorphismus:

$$\begin{aligned} \psi : A[X] &\to \mathrm{End}_{\mathbb{Z}}(M) \\ a(X) &\mapsto a(f) \end{aligned}$$

(vergleiche 2.1 i))

Weil f surjektiv ist, gilt $f(M) = (X)M \overset{f \text{ surjektiv}}{=} M = \mathrm{id}_M(M)$.
Aus dem Satz 2.11 von Cayley-Hamilton mit $A[X]$ als Ring, (X) als Ideal und id_M als Endomorphismus folgt die Existenz eines Polynoms $P(Y) = Y^n + a_1 Y^{n-1} + \ldots + a_n \in A[X][Y]$ mit $a_i \in \left(X^i\right) \subseteq A[X]$ und

$$0 = P(\mathrm{id}_M) = \mathrm{id}_M + a_1 \mathrm{id}_M + \ldots + a_n$$

in $\mathrm{End}_{A[X]}(M)$. Wegen $a_i \in (X)$ folgt durch Ausklammern von X

$$P(Y) = Y^n + g(X,Y) \cdot X$$

für ein geeignetes Polynom $g \in A[X,Y]$ und somit

$$0 = \mathrm{id}_M + g(\mathrm{id}_M, f) \circ f$$

in $\mathrm{End}_A(M)$ für ein geeignetes Polynom g. Damit gilt $\mathrm{id}_M = g(\mathrm{id}_M, f) \circ (-f)$, also ist f injektiv und damit ein Isomorphismus. $\square_{2.12}$

2.13 **Korollar** (Isomorphie erhält Dimension)

Sei $A \neq \{0\}$ ein Ring.
Dann folgt für alle $n,m \in \mathbb{N}_{\geq 1}$ aus der Existenz eines A-linearen Isomorphismus $f : A^n \xrightarrow{\sim} A^m$, dass $n = m$ gilt.

1. Beweis

Sei ohne Einschränkung $n \geq m$, so betrachte die Projektion π auf die ersten m Summanden. Dann ist

$$A^m \underset{f}{\xrightarrow{\sim}} A^n = \underbrace{A \oplus \ldots \oplus A}_{n\text{-mal}} \overset{\pi}{\twoheadrightarrow} A^m$$

ein surjektiver A-linearer Endomorphismus des endlich erzeugten A-Moduls A^m und nach 2.12 also ein Isomorphismus. Damit ist π ein Isomorphismus, also gilt:

$$(0) = \ker(\pi) = A^{n-m}$$

Wegen $A \neq \{0\}$ folgt $n - m = 0$, also $n = m$. $\square_{\text{1. Beweis}}$

2. Beweis

Wegen $A \neq \{0\}$, 1.22 und 1.18 ii) existiert ein maximales Ideal $\mathfrak{m}$ und somit ein Körper $k \cong {}^{A}\!/_{\mathfrak{m}}$ und ein Ringhomomorphismus $A \to k$. Dann ist

$$f \oplus_A 1 : A^n \oplus_A k \xrightarrow{\sim} A^m \oplus_A k$$

ein Isomorphismus von n- und m-dimensionalen k-Vektorräumen. Also gilt $n = m$ nach dem Basisergänzungssatz aus linearer Algebra I. $\square_{\text{2. Beweis}}$

2.14 Bemerkung

i) Offenbar gilt 2.13 nicht für den Nullring.

ii) Es existiert ein notwendigerweise nicht kommutativer Ringe $R \neq \{0\}$ für den $R \cong R^2$ als R-Modul gilt.

2.15 Korollar

Seien A ein Ring, M ein endlich erzeugter A-Modul und $I \subseteq A$ ein Ideal mit $IM = M$.
Dann existiert ein $x \in A$ mit $x \equiv 1 \mod I$ und $xM := \{xm \mid m \in M\} = (0)$.

Beweis

Wähle in Satz 2.11 von Cayley-Hamilton $f := \mathrm{id}_M$ und dann in dortiger Notation:

$$x := 1 + \underbrace{a_1 + \ldots + a_n}_{\in I} \equiv 1 \mod I$$

$\square_{2.15}$

2.16 **Lemma** (von Nakayama) **und Definition** (Jacobsonradikal)

Seien A ein Ring, M ein endlich erzeugter A-Modul und

$$I \subseteq \mathrm{Jac}\,(A) := \bigcap_{\mathfrak{m} \subseteq A \text{ max. Ideal}} \mathfrak{m}$$

ein Ideal, das im *Jacobsonradikal von* A enthalten ist. Dann folgt aus $IM = M$ schon $M = (0)$.

Beweis

Nach 2.15 existiert ein $x \in A$ mit $xM = (0)$ und $x \equiv 1 \mod I$. Es folgt $1 - x \in \mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m} \subseteq A$, also $x \notin \mathfrak{m}$, da sonst der Widerspruch $1 = (1-x) + x \in \mathfrak{m}$ folgte, und damit ist $x \in A^*$ nach 1.24 ii) $\Rightarrow$ i). Aus $xM = 0$ und $x \in A^*$ folgt $M = (0)$. $\square_{2.16}$

2.17 Beispiel

Sei $\big(A := \mathbb{Z}_{(p)}, \mathfrak{m} := (p)\big)$ ist nach 1.28 ein lokaler Ring, also gilt $\mathrm{Jac}\,(A) = \mathfrak{m} = (p) \subseteq \mathbb{Z}_{(p)}$.
Für $M := \mathbb{Q}$ aufgefasst als A-Modul – beachte, dass $A \subseteq \mathbb{Q}$ ein Unterring ist – gilt:

$$\mathfrak{m}M = (p) \cdot \mathbb{Q} = \mathbb{Q} = M$$

Wegen $M \neq 0$ folgt aus 2.16, dass M als A-Modul nicht endlich erzeugt ist, beziehungsweise, dass man in 2.16 nicht auf „M endlich erzeugt“ verzichten kann.

2.18 **Proposition** (minimales Erzeugendensystem)

Sei $(A, \mathfrak{m})$ ein lokaler Ring, M ein endlich erzeugter A-Modul und für $x_1, \ldots, x_n \in M$ gelte, dass

$$\{\overline{x}_i\}_{1 \leq i \leq n} \subseteq {}^{M}\!/_{\mathfrak{m}M}$$

eine Basis dieses ${}^{A}\!/_{\mathfrak{m}} = \kappa(\mathfrak{m})$-Vektorraums ist. Dann ist $\{x_1, \ldots, x_n\} \subseteq M$ ein minimales Erzeugendensystem des A-Moduls M.

Beweis

Für

$$N := \sum_{i=1}^{N} Ax_i \subseteq M$$

ist die Komposition $N \hookrightarrow M \overset{\pi}{\twoheadrightarrow} {}^{M}\!/_{\mathfrak{m}M}$ surjektiv, da alle $\overline{x}_i$ im Bild liegen, also gilt:

$$M = \pi(N) = N + \mathfrak{m}M$$

Es folgt ${}^{M}\!/_{N} \subseteq \mathfrak{m} \cdot \left({}^{M}\!/_{N}\right)$ und damit ${}^{M}\!/_{N} = (0)$ nach dem Lemma 2.16 von Nakayama, da $\mathrm{Jac}\,(A) = \mathfrak{m}$ ist. Damit gilt:

$$M = N = \sum_{i=1}^{n} Ax_i$$

Also ist $\{x_1, \ldots, x_n\} \subseteq M$ ein Erzeugendensystem, dessen Minimalität sofort aus derjenigen von $\{\overline{x_u}\}_{1 \leq i \leq n}$ folgt. $\square_{2.18}$

2.19 **Definition** (exakte Folge)

Sei A ein Ring. Eine Folge von A-Moduln und A-linearen Abbildungen

$$\ldots \to M_{i-1} \overset{f_{i-1}}{\to} M_i \overset{f_i}{\to} M_{i+1} \to \ldots$$

heißt *exakt an der Stelle* M_i, falls gilt:

$$\operatorname{im}(f_{i-1}) = \ker(f_i)$$

(„$\subseteq$“ bedeutet $f_i \circ f_{i-1} = 0$ und „$\supseteq$“ bedeutet $f_i(x) = 0 \Rightarrow x = f_{i-1}(y)$.)
Sie heißt *exakt*, falls sie an jeder Stelle exakt ist.

2.20 **Beispiel und Definition** (kurze exakte Folge)

In der Situation von 2.19 gilt:

i) $0 \to M \overset{f}{\to} N$ exakt $\Leftrightarrow 0 = \ker(f) \Leftrightarrow f$ ist injektiv.

ii) $M \overset{f}{\to} N \to 0$ exakt $\Leftrightarrow \operatorname{im}(f) = N \Leftrightarrow f$ ist surjektiv.

iii) $0 \to M \overset{f}{\to} N \overset{g}{\to} L \to 0$ exakt $\Leftrightarrow f$ injektiv, g surjektiv und $\operatorname{im}(f) = \ker(g)$.
In diesem Fall heißt die $0 \to M \overset{f}{\to} N \overset{g}{\to} L \to 0$ *eine kurze exakte Folge.*

2.21 **Proposition**

Sei A ein Ring.

i) Eine Folge $\mathscr{E} = \left(M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0\right)$ von A-Moduln ist genau dann exakt, wenn für alle A-Moduln N die Folge

$$\operatorname{Hom}_A(\mathscr{E},N) := \left(0 \to \operatorname{Hom}_A(M'',N) \overset{g^*}{\to} \operatorname{Hom}_A(M,N) \overset{f^*}{\to} \operatorname{Hom}_A(M',N)\right)$$

exakt ist.

ii) Eine Folge $\mathscr{E} = \left(0 \to M' \overset{f}{\to} M \overset{g}{\to} M''\right)$ von A-Moduln ist genau dann exakt, wenn für alle A-Moduln N die Folge

$$\operatorname{Hom}_A(N,\mathscr{E}) := \left(0 \to \operatorname{Hom}_A(N,M') \overset{f_*}{\to} \operatorname{Hom}_A(N,M) \overset{g_*}{\to} \operatorname{Hom}_A(N,M'')\right)$$

exakt ist.

Beweis

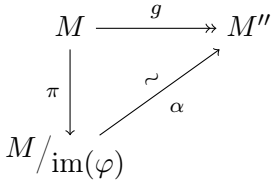
i) Sei $\mathscr{E}$ exakt. Zeige die Exaktheit von $\mathrm{Hom}_A(\mathscr{E},N)$ an der Stelle $\mathrm{Hom}_A(M,N)$:
Für $\varphi \in \mathrm{Hom}_A(M'',N)$ gilt:

$$(f^* \circ g^*)(\varphi) = \varphi \circ \underbrace{g \circ f}_{=0} \overset{\mathrm{im}(f) \subseteq \ker(g)}{=} 0$$

Ist umgekehrt $\varphi \in \ker(f^*) \subseteq \mathrm{Hom}_A(M,N)$, so gilt $0 = f^*(\varphi) = \left(M' \overset{f}{\to} M \overset{\varphi}{\to} N\right)$, das heißt $\varphi(\mathrm{im}(f)) = 0$ und wegen 2.4 iii) (mit $N = \mathrm{im}(\varphi)$ und $L = N$ in dortiger Notation) existiert genau eine A-lineare Abbildung $\psi : {}^{M}\!/_{\mathrm{im}(f)} \to N$ mit:

$$\varphi = \left(M \overset{\pi}{\twoheadrightarrow} {}^{M}\!/_{\mathrm{im}(f)} \overset{\psi}{\to} N\right)$$

Andererseits faktorisiert g über einen Isomorphismus $\alpha : {}^{M}\!/_{\mathrm{im}(f)} \twoheadrightarrow M''$:



Da g surjektiv ist. Es folgt:

$$\varphi = \psi \circ \pi = \psi \circ \alpha^{-1} \circ \alpha \circ \pi = \psi \circ \alpha^{-1} \circ g = g^*\left(\psi \circ \alpha^{-1}\right) \in \mathrm{im}(g^*)$$

Insgesamt gilt also $\ker(f^*) = \mathrm{im}(g^*)$. Der Rest des Beweises bleibt als Übung.

$\square_{2.21}$

2.22 Bemerkung

2.21 überträgt sich nicht auf exakte Folgen $\mathscr{E}$ beliebiger Gestalt.
Zum Beispiel ist

$$\mathscr{E} := \left(0 \to \mathbb{Z} \overset{(\cdot 2)}{\to} \mathbb{Z}\right)$$
$$x \mapsto 2x$$

eine exakte Folge von $\mathbb{Z}$-Moduln, aber die Folge

$$\mathrm{Hom}_{\mathbb{Z}}(\mathscr{E},\mathbb{Z}) = \left(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \overset{(\cdot 2)^*}{\to} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \overset{0^*}{\to} \mathrm{Hom}_{\mathbb{Z}}(0,\mathbb{Z}) = 0\right)$$

ist nicht exakt, da $\mathrm{id}_{\mathbb{Z}} \in \ker(0^*) \setminus \mathrm{im}((\cdot 2)^*)$ liegt, denn sonst wäre $\mathrm{id}_{\mathbb{Z}} = (\cdot 2)^*(f)$ für eine geeignete $\mathbb{Z}$-lineare Abbildung $f : \mathbb{Z} \to \mathbb{Z}$, also

$$1 = \mathrm{id}_{\mathbb{Z}}(1) = ((\cdot 2)^*(f))(1) = f(2 \cdot 1) = 2 \cdot f(1)$$

in $\mathbb{Z}$. Dies ist ein Widerspruch, da $1 \notin 2 \cdot \mathbb{Z}$ ist.

2.23 Projektive Moduln

2.23.1 Definition (spalten, direkter Summand)

i) Eine kurze exakte Folge $0 \to M' \to M \overset{\pi}{\underset{s}{\rightleftarrows}} M'' \to 0$ von A-Moduln *spaltet* genau dann, wenn es eine A-lineare Abbildung $s : M'' \to M$ mit $\pi \circ s = \mathrm{id}_{M''}$ gibt.

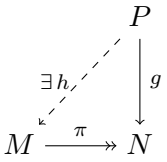
ii) Ein A-Untermodul $N \overset{\iota}{\hookrightarrow} M$ ist genau dann *ein direkter Summand (von M)*, wenn eine A-lineare Abbildung $f : M \to N$ mit $f \circ \iota = \mathrm{id}_N$ existiert.
(In diesem Fall gilt $M = N \oplus \ker(f)$.)
Zum Beispiel ist $2\mathbb{Z} \subseteq \mathbb{Z}$ kein direkter Summand und $0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ spaltet nicht, da die einzige $\mathbb{Z}$-lineare Abbildung von $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ die Nullabbildung ist.

2.23.2 Proposition und Definition (Lift, projektiver Modul)

Sei A ein Ring. Für einen A-Modul P sind äquivalent:

i) Jede kurze exakte Folge von A-Moduln der Form $0 \to M' \to M \to P \to 0$ spaltet.

ii) Für jeden A-linearen Epimorphismus $\pi : M \twoheadrightarrow N$ in einen Ring N und jede A-lineare Abbildung $g : P \to N$ existiert *ein Lift von g*, also eine A-lineare Abbildung $h : P \to M$ mit $\pi \circ h = g$.
Skizze:

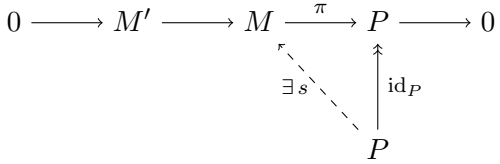


iii) P ist direkter Summand eines freien A-Moduls.

In diesem Fall heißt der A-Modul P *projektiv*.

Beweis

„ii) ⇒ i)“: Betrachte:



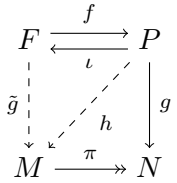
Weil π surjektiv ist und wegen ii) existiert eine A-lineare Abbildung $s : P \to M$ mit $\mathrm{id}_P = \pi \circ s$, das heißt obige Folge spaltet.
„i) ⇒ iii)“: Es existiert ein freier A-Modul F zusammen mit einem A-linearen Epimorphismus $\pi : F \twoheadrightarrow P$, zum Beispiel $F = A^{(P)} \twoheadrightarrow P$ mit der kanonischen Projektion.

Wegen i) spaltet die kurze exakte folge $0 \to \ker(\pi) \to F \xrightarrow{\pi} P \to 0$, das heißt es existiert eine A-lineare Abbildung $\iota : P \to F$ mit $\pi \circ \iota = \mathrm{id}_P$. Damit ist $P' := \iota(P) \subseteq F$ ein zu P isomorpher A-Modul, der durch $f := \iota \circ \pi : F \to P'$ als direkter Summand von F erkannt wird.

„iii) ⇒ ii)“: Nach Voraussetzung gilt $P \xhookrightarrow{\iota} F$ für einen freien A-Modul F und es existiert eine A-lineare Abbildung $f : F \to P$ mit:

$$f \circ \iota = \mathrm{id}_P \tag{2.1}$$

Betrachte:



Sei $X \subseteq F$ eine A-Basis. Weil F frei ist, existiert eine A-lineare Abbildung $\tilde{g} : F \to M$, sodass für alle $x \in X$ gilt:

$$\pi \circ \tilde{g}(x) = g \circ f(x)$$

Man wählt einfach für $\tilde{g}(x)$ ein Element aus $\pi^{-1}(g(f(x))) \neq \emptyset$, was immer geht, da π surjektiv ist. Weil F frei ist und $\tilde{g}$ dadurch auf einer Basis von F bestimmt ist, ist F schon vollständig festgelegt und es folgt:

$$\pi \circ \tilde{g} = g \circ f \tag{2.2}$$

Setze nun $h := \tilde{g} \circ \iota$ und rechne:

$$\pi \circ h = \pi \circ \tilde{g} \circ \iota \overset{2.2}{=} g \circ f \circ \iota \overset{2.1}{=} g \circ \mathrm{id}_P = g$$

Daher ist h ein Lift von g. □2.23.2

2.23.3 Proposition

Äquivalent zu i) bis iii) in 2.23.2 ist ebenfalls:

iv) Für jede kurze exakte Folge von A-Moduln $\mathscr{E} = (0 \to M' \to M \to M'' \to 0)$ ist die Folge $\mathrm{Hom}_A(P,\mathscr{E})$ ebenfalls exakt.

Beweis

Der Beweis bleibt als Übung. □2.23.3

2.24 **Definition** (bilineare Abbildung)

Seien A ein Ring und M,N,L drei A-Moduln.

Eine Abbildung $f : M \times N \to L$ heißt *A-bilinear*, falls für alle $m_0 \in M$ und alle $n_0 \in N$ die Abbildungen

$$\begin{aligned} M &\to L \\ m &\mapsto f(m,n_0) \end{aligned}$$

und

$$\begin{aligned} N &\to L \\ n &\mapsto f(m_0,n) \end{aligned}$$

beide A-linear sind.

2.25 Satz und Definition (Tensorprodukt)

Seien A ein Ring und M,N zwei A-Moduln. Dann existiert ein A-Modul $M \otimes_A N$ und eine A-bilineare Abbildung

$$\tau : M \times N \to M \otimes_A N$$

so, dass für jede A-bilineare Abbildung $f : M \times N \to L$ genau eine A-lineare Abbildung $\alpha : M \otimes_A N \to L$ mit $f = \alpha \circ \tau$ existiert.
Der A-Modul $M \otimes_A N$, genauer die A-bilineare Abbildung τ, heißt *das Tensorprodukt von M und N (über A).*
Schreibe $m \otimes n := \tau(m,n)$ für alle $(m,n) \in M \times N$. Dann kann man jedes $x \in M \otimes_A N$ als

$$x = \sum_{i=1}^{n} m_i \otimes n_i$$

für ein $n \in \mathbb{N}_{\geq 0}$ und geeignete $m_i \in M$ und $n_i \in N$ schreiben.

Beweis

Der Beweis ist genauso wie in dem aus der Linearen Algebra II bekannten Fall, dass A ein Körper ist. $\square_{2.25}$

2.26 Bemerkung und Definition $(f \otimes g)$

Seien A ein Ring, M,M',N,N' vier A-Moduln und $f : M \to M'$,$g : N \to N'$ zwei A-lineare Abbildungen.
Dann existiert genau eine A-lineare Abbildung $f \otimes g : M \otimes_A N \to M' \otimes_A N'$, sodass für alle $(m,n) \in M \times N$ gilt:

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

Ferner existiert genau eine A-lineare Abbildung (im Allgemeinen kein Isomorphismus)

$$\mathrm{Hom}_A(M,M') \otimes_A \mathrm{Hom}_A(N,N') \to \mathrm{Hom}_A(M \otimes_A N, M' \otimes_A N')$$

mit:

$$(f) \otimes (g) \mapsto (f \otimes g)$$

Achtung Notationsüberlastung!
$(f) \otimes (g)$ wie in 2.25 und $(f \otimes g)$ wie in 2.26.

2.27 **Satz** (natürliche Isomorphismen)

Seien A ein Ring, M,N zwei A-Moduln, I eine Menge und für alle $i \in I$ sei M_i ein A-Modul. Die folgenden Vorschriften definieren eindeutige A-lineare Abbildungen und jede solche ist ein natürlicher Isomorphismus:

i)
$$\begin{aligned} M \otimes_A N &\overset{\sim}{\underset{\neq}{\to}} N \otimes_A M \\ m \otimes n &\mapsto n \otimes m \end{aligned}$$

(Beispiel: $\mathrm{End}_k\left(k^n\right) \overset{\sim}{\underset{\neq}{\to}} M_n(k)$ ist nicht natürlich, sondern von der Basis abhängig.)

ii)
$$\begin{aligned} (M \otimes_A N) \otimes_A L &\overset{\sim}{\to} M \otimes_A (N \otimes_A L) \\ (m \otimes n) \otimes l &\mapsto m \otimes (n \otimes l) \end{aligned}$$

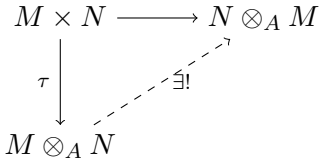
iii)
$$\begin{aligned} \left(\bigoplus_{i \in I} M_i\right) \otimes_A N &\overset{\sim}{\to} \left(\bigoplus_{i \in I} M_i \otimes_A N\right) \\ (m_i)_{i \in I} \otimes n &\mapsto (m_i \otimes n)_{i \in I} \end{aligned}$$

iv)
$$\begin{aligned} A \otimes_A M &\overset{\sim}{\to} M \\ a \otimes m &\mapsto am \end{aligned}$$

Beweis

i) Existenz und Eindeutigkeit der linearen Abbildung folgen aus 2.25 aus der offensichtlichen Bilinearität von:

$$\begin{aligned} M \times N &\to N \otimes_A M \\ (m,n) &\mapsto n \otimes m \end{aligned}$$



Die Abbildung ist ein Isomorphismus, da

$$\begin{aligned} N \otimes_A M &\to M \otimes_A N \\ n \otimes m &\mapsto m \otimes n \end{aligned}$$

ihr Inverses ist.

Die Natürlichkeit bedeutet hier:

Sind $f : M \to M'$ und $g : N \to N'$ beide A-linear, so ist das Diagramm

$$\begin{array}{ccc} M \otimes_A N & \xrightarrow[\text{i)}]{\sim} & N \otimes_A M \\ {\scriptstyle f \otimes g}\downarrow & & \downarrow{\scriptstyle g \otimes f} \\ M' \otimes_A N' & \xrightarrow[\text{i)}]{\sim} & N' \otimes_A M' \end{array}$$

kommutativ, was klar ist:

$$\begin{array}{ccc} m \otimes_A n & \longmapsto & n \otimes_A m \\ \downarrow & & \downarrow \\ f(m) \otimes g(n) & \longmapsto & g(n) \otimes f(m) \end{array}$$

Zudem sind die $m \otimes n$ Erzeuger, womit die Aussage folgt.
ii), iii) und iv) folgen analog. $\square_{2.27}$

2.28 Satz

Seien A ein Ring und M,N,L drei A-Moduln. Dann ist die Abbildung

$$\varphi(M,N,L) : \mathrm{Hom}_A(M \otimes_A N,L) \xrightarrow{\sim} \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,L))$$

für alle $\alpha \in \mathrm{Hom}_A(M \otimes_A N,L)$, $m \in M$ und $n \in N$ definiert durch

$$\varphi(M,N,L)(\alpha)(m)(n) := \alpha(m \otimes n) \tag{2.3}$$

ein natürlicher A-linearer Isomorphismus.

Beweis

Man sieht leicht, dass $\varphi(M,N,L)$ wohldefiniert ist.

Behauptung Es existiert genau eine A-lineare Abbildung

$$\psi : \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,L)) \to \mathrm{Hom}_A(M \otimes_A N,L)$$

für die für alle $f \in \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,L))$, $m \in M$ und $n \in N$ gilt:

$$\psi(f)(m \otimes n) = f(m)(n) \tag{2.4}$$

Beweis Für gegebenes f ist die Abbildung

$$\begin{aligned} M \times N &\to L \\ (m,n) &\to f(m)(n) \end{aligned}$$

schon A-bilinear. Also existiert genau eine A-lineare Abbildung $\psi(f) : M \otimes_A N \to L$ mit $\psi(f)(m \otimes n) = f(m)(n)$.
Dann sieht man leicht, dass $f \mapsto \psi(f)$ schon A-linear ist. $\square_{\text{Behauptung}}$

Behauptung $\psi = \varphi(M,N,L)^{-1}$ (Insbesondere ist damit $\varphi(M,N,L)$ ein A-linearer Isomorphismus.)

Beweis Für $f \in \mathrm{Hom}_A(M \otimes_A N,L)$, $m \in M$ und $n \in N$ rechne:

$$\psi(\varphi(M,N,L)(f))(m \otimes n) \overset{(2.4)}{=} (\varphi(M,N,L)(f))(m)(n) = \overset{(2.3)}{=} f(m \otimes n)$$

Also folgt $\psi \circ \varphi(M,N,L) = \mathrm{id}$ und analog folgt $\varphi(M,N,L) \circ \psi = \mathrm{id}$. $\square_{\text{Behauptung}}$

Die Natürlichkeit bedeutet hier:
Sind $a : M' \to M$, $b : N' \to N$ und $c : L \to L'$ alle A-linear, so ist das Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_A(M \otimes_A N,L) & \xrightarrow[\varphi(M,N,L)]{\sim} & \mathrm{Hom}_A(M,\mathrm{Hom}_A(N,L)) \\ \downarrow{\scriptstyle (a \otimes b)^* \circ c_*} & & \downarrow{\scriptstyle (b^* \circ c_*)_* \circ a^*} \\ \mathrm{Hom}_A(M' \otimes_A N',L') & \xrightarrow[\varphi(M',N',L')]{\sim} & \mathrm{Hom}_A(M',\mathrm{Hom}_A(N',L')) \end{array}$$

kommutativ.
Rechne dazu für beliebige $\alpha \in \mathrm{Hom}_A(M \otimes_A N,L)$, $m' \in M'$ und $n' \in N'$ einerseits

$$\begin{aligned} \left(\varphi\left(M',N',L'\right) \circ \left((a \otimes b)^* \circ c_*\right)\right)(\alpha)\left(m'\right)\left(n'\right) &= \varphi\left(M',N',L'\right)\left(\left((a \otimes b)^* \circ c_*\right)(\alpha)\right)\left(m'\right)\left(n'\right) = \\ &\overset{(2.3)}{=} \left(\left((a \otimes b)^* \circ c_*\right)(\alpha)\right)\left(m' \otimes n'\right) = \\ &\overset{2.3\text{ iii)}}{=} c\left(\alpha\left((a \otimes b)\left(m' \otimes n'\right)\right)\right) = \\ &\overset{2.26}{=} c\left(\alpha\left(a\left(m'\right) \otimes b\left(n'\right)\right)\right) \end{aligned}$$

und andererseits:

$$\begin{aligned} \left(\left(\left(b^* \circ c_*\right)_* \circ a^*\right) \circ \varphi(M,N,L)\right)(\alpha)\left(m'\right)\left(n'\right) &\overset{2.3\text{ iii)}}{=} c\left(\left(\varphi(M,N,L)(\alpha) \circ a\right)\left(m'\right)\left(b'\left(n'\right)\right)\right) = \\ &\overset{(2.3)}{=} c\left(\alpha\left(a\left(m'\right) \otimes b\left(n'\right)\right)\right) \end{aligned}$$

$\square_{2.28}$

2.29 **Bemerkung und Definition** (Restriktion, Skalarerweiterung)

Seien $f : A \to B$ ein Ringhomomorphismus, M ein A-Modul und N ein B-Modul.

i) Vermöge $a \cdot n := f(a) \cdot n$ für alle $a \in A$ und $n \in N$ ist N ein A-Modul, *die Restriktion $f_*(N)$ von N entlang f.*

ii) Auf dem A-Modul $f^*(M) := B \otimes_A M$ wird durch

$$b \cdot \left(b' \otimes m\right) := \left(bb'\right) \otimes m$$

für alle $b,b' \in B$ und $m \in M$ die Struktur eines B-Moduls definiert, *die Skalarerweiterung von M entlang f.*

2.30 Beispiel

i) Sind A ein Ring, M ein A-Modul und $f : \mathbb{Z} \to A$ der eindeutige Ringhomomorphismus, so ist $f_* (M)$ die M zugrunde liegende abelsche Gruppe.

ii) Sind A ein Integritätsring (Abkürzung: IR), M ein endlich erzeugter A-Modul und

$$\iota : A \hookrightarrow k := \operatorname{Quot}(A)$$

der Quotientenkörper von A, zum Beispiel $\mathbb{Z} = A \hookrightarrow k = \mathbb{Q}$, so ist $\iota^* (M) = k \otimes_A M$ ein endlich-dimensionaler k-Vektorraum und $\dim_k (\iota^* (M))$ heißt *der Rang von M*.

2.31 Satz

Seien $f : A \to B$ ein Ringhomomorphismus, M ein A-Modul und N ein B-Modul.
Dann ist die Abbildung

$$\begin{aligned} \Phi : \operatorname{Hom}_A (M, f_* (N)) &\xrightarrow{\sim} \operatorname{Hom}_B (f^* (M), N) \\ \varphi &\mapsto (b \otimes m \mapsto b \cdot \varphi (m)) \end{aligned} \tag{2.5}$$

wohldefiniert und ein Isomorphismus abelscher Gruppen.

Beweis

Zunächst ist für gegebenes A-lineares $\varphi : M \to f_* (N)$ die Abbildung

$$\begin{aligned} B \times M &\to N \\ (b, m) &\mapsto b \cdot \varphi (m) \end{aligned}$$

schon A-bilinear. Also existiert nach der universellen Eigenschaft des Tensorprodukts genau eine A-lineare Abbildung

$$\psi : B \otimes_A M = f^* (M) \to N$$

für die für alle $b \in B$ und $m \in M$ gilt:

$$b \otimes m \mapsto b \cdot \varphi (m)$$

Wegen

$$\begin{aligned} \psi \left(b \cdot \left(b' \otimes m \right) \right) &\overset{2.29\,\text{ii)}}{=} \psi \left(\left(bb' \right) \otimes m \right) \overset{(2.5)}{=} \left(bb' \right) \cdot \varphi (m) = \\ &\overset{N \text{ ist } B\text{-Modul}}{=} b \cdot \left(b' \cdot \varphi (m) \right) \overset{(2.5)}{=} b \cdot \psi \left(b' \otimes m \right) \end{aligned}$$

ist ψ sogar B-linear und damit ist Φ wohldefiniert.
Für $\psi \in \operatorname{Hom}_B (f^* (M), N)$ setze:

$$\begin{aligned} \Gamma (\psi) := \Big(M \to f^* (M) = B \otimes_A M &\xrightarrow{\psi} N \Big) \\ m \mapsto 1 \otimes m \quad &\mapsto \quad \psi (1 \otimes m) \end{aligned} \tag{2.6}$$

Wegen

$$\Gamma(\psi)(am) = \psi(1 \otimes (am)) = \psi(a(1 \otimes m)) = a\psi(1 \otimes m)$$

ist $\Gamma(\psi) \in \mathrm{Hom}_A(M, f_*(N))$.
Um zu sehen, dass Φ und Γ zueinander invers sind, rechne einerseits für beliebige A-lineare Abbildungen $\varphi \in \mathrm{Hom}_A(M, f_*(N))$ und $m \in M$

$$(\Gamma \circ \Phi)(\varphi)(m) = \Gamma(\Phi(\varphi))(m) \overset{(2.6)}{=} \Phi(\varphi)(1 \otimes m) \overset{(2.5)}{=} 1 \cdot \varphi(m) = \varphi(m)$$

also $\Gamma \circ \Phi = \mathrm{id}$, und andererseits für beliebige $\psi \in \mathrm{Hom}_B(f^*(M), N)$, $b \in B$ und $m \in M$:

$$(\Phi \circ \Gamma)(\psi)(b \otimes m) = \Phi(\Gamma(\psi))(b \otimes m) \overset{(2.5)}{=} b \cdot (\Gamma(\psi)(m)) \overset{(2.6)}{=} b \cdot \psi(1 \otimes m) =$$
$$\overset{\psi \text{ linear}}{=} \psi(b(1 \otimes m)) \underset{f^*(M)}{\overset{\text{Definition von}}{=}} \psi(b \otimes m)$$

Also gilt $\Phi \circ \Gamma = \mathrm{id}$. $\square_{2.31}$

2.32 Beispiel

i) Wähle $M = f_*(N)$ in 2.31 und erhalte:

$$\Phi : \mathrm{Hom}_A(f_*(N), f_*(N)) \xrightarrow{\sim} \mathrm{Hom}_B(f^*(f_*(N)), N)$$

Definiere:

$$\mathrm{can}_B := \Phi\left(\mathrm{id}_{f_*(N)}\right)$$

Dies ist eine kanonische B-lineare Abbildung für den B-Modul N:

$$\mathrm{can}_B : f^*(f_*(N)) = B \otimes_A N \to N$$

Aus der Definition (2.5) von Φ folgt, dass für alle $b \in B$ und $n \in N$ gilt:

$$\mathrm{can}_B(b \otimes n) = b \cdot n$$

ii) Wähle $N = f^*(M)$ in 2.31 und erhalte:

$$\Phi : \mathrm{Hom}_A(M, f_*(f^*(M))) \xrightarrow{\sim} \mathrm{Hom}_B(f^*(M), f^*(M))$$
$$\mathrm{can}_A := \Phi^{-1}\left(\mathrm{id}_{f^*(M)}\right) = \Gamma\left(\mathrm{id}_{f^*(M)}\right)$$

Dies ist eine kanonische A-lineare Abbildung für den A-Modul N:

$$\mathrm{can}_A : M \to f_*(f^*(M)) = B \otimes_A M$$

Aus der Definition (2.6) von Γ folgt, dass für alle $m \in M$ gilt:

$$\mathrm{can}_A(m) = 1 \otimes m$$

2.33 Proposition

Seien $f : A \to B$ ein Ringhomomorphismus, M ein A-Modul und N ein B-Modul.

i) Sind N als B-Modul und B als A-Modul endlich erzeugt, so ist auch der A-Modul $f_*(N)$ endlich erzeugt.

ii) Ist M als A-Modul endlich erzeugt, so auch $f^*(M)$ als B-Modul.

Beweis

i) Seien

$$N = \sum_{i=1}^{n} B \cdot n_i \tag{2.7}$$

und

$$B = \sum_{i=1}^{m} b_i A \tag{2.8}$$

für geeignete $m,n \in \mathbb{N}_{\geq 0}$, $n_i \in N$ und $b_i \in B$.

Dann schreibt sich jedes $n \in N$ für geeignete $\tilde{b}_i \in B$ und $a_j \in A$ in der Form:

$$n \overset{(2.7)}{=} \sum_{i=1}^{n} \tilde{b}_i n_i \overset{(2.8)}{=} \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_j b_j \right) n_i = \sum_{i,j}^{n,m} a_j (b_j n_i)$$

Es folgt:

$$f_*(N) = N = \sum_{i,j=1}^{n,m} A \cdot (b_j n_i)$$

Also ist der A-Modul $f_*(N)$ endlich erzeugt.

ii) Sind $x_1, \ldots, x_n \in M$ nun A-Modul-Erzeuger, so sind $1 \otimes x_1, \ldots, 1 \otimes x_n \in f^*(M) = B \otimes_A M$ schon B-Modul-Erzeuger. $\square_{2.33}$

2.34 Satz (Rechtsexaktheit des Tensorprodukts)

Seien A ein Ring, $\mathscr{E} := \left(M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0 \right)$ eine exakte Folge von A-Moduln und N ein A-Modul. Dann ist die Folge von A-Moduln

$$\mathscr{E} \otimes_A N := \left(M' \otimes_A N \overset{f \otimes \mathrm{id}_N}{\to} M \otimes_A N \overset{g \otimes \mathrm{id}_N}{\to} M'' \otimes_A N \to \{0\} \otimes_A N = 0 \right)$$

auch exakt.

Beweis

Für jeden A-Modul L ist

$$\mathrm{Hom}_A(\mathscr{E} \otimes_A N, L) \underset{2.28}{\tilde{\to}} \mathrm{Hom}_A(\mathscr{E}, \mathrm{Hom}_A(N, L))$$

exakt nach 2.21 i) „⇒“.
Da L beliebig ist, ist also auch die Folge $\mathscr{E} \otimes_A N$ exakt nach 2.21 i) „⇐“. $\square_{2.34}$

2.35 Proposition und Definition (flacher Modul)

Sei A ein Ring. Für einen A-Modul M sind äquivalent:

i) Für jede exakte Folge $\mathscr{E}$ von A-Moduln ist die Folge $\mathscr{E} \otimes_A M$ exakt.

ii) Für jede kurze exakte Folge $\mathscr{E}$ von A-Moduln ist die kurze Folge $\mathscr{E} \otimes_A M$ exakt.

iii) Für jeden A-linearen Monomorphismus $f : N' \hookrightarrow N$ ist auch $f \otimes \mathrm{id}_M : N' \otimes_A M \to N \otimes_A M$ injektiv.

iv) Für beliebige endlich erzeugte A-Moduln N und N' und jeden A-linearen Monomorphismus $f : N' \hookrightarrow N$ ist auch $f \otimes \mathrm{id}_M : N' \otimes_A M \to N \otimes_A M$ injektiv.

In diesem Fall heißt der A-Modul M *flach*.
Zum Beispiel ist $\mathbb{Z}/n\mathbb{Z}$ kein flacher $\mathbb{Z}$-Modul für $n \in \mathbb{N}_{\geq 1}$, denn $n \cdot \overline{1} = \overline{n} = \overline{0}$.

