Algebra II

Prof. G. Wiese

Institut für experimentelle Mathematik
Universität Duisburg-Essen
gabor.wiese@uni-due.de

SS 09

Stand: 15. April 2010

Inhaltsverzeichnis

Kapitel I

Moduln über Ringen (I)

Sofern nicht anders angegeben bezeichne in diesem Kapitel R einen, nicht notwendig kommutativen, Ring und $\mathbb{K}$ einen Körper.

1 Grundbegriffe

Definition 1.1 *(R-Linksmodul)*
Eine abelsche Gruppe M zusammen mit einer Abbildung:

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto r \cdot m \end{aligned}$$

heißt R-Linksmodul, falls für alle $r, s \in R$ und für alle $x, y \in M$ gelten:
(i) $r(x+y) = rx + ry$
(ii) $(r+s)x = rx + sx$
(iii) $(rs)x = r(sx)$ *und*
(iv) $1_R \cdot x = x$
Analog definieren wir R-Rechtsmoduln und R-Doppelmoduln.
Konvention: Für R-Linksmodul schreiben wir im Folgenden: R-Modul.

Beispiel 1 *(R-Moduln)*

- *Sei R ein Körper, dann sind die R-Moduln die R-Vektorräume.*
- *Sei R ein Ring, dann ist R ein R-Links-/Rechts-/Doppelmodul durch: $R \times R \to R$, $(r, s) \mapsto rs$*
- *Sei $\mathfrak{a} \trianglelefteq R$ ein Linksideal von R, dann ist $\mathfrak{a}$ ein R-Linksmodul. Umgekehrt ist jeder R-Linksmodul $\mathfrak{a} \subset R$ ein Linksideal von R.*

Definition 1.2 *(Untermodul, einfacher Modul, einfacher Ring)*

(1) Sei M ein R Modul. Eine Teilmenge $N \subseteq M$ ist ein Untermodul von M, falls N ein R Modul bzgl. der eingeschränkten Abbildung ist.
Notation: $N \leq M$.
(2) Ein Modul M heißt einfacher R-Modul, falls die einzigen

Untermoduln von M der Nullmodul $\underline{0}$ und M sind.

(3) R heißt einfacher Ring, falls R als R-Doppelmodul einfach ist.
($\Leftrightarrow \underline{0}, R$ sind die einzigen beidseitigen Ideale.)

Definition und Bemerkung 1.3 *(Faktor-, Quotientenmodul)*
Sei $N \leq M$. Die Relation $x \sim y \Leftrightarrow x - y \in N$ ist eine Äquivalenzrelation. Die Äquivalenzklassen ($\overline{x} = x + N$) bilden den R-Modul ${}^{M}\!/_{N}$:

$$\begin{array}{rcl} R \times {}^{M}\!/_{N} & \to & {}^{M}\!/_{N} \\ (r, \overline{x}) & \mapsto & \overline{rx} \end{array}$$

${}^{M}\!/_{N}$ heißt Faktor- bzw. Quotientenmodul oder einfach Quotient von M nach N.

Beispiel 2 *Sei $\mathfrak{a} \trianglelefteq R$. Der Faktormodul ${}^{R}\!/_{\mathfrak{a}}$ ist gleich mit dem Faktorring ${}^{R}\!/_{\mathfrak{a}}$*[1]*.*

Definition 1.4 *(R-Homomorphismen)*
Seien M und N R-Moduln. Eine Abbildung $\phi : M \to N$ heißt R-Homomorphismus, falls für alle $x, y \in M$ und für alle $r \in R$ gilt:

$$\phi(rx + y) = r \cdot \phi(x) + \phi(y)$$

Ähnlich wie im letzten Semester verwenden wir die Notation: $Hom_R(M, N)$ für die Menge der R-Homomorphismen von M nach N.
Weiter definieren wir: $End_R(M) := Hom_R(M, M)$.

Bemerkung 1.5 *Seien M und N zwei R-Moduln. Es gelten*

(a) $(\mathrm{Hom}_R(M, N), +)$ ist abelsche Gruppe durch
$\forall \varphi, \psi \in \mathrm{Hom}_R(M, N) \, \forall x \in M : \quad (\varphi + \psi)(x) := \varphi(x) + \psi(x)$

(b) Ist R kommutativ, so ist $\mathrm{Hom}_R(M, N)$ ein R-Modul durch:
$\forall \varphi \in \mathrm{Hom}_R(M, N) \, \forall r \in R \, \forall x \in M : \quad (r\varphi)(x) := r \cdot \varphi(x)$

Anmerkung zu 1.5 b
Die gegebene Abbildung muss wieder ein Homomorphismus sein, sei also $s \in R$. Es gilt: $r \cdot \varphi)(sx) = r\varphi(sx) = rs\varphi(x)$
Da R nach Voraussetzung kommutativ ist gilt: $rs = sr$, somit: $rs\varphi(x) = s(r\varphi)(x)$

Beispiel 3 *($\mathbb{K}$-Vektorraum V als $\mathbb{K}[X]$-Modul)*
Seien V ein $\mathbb{K}$-Vektorraum mit $dim_{\mathbb{K}}(V) = n \in \mathbb{N}$ und $\phi \in End_{\mathbb{K}}(V)$,
dann ist V ein $\mathbb{K}[X]$-Modul, via

$$\begin{array}{rcl} \mathbb{K}[X] \times V & \to & V \\ \left(\sum_{i=0}^{n} a_i X^i, v \right) & \mapsto & \sum_{i=0}^{n} a_i \phi^i(v) \end{array}$$

mit ϕ^i ist die i-fache Hinternanderausführung von ϕ.

[1] Vgl. L2: Definition 4.6, S.14

Satz 1.6 *(Homomorphiesatz)*
Seien M und N zwei R-Moduln und $\varphi \in \mathrm{Hom}_R(M,N)$. Es gelten:
(a) $\mathrm{Ker}(\varphi) \leq M$ *und* $\mathrm{Im}(\varphi) \leq N$
(b) φ induziert einen Ring-Isomorphismus:

$$\begin{aligned} \tilde{\varphi} : {}^{M}\!/_{\mathrm{Ker}(\varphi)} &\to \mathrm{Im}(\varphi) \\ m + \mathrm{Ker}(\varphi) &\mapsto \varphi(m) \end{aligned}$$

Beweis. Wir kennen (a) und (b) für abelsche Gruppen aus Algebra I[2], daher genügt es die Skalarmultiplikation zu zeigen.
zu a) $x \in \mathrm{Ker}(\varphi) \Rightarrow \varphi(rx) = r\varphi(x) = r \cdot 0 = 0 \Rightarrow rx \in \mathrm{Ker}(\varphi) \Rightarrow \mathrm{Ker}(\varphi) \leq M$
Analog folgt $\mathrm{Im}(\varphi) \leq N$.
zu b) Es