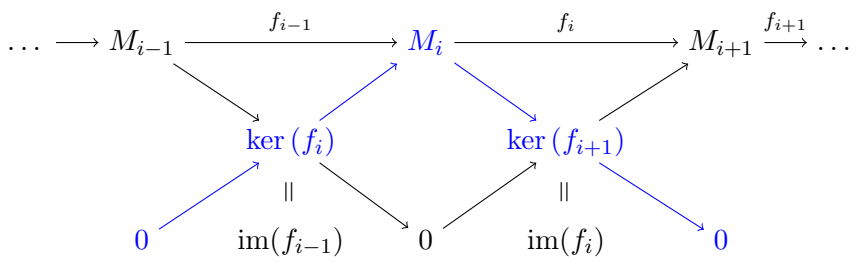
Beweis

Die Implikationen „i) ⇒ ii)“ und „iii) ⇒ iv)“ sind klar.
„ii) ⇒ iii)“ folgt, indem man die kurze exakte Folge

$$0 \to N' \xrightarrow{f} N \to \mathrm{koker}(f) \to 0$$

betrachtet.
„iv) ⇒ iii)“ folgt, da jeder A-Modul die Vereinigung seiner endlich erzeugten A-Untermoduln ist. Dies ist klar, da jeder A-Modul die Vereinigung seiner Elemente ist und diese in den von ihnen erzeugten A-Moduln sind und diese damit endlich erzeugt sind.
iii) ⇒ ii) ergibt sich aus 2.34, da die Injektivität nach iii) erhalten bleibt.
ii) ⇒ i): Zerlege eine beliebige exakte Folge $(M_i, f_i)_{i \in \mathbb{Z}}$ für alle $i \in \mathbb{Z}$ in kurze exakte Folgen

$$0 \to \ker(f_i) \to M_i \to \mathrm{im}(f_i) = \ker(f_{i+1}) \to 0$$



und wende $\otimes_A M$ an. $\square_{2.35}$

2.36 **Proposition** (projektiv impliziert flach)

Sei A ein Ring. Jeder projektive (und insbesondere jeder freie) A-Modul M ist flach.

Beweis

Sei $\alpha : L' \hookrightarrow L$ eine injektive A-lineare Abbildung. Zu zeigen ist, dass die Abbildung

$$\mathrm{id}_M \otimes \alpha : M \otimes_A L' \to M \otimes_A L$$

injektiv ist.

1. Fall: M ist frei, also $M \cong A^{(I)} = \bigoplus_{i \in I} A$. Das Diagramm

$$\begin{array}{ccc} M \otimes_A L' & \longrightarrow & M \otimes_A L \\ \wr\downarrow & & \wr\downarrow \\ \bigoplus_{i\in I}(A \otimes_A L') & \longrightarrow & \bigoplus_{i\in I}(A \otimes_A L) \\ \wr\downarrow & & \wr\downarrow \\ \bigoplus_{i\in I} L' & \longrightarrow & \bigoplus_{i\in I} L \\ (l'_i)_{i\in I} & \longmapsto & (\alpha(l'_i))_{i\in I} \end{array}$$

   kommutiert, weil die senkrechten Isomorphismen natürlich sind. Außerdem ist die unterste Abbildung injektiv, weil α injektiv ist, und eine Abbildung in eine direkte Summe genau dann injektiv ist, wenn die Abbildung in die einzelnen Summanden injektiv ist. Also ist M flach.

2. Fall: M ist projektiv, also direkter Summand eines freien A-Moduls, das heißt es gibt einen A-Modul N mit $M + N \cong A^{(I)}$. Dann ist das Diagramm

$$\begin{array}{ccc} A^{(I)} \otimes_A L' & \hookrightarrow & A^{(I)} \otimes_A L \\ \wr\downarrow & & \wr\downarrow \\ (M \otimes_A L') \oplus (N \otimes_A L') & \longrightarrow & (M \otimes_A L') \oplus (N \otimes_A L') \\ (m \otimes l', n \otimes \tilde{l}') & \longmapsto & (m \otimes \alpha(l'), n \otimes \alpha(\tilde{l}')) \end{array}$$

   kommutativ und somit auch $m \otimes l' \mapsto m \otimes \alpha(l')$ injektiv, also M flach.

$\square_{2.36}$

2.37 Proposition

Seien A ein Ring und M ein A-Modul. Dann sind äquivalent:

i) M ist flach.

ii) Für jedes endlich erzeugte Ideal $\iota : I \hookrightarrow A$ von A ist die Abbildung

$$\iota \otimes \mathrm{id}_M : I \otimes_A M \hookrightarrow A \otimes_A M \underset{2.27\,\mathrm{iv})}{\cong} M$$

injektiv (und induziert damit einen A-linearen Isomorphismus $I \otimes_A M \xrightarrow{\sim} IM \subseteq M$, denn $\mathrm{im}\,(\iota \otimes \mathrm{id}_M) = IM$ ist klar).

Beweis

i) $\Rightarrow$ ii) ist klar, da ii) das Kriterium von 2.35 iv) verschärft.
ii) $\Rightarrow$ i) wird später bewiesen. $\square_{2.37}$

2.38 Korollar und Definition (torsionsfrei)

i) Seien A ein Ring, M ein flacher A-Modul und $a \in A$ kein Nullteiler.
Dann gilt $\{x \in M | ax = 0\} = \{0\}$ und man nennt M *torsionsfrei*.

ii) Seien A ein Hauptidealring und M ein A-Modul, sodass für alle $a \in A \setminus \{0\}$ gilt:

$$\{x \in M | ax = 0\} = \{0\} \tag{2.9}$$

Dann ist M ein flacher A-Modul.

Bemerkung

Es existieren Moduln über Integritätsringen, die (2.9) erfüllen, aber nicht flach sind.

Beweis

i) Die Abbildung

$$\begin{aligned} \cdot a : A &\hookrightarrow A \\ x &\mapsto ax \end{aligned}$$

ist offenbar A-linear und injektiv, da a kein Nullteiler ist.

Da M flach ist, ist auch die Abbildung $A \otimes_A M \overset{(\cdot a)\otimes \mathrm{id}_M}{\hookrightarrow} A \otimes_A M$ injektiv. Mit der Abbildung f aus 2.27 iv) kommutiert das Diagramm:

$$\begin{array}{ccc} A \otimes_A M & \xhookrightarrow{(\cdot a) \otimes \mathrm{id}_M} & A \otimes_A M \\ \wr \downarrow f & & \wr \downarrow f \\ M & \xhookrightarrow{\cdot a} & M \end{array}$$

Für $x \in M$ rechne:

$$f\left(((\cdot a) \otimes \mathrm{id})\left(f^{-1}(x)\right)\right) \overset{2.27}{=} f\left(((\cdot a) \otimes \mathrm{id})(1 \otimes x)\right) = f(a \otimes x) \overset{2.27}{=} ax$$

$\square_{\text{i)}}$

ii) Wegen 2.37 zeige:

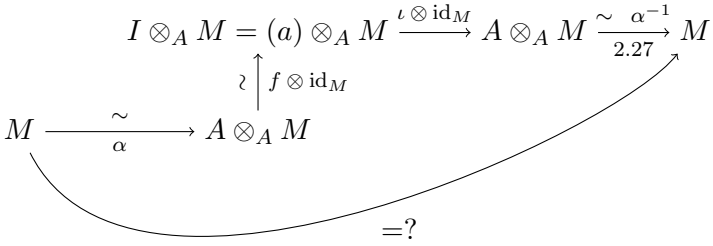
Für jedes (endlich erzeugte) Ideal $\iota : I \hookrightarrow A$ ist $\iota \otimes \mathrm{id}_M$ injektiv.

Für $I = (0)$ ist dies klar. Sei also $I \neq (0)$.

Da A ein Hauptidealring ist, gilt dann $I = (a)$ mit einem geeigneten $a \in A \setminus \{0\}$ und

$$\begin{aligned} f : A &\xrightarrow{\sim} (a) \\ x &\mapsto ax \end{aligned}$$

ist ein A-linearer Isomorphismus. Betrachte:



Rechne für $x \in M$:

$$\begin{aligned} \left(\alpha^{-1} \circ (\iota \otimes \mathrm{id}_M) \circ (f \otimes \mathrm{id}_M) \circ \alpha\right)(x) = \left(\alpha^{-1} \circ (\iota \otimes \mathrm{id}_M) \circ (f \otimes \mathrm{id}_M)\right)(1 \otimes x) = \\ = \alpha^{-1}\left(\underbrace{f(1)}_{=a} \otimes x\right) = ax \end{aligned}$$

Nach Voraussetzung ist $M \overset{\cdot a}{\hookrightarrow} M$ injektiv und es folgt, dass auch $\iota \otimes \mathrm{id}_M$ injektiv ist. $\square_{2.38}$

2.39 Lemma

Seien A ein Ring, M und N zwei A-Moduln und $\{n_i\}_{i \in I} \subseteq N$ ein Erzeugendensystem, das heißt:

$$N = \sum_{i \in I} An_i$$

Dann gelten:

i) Jedes $x \in M \otimes_A N$ schreibt sich als

$$x = \sum_{i \in I} m_i \otimes n_i$$

mit geeigneten $m_i \in M$, die fast alle Null sind.

ii) In der Situation von i) sind äquivalent:

a) $x = 0$

b) Es existieren Elemente $m'_j \in M$ für $j \in J$, die fast alle Null sind, und $a_{ij} \in A$ für $i \in I$ und $j \in J$, die fast alle Null sind, mit:

1. $m_i = \sum_{j \in J} a_{ij} m'_j$ für alle $i \in I$.
2. $0 = \sum_{i \in I} a_{ij} n_i$ für alle $j \in J$.

Beweis

i) Die eindeutige A-lineare Abbildung

$$\begin{aligned} \pi : A^{(I)} &\twoheadrightarrow N \\ \underset{i \in I}{\forall} \quad e_i &\mapsto n_i \end{aligned}$$

ist surjektiv. Nach 2.34 und 2.27 i) also auch:

$$\begin{array}{ccc} M \otimes_A A^{(I)} & \xrightarrow{\mathrm{id}_M \otimes \pi} & M \otimes_A N \\ \wr \downarrow & \nearrow & \\ \bigoplus_{i \in I} M & & \end{array}$$

f, 2.27 i)

Rechne für $(m_i)_{i \in I} \in \bigoplus_{i \in I} M$:

$$\left((\mathrm{id}_M \otimes \pi) \circ f^{-1}\right)\left((m_i)_{i \in I}\right) = (\mathrm{id}_M \otimes \pi)\left(\sum_{i \in I} m_i \otimes e_i\right) = \sum_{i \in I} m_i \otimes n_i$$

$\square_{\text{i)}}$

ii) „b) ⇒ a)“:

$$\begin{aligned} x = \sum_{i \in I} m_i \otimes n_i &\overset{1.}{=} \sum_{i \in I} \left(\sum_{j \in J} a_{ij} m'_j\right) \otimes n_i = \sum_{i \in I, j \in J} \left(a_{ij} m'_j\right) \otimes n_i = \\ &= \sum_{i \in I, j \in J} m'_j \otimes (a_{ij} n_i) = \sum_{j \in J} m'_j \otimes \underbrace{\left(\sum_{i \in I} a_{ij} n_i\right)}_{=0} \overset{2.}{=} 0 \end{aligned}$$

„a) ⇒ b)“: Betrachte den Spezialfall, dass $N = \bigoplus_{i \in I} An_i$ ist, das heißt, das Erzeugendensystem $\{n_i\}_{i \in I}$ ist sogar eine Basis. Dann folgt:

$$\begin{aligned} M \otimes_A N &\xrightarrow{\sim} \bigoplus_{i \in I} M \\ x = \sum_{i \in I} m_i \otimes n_i &\mapsto (m_i)_{i \in I} \end{aligned}$$

Aus $x = 0$ folgt für alle $i \in I$ schon $m_i = 0$.

Damit gilt b) für $m_i' := 0$ und $a_{ij} := 0$ für alle i,j.

Sei nun N beliebig.

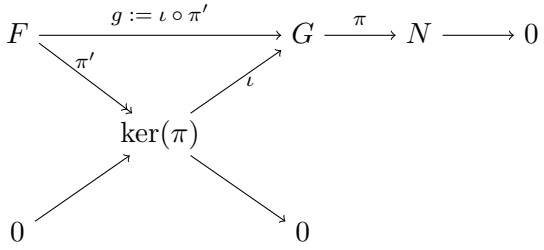
Behauptung Es existiert eine exakte Folge von A-Moduln

$$F \overset{g}{\to} G \overset{\pi}{\to} N \to 0$$

mit freien A-Moduln F und G.

Beweis Zunächst existiert ein freier A-Modul G mit $\pi : G \twoheadrightarrow N$, also ist $G \overset{\pi}{\to} N \to 0$ exakt. Dann existiert ein freier A-Modul F mit $\pi' : F \twoheadrightarrow \ker(\pi)$ und erhalte:

$$\mathscr{E} := (F \overset{g:=\iota\circ\pi'}{\to} G \overset{\pi}{\to} N \to 0)$$



Nach der Definition ist diese Folge exakt. $\square_{\text{Behauptung}}$

Wegen 2.34 ist dann auch

$$M \otimes_A \mathscr{E} = \left(M \otimes_A F \overset{\mathrm{id}\otimes g}{\to} M \otimes_A G \overset{\mathrm{id}\otimes\pi}{\to} M \otimes_A N \to 0\right)$$

exakt. Wähle $g_i \in G$ mit $\pi(g_i) = n_i$. Dann gilt für

$$y := \sum_{i\in I} m_i \otimes g_i \in M \otimes_A G$$

nun:

$$(\mathrm{id} \otimes \pi)(y) = \sum_{i\in I} m_i \otimes n_i = x = 0$$

Also ist $y \in \ker(\mathrm{id} \otimes \pi) = \mathrm{im}(\mathrm{id} \otimes g)$, das heißt

$$y = (\mathrm{id} \otimes g)\left(\sum_{j\in J} m_j' \otimes f_j\right) = \sum_{j\in J} m_j' \otimes g(f_j)$$

mit geeigneten $f_j \in F$ und $m_j' \in M$. Schreibe nun in G

$$g(f_j) = \sum_{i\in I} a_{ij} g_i$$

mit geeigneten $a_{ij} \in A$ und erhalte:

$$0 = y - y = \sum_{i\in I} m_i \otimes g_i - \sum_{j\in J} m_j' \otimes \left(\sum_{i\in I} a_{ij} g_i\right) =$$

$$= \sum_{i\in I} \left(m_i - \sum_{j\in J} a_{ij} m_j'\right) \otimes g_i \in M \otimes_A G$$

Da G frei ist, folgt aus dem Spezialfall:

1. Für alle $i \in I$ gilt:

$$m_i = \sum_{j \in J} a_{ij} m'_j$$

2. Für alle $j \in J$ gilt:

$$0 \overset{(\pi \circ g = 0)}{=} \pi\left(g\left(f_j\right)\right) = \pi\left(\sum_{i \in I} a_{ij} g_i\right) = \sum_{i \in I} a_{ij} \cdot \pi\left(g_i\right) = \sum_{i \in I} a_{ij} \cdot n_i$$

$\square_{\text{ii)}}$

2.40 Beispiel

i) Ist $N = A \cdot n$ durch ein Element n erzeugt und M beliebig, so schreibt sich jedes Element $x \in M \otimes_A N$ als $x = m \otimes n$ mit einem geeigneten $m \in M$ und es gilt:

$$x = 0 \quad \Leftrightarrow \quad \underset{a \in A, m' \in M}{\exists} : m = am' \wedge a \cdot n = 0$$

ii) Wähle in i) nun $A = k[t]$ für einen Körper k, $N = {k[t]}/{\left(t^2\right)} \ni n := \overline{t} \neq 0$ und zudem $M = {k[t]}/{(t)} \ni m := \overline{1} \neq 0$. Dann gilt:

$$x = m \otimes n = \overline{1} \otimes \overline{t} = \overline{1} \otimes \left(t \cdot \overline{1}\right) = t \cdot \left(\overline{1} \otimes \overline{1}\right) = \overline{t} \otimes \overline{1} = \overline{0} \otimes \overline{1} = 0$$

Aber die Bedingung aus i) gilt nicht. Man sieht, dass auf die Bedingung $N = An$ in i) nicht verzichtet werden kann.

2.41 Korollar (Kriterium für flach)

Seien A ein Ring und M ein A-Modul. Dann sind äquivalent:

i) M ist flach.

ii) Für jede Relation

$$0 = \sum_{i \in I} \alpha_i m_i \in M$$

mit $\alpha_i \in A$ und $m_i \in M$ existieren $m'_j \in M$ für $j \in J$ und $a_{ij} \in A$ für $i \in I$ und $j \in J$, sodass für alle $i \in I$ schon

$$m_i = \sum_{j \in J} a_{ij} m'_j$$

gilt und für alle $j \in J$:

$$\sum_{i \in I} a_{ij} \alpha_i = 0$$

Beweis

Dies folgt aus 2.37 und 2.39. $\square_{2.41}$

2.42 Beispiel und Definition (Torsionsuntermodul)

i) Seien A ein Integritätsring und M ein A-Modul. Dann ist

$$T(M) := \left\{ x \in M \,\middle|\, \exists_{a \in A \setminus \{0\}} : ax = 0 \right\} \subseteq M$$

ein A-Untermodul, *der Torsionsuntermodul von* M.

Ist $T(M) = \{0\}$, so heißt M *torsionsfrei*.

2.38 i) bedeutet also, dass über einem Integritätsring jeder flache Modul torsionsfrei ist.

ii) Vergleiche mit der Bemerkung zu 2.38:

Sei k ein Körper, dann ist $A := k[X,Y]$ ein Integritätsring, aber kein Hauptidealring.

Der Modul $M := (X,Y) \subseteq A$ ist ein torsionsfreier A-Modul, der nicht flach ist.

Beweis

Dass A ein Integritätsring ist, folgt aus der Gradformel für Polynome und daher gilt $T(A) = \{0\}$. Aus $M \subseteq A$ folgt $T(M) = \{0\}$.

Angenommen M wäre flach. Aus der A-linearen Relation

$$\underbrace{Y}_{=:\alpha_1} \cdot \underbrace{X}_{=:m_1} + \underbrace{(-X)}_{=:\alpha_2} \cdot \underbrace{Y}_{=:m_2} = 0$$

in M würde dann mit 2.41 „i) $\Rightarrow$ ii)“ folgen, dass es ein $n \in \mathbb{N}$, $m'_1, \ldots, m'_n \in M$ und $\alpha_{ij} \in A$ für $1 \leq i,j \leq n$ gibt, mit

$$X = \sum_{j=1}^{n} a_{1j} m'_j \qquad\qquad Y = \sum_{j=1}^{n} a_{2j} m'_j$$

und für alle $1 \leq j \leq n$:

$$0 = \sum_{i=1}^{2} a_{ij} \alpha_j = a_{1j} Y - a_{2j} X$$

Damit würde für alle $1 \leq j \leq n$ in A folgen:

$$X \,|\, a_{2j} X = a_{1j} Y$$

Wegen $X \nmid Y$ und weil X ein Primelement ist, folgt für alle $1 \leq j \leq n$ schon

$$a_{ij} = X \cdot a'_{1j}$$

mit geeigneten $a'_{ij} \in A$.

Zusammen ergibt das:

$$X = \sum_{j=1}^{n} X \cdot a'_{1j} \cdot m'_j$$

Wegen $0 \neq X \in A$ und $T(M) = \{0\}$ folgt:

$$1 = \sum_{j=1}^{m} \underbrace{a'_{ij}}_{\in A} \cdot \underbrace{m'_j}_{\in M} \in M = (X,Y) \subsetneq A$$

Dies ist ein Widerspruch. $\square_{\text{ii)}}$

2.43 **Definition** (Algebra)

Sei A ein Ring.

i) Eine *A-Algebra* ist ein Tupel (B,β), wobei B ein Ring und $\beta : A \to B$ ein Ringhomomorphismus ist.

ii) Sind (B,β) und (C,γ) zwei A-Algebren, so ist ein *A-Algebrenhomomorphismus (von B nach C)* eine Abbildung $f : B \to C$, die ein Ringhomomorphismus ist und $f \circ \beta = \gamma$ erfüllt.

iii) Ist für eine A-Algebra (B,β) die Abbildung β aus dem Kontext klar, so lässt man sie in der Notation fort.

iv) Eine A-Algebra B heißt:

   a) *endlich* $:\Leftrightarrow$ B als A-Modul ist endlich erzeugt.
   (Ist (B,β) eine A-Algebra, so ist B ein A-Modul vermöge $a \cdot b := \beta(a)\, b$ für alle $a \in A$ und $b \in B$.)

   b) *endlich erzeugt* $:\Leftrightarrow$ Es gibt ein $n \in \mathbb{N}$ und einen surjektiven A-Algebrenhomomorphismus $A[X_1,\ldots,X_n] \twoheadrightarrow B$, das heißt es gibt ein $n \in \mathbb{N}$ und $b_1,\ldots,b_n \in B$ so, dass sich jedes $b \in B$ schreibt als

$$b = \sum_{i_1,\ldots,i_n \in \mathbb{N}} a_{i_1\ldots i_n} b_1^{i_1} \cdot \ldots \cdot b_n^{i_n}$$

   mit geeigneten $a_{i_1\ldots i_n} \in A$, die fast alle Null sind.

2.44 **Beispiel**

i) Jede endliche Algebra ist endlich erzeugt, denn jede Linearkombination ist ein Polynom vom Grad 1.

ii) Die A-Algebra $A[X]$ ist endlich erzeugt, aber nicht endlich, da alle Potenzen von X schon A-linear unabhängig sind.

2.45 **Konstruktion** (Multiplikation im Tensorprodukt)

Seien A ein Ring und (B,β) und (C,γ) zwei A-Algebren, so setze $D := B \otimes_A C$. Die Abbildung

$$\begin{aligned}(B \times C) \times (B \times C) &\to B \times C \\ \big((b,c)\,,\big(b',c'\big)\big) &\mapsto \big(bb',cc'\big)\end{aligned}$$

ist A-*multilinear*, das heißt linear in jedem Argument, und faktorisiert also über eine A-lineare Abbildung

$$D \otimes_A D \overset{\tilde{\mu}}{\to} D$$

und

$$\mu := \Big(D \times D \underset{2.25}{\overset{\tau}{\to}} D \otimes_A D \overset{\tilde{\mu}}{\to} D\Big)$$

ist A-bilinear, sodass für alle $b,b' \in B$ und $c,c' \in C$ gilt:

$$\mu\left(b \otimes c,b' \otimes c'\right) = \big(bb'\big) \otimes \big(cc'\big)$$

2.46 **Satz**

In der Situation von 2.45 gelten:

i) Das Tupel $(D, + ,\mu,0 \otimes 0,1 \otimes 1)$ ist ein Ring.

ii) Die Abbildungen

$$\begin{aligned}\iota_B : B &\to D \\ b &\mapsto b \otimes 1\end{aligned}$$

und

$$\begin{aligned}\iota_C : C &\to D \\ c &\mapsto 1 \otimes c\end{aligned}$$

sind Ringhomomorphismen und es gilt:

$$\iota_B \circ \beta = \iota_C \circ \gamma$$

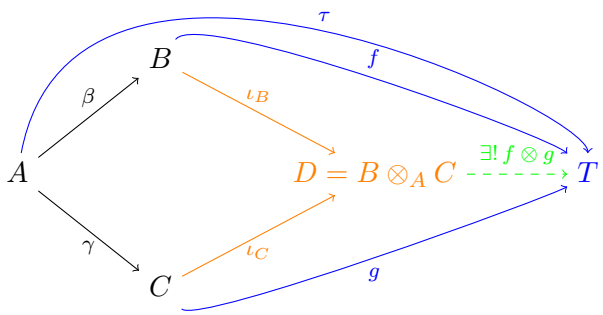
iii) Sind (T,τ) eine A-Algebra und $f : B \to T$ und $g : C \to T$ zwei A-Algebrenhomomorphismen, so existiert genau ein A-Algebrenhomomorphismus

$$f \otimes g : D = B \otimes_A C \to T$$

mit:

$$(f \otimes g) \circ \iota_B = f \qquad\qquad (f \otimes g) \circ \iota_C = g$$

Skizze



Beweis

i) D ist ein A-Modul und somit insbesondere $(D,+)$ eine abelsche Gruppe. Dass $0 \otimes 0$ das neutrale Element der Addition ist, ist klar.

Da für alle $b,b',b'' \in B$ und $c,c',c'' \in C$ nun

$$\begin{aligned}\mu\left(\mu\left(b \otimes c, b' \otimes c'\right), b'' \otimes c''\right) &= \mu\left(\left(bb'\right) \otimes \left(cc'\right), b'' \otimes c''\right) = \left(bb'b''\right) \otimes \left(cc'c''\right) = \\ &= \mu\left(b \otimes c, \left(b'b''\right) \otimes \left(c'c''\right)\right) = \mu\left(b \otimes c, \mu\left(b' \otimes c', b'' \otimes c''\right)\right)\end{aligned}$$

gilt, ist μ assoziativ, und wegen

$$\mu\left(b \otimes c, b' \otimes c'\right) = \left(bb'\right) \otimes \left(cc'\right) = \left(b'b\right) \otimes \left(c'c\right) = \mu\left(b' \otimes c', b \otimes c\right)$$

ist μ kommutativ. Weiter gilt:

$$\mu\left(b \otimes c, 1 \otimes 1\right) = \left(b \cdot 1\right) \otimes \left(c \cdot 1\right) = b \otimes c$$

Also ist $1 \otimes 1$ das neutrale Element der Multiplikation. Die Distributivgesetze folgen direkt aus der A-Bilinearität von μ. $\square_{\text{i)}}$

ii) Dass ι_B und ι_C Ringhomomorphismen sind, ist klar.

Für $a \in A$ rechne in $D = B \otimes_A C$:

$$\begin{aligned}\left(\iota_B \circ \beta\right)(a) = \iota_B\left(\beta\left(a\right)\right) = \beta\left(a\right) \otimes 1 &\overset{\substack{A\text{-Modulstruktur} \\ \text{auf } B}}{=} \left(a \cdot 1\right) \otimes 1 = \\ &\overset{\substack{\text{Bilinearität} \\ \text{des Tensorprodukts}}}{=} 1 \otimes \left(a \cdot 1\right) = \overset{\substack{A\text{-Modulstruktur} \\ \text{auf } C}}{=} 1 \otimes \gamma\left(a\right)\end{aligned}$$

$\square_{\text{ii)}}$

iii) Eindeutigkeit:

Sei $x \in D$ beliebig, so gibt es ein geeignetes $n \in \mathbb{N}$ und geeignete $b_i \in B$ und $c_i \in C$ mit:

$$x = \sum_{i=1}^{n} b_i \otimes c_i$$

Es folgt:

$$(f \otimes g)(x) = \sum_{i=1}^{n} (f \otimes g)\left(\underbrace{(b_i \otimes 1)}_{=\iota_B(b_i)} \cdot \underbrace{(1 \otimes c_i)}_{\iota_C(c_i)} \right) =$$

$$= \sum_{i=1}^{n} \underbrace{(f \otimes g)(\iota_B(b_i))}_{\overset{\text{Vor.}}{=} f(b_i)} \cdot \underbrace{(f \otimes g)(\iota_C(c_i))}_{\overset{\text{Vor.}}{=} g(c_i)} = \sum_{i=1}^{n} f(b_i) \cdot g(c_i)$$

Existenz:

Die Abbildung

$$\begin{aligned} \Phi : B \times C &\to T \\ (b,c) &\mapsto f(b) \cdot g(c) \end{aligned}$$

ist A-bilinear, denn zum Beispiel gilt für alle $a \in A$, $b \in B$ und $c \in C$ in T:

$$\Phi(ab,c) = f(ab) \cdot g(c) = f(\beta(a)\, b) \cdot g(c) =$$

$$= \underbrace{f(\beta(a))}_{\overset{\text{Vor.}}{=} \tau(a)} \cdot \underbrace{f(b) \cdot g(c)}_{=\Phi(b,c)} \overset{\substack{A\text{-Modulstruktur} \\ \text{auf } T}}{=} a \cdot \Phi(b,c)$$

Also existiert eine A-lineare Abbildung

$$f \otimes g : D \to T$$

mit

$$(f \otimes g)(b \otimes c) = f(b) \cdot g(c)$$

für alle $b \in B$ und $c \in C$.

Man sieht leicht, dass $f \otimes g$ ein Ringhomomorphismus ist und rechnet dann zum Beispiel für $b \in B$ in T:

$$((f \otimes g) \circ \iota_B)(b) = (f \otimes g)(b \otimes 1) = f(b) \cdot \underbrace{g(1)}_{=1} = f(b)$$

Ebenso gilt für $c \in C$ in T:

$$((f \otimes g) \circ \iota_C)(c) = (f \otimes g)(1 \otimes c) = \underbrace{f(1)}_{=1} \cdot g(c) = g(c)$$

Insbesondere ist damit

$$f \otimes g : (D, \iota_B \circ \beta = \iota_C \circ \gamma) \to (T, \tau)$$

ein A-Algebrenhomomorphismus. $\square_{\text{iii)}}$

2.47 Beispiel und Definition (Basiswechsel)

i) Ist A ein Ring, so besteht eine Isomorphie von A-Algebren:

$$\begin{array}{rcc} & A[X,Y] \overset{\cong}{=} A[X] \otimes_A A[Y] & \\ A\text{-Modul-Basen: } & \left\{X^i Y^j\right\} & \left\{X^i\right\} \cdot \left\{Y^j\right\} \end{array}$$

ii) Für jeden Ring A besteht eine in A natürliche Isomorphie von A-Algebren

$$\varphi : A[X] \overset{\sim}{\to} A \otimes_{\mathbb{Z}} \mathbb{Z}[X]$$

mit

$$\varphi(a) = a \otimes 1$$

für alle $a \in A$.

iii) Sind $f : A \to B$ ein Ringhomomorphismus und C eine endliche (beziehungsweise endlich erzeugte) A-Algebra, so ist die B-Algebra $B \otimes_A C$ endlich (beziehungsweise endlich erzeugt).

$$\begin{array}{ccc} A & \longrightarrow & C \\ {\scriptstyle f}\downarrow & & \downarrow \\ B & \longrightarrow & B \otimes_A C \end{array}$$

$B \otimes_A C$ nennt man *den Basiswechsel der A-Algebra C entlang f.*

Beweis

i) Die Inklusionen

$$A[X], A[Y] \hookrightarrow A[X,Y] = A[X][Y] = A[Y][X]$$

sind A-Algebrenhomomorphismen.

Nach 2.46 gibt es also genau einen A-Algebrenhomomorphismus

$$F : A[X] \otimes_A A[Y] \to A[X,Y]$$

mit

$$F(f(X) \otimes g(Y)) = f(X) \cdot g(Y)$$

für alle $f \in A[X]$ und $g \in A[Y]$.

Wegen der universellen Eigenschaft der A-Algebra $A[X,Y]$ existiert genau ein A-Algebrenhomomorphismus

$$G : A[X,Y] \to A[X] \otimes_A A[Y]$$

mit folgenden Bildern der Variablen:

$$G(X) = X \otimes 1 \qquad\qquad G(Y) = 1 \otimes Y$$

Man sieht leicht $F = G^{-1}$. Zum Beispiel gilt:

$$F \circ G \overset{(!)}{=} \mathrm{id}_{A[X,Y]}$$

Dazu ist zu prüfen, dass

$$(F \circ G)(X) = X$$

und

$$(F \circ G)(Y) = Y$$

gelten:

$$(F \circ G)(X) = F(X \otimes 1) = X \cdot 1 = X$$
$$(F \circ G)(Y) = F(1 \otimes Y) = 1 \cdot Y = Y$$

$\square_{\text{i)}}$

ii) Da $X \in A[X]$ die A-Algebra $A[X]$ erzeugt, ist durch

$$\alpha(X) = 1 \otimes X$$

ein eindeutiger$A$-Algebrenhomomorphismus definiert. Jedes $f(X) \in A[X]$ lässt sich mit $n \in \mathbb{N}$ und $a_k \in A$ für $k \in \{0,1,\ldots,n\}$ als

$$f(X) = \sum_{k=0}^{n} a_k X^k$$

darstellen. Für dieses gilt:

$$\alpha(f(X)) = \alpha\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} a_k \cdot (\alpha(X))^k = \sum_{k=0}^{n} a_k \cdot (1 \otimes X)^k =$$
$$= \sum_{k=0}^{n} a_k \cdot \left(1 \otimes X^k\right) = \sum_{k=0}^{n} a_k \otimes X^k$$

Sei $v \in A \otimes_{\mathbb{Z}} \mathbb{Z}[X]$. Dann kann man es mit $n \in \mathbb{N}$, $a_k \in A$ und $f_k(X) \in \mathbb{Z}[X]$ für $k \in \{0,\ldots,n\}$ darstellen als:

$$v = \sum_{k=0}^{n} a_k \otimes f_k(X)$$

$f_k(X)$ besitzt mit $m_k \in \mathbb{N}$ und $z_{k,l} \in \mathbb{Z}$ eine Darstellung:

$$f_k(X) = \sum_{l=0}^{m_k} z_{k,l} X^l$$

Wegen

$$A \ni z_{k,l} \cdot a_k := \operatorname{sgn}(z_{k,l}) \cdot \sum_{j=1}^{|z_{k,l}|} a_k = \begin{cases} \sum_{j=1}^{z_{k,l}} a_k & \text{falls } z_{k,l} > 0 \\ 0 & \text{falls } z_{k,l} = 0 \\ -\sum_{j=1}^{z_{k,l}} a_k & \text{falls } z_{k,l} < 0 \end{cases}$$

folgt aus der $\mathbb{Z}$-Bilinearität des Tensorprodukts:

$$v = \sum_{k=0}^{n} a_k \otimes \left(\sum_{l=0}^{m_k} z_{k,l} X^l \right) = \sum_{k=0}^{n} \sum_{l=0}^{m_k} z_{k,l} \cdot \left(a_k \otimes X^l \right) = \sum_{k=0}^{n} \sum_{l=0}^{m_k} z_{k,l} \cdot a_k \cdot (1 \otimes X)^l$$

Daher ist $1 \otimes X \in A \otimes_{\mathbb{Z}} \mathbb{Z}[X]$ ein Erzeuger der A-Algebra $A \otimes_{\mathbb{Z}} \mathbb{Z}[X]$. Deswegen ist durch

$$\beta(1 \otimes X) = X$$

ein eindeutiger$A$-Algebrenhomomorphismus definiert $\beta : A \otimes_{\mathbb{Z}} \mathbb{Z}[X] \to A[X]$ definiert. Wegen

$$\begin{aligned} (\beta \circ \alpha)(X) &= \beta(1 \otimes X) = X \\ (\alpha \circ \beta)(1 \otimes X) &= \alpha(X) = 1 \otimes X \end{aligned}$$

ist β invers zu α und somit α ein Isomorphismus.
Die Natürlichkeit im Ring A bedeutet, dass für einen Ring B mit einem Ringhomomorphismus $g : A \to B$ das Diagramm

$$\begin{array}{ccc} A[X] & \xrightarrow[\alpha_A]{\sim} & A \otimes_{\mathbb{Z}} \mathbb{Z}[X] \\ \downarrow{\scriptstyle \tilde{g}} & & \downarrow{\scriptstyle g \otimes \mathrm{id}} \\ B[X] & \xrightarrow[\alpha_B]{\sim} & B \otimes_{\mathbb{Z}} \mathbb{Z}[X] \end{array}$$

kommutiert. Dabei sind

$$\begin{aligned} \tilde{g} : A[X] &\to g_*(B[X]) \\ \sum_{i=0}^{n} a_i X^i &\mapsto \sum_{i=0}^{n} g(a_i) X^i \end{aligned}$$

und

$$\begin{aligned} g \otimes \mathrm{id} : A \otimes_{\mathbb{Z}} \mathbb{Z}[X] &\to g_*(B \otimes_{\mathbb{Z}} \mathbb{Z}[X]) \\ \sum_{i=0}^{n} a_i \otimes f_i(X) &\mapsto \sum_{i=0}^{n} g(a_i) \otimes f_i(X) \end{aligned}$$

zwei A-Algebrenhomomorphismen. Nun gilt aber für den Erzeuger X von $A[X]$:

$$\begin{aligned} ((g \otimes \mathrm{id}) \circ \alpha_A)(X) = (g \otimes \mathrm{id})(1 \otimes X) = g(1) \otimes X = 1 \otimes X = \\ = \alpha_B(X) = \alpha_B(\tilde{g}(X)) = (\alpha_B \circ \tilde{g})(X) \end{aligned}$$

Also kommutiert das Diagramm. $\square_{\text{ii)}}$

iii) Sei C endlich, das heißt der A-Modul C ist endlich erzeugt, also gibt es ein $n \in \mathbb{N}$ und $c_1, \ldots, c_n \in C$, sodass für jedes Element $c \in C$ mit geeigneten $a_k \in A$ gilt:

$$c = \sum_{k=1}^{n} a_k c_k$$

Jedes Element $v \in B \otimes_A C$ lässt sich mit geeigneten $b_l \in B$ und $c_l \in C$ darstellen als:

$$\begin{aligned} v &= \sum_{l=1}^{m} b_l \otimes c_l = \sum_{l=1}^{m} b_l \otimes \left(\sum_{k=1}^{n} a_{l,k} c_k \right) = \sum_{l=1}^{m} \sum_{k=1}^{n} a_{l,k} \left(b_l \otimes c_k \right) = \\ &= \sum_{l=1}^{m} \sum_{k=1}^{n} a_{l,k} \cdot b_l \left(1 \otimes c_k \right) = \sum_{k=1}^{n} \underbrace{\sum_{l=1}^{m} f\left(a_{l,k} \right) b_l}_{\in B} \left(1 \otimes c_k \right) \end{aligned}$$

Also ist v eine Linearkombination der $1 \otimes c_k$ und somit $B \otimes_A C$ endlich.
Sei C endlich erzeugt, das heißt es gibt ein $n \in \mathbb{N}$ und einen surjektiven A-Algebrenhomomorphismus $f : A\left[X_1, \ldots, X_n\right] \to C$.
Dann ist der durch

$$g\left(X_i\right) = 1 \otimes f\left(X_i\right)$$

eindeutig definierte B-Algebrenhomomorphismus

$$g : B\left[X_1, \ldots, X_n\right] \to B \otimes_A C$$

ebenfalls surjektiv, denn für ein $v \in B \otimes_A C$ gilt mit geeigneten $\alpha_l \in A\left[X_1, \ldots, X_n\right]$:

$$v = \sum_{l=1}^{m} b_l \otimes c_l = \sum_{l=1}^{m} b_l \otimes f\left(\alpha_l\right) = \sum_{l=1}^{m} b_l \cdot \left(1 \otimes f\left(\alpha_l\right)\right) = \sum_{l=1}^{m} b_l \cdot g\left(\alpha_l\right) = g\left(\sum_{l=1}^{m} b_l \alpha_l \right)$$

Daher ist $B \otimes_A C$ endlich erzeugt. $\square_{\text{iii)}}$

2.48 Lemma

Seien A ein Ring, $I \subseteq A$ ein Ideal und M ein A-Modul.
Dann ist die Abbildung

$$\varphi^{-1} : {}^{A}\!/_{I} \otimes_A M \xrightarrow{\sim} {}^{M}\!/_{IM}$$

ein in dem A-Modul M natürlicher Isomorphismus.

Beweis

Betrachte die kurze exakte Folge:

$$0 \to I \xhookrightarrow{\iota} A \overset{\pi}{\twoheadrightarrow} {}^{A}\!/_{I} \to 0$$

Aufgrund der Rechtsexaktheit des Tensorprodukts ist auch die Folge

$$I \otimes_A M \overset{\iota \otimes \mathrm{id}}{\to} A \otimes_A M \overset{\pi \otimes \mathrm{id}}{\to} {}^{A}\!/_{I} \otimes_A M \to 0$$

exakt, also insbesondere:

$$\ker(\pi \otimes \mathrm{id}) = \mathrm{im}(\iota \otimes \mathrm{id})$$

Nun ist aber

$$\begin{aligned} \alpha : M &\xrightarrow{\sim} A \otimes_A M \\ m &\mapsto 1 \otimes m \end{aligned}$$

ein Isomorphismus mit der Umkehrabbildung:

$$\begin{aligned} \alpha^{-1} : A \otimes_A M &\xrightarrow{\sim} M \\ a \otimes m &\mapsto a \cdot m \end{aligned}$$

Betrachte nun

$$I \otimes_A M \overset{\iota\otimes\mathrm{id}}{\to} A \otimes_A M \underset{\alpha^{-1}}{\overset{\sim}{\to}} M \underset{\alpha}{\overset{\sim}{\to}} A \otimes_A M \overset{\pi\otimes\mathrm{id}}{\twoheadrightarrow} {}^{A}\!/_{I} \otimes_A M \to 0$$

also:

$$I \otimes_A M \overset{f:=\alpha^{-1}\circ(\iota\otimes\mathrm{id})}{\to} M \overset{g:=(\pi\otimes\mathrm{id})\circ\alpha}{\twoheadrightarrow} {}^{A}\!/_{I} \otimes_A M \to 0$$

Da α ein Isomorphismus ist, gilt noch immer:

$$\ker(g) = \mathrm{im}(f) = f(I \otimes_A M) = IM$$

Da g surjektiv ist folgt damit aus dem Homomorphiesatz, dass

$$\begin{aligned} \varphi : {}^{M}\!/_{IM} &\xrightarrow{\sim} {}^{A}\!/_{I} \otimes_A M \\ m + IM &\mapsto g(m) = (1 + I) \otimes_A m \end{aligned}$$

ein Isomorphismus von A-Moduln ist.
Sei nun $f : M \to N$ eine A-lineare Abbildung, so kommutiert das Diagramm

$$\begin{array}{ccc} {}^{A}\!/_{I} \otimes_A M & \xrightarrow{\varphi_M} & {}^{M}\!/_{IM} \\ {\scriptstyle \mathrm{id}\otimes f}\downarrow & & \downarrow{\scriptstyle \overline{f}} \\ {}^{A}\!/_{I} \otimes_A N & \xrightarrow{\varphi_N} & {}^{N}\!/_{IN} \end{array}$$

wegen:

$$\begin{array}{ccc} (a + I) \otimes m & \xmapsto{\varphi_M} & am + IM \\ {\scriptstyle \mathrm{id}\otimes f}\downarrow & & \downarrow{\scriptstyle \overline{f}} \\ (a + I) \otimes f(m) & \xmapsto{\varphi_N} & a \cdot f(m) + IN \end{array}$$

Also ist die Isomorphie natürlich. $\square_{2.48}$

2.49 **Beispiel** (Die Fasern von $\operatorname{Spec}(\mathbb{Z}[\mathbf{i}]) \to \operatorname{Spec}(\mathbb{Z})$)

Vergleiche mit 1.36 v).

$$\begin{array}{ccccccccc}
\operatorname{Spec}(\mathbb{Z}[\mathbf{i}]) \setminus \{0\}: & (1+\mathbf{i}) & (3) & (1+2\mathbf{i}, 1-2\mathbf{i}) & (7) & (11) & (3+2\mathbf{i}), (3-2\mathbf{i}) \\
\pi \downarrow \ \mathfrak{p} \mapsto (\mathfrak{p} \cap \mathbb{Z}) & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\operatorname{Spec}(\mathbb{Z}) \setminus \{0\}: & (2) & (3) & (5) & (7) & (11) & (13)
\end{array}$$

Es gilt

$$(\mathbb{Z} \hookrightarrow \mathbb{Z}[\mathbf{i}])^* (\mathfrak{p}) = \mathfrak{p} \cap \mathbb{Z}$$

und:

$$\left|\pi^{-1}((p))\right| = \begin{cases} 1 & \text{falls } p = 2 \text{ oder } p \equiv 3 \mod 4 \\ 2 & \text{falls } p \equiv 1 \mod 4 \end{cases}$$

Genauer ist die Menge $\pi^{-1}((p))$ sogar das Spektrum eines Ringes, nämlich

$$\pi^{-1}((p)) = \operatorname{Spec}(\mathbb{Z}[\mathbf{i}] \otimes_{\mathbb{Z}} \mathbb{F}_p)$$

und für die $\mathbb{F}_p$-Algebra

$$\mathbb{F}_p \to \mathbb{Z}[\mathbf{i}] \otimes_{\mathbb{Z}} \mathbb{F}_p$$

kommutiert das Diagramm

$$\begin{array}{ccc}
\mathbb{Z} & \longrightarrow & \mathbb{Z}[\mathbf{i}] \\
\downarrow & & \downarrow \\
\mathbb{Z}/(p) = \mathbb{F}_p & \longrightarrow & \mathbb{Z}[\mathbf{i}] \otimes_{\mathbb{Z}} \mathbb{F}_p
\end{array}$$

und es gilt:

$$\begin{aligned}
\mathbb{Z}[\mathbf{i}] \otimes_{\mathbb{Z}} \mathbb{F}_p &\cong \mathbb{Z}[X]/(X^2+1) \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \underset{2.48}{\cong} \mathbb{Z}[X]/(p, X^2+1) \cong \\
&\cong \mathbb{F}_p[X]/(X^2+1) \underset{(*)}{\cong} \begin{cases} \mathbb{F}_2[X]/\left((X+1)^2\right) & ;\ p = 2 \\ \mathbb{F}_p \times \mathbb{F}_p & ;\ p \equiv 1 \mod 4 \\ \mathbb{F}_{p^2} & ;\ p = 3 \mod 4 \end{cases}
\end{aligned}$$

Denn die Zerlegung in irreduzible Faktoren ist gegeben durch

$$\mathbb{F}_p[X] \ni X^2 + 1 = \begin{cases} (X+1)^2 & ;\ p = 2 \\ (X-\alpha)(X+\alpha) = X^2 - \alpha^2 & ;\ p \equiv 1 \mod 4,\ \left(\alpha \in \mathbb{F}_p^* \text{ geeignet}\right) \\ X^2 + 1 & ;\ p \equiv 3 \mod 4 \end{cases}$$

Dann folgt $(*)$ im Fall $p \equiv 1 \mod 4$ aus dem Chinesischen Restsatz 1.35.

3 Lokalisierung

3.1 **Satz und Definition** (multiplikativ abgeschlossen, Quotientenring)

i) Seien $f : A \to B$ ein Ringhomomorphismus und $S := f^{-1}(B^*)$. Dann gelten:

   a) $1 \in S$
   b) Für alle $s,t \in S$ gilt $st \in S$.

   Eine Teilmenge $S \subseteq A$ mit den Eigenschaften a) und b) heißt *multiplikativ abgeschlossen.*

ii) Seien A ein Ring und $S \subseteq A$ multiplikativ abgeschlossen. Dann existiert eine bis auf eindeutige Isomorphie eindeutige A-Algebra

$$f : A \to S^{-1}A$$

   so, dass für alle A-Algebren $g : A \to B$ äquivalent sind:

   a) $g(S) \subseteq B^*$
   b) Es existiert genau ein A-Algebrenhomomorphismus $\varphi : S^{-1}A \to B$.

$$\begin{array}{ccc} S \subseteq A & \xrightarrow{\ g\ } & B \\ {\scriptstyle f}\big\downarrow & \nearrow_{\exists!\varphi} & \\ S^{-1}A & & \end{array} \quad \Leftrightarrow \quad g(S) \subseteq B^*$$

   Dabei gilt:

$$f(S) \subseteq \left(S^{-1}A\right)^*$$

   Die A-Algebra $\left(A \xrightarrow{f}\right) S^{-1}A$ heißt *der Quotientenring von A bezüglich S.*

Beweis

i) a) Wegen $f(1) = 1 \in B^*$ ist $1 \in S$.
   b) Seien $s,t \in S$, also $f(s), f(t) \in B^*$, dann folgt nach 1.13:

$$B^* \ni f(s) \cdot f(t) = f(st)$$

   Also ist $st \in S$.

ii) Konstruktion:

Definiere auf der Menge $A \times S$ die Relation:

$$(a,s) \sim (b,t) \quad :\Leftrightarrow \quad \underset{u \in S}{\exists} : u\,(at - bs) = 0 \in A \tag{3.1}$$

Man prüft, dass $\sim$ eine Äquivalenzrelation ist und schreibt:

$$\frac{a}{s} := [(a,s)] \in {}^{A \times S}\!/_{\sim} =: S^{-1}A$$

Man setzt in $S^{-1}A$

$$0 := \frac{0}{1} \qquad\qquad 1 := \frac{1}{1}$$

und für alle $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$:

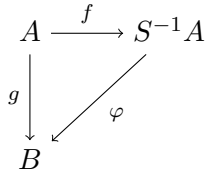
$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

Man prüft, dass $+$ und $\cdot$ wohldefiniert sind, $\left(S^{-1}A, +, \cdot, 0, 1\right)$ ein kommutativer Ring ist und

$$f : A \to S^{-1}A$$
$$a \mapsto \frac{a}{1}$$

ein Ringhomomorphismus ist.

„a) $\Rightarrow$ b)“: Zeige, dass genau ein Ringhomomorphismus $\varphi : S^{-1}A \to B$ existiert, sodass das Diagramm



kommutiert.

Eindeutigkeit:

Für alle $a \in A$ und $s \in S$ rechne:

$$\varphi\left(\frac{a}{s}\right) = \varphi\left(\frac{a}{1} \cdot \left(\frac{s}{1}\right)^{-1}\right) = \varphi\left(f\,(a) \cdot f\,(s)^{-1}\right) = \varphi\,(f\,(a)) \cdot \varphi\,(f\,(s))^{-1} = g\,(a) \cdot g\,(s)^{-1}$$

Existenz:

Für ein beliebiges $\frac{a}{s} \in S^{-1}A$ setze:

$$\varphi\left(\frac{a}{s}\right) := g\,(a) \cdot g\,(s)^{-1}$$

Beachte, dass nach Voraussetzung $g(S) \subseteq B^*$ ist.

Man prüft, dass φ wohldefiniert und ein Ringhomomorphismus ist. Dann folgt für alle $a \in A$:

$$\varphi(f(a)) = \varphi\left(\frac{a}{1}\right) = g(a) \cdot \underbrace{g(1)^{-1}}_{=1} = g(a)$$

$\square_{\text{a)} \Rightarrow \text{b)}}$

„b) $\Rightarrow$ a)“: Für alle $s \in S$ gilt in $S^{-1}A$:

$$f(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1} = 1$$

Also gilt $f(S) \subseteq \left(S^{-1}A\right)^*$ und es folgt:

$$g(S) \overset{\text{b)}}{=} \varphi(f(S)) \subseteq \varphi\left(\left(S^{-1}A\right)^*\right) \subseteq B^*$$

$\square_{\text{b)} \Rightarrow \text{a)}}$

Sei nun $\tilde{f} : A \to \tilde{A}$ eine weitere A-Algebra neben $f : A \to S^{-1}A$, für die gilt:

Für alle A-Algebren $g : A \to B$ sind äquivalent:

a') $g(S) \subseteq B^*$

b') Es existiert genau ein A-Algebrenhomomorphismus $\varphi : \tilde{A} \to B$.

Behauptung Es existiert genau ein A-Algebrenisomorphismus $\alpha : S^{-1}A \xrightarrow{\sim} \tilde{A}$.

Beweis Da $\mathrm{id}_{\tilde{A}}$ ein A-Algebrenhomomorphismus ist, folgt aus „b') $\Rightarrow$ a')“ für $B = \tilde{A}$, dass $\tilde{f}(S) \subseteq \left(\tilde{A}\right)^*$ gilt. Damit folgt aus „a) $\Rightarrow$ b)“, dass genau ein A-Algebrenhomomorphismus $\alpha : S^{-1}A \to \tilde{A}$ existiert. $\square_{\text{Behauptung}}$

Analog existiert genau ein A-Algebrenhomomorphismus $\beta : \tilde{A} \to S^{-1}A$.

Die Komposition $\beta \circ \alpha : S^{-1}A \to S^{-1}A$ ist ein A-Algebrenhomomorphismus.

Wegen „a) $\Rightarrow$ b)“ für $B := S^{-1}A$ existiert aber genau ein A-Algebrenhomomorphismus $S^{-1}A \to S^{-1}A$. Da $\mathrm{id}_{S^{-1}A}$ ein solcher ist, folgt $\beta \circ \alpha = \mathrm{id}_{S^{-1}A}$. Analog folgt $\alpha \circ \beta = \mathrm{id}_{\tilde{A}}$.

$\square_{3.1}$

3.2 Bemerkung

Seien A ein Ring, $S \subseteq A$ multiplikativ abgeschlossen und für alle $s \in S$ sei X_s eine Variable. Dann existiert genau ein A-Algebrenhomomorphismus

$$\alpha : S^{-1}A \to \tilde{A} := A\left[X_s \middle| s \in S\right] \Big/ I := \left(s \cdot X_s - 1 \middle| s \in S\right)$$

und α ist ein Isomorphismus.

Beweis

Die universelle Eigenschaft der A-Algebra $f : A \to S^{-1}A$ ist:
Für alle A-Algebren $g : A \to B$ ist äquivalent:

a) $g(S) \subseteq B^*$

b) Es existiert genau ein A-Algebrenhomomorphismus $\varphi : S^{-1}A \to B$ mit $g = \varphi \circ f$.

Zeige nun, dass auch die A-Algebra

$$\begin{aligned} \tilde{f} : A &\to \tilde{A} \\ a &\mapsto \overline{a} = a + I \end{aligned}$$

diese universelle Eigenschaft erfüllt. Sei also $g : A \to B$ eine A-Algebra.
„a) ⇒ b)“: Es gelte $g(S) \subseteq B^*$.
Exsitenz: Es gibt aufgrund der universellen Eigenschaft des Polynomrings genau ein A-Algebrenhomomorphismu

$$\begin{aligned} \psi : A\left[X_s \middle| s \in S\right] &\to B \\ X_s &\mapsto (g(s))^{-1} \end{aligned}$$

Dieser ist wegen $g(s) \in B^*$ wohldefiniert. Sei nun $f_s = sX_s - 1 \in I$, so folgt:

$$\psi(f_s) = f_s\left((g(s))^{-1} | s \in S\right) = s \cdot (g(s))^{-1} - 1 = g(s)(g(s))^{-1} - 1 = 0$$

Also gilt $I = (f_s | s \in S) \subseteq \ker(\psi)$ und somit ist die Abbildung

$$\begin{aligned} \tilde{\varphi} : \tilde{A} &\to B \\ f(X_s | s \in S) + I &\mapsto f\left((g(s))^{-1} | s \in S\right) \end{aligned}$$

wohldefiniert und ein A-Algebrenhomomorphismus ist. Zudem gilt:

$$\left(\tilde{\varphi} \circ \tilde{f}\right)(a) = \tilde{\varphi}(a + I) = a \cdot \tilde{\varphi}(1 + I) = a \cdot 1 = g(a)$$

Eindeutigkeit: Sei $\tilde{\varphi}' : \tilde{A} \to B$ ein weiterer A-Algebrenhomomorphismus. Es gilt für alle $s \in S$:

$$\begin{aligned} 0 = \tilde{\varphi}'\left(\overline{0}\right) = \tilde{\varphi}'\left(\overline{sX_s - 1}\right) = s \cdot \tilde{\varphi}'\left(\overline{X_s}\right) - \tilde{\varphi}'\left(\overline{1}\right) = g(s)\,\tilde{\varphi}'\left(\overline{X_s}\right) - 1 \\ 1 = g(s) \\ \tilde{\varphi}'\left(\overline{X_s}\right) = (g(s))^{-1} = \varphi\left(\overline{X}_s\right) \end{aligned}$$

Da die $\overline{X_s}$ die A-Algebra $\tilde{A}$ erzeugen, ist $\tilde{\varphi}'$ durch die Bilder der $\overline{X_s}$ eindeutig festgelegt.
„b) ⇒ a)“: Sei $\varphi : \tilde{A} \to B$ mit $\tilde{\varphi} \circ \tilde{f} = g$. Dann gilt für alle $s \in S$:

$$\begin{aligned} 0 = \tilde{\varphi}\left(\overline{0}\right) = \tilde{\varphi}\left(\overline{sX_s - 1}\right) = \tilde{\varphi}\left(\overline{sX_s}\right) - \tilde{\varphi}\left(\overline{1}\right) \\ \tilde{\varphi}\left(\overline{1}\right) = \tilde{\varphi}\left(\overline{sX_s}\right) \end{aligned}$$

$$1 = g(1) = \left(\tilde{\varphi} \circ \tilde{f}\right)(1) = \tilde{\varphi}\left(\overline{1}\right) = \tilde{\varphi}\left(\overline{sX_s}\right) = s \cdot \tilde{\varphi}\left(\overline{X_s}\right) = g(s)\,\tilde{\varphi}\left(\overline{X_s}\right)$$

Also ist $g(s) \in B^*$und somit hat $\tilde{A}$ die universelle Eigenschaft hat von $S^{-1}A$. Daher folgt aus der Eindeutigkeit von $S^{-1}A$ schon die Behauptung. $\square_{3.2}$

3.3 Bemerkung, Beispiel und Definition (Quotientenkörper)

Seien A ein Ring und $S \subseteq A$ multiplikativ abgeschlossen.

i) Ist A ein Integritätsring und gilt $0 \notin S$, so ist (3.1) in 3.1 äquivalent zu:

$$(a,s) \sim (b,t) \quad \Leftrightarrow \quad at - bs = 0 \in A$$

Dies ist die naheliegende Definition von „$\frac{a}{s} = \frac{b}{t}$“. Im Allgemeinen ist dies jedoch keine Äquivalenzrelation.

ii) Ist A ein Integritätsring, so ist $S := A \setminus \{0\} \subseteq A$ multiplikativ abgeschlossen, da $1 \neq 0$ ist und für $a,b \in S$ schon $ab \neq 0$, also $ab \in S$ folgt.

$$Q(A) := \operatorname{Quot}(A) := (A \setminus \{0\})^{-1} A = \left\{ \frac{a}{b} \middle| a,b \in A, b \neq 0 \right\}$$

heißt *der Quotientenkörper von A*. Es gilt zum Beispiel:

$$Q(\mathbb{Z}) = \mathbb{Q}$$

iii) Ist $p \in \mathbb{Z}$ eine Primzahl, so ist $\mathbb{Z} \setminus (p) \subseteq \mathbb{Z}$ multiplikativ abgeschlossen, da $p \neq 1$ und für $a,b \in \mathbb{Z}$ aus $ab \in (p)$ schon $a \in (p)$ oder $b \in (p)$ gilt.

$$(\mathbb{Z} \setminus (p))^{-1} \mathbb{Z} = \left\{ \frac{a}{b} \middle| a,b \in \mathbb{Z}, p \not| b \right\} = \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$$

iv) Es gilt $S^{-1}A = \{0\}$ genau dann, wenn $0 \in S$ ist.

Beweis

Siehe Algebra. $\square_{3.3}$

3.4 Beispiel und Definition (Lokalisierung, Funktionenkörper)

Sei A ein Ring.

i) Ist $\mathfrak{p} \subseteq A$ ein Primideal, so ist $A \setminus \mathfrak{p} \subseteq A$ multiplikativ abgeschlossen und

$$\left(A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} A, \mathfrak{m} := f_*(\mathfrak{p}) = \mathfrak{p} A_{\mathfrak{p}} \right)$$

ist ein lokaler Ring, *die Lokalisierung von A bei $\mathfrak{p}$*. Hier ist:

$$\begin{aligned} f : A &\to A_{\mathfrak{p}} \\ a &\mapsto \frac{a}{1} \end{aligned}$$

Beweis

$A \setminus \mathfrak{p}$ ist nach 1.18 i) multiplikativ abgeschlossen.
Nach 1.36 i) schreibt sich jedes $x \in f_* (g)$ als

$$x = \sum_{i=1}^{n} \frac{a_i}{s_i} b_i$$

mit $n \in \mathbb{N}$ und geeigneten $b_i \in \mathfrak{p}$, $a_i \in A$ und $s_i \in S$. Also:

$$x = \frac{\sum_{i=1}^{n} a_i b_i \prod_{j=1, j\neq 1}^{n} s_j}{\prod_{i=1}^{n} s_i} =: \frac{b}{s}$$

mit $s \in S$ und $b \in \mathfrak{p}$, da $b_i \in \mathfrak{p}$ und $\mathfrak{p}$ ein Ideal ist. Es folgt:

$$f_* (\mathfrak{p}) = \mathfrak{p} A_{\mathfrak{p}}$$

Wäre $1 \in \mathfrak{m} = \mathfrak{p} A_{\mathfrak{p}}$, so folgte:

$$\frac{1}{1} = \frac{b}{s}$$

für geeignete $b \in \mathfrak{p}$ und $s \in S$. Also gibt es ein $t \in A \setminus \mathfrak{p}$ mit:

$$t(s - b) = 0$$
$$ts = tb \in \mathfrak{p}$$

Dies ist ein Widerspruch, da s,$t \notin \mathfrak{p}$ sind. Also gilt $1 \notin \mathfrak{m}$ und damit ist $\mathfrak{m} \subsetneq A_{\mathfrak{p}}$.
Jedes $x \in A_{\mathfrak{p}} \setminus \mathfrak{p} A_{\mathfrak{p}}$ schreibt sich mit geeigneten $a \in A$ und $s \in A \setminus \mathfrak{p}$ als:

$$x = \frac{a}{s}$$

Wegen $x \notin \mathfrak{p} A_{\mathfrak{p}}$ gilt $a \in A \setminus \mathfrak{p}$ und es folgt $A_{\mathfrak{p}} \ni \frac{s}{a} = x^{-1}$. Also ist $x \in A_{\mathfrak{p}}^*$.
Insgesamt ist $\mathfrak{m} \subsetneq A_{\mathfrak{p}}$ und $A_{\mathfrak{p}} \setminus \mathfrak{m} \subseteq A_{\mathfrak{p}}^*$, also ist nach 1.27 $(A_{\mathfrak{p}}, \mathfrak{m})$ ein lokaler Ring. $\square_{\text{i)}}$

Bemerkung

Es gilt:

$$A_{\mathfrak{p}} / \mathfrak{p} A_{\mathfrak{p}} \cong \operatorname{Quot}\left(A / \mathfrak{p} \right) (= \kappa(\mathfrak{p}))$$

ii) Für $a \in A$ ist $S := \left\{ a^n \middle| n \in \mathbb{N} \right\} \subseteq A$ multiplikativ abgeschlossen (und die kleinste multiplikativ abgeschlossene Menge, die a enthält).
Man schreibt in diesem Fall:

$$S^{-1} A =: A\left[a^{-1}\right]$$

Es gilt:

$$A\left[a^{-1}\right] \cong A[X] / (aX - 1)$$

(vergleiche 3.2)
Zum Beispiel ist für ein $n \in \mathbb{N}_{\geq 1}$:

$$\mathbb{Z}\left[\frac{1}{n}\right] = \left\{ \frac{a}{n^b} \middle| a \in \mathbb{Z}, b \in \mathbb{N} \right\} \subseteq \mathbb{Q}$$

iii) Für einen Körper k gelten:

$$\begin{aligned} A := k[t] \subseteq A_{(t)} &= \left\{ \frac{f(t)}{g(t)} \middle| f,g \in k[t] \wedge g \notin (t) \right\} = \\ &= \left\{ \frac{f(t)}{g(t)} \middle| f,g \in k[t] \wedge g(0) \neq 0 \right\} \subseteq \\ &\subseteq Q(A) = \left\{ \frac{f(t)}{g(t)} \middle| f,g \in k[t] \wedge g \neq 0 \right\} =: k(t) \end{aligned}$$

Der Körper $k(t)$ heißt *der Funktionenkörper in einer Variablen t über k.*

Beispiel

Für $\mathfrak{p} := (0) \in \operatorname{Spec}(\mathbb{C}[t])$ ist:

$$\kappa(\mathfrak{p}) = \mathbb{C}(t)$$

3.5 **Konstruktion** (Modul-Lokalisierung)

Seien A ein Ring, $S \subseteq A$ multiplikativ abgeschlossen und M ein A-Modul.
Auf $M \times S$ ist die Relation

$$(x,s) \sim (y,t) \quad :\Leftrightarrow \quad \underset{u \in S}{\exists} : u(xt - ys) = 0$$

eine Äquivalenzrelation und

$$S^{-1}M := {}^{S \times M}\!/_{\sim}$$

wird ein $S^{-1}A$-Modul vermöge für alle $s,t \in S$, $x,y \in M$ und $a \in A$:

$$\begin{aligned} \frac{x}{s} + \frac{y}{t} &:= \frac{tx + sy}{st} \\ \frac{a}{s} \cdot \frac{x}{t} &:= \frac{ax}{st} \end{aligned}$$

Hier ist $\frac{x}{s} := [(x,s)]$.
Ist $f : M \to N$ eine A-lineare Abbildung, so ist

$$\begin{aligned} \left(S^{-1}f\right) : S^{-1}M &\to S^{-1}N \\ \frac{x}{s} &\mapsto \frac{f(x)}{s} \end{aligned}$$

wohldefiniert und $S^{-1}A$-linear.

3.6 **Satz** (Lokalisierung ist exakt)

Sei A ein Ring und $S \subseteq A$ multiplikativ abgeschlossen. Ist dann

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

eine exakte Folge von A-Moduln, so ist auch die Folge

$$S^{-1}M' \overset{S^{-1}f}{\to} S^{-1}M \overset{S^{-1}g}{\to} S^{-1}M''$$

von $S^{-1}A$-Moduln exakt.

Beweis

Zunächst gilt:

$$\left(S^{-1}g\right) \circ \left(S^{-1}f\right) = S^{-1}\left(g \circ f\right) = S^{-1}\left(0\right) = 0$$

Also ist $\operatorname{im}\left(S^{-1}f\right) \subseteq \ker\left(S^{-1}g\right)$.
Sei $x \in \ker\left(S^{-1}g\right) \subseteq S^{-1}M$. Dann gilt für geeignete $m \in M$ und $s \in S$:

$$x = \frac{m}{s}$$

Es gilt:

$$0 = \left(S^{-1}g\right)\left(x\right) \overset{3.5}{=} \frac{g\left(m\right)}{s} \in S^{-1}M''$$

Aus 3.5 folgt insbesondere, dass ein $u \in S$ existiert mit:

$$ug\left(m\right) = 0 \in M''$$

Also ist:

$$0 = g\left(um\right)$$

Daher ist $um \in \ker\left(g\right) = \operatorname{im}\left(f\right)$ und man kann für ein geeignetes $m' \in M'$ schreiben:

$$um = f\left(m'\right)$$

Das heißt:

$$x = \frac{m}{s} \overset{u \in S}{=} \frac{um}{us} = \frac{f\left(m'\right)}{us} = \left(S^{-1}f\right)\left(\frac{m'}{us}\right) \in \operatorname{im}\left(S^{-1}f\right)$$

$\square_{3.6}$

3.7 Korollar

Seien A ein Ring, $S \subseteq A$ multiplikativ abgeschlossen und $N \subseteq M$ zwei A-Moduln. Dann gilt

$$\left(S^{-1}M\right)\Big/\left(S^{-1}N\right) \overset{\sim}{=} S^{-1}\left(M\Big/N\right)$$

als $S^{-1}A$-Moduln.
(Allgemein vertauscht Quotientenbildung mit jeder exakten Operation.)

Beweis

Nach Voraussetzung ist die Folge

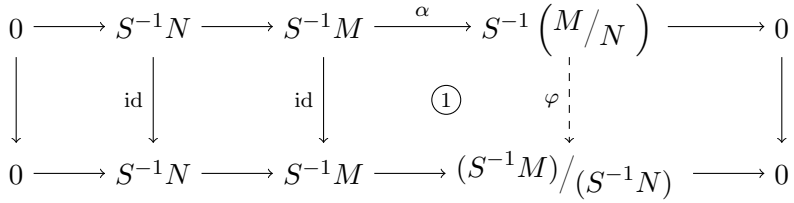
$$0 \to N \to M \to M\Big/N \to 0$$

exakt. Nach 3.6 also auch:

$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}\left(M\Big/N\right) \to 0$$

Insbesondere ist $S^{-1}N \subseteq S^{-1}M$ ein $S^{-1}A$-Untermodul. Betrachte:

$$0 \to S^{-1}N \to S^{-1}M \to \left(S^{-1}M\right)\Big/\left(S^{-1}N\right) \to 0$$



Aus dem Homomorphiesatz folgt, dass genau ein $S^{-1}A$-linearer Isomorphismus φ existiert, sodass ① kommutiert, denn α ist surjektiv und $\ker(\alpha) \cong S^{-1}N$. $\square_{3.7}$

3.8 **Satz** (Lokalisierung als Tensorprodukt)

Seien A ein Ring, $S \subseteq A$ multiplikativ abgeschlossen und M ein A-Modul. Dann existiert genau eine A-lineare Abbildung

$$\varphi_M : S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$$

mit

$$\varphi_M\left(\frac{a}{s} \otimes m\right) = \frac{am}{s}$$

für alle $a \in A$, $s \in S$ und $m \in M$, und φ_M ist ein in M natürlicher $S^{-1}A$-linearer Isomorphismus. Also ist die Lokalisierung eines Moduls ein Spezialfall eines Basiswechsels.

Beweis

Für die erste Aussage ist wegen 2.25 nur die A-Bilinearität der Abbildung

$$\begin{aligned} S^{-1}A \times M &\to S^{-1}M \\ \left(\frac{a}{s}, m\right) &\mapsto \frac{am}{s} \end{aligned}$$

zu zeigen und diese ist klar. Folgende Rechnung zeigt, dass φ_M sogar $S^{-1}A$-linear ist:

$$\varphi_M\left(\frac{a}{s} \cdot \left(\frac{a'}{s'} \otimes m\right)\right) = \varphi_M\left(\frac{aa'}{ss'} \otimes m\right) = \frac{(aa')\,m}{ss'} = \frac{a}{s} \cdot \frac{a'm}{s'} = \frac{a}{s} \cdot \varphi_M\left(\frac{a'}{s'} \otimes m\right)$$

Es ist klar, dass φ_M surjektiv ist, denn für $m \in M$ und $s \in S$ gilt:

$$\frac{m}{s} = \varphi_M\left(\frac{1}{s} \otimes m\right)$$

Sei nun $x \in \ker(\varphi_M) \subseteq S^{-1}A \otimes_A M$. Wie im Beweis von 3.4 i) („Hauptnenner“) sieht man, dass für geeignete $s \in S$ und $m \in M$ schon $x = \frac{1}{s} \otimes m$ gilt. Es folgt:

$$0 = \varphi_M(x) = \frac{m}{s} \in S^{-1}M$$

Daher existiert ein $u \in S$ mit $u \cdot m = 0$ in M. Also ist

$$x = \frac{1}{s} \otimes m = \frac{u}{su} \otimes m = \frac{1}{us} \otimes \underbrace{(um)}_{=0} = 0$$

ein $S^{-1}A$-linearer Isomorphismus, dessen Natürlichkeit in M dann klar ist. $\square_{3.8}$

3.9 Korollar und Definition (flache Algebra)

Sind A ein Ring und $S \subseteq A$ multiplikativ abgeschlossen, so ist

$$\begin{aligned} A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

eine flache A-Algebra, das heißt eine A-Algebra, deren zugrunde liegender A-Modul flach ist.

Beweis

Ist $\mathscr{E}$ eine exakte Folge von A-Moduln, so ist die Folge $S^{-1}A \otimes_A \mathscr{E} \underset{3.8}{\cong} S^{-1}\mathscr{E}$ von $S^{-1}A$-Moduln nach 3.6 exakt. $\square_{3.9}$

3.10 Beispiel

Es folgt nochmal, dass $\mathbb{Q} = (\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z}$ ein flacher $\mathbb{Z}$-Modul ist. (vergleiche 2.38, ii))
Genauso ist für einen Körper k nun $k(T)$ ein flacher $k[T]$-Modul.
Diese Aussagen folgen auch direkt, da $\mathbb{Z}$ und $k[T]$ torsionsfreie Hauptidealringe sind.
Allgemeiner ist $k(T_1, \ldots, T_n) := \mathrm{Quot}(k[T_1, \ldots, T_n])$ ein flacher $k[T_1, \ldots, T_n]$-Modul. Beachte, dass $k[T_1, \ldots, T_n]$ für $n \geq 2$ kein Hauptidealring ist.

3.11 Proposition (Projektionsformel)

Seien $f : A \to B$ ein Ringhomomorphismus, M ein A-Modul und N ein B-Modul.
Dann existiert ein natürlicher Isomorphismus von A-Moduln:

$$N \otimes_B (B \otimes_A M) \overset{\text{Def.}}{=} f_*(N \otimes_B f^*(M)) \cong f_*(N) \otimes_A M \overset{\text{Def.}}{=} N \otimes_A M$$

Beweis

Für jedes $b \in B$ ist

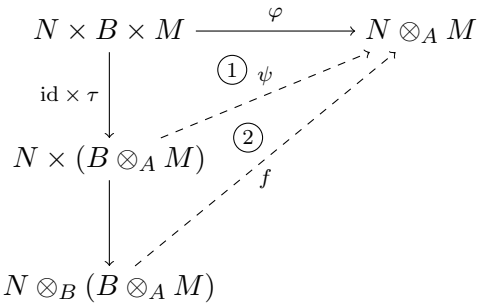
$$\begin{aligned} N \times M &\to N \otimes_A M \\ (n,m) &\mapsto (bn) \otimes m \end{aligned}$$

eine A-bilineare Abbildung, induziert also eine A-lineare Abbildung:

$$\cdot b : N \otimes_A M \to N \otimes_A M$$

Mit diesen Abbildungen als Skalarmultiplikation ist $N \otimes_A M$ ein B-Modul. Betrachte nun die Abbildung:

$$\begin{aligned} \varphi : N \times (B \times M) &\to N \otimes_A M \\ (n,b,m) &\mapsto (bn) \otimes m \end{aligned}$$



Zu ①: Für jedes $n \in N$ ist $\varphi(n,.,.)$ schon A-bilinear, also faktorisiert φ eindeutig über ein ψ.
Zu ②: ψ ist B-bilinear nach Definition der B-Modulstruktur auf $N \otimes_A M$. Also faktorisiert ψ eindeutig über eine B-lineare Abbildung f.
Die Abbildung

$$\begin{aligned} N \times M &\to N \otimes_B (B \otimes_A N) \\ (n,m) &\mapsto n \otimes 1 \otimes m \end{aligned}$$

ist A-bilinear, faktorisiert also über eine A-lineare Abbildung:

$$g : N \otimes_A M \to N \otimes_B (B \otimes_A N)$$

Um zu sehen, dass f und g zueinander invers sind, rechne auf den Erzeugern einerseits

$$f(g(n \otimes m)) = f(n \otimes 1 \otimes m) = (1 \cdot n) \otimes m = n \otimes m$$

und andererseits:

$$g(f(n \otimes b \otimes m)) = g((bn) \otimes m) = (bn) \otimes 1 \otimes m = n \otimes b \otimes m \in N \otimes_B (B \otimes_A M)$$

$\square_{3.11}$

3.12 **Korollar** (Basiswechsel vertauscht mit Tensorprodukt)

Sind $f : A \to B$ ein Ringhomomorphismus und M_1 und M_2 zwei A-Moduln, so existiert ein natürlicher Isomorphismus von B-Moduln:

$$(B \otimes_A M_1) \otimes_B (B \otimes M_2) = f^*(M_1) \otimes_{f^*(A)} f^*(M_2) \tilde{=} f^*(M_1 \otimes_A M_2) = B \otimes_A (M_1 \otimes_A M_2)$$

Beweis

Beachte $f^*(A) \tilde{=} B \otimes_A A \tilde{=} B$.
Erhalte aus der Proposition 3.11 mit $M := M_2$ und $N := f^*(M_1)$ einen A-linearen Isomorphismus:

$$\begin{aligned} f_*(f^*(M_1) \otimes_B f^*(M_2)) \tilde{\to} f_*(f^*(M_1)) \otimes_A M_2 \tilde{=} (B \otimes_A M_1) \otimes_A M_2 \tilde{=} \\ \tilde{=} B \otimes_A (M_1 \otimes_A M_2) \tilde{=} f_*(f^*(M_1 \otimes_A M_2)) \end{aligned}$$

Dieser ist B-linear. $\square_{3.12}$

3.13 Proposition

Seien A ein Ring, $S \subseteq A$ multiplikativ abgeschlossen und M und N zwei A-Moduln.
Dann existiert genau eine $S^{-1}A$-lineare Abbildung

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_A N)$$

mit

$$\left(\frac{m}{s} \otimes \frac{n}{t}\right) \mapsto \frac{m \otimes n}{st}$$

für alle $m \in M$, $n \in N$ und $s,t \in S$, und dieser ist ein natürlicher Isomorphismus.

Beweis

Dies ist ein Spezialfall von 3.12 mit $f : A \to S^{-1}A =: B$, $M_1 := M$ und $M_2 := N$.
Man prüft noch, dass die Komposition der Isomorphismen wie angegeben ist. $\square_{3.13}$

3.14 Korollar

Sind A ein Ring, $\mathfrak{p} \subseteq A$ ein Primideal und M und N zwei A-Moduln, so existiert ein kanonischer Isomorphismus

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{\sim} (M \otimes_A N)_{\mathfrak{p}}$$

von $A_{\mathfrak{p}}$-Moduln.

Beweis

Wähle $S = A \setminus \mathfrak{p}$ in 3.13. $\square_{3.14}$

3.15 Definition (lokale Eigenschaft)

Sei A ein Ring. Eine Eigenschaft $\mathcal{P}$ von A-Moduln heißt *lokal*, falls gilt:
Jeder A-Moduln M besitzt $\mathcal{P}$ genau dann, wenn für alle Primideale $\mathfrak{p} \subseteq A$ der $A_{\mathfrak{p}}$-Modul $M_{\mathfrak{p}}$ die Eigenschaft $\mathcal{P}$ besitzt.

3.16 Proposition (Null zu sein ist eine lokale Eigenschaft)

Seien A ein Ring und M ein A-Modul, dann sind äquivalent:

i) $M = 0$

ii) Für alle Primideale $\mathfrak{p} \subseteq A$ gilt $M_{\mathfrak{p}} = 0$.

iii) Für alle maximalen Ideale $\mathfrak{m} \subseteq A$ gilt $M_{\mathfrak{m}} = 0$.

Beweis

i) $\Rightarrow$ ii) folgt, da der einzige mögliche Zähler eines Elements von $M_\mathfrak{p}$ Null ist.

ii) $\Rightarrow$ iii) ist klar, da jedes maximale Ideal ein Primideal ist.

iii) $\Rightarrow$ i): Sei $x \in M$. Dann ist $I := \{a \in A | ax = 0\} \subseteq A$ ein Ideal.

Ist $\mathfrak{m} \subseteq A$ ein maximales Ideal, so gilt $0 = \frac{x}{1}$ im Modul $0 = M_\mathfrak{m} = (A \setminus \mathfrak{m})^{-1} M$.
Also gibt es ein $a \in A \setminus \mathfrak{m}$ mit:

$$0 = a(1 \cdot x - 1 \cdot 0) = ax \in M$$

Es folgt $a \in I \setminus \mathfrak{m}$, also $I \not\subseteq \mathfrak{m}$.

Da $\mathfrak{m}$ beliebig ist, folgt aus 1.23, dass $I = A$ gilt. Es folgt:

$$x = 1 \cdot x \overset{1 \in I}{=} 0$$

$\square_{3.16}$

3.17 **Proposition** (Mono- bzw. Epimorphimus zu sein ist eine lokale Eigenschaft)

Seien A ein Ring, M und N zwei A-Moduln und $f : M \to N$ eine A-lineare Abbildung.
Dann sind äquivalent:

i) f ist injektiv (beziehungsweise surjektiv).

ii) Für alle Primideale $\mathfrak{p} \subseteq A$ ist

$$f_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}(f) : M_\mathfrak{p} \to N_\mathfrak{p}$$

injektiv (beziehungsweise surjektiv).

iii) Für alle maximalen Ideale $\mathfrak{m} \subseteq A$ ist

$$f_\mathfrak{m} := (A \setminus \mathfrak{m})^{-1}(f) : M_\mathfrak{m} \to N_\mathfrak{m}$$

injektiv (beziehungsweise surjektiv).

Beweis

i) $\Rightarrow$ ii) folgt aus der Exaktheit der Lokalisierung 3.6 angewandt auf die exakte Folge

$$0 \to M \xrightarrow{f} N$$

beziehungsweise:

$$M \xrightarrow{f} N \to 0$$

ii) $\Rightarrow$ iii): Jedes maximale Ideal ist nach 1.19 ein Primideal.

iii) ⇒ i): Betrachte die exakte Folge

$$0 \to \ker(f) \to M \xrightarrow{f} N \to \operatorname{koker}(f) = {}^{N}\!/_{\operatorname{im}(f)} \to 0$$

von A-Moduln. Für jedes maximale Ideal $\mathfrak{m} \subseteq A$ ist dann nach 3.6 die Folge

$$0 \to \ker(f)_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{f} N_{\mathfrak{m}} \to \operatorname{koker}(f)_{\mathfrak{m}} \to 0$$

von $A_{\mathfrak{m}}$-Moduln exakt, und wie im Beweis von 3.7 ergibt der Homomorphiesatz angewandt auf das Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker(f)_{\mathfrak{m}} & \longrightarrow & M_{\mathfrak{m}} & \longrightarrow & N_{\mathfrak{m}} & \longrightarrow & \operatorname{koker}(f)_{\mathfrak{m}} & \longrightarrow & 0 \\
\downarrow & & \cong\,\vdots\downarrow & & \mathrm{id}\downarrow & & \mathrm{id}\downarrow & & \cong\,\vdots\downarrow & & \downarrow \\
0 & \longrightarrow & \ker(f_{\mathfrak{m}}) & \longrightarrow & M_{\mathfrak{m}} & \longrightarrow & N_{\mathfrak{m}} & \longrightarrow & \operatorname{koker}(f_{\mathfrak{m}}) & \longrightarrow & 0
\end{array}$$

die Isomorphien:

$$\ker(f)_{\mathfrak{m}} \cong \ker(f_{\mathfrak{m}})$$
$$\operatorname{koker}(f)_{\mathfrak{m}} \cong \operatorname{koker}(f_{\mathfrak{m}})$$

Ist $f_{\mathfrak{m}}$ injektiv (bzw. surjektiv), so folgt $\ker(f)_{\mathfrak{m}} = 0$ (bzw. $\operatorname{koker}(f)_{\mathfrak{m}} = 0$) für alle maximalen Ideale $\mathfrak{m} \subseteq A$. Nach 3.16 iii) ⇒ i) ist daher $\ker(f) = 0$ (bzw. $\operatorname{koker}(f) = 0$), das heißt f ist injektiv (bzw. surjektiv). $\square_{3.17}$

3.18 **Proposition** (Flach zu sein ist eine lokale Eigenschaft)

Seien A ein Ring und M ein A-Modul. Dann sind äquivalent:

i) M ist ein flacher A-Modul.

ii) Für alle Primideale $\mathfrak{p} \subseteq A$ ist $M_{\mathfrak{p}}$ ein flacher $A_{\mathfrak{p}}$-Modul.

iii) Für alle maximalen Ideale $\mathfrak{m} \subseteq A$ ist $M_{\mathfrak{m}}$ ein flacher $A_{\mathfrak{m}}$-Modul.

Beweis

i) ⇒ ii): Für eine exakte Folge $\mathscr{E}$ von $A_{\mathfrak{p}}$-Moduln gilt:

$$\mathscr{E} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \underset{3.8}{\cong} \mathscr{E} \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}} \otimes_A M) \underset{3.11}{\cong} \mathscr{E} \otimes_A M$$

und diese Folge ist exakt, da $\mathscr{E}$ auch vermöge $A \to A_{\mathfrak{p}}$ aufgefasst als Folge von A-Moduln exakt ist, und M ein flacher A-Modul ist.

ii) ⇒ iii) ist klar.

iii) ⇒ i): Wegen dem Flachheitskriterium 2.35 iii) zeige:

Ist $\iota : N' \hookrightarrow N$ ein A-linearer Monomorphismus, so ist $\iota \otimes \mathrm{id} : N' \otimes_A M \to N \otimes_A M$ injektiv.

Da Monomorphismus zu sein eine lokale Eigenschaft ist, genügt es nach 3.17 iii) ⇒ i) zu zeigen, dass für alle maximalen Ideale $\mathfrak{m} \subseteq A$ die $A_\mathfrak{m}$-lineare Abbildung

$$(\iota \otimes \mathrm{id})_\mathfrak{m} : \left(N' \otimes_A M\right)_\mathfrak{m} \to (N \otimes_A M)_\mathfrak{m}$$

injektiv ist.

$$\begin{array}{lcc} (\iota \otimes \mathrm{id})_\mathfrak{m} : & (N' \otimes_A M)_\mathfrak{m} & \longrightarrow (N \otimes_A M)_\mathfrak{m} \\ & \wr \downarrow 3.14 & \wr \downarrow 3.14 \\ \iota_\mathfrak{m} \otimes \mathrm{id}_{M_\mathfrak{m}} : & N'_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} & \longrightarrow N_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \end{array}$$

Nun ist mit ι auch $\iota_\mathfrak{m}$ injektiv, da Lokalisierung nach 3.6 exakt ist, und da $M_\mathfrak{m}$ ein flacher $A_\mathfrak{m}$-Modul ist, ist auch $\iota_\mathfrak{m} \otimes \mathrm{id}_{M_\mathfrak{m}}$ und damit $(\iota \otimes \mathrm{id}_M)_\mathfrak{m}$ injektiv. $\square_{3.18}$

3.19 **Satz** (Idealtheorie von $S^{-1}A$)

Seien A ein Ring, $S \subseteq A$ multiplikativ abgeschlossen und $f : A \to S^{-1}A$ der kanonische Ringhomomorphismus.

i) Für jedes Ideal $J \subseteq S^{-1}A$ gilt $J = f_*\left(f^*(J)\right)$. Insbesondere ist jedes Ideal von $S^{-1}A$ Bild eines Ideals von A.

ii) Für jedes Ideal $I \subseteq A$ gilt $f^*\left(f_*(I)\right) = \bigcup_{s \in S} \left\{x \in A \middle| sx \in I\right\}$. Insbesondere gilt:

$$f_*(I) = (1) \quad \Leftrightarrow \quad I \cap S \neq \emptyset$$

iii) Für ein Ideal $I \subseteq A$ gilt $I = f^*\left(f_*(I)\right)$ genau dann, wenn kein Element aus S ein Nullteiler in ${}^{A}\!/_{I}$ wird.

iv) Die Abbildungen

$$f^* : \mathrm{Spec}\left(S^{-1}A\right) \underset{\sim}{\overset{\sim}{\rightleftarrows}} \left\{\mathfrak{p} \in \mathrm{Spec}\,(A) \,|\, \mathfrak{p} \cap S = \emptyset\right\} : f_*$$

sind wohldefiniert und zueinander inverse Bijektionen.

Beweis

i) Allgemein gilt $f_*\left(f^*(J)\right) \subseteq J$:
$f_*\left(f^*(J)\right) = \left(f\left(f^{-1}(J)\right)\right)$ ist das von $f\left(f^*(J)\right)$ erzeugte Ideal in $B := S^{-1}A$.
Sei $y \in f_*\left(f^*(J)\right)$, so gibt es ein $n \in \mathbb{N}$ und für $0 \leq k \leq n$ Elemente $x_k \in f^*(J)$ und $b_k \in B$ mit:

$$y = \sum_{k=0}^{n} b_k f(x_k)$$

Wegen $x_k \in f^*(J)$ gibt es Elemente $z_k \in J$ mit $f(x_k) = z_k$. Also gilt, weil J ein Ideal ist:

$$y = \sum_{k=0}^{n} b_k f(x_k) = \sum_{k=0}^{n} b_k z_k \in J$$

Daher ist $f_*(f^*(J)) \subseteq J$.

Sei nun $x \in J \subseteq S^{-1}A$. Schreibe $x = \frac{a}{s}$ mit geeigneten $a \in A$ und $s \in S$. Dann gilt:

$$f(a) = \frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} = \frac{s}{1} \cdot x \in J$$

Also ist $a \in f^*(J)$ und somit:

$$\frac{a}{1} = f(a) \in f_*(f^*(J))$$

Weil J ein Ideal ist, folgt:

$$x = \frac{a}{1} \cdot \frac{1}{s} \in f_*(f^*(J))$$

$\square_{\text{i)}}$

ii) Für alle $a \in A$ gilt:

$$\begin{aligned} a \in f^*(f_*(I)) \quad &\Leftrightarrow \quad \frac{a}{1} = f(a) \in f_*(I) \overset{①}{=} \left\{ \frac{x}{s} \middle| x \in I, s \in S \right\} \quad \Leftrightarrow \\ &\Leftrightarrow \quad \underset{x \in I, s \in S}{\exists} \frac{a}{1} = \frac{x}{s} \in S^{-1}A \quad \Leftrightarrow \\ &\Leftrightarrow \quad \underset{x \in I, s, t \in S}{\exists} t(as - x) = 0 \in A \quad \Leftrightarrow \\ &\overset{②}{\Leftrightarrow} \quad a \in \bigcup_{\tilde{t} \in S} \left\{ a \in A \middle| \tilde{t}a \in I \right\} \supseteq I \end{aligned}$$

Zu ①: $\supseteq$ ist klar und $\subseteq$ folgt mit Bildung des „Hauptnenners“.

Zu ②: „$\Rightarrow$“: Wähle $\tilde{t} := ts$ und beachte $\tilde{t}a = tx \in I$.

„$\Leftarrow$“: Setze $x := \tilde{t}a \in I$, $s := \tilde{t} \in S$ und $t = 1 \in S$. Dann folgt:

$$0 = t \cdot \left(a \cdot \tilde{t} - x \right)$$

Es folgt insbesondere:

$$\begin{aligned} f_*(I) = (1) \quad &\Leftrightarrow \quad f^*(f_*(I)) = (1) \quad \Leftrightarrow \\ &\overset{\text{ii)}}{\Leftrightarrow} \quad 1 \in \bigcup_{s \in S} \left\{ x \in A \middle| sx \in I \right\} \quad \Leftrightarrow \\ &\overset{\text{ii)}}{\Leftrightarrow} \quad \underset{s \in S}{\exists} : s \cdot 1 \in I \quad \Leftrightarrow \quad S \cap I \neq \emptyset \end{aligned}$$

$\square_{\text{ii)}}$

iii) Allgemein gilt $I \subseteq f^*(f_*(I))$:

$f_*(I) = (f(I)) \subseteq S^{-1}A$ ist das von $f(I)$ erzeugte Ideal.

$$f^*(f_*(I)) = f^{-1}((f(I)))$$

Sei $x \in I$, so folgt $y := f(x) \in f(I) \subseteq f_*(I)$. Also gilt:

$$x \in f^{-1}(f(x)) = f^{-1}(y) \subseteq f^{-1}(f_*(I)) = f^*(f_*(I))$$

Das heißt, es gilt $I \subseteq f^*(f_*(I))$.
Mit der Projektion $\pi : A \twoheadrightarrow {}^{A}\!/_{I}$ folgt:

$$I \subseteq f^*(f_*(I)) \overset{\text{ii)}}{=} \bigcup_{s\in S} \{x \in A | sx \in I\} \overset{①}{=} \bigcup_{s\in S} \pi^{-1}\left(\left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, s\overline{x} = \overline{0}\right\}\right)$$

Zu ①:

- „$\subseteq$“: Ist $s \in S$ und $x \in A$ mit $sx \in I$, so folgt:

  $$s\pi(x) = \pi(sx) \overset{sx\in I}{=} \overline{0}$$

  Also gilt

  $$\pi(x) \in \left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, s\overline{x} = \overline{0}\right\}$$

  und somit:

  $$x \in \pi^{-1}\left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, s\overline{x} = \overline{0}\right\}$$

- „$\supseteq$“: Ist $s \in S$ und $x \in \pi^{-1}\left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, s\overline{x} = \overline{0}\right\}$, das heißt:

  $$\overline{0} = s \cdot \pi(x) = \pi(sx)$$

  Also ist $sx \in I$.

Ist nun $I = f^*(f_*(I))$, das heißt:

$$I = \bigcup_{s\in S} \pi^{-1}\left(\left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, s\overline{x} = \overline{0}\right\}\right)$$

Also folgt aus $s\overline{x} = 0$ schon $x \in I$, also $\overline{x} = 0$, und daher ist s kein Nullteiler in ${}^{A}\!/_{I}$.

Ist andererseits kein $s \in S$ ein Nullteiler in ${}^{A}\!/_{I}$, so folgt aus $s\overline{x} = 0$ schon $\overline{x} = 0$ und somit:

$$\begin{aligned} f^*(f_*(I)) &= \bigcup_{s\in S} \pi^{-1}\left(\left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, s\overline{x} = \overline{0}\right\}\right) = \bigcup_{s\in S} \pi^{-1}\left(\left\{\overline{x} \in {}^{A}\!/_{I} \,\middle|\, \overline{x} = \overline{0}\right\}\right) = \\ &= \pi^{-1}\left(\{\overline{0}\}\right) = \ker(\pi) = I \end{aligned}$$

$\square_{\text{iii)}}$

iv) Ist $\mathfrak{q} \subseteq S^{-1}A$ ein Primideal, so auch $\mathfrak{p} := f^*(\mathfrak{q}) \subseteq A$. Wäre $\mathfrak{p} \cap S \neq \emptyset$, so folgte der Widerspruch:

$$(1) \overset{\text{ii)}}{=} f_*(\mathfrak{p}) = f_*(f^*(\mathfrak{q})) \overset{\text{i)}}{=} \mathfrak{q}$$

Also ist f^* wohldefiniert.

Für ein Primideal $\mathfrak{p} \subseteq A$ mit $\mathfrak{p} \cap S = \emptyset$ folgt

$$\mathfrak{q} := f_* (\mathfrak{p}) \overset{\text{ii)}}{\neq} (1)$$

und:

$$\{0\} \neq \left(S^{-1}A\right)/_{\mathfrak{q}} \underset{3.7}{\simeq} S^{-1}\left(A/_{\mathfrak{p}}\right) \subseteq \text{Quot}\left(A/_{\mathfrak{p}}\right)$$

Also ist $\left(S^{-1}A\right)/_{\mathfrak{q}}$ ein Integritätsring, also $\mathfrak{q} \subseteq S^{-1}A$ ein Primideal und somit f_* wohldefiniert.

Wegen i) gilt $f_* \circ f^* = \text{id}_{\text{Spec}(S^{-1}A)}$.

Für ein Primideal $\mathfrak{p} \subseteq A$ mit $\mathfrak{p} \cap S = \emptyset$ ist $A/_{\mathfrak{p}}$ ein Integritätsring und somit nullteilerfrei. Wegen $\mathfrak{p} \cap S = \emptyset$ ist für alle $s \in S$ nun $\overline{s} \neq \overline{0}$ und somit $\overline{s}$ kein Nullteiler in $A/_{\mathfrak{p}}$. Nach iii) ist also $f^* \circ f_* = \text{id}$.

Für ein Primideal $\mathfrak{p} \subseteq A$ mit $\mathfrak{p} \cap S = \emptyset$ folgt auch direkt:

$$(f^* \circ f_*)(\mathfrak{p}) \overset{\text{ii)}}{=} \bigcup_{s \in S} \{x \in A | sx \in \mathfrak{p}\} \underset{S \cap \mathfrak{p} = \emptyset}{\overset{\mathfrak{p} \text{ PI}}{=}} \bigcup_{s \in S} \{x \in A | x \in \mathfrak{p}\} = \mathfrak{p}$$

Also gilt $f^* \circ f_* = \text{id}$. $\square_{\text{iv)}}$

3.20 Korollar (Nilradikal und Lokalisierung vertauschen)

Sind A ein Ring und $S \subseteq A$ multiplikativ abgeschlossen, so gilt für das Nilradikal:

$$\mathfrak{N}\left(S^{-1}A\right) = S^{-1}\left(\mathfrak{N}(A)\right) \subseteq S^{-1}A$$

Beweis

„$\subseteq$“: Sei $x \in \mathfrak{N}\left(S^{-1}A\right)$, das heißt es gibt ein $n \in \mathbb{N}_{\geq 1}$ mit $x^n = 0$. Schreibe $x = \frac{a}{s}$ mit $a \in A$ und $s \in S$ und erhalte:

$$0 = x^n = \frac{a^n}{s^n}$$

Also gibt es ein $t \in S$ mit:

$$\begin{aligned} 0 &= t\left(a^n \cdot 1 - 0 \cdot s^n\right) = ta^n \\ 0 &= t^n a^n = (ta)^n \end{aligned}$$

Also ist $ta \in \mathfrak{N}(A)$ und wegen s,$t \in S$ gilt:

$$x = \frac{a}{s} = \frac{ta}{ts} \in S^{-1}\left(\mathfrak{N}(A)\right)$$

Also ist $\mathfrak{N}\left(S^{-1}A\right) \subseteq S^{-1}\left(\mathfrak{N}(A)\right)$.

„$\supseteq$“: Sei $x \in S^{-1}\left(\mathfrak{N}(A)\right)$, also gibt es ein $a \in \mathfrak{N}(A)$, ein $n \in \mathbb{N}$ und ein $s \in S$ mit $x = \frac{a}{s}$ und $a^n = 0$. Dann gilt:

$$x^n = \frac{a^n}{s^n} = \frac{0}{s^n} = 0$$

Also ist $s \in \mathfrak{N}\left(S^{-1}A\right)$ und somit $S^{-1}\left(\mathfrak{N}(A)\right) \subseteq \mathfrak{N}\left(S^{-1}A\right)$. $\square_{3.20}$

3.21 Korollar

Sind A ein Ring und $\mathfrak{p} \subseteq A$ ein Primideal, so ist die Abbildung

$$f^* : \operatorname{Spec}(A_\mathfrak{p}) \xrightarrow{\sim} \left\{\mathfrak{q} \in \operatorname{Spec}(A) \,\middle|\, \mathfrak{q} \subseteq \mathfrak{p}\right\}$$

Beweis

Nach 3.19 iv) für $S = A \setminus \mathfrak{p}$ ist

$$f^* : \operatorname{Spec}(A_\mathfrak{p}) \xrightarrow{\sim} \left\{\mathfrak{q} \in \operatorname{Spec}(A) \,\middle|\, \mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset\right\}$$

und es gilt:

$$\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset \quad \Leftrightarrow \quad \mathfrak{q} \subseteq \mathfrak{p}$$

$\square_{3.21}$

3.22 Proposition und Definition (endlich präsentiert)

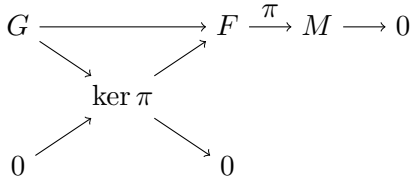
Seien A ein Ring und M ein A-Modul.

i) M heißt genau dann *endlich präsentiert*, wenn eine exakte Folge

$$G \to F \xrightarrow{\pi} M \to 0$$

von A-Moduln existiert, wobei F und G endlich erzeugt und frei sind.

(Also ist M insbesondere endlich erzeugt, da π surjektiv ist. Außerdem gibt es zwischen den Erzeugern nur endlich viele Relationen.)



ii) Ist M endlich präsentiert und $f : A \to B$ ein Ringhomomorphismus, so ist der B-Modul $f^*(M)$ endlich präsentiert.

(Das heißt "endlich präsentiert" ist stabil unter Basiswechsel.)

Beweis

Nach der Rechtsexaktheit des Tensorprodukts 2.34 ist die Folge

$$f^*(G) \to f^*(F) \to f^*(M) \to 0$$

von B-Moduln exakt.

$f^*(G)$ und $f^*(F)$ sind endlich erzeugt und frei, da $f^*(A^n) \cong B^n$ ist. $\square_{\text{ii)}}$

3.23 **Proposition** (flach ist stabil unter Basiswechsel)

Sind $f : A \to B$ ein Ringhomomorphismus und M ein flacher A-Modul, so ist der B-Modul $f^*(M)$ flach.

Beweis

Ist $\mathcal{E}$ eine exakte Folge von B-Moduln, so gilt nach der Projektionsformel die Isomorphie:

$$f_*(\mathcal{E} \otimes_B f^*(M)) \underset{3.11}{\cong} f_*(\mathcal{E}) \otimes_A M$$

Nun ist $f_*(\mathcal{E}) \otimes_A M$ eine exakte Folge von A-Moduln, da $f_*(\mathcal{E})$ eine exakte Folge von A-Moduln und M ein flacher A-Modul ist. Also ist auch die Folge $\mathcal{E} \otimes_B f^*(M)$ von B-Moduln exakt. Beachte, dass Exaktheit eine Eigenschaft der abelschen Gruppe ist und nicht von der Multiplikation abhängt. $\square_{3.23}$

3.24 **Lemma** (endlich präsentiert und flach impliziert projektiv)

Seien A ein Ring und M ein A-Modul.

i) Es sind äquivalent:

   a) M ist flach.
   b) Sind F ein endlich erzeugter, freier A-Modul, $\alpha : F \to M$ eine A-lineare Abbildung und $f \in \ker(\alpha)$, so existieren ein endlich erzeugter, freier A-Modul G und A-lineare Abbildungen $\beta : G \to M$ und $\gamma : F \to G$, sodass $\gamma(f) = 0$ und $\alpha = \beta \circ \gamma$ gelten.
   c) Sind F ein endlich erzeugter, freier A-Modul, $\alpha : F \to M$ eine A-lineare Abbildung und $K \subseteq \ker(\alpha)$ ein Untermodul, so existieren ein endlich erzeugter, freier A-Modul G und A-lineare Abbildungen $\beta : G \to M$ und $\gamma : F \to G$, sodass $\gamma(K) = 0$ und $\alpha = \beta \circ \gamma$ gelten.

ii) Sei M ein endlich präsentierter flacher A-Modul. Dann ist M projektiv.

Beweis

i) „a) ⇒ b)“: Sei F ein endlich erzeugter freier A-Modul, also $F \cong A^n$ mit $n \in \mathbb{N}$, und $\alpha : F \to M$ eine A-lineare Abbildung, definiert durch $\alpha(e_i) = m_i$, und $f \in \ker(\alpha)$. Also:

$$f = \sum_{i=1}^{n} \underbrace{\alpha_i}_{\in A} e_i$$

$$0 = \alpha(f) = \sum_{i=1}^{n} \alpha_i \underbrace{f(e_i)}_{=:m_i \in M} = \sum_{i=1}^{n} \alpha_i m_i$$

Dass M flach ist, ist äquivalent zur Existenz von einem $k \in \mathbb{N}$, $m'_j \in M$ für $j \in \{1, \ldots, k\}$ und $a_{ij} \in A$, sodass für alle $i \in \{1, \ldots, n\}$

$$m_i = \sum_{j=1}^{k} a_{ij} m'_j$$

gilt und für alle $j \in \{1, \ldots, k\}$:

$$0 = \sum_{i=1}^{n} a_{ij} \alpha_i$$

Definiere also $G := A^k$ und $\beta : G \to M$ mit $\beta(e_j) := m'_j$ und $\gamma : F \to G$ mit:

$$\gamma(e_i) = \sum_{j=1}^{k} a_{ij} e_j$$

Dann gilt:

$$\gamma(f) = \sum_{i=1}^{n} \alpha_i \gamma(e_i) = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{k} a_{ij} e_j = \sum_{j=1}^{k} \underbrace{\left(\sum_{i=1}^{n} \alpha_i a_{ij} \right)}_{=0} e_j = 0$$

$$(\beta \circ \gamma)(e_i) = \beta \left(\sum_{j=1}^{k} a_{ij} e_j \right) = \sum_{j=1}^{k} a_{ij} \underbrace{\beta(e_j)}_{=m'_j} = \sum_{j=1}^{k} a_{ij} m'_j = m_i = \alpha(e_i)$$

„b) $\Rightarrow$ a)“: Zeige Flachheit über das Gleichungskriterium 2.41:

Betrachte eine Relation mit $n \in \mathbb{N}$, $n_i \in A$ und $m_i \in M$ für $i \in \{1, \ldots, n\}$:

$$\sum_{i=1}^{n} n_i m_i = 0 \in M$$

Nun sei $(b_1, \ldots, b_n)$ eine Basis von $F \cong A^n$ und $\alpha : F \to M$ eine A-lineare Abbildung, festgelegt durch die Bilder $\alpha(b_i) := m_i$ der Basiselemente.

Definiere nun:

$$f := \sum_{i=1}^{n} n_i b_i \in F$$

$$\Rightarrow \quad \alpha(f) = \alpha \left(\sum_{i=1}^{n} n_i b_i \right) = \sum_{i=1}^{n} n_i m_i = 0$$

Also ist $f \in \ker(\alpha)$. Nach Voraussetzung existiert ein endlich erzeugter, freier A-Modul $G \cong A^m$ mit Basis $(c_1, \ldots, c_m)$ und A-lineare Abbildungen $\gamma : F \to G$ und $\beta : G \to M$, sodass $\gamma(f) = 0$ ist und folgendes Diagramm kommutiert:

$$\begin{array}{ccc} F & \xrightarrow{\alpha} & M \\ {\scriptstyle\gamma}\downarrow & \nearrow_{\beta} & \\ G & & \end{array}$$

Stelle nun die Bilder $\gamma(b_i)$ in der Basis $(c_1,\ldots,c_m)$ mit $a_{ij} \in A$ dar

$$\gamma(b_i) = \sum_{j=1}^{m} a_{ij} c_j$$

und definiere:

$$m'_j := \beta(c_j)$$

Damit folgt:

$$\sum_{j=1}^{m} a_{ij} m'_j = \sum_{j=1}^{m} a_{ij} \beta(c_j) = \beta\left(\sum_{j=1}^{m} a_{ij} c_j\right) = \beta(\gamma(b_i)) = \alpha(b_i) = m_i$$

$$0 = \gamma(f) = \gamma\left(\sum_{i=1}^{n} n_i b_i\right) = \sum_{i=1}^{n} n_i \sum_{j=1}^{m} a_{ij} c_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} n_i\right) c_j$$

Da die $c_1,\ldots,c_m$ als Basiselemente linear unabhängig sind, folgt für alle $j \in \{1,\ldots,m\}$:

$$\sum_{i=1}^{n} a_{ij} n_i = 0$$

Also ist M flach.

„b) $\Rightarrow$ c)“: Induktion über die Dimension l des Moduls K.
Induktionsanfang bei $l = 1$: Dies ist a) $\Rightarrow$ b) für $K = (f)$, denn mit $f \in \ker(\alpha)$ ist auch $(f) \in \ker(\alpha)$.
Induktionsschritt $l \rightsquigarrow l+1$: Sind F ein endlich erzeugter, freier A-Modul, $\alpha : F \to M$ eine A-lineare Abbildung und $K = (f_1,\ldots,f_{l+1}) \subseteq \ker(\alpha)$ ein Untermodul.
Dann hat $(f_1,\ldots,f_l) \subseteq \ker(\alpha)$ Dimension l und nach Induktionsvoraussetzung existiert ein endlich erzeugter, freier A-Modul G_1 und A-lineare Abbildungen

$$\begin{aligned} \beta_1 &: G_1 \to M \\ \gamma_1 &: F \to G_1 \end{aligned}$$

mit $\gamma_1((f_1,\ldots,f_l)) = 0$ und $\alpha = \beta_1 \circ \gamma_1$.
Außerdem hat $(\gamma_1(f_{l+1})) \subseteq \ker(\beta_1)$ Dimension 1 und nach Induktionsanfang existiert ein endlich erzeugter, freier A-Modul G_2 und A-lineare Abbildungen

$$\begin{aligned} \beta_2 &: G_2 \to M \\ \gamma_2 &: G_1 \to G_2 \end{aligned}$$

mit $\gamma_2((f_{l+1})) = 0$ und $\beta_1 = \beta_2 \circ \gamma_2$.
Dann ist $G := G_2$ ein freier A-Modul und

$$\begin{aligned} \beta := \beta_2 : G &\to M \\ g &\mapsto \beta_2(g) \end{aligned}$$

und

$$\begin{aligned} \gamma := \gamma_2 \circ \gamma_1 : F &\to G \\ f &\mapsto (\gamma_2 \circ \gamma_1)(f) \end{aligned}$$

zwei A-lineare Abbildungen und es gilt:

$$\gamma(K) = \gamma_2(\gamma_1((f_1, \ldots, f_{l+1}))) = \gamma_2((\gamma_1(f_{l+1}))) = 0$$
$$(\beta \circ \gamma)(f) = (\beta_2 \circ \gamma_2 \circ \gamma_1)(f) = (\beta_1 \circ \gamma_1)(f) = \alpha(f)$$

„c) $\Rightarrow$ b)“: Dies ist klar, da b) der Spezialfall $K = (f)$ von c) ist, denn mit $f \in \ker(\alpha)$ ist auch $(f) \in \ker(\alpha)$. $\square_{\text{i)}}$

ii) F ist ein endlich erzeugter, freier A-Modul, $\alpha : F \to M$ eine A-lineare Abbildung und $K := a(G) = \ker(\alpha)$ ein endlich erzeugter Modul, da G endlich erzeugt ist.
Da M flach ist, existieren ein endlich erzeugter, freier A-Modul $\tilde{G}$ und A-lineare Abbildungen $\beta : \tilde{G} \to M$ und $\gamma : F \to \tilde{G}$, sodass $\gamma(K) = 0$ und $\alpha = \beta \circ \gamma$ gelten.
Da α surjektiv ist und wegen $K = \ker(\alpha) = \ker(\beta \circ \gamma)$ und $\gamma(K) = 0$ gilt:

$$\beta\big|_{\gamma(F)} : \gamma(F) \xrightarrow{\sim} \alpha(F) = M$$

Daher ist $\iota := \left(\beta\big|_{\gamma(F)}\right)^{-1} : M \to \tilde{G}$ injektiv und somit M ein Untermodul des freien Moduls $\tilde{G}$. Außerdem gibt es die Abbildung $\beta : \tilde{G} \to M$ mit $\beta \circ \iota = \mathrm{id}_M$. Also ist M ein direkter Summand von $\tilde{G}$ und somit projektiv. $\square_{\text{ii)}}$

3.25 Satz

Für endlich präsentierte Moduln ist die Eigenschaft projektiv zu sein eine lokale Eigenschaft, genauer gilt:
Sind A ein Ring und M ein endlich präsentierter A-Modul, dann sind äquivalent:

i) M ist projektiv.

ii) Für alle $\mathfrak{p} \in \mathrm{Spec}(A)$ ist der $A_{\mathfrak{p}}$-Modul $M_{\mathfrak{p}}$ projektiv.

iii) Für alle maximalen Ideale $\mathfrak{m} \in \mathrm{Spec}(A)$ ist der $A_{\mathfrak{m}}$-Modul $M_{\mathfrak{m}}$ projektiv.

Beweis

i) $\Rightarrow$ ii): Weil projektiv nach 2.36 flach impliziert und flach nach 3.23 stabil unter Basiswechsel ist, ist der $A_{\mathfrak{p}}$-Modul $M_{\mathfrak{p}}$ flach. Außerdem ist $M_{\mathfrak{p}}$ nach und 3.22 ii) endlich präsentiert.

Nach 3.24 ist $M_{\mathfrak{p}}$ projektiv.

ii) $\Rightarrow$ iii) ist klar.

iii) $\Rightarrow$ i): Da projektiv nach 2.36 flach impliziert, ist $M_{\mathfrak{m}}$ flach. Also ist, da flach zu sein nach 3.18 iii) eine lokale Eigenschaft ist, die zu prüfen auf maximalen Idealen ausreicht, ist M ein flacher A-Modul. Nach 3.24 folgt, da M endlich präsentiert und flach ist, dass M bereits ein projektiver A-Modul ist. $\square_{3.25}$

3.26 Lemma

Seien B ein Integritätsring und $J \subseteq B$ ein Ideal.

Dann ist J genau dann ein freier B-Modul, wenn J ein Hauptideal ist. In diesem Fall ist J frei vom Rang 0 oder 1.

Beweis

Sei ohne Einschränkung $J \neq (0)$, da für (0) vom Rang 0 die Behauptung klar ist.
„$\Leftarrow$“: Ist J ein Hauptideal, so gilt $J = (b)$ mit einem geeignete $b \in B \setminus \{0\}$. Dann ist

$$\begin{aligned} B &\xrightarrow{\sim} (b) = J \\ x &\mapsto bx \end{aligned}$$

ein B-linearer Isomorphismus, denn Linearität und Surjektivität sind klar und die Injektivität folgt, da B ein Integritätsring ist. Also ist J ein freier B-Modul vom Rang 1.
„$\Rightarrow$“: Sei umgekehrt J frei, so existiert ein B-Modul-Isomorphismus $J \cong B^{(X)}$ für eine geeignete Menge X. Wäre $|X| \geq 2$, so gäbe es zwei $a,b \in J \setminus \{0\}$, die B-linear unabhängig sind. Dies ist ein Widerspruch zur linearen Relation:

$$a \cdot b + (-b) \cdot a = 0$$

Also gilt $|X| \leq 1$ und wegen $J \neq (0)$ sogar $|X| = 1$. Insbesondere existiert ein $b \in J$ mit $J = B \cdot b = (b)$, das heißt J ist ein Hauptideal. $\square_{3.26}$

3.27 **Beispiel** (frei zu sein ist keine lokale Eigenschaft)

Die Teilmenge $A := \mathbb{Z}\left[\sqrt{-5}\right] := \left\{a + b\sqrt{-5} \middle| a,b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$ ist ein Unterring, was leicht nachzurechnen ist.

Das Ideal $I := \left(2,1 + \sqrt{-5}\right) \subseteq A$ ist ein endlich präsentierter A-Modul so, dass für alle maximalen Ideale $\mathfrak{m} \subseteq A$ der $A_\mathfrak{m}$-Modul $I_\mathfrak{m}$ frei ist, daher ist nach 3.25 iii) $\Rightarrow$ i) I projektiv. Aber I selbst ist nicht frei.

Beweis

Nach Definition ist I durch $2,1+\sqrt{-5}$ erzeugt, also endlich erzeugt, und daher ist die Abbildung

$$\begin{aligned} \varphi : A^2 &\twoheadrightarrow I \\ (a,b) &\mapsto 2a + b\sqrt{-5} \end{aligned}$$

surjektiv und offenbar A-linear. Sei $(a,b) \in \ker(\varphi)$, dann gilt:

$$\begin{aligned} 2a + \sqrt{-5} \cdot b &= 0 \\ 2a &= -\sqrt{-5} \cdot b \end{aligned}$$

Daher ist die Abbildung

$$\begin{aligned} \psi : A &\twoheadrightarrow \ker(\varphi) \\ u &\mapsto \left(-\sqrt{-5}u, 2u\right) \end{aligned}$$

wohldefiniert und surjektiv und offenbar A-linear und somit ist

$$A \xrightarrow{\psi} A^2 \xrightarrow{\varphi} I \to 0$$

eine exakte Folge, und, da A und A^2 endlich erzeugt und frei sind, ist I endlich präsentiert.

Da $A \subseteq A_{\mathfrak{m}} \subseteq \operatorname{Quot}(A) \subseteq \mathbb{C}$ Unterringe sind, sind A und alle Lokalisierungen $A_{\mathfrak{m}}$ Integritätsringe und man kann die Behauptung anwenden.
Zeige zunächst, dass für alle maximalen Ideale $\mathfrak{m} \subseteq A$ das Ideal $I_{\mathfrak{m}} = \left(2,1+\sqrt{-5}\right)_{\mathfrak{m}} \subseteq A_{\mathfrak{m}}$ ein Hauptideal ist, denn dann ist $I_{\mathfrak{m}}$ nach 3.26 ein freier $A_{\mathfrak{m}}$-Modul:
Es gilt $\mathfrak{m} \cap \mathbb{Z} = (p)$ mit einer geeigneten Primzahl $p \in \mathbb{Z}$, denn für die $\mathbb{Z}$-lineare Abbildung

$$\begin{aligned} f : A &\to \mathbb{Z} \\ a + b\sqrt{-5} &\mapsto a \end{aligned}$$

ist $f_*(\mathfrak{m}) = \mathfrak{m} \cap \mathbb{Z}$ als Bild eines Primideals ein Primideal (vergleiche 2.49).
Ist $p \neq 2$, so folgt $2 \notin \mathfrak{m}$. Nach 1.27 i) „$\Leftarrow$“ ist also $2 \in A \setminus \mathfrak{m} \subseteq A_{\mathfrak{m}}^*$, da $(A_{\mathfrak{m}},\mathfrak{m})$ ein lokaler Ring ist, und es folgt, dass

$$I_{\mathfrak{m}} = \left(2,1+\sqrt{-5}\right)_{\mathfrak{m}} = (1)_{\mathfrak{m}} = A_{\mathfrak{m}}$$

ein Hauptideal ist.
Ist $p = 2$, so behaupten wir:

$$\frac{\left(1+\sqrt{-5}\right)^2}{2} = \frac{1-5+2\sqrt{-5}}{2} = -2+\sqrt{-5} =: u \notin \mathfrak{m}$$

Andernfalls gelten $2 = p \in \mathfrak{m}$ und $u = -2+\sqrt{-5} \in \mathfrak{m}$, also auch

$$\begin{aligned} \sqrt{-5} &= 2 + \left(-2+\sqrt{5}\right) \in \mathfrak{m} \\ -5 &= \left(\sqrt{-5}\right)^2 \in \mathfrak{m} \end{aligned}$$

und damit folgt der Widerspruch $-5+3\cdot 2 = 1 \in \mathfrak{m}$.
Wegen $u \notin \mathfrak{m}$ gilt nach 1.27 i) „$\Leftarrow$“ schon $u \in A^*$ und somit auch $u \in A_{\mathfrak{m}}^*$. Also gilt:

$$\begin{aligned} \left(1+\sqrt{-5}\right)^2 &= -4+2\sqrt{-5} = 2\cdot\left(-2+\sqrt{-5}\right) \\ 2 &= \underbrace{u^{-1}}_{\in A_{\mathfrak{m}}} \left(1+\sqrt{-5}\right)^2 \in \left(1+\sqrt{-5}\right)\cdot A_{\mathfrak{m}} \end{aligned}$$

Daher ist

$$I_{\mathfrak{m}} = \left(2,1+\sqrt{-5}\right) A_{\mathfrak{m}} = \left(1+\sqrt{-5}\right) A_{\mathfrak{m}}$$

wieder ein Hauptideal.
Zeige noch, dass $I \subseteq A$ selbst kein Hauptideal ist. Dann folgt nach 3.26, dass I nicht frei ist.
Angenommen

$$I = \left(2,1+\sqrt{-5}\right) = \left(a+b\cdot\sqrt{-5}\right) \subseteq A = \mathbb{Z}\left[\sqrt{-5}\right]$$

wäre ein Hauptideal mit geeigneten $a,b \in \mathbb{Z}$. Berechne zunächst den Quotienten:

$$\begin{aligned} A/I &= \mathbb{Z}\left[\sqrt{-5}\right]/\left(2,1+\sqrt{-5}\right) \cong \left(\mathbb{Z}[X]/\left(X^2+5\right)\right)/\left(2,1+\overline{X}\right) \cong \\ &\cong \mathbb{Z}[X]/\left(2,1+X,X^2+5\right) \cong \mathbb{Z}/\left(2,(-1)^2+5=6\right) \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 \end{aligned}$$

Andererseits sieht man leicht, dass gilt für $a+b\sqrt{-5} \in A \setminus \{0\}$:

$$\begin{aligned} A/(a+b\sqrt{-5}) &= \mathbb{Z}[\sqrt{-5}]/(a+b\sqrt{-5}) \cong \left(\mathbb{Z}[X]/(X^2+5)\right)/(a+b\overline{X}) \cong \\ &\cong \mathbb{Z}[X]/(a+bX, X^2+5) \cong \mathbb{Z}/\left((-a)^2+5b^2 = a^2+5b^2\right) \end{aligned}$$

Also gilt:

$$\left|A/(a+b\sqrt{-5})\right| = \left|\mathbb{Z}/(a^2+5b^2)\right| = a^2+5b^2$$

Es folgte $a^2+5b^2 = 2$ im Widerspruch zu $a,b \in \mathbb{Z}$. $\square_{3.27}$

3.28 Beispiel

Wie kann man $\operatorname{Spec}(\mathbb{C}[X])$ und $\operatorname{Spec}(\mathbb{R}[X])$ skizzieren?
$\mathbb{C}[X]$ und $\mathbb{R}[X]$ sind Hauptidealringe, also sind die Primideale außer dem Nullideal normierte irreduzible Polynome.
$\mathbb{C}$ ist algebraisch abgeschlossen, das heißt die irreduziblen Polynome sind linear, also gilt:

$$\operatorname{Spec}(\mathbb{C}[X]) = \{(X-\alpha) \mid \alpha \in \mathbb{C}\} \cup \{(0)\}$$

Bemerkung: Ist k ein beliebiger Körper, dann gilt:

$$\operatorname{Spec}(k[X]) \cong \{0\} \cup \overline{k}/G_k$$

Für $k = \mathbb{C}$ ist die absolute Galoisgruppe

$$G_{\mathbb{C}} = \operatorname{Gal}\left(\mathbb{C}/\mathbb{C}\right) = \{1\}$$

und für $k = \mathbb{R}$ ist

$$G_{\mathbb{R}} = \operatorname{Gal}\left(\mathbb{C}/\mathbb{R}\right) = \left\{1, \overline{\cdot}\right\}$$

mit der komplexen Konjugation $\overline{\cdot}$.
Sei $f \in \mathbb{R}[X]$ normiert, dann gilt in $\mathbb{C}[X]$

$$f(x) = \prod_{i=1}^{n}(X-\alpha_i)\prod_{j=1}^{m}(X-\beta_i)\left(X-\overline{\beta_i}\right)$$

mit geeigneten $\alpha_i \in \mathbb{R}$ und $\beta_i \in \mathbb{C} \setminus \mathbb{R}$. Ist $f \in \mathbb{R}[X]$ irreduzibel, so folgt:

$$f(X) = \begin{cases} X-\alpha & \alpha \in \mathbb{R} \\ (X-\beta)\left(X-\overline{\beta}\right) = X^2 - 2\operatorname{Re}(\beta)X + |\beta|^2 & \beta \in \mathbb{C}\setminus\mathbb{R} \end{cases}$$

Also gilt:

$$\begin{aligned} \operatorname{Spec}(\mathbb{R}[X]) &= \left\{(X-\alpha), \left(X^2 - 2\operatorname{Re}(\beta)X + |\beta|^2\right) \mid \alpha \in \mathbb{R}, \beta \in \mathbb{C}\setminus\mathbb{R}\right\} \cup \{(0)\} = \\ &= \left\{(X-\alpha), \left(X^2 - 2\operatorname{Re}\left(\overline{\beta}\right)X + \left|\overline{\beta}\right|^2\right) \mid \alpha \in \mathbb{R}, \beta \in \mathbb{C}\setminus\mathbb{R}\right\} \cup \{(0)\} \end{aligned}$$

Behauptung: Die abgeschlossenen Teilmengen von $Z = \operatorname{Spec}(A := \mathbb{C}[X])$ beziehungsweise $Z = \operatorname{Spec}(A := \mathbb{R}[X])$ sind genau die endlichen Teilmengen und X.

Beweis: Sei $Y \subseteq X$ abgeschlossen, so gibt es nach der Definition der Zariski-Topologie ein Ideal $I \subseteq A$ mit:

$$Y = V(I) := \left\{\mathfrak{p} \subseteq A \text{ Primideal} \middle| I \subseteq \mathfrak{p}\right\}$$

Da A ein Hauptidealring ist, gibt es ein $f \in A$ mit $(f) = I$. Für ein Primideal $\mathfrak{p} = (g)$, das heißt g ist irreduzibel, gilt:

$$(f) = I \subseteq \mathfrak{p} = (g) \quad \Leftrightarrow \quad g \middle| f$$

Dann folgt:
Ist $f = 0$, so ist $Y = Z$.
Ist $f \neq 0$, so ist $f = \prod_i g_i$ mit irreduziblen g_i und $Y = V((f)) = \{(g_i)\}$. $\square_{\text{Behauptung}}$

Berechne die Restklassenkörper:
Sei $\mathfrak{p} \in \operatorname{Spec}(\mathbb{C}[X])$.

1. Fall: $\mathfrak{p} = (0)$, dann gilt:
$$\kappa((0)) = \operatorname{Quot}\left(\mathbb{C}[X]/_{(0)}\right) = \operatorname{Quot}(\mathbb{C}[X]) = \mathbb{C}(X)$$
2. Fall: $\mathfrak{p} = (X - \alpha)$ für ein $\alpha \in \mathbb{C}$, so gilt:
$$\kappa(\mathfrak{p}) = \operatorname{Quot}\Bigg(\underbrace{\mathbb{C}[X]/_{(X-\alpha)}}_{=\mathbb{C}}\Bigg) = \mathbb{C}$$
Für
$$\mathbb{C}[X]/_{(X-\alpha)} \cong \mathbb{C}$$
betrachte den Einsetzungshomomorphismus:
$$\begin{array}{ccc} \mathbb{C}[X] & \twoheadrightarrow & \mathbb{C}, \qquad X \mapsto \alpha \\ \downarrow & \nearrow & \\ \mathbb{C}[X]/_{(X-\alpha)} & & \end{array}$$

Nun sei $\mathfrak{p} \in \operatorname{Spec}(\mathbb{R}[X])$:

1. Fall: $\mathfrak{p} = (0)$, so folgt wie oben $\kappa((0)) = \mathbb{R}[X]$.
2. Fall: $\mathfrak{p} = (X - \alpha)$ mit $\alpha \in \mathbb{R}$, so folgt wie oben $\kappa(\mathfrak{p}) = \mathbb{R}$.
3. Fall: $\mathfrak{p} = \left(f(X) := X^2 - 2\operatorname{Re}(\beta) + |\beta|^2\right)$ mit $\beta \in \mathbb{C} \setminus \mathbb{R}$, dann folgt:
$$\kappa(\mathfrak{p}) = \operatorname{Quot}\left(\mathbb{R}[X]/_{(f)}\right)$$
Betrachte den Einsetzungshomomorphismus:
$$\begin{aligned} \varphi : \mathbb{R}[X] &\to \mathbb{C} \\ X &\mapsto \beta \end{aligned}$$
Dieser ist wegen $\beta \notin \mathbb{R}$ surjektiv und es ist $\ker(\varphi) = (f)$, denn betrachte:

$$\begin{array}{ccc} \mathbb{R}[X] & \twoheadrightarrow & \mathbb{C} \\ \downarrow & \nearrow & \\ \mathbb{R}[X]/(f) & & \end{array}$$

Da $f = \operatorname{Mipo}_{\mathbb{R}}(\beta)$ vom Grad 2 ist, ist $\dim_{\mathbb{R}}\left(\mathbb{R}[X]/(f)\right) = 2$, also folgt Isomorphie. Daher gilt:

$$\kappa(\mathfrak{p}) = \operatorname{Quot}(\mathbb{C}) = \mathbb{C}$$

Berechne nun die Fasern:
Sei $\mathfrak{p} \in \operatorname{Spec}(A)$.

$$\begin{array}{ccc} A = \mathbb{C}[X] & \rightarrowtail & B = \mathbb{C}[X,Y]/(Y^2 - X) \\ \downarrow & & \downarrow \\ \kappa(\mathfrak{p}) & \longrightarrow & \kappa(\mathfrak{p}) \otimes_A B =: B_{\mathfrak{p}} \end{array}$$

1. Fall: $\mathfrak{p} = (0)$, $\kappa(\mathfrak{p}) = \mathbb{C}(X)$ und mit $\mathbb{C}(X) = S^{-1}A$ für $A := \mathbb{C}[X]$ und $S := A \setminus \{0\}$ gilt:

$$B_{\mathfrak{p}} = \underbrace{\mathbb{C}(X)}_{=S^{-1}A} \otimes_{\mathbb{C}[X]} \underbrace{\mathbb{C}[X,Y]/(Y^2 - X)}_{=M} \cong S^{-1}\left(\mathbb{C}[X,Y]/(Y^2 - X)\right) \cong$$
$$\underset{S^{-1} \text{ exakt}}{\cong} \left(S^{-1}(\mathbb{C}[X,Y])\right)/(Y^2 - X) \cong \mathbb{C}(X)[Y]/(Y^2 - X)$$

   Das Polynom $Y^2 - X \in \mathbb{C}(X)[Y]$ ist irreduzibel, da es Eisenstein bezüglich dem Primelement X ist.
   Also ist $\kappa(\mathfrak{p}) = \mathbb{C}(X) \subseteq B_{\mathfrak{p}}$ eine Körpererweiterung vom Grad 2.

2. Fall: $\mathfrak{p} = (X - \alpha)$ mit $\alpha \in \mathbb{C}$. Dann gilt:

$$B_{\mathfrak{p}} = \underbrace{\operatorname{Quot}\left(\mathbb{C}[X]/(X - \alpha)\right)}_{=\kappa(\mathfrak{p}) \cong \mathbb{C}} \otimes_{\mathbb{C}[X]} \mathbb{C}[X,Y]/(Y^2 - X) \cong$$
$$\underset{(X-\alpha) \text{ maximal}}{\cong} A := \mathbb{C}[X]/I := (X - \alpha) \otimes_{\mathbb{C}[X]} \underbrace{\mathbb{C}[X,Y]/(Y^2 - X)}_{=:M} \cong$$
$$\underset{2.48}{\cong} \left(\mathbb{C}[X,Y]/(Y^2 - X)\right)/(X - \alpha) \cdot \left(\mathbb{C}[X,Y]/(Y^2 - X)\right) \cong$$
$$\cong \left(\mathbb{C}[X,Y]/(Y^2 - X)\right)/\left((X - \alpha)/(X - \alpha) \cdot (Y^2 - X)\right) \cong$$
$$\underset{2.8 \text{ ii)}}{\cong} \left(\mathbb{C}[X,Y]/(Y^2 - X)\right)/\left((Y^2 - X, X - \alpha)/(Y^2 - X)\right) \cong$$
$$\underset{2.8 \text{ i)}}{\cong} \mathbb{C}[X,Y]/(Y^2 - X, X - \alpha) \cong$$
$$\cong \left(\mathbb{C}[X,Y]/(X - \alpha)\right)/(Y^2 - \underbrace{\overline{X}}_{=\alpha}) \cong \mathbb{C}[Y]/(Y^2 - \alpha) \cong$$
$$\cong \begin{cases} \mathbb{C}[Y]/(Y - \sqrt{\alpha})(Y + \sqrt{\alpha}) \cong \mathbb{C} \times \mathbb{C} & \alpha \neq 0 \\ \mathbb{C}[Y]/Y^2 & \alpha = 0 \end{cases}$$

Für 2.8 ii)

$$M_2/M_1 \cap M_2 \xrightarrow{\sim} M_1 + M_2/M_1$$

verwende hier

$$M_1 := \left(Y^2 - X\right) \qquad M_2 := (X - \alpha)$$

und beachte

$$M_1 \cap M_2 = \left(Y^2 - X\right) \cdot (X - \alpha) = M_1 \cdot M_2 \qquad M_1 + M_2 = \left(Y^2 - X, X - \alpha\right)$$

und für 2.8 i)

$$\left(L/M\right)/\left(N/M\right) \cong L/N$$

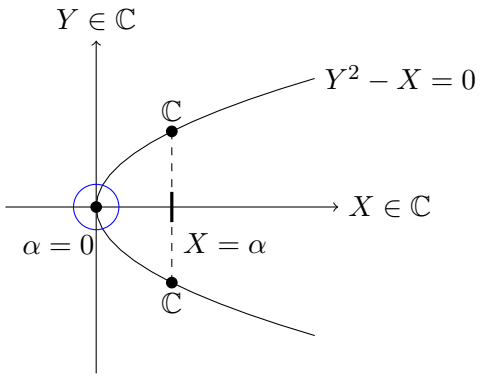
verwende hier:

$$L := \mathbb{C}[X,Y] \qquad M := \left(Y^2 - X\right) \qquad N := \left(Y^2 - X, X - \alpha\right)$$

Beachte:

$$\mathfrak{N}(\mathbb{C} \times \mathbb{C}) = (0)$$
$$\mathfrak{N}\left(\mathbb{C}[Y]/Y^2\right) = (Y) \neq (0)$$

Skizze:



4 Ganze Ringerweiterungen

4.1 Definition (ganz)

Ein Ringhomomorphismus $f : A \to B$ (und die A-Algebra B) heißt genau dann *ganz*, wenn für alle $b \in B$ ein $n \in \mathbb{N}_{\geq 1}$ und $a_0, \ldots, a_{n-1} \in A$ mit

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

existieren, das heißt es existiert ein normiertes $f \in A[X]$ mit $f(b) = 0$.
(Vergleiche mit algebraischen Körpererweiterungen aus der Algebra.)

4.2 Bemerkung und Definition (Ringerweiterung)

i) $f : A \to B$ ist genau dann ganz, wenn die Inklusion $f(A) \subseteq B$ ganz ist.

ii) Eine *Ringerweiterung* ist ein Ring B zusammen mit einem Unterring $A \subseteq B$ oder äquivalent ein injektiver Ringhomomorphismus.

Eine Ringerweiterung heißt *ganz*, falls die Inklusion $A \subseteq B$ ganz ist.

iii) Ist k ein Körper, so gilt für eine k-Algebra B:

B ist eine ganze k-Algebra. $\Leftrightarrow$ B ist algebraisch über k.

Beweis

„$\Rightarrow$“: Ganz bedeutet, dass es für alle $b \in B$ ein normiertes Polynom $f \in k[X]$ mit $f(b) = 0$ gibt. Algebraisch heißt, dass es für alle $b \in B$ ein (nicht notwendig normiertes) Polynom $f \in k[X] \setminus \{0\}$ mit $f(b) = 0$ gibt.

Dies ist offenbar erfüllt, da das Nullpolynom nicht normiert ist.

„$\Leftarrow$“: Sei $b \in B$, so gibt es ein $f \in k[X] \setminus \{0\}$ mit $f(b) = 0$. Schreibe mit geeigneten $a_i \in k$ für $i \in \{0, \ldots, n\}$ und $a_n \neq 0$:

$$f(X) = a_n X^n + \ldots + a_0$$

Also gilt:

$$\left(a_n^{-1} f\right)(b) = a_n^{-1} \cdot f(b) = 0$$

Da $a_n^{-1} f \in k[X]$ normiert ist, ist b ganz über k. $\square_{\text{iii)}}$

4.3 Definition (ganz abgeschlossen, normal)

Sei $A \subseteq B$ eine Ringerweiterung.

i) Ein Element $b \in B$ heißt genau dann *ganz über* A, wenn ein normiertes $f \in A[X]$ mit $f(b) = 0$ existiert.

ii) $A \subseteq B$ heißt genau dann *ganz abgeschlossen*, falls gilt:

$$\{b \in B \mid b \text{ ist ganz über } A\} = A$$

(„$\supseteq$“ gilt immer!)

iii) Ein Integritätsring A heißt genau dann *ganz abgeschlossen* (oder *normal*), wenn die Ringerweiterung $A \subseteq \mathrm{Quot}(A)$ ganz abgeschlossen ist.

4.4 Proposition ($\mathbb{Z}$ ist normal)

$\mathbb{Z}$ ist normal.

Beweis

Nach 4.3 iii) und ii) ist zu zeigen: Ist $x \in \mathbb{Q}$ ganz über $\mathbb{Z}$, so ist $x \in \mathbb{Z}$.
Sei also $x \in \mathbb{Q}$ ganz über $\mathbb{Z}$. Schreibe $x = \frac{a}{b}$ mit $a,b \in \mathbb{Z}$ und $\mathrm{ggT}(a,b) = 1$.
Da x ganz über $\mathbb{Z}$ ist, gibt es geeignete $a_i \in \mathbb{Z}$ mit:

$$\begin{aligned} 0 &= x^n + a_{n-1}x^{n-1} + \ldots + a_0 = \frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \ldots + a_0 \qquad / \cdot b^n \\ 0 &= a^n + (ba_{n-1})\,a^{n-1} + \ldots + (b^n a_0) \\ a^n &= -b\left(a_{n-1}a^{n-1} + \ldots + b^{n-1}a_0\right) \end{aligned}$$

Angenommen es existiert eine Primzahl $p \in \mathbb{Z}$ mit $p|b$, so folgt $p|a^n$ und somit $p|a$, da p eine Primzahl ist. Dies ist ein Widerspruch, da a und b teilerfremd sind. Also gilt $b \in \mathbb{Z}^* = \{\pm 1\}$ und es folgt:

$$x = \frac{a}{b} = \pm a \in \mathbb{Z}$$

$\square_{4.4}$

4.5 Bemerkung

i) Für alle $\alpha \in \mathbb{Q}$ gibt es ein $f \in \mathbb{Z}[X] \setminus \{0\}$ mit $f(\alpha) = 0$, denn für $\alpha = \frac{a}{b}$ gilt:

$$(bX - a)(\alpha) = 0$$

Aber $bX - a$ ist nicht normiert.

ii) 4.4 gilt mit demselben Beweis allgemeiner für alle faktoriellen Ringe anstelle von $\mathbb{Z}$, zum Beispiel für $k[X_1, \ldots, X_n]$ mit einem Körper k und $n \in \mathbb{N}$, das heißt faktorielle Ringe sind normal.

$\mathbf{i}, \sqrt{5}, \sqrt{7}, \sqrt{11} \in \mathbb{C}$ sind ganz über $\mathbb{R}$, mit den Minimalpolynomen $X^2 + 1$, $X^2 - 5$, $X^2 - 7$ und $X^2 - 11$. Was ist mit $\mathbf{i} + \sqrt{5}$ oder $\mathbf{i} + \sqrt{5} + \sqrt{7} - \sqrt{11}$?

4.6 **Proposition** (Charakterisierung von ganz)

Sind $A \subseteq B$ eine Ringerweiterung und $b \in B$ ein Element, so sind äquivalent:

i) b ist ganz über A.

ii) Die von b erzeugte A-Unteralgebra $A \subseteq A[b] \subseteq B$ ist endlich.

iii) Es existiert ein Ring C mit $A \subseteq C \subseteq B$ und $b \in C$, der endlich über A ist.

Beweis

„i) $\Rightarrow$ ii)“: Betrachte den Einsetzungshomomorphismus:

$$\begin{aligned} \varphi : A[X] &\to B \\ X &\mapsto b \end{aligned}$$

Nun gilt:

$$A[b] = \operatorname{im}(\varphi) \cong A[X]/\ker(\varphi)$$

Da b ganz über A ist, existiert ein normiertes $f \in A[X]$ mit $f(b) = 0$, das heißt $(f) \subseteq \ker(\varphi)$ und

$$A[b] \cong A[X]/\ker(\varphi) \overset{\overline{\mathrm{id}}}{\twoheadleftarrow} A[X]/(f)$$

ist ein Quotient des A-Moduls $A[X]/(f)$.
Ist $n := \deg(f)$, so folgt aus Division mit Rest durch das normierte (!) Polynom f, dass $A[X]/(f)$ ein freier A-Modul mit Basis $\left\{\overline{X}^i\right\}_{0 \le i \le n-1}$ ist. Also ist mit $A[X]/(f)$ auch der Quotient $A[X]/\ker(\varphi) \cong A[b]$ endlich, das heißt die A-Algebra $A[b]$ ist endlich. $\square_{\text{i)} \Rightarrow \text{ii)}}$
„ii) $\Rightarrow$ iii)“: Wähle $C := A[b]$.
„iii) $\Rightarrow$ i)“: Die Abbildung

$$\begin{aligned} \varphi : C &\to C \\ c &\mapsto bc \end{aligned}$$

ist A-linear. Nach dem Satz von Cayley-Hamilton 2.11 existiert ein normiertes $f \in A[X]$ mit $f(\varphi) = 0$ in $\operatorname{End}_A(C)$. Es folgt in B:

$$f(b) = f(\varphi)(1) = 0$$

Also ist b ganz über A. $\square_{4.6}$

4.7 **Bemerkung** (Beziehung zwischen endlich und ganz)

Wegen 4.6 „iii) $\Rightarrow$ i)“ ist jede endliche Ringerweiterung ganz.
Die Umkehrung gilt im Allgemeinen nicht. Eine Ringerweiterung genau dann ganz ist, wenn sie Vereinigung ihrer endlichen Teilerweiterungen ist:

Seien $A \subseteq B$ eine Ringerweiterung.

$$M := \{C \subseteq B \mid C \text{ ist endliche } A\text{-Algebra}\}$$
$$V := \bigcup_{C \in M} C$$

$A \subseteq B$ ist genau dann ganz, wenn B die Vereinigung aller endlichen A-Unteralgebren von B ist, in Zeichen:

$$A \subseteq B \text{ ganz} \quad \Leftrightarrow \quad B = V$$

Beweis

„⇒“: Sei $A \subseteq B$ ganz. Dann ist jedes $b \in B$ ganz über A. Daher ist die A-Unteralgebra $A[b] \subseteq B$ endlich und es gilt $b \in A[b]$. Somit folgt $A[b] \in M$ und es gilt für alle $\tilde{b} \in B$:

$$\tilde{b} \in A\left[\tilde{b}\right] \subseteq \bigcup_{b \in B} A[b] \subseteq \bigcup_{C \in M} C = V \subseteq B$$

Also folgt $B \subseteq V \subseteq B$ und somit $B = V$.
„⇐“: Sei $B = V$. Dann gilt für alle $b \in B$ schon:

$$b \in V = \bigcup_{C \in M} C$$

Also gibt es ein $C \in M$ mit $b \in C$. Da $A \subseteq C \subseteq B$ gilt und C endlich ist, folgt, dass b ganz über A ist. Da dies für alle $b \in B$ gilt, ist $A \subseteq B$ ganz. $\square_{4.7}$

4.8 Korollar

Seien $A \subseteq B$ eine Ringerweiterung, $n \in \mathbb{N}_{\geq 1}$ und $b_1, \ldots, b_n \in B$ ganz über A. Dann ist die A-Algebra $A[b_1, \ldots, b_n]$ endlich.

Beweis

Induktion über n:

Induktionsanfang bei $n = 1$: 4.6 i) ⇒ ii).

Induktionsschritt $n - 1 \rightsquigarrow n$: Schreibe $A \subseteq A_r := A[b_1, \ldots, b_r] \subseteq B$ für $1 \leq r \leq n$.

Nach Induktionsvoraussetzung ist A_{n-1} eine endliche A-Algebra. Da b_n ganz über A ist, ist b_n auch ganz über A_{n-1}, denn es gilt $A \subseteq A_{n-1}$ und somit ist jedes $f \in A[X]$ schon Element von $A_{n-1}[X]$.

Also ist A_n eine endliche A_{n-1}-Algebra nach 4.6 i) ⇒ ii) für $(A \subseteq B) := (A_{n-1} \subseteq A_n)$.

Wegen 2.33 i) für $B := A_{n-1}$ und den B-Modul $N := A_n$ ist A_n eine endliche A-Algebra.

$$A \overset{\text{endlich}}{\subseteq} A_{n-1} \overset{\text{endlich}}{\subseteq} A_n$$

$$\Rightarrow \quad A \overset{\text{endlich}}{\subseteq} A_n$$

$\square_{4.8}$

4.9 Korollar und Definition (ganzer Abschluss)

Ist $A \subseteq B$ eine Ringerweiterung, so ist

$$A \subseteq C := \left\{ b \in B \middle| b \text{ ganz über } A \right\} \subseteq B$$

eine A-Unteralgebra, *der ganze Abschluss von A in B*. Schreibweise:

$$\overline{A}^B := C$$

Zum Beispiel ist $\overline{A}^A = A$.

Beweis

Für $a \in A$ ist

$$f(X) := X - a \in A[X]$$

normiert und erfüllt $f(a) = 0$. Es folgt $A \subseteq C$. Wegen $1{,}0 \in A \subseteq C$ ist nur noch die Stabilität von C unter Addition und Multiplikation zu zeigen:
Seien also $x,y \in C$. Wegen 4.8 ist $A \subset A[x,y]$ eine endliche A-Algebra, also ganz, und es folgt $C \supseteq A[x,y] \ni x - y, xy$. $\square_{4.9}$

4.10 Beispiel

Der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}[\mathbf{i}]$ ist $\mathbb{Z}[\mathbf{i}]$.

$$\begin{array}{ccccc} \mathbb{Z}[\mathbf{i}] & \subsetneq & \mathbb{Z}[\mathbf{i}] & \hookrightarrow & \mathbb{Q}[\mathbf{i}] \\ & \nwarrow & \uparrow & & \uparrow \\ & & \mathbb{Z}[\mathbf{i}] & \hookrightarrow & \mathbb{Q} \end{array}$$

Beweis

„$\supseteq$“: Für $x = a + b\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$ mit geeigneten $a,b \in \mathbb{Z}$ gilt in $\mathbb{Z}[\mathbf{i}][X]$:

$$f(X) := (X - x)(X - \overline{x}) = X^2 - (x + \overline{x})X + (x\overline{x}) = X^2 - (2a)X + \left(a^2 + b^2\right)$$

Also ist $f \in \mathbb{Z}[X]$ normiert und $f(x) = 0$. Also ist x ganz über $\mathbb{Z}$.
„$\subseteq$“: Sei $x = a + b\mathbf{i} \in \mathbb{Q}[\mathbf{i}]$ mit geeigneten $a,b \in \mathbb{Q}$ ganz über $\mathbb{Z}$. Zu zeigen ist $a,b \in \mathbb{Z}$.
Es existiert ein normiertes $f \in \mathbb{Z}[X]$ mit $f(x) = 0$ und es folgt:

$$0 = \overline{f(x)} = \overline{f}(\overline{x}) \overset{f \in \mathbb{Z}[X]}{=} f(\overline{x})$$

Also ist $\overline{x}$ ganz über $\mathbb{Z}$. Wegen 4.9 sind dann auch $x + \overline{x} = 2a \in \mathbb{Q}$ und $x \cdot \overline{x} = a^2 + b^2 \in \mathbb{Q}$ ganz über $\mathbb{Z}$.
Da $\mathbb{Z}$ nach 4.4 normal ist, folgen $a' := 2a \in \mathbb{Z}$ und $z := a^2 + b^2 \in \mathbb{Z}$. Schreibe

$$a = \frac{a'}{2} \qquad\qquad b = \frac{c}{d}$$

mit $c,d \in \mathbb{Z}$, $\mathrm{ggT}\,(c,d) = 1$ und $d > 0$. Es folgt:

$$z = a^2 + b^2 = \frac{(a')^2}{4} + \frac{c^2}{d^2} = \frac{(a')^2 d^2 + 4c^2}{4d^2} \in \mathbb{Z}$$

Daher ist 4 ein Teiler von $(a')^2 d^2$ und somit gilt $2|a'$ oder $2|d$.

1. Fall: Aus $2|a'$ folgt $a = \frac{a'}{2} \in \mathbb{Z}$ und somit ist $b^2 = z - a^2 \in \mathbb{Z}$, also ist $b \in \mathbb{Q}$ ganz über $\mathbb{Z}$ mit dem Polynom $X^2 - b^2 \in \mathbb{Z}[X]$. Da $\mathbb{Z}$ normal ist, folgt $b \in \mathbb{Z}$.

2. Fall: Für $2|d$ schreibe $d = 2d'$ mit geeignetem $d' \in \mathbb{Z}$. Es gilt:

$$\mathbb{Z} \ni z = a^2 + b^2 = \frac{(a')^2}{4} + \frac{c^2}{4(d')^2} = \frac{1}{4}\left((a')^2 + \frac{c^2}{(d')^2}\right) \overset{a' \in \mathbb{Z}}{\Rightarrow} \frac{c^2}{(d')^2} \in \mathbb{Z}$$

Wegen $\mathrm{ggT}\,(c,d) = 1$ gilt auch $\mathrm{ggT}\left(c^2, (d')^2\right) = 1$ und somit $(d')^2 \in \mathbb{Z}^*$, also $(d')^2 = 1$. Mit $d > 0$ folgt $d' > 0$, also $d' = 1$. Dann gilt $4\mathbb{Z} \ni (a')^2 + c^2$. Wegen

$$\left(\mathbb{Z}/4\mathbb{Z}\right)^2 := \left\{x^2 | x \in \mathbb{Z}/4\mathbb{Z}\right\} = \{\overline{0},\overline{1}\}$$

folgt aus

$$(a')^2 + c^2 \equiv 0 \mod 4$$

schon:

$$\begin{aligned} (a')^2 \equiv c^2 &\equiv 0 \mod 4 \\ \Rightarrow \quad a' \equiv c &\equiv 0 \mod 2 \end{aligned}$$

Insbesondere gilt $2|a'$ und damit $a,b \in \mathbb{Z}$ nach Fall 1.

$\square_{4.10}$

4.11 **Korollar** (Transitivität der Ganzheit)

Seien $A \subseteq B$ eine ganze Ringerweiterung, $B \subseteq C$ eine Ringerweiterung und $x \in C$ ganz über B, so ist x ganz über A.

Beweis

Da x ganz über B ist, gilt für ein $n \in \mathbb{N}$ und geeignete $b_0, \ldots, b_{n-1} \in B$:

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0$$

Also ist x ganz über $A' := A[b_0, \ldots, b_{n-1}]$ und $A'[x]$ ist endlich über A' nach 4.6 i) $\Rightarrow$ ii).
Nach 4.8 ist A' endlich über A und es folgt aus der Transitivität der Endlichkeit 2.33 i), dass $A'[x]$ endlich über A ist. Also folgt aus 4.6 iii) $\Rightarrow$ i) mit $C := A'[x]$, dass x ganz über A ist.

4.12 **Korollar** (ganzer Abschluss ist ganz abgeschlossen)

Sind $A \subseteq B$ eine Ringerweiterung und $A \subseteq C := \overline{A}^B \subseteq B$ der ganze Abschluss von A in B, so ist $C \subseteq B$ ganz abgeschlossen, in Zeichen:

$$\overline{\left(\overline{A}^B\right)}^B = \overline{A}^B$$

Beweis

Ist x in B ganz über C, so ist x nach 4.11 auch ganz über A, denn $A \subseteq C$ ist ganz. Somit folgt $x \in C$. $\square_{4.12}$

4.13 **Proposition** (ganz stabil unter Quotientenbildung und Basiswechsel)

Sei $A \subseteq B$ eine ganze Ringerweiterung.

i) Ist $J \subseteq B$ ein Ideal, so ist ${}^{A}\!/_{J \cap A} \subseteq {}^{B}\!/_{J}$ eine ganze Ringerweiterung.

$$\begin{array}{ccc} A & \xhookrightarrow{\quad\iota\quad} & B \\ \downarrow & & \downarrow \pi \\ {}^{A}\!/_{(J \cap A)} & \xrightarrow{\ker(\pi \circ \iota) = J \cap A} & {}^{B}\!/_{J} \end{array}$$

ii) Ist $A \to C$ eine A-Algebra, so ist der Basiswechsel

$$\begin{aligned} f : C &\to C \otimes_A B \\ c &\mapsto c \otimes 1 \end{aligned}$$

eine ganze C-Algebra.

iii) Ist $I \subseteq A$ ein Ideal, so ist

$${}^{A}\!/_{I} \to {}^{B}\!/_{BI}$$

ganz.

Beweis

i) Ist $x \in {}^{B}\!/_{J}$, so existiert ein $b \in B$ mit $x = b + J$. Da $A \subseteq B$ ganz ist, existiert ein normiertes Polynom $f \in A[X]$ mit $f(b) = 0$ in B. Es folgt in ${}^{B}\!/_{J}$:

$$0 = \overline{f(b)} = \overline{f}(b + J) = \overline{f}(x)$$

Dabei ist $\overline{f} \in \left({}^{A}\!/_{A \cap J}\right)[X]$ normiert. Also ist $x = b + J$ ganz über ${}^{A}\!/_{A \cap J}$. $\square_{\text{i)}}$

ii) Da die Summe ganzer Elemente nach 4.3 ganz ist, genügt es zu zeigen, dass jeder elementare Tensor $c \otimes b \in C \otimes_A B$ ganz über C ist. Wegen4.6 i) $\Rightarrow$ ii) ist $A \subseteq A[b]$ endlich. Also ist nach 2.33 ii) auch der Basiswechsel $C \to C_A A[b]$ ein endlicher C-Modul. Damit ist das Bild $\operatorname{im}(\varphi) \subseteq C \otimes_A B$ der C-linearen Abbildung

$$\varphi : \mathrm{id}_C \otimes (A[b] \hookrightarrow B) : C \otimes_A A[b] \to C \otimes_A B$$

ein endlich erzeugter C-Modul, der offenbar $c = c \otimes b$ enthält. Also ist x ganz über C nach 4.6 iii) $\Rightarrow$ i). $\square_{\text{ii)}}$

iii) Wähle in ii) $A \twoheadrightarrow C := {}^{A}\!/_{I}$ und beachte die Rechenregeln für das Tensorprodukt.

$$C = {}^{A}\!/_{I} \to C \otimes_A B = {}^{A}\!/_{I} \otimes_A B \cong {}^{B}\!/_{IB}$$

$\square_{\text{iii)}}$

4.14 **Korollar** (ganz stabil unter Lokalisierung)

Sind $A \subseteq B$ eine ganze Ringerweiterung und $S \subseteq A$ multiplikativ abgeschlossen, so ist auch die Ringerweiterung $S^{-1}A \subseteq S^{-1}B$ ganz.

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ C = S^{-1}A & \overset{\text{ganz}}{\hookrightarrow} & S^{-1}A \otimes_A B \cong S^{-1}B \end{array}$$

Beweis

Nach 3.6 ist die Lokalisierung exakt und somit $S^{-1}A \hookrightarrow S^{-1}A \otimes_A B$ injektiv, also eine Ringerweiterung. Nach 3.8 gilt:

$$S^{-1}A \otimes_A B \cong S^{-1}B$$

Nach 4.13 ii) mit $C := S^{-1}A$ ist also die Ringerweiterung $S^{-1}A \subseteq S^{-1}B$ ganz. $\square_{4.14}$

4.15 **Proposition**

Sind $A \subseteq B$ eine ganze Ringerweiterung von Integritätsringen, so sind äquivalent.

i) A ist ein Körper.

ii) B ist ein Körper.

Beweis

„i) ⇒ ii)“: Zu zeigen ist $B \setminus \{0\} \subseteq B^*$.
Sei $0 \neq b \in B$, so gibt es ein minimales $n \in \mathbb{N}$ und geeignete $a_0, \ldots, a_{n-1} \in A$ mit:

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

Damit folgt:

$$-a_0 = b \cdot \underbrace{\left(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1\right)}_{=:c} \in B$$

Wäre $a_0 = 0$, so folgte aus $b \neq 0$, weil B ein Integritätsring ist, dass $c = 0$ ist. Dies ist ein Widerspruch zur Minimalität von n.
Also gilt $a_0 \neq 0$ und wegen i) gilt $a_0 \in A^* \subseteq B^*$. Es folgt:

$$b \cdot (-a_0)^{-1} \cdot c = 1 \in B$$

Daher ist $b \in B^*$. $\square_{\text{i) ⇒ ii)}}$

„ii) ⇒ ii)“: Zu zeigen ist $A \setminus \{0\} \subseteq A^*$.
Sei $0 \neq a \in A$, so folgt aus ii) schon $a \in B^*$, das heißt es existiert ein $b \in B$ mit:

$$ab = 1 \in B$$

Zeige nun $b \in A$, womit

$$ab = 1 \in A$$

folgt. Da $A \subseteq B$ ganz ist, gibt es ein $n \in \mathbb{N}$ und geeignete $a_i \in A$ mit:

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

Es folgt:

$$b \overset{ab=1}{=} b^n a^{n-1} = -\left(a_{n-1}\underbrace{b^{n-1}a^{n-1}}_{=1} + a_{n-2}\underbrace{b^{n-2}a^{n-1}}_{=a} + \ldots + a_0 a^{n-1}\right) \in A$$

$\square_{4.15}$

4.16 Korollar

Seien $A \subseteq B$ eine ganze Ringerweiterung und $\mathfrak{q} \subseteq B$ ein Primideal, so betrachte das Primideal $\mathfrak{p} := A \cap \mathfrak{q} \subseteq A$. Dann ist $\mathfrak{q} \subseteq B$ genau dann maximal, wenn $\mathfrak{p} \subseteq A$ maximal ist.

Beweis

$A/\mathfrak{p} \subseteq B/\mathfrak{q}$ ist nach 4.13 i) eine ganze Ringerweiterung von Integritätsringen (nach 1.18 i)), also gilt:

$$\mathfrak{q} \subseteq B \text{ maximal} \overset{1.18\text{ ii)}}{\Leftrightarrow} B/\mathfrak{q} \text{ Körper} \overset{4.15}{\Leftrightarrow} A/\mathfrak{p} \text{ Körper} \overset{1.18\text{ ii)}}{\Leftrightarrow} \mathfrak{p} \subseteq A \text{ maximal}$$

$\square_{4.16}$

4.17 Beispiel

i) Die Erweiterung $\mathbb{Z} \subseteq \mathbb{Z}[\mathbf{i}]$ ist nach 4.10 ganz.

$\mathbb{Z}[\mathbf{i}]$ ist ein Hauptidealring, also ist jedes von Null verschiedene Primideal $(0) \neq \mathfrak{p} \subseteq \mathbb{Z}[\mathbf{i}]$ maximal.

Aus 4.16 folgt, dass $\mathfrak{p} \cap \mathbb{Z} \subseteq \mathbb{Z}$ maximal ist, das heißt es gilt $\mathfrak{p} \cap \mathbb{Z} = (p)$ für eine Primzahl p und *nicht* $\mathfrak{p} \cap \mathbb{Z} = (0)$. (vergleiche 2.49)

ii) Für die Erweiterung $A := \mathbb{Z} \subseteq B := \mathbb{Q}$ ist $\mathfrak{q} := (0)$ in B maximal, aber $\mathfrak{q} \cap A = (0) \subseteq \mathbb{Z}$ ist nicht maximal. Also kann man auf die Voraussetzung ganz nicht verzichten. ($\mathbb{Z} \subseteq \mathbb{Q}$ ist nach 4.10 nicht ganz.)

4.18 Korollar

Seien $A \subseteq B$ eine ganze Ringerweiterung, $\mathfrak{q} \subseteq \mathfrak{q}' \subseteq B$ Primideale, und es gelte $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Dann folgt $\mathfrak{q} = \mathfrak{q}'$. (Dies ist klar, wenn $\mathfrak{q} \cap A$ maximal ist.)

$$\begin{array}{ccccc} \mathfrak{q} & \subseteq & \mathfrak{q}' & \subseteq & B \\ & \diagdown & \diagup & & \mid \text{ganz} \\ & & \mathfrak{p} & \subseteq & A \end{array}$$

Beweis

Für $\mathfrak{p} := \mathfrak{q} \cap A \subseteq A$ ist $A_\mathfrak{p} \subseteq B_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1} B$ eine ganze Ringerweiterung, da nach 3.6 Lokalisieren exakt ist und nach 4.14 Ganzheit erhält. Nach 3.19 iv) sind

$$\mathfrak{q}_1 := \mathfrak{q} B_\mathfrak{p} \subseteq \mathfrak{q}_2 := \mathfrak{q}' B_\mathfrak{p}$$

Primideale, denn aus $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$ folgt:

$$\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset = \mathfrak{q}' \cap (A \setminus \mathfrak{p})$$

Weiter ist

$$\mathfrak{q}_1 \cap A_\mathfrak{p} = (\mathfrak{q} B_\mathfrak{p}) \cap A_\mathfrak{p} = (\mathfrak{q} \cap A)\, A_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p} \subseteq A_\mathfrak{p}$$

maximal nach 3.4 i). Ebenso folgt $\mathfrak{q}_2 \cap A_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$ und aus 4.16 folgt nun, dass $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq B_\mathfrak{p}$ beide maximal sind, also gilt $\mathfrak{q}_1 = \mathfrak{q}_2$ und es folgt:

$$\mathfrak{q} \overset{3.19\ \text{i)}}{=} (\mathfrak{q} B_\mathfrak{p}) \cap B = \mathfrak{q}_1 \cap B = \mathfrak{q}_2 \cap B = \left(\mathfrak{q}' B_\mathfrak{p}\right) \cap B \overset{3.19\ \text{i)}}{=} \mathfrak{q}'$$

$\square_{4.18}$

4.19 Beispiel

i) Seien $A = k$ ein Körper und $k = A \subseteq B := k[X]$. Dann sind $\mathfrak{q} := (0) \subsetneq \mathfrak{q}' := (X)$ Primideale mit $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = (0)$. Die Erweiterung $k \subseteq k[X]$ ist nicht ganz.

$$\begin{array}{ccccc} (0) & \subsetneq & (X) & \subseteq & k[X] \\ & \diagdown & \diagup & & | \\ & & (0) & \subseteq & k \end{array}$$

ii) Die Ringerweiterung $A := \mathbb{Z} \subseteq B := \mathbb{Z}[\mathbf{i}]$ ist ganz. $\mathfrak{q} := (1+2\mathbf{i}) \subseteq B$ und $\mathfrak{q}' := (1-2\mathbf{i}) \subseteq B$ sind Primideale mit $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = (5) \subseteq \mathbb{Z}$, aber es gilt $\mathfrak{q} \neq \mathfrak{q}'$ und weder $\mathfrak{q} \subseteq \mathfrak{q}'$ noch $\mathfrak{q}' \subseteq \mathfrak{q}$.

$$\begin{array}{ccccc} \mathfrak{q} & \neq & \mathfrak{q}' & \subseteq & \mathbb{Z}[\mathbf{i}] \\ & \diagdown & \diagup & & | \text{ ganz} \\ & & (5) & \subseteq & \mathbb{Z} \end{array}$$

4.20 Satz

Seien $\iota : A \subseteq B$ eine ganze Ringerweiterung und $\mathfrak{p} \subseteq A$ ein Primideal. Dann existiert ein Primideal $\mathfrak{q} \subseteq B$ mit $\mathfrak{p} = \mathfrak{q} \cap A$.
(Äquivalent: Die Abbildung $\operatorname{Spec}(\iota) : \operatorname{Spec}(B) \twoheadrightarrow \operatorname{Spec}(A)$ ist surjektiv.)

Beweis

Betrachte folgendes kommutatives Diagramm von Ringen:

$$\begin{array}{ccc} A & \xhookrightarrow{\iota} & B \\ {\scriptstyle \iota_A^{(A_\mathfrak{p})}}\downarrow & & {\scriptstyle \iota_B^{(A_\mathfrak{p})}}\downarrow \\ A_\mathfrak{p} & \xhookrightarrow{\iota_\mathfrak{p}} & B_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1} B \end{array}$$

Wegen $A_\mathfrak{p} \neq (0)$, da $0 \in \mathfrak{p}$ ist $B_\mathfrak{p} \neq (0)$, also existiert nach dem Lemma von Zorn ein maximales Ideal $\mathfrak{m} \subseteq B_\mathfrak{p}$.
Da $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ nach 4.14 ganz ist, ist $\iota_\mathfrak{p}^{-1}(\mathfrak{m}) \subseteq A_\mathfrak{p}$ nach 4.16 maximal.
Da $A_\mathfrak{p}$ lokal ist, folgt $\iota_\mathfrak{p}^{-1}(\mathfrak{m}) = \mathfrak{p}A_\mathfrak{p} \subseteq A_\mathfrak{p}$. Nun ist

$$\mathfrak{q} := \left(\iota_B^{(A\setminus\mathfrak{p})}\right)^{-1}(\mathfrak{m}) \subseteq B$$

ein Primideal mit:

$$\mathfrak{q} \cap A = \left(\iota_A^{(A\setminus\mathfrak{p})}\right)^{-1}\left(\iota_\mathfrak{p}^{-1}(\mathfrak{m})\right) = \left(\iota_A^{(A\setminus\mathfrak{p})}\right)^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$$

$\square_{4.20}$

4.21 Satz („Going-up theorem“)

Seien $A \subseteq B$ eine ganze Ringerweiterung, $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ldots \subseteq \mathfrak{p}_n \subseteq A$ Primideale, $0 \leq m < n$ und $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m \subseteq B$ Primideale mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.
Dann existieren Primideale $\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \ldots \subseteq \mathfrak{q}_n \subseteq B$ mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle Indizes $i \in \{m+1, \ldots, n\}$.
Skizze:

$$\begin{array}{ccccccccccc} \mathfrak{q}_1 & \subseteq & \ldots & \subseteq & \mathfrak{q}_m & \subseteq & \mathfrak{q}_{m+1} & \subseteq & \ldots & \subseteq & \mathfrak{q}_n & \subseteq & B \\ | & & & & | & & | & & & & | & & \uparrow \text{ganz} \\ \mathfrak{p}_1 & \subseteq & \ldots & \subseteq & \mathfrak{p}_m & \subseteq & \mathfrak{p}_{m+1} & \subseteq & \ldots & \subseteq & \mathfrak{p}_n & \subseteq & A \end{array}$$

Beweis

Der Fall $m = 0$ und $n = 1$ folgt aus 4.20. Durch Induktion kann man $m = 1$ und $n = 2$ angenommen werden, das heißt:

$$\begin{array}{ccccc} \mathfrak{q}_1 & \subseteq & \mathfrak{q}_2 & \subseteq & B \\ | & & | & & \uparrow \text{ganz} \\ \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 & \subseteq & A \end{array}$$

Die Ringerweiterung $\overline{A} := {}^{A}\!/_{\mathfrak{p}_1} \subseteq \overline{B} := {}^{B}\!/_{\mathfrak{q}_1}$ ist wegen $\mathfrak{p}_1 = A \cap \mathfrak{q}_1$ nach 4.13 i) ganz.
Wegen 4.20 existiert ein Primideal $\overline{\mathfrak{q}_2} \subseteq \overline{B}$ mit $\overline{\mathfrak{q}_2} \cap \overline{A} = \overline{\mathfrak{p}_2} := {}^{\mathfrak{p}_2}\!/_{\mathfrak{p}_1} \subseteq \overline{A}$.
Das Urbild $\mathfrak{q}_2 := \left(B \twoheadrightarrow \overline{B}\right)^{-1}(\overline{\mathfrak{q}_2}) \subseteq B$ ist ein Primideal mit:

$$\mathfrak{q}_2 \cap A = \left(A \twoheadrightarrow \overline{A}\right)^{-1}(\overline{\mathfrak{p}_2}) = \mathfrak{p}_2$$

$\square_{4.21}$

5 Der Hilbertsche Nullstellensatz

5.1 Beispiel

Algebra	Geometrie
$\mathbb{C}[X]$	$\mathbb{C} = \mathbb{R} \oplus \mathbf{i}\mathbb{R} \tilde{=} \mathbb{R}^2$
$\mathbb{C}[X] \ni f \longmapsto$	$\mathcal{N}(f) := \{z \in \mathbb{C} \mid f(z) = 0\}$
$\mathbb{C}[X] \supseteq \{f \in \mathbb{C}[X] \mid \forall_{x \in M} f(x) = 0\} =: I(M) \longmapsfrom$	$M \subseteq \mathbb{C}$

Allgemeiner: Sei $I \subseteq \mathbb{C}[X]$ ein Ideal, so ist die Nullstellenmenge:

$$\mathcal{N}(I) := \left\{ z \in \mathbb{C} \,\middle|\, \underset{f \in I}{\forall} \; f(z) = 0 \right\}$$

Dann gilt $\mathcal{N}(f) = \mathcal{N}((f))$.
Man sieht leicht:

- Ist $M \subseteq \mathbb{C}$ unendlich, so gilt:

$$I(M) = (0)$$

- Ist $M = \{z_1, \ldots, z_n\} \subseteq \mathbb{C}$ endlich, so gilt:

$$I(M) = \left(\prod_{i=1}^{n} (X - z_i) \right)$$

Es folgt:

$$\mathcal{N}(I(M)) = \begin{cases} M & \text{falls } M \text{ endlich} \\ \mathbb{C} & \text{falls } M \text{ unendlich} \end{cases}$$

Nach 3.28 ist also $\mathcal{N}(I(M))$ genau der Abschluss von M in der Zariski-Topologie auf:

$$\begin{aligned} \operatorname{MaxSpec}(\mathbb{C}[X]) := \{\mathfrak{m} \subseteq \mathbb{C}[X] \mid \mathfrak{m} \text{ ist maximles Ideal}\} &\tilde{=} \mathbb{C} \\ X - \alpha &\mapsto \alpha \end{aligned}$$

Sei $f \in \mathbb{C}[X]$. Für $f = 0$ gilt:

$$I(\mathcal{N}((0))) = I(\mathbb{C}) = (0)$$

Sei $f \in \mathbb{C}[X]^* = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$, so gilt:

$$I(\mathcal{N}((f))) = I(\emptyset) = (1) = (f)$$

Andernfalls betrachte die Primfaktorzerlegung von f:

$$f(X) = \alpha \cdot \prod_{i=1}^{n} (X - z_i)^{n_i}$$

Dabei sind $\alpha \in \mathbb{C}^*$, $n \in \mathbb{N}_{\geq 1}$, $z_i \in \mathbb{C}$ und $n_i \in \mathbb{N}_{\geq 1}$ geeignet gewählt.
Dann gilt $\mathcal{N}((f)) = \{z_1, \ldots, z_n\}$, also folgt:

$$I(\mathcal{N}((f))) = \left(\prod_{i=1}^{n} (X - z_i) \right) = \sqrt{(f)}$$

Denn ist $g \in (\prod_{i=1}^{n} (X - z_i))$, so folgt mit $m := \max\{n_i | 1 \leq i \leq n\}$ schon $g^m \in (f)$, also $g \in \sqrt{(f)}$.
Ist hingegen $g \in \sqrt{(f)}$, so gibt es ein $m \in \mathbb{N}$ mit $g^m \in (f)$. Insbesondere sind alle $(X - z_i)$ Teiler von g^m und da dies irreduzible Faktoren, also Primfaktoren sind, da $\mathbb{C}[X]$ faktoriell ist, sind dies auch Teiler von g. Also folgt $g \in (\prod_{i=1}^{n} (X - z_i))$.
In jedem Fall gilt:

$$I(\mathcal{N}((f))) = \sqrt{(f)}$$

5.2 **Definition** (Nullstellenmenge, Verschwindungsideal)

Seien k ein Körper, $n \in \mathbb{N}_{\geq 1}$ und $A := k[X_1, \ldots, X_n]$.

i) Für ein Ideal $I \subseteq A$ heißt

$$k^n \supseteq \mathcal{N}(I) := \left\{ (\alpha_1, \ldots, \alpha_n) \in k^n \,\middle|\, \underset{f \in I}{\forall} : f(\alpha_1, \ldots, \alpha_n) = 0 \right\}$$

die Nullstellenmenge von I. Eine Teilmenge $M \subseteq k^n$ heißt *algebraisch*, falls $M = \mathcal{N}(I)$ für ein geeignetes Ideal $I \subseteq A$ gilt.

ii) Für eine Teilmenge $M \subseteq k^n$ ist

$$A \supseteq I(M) := \left\{ f \in A \,\middle|\, \underset{x \in M}{\forall} : f(x) = 0 \right\}$$

ein Ideal und heißt *das Verschwindungsideal von M*.

5.3 **Satz** (Hilbertscher Nullstellensatz)

Seien k ein algebraisch abgeschlossener Körper und $n \in \mathbb{N}_{\geq 1}$.
Dann gilt für jedes Ideal $J \subseteq A := k[X_1, \ldots, X_n]$:

$$I(\mathcal{N}(J)) = \sqrt{J}$$

Die Abbildungen

$$\begin{array}{c}\left\{J \middle| J \subseteq A \text{ Ideal mit } J = \sqrt{J}\right\} \underset{\sim}{\overset{\sim}{\leftrightarrows}} \left\{M \middle| M \subseteq k^n \text{ algebraisch}\right\} \\ J \mapsto \mathcal{N}(J) \\ I(M) \hookleftarrow M\end{array}$$

sind wohldefiniert und zueinander invers. Insbesondere sind beide bijektiv.
Der Beweis benötigt erhebliche Vorarbeit.

5.4 Bemerkung und Beispiel

i) Für jede Teilmenge $M \subseteq k^n$ gilt:

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

Beweis

Nach Definition des Radikals gilt:

$$\sqrt{I(M)} = \left\{ f \in k[X_1, \ldots, X_n] \,\middle|\, \underset{n \in \mathbb{N}}{\exists} : f^n \in I(M) \right\} \supseteq I(M)$$

Sei nun $f \in \sqrt{I(M)}$, also gibt es ein $n \in \mathbb{N}$ mit $f^n \in I(M)$. Es folgt für alle $x \in M$:

$$0 = (f^n)(x) = (f(x))^n \in k$$

Da k ein Körper ist, folgt $f(x) = 0$, also $f \in I(M)$. $\square_{\text{i)}}$

ii) Für $k = \mathbb{C}$ ist die Teilmenge

$$\mathbb{C} \supseteq S^1 := \left\{ z \in \mathbb{C} \middle| |z|^2 = 1 \right\}$$

nicht algebraisch, denn nach 5.1 ist die einzige unendliche algebraische Teilmenge von $\mathbb{C}$ schon $\mathbb{C}$ selbst.

Betrachte nun $\mathbb{C} \cong \mathbb{R} + \mathbf{i}\mathbb{R}$. Für $k = \mathbb{R}$ gilt:

$$\begin{array}{c}\mathbb{R}^2 \supseteq \mathcal{N}\left(\left(X^2 + Y^2 - 1\right)\right) = \left\{(x,y) \in \mathbb{R}^2 \middle| x^2 + y^2 = 1\right\} \cong S^1 \\ \mathbb{R}^2 \cong \mathbb{C} \hookleftarrow S^1\end{array}$$

iii) Für $k = \mathbb{R}$ und $n = 1$ gilt:

$$\begin{array}{c}I\left(\mathcal{N}\left(\left(X^2+1\right)\right)\right) = I\left(\left\{x \in \mathbb{R} \middle| x^2 + 1 = 0\right\}\right) = I(\emptyset) = \\ = (1) = \mathbb{R}[X] \neq \sqrt{(X^2+1)} = \left(X^2+1\right)\end{array}$$

Also kann man im Hilbertschen Nullstellensatz 5.3 nicht auf die Voraussetzung „k algebraisch abgeschlossen“ verzichten.

5.5 Korollar

Seien k ein algebraisch abgeschlossener Körper, $n,m \in \mathbb{N}_{\geq 1}$ und $f_1,\ldots,f_m \in k[X_1,\ldots,X_n]$. Dann sind äquivalent:

i) Es gibt ein $(\alpha_1,\ldots,\alpha_n) \in k^n$ mit $f_i(\alpha_1,\ldots,\alpha_n) = 0$ für alle $1 \leq i \leq m$.

ii) Keine Linearkombination mit beliebigen $g_i \in k[X_1,\ldots,X_n]$ erfüllt:

$$\sum_{i=1}^{n} g_i f_i = 1$$

Beweis

„i) ⇒ ii)“: Aus

$$\sum_{i=1}^{n} g_i f_i = 1$$

folgte der Widerspruch:

$$1 = \left(\sum_{i=1}^{n} g_i f_i\right)(\alpha_1,\ldots,\alpha_n) = \sum_{i=1}^{n} g_i(\alpha_1,\ldots,\alpha_n)\underbrace{f_i(\alpha_1,\ldots,\alpha_n)}_{=0} = 0$$

„ii) ⇒ i)“: Die Voraussetzung besagt:

$$J := (f_1,\ldots,f_m) \neq (1)$$

Zu zeigen ist, dass $\mathcal{N}(J) \neq \emptyset$. Andernfalls hätte man:

$$\sqrt{J} \overset{5.3}{=} I(\mathcal{N}(J)) = I(\emptyset) = (1)$$

Also folgte auch $J = (1)$, denn aus $1 \in \sqrt{J}$ folgt $1^n = 1 \in J$ für ein geeignetes $n \in \mathbb{N}$. Dies ist ein Widerspruch. $\square_{5.5}$

5.6 Definition (Jacobson)

Ein Ring heißt *Jacobson*, falls jedes seiner Primideale Durchschnitt von maximalen Idealen ist.

5.7 Beispiel

i) Jeder Körper ist Jacobson, da das einzige Primideal (0) schon maximal ist.

ii) $\mathbb{Z}$ ist Jacobson. Das einzige nicht-maximale Primideal ist (0) und es gilt:

$$(0) = \bigcap_{p \text{ Primzahl}} (p)$$

Außerdem ist jedes $(p) \subseteq \mathbb{Z}$ maximal.

iii) Sind A Jacobson und $I \subseteq A$ ein Ideal, so ist ${}^{A}/_{I}$ Jacobson.
Dies folgt aus 1.5 iii).

iv) Ist A ein lokaler Integritätsring, so gilt:

$$A \text{ Jacobsen} \Leftrightarrow A \text{ Körper}$$

Beweis

„⇐“: i).

„⇒“: Sei $\mathfrak{m} \subseteq A$ das einzige maximale Ideal. Da A ein Integritätsring ist, ist $(0) \subseteq A$ ein Primideal. Da A Jacobson ist, folgt $(0) = \mathfrak{m}$, da $\mathfrak{m}$ das einzige maximale Ideal ist. Also ist $A \cong {}^{A}/_{(0)} = {}^{A}/_{\mathfrak{m}}$ ein Körper. $\square_{\text{iv)}}$

5.8 **Proposition** (Charakterisierung Jacobson)

Für einen Ring A sind äquivalent:

i) A ist Jacobson.

ii) Es gilt:

$$\operatorname{Jac}(A) = \mathfrak{N}(A)$$

iii) Für jedes Ideal $I \subseteq A$ gilt:

$$\operatorname{Jac}\left({}^{A}/_{I}\right) = \mathfrak{N}\left({}^{A}/_{I}\right)$$

iv) Für jedes $\mathfrak{p} \in \operatorname{Spec}(A)$ gilt:

$$\operatorname{Jac}\left({}^{A}/_{\mathfrak{p}}\right) = (0)$$

Beweis

„i) ⇒ ii)“: Es gilt:

$$\mathfrak{N}(A) \overset{1.30}{=} \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p} \overset{\text{i)}}{=} \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \left(\bigcap_{\mathfrak{p} \subseteq \mathfrak{m} \in \operatorname{MaxSpec}(A)} \mathfrak{m} \right) = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec}(A)} \mathfrak{m} \overset{\text{Definition}}{=} \operatorname{Jac}(A)$$

„ii) ⇒ iii)“: Wegen 5.7 iii) ist ${}^{A}/_{I}$ auch Jacobson und die Behauptung folgt aus ii).
„iii) ⇒ iv)“: Ist $\mathfrak{p} \subseteq A$ ein Primideal, so ist ${}^{A}/_{\mathfrak{p}}$ ein Integritätsring, also folgt aus iii):

$$\operatorname{Jac}\left({}^{A}/_{\mathfrak{p}}\right) = \mathfrak{N}\left({}^{A}/_{\mathfrak{p}}\right) = (0)$$

„iv) ⇒ i)“: Ist $\mathfrak{p} \subseteq A$ ein Primideal, so gilt nach der Korrespondenz von Primidealen im Ring und Quotientenring:

$$\left(\bigcap_{\mathfrak{p}\subseteq\mathfrak{m}\in\operatorname{MaxSpec}(A)} \mathfrak{m}\right)\Big/_{\mathfrak{p}} \cong \bigcap_{\overline{\mathfrak{m}}\in\operatorname{MaxSpec}\left(A/\mathfrak{p}\right)} \overline{\mathfrak{m}} = \operatorname{Jac}\left(A/\mathfrak{p}\right) \overset{\text{iv)}}{=} (0)$$

Also gilt:

$$\mathfrak{p} = \bigcap_{\mathfrak{p}\subseteq\mathfrak{m}\in\operatorname{MaxSpec}(A)} \mathfrak{m}$$

$\square_{5.8}$

5.9 Beispiel

Für einen Hauptidealring A, der kein Körper ist, sind äquivalent:

i) A ist Jacobson.

ii) $|\operatorname{Spec}(A)| = \infty$

(vergleiche 5.7 ii))
$\mathbb{Z}_{(p)}$ ist ein Hauptidealring mit $\left|\operatorname{Spec}\left(\mathbb{Z}_{(p)}\right)\right| = 2$, also nicht Jacobson.

Beweis

Da A kein Körper ist, gilt:

$$\operatorname{Spec}(A) = \{(0)\} \dot\cup \left\{\mathfrak{m}\middle|\mathfrak{m} \subseteq A \text{ maximales Ideal}\right\} = \{(0)\} \dot\cup \underbrace{\operatorname{MaxSpec}(A)}_{\neq\emptyset}$$

Schreibe $\mathfrak{m} = (f_m) \in \operatorname{MaxSpec}(A)$ für geeignetes $f_m \in A$, was möglich ist, da A ein Hauptidealring ist.
„i) ⇒ ii)“: Wäre $|\operatorname{Spec}(A)| < \infty$, so folgte mit dem Chinesischen Restsatz:

$$(0) \overset{\text{i)}}{=} \bigcap_{\mathfrak{m}\in\operatorname{MaxSpec}(A)} (f_m) \underset{1.35}{\overset{|\operatorname{Spec}(A)|<\infty}{=}} \left(\prod_{\mathfrak{m}\in\operatorname{MaxSpec}(A)} f_m\right)$$

Also folgte:

$$\prod_{\mathfrak{m}\in\operatorname{MaxSpec}(A)} f_m = 0$$

Dies ist ein Widerspruch zu $f_m \neq 0$, da A als Hauptidealring ein Integritätsring ist.
„ii) ⇒ i)“: Offenbar ist jedes maximale Ideal Durchschnitt maximaler Ideale. Zeige also nur:

$$(0) = \bigcap_{\mathfrak{m}\in\operatorname{MaxSpec}(A)} (f_m) = \operatorname{Jac}(A)$$

Ein $f \in \operatorname{Jac}(A)$ hat wegen ii) unendlich viele Primteiler, also gilt $f = 0$, da jeder Hauptidealring faktoriell ist. $\square_{5.9}$

5.10 Proposition

Sind $f : A \to B$ ein ganzer Ringhomomorphismus und A Jacobson, so ist B auch Jacobson.

Beweis

Es ist $\operatorname{im}(f) \cong {}^{A}\!/_{\ker(f)}$ Jacobson nach 5.7 iii) und die Ringerweiterung $\operatorname{im}(f) \subseteq B$ ist ganz.
Sei also ohne Einschränkung $A \subseteq B$ eine ganze Ringerweiterung.
Sei $\mathfrak{p} \subseteq B$ ein Primideal, so ist $\mathfrak{q} := A \cap \mathfrak{p}$ ein Primideal und da A Jacobson ist, gibt es eine Menge $\{\mathfrak{m}_i\}_{i \in I}$ von maximalen Idealen von A mit:

$$\mathfrak{q} = \bigcap_{i \in I} \mathfrak{m}_i$$

Bildchen:

$$\begin{array}{ccccccc} \mathfrak{p} & \subseteq & \tilde{\mathfrak{p}} & \subseteq & \mathfrak{p}_i & \subseteq & B \\ | & \diagup & & & | & & \uparrow \text{ganz} \\ \mathfrak{q} & & \subseteq & & \mathfrak{m}_i & \subseteq & A \end{array}$$

Nach dem Going-up theorem 4.21 existiert für jedes $i \in I$ ein Primideal $\mathfrak{p}_i \subseteq B$ mit $\mathfrak{p} \subseteq \mathfrak{p}_i$ und $\mathfrak{p}_i \cap A = \mathfrak{m}_i$.
Wegen 4.16 ist jedes $\mathfrak{p}_i \subseteq B$ sogar ein maximales Ideal.
Nun gelten

$$\mathfrak{p} \subseteq \tilde{\mathfrak{p}} := \bigcap_{i \in I} \mathfrak{p}_i \subseteq B$$

und:

$$\mathfrak{q} = \mathfrak{p} \cap A \subseteq \tilde{\mathfrak{p}} \cap A = \bigcap_{i \in I} (\mathfrak{p}_i \cap A) = \bigcap_{i \in I} \mathfrak{m}_i = \mathfrak{q}$$

Daher gilt $\mathfrak{p} \cap A = \tilde{\mathfrak{p}} \cap A$. Aus einer leichten Verallgemeinerung (für $\mathfrak{q}'$ kein Primideal) von 4.18 folgt, dass $\mathfrak{p} = \tilde{\mathfrak{p}}$ gilt.
Also ist $\mathfrak{p}$ Durchschnitt maximaler Ideale von B. $\square_{5.10}$

5.11 Satz (Hauptsatz über Jacobson-Ringe)

Seien A Jacobson und $f : A \to B$ eine endlich erzeugte A-Algebra, dann gelten:

i) B ist Jacobson.

ii) Ist $\mathfrak{m}' \subseteq B$ ein maximales Ideal, so ist auch $\mathfrak{m} := f^{-1}(\mathfrak{m}') \subseteq A$ ein maximales Ideal und die Erweiterung der Restklassenkörper

$$\kappa(\mathfrak{m}) = {}^{A}\!/_{\mathfrak{m}} \subseteq \kappa(\mathfrak{m}') = {}^{B}\!/_{\mathfrak{m}'}$$

ist endlich.

Bemerkung

$\mathbb{Z}$ ist Jacobson und jeder Ring ist eine $\mathbb{Z}$-Algebra, aber nicht notwendigerweise Jacobson. Also kann man auf die Voraussetzung „endlich erzeugt“ nicht verzichten.
Insbesondere ist $\mathbb{Z}_{(p)}$ als $\mathbb{Z}$-Algebra nicht endlich erzeugt, da $\mathbb{Z}_{(p)}$ nicht Jacobson ist.

5.12 Lemma

5.11 gilt, für $(f : A \to B) := (k \subseteq k[X])$ für einen Körper k.

Beweis

i) Da $k[X]$ ein Hauptidealring ist, zeige wegen 5.9 ii) $\Rightarrow$ i) nur, dass $|\mathrm{Spec}(k[X])| = \infty$ gilt, das heißt es gibt unendlich viele normierte irreduzible Polynome, denn zwei Polynome erzeugen genau dann dasselbe Hauptideal, wenn sie sich um einen konstanten Faktor unterscheiden.

Angenommen es gäbe nur die endlich vielen normierten irreduziblen Polynome $f_1, \ldots, f_n$. Sei ohne Einschränkung $f_1 = X$. Dann folgte für

$$F := \left(\prod_{i=1}^{n} f_i \right) + 1$$

schon:

$$\deg(F) \geq \deg(f_1) = 1$$

Also gilt $F \notin (k[X])^*$. Daher gibt es ein normiertes irreduzibles $f \in k[X]$ mit $f \mid F$. Wäre $f = f_i$, so folgte aus der Definition von F, dass $f_i \mid 1$ gelten würde. Dies ist aber ein Widerspruch dazu, dass f_i prim ist. Also ist $f \notin \{f_1, \ldots, f_n\}$ ein normiertes irreduzibles Polynom. Dies ist ein Widerspruch dazu, dass dies die einzigen Primelemente sind. $\square_{\text{i)}}$

ii) Ist $\mathfrak{m}' \subseteq k[X]$ maximal, so gilt $\mathfrak{m}' := (f)$ für ein normiertes irreduzibles $f \in k[X]$ und es folgt, dass für die Erweiterung

$$\kappa(\underbrace{\mathfrak{m}' \cap k}_{=(0)}) = k \subseteq \kappa(\mathfrak{m}') = {}^{k[X]}\!/_{(f)}$$

gilt:

$$\dim_k(E) = \deg(f) < \infty$$

$\square_{\text{ii)}}$

5.13 Lemma

Für einen Ring A sind äquivalent:

i) A ist Jacobson.

ii) Sind $\mathfrak{p} \subseteq A$ ein Primideal und $x \in {}^{A}\!/_{\mathfrak{p}}$ so, dass $\left({}^{A}\!/_{\mathfrak{p}} \right)[x^{-1}]$ ein Körper ist, so ist ${}^{A}\!/_{\mathfrak{p}}$ ein Körper.

Bemerkung

Für alle $x \in \mathbb{Z}$ gilt $\mathbb{Z}\left[x^{-1}\right] \subsetneq \mathbb{Q}$. Also ist $\mathbb{Z}$ Jacobson.
Für alle Primzahlen $p \in \mathbb{Z}$ gilt $\mathbb{Z}_{(p)}\left[p^{-1}\right] = \mathbb{Q} = \operatorname{Quot}\left(\mathbb{Z}_{(p)}\right)$, aber $\mathbb{Z}_{(p)} \subsetneq \mathbb{Q}$, weswegen $\mathbb{Z}_{(p)}$ nicht Jacobson ist.

Beweis

„i) ⇒ ii)“: Wäre ${}^{A}\!/_{\mathfrak{p}}$ kein Körper, so müsste $x \notin \left({}^{A}\!/_{\mathfrak{p}}\right)^*$ gelten, da sonst ${}^{A}\!/_{\mathfrak{p}} = {}^{A}\!/_{\mathfrak{p}}\left[x^{-1}\right]$ ein Körper wäre.
Da der Nullring kein Körper ist, ist $x \neq 0$. Also läge x nach 1.24 in einem maximalen Ideal $(0) \neq \mathfrak{m} \subseteq {}^{A}\!/_{\mathfrak{p}}$ und das Primideal $(0) \subseteq {}^{A}\!/_{\mathfrak{p}}$ wäre nicht maximal, da $(0) \subsetneq \mathfrak{m}$ gilt. Da (0) das einzige Primideal in ${}^{A}\!/_{\mathfrak{p}}\left[x^{-1}\right]$ ist, da dies ein Körper ist, muss nach 3.19 iv) (mit $S := \left\{x^n \middle| n \geq 0\right\}$) schon ein x^n, also auch x, in alle maximalen Idealen von ${}^{A}\!/_{\mathfrak{p}}$ liegen. Es folgt:

$$x \in \operatorname{Jac}\left({}^{A}\!/_{\mathfrak{p}}\right) \underset{5.8\ \text{i)} \Rightarrow \text{iv)}}{\overset{\text{i)}}{=}} (0)$$

Dies ist wegen $x \neq 0$ ein Widerspruch.
„ii) ⇒ i)“: Wegen 5.85.8 iv) ⇒ i) zeige für alle $\mathfrak{p} \in \operatorname{Spec}(A)$ nun $\operatorname{Jac}\left({}^{A}\!/_{\mathfrak{p}}\right) = (0)$.
Angenommen dies gilt nicht, dann ist ${}^{A}\!/_{\mathfrak{p}}$ ein Integritätsring und es gibt ein $0 \neq x \in \operatorname{Jac}\left({}^{A}\!/_{\mathfrak{p}}\right)$. Insbesondere ist ${}^{A}\!/_{\mathfrak{p}}$ kein Körper.
Nach 3.19 iv) besitzt $\left({}^{A}\!/_{\mathfrak{p}}\right)\left[x^{-1}\right]$ keine von Null verschiedenen maximalen Ideale, ist also ein Körper. Dies ist ein Widerspruch zu ii). $\square_{5.13}$

5.14 Proposition

Seien A ein Jacobson Integritätsring und $A \subseteq B$ eine von einem Element erzeugte A-Algebra, die auch ein Integritätsring ist, und in der ein Element $b \in B$ existiert, sodass $B\left[b^{-1}\right]$ ein Körper ist.
Dann ist $A \subseteq B$ eine endliche Körpererweiterung.

Beweis

Nach Voraussetzung gilt

$$B \cong {}^{A[X]}\!/_{Q}$$

als A-Algebra für ein geeignetes Ideal $Q \subseteq A[X]$.

$$\begin{array}{ccc} A[X] & \xrightarrow{X \mapsto x} & B \ni x \\ \uparrow & \nearrow & \\ A & & \end{array}$$

Behauptung I: $Q \neq (0)$

Beweis: Sonst wäre $B \cong A[X]$ und $b = f(X) \in A[X]$ so, dass $B\left[b^{-1}\right] = A[X]\left[(f(X))^{-1}\right]$ ein Körper ist.
Es gilt $A \subseteq B \overset{B \text{ Integritätsring}}{\subseteq} B\left[b^{-1}\right]$ und es folgt:

$$K := \text{Quot}(A) \subseteq B\left[b^{-1}\right]$$

Daher gilt:

$$A[X]\left[(f(X))^{-1}\right] = K[X]\left[(f(X))^{-1}\right]$$

Dies ist ein Körper. Wegen 5.12 und 5.13 i) $\Rightarrow$ ii) (mit $\mathfrak{p} = (0)$) ist $K[X]$ ein Körper. Dies ist ein Widerspruch, da $0 \neq X \notin (K[X])^* = K^*$ ist. $\square_{\text{Behauptung I}}$

Behauptung II: Es existiert ein $a \in A \setminus \{0\}$ so, dass $A\left[a^{-1}\right] \subseteq B\left[b^{-1}\right]$ ganz ist.
(Bemerke, dass $B\left[b^{-1}\right]$ ein Körper ist, also $A\left[a^{-1}\right] \subseteq B\left[b^{-1}\right]$.)

Beweis: Wir haben mit $x := X + Q$:

$$A \subseteq B \cong A[X]/_Q = A[x] \subseteq B\left[b^{-1}\right] = A\left[x, b^{-1}\right] \tag{5.1}$$

Nach Behauptung I existiert ein $0 \neq p \in Q \subseteq A[X]$ mit $p(x) = 0$ in B. Wegen $n := \deg(p) \geq 1$ kann man mit $a_n \neq 0$ schreiben:

$$p(X) = a_n X^n + \ldots + a_0$$

Es folgt in $B\left[b^{-1}\right]$:

$$x^n + \left(a_{n-1}a_n^{-1}\right)x^{n-1} + \ldots + \left(a_0 a_n^{-1}\right) = 0 \tag{5.2}$$

Dies ist eine Ganzheitsgleichung für x über $A\left[a_n^{-1}\right]$, also ist $A\left[a_n^{-1}\right] \subseteq A[x]$ eine ganze Ringerweiterung.
Wegen $B = A[x] \ni b$ ist also ebenfalls b ganz über $A\left[a_n^{-1}\right]$, schreibe also

$$b^m + \alpha_{m-1}b^{m-1} + \ldots + \alpha_0 = 0$$

mit einem minimalen $m \in \mathbb{N}_{\geq 1}$ und geeigneten $\alpha_i \in A\left[a_n^{-1}\right]$. Es gilt $\alpha_0 \neq 0$, denn sonst wäre

$$b^{m-1} + \alpha_{m-1}b^{m-2} + \ldots + \alpha_1 = 0$$

im Widerspruch zur Minimalität von m. Nach Division durch $b^m \cdot \alpha_0$ gilt in $B\left[b^{-1}\right]$:

$$\left(b^{-1}\right)^m + \left(\alpha_1\alpha_0^{-1}\right)\left(b^{-1}\right)^{m-1} + \ldots + \left(\alpha_{m-1}\alpha_0^{-1}\right)b^{-1} + \alpha_0^{-1} = 0 \tag{5.3}$$

Dies ist eine Ganzheitsgleichung für b^{-1} über $A\left[a_n^{-1}, \alpha_0^{-1}\right]$ und für ein geeignetes $a \in A$ gilt:

$$A\left[a_n^{-1}, \alpha_0^{-1}\right] = A\left[a^{-1}\right]$$

(Dies geht analog zu $\mathbb{Z}\left[\frac{1}{2}, \frac{1}{3}\right] = \mathbb{Z}\left[\frac{1}{6}\right]$.)
Aus (5.1), (5.2) und (5.3) folgt die Behauptung. $\square_{\text{Behauptung II}}$

Da $A\left[a^{-1}\right] \subseteq B\left[b^{-1}\right]$ eine ganze Ringerweiterung von Integritätsringen und $B\left[b^{-1}\right]$ ein Körper ist, folgt nach (4.15) ii) $\Rightarrow$ i), dass $A\left[a^{-1}\right]$ ein Körper ist.
Weil A Jacobson ist ist, folgt aus 5.13 ii) $\Rightarrow$ i) mit $\mathfrak{p} := (0)$ und $x := a$, dass A ein Körper ist. Damit ist sogar $B\left[b^{-1}\right] \supseteq A\left[a^{-1}\right] = A$ ganz, insbesondere ist $A \subseteq B$ ganz. Wegen 4.15 i) $\Rightarrow$ ii) ist B ein Körper, und es folgt $B = B\left[b^{-1}\right]$. Da

$$A \subseteq B \overset{(5.1)}{=} A\left[x,b^{-1}\right]$$

gilt, folgt aus 4.8, dass $A \subseteq B$ endlich ist. $\square_{5.14}$

Beweis von 5.11

Induktion über die Anzahl n von A-Algebrenerzeugern von B.

- $n = 0$: Dann gilt $A = B$ und die Aussage ist trivial.
- $n = 1$:
  i) Wir verifizieren 5.13 ii) für B, womit folgt, dass B Jacobson ist:
  Sind $\mathfrak{p} \subseteq B$ ein Primideal und $x \in {}^{B}\!/_{\mathfrak{p}}$ so, dass $\left({}^{B}\!/_{\mathfrak{p}}\right)\left[x^{-1}\right]$ ein Körper ist, so ist ${}^{B}\!/_{\mathfrak{p}}$ ein Körper.
  Zeige: ${}^{B}\!/_{\mathfrak{p}}$ ist ein Körper. Es ist

  $$A' := {}^{A}\!/_{f^{-1}(\mathfrak{p})} \subseteq B' := {}^{B}\!/_{\mathfrak{p}}$$

  eine von einem einzigen Element erzeugte A'-Algebra (wegen $n = 1$). A' und B' sind Integritätsringe, A' ist Jacobson, was aus 5.7 folgt, da A Jacobson ist, und für $b := x \in B'$ ist $B'\left[b^{-1}\right]$ ein Körper. Aus 5.14 folgt insbesondere, dass B' ein Körper ist. $\square_{\text{i)}}$
  ii) Seien $\mathfrak{m}' \subseteq B$ ein maximales Ideal, dann ist wie oben 5.14 auf

  $${}^{A}\!/_{f^{-1}(\mathfrak{m}')} \subseteq {}^{B}\!/_{\mathfrak{m}'}$$

  anwendbar, und es folgt, dass ${}^{A}\!/_{f^{-1}(\mathfrak{m}')}$ ein Körper ist. Also ist $\mathfrak{m} := f^{-1}(\mathfrak{m}') \subseteq A$ maximal. Nach 5.14 ist

  $$\kappa(\mathfrak{m}) = {}^{A}\!/_{\mathfrak{m}} \subseteq {}^{B}\!/_{\mathfrak{m}'} = \kappa(\mathfrak{m}')$$

  endlich. $\square_{\text{ii)}}$
- $n > 1$: Es gelte $B = A[b_1, \ldots, b_n]$. Faktorisiere:

  $$f = \left(A \overset{f_1}{\to} A' := A[b_1, \ldots, b_{n-1}] \overset{f_2}{\to} B = A'[b_n]\right)$$

  i) Nach Induktionsvoraussetzung ist A' Jacobson, also nach Fall $n = 1$ auch B. $\square_{\text{i)}}$
  ii) Ist $\mathfrak{m}' \subseteq B$ maximal, so nach Fall $n = 1$ auch $\tilde{\mathfrak{m}} := f_2^{-1}(\mathfrak{m}) \subseteq A'$ und damit nach Induktionsvoraussetzung auch:

  $$A \supseteq f_1^{-1}(\tilde{\mathfrak{m}}) = f^{-1}(\mathfrak{m}') =: \mathfrak{m}$$

  Nach Induktionsvoraussetzung beziehungsweise Fall $n = 1$ ist die Erweiterung $\kappa(\mathfrak{m})$ ist die Erweiterung $\kappa(\mathfrak{m}) \subseteq \kappa(\tilde{\mathfrak{m}})$ beziehungsweise $\kappa(\tilde{\mathfrak{m}}) \subseteq \kappa(\mathfrak{m}')$ endlich. Nach der Transitivität der Endlichkeit 2.33 i) ist $\kappa(\mathfrak{m}) \subseteq \kappa(\mathfrak{m}')$ endlich. $\square_{\text{ii)}}$

$\square_{5.11}$

5.15 Proposition

Seien k ein algebraisch abgeschlossener Körper und $n \in \mathbb{N}_{\geq 1}$. Dann sind die Abbildungen

$$\begin{aligned} k^n &\overset{\sim}{\leftrightarrows} \left\{\mathfrak{m} \middle| \mathfrak{m} \subseteq k[X_1,\ldots,X_n] \text{ maximales Ideal}\right\} \\ \underline{\alpha} = (\alpha_1,\ldots,\alpha_n) &\overset{\sim}{\mapsto} \mathfrak{m}_{\underline{\alpha}} := (X_1 - \alpha_1,\ldots,X_n - \alpha_n) \\ \mathcal{N}(\mathfrak{m}) &\overset{\sim}{\mapsfrom} \mathfrak{m} \end{aligned}$$

wohldefiniert und zueinander inverse Bijektionen.

Beweis

Für $\underline{\alpha} \in k^n$ ist der Einsetzungshomomorphismus

$$\begin{aligned} k[X_1,\ldots,X_n] &\twoheadrightarrow k \\ X_i &\mapsto \alpha_i \end{aligned}$$

surjektiv und der Kern ist $\mathfrak{m}_{\underline{\alpha}}$, also gilt:

$$k[X_1,\ldots,X_n]/\mathfrak{m}_{\underline{\alpha}} \cong k$$

Daher ist $\mathfrak{m}_{\underline{\alpha}}$ ein maximales Ideal, das heißt $\underline{\alpha} \mapsto \mathfrak{m}_{\underline{\alpha}}$ ist wohldefiniert.
Ist $\mathfrak{m} \subseteq k[X_1,\ldots,X_n]$, so folgt aus 5.11 mit $(f : A \to B) := (k \to k[X_1,\ldots,X_n])$, dass

$$k \cong k/\underbrace{(k \cap \mathfrak{m})}_{=(0)} \subseteq k[X_1,\ldots,X_n]/\mathfrak{m} =: E$$

eine endliche Körpererweiterung ist.
Da k algebraisch abgeschlossen ist, ist $k = E$ und wir definieren für $1 \leq i \leq n$:

$$\alpha_i := \left(k[X_1,\ldots,X_n] \twoheadrightarrow k[X_1,\ldots,X_n]/\mathfrak{m} \cong k\right)(X_i) \in k$$

Für $\underline{\alpha} := (\alpha_1,\ldots,\alpha_n)$ folgt $\mathfrak{m}_{\underline{\alpha}} \subseteq \mathfrak{m}$. Da $\mathfrak{m}_{\underline{\alpha}}$ und $\mathfrak{m}$ maximal sind, folgt $\mathfrak{m} = \mathfrak{m}_{\underline{\alpha}}$. Daher gilt:

$$\mathcal{N}(\mathfrak{m}) = \mathcal{N}\left(\mathfrak{m}_{\underline{\alpha}}\right) = \{\underline{\alpha}\}$$

Also ist $\mathfrak{m} \mapsto \mathcal{N}(\mathfrak{m})$ wohldefiniert. Die Abbildungen sind zueinander invers. $\square_{5.15}$

Beweis von 5.3

Für ein Ideal $J \subseteq A := k[X_1,\ldots,X_n]$ ist die Relation $J \subseteq I(\mathcal{N}(J))$ nach Definition klar. Aus 5.14 ii) mit $M := \mathcal{N}(J)$ folgt $\sqrt{J} \subseteq I(\mathcal{N}(J))$.
Zeige: $I(\mathcal{N}(J)) \subseteq \sqrt{J}$
Die Abbildung

$$\begin{aligned} \mathcal{N}(J) &\overset{\sim}{\to} \operatorname{MaxSpec}\left(A/J\right) := \left\{\text{maximale Ideale von } A/J\right\} \\ \underline{\alpha} &\mapsto \mathfrak{m}_{\underline{\alpha}}/J \end{aligned}$$

ist wohldefiniert und bijektiv. Dabei ist $\mathfrak{m}_{\underline{\alpha}}$ wie in 5.15 wohldefiniert, denn $\mathfrak{m}_{\underline{\alpha}} \subseteq A$ ist ein maximales Ideal und es gilt:

$$J \subseteq \mathfrak{m}_{\underline{\alpha}} = \left\{ f \in A \middle| f\left(\underline{\alpha}\right) = 0 \right\}$$

Denn $f\left(\underline{\alpha}\right) = 0$ gilt für $f \in J$ und $\underline{\alpha} \in \mathcal{N}\left(J\right)$. Aus 5.15 folgt die Bijektivität.
(Beachte: Für alle $\underline{\alpha} \in k^n$ gilt: $J \subseteq \mathfrak{m}_{\underline{\alpha}} \Leftrightarrow \underline{\alpha} \in \mathcal{N}\left(J\right)$)
Nun ist 5.7 i), 5.11 und 5.7 ii) ist der Ring ${}^{A}\!/_{J}$ Jacobson, und es folgt:

$$\mathfrak{N}\left({}^{A}\!/_{J}\right) \overset{5.8\text{ ii)}}{=} \operatorname{Jac}\left({}^{A}\!/_{J}\right) = \bigcap_{\underline{\alpha} \in \mathcal{N}(J)} {}^{\mathfrak{m}_{\underline{\alpha}}}\!/_{J}$$

Damit folgt:

$$\sqrt{J} = \left(A \twoheadrightarrow {}^{A}\!/_{J}\right)^{-1} \left(\mathfrak{N}\left({}^{A}\!/_{J}\right)\right) = \bigcap_{\underline{\alpha} \in \mathcal{N}(J)} \mathfrak{m}_{\underline{\alpha}} =$$

$$\overset{\text{Def. von } \mathfrak{m}_{\underline{\alpha}}}{=} \bigcap_{\underline{\alpha} \in \mathcal{N}(J)} \left\{ f \in A \middle| \underset{\underline{\alpha} \in \mathcal{N}(J)}{\forall} : f\left(\underline{\alpha}\right) = 0 \right\} = I\left(\mathcal{N}\left(J\right)\right)$$

Der Rest ist dann klar. $\square_{5.3}$

6 Endlichkeitsbedingungen

6.1 **Erinnerung** (teilweise geordnete Menge)

Eine *teilweise geordnete Menge* ist ein Paar $(\Sigma, \leq)$ bestehend aus einer Menge Σ und einer Relation $\leq$, sodass für alle $x,y,z \in \Sigma$ gelten:

i) $x \leq x$

ii) $(x \leq y) \wedge (y \leq z) \Rightarrow x \leq z$

iii) $(x \leq y) \wedge (y \leq x) \Rightarrow x = y$

6.2 **Proposition und Definition** (aufsteigende Folge, stationär)

Für eine teilweise geordnete Menge $(\Sigma, \leq)$ sind äquivalent:

i) Jede *aufsteigende Folge in* Σ, das heißt für alle $n \in \mathbb{N}$ ist $x_n \in \Sigma$ und es gilt $x_n \leq x_{n+1}$, ist *stationär*, das heißt es gibt ein $N \in \mathbb{N}$, sodass für alle $n \geq N$ schon $x_n = x_n$ gilt.

ii) Jede nicht-leere Teilmenge Σ hat ein maximales Element.

Beweis

„i) $\Rightarrow$ ii)“: Angenommen $\emptyset \neq \Sigma' \subseteq \Sigma$ besitzt kein maximales Element. Dann wähle induktiv $x_n \in \Sigma'$ für $n \in \mathbb{N}$ wie folgt:

$n = 0$: Wähle $x_0 \in \Sigma'$ beliebig, was möglich ist, da Σ' nicht-leer ist.

$n > 0$: Da $x_{n-1} \in \Sigma'$ nicht maximal ist, gibt es ein Element $x_n \in \Sigma'$ mit $x_{n-1} \leq x_n$ und $x_{n-1} \neq x_n$. Offenbar ist $x_0,x_1,\ldots \in \Sigma$ eine nicht-stationäre aufsteigende Folge im Widerspruch zu i). $\square_{\text{i) } \Rightarrow \text{ ii)}}$

„ii) $\Rightarrow$ i)“: Die Teilmenge $\emptyset \neq \Sigma' := \{x_n | n \geq 0\} \subseteq \Sigma$ besitzt ein maximales Element x_N. Für alle $n \geq N$ folgt dann aus $x_n \geq x_N$ bereits $x_n = x_N$, also ist die Folge $x_0 \leq x_1 \leq \ldots$ stationär. $\square_{6.2}$

6.3 **Definition** (Noethersch, Artinsch)

Seien A ein Ring und M ein A-Modul.

i) M heißt *Noethersch* (bzw. *Artinsch*), wenn

$$(\Sigma, \leq) := \left(\left\{M' \middle| M' \subseteq M \text{ ist } A\text{-Untermodul}\right\}, \left(M' \leq M''\right) := \left(M' \subseteq M''\right)\right)$$
$$\left(\text{bzw. } (\Sigma, \leq) := \left(\left\{M' \middle| M' \subseteq M \text{ ist } A\text{-Untermodul}\right\}, \left(M' \leq M''\right) := \left(M' \supseteq M''\right)\right)\right)$$

die Bedingung in 6.2 erfüllt.

ii) Der Ring A heißt *Noethersch* (bzw. *Artinsch*), wenn A als A-Modul Noethersch (bzw. Artinsch) ist.

(Erinnerung: Die A-Untermodul von A sind genau die Ideale von A.)

6.4 Beispiel

i) Jeder endliche Modul ist sowohl Artinsch als auch Noethersch, zum Beispiel ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ für $n \in \mathbb{N}_{\geq 1}$.

ii) Der Ring $\mathbb{Z}$ ist (wie jeder Hauptidealring) Noethersch, aber $\mathbb{Z}$ ist nicht Artinsch.

Beweis

Ist $(a_0) \subsetneq (a_1) \subsetneq \ldots$ eine echt aufsteigende Folge von Idealen in $\mathbb{Z}$, die alle Hauptideale sind, da $\mathbb{Z}$ ein Hauptidealring ist, so gilt für alle a_0,$a_1, \ldots \in \mathbb{Z}$, dass a_{n+1} ein echter Teiler von a_n ist. Da a_0 Produkt endlich vieler Primfaktoren und einer Einheit ist, weil jeder Hauptidealring faktoriell ist, existiert ein n mit $(a_n) = (1)$. Also ist $\mathbb{Z}$ (wie jeder Hauptidealring) Noethersch.

Da

$$(2) \supsetneq \left(2^2\right) \supsetneq \left(2^3\right) \supsetneq \ldots$$

eine unendlich lange, echt absteigende Folge von Idealen in $\mathbb{Z}$ ist, ist $\mathbb{Z}$ nicht Artinsch.$\square_{\text{ii)}}$

iii) Für eine Primzahl p ist der $\mathbb{Z}$-Modul

$$G := {}^{\mathbb{Z}\left[p^{-1}\right]}\!/_{\mathbb{Z}}$$

nicht Noethersch, aber Artinsch.

Beweis

Die Folge von $\mathbb{Z}$-Untermoduln

$$G_n := {}^{\mathbb{Z} \cdot p^{-n}}\!/_{\mathbb{Z}} = \left\{ \frac{a}{p^n} + \mathbb{Z} \middle| a \in \mathbb{Z} \right\} \subseteq G$$

ist strikt aufsteigend, denn es ist $\frac{1}{p^n} + \mathbb{Z} \in G_n \setminus G_{n-1}$, also ist G nicht Noethersch.

Man kann zeigen, dass die $G_n \subsetneq G$ die einzigen echten $\mathbb{Z}$-Untermoduln sind.

Also ist G Artinsch, denn jede absteigende Folge von Untermoduln ist

$$(G_n) \supsetneq (G_k) \supsetneq \ldots \supsetneq (G_0)$$

mit $k < n$. Wegen $G_0 = (0)$ muss diese Folge abbrechen. $\square_{\text{iii)}}$

iv) Mit ii), iii) und der exakten Folge von $\mathbb{Z}$-Moduln

$$0 \to \mathbb{Z} \to \mathbb{Z}\left[p^{-1}\right] \to G \to 0$$

folgt aus 6.7, dass der $\mathbb{Z}$-Modul $\mathbb{Z}\left[p^{-1}\right]$ weder Noethersch noch Artinsch ist.

Beachte: $\mathbb{Z}\left[p^{-1}\right]$ aufgefasst als $\mathbb{Z}\left[p^{-1}\right]$-Modul *ist* nach ii) Noethersch, da dies ein Hauptidealring ist.

6.5 **Proposition** (Hinreichende Bedingungen für Isomorphismen)

Seien A ein Ring, M ein A-Modul und $\varphi \in \mathrm{End}_A(M)$.

i) Ist φ surjektiv und M Noethersch, so ist φ ein Isomorphismus.

ii) Ist φ injektiv und M Artinsch, so ist φ ein Isomorphismus.

Beweis

i) Die aufsteigende Folge von A-Untermoduln

$$\ker(\varphi) \subseteq \ker\left(\varphi^2\right) \subseteq \ker\left(\varphi^3\right) \subseteq \ldots \subseteq M$$

ist, da M Noethersch ist, stationär, das heißt es gibt es ein $n \in \mathbb{N}_{\geq 1}$ mit:

$$\ker(\varphi^n) = \ker\left(\varphi^{n+1}\right) \tag{6.1}$$

Sei $x_1 \in \ker(\varphi)$. Da φ surjektiv ist, existiert eine Folge $x_1, x_2, \ldots \in M$ mit $\varphi(x_{m+1}) = x_m$ für alle $m \in \mathbb{N}_{\geq 1}$. Es folgt:

$$x_1 = \varphi(x_2) = \varphi^2(x_3) = \ldots = \varphi^n(x_{n+1})$$

Also gilt:

$$0 \overset{x_1 \in \ker(\varphi)}{=} \varphi(x_1) = \varphi(\varphi^n(x_{n+1})) = \varphi^{n+1}(x_{n+1})$$

Daher gilt wegen (6.1):

$$0 = \varphi^n(x_{n+1}) = x_1$$

Also ist $\ker(\varphi) = 0$, das heißt φ ist injektiv und damit ein Isomorphismus. $\square_{\text{i)}}$

ii) Die absteigende Folge von A-Untermoduln

$$M \supseteq \mathrm{im}(\varphi) \supseteq \mathrm{im}\left(\varphi^2\right) \supseteq \mathrm{im}\left(\varphi^3\right) \supseteq \ldots$$

ist, da M Artinsch ist, stationär, das heißt es gibt es ein $n \in \mathbb{N}_{\geq 1}$ mit:

$$\mathrm{im}(\varphi^n) = \mathrm{im}\left(\varphi^{n+1}\right) \tag{6.2}$$

Sei $x_1 \in M$. Definiere eine Folge $x_1, x_2, \ldots \in M$ durch $x_{m+1} := \varphi(x_m)$ für alle $m \in \mathbb{N}_{\geq 1}$. Es folgt:

$$\varphi^n(x_1) = \varphi^{n-1}(x_2) = \varphi^{n-2}(x_3) = \ldots = \varphi(x_n) = x_{n+1} \in \mathrm{im}(\varphi^n)$$

Daher gilt wegen (6.2):

$$x_{n+1} \in \operatorname{im}\left(\varphi^{n+1}\right)$$

Daher gibt es ein $x \in M$ mit $\varphi^{n+1}(x) = x_{n+1}$. Also gilt:

$$\varphi^n(\varphi(x)) = \varphi^{n+1}(x) = x_{n+1} = \varphi^n(x_1)$$

Da mit φ auch φ^n injektiv ist, folgt $x_1 = \varphi(x)$ und somit $x_1 \in \operatorname{im}(\varphi)$.
Also ist $M = \operatorname{im}(\varphi)$, das heißt φ ist surjektiv und damit ein Isomorphismus. $\square_{\text{ii)}}$

6.6 **Proposition** (Charakterisierung von Noethersch)

Seien A ein Ring und M ein A-Modul. Dann sind äquivalent:

i) M ist Noethersch.

ii) Jeder A-Untermodul von M ist endlich erzeugt.

Beweis

„i) $\Rightarrow$ ii)“: Seien $M' \subseteq M$ ein Untermodul und:

$$\Sigma := \left\{M'' \middle| M'' \subseteq M' \text{ endlich erzeugter Untermodul}\right\}$$

Wegen $0 \in \Sigma$ ist Σ nicht leer und nach (6.2) ii) existiert ein maximales $M'' \in \Sigma$.
Wäre $M'' \subsetneq M'$, so existierte ein $x \in M' \setminus M''$ und wir hätten:

$$M'' \subsetneq M'' + Ax \subseteq M'$$

Da $M'' + Ax$ endlich erzeugt ist, wäre dies ein Widerspruch zur Maximalität von M''.
Somit gilt $M' = M''$. $\square_{\text{i)} \Rightarrow \text{ii)}}$
„ii) $\Rightarrow$ i)“: Sei

$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M$$

eine Folge von A-Untermoduln. Dann ist

$$M' := \bigcup_{n \geq 1} M_n \subseteq M$$

ein A-Untermodul, also endlich erzeugt nach ii), das heißt es gibt ein $n \in \mathbb{N}$ und geeignete $x_i \in M'$ mit:

$$M' = \sum_{i=1}^{n} Ax_i$$

Offenbar existiert ein $N \in \mathbb{N}$ mit $x_1, \ldots, x_n \in M_N$, und es folgt $M_N = M'$.
Also gilt $M_{N+k} = M_N$ für alle $k \in \mathbb{N}$ und die Folge ist daher stationär. $\square_{6.6}$

6.7 Proposition

Seien A ein Ring und

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

eine kurze exakte Folge von A-Moduln. Dann sind äquivalent:

i) M ist Noethersch (bzw. Artinsch).

ii) M' und M'' sind Noethersch (bzw. Artinsch).

Beweis

„i) $\Rightarrow$ ii)“: Sei $(M'_k)_{k\in\mathbb{N}}$ eine aufsteigende (bzw. absteigende) Folge von A-Untermoduln von M', dann ist $(f(M'_k))_{k\in\mathbb{N}}$ eine aufsteigende (bzw. absteigende) Folge von A-Untermoduln von M und somit stationär. Da f injektiv ist, gilt $f^{-1}(f(M'_k)) = M'_k$, also ist auch $(M'_k)_{k\in\mathbb{N}}$ stationär und daher ist M' Noethersch (bzw. Artinsch).
Sei $(M''_k)_{k\in\mathbb{N}}$ eine aufsteigende (bzw. absteigende) Folge von A-Untermoduln von M'', dann ist $\left(g^{-1}(M''_k)\right)_{k\in\mathbb{N}}$ eine aufsteigende (bzw. absteigende) Folge von A-Untermoduln von M und somit stationär. Da g surjektiv ist, gilt $g\left(g^{-1}(M''_k)\right) = M''_k$, also ist auch $(M''_k)_{k\in\mathbb{N}}$ stationär und somit ist M'' Noethersch (bzw. Artinsch).
„ii) $\Rightarrow$ i)“: Sei $(M_k)_{k\in\mathbb{N}}$ eine aufsteigende (bzw. absteigende) Folge von A-Untermoduln von M, dann sind $\left(f^{-1}(M_k)\right)_{k\in\mathbb{N}} \subseteq M'$ und $(g(M_k))_{k\in\mathbb{N}} \subseteq M''$ aufsteigende (bzw. absteigende) Folgen von A-Untermoduln und somit stationär, also gibt es $n_1,n_2 \in \mathbb{N}$, sodass für alle $m_1 \geq n_1$ (bzw. $m_1 \leq n_1$) und alle $m_2 \geq n_2$ (bzw. $m_2 \leq n_2$) gilt:

$$g(M_{n_1}) = g(M_m) \qquad f^{-1}(M_{n_2}) = f^{-1}(M_m)$$

Sei nun $n = \max\{n_1,n_2\}$ (bzw. $n = \min\{n_1,n_2\}$), so gilt für alle $m \geq n$ (bzw. $m \leq n$):

$$g(M_m) = g(M_n) \qquad f^{-1}(M_m) = f^{-1}(M_n)$$

Sei $x \in M_m$ für ein $m \geq n$ (bzw. $m \leq n$). Falls $x \in \operatorname{im}(f)$ liegt, gibt es ein $x' \in M'$ mit $f(x') = x$. Wegen $f^{-1}(M_m) = f^{-1}(M_n)$ gilt $x' \in f^{-1}(M_n)$ und somit $x = f(x') \in M_n$.
Falls $x \notin \operatorname{im}(f) = \ker(g)$ liegt, folgt $0 \neq g(x) \in g(M_m) = g(M_n)$. Also gibt es ein $y \in M_n$ mit:

$$\begin{aligned} g(x) &= g(y) \\ g(x-x) &= 0 \\ x-y &\in \ker(g) = \operatorname{im}(f) \end{aligned}$$

Wie oben gezeigt, gilt dann $x - y \in M_n$. Somit ist auch $x = y + (x-y) \in M_n$. Also gilt $M_m = M_n$ und somit ist M Noethersch (bzw. Artinsch). $\square_{6.7}$

6.8 Korollar (stabil unter direkter Summe)

Seien A ein Ring, $n \in \mathbb{N}_{\geq 1}$ und $M_1,\ldots,M_n$ Noethersche (bzw. Artinsche) A-Moduln.

Dann ist der A-Modul $\bigoplus_{i=1}^{n} M_i$ Noethersch (bzw. Artinsch).

Beweis

Führe eine Induktion über n durch:

Der Induktionsanfang bei $n = 1$ ist wegen $\bigoplus_{i=1}^{1} M_i = M_i$ klar.

Induktionsschritt $n-1 \rightsquigarrow n$: Nach Induktionsvoraussetzung ist $\bigoplus_{i=1}^{n-1} M_i$ ein Noetherscher (bzw. Artinsche) A-Modul und nach Voraussetzung gilt dies auch für M_n. Daher folgt die Behauptung für n aus 6.7 angewandt auf die exakte Folge:

$$0 \to \bigoplus_{i=1}^{n-1} M_i \xrightarrow{f} \bigoplus_{i=1}^{n} M_i \xrightarrow{g} M_n \to 0$$

$$f(x_1, \ldots, x_{n-1}) := (x_1, \ldots, x_{n-1}, 0)$$
$$g(x_1, \ldots, x_n) := x_n$$

$\square_{6.8}$

6.9 Beispiel

i) Wegen 6.3 ii) und 6.6 mit $A = M$ ist ein Ring A genau dann Noethersch, wenn jedes seiner Ideale endlich erzeugt ist.

ii) Wegen i) ist jeder Hauptidealring Noethersch.
Ist k ein Körper, so ist der Polynomring $k\left[X_n \middle| n \in \mathbb{N}\right]$ nicht Noethersch, denn

$$\mathfrak{m} := \left(X_n \middle| n \in \mathbb{N}\right)$$

ist nicht endlich erzeugt.

iii) Ein Körper ist sowohl Artinsch, als auch Noethersch, da der einzige echte A-Untermodul (0) ist.

6.10 Proposition

Sind A ein Noetherscher (bzw. Artinscher) Ring und M ein endlich erzeugter A-Modul, so ist der Modul M auch Noethersch (bzw. Artinsch).

Beweis

Da M endlich erzeugt ist, existiert ein $n \in \mathbb{N}$ und eine kurze exakte Folge von A-Moduln:

$$0 \to K \to A^n = \bigoplus_{i=1}^{n} A \to M \to 0$$

Nach 6.8 (mit $M_1 = \ldots = M_n = A$) ist A^n als direkte Summe Noethersch (bzw. Artinsch) und nach 6.7 „i) $\Rightarrow$ ii)“ gilt dies auch für K und M. $\square_{6.10}$

6.11 Proposition

Seien A ein Noetherscher (bzw. Artinscher) Ring und $I \subseteq A$ ein Ideal, dann ist der Ring ${}^{A}/_{I}$ Noethersch (bzw. Artinsch).

Beweis

Wegen der kurzen exakten Folge von A-Moduln

$$0 \to I \to A \to {}^{A}/_{I} \to 0$$

und 6.7 „i) $\Rightarrow$ ii)“ ist der A-Modul ${}^{A}/_{I}$ Noethersch (bzw. Artinsch).
Dasselbe gilt dann für den ${}^{A}/_{I}$-Modul ${}^{A}/_{I}$, denn die A-Untermoduln von ${}^{A}/_{I}$ und die ${}^{A}/_{I}$-Untermoduln von ${}^{A}/_{I}$ sind dieselben, da die Multiplikation in ${}^{A}/_{I}$ gerade über die Multiplikation in A definiert ist. $\square_{6.11}$

6.12 Proposition

Seien $A = k$ ein Körper und $M = V$ ein A-Modul, das heißt ein k-Vektorraum. Dann sind äquivalent:

i) $\dim_k(V) < \infty$

ii) V ist Noethersch.

iii) V ist Artinsch.

Beweis

Ein Vektorraum ist genau dann endlich erzeugt, wenn er endlich-dimensional ist. Damit folgt die Äquivalenz von i) und ii) aus 6.6 und Linearer Algebra I, denn jeder Untervektorraum von V ist endlich-dimensional, wenn V endlich-dimensional ist.
„i) $\Rightarrow$ iii)“: Eine strikt fallende Folge von Untervektorräumen $V \supseteq V_1 \supsetneq V_2 \supsetneq \dots$ erfüllt:

$$0 \leq \dim_k(V_{i+1}) \leq \dim_k(V_i) - 1$$

Also ist die Folge endlich, da der einzige Vektorraum mit Dimension 0 schon $V_n = \{0\}$ ist.
„iii) $\Rightarrow$ i)“: Wäre $\dim_k(V) = \infty$, so existierte eine unendliche linear unabhängige Teilmenge $\{v_n | n \in \mathbb{N}\} \subseteq V$ und

$$V_n := \sum_{m \geq n} k \cdot v_m$$

wäre eine unendlich lange Folge von strikt fallenden Untervektorräumen von V. $\square_{6.12}$

6.13 Korollar

Sei A ein Ring, in dem das Nullideal Produkt endlich vieler maximaler Ideale ist. Dann ist A genau dann Noethersch, wenn A Artinsch ist.

Beweis

Schreibe:

$$(0) = \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_n \subseteq A$$

Dabei müssen die maximalen Ideale $\mathfrak{m}_i$ nicht paarweise verschieden sein. Erhalte eine absteigende Folge von A-Untermoduln:

$$I_0 := A \supseteq I_1 := \mathfrak{m}_1 \supseteq I_2 := \mathfrak{m}_1 \cdot \mathfrak{m}_2 \supseteq \ldots \supseteq I_n := \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_n = (0)$$

Dann ist für alle $0 \leq k \leq n-1$ der Quotient ${}^{I_k}\!/_{I_{k+1}}$ ein ${}^{A}\!/_{\mathfrak{m}_{k+1}}$-Vektorraum, denn es gilt $\mathfrak{m}_{k+1} \cdot I_k \subseteq I_{k+1}$.
Es folgt:

$$\begin{aligned} A \text{ Noethersch} &\overset{6.7}{\Leftrightarrow} \underset{0\leq k\leq n-1}{\forall} : \text{ der } A\text{-Modul } {}^{I_k}\!/_{I_{k+1}} \text{ ist Noethersch} \\ &\overset{\text{Beweis von 6.11}}{\Leftrightarrow} \underset{0\leq k\leq n-1}{\forall} : \text{ der } {}^{A}\!/_{\mathfrak{m}_{k+1}}\text{-Vektorraum } {}^{I_k}\!/_{I_{k+1}} \text{ ist Noethersch} \\ &\overset{6.12\ \text{ii)}\Leftrightarrow\text{iii)}}{\Leftrightarrow} \underset{0\leq k\leq n-1}{\forall} : \text{ der } {}^{A}\!/_{\mathfrak{m}_{k+1}}\text{-Vektorraum } {}^{I_k}\!/_{I_{k+1}} \text{ ist Artinsch} \\ &\overset{6.7}{\Leftrightarrow} A \text{ ist Artinsch} \end{aligned}$$

$\square_{6.13}$

6.14 Beispiel

Sind A ein Hauptidealring und $0 \neq I \subseteq A$ ein Ideal, so ist ${}^{A}\!/_{I}$ Artinsch.
Zum Beispiel: ${}^{k[X]}\!/_{(X^n)}$

Beweis

Da A ein Hauptidealring ist, ist A nach 6.4 oder auch 6.9 Noethersch. Nach 6.11 ist dann auch ${}^{A}\!/_{I}$ Noethersch.
Da A ein Hauptidealring ist, gibt es ein $a \in A \setminus \{0\}$ mit $(0) \neq I = (a)$. Aus demselben Grund ist A faktoriell und somit gibt es endlich viele Primfaktoren $p_1, \ldots, p_n$ (nicht notwendig paarweise verschieden) und eine Einheit $e \in A^*$ mit:

$$a = e \prod_{i=1}^{n} p_n$$

Nun ist $(p_k) \subseteq A$ ein Primideal und da A ein Hauptidealring ist, auch ein maximales Ideal, denn aus $(p_k) \subsetneq (m)$ folgt $m | p_k$, also $m \in A^*$ und somit $(m) = A$. Zudem gilt:

$$(a) = (p_1) \cdot \ldots \cdot (p_n)$$

In ${}^{A}\!/_{I}$ folgt:

$$(0) = {}^{(a)}\!/_{(a)} = {}^{(p_1) \cdot \ldots \cdot (p_n)}\!/_{(a)} = {}^{(p_1)}\!/_{(a)} \cdot \ldots \cdot {}^{(p_n)}\!/_{(a)}$$

Zudem sind die Ideale ${}^{(p_k)}/_{(a)} \subseteq {}^{A}/_{(a)}$ maximal, denn

$$ {}^{A}/_{(a)} \,/{}^{(p_k)}/_{(a)} \cong {}^{A}/_{(p_k)} $$

ist ein Körper, da $(p_k) \subseteq A$ maximal ist. Nach 6.13 ist also ${}^{A}/_{I}$ auch Artinsch, da der Ring Noethersch ist. $\square_{6.14}$

7 Noethersche Ringe

7.1 Erinnerung

Für einen Ring A sind äquivalent:

i) Jede nicht-leere Menge von Idealen besitzt ein maximales Element (bezüglich der Inklusion).

ii) Jede aufsteigende Folge von Idealen in A ist stationär.

iii) Jedes Ideal von A ist endlich erzeugt.

Ein solcher Ring A heißt Noethersch.

Beweis

Vergleiche mit den Definitionen 6.3 ii) und 6.2 und der Proposition 6.6. $\square_{7.1}$

7.2 **Satz** (endlich viele minimale Primideale)

Die Menge der minimalen Primideale eines Noetherschen Ringes A ist endlich.

Beweis

Angenommen A wäre ein Noetherscher Ring mit unendlich vielen minimalen Primidealen.
Betrachte die Menge:

$$\Sigma := \left\{ I \subseteq A \middle| I \text{ ist Ideal und } {}^{A}\!/_{I} \text{ besitzt unendlich viele minimale Primideale} \right\}$$

Da ${}^{A}\!/_{(0)} \cong A$ nach Annahme unendlich vielen minimalen Primidealen besitzt, ist $(0) \in \Sigma$ und somit Σ nicht leer. Wegen 7.1 i) existiert ein maximales Element $I \in \Sigma$.
Für den Ring $A' := {}^{A}\!/_{I}$ gelten:

1. A' ist nach 6.11 Noethersch.
2. A' besitzt wegen $I \in \Sigma$ unendlich viele minimale Primideale.
3. Für jedes Ideal $(0) \neq J \subseteq A'$ besitzt ${}^{A'}\!/_{J}$ wegen der Maximalität von $I \in \Sigma$ nur endlich viele minimale Primideale.

Offenbar ist wegen 2. das Ideal $(0) \subseteq A'$ kein Primideal, da es sonst das einzige minimale Primideal wäre. Das heißt A' ist kein Integritätsring und daher gibt es $x,y \in A' \setminus \{0\}$ mit $xy = 0$. Ist $\mathcal{P} \subseteq A'$ ein Primideal, so folgt $xy = 0 \in \mathcal{P}$ und da $\mathcal{P}$ ein Primideal ist, folgt $x \in \mathcal{P}$ oder $y \in \mathcal{P}$.

Da dies für jedes der unendlich vielen minimalen Primideal gilt, können wir ohne Einschränkung annehmen, dass $x \in \mathcal{P}$ für unendlich viele minimale Primideale $\mathcal{P} \subseteq A'$ gilt.

Offenbar ist für jedes solche $\mathcal{P}$ nun ${}^{\mathcal{P}}\!/_{(x)} \subseteq {}^{A'}\!/_{(x)}$ ein minimales Primideal, also besitzt ${}^{A'}\!/_{(x)}$ unendlich viele minimale Primideale im Widerspruch zu 3. und $x \neq 0$. $\square_{7.2}$

7.3 Beispiel

Seien k ein algebraisch abgeschlossener Körper, $n,m \in \mathbb{N}_{\geq 1}$ und $f_1,\ldots,f_m \in k[X_1,\ldots,X_n]$.

Für $J := (f_1,\ldots,f_m)$ ist die Abbildung

$$\mathcal{N}(J) := \left\{ \underline{\alpha} \in k^n \,\middle|\, \underset{1\leq i\leq m}{\forall} f_i(\underline{\alpha}) = 0 \right\} \xrightarrow{\sim} \operatorname{MaxSpec}\left({}^{k[X_1,\ldots,X_n]}\!/_J \right)$$
$$\underline{\alpha} \mapsto {}^{\mathfrak{m}_{\underline{\alpha}}}\!/_J$$

bijektiv. (vergleiche Beweis von 5.3)

Der Ring ${}^{k[X_1,\ldots,X_n]}\!/_J$ ist eine endlich erzeugte k-Algebra, also nach 7.6 ii) Noethersch.

Seien $\{\mathcal{P}_1,\ldots,\mathcal{P}_N\}$ seine minimalen Primideale. Dann gilt:

$$\mathcal{N}(J) = \bigcup_{i=1}^{N} \mathcal{N}(\mathcal{P}_i)$$

Dies ist eine Verallgemeinerung der Zerlegung eines Polynoms in irreduzible Faktoren, also des Falls $n = 1$.

7.4 Satz (Stabilitätseigenschaften)

Sei A ein Noetherscher Ring.

i) Ist $I \subseteq A$ ein Ideal, so ist ${}^{A}\!/_{I}$ Noethersch.

ii) Jede endliche A-Algebra B ist Noethersch.

iii) Ist $S \subseteq A$ multiplikativ abgeschlossen, so ist $S^{-1}A$ Noethersch.

iv) Ist $\mathfrak{p} \subseteq A$ ein Primideal, so ist $A_{\mathfrak{p}}$ Noethersch.

v) Ist M ein endlich erzeugter A-Modul, so ist M Noethersch und endlich präsentiert.

Beweis

i) 6.11

ii) Jedes Ideal von B ist insbesondere ein A-Untermodul von B und der A-Modul B ist nach 6.10 Noethersch.

iii) 7.1 ii) und 3.19.

iv) Wähle $S := (A \setminus \mathfrak{p})$ in iii).

v) Die erste Aussage ist 6.10. Nach Voraussetzung existiert ein $n \geq 0$ und ein A-linearer Epimorphismus $\pi : A^n \twoheadrightarrow M$. Erhalte eine kurze exakte Folge:

$$0 \to K := \ker(\pi) \to A^n \xrightarrow{\pi} M \to 0$$

Da A^n nach 6.10 Noethersch ist und nach 6.6 i) $\Rightarrow$ ii) folgt, dass der A-Modul $K \hookrightarrow A^n$ endlich erzeugt ist, also ist obige Folge eine endliche Präsentation von M. $\square_{7.4}$

7.5 **Satz** (Hilbertscher Basissatz)

Ist A ein Noetherscher Ring, so auch $A[X]$.

Beweis

Sei $I \subseteq A[X]$ ein Ideal. Wegen 7.1 iii) ist zu zeigen, dass I endlich erzeugt ist.
Für ein Polynom $f \in A[X]$ schreibe:

$$l(f) := \begin{Bmatrix} \text{höchster Koeffizient von } f & \text{falls } f \neq 0 \\ 0 & \text{sonst} \end{Bmatrix} \in A$$

Behauptung I: $J := \{l(f) \,|\, f \in I\} \subseteq A$ ist ein Ideal.

Beweis: Es gilt

$$l(f) - l(g) = l\underbrace{\left(f \cdot X^{\deg(g)-\deg(f)} - g\right)}_{\in I}$$

falls $\deg(g) \geq \deg(f)$, sonst analog. Für alle $a \in A$ ist:

$$a \cdot l(f) = l\underbrace{(af)}_{\in I}$$

$\square_{\text{Behauptung I}}$

Da A Noethersch ist, folgt nach 6.6 nun $J = (a_1, \ldots, a_n)$ für ein $n \in \mathbb{N}_{\geq 1}$ und geeignete $a_i \in A$. Nach Definition gibt es $f_i \in I$ $(1 \leq i \leq n)$ mit $a_i = l(f_i)$. Setze:

$$r := \max_{1 \leq i \leq m} (\deg(f_i))$$
$$M := \sum_{i=0}^{r-1} A \cdot X^i \subseteq A[X]$$
$$I' := (f_1, \ldots, f_n) \subseteq A[X]$$

Behauptung II: $I = (I \cap M) + I'$

Beweis: „$\supseteq$“: Dies ist wegen $f_i \in I$, also $I' \subseteq I$ und $I \cap M \subseteq I$ klar.
„$\subseteq$“: Ansonsten sei $f \in I \setminus ((I \cap M) + I')$ von minimalem Grad $N \in \mathbb{N}$ gewählt. Nach Definition von M gilt:

$$n \geq r = \max_{1 \leq i \leq m} (\deg(f_i))$$

Es folgt $N \geq \deg(f_i)$ für alle $1 \leq i \leq m$. Wegen $f \in I$ gilt mit geeigneten $\alpha_i \in A$:

$$J \ni l(f) = \sum_{i=1}^{n} \alpha_i a_i$$

Betrachte:

$$g := \sum_{i=1}^{N} \alpha_i f_i X^{n-\deg(f_i)} \qquad h := f - g$$
$$\deg(g) = N$$

Damit folgt:

$$l(h) = l(f-g) = l(f) - \sum_{i=1}^{n} \alpha_i \underbrace{l\left(f_i \cdot X^{N-\deg(f_i)}\right)}_{=l(f_i)=a_i} = 0$$

Also gilt:

$$N > \deg(h)$$

Nun gelten $f \in I$ und $f_i \in I$ und somit auch $h \in I$. Wegen $N > \deg(h)$ und der Minimalität von N folgt $h \in I' + (I \cap M)$. Wegen $g \in I'$ folgt $f = h + g \in I' + (I \cap M)$. Dies ist ein Widerspruch zu $f \in I \setminus ((I \cap M) + I')$. $\square_{\text{Behauptung II}}$

Da A Noethersch ist und M ein endlich erzeugter A-Modul ist, also auch Noethersch ist. Somit ist auch der A-Modul $M \cap I \subseteq M$ endlich erzeugt. Sind $g_1, \ldots, g_m \in I \cap M$ nun A-Modul-Erzeuger von $M \cap I$, so folgt:

$$I \overset{\text{Beh. II}}{=} (g_1, \ldots, g_m) + (f_1, \ldots, f_n)$$

Somit ist I endlich erzeugt. $\square_{7.5}$

7.6 **Korollar** (endlich erzeugte Algebra Noethersch)

i) Ist A ein Noetherscher Ring, so ist jede endlich erzeugte A-Algebra B Noethersch. (vergleiche 7.4 iii))

ii) Jeder endlich erzeugter Ring und jede über einem Körper endlich erzeugte Algebra ist Noethersch.

Beweis

i) Als A-Algebra gilt für ein geeignetes $n \in \mathbb{N}_{\geq 1}$ und einem geeigneten $Q \subseteq A[X_1, \ldots, X_n]$:

$$B \cong A[X_1, \ldots, X_n] / Q$$

Induktiv folgt aus 7.5, dass $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, und damit nach 7.4 i) auch B, Noethersch ist.

ii) Da $\mathbb{Z}$ und jeder Körper Noethersch sind, folgt dies direkt aus i).

7.7 Korollar

Seien k ein Körper, $n \in \mathbb{N}_{\geq 1}$, I eine Menge und für jedes $i \in I$ sei $f_i \in k[X_1, \ldots, X_n]$.
Dann existiert eine *endliche* Teilmenge $I_0 \subseteq I$ so, dass für alle $\underline{\alpha} \in k^n$ gilt:

$$\left(\underset{i \in I_0}{\forall} : f_i(\underline{\alpha}) = 0 \right) \Rightarrow \left(\underset{i \in I}{\forall} : f_i(\underline{\alpha}) = 0 \right)$$

Das heißt, die Nullstellenmenge $\mathcal{N}\left(f_i \middle| i \in I\right)$ kann durch endlich viele Gleichungen beschrieben werden.

Beweis

Da k Noethersch ist, gilt dies nach 7.6 auch für die endlich erzeugte k-Algebra $k[X_1, \ldots, X_n]$.
Betrachte das Ideal $J := \left(f_i \middle| i \in I\right) \subseteq k[X_1, \ldots, X_n]$. Dieses ist nach 6.6 endlich erzeugt, es gibt also eine endliche Menge $I_0 \subseteq I$ mit $J = \left(f_i \middle| i \in I_0\right)$. Sei $\underline{\alpha} \in k^n$ mit $f_i(\underline{\alpha}) = 0$ für alle $i \in I_0$.
Ist $f \in J$, so gibt es $a_i \in k$ für alle $i \in I_0$ mit:

$$f = \sum_{i \in I_0} a_i f_i$$

Es folgt:

$$f(\underline{\alpha}) = \sum_{i \in I_0} a_i \underbrace{f_i(\underline{\alpha})}_{=0} = 0$$

$\square_{7.7}$

8 Artinsche Ringe

8.1 Proposition

Sei A ein Ring.

i) Sind $n \in \mathbb{N}_{\geq 1}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq A$ Primideale und $I \subseteq A$ ein Ideal mit $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, so existiert ein $1 \leq i \leq n$ mit $I \subseteq \mathfrak{p}_i$.

ii) Sind $n \in \mathbb{N}_{\geq 1}$, $I_1, \ldots, I_n \subseteq A$ und $\mathfrak{p} \subseteq A$ ein Primideal mit $\bigcap_{i=1}^{n} I_i \subseteq \mathfrak{p}$, so existiert ein $1 \leq i \leq n$ mit $I_i \subseteq \mathfrak{p}$.
Im Fall $\mathfrak{p} = \bigcap_{i=1}^{n} I_i$ existiert ein $1 \leq i \leq n$ mit $\mathfrak{p} = I$.

Beweis

i) Durch Induktion über $n \geq 1$ zeigen wir die äquivalente Aussage:

$$\left(\underset{1 \leq i \leq n}{\forall} : I \not\subseteq \mathfrak{p}_i \right) \Rightarrow \left(I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i \right)$$

$n = 1$: Ist klar.

$n > 1$: Für alle $1 \leq i \leq n$ existiert nach Induktionsvoraussetzung angewendet auf die $(n-1)$ Primideale $\mathfrak{p}_1, \ldots, \widehat{\mathfrak{p}_i}, \ldots, \mathfrak{p}_n$ ein

$$x_i \in I \tag{8.1}$$

mit:

$$x_i \notin \mathfrak{p}_j \underset{1 \leq j \leq n, j \neq i}{\forall} \tag{8.2}$$

1. Fall: Es gilt $x_{i_0} \notin \mathfrak{p}_{i_0}$ für ein $1 \leq i_0 \leq n$. Dann gelten $x_{i_0} \in I$ und $x_{i_0} \notin \mathfrak{p}_j \, \forall_{1 \leq j \leq n}$, also $I \subsetneq \bigcup_{i=1}^{n} \mathfrak{p}_i$. $\square_{\text{1. Fall}}$

2. Fall: Es gilt $x_i \in \mathfrak{p}_i$ für alle $1 \leq i \leq n$. Betrachte für alle $1 \leq i \leq n$:

$$p_i := x_1 \cdot \ldots \cdot \hat{x}_i \cdot \ldots \cdot x_n$$

Dann gelten:

$$\underset{1\le i\le n}{\forall} : p_i \in I \quad \text{(wegen } n \geq 2 \text{ und (8.1))} \tag{8.3}$$

$$\underset{1\le i\neq j\le n}{\forall} : p_i \in \mathfrak{p}_j \quad \text{(wegen } x_j \in \mathfrak{p}_j \text{ und } p_i \in (x_j)) \tag{8.4}$$

$$\underset{1\le i\le n}{\forall} : p_i \notin \mathfrak{p}_i \tag{8.5}$$

Letzteres gilt, denn sonst müsste, da $\mathfrak{p}_i$ ein Primideal ist und wegen der Definition von p_i schon $x_j \in \mathfrak{p}_i$ für ein $i \neq j$ gelten. (vergleiche (8.2))
Es folgt

$$y := \sum_{i=1}^{n} p_i \overset{(8.3)}{\in} I$$

und für alle $1 \leq i \leq n$ schon $y \notin \mathfrak{p}_i$, denn sonst folgt $\mathfrak{p}_i \ni y = \sum_{i=1}^{n} p_i$ und mit (8.4) schon $p_i \in \mathfrak{p}_i$ im Widerspruch zu (8.5).

Also gilt $\mathfrak{p} \in I \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i$ und damit $I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. $\square_{\text{i)}}$

ii) Angenommen dies gilt nicht, das heißt es gelte:

$$\underset{1\le i\le n}{\forall} : I_i \not\subseteq \mathfrak{p} \Rightarrow \underset{1\le i\le n}{\forall} \underset{x_i\in I_i}{\exists} x_i \notin \mathfrak{p} \Rightarrow x := \prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$$

Da $\mathfrak{p}$ ein Primideal ist und wegen $x_i \notin \mathfrak{p}$ gilt $x \notin \mathfrak{p}$. Es folgt $x \in (\bigcap_{i=1}^{n} I_i) \setminus \mathfrak{p}$. Dies ist ein Widerspruch zu $\bigcap_{i=1}^{n} I_i \subseteq \mathfrak{p}$.
Gilt nun sogar $\bigcap_{i=1}^{n} I_i = \mathfrak{p}$, so existiert wieder ein $1 \leq i \leq n$ mit $I_i \subseteq \mathfrak{p} = \bigcap_{i=1}^{n} I_i \subseteq I_i$ und es folgt $\mathfrak{p} = I_i$.

$\square_{8.1}$

8.2 **Proposition** (jedes Primideal maximal)

In einem Artinschen Ring ist jedes Primideal maximal.

Beweis

Sei $\mathfrak{p} \subseteq A$ ein Primideal. Wegen 6.7 i) $\Rightarrow$ ii) ist $A/\mathfrak{p}$ ein Artinscher Integritätsring.
Für $0 \neq x \in A/\mathfrak{p}$ erhalte die stationäre Folge mit geeignetem $n \in \mathbb{N}_{\geq 1}$:

$$(x) \supseteq \left(x^2\right) \supseteq \ldots \supseteq (x^n) = \left(x^{n+1}\right)$$

Es folgt mit geeignetem $y \in A/\mathfrak{p}$:

$$x^n = y \cdot x^{n+1}$$

Da $A/\mathfrak{p}$ ein Integritätsring ist, kann man durch x^n teilen und es folgt:

$$1 = xy$$

Also ist $x \in \left(A/\mathfrak{p}\right)^*$. Insgesamt gilt $\left(A/\mathfrak{p}\right) \setminus \{0\} \subseteq \left(A/\mathfrak{p}\right)^*$ und somit ist $A/\mathfrak{p}$ ein Körper, das heißt $\mathfrak{p} \subseteq A$ ist maximal. $\square_{8.2}$

8.3 Proposition (endlich viele maximale Ideale)

Ein Artinscher Ring besitzt nur endlich viele maximale Ideale.

Beweis

Sei ohne Einschränkung $A \neq \{0\}$. Betrachte die Menge von Idealen:

$$\Sigma := \{\text{endliche Durchschnitte maximaler Ideale von } A\}$$

Wegen $A \neq \{0\}$ ist $\Sigma \neq \emptyset$, da es dann ein maximales Ideal gibt, und dieses sein eigener Durchschnitt ist.

Da A Artinsch ist, existiert ein bezüglich der Inklusion minimales $I \in \Sigma$.

Schreibe $I = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ für $n \geq 1$ und geeignete maximale Ideale $\mathfrak{m}_i \subseteq A$. Ist nun $\mathfrak{m} \subseteq A$ ein beliebiges maximales Ideal, so folgt aus der Minimalität von I:

$$\mathfrak{m} \cap I = I$$

Denn I ist Durchschnitt endlich vieler maximaler Ideale, also auch $\mathfrak{m} \cap I$, aber I ist minimal mit dieser Eigenschaft. Also gilt $I \subseteq \mathfrak{m}$.

Aus 8.1 ii) mit $I_i := \mathfrak{m}_i$ und $\mathfrak{p} := \mathfrak{m}$ folgt $\mathfrak{m}_i \subseteq \mathfrak{m}$ für ein $1 \leq i \leq n$.

Da $\mathfrak{m}_i$ und $\mathfrak{m}$ beide maximal sind, folgt $\mathfrak{m}_i = \mathfrak{m}$. Also sind $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ bereits alle maximalen Ideale von A. $\square_{8.3}$

8.4 Proposition

Ist A ein Artinscher Ring, so existiert ein $N \geq 1$ mit $\mathfrak{N}(A)^N = (0)$.

Beweis

Schreibe $\mathfrak{N} := \mathfrak{N}(A)$. Wir haben die stationäre Folge mit geeignetem $N \in \mathbb{N}_{\geq 1}$.

$$\mathfrak{N} \supseteq \mathfrak{N}^2 \supseteq \ldots \supseteq \mathfrak{N}^N = \mathfrak{N}^{N+1} =: I$$

Beachte, dass für alle $k \in \mathbb{N}$ schon $\mathfrak{N}^{N+k} = \mathfrak{N}^N$ gilt.

Angenommen es wäre $I \neq (0)$. Betrachte:

$$\Sigma := \left\{ J \subseteq A \middle| J \text{ ist Ideal } JI \neq (0) \right\}$$

Wegen

$$I \cdot I = \mathfrak{N}^{2N} = \mathfrak{N}^N = I$$

gilt $I \in \Sigma$, also $\Sigma \neq \emptyset$. Da A Artinsch ist, existiert ein minimales $J \in \Sigma$. Aus $IJ \neq (0)$ folgt, dass es ein $x \in J$ mit $I \cdot (x) \neq (0)$ gibt. Aus der Minimalität von J folgt $J = (x)$. Weiter gilt:

$$((x)\, I)\, I = (x)\, I^2 = (x)\, I \neq (0)$$

Also ist $(x)\, I \in \Sigma$. Aus $(x)\, I \subseteq (x)$ und der Minimalität von $(x) \in \Sigma$ folgt $(x)\, I = (x)$ und damit $x = xy$ für ein geeignetes $y \in I$. Es folgt für alle $n \in \mathbb{N}$:

$$x = xy = xy^2 = \ldots = xy^n$$

Wegen $y \in I \subseteq \mathfrak{N}(A)$ gibt es ein $n \in \mathbb{N}$ mit $y^n = 0$ und es folgt $x = 0$. Also ist $J = (x) = (0)$ im Widerspruch zu $JI \neq (0)$. $\square_{8.4}$

8.5 **Definition und Beispiel** (Krull-Dimension)

Sei A ein Ring.

i) Eine *Kette von Primidealen in A* ist eine strikt aufsteigende Folge $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ von Primidealen.

   $n \in \mathbb{N}$ heißt *die Länge der Kette*.

ii) Die *(Krull-)Dimension* ist das Supremum über die Länge aller Ketten von Primidealen in A, geschrieben:

$$\dim(A) \in \mathbb{N} \cup \{\infty\}$$

iii) Für einen Körper k gilt $\dim(k) = 0$.

   Für einen Hauptidealring A, der kein Körper ist, gilt $\dim(A) = 1$, denn jedes von (0) verschiedene Primideal ist maximal.

   Ist k ein Körper, so gilt $\dim\left(k\left[X_n \middle| n \in \mathbb{N}\right]\right) = \infty$, denn die Kette

$$(X_1) \subsetneq (X_1,X_2) \subsetneq (X_1,X_2,X_3) \subsetneq \ldots$$

   von Primidealen ist unendlich lang.

   Es existieren sogar Noethersche Ringe A mit $\dim(A) = \infty$. (ohne Beweis)

iv) Für eine ganze Ringerweiterung $A \subseteq B$ gilt nach dem „Going-up-theorem“ 4.21:

$$\dim(A) \leq \dim(B)$$

v) Die Primidealkette

$$(0) \subsetneq (X) \subsetneq (2,X) \subseteq \mathbb{Z}[X]$$

   zeigt $\dim(\mathbb{Z}[X]) \geq 2$. Es gilt sogar $\dim(\mathbb{Z}[X]) = 2$ und allgemeiner:

   Ist A Noethersch, so ist $\dim(A[X]) = \dim(A) + 1$. (ohne Beweis)

8.6 **Satz** (Charakterisierung Artinscher Ring)

Für einen Ring A sind äquivalent:

i) A ist Artinsch.

ii) A ist Noethersch und es gilt $\dim(A) = 0$.

Beweis

„i) ⇒ ii)“: Wegen 8.2 gilt $\dim(A) = 0$. Damit sind die endlich vielen (vergleiche 8.3) maximalen Ideale $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ bereits alle Primideale von A und es gilt:

$$\prod_{i=1}^{n} \mathfrak{m}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{m}_i \overset{1.30}{=} \mathfrak{N}(A)$$

Nach 8.4 existiert ein $N \in \mathbb{N}_{\geq 1}$ mit:

$$(0) = (\mathfrak{N}(A))^N \supseteq \left(\prod_{i=1}^{n} \mathfrak{m}_i \right)^N = \prod_{i=1}^{n} \mathfrak{m}_i^N$$

Also gilt:

$$\prod_{i=1}^{n} \mathfrak{m}_i^N = 0$$

Daher ist $(0) \subseteq A$ ein Produkt maximaler Ideale und aus 6.13 folgt, dass A Noethersch ist. $\square_{\text{i) ⇒ ii)}}$

„ii) ⇒ i)“: Seien $\mathfrak{m}_1, \ldots, \mathfrak{m}_n \subseteq A$ die minimalen Primideale (vergleiche 7.2). Wegen $\dim(A) = 0$ sind diese Ideale sogar maximal und bilden damit sogar alle Primideale von A. Also gilt:

$$\mathfrak{N}(A) \overset{1.30}{=} \bigcap_{i=1}^{n} \mathfrak{m}_i$$

Nun ist $\mathfrak{N}(A) \subseteq A$ endlich erzeugt, da A Noethersch ist, also $\mathfrak{N}(A) = (a_1, \ldots, a_m)$.
Für $1 \leq k \leq m$ ist $a_k \in \mathfrak{N}(A)$, also nilpotent, das heißt es gibt ein $n_k \in \mathbb{N}$ mit $a_k^{n_k} = 0$. Für

$$n_x := \max\{n_1, \ldots, n_m\} \qquad\qquad N := n_x \cdot m$$

gilt dann für alle a_k schon $a_k^N = a_k^{n_x} = 0$. Sei $a \in \mathfrak{N}(A)$, so gibt es $\alpha_1, \ldots, \alpha_m \in A$ mit:

$$a = \sum_{k=1}^{m} \alpha_k a_k$$

$$a^N = \left(\sum_{k=1}^{m} \alpha_k a_k \right)^N = \sum_{i_1 + \ldots + i_m = N} c_{i_1 \ldots i_m} a_1^{i_1} a_2^{i_2} \ldots a_m^{i_m} \tag{8.6}$$

Dabei sind $c_{i_1 \ldots i_m} \in A$ geeignet gewählt. Wegen $i_1 + \ldots + i_m = N = n_x \cdot m$ gilt:

$$i_k := \max\{i_1, \ldots, i_m\} \geq n_x$$

Denn andernfalls würde gelten:

$$N = i_1 + \ldots + i_m \leq m \cdot i_k < m \cdot n_x = N$$

Dann ist aber $a_k^{i_k} = 0$ und somit verschwindet jeder Summand in (8.6), das heißt es gilt $a^N = 0$.
Insgesamt ist $(\mathfrak{N}(A))^N = \left(\sqrt{(0)}\right)^N \subseteq (0)$, das heißt:

$$(0) = (\mathfrak{N}(A))^N = \left(\bigcap_{i=1}^{n} \mathfrak{m}_i\right)^N \supseteq \left(\prod_{i=1}^{n} \mathfrak{m}_i\right)^N = \prod_{i=1}^{n} \mathfrak{m}_i^N$$

Also ist $(0) \subseteq A$ Produkt maximaler Ideale und aus 6.13 folgt, dass A Artinsch ist. $\square_{8.6}$

8.7 Proposition

Sei $(A,\mathfrak{m})$ ein Noetherscher lokaler Ring. Dann gilt genau eine der folgenden Aussage:

i) Für alle $n \in \mathbb{N}$ gilt $\mathfrak{m}^{n+1} \subsetneq \mathfrak{m}^n$.

ii) Es gibt ein $n \in \mathbb{N}$ mit $\mathfrak{m}^n = (0)$. In diesem Fall ist A Artinsch.

Beweis

Gelte i) nicht, das heißt es gibt ein $n \in \mathbb{N}$ mit $\mathfrak{m}^{n+1} = \mathfrak{m}^n$. Dann folgt:

$$\mathfrak{m} \cdot \mathfrak{m}^n = \mathfrak{m}^n$$

Da A Noethersch ist, ist der A-Modul $\mathfrak{m}^n \subseteq A$ endlich erzeugt. Wegen $\mathfrak{m} = \mathrm{Jac}(A)$ folgt aus dem Lemma von Nakayama 2.16 schon $\mathfrak{m}^n = (0)$.
Ist nun $\mathfrak{p} \subseteq A$ ein Primideal, so gilt:

$$\begin{aligned} & (0) = \mathfrak{m}^n \subseteq \mathfrak{p} \subseteq \mathfrak{m} \\ \Rightarrow \quad & \mathfrak{m} \subseteq \sqrt{(0)} \subseteq \underbrace{\sqrt{(\mathfrak{p})}}_{=\mathfrak{p}} \subseteq \underbrace{\sqrt{(\mathfrak{m})}}_{=\mathfrak{m}} \\ & \mathfrak{m} \subseteq \mathfrak{p} \subseteq \mathfrak{m} \end{aligned}$$

Also ist $\mathfrak{m} \in A$ das einzige Primideal und daher gilt $\dim(A) = 0$. Aus 8.6 ii) $\Rightarrow$ i) folgt, dass A Artinsch ist. $\square_{8.7}$

8.8 Beispiel

Für $n \in \mathbb{N}_{>0}$ ist $\mathbb{Z}/n\mathbb{Z}$ Artinsch, da $\left|\mathbb{Z}/n\mathbb{Z}\right| = n < \infty$ ist. Ist

$$n = \prod_{i=1}^{r} p_i^{n_i}$$

die Primfaktorzerlegung, so gilt nach dem Chinesischen Restsatz:

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{r} \left(\mathbb{Z}/p_i^{n_i}\mathbb{Z}\right)$$

Jeder der Ringe $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ ist Artinsch und lokal mit maximalem Ideal $p_i \cdot \left(\mathbb{Z}/p_i^{n_i}\mathbb{Z}\right)$.

8.9 **Satz** (Struktur Artinscher Ringe)

Jeder Artinsche Ring ist endliches Produkt Artinscher lokaler Ringe.

Beweis

Sei $\{\mathfrak{m}_1,\ldots,\mathfrak{m}_n\}$ die maximalen Ideal von A (vergleiche 8.3).
Nach dem Beweis von 8.6 „i) $\Rightarrow$ ii)“ gilt für geeignetes $N \in \mathbb{N}_{\geq 1}$:

$$(0) = \prod_{i=1}^{n} \mathfrak{m}_i^N$$

Behauptung: Für alle $1 \leq i,j \leq n$ mit $i \neq j$ gilt: $\mathfrak{m}_i^N + \mathfrak{m}_j^N = (1)$

Beweis: Wegen $\mathfrak{m}_i \neq \mathfrak{m}_j$ gilt ohne Einschränkung für $\mathfrak{m}_i$ die echte Inklusion $\mathfrak{m}_i \subsetneq \mathfrak{m}_i + \mathfrak{m}_j$ und, da $\mathfrak{m}_i$ maximal ist, folgt $\mathfrak{m}_i + \mathfrak{m}_j = (1)$, also $1 = x_i + x_j$ für geeignete $x_i \in \mathfrak{m}_i$ und $x_j \in \mathfrak{m}_j$. Es folgt:

$$1 = 1^{2N} = (x_i + x_j)^{2N} = \sum_{k=0}^{2N} \left(\begin{array}{c} 2N \\ k \end{array} \right) x_i^k x_j^{2N-k}$$

Für jedes $0 \leq k \leq 2N$ gilt:

$$x_i^k x_j^{2N-k} \in \begin{cases} \mathfrak{m}_i^N & \text{falls } k \geq N \\ \mathfrak{m}_j^N & \text{falls } k \leq N \end{cases}$$

Also folgt $1 \in \mathfrak{m}_i^N + \mathfrak{m}_j^N$. $\square_{\text{Behauptung}}$

Nach der Behauptung sind die $\mathfrak{m}_i^N,\ldots,\mathfrak{m}_n^N$ paarweise komaximal und aus dem Chinesischen Restsatz 1.35 a) i) folgt

$$\bigcap_{i=1}^{n} \mathfrak{m}_i^N = \prod_{i=1}^{n} \mathfrak{m}_i^N = (0)$$

und aus 1.35 a) ii) und b) folgt, dass

$$\begin{aligned} A &\xrightarrow{\sim} \prod_{i=1}^{n} {}^{A}\!/_{\mathfrak{m}_i^N} \\ x &\mapsto \left(x \mod \mathfrak{m}_i^N\right)_{1 \leq i \leq n} \end{aligned}$$

ein Ringisomorphismus ist. Offenbar ist jeder der Ringe ${}^{A}\!/_{\mathfrak{m}_i^N}$ als Quotient eines Artinschen Rings Artinsch und zudem lokal mit maximalem Ideal ${}^{\mathfrak{m}_i}\!/_{\mathfrak{m}_i^N}$, denn das Bild der $\mathfrak{m}_j$ für $j \neq i$ in ${}^{A}\!/_{\mathfrak{m}_i^N}$ ist das Einsideal: Es gilt $\mathfrak{m}_j^N \subseteq \mathfrak{m}_j$ und somit:

$$(1) = \mathfrak{m}_j^N + \mathfrak{m}_i^N \subseteq \mathfrak{m}_j + \mathfrak{m}_i^N$$

Also ist $\mathfrak{m}_j + \mathfrak{m}_i^N = (1)$ und es folgt:

$$\left(\text{Bild von } \mathfrak{m}_j \text{ in } {}^{A}\!/_{\mathfrak{m}_i^N}\right) = {}^{\left(\mathfrak{m}_j + \mathfrak{m}_i^N\right)}\!/_{\mathfrak{m}_i^N} = {}^{(1)}\!/_{\mathfrak{m}_i^N} = {}^{A}\!/_{\mathfrak{m}_i^N}$$

$\square_{8.9}$

8.10 Proposition

Seien $(A,\mathfrak{m})$ ein Artinscher lokaler Ring mit Restklassenkörper $k = {}^{A}\!/_{\mathfrak{m}}$. Dann sind folgende Aussagen äquivalent:

i) Jedes Ideal in A ist ein Hauptideal. (Beachte: Im Allgemeinen ist A kein Integritätsring und somit kein Hauptidealring, zum Beispiel $A = {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$.)

ii) Das Ideal $\mathfrak{m}$ ist ein Hauptideal.

iii) Es gilt:

$$\dim_k \left({}^{\mathfrak{m}}\!/_{\mathfrak{m}^2} \right) \leq 1$$

Beweis

„i) ⇒ ii)“ ist klar.
„ii) ⇒ iii)“: Wegen $\mathfrak{m} \cdot {}^{\mathfrak{m}}\!/_{\mathfrak{m}^2} = (0)$ ist ${}^{\mathfrak{m}}\!/_{\mathfrak{m}^2}$ ein $k = {}^{A}\!/_{\mathfrak{m}}$ -Vektorraum. Wegen $\mathfrak{m} = (x)$ ist $x + \mathfrak{m}^2 \in {}^{\mathfrak{m}}\!/_{\mathfrak{m}^2}$ ein k-Erzeugendensystem und somit folgt iii).
„iii) ⇒ ii)“: Ist $\dim_k \left({}^{\mathfrak{m}}\!/_{\mathfrak{m}^2} \right) = 0$, so gilt $\mathfrak{m} = \mathfrak{m}^2$, also $\mathfrak{m} = (0)$ nach dem Lemma von Nakayama, denn alle Ideale sind endlich erzeugt, weil A insbesondere Noethersch ist. Damit ist A ein Körper und i) ist klar.
Gelte nun $\dim_k \left({}^{\mathfrak{m}}\!/_{\mathfrak{m}^2} \right) = 1$, dann gibt es ein $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ und $0 \neq x + \mathfrak{m}^2 \in {}^{\mathfrak{m}}\!/_{\mathfrak{m}^2}$ ist eine k-Basis, das heißt $\mathfrak{m} = (x) + \mathfrak{m}^2$, und für den A-Untermodul $(x) \subseteq \mathfrak{m}$ gilt:

$$\mathfrak{m} \cdot \left({}^{\mathfrak{m}}\!/_{(x)} \right) = {}^{\mathfrak{m}^2 + (x)}\!/_{(x)} = {}^{\mathfrak{m}}\!/_{(x)}$$

Mit $\mathfrak{m}$ ist auch ${}^{\mathfrak{m}}\!/_{(x)}$ endlich erzeugt und zudem ist $\mathfrak{m} = \mathrm{Jac}\,(A)$ und somit folgt aus dem Lemma von Nakayama 2.16 schon ${}^{\mathfrak{m}}\!/_{(x)} = (0)$, das heißt $\mathfrak{m} = (x)$ ist ein Hauptideal.
„ii) ⇒ i)“: Sei nun $(0) \subsetneq I \subsetneq A$ ein Ideal.
Wegen $\mathfrak{m} = \mathfrak{N}\,(A)$, 8.4 und $I \neq (0), (1)$ existiert ein $n \geq 1$ mit $I \subseteq \mathfrak{m}^n = (x^n)$ und $I \not\subseteq \mathfrak{m}^{n+1} = \left(x^{n+1}\right)$.
Also existiert ein $y \in I \setminus \left(x^{n+1}\right)$ und wegen $I \subseteq (x^n)$ gilt $y = ax^n$ für ein geeignetes $a \in A$ und $a \notin (x)$, da $y \notin \left(x^{n+1}\right)$ ist. Wegen $a \notin (x) = \mathfrak{m} \subseteq A$ und weil $(A,\mathfrak{m})$ lokal ist, folgt $a \in A^*$ und damit $x^n = a^{-1}y \in I$, also $(x^n) \subseteq I$ und damit $I = (x^n)$, das heißt I ist ein Hauptideal. $\square_{8.10}$

8.11 Beispiel

i) Ein Artinscher Ring A, der ein Hauptidealring ist, ist ein Körper.

Beweis

Da A Artinsch ist, ist jedes Primideal maximal und somit ist A Jacobson. Außerdem hat A nur endlich viele maximale Ideale, das heißt endlich viele Primideale, also $|\mathrm{Spec}\,(A)| < \infty$.
Wäre A kein Körper, so folgt aus 5.9 schon $|\mathrm{Spec}\,(A)| = \infty$ im Widerspruch zu $|\mathrm{Spec}\,(A)| < \infty$. $\square_{\text{i)}}$

ii) Für $A = {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$ für eine Primzahl $p \in \mathbb{Z}$ und $n \in \mathbb{N}_{\geq 1}$ gelten die Bedingungen in 8.10.

iii) Seien $n \in \mathbb{N}_{\geq 1}$, k ein Körper und $A = {}^{k[X_1,\ldots,X_n]}\!/_{(X_1,\ldots,X_n)^2}$. Da $\mathfrak{m} := (X_1,\ldots,X_n) \subseteq k[X_1,\ldots,X_n]$ maximal ist, ist der lokale Ring $\left(A, \overline{\mathfrak{m}} := {}^{\mathfrak{m}}\!/_{\mathfrak{m}^2}\right)$ Artinsch, denn er ist Noethersch und $\dim(A) = 0$, und es gilt:

$$\dim_k \left({}^{\overline{\mathfrak{m}}}\!/_{\overline{\mathfrak{m}}^2}\right) = n$$

(vergleiche Blatt 2 Aufgabe 2 iii))

9 Etwas homologische Algebra

Sei A stets ein Ring.

9.1 **Bemerkung und Definition** (Komplex, Differential, Kohomologie)

Seien $C_\bullet = \left(\ldots \to C_n \overset{f_n}{\to} C_{n-1} \to \ldots\right)$ eine exakte Folge von A-Moduln und M ein A-Modul. Dann ist die Folge

$$D_\bullet := C_\bullet \otimes_A M := \left(\ldots \to D_n := C_n \otimes_A M \overset{f_n \otimes \mathrm{id}_M =: \partial_n}{\to} D_{n-1} := C_{n-1} \to \ldots\right)$$

ist im Allgemeinen nicht mehr exakt, genauer:

$$M \text{ flach} \quad \Leftrightarrow \quad C_\bullet \otimes_A M \text{ ist exakt für alle } C_\bullet$$

Aber es gilt immer noch für alle $n \in \mathbb{Z}$:

$$\partial_{n-1} \circ \partial_n = \underbrace{(f_{n-1} \circ f_n)}_{=0} \otimes \mathrm{id}_M = 0$$

Das heißt:

$$\mathrm{im}\,(\partial_n) \subseteq \ker(\partial_{n-1})$$

Ferner ist $D_\bullet$ an der Stelle D_{n-1} genau dann exakt, wenn dies eine Gleichheit ist.
Ein *Komplex (von A-Moduln)* ist eine Folge von A-Moduln $(D_n, \partial_n : D_n \to D_{n-1})_{n\in\mathbb{Z}}$ so, dass für alle $n \in \mathbb{Z}$ gilt

$$\mathrm{im}\,(\partial_n) \subseteq \ker(\partial_{n-1})$$

oder äquivalent $\partial_{n-1} \circ \partial_n = 0$ für alle $n \in \mathbb{Z}$. Die Abbildungen ∂_n heißen *Differentiale von $D_\bullet$*.
Für alle $n \in \mathbb{Z}$ heißen

$$D_n \supseteq Z_n(D_\bullet) := \ker(\partial_n)$$

die n-Zykel (von $D_\bullet$),

$$D_n \supseteq B_n(D_\bullet) = B_n := im\,(\partial_{n+1})$$

die n-Ränder (von $D_\bullet$) und

$$H_n(D_\bullet) = H_n := {}^{Z_n}\!/_{B_n}$$

die n-te Homologie (von $D_\bullet$).
Genau dann ist $D_\bullet$ exakt, wenn $H_n(D_\bullet) = 0$ für alle $n \in \mathbb{Z}$ gilt.

9.2 Definition und Bemerkung (freie Auflösung)

Sei M ein A-Modul. *Eine freie Auflösung von M* ist eine exakte Folge von A-Moduln

$$\Big(\ldots \to F_1 \xrightarrow{f_1} F_0 \to M \to 0\Big) =: (F_\bullet \to M \to 0)$$

in der alle F_i frei sind. Jeder Modul besitzt (viele verschiedene) freie Auflösungen.
Für einen weiteren A-Modul N definiere für alle $n \in \mathbb{N}$ die *höheren Torsionsmodule*:

$$\operatorname{Tor}_n^A(M,N) := H_n(F_\bullet \otimes_A N)$$

Es ist *nicht* klar, ob das wohldefiniert, das heißt unabhängig von der Wahl von $F_\bullet$ ist.

9.3 Beispiel

Es gelten die Voraussetzungen von 9.2.

i) Ist N flach, so ist $F_\bullet \otimes_A N$ an allen Stellen $n \in \mathbb{N}_{>0}$ exakt, also gilt $\operatorname{Tor}_n^A(M,N) = 0$.

ii) Berechne $\operatorname{Tor}_0^A(M,N)$: Sei

$$F_1 \to F_0 \to M \to 0$$

eine exakt Folge und F_1,F_0 frei. Wegen der Rechtsexaktheit des Tensorprodukts 2.34 ist

$$F_1 \otimes_A N \xrightarrow{\partial_1} F_0 \otimes_A N \to M \otimes_A N \to 0$$

exakt. Es folgt:

$$\operatorname{Tor}_0^A(M,N) = H_0(F_0 \otimes_A N) = \ker(\partial_0)/\operatorname{im}(\partial_1) \cong M \otimes_A N$$

Insbesondere ist $\operatorname{Tor}_0^A(M,N)$ unabhängig von der Wahl von $F_\bullet$.

Anhang

Danksagungen

Mein besonderer Dank geht an Professor Naumann, der diese Vorlesung hielt und es mir gestattete, diese Vorlesungsmitschrift zu veröffentlichen.

Außerdem möchte ich mich ganz herzlich bei allen bedanken, die durch aufmerksames Lesen Fehler gefunden und mir diese mitgeteilt haben.

Andreas Völklein

GNU Free Documentation License

0. Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. Applicability and definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "**publisher**" means any person or entity that distributes copies of the Document to the public.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that

these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. Verbatim copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. Copying in quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution

and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. Combining documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. Collections of documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. Aggregation with independent works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. Future revisions of this license

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `https://www.gnu.org/copyleft/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. Relicensing

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

Addendum: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation;
>
> with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

> A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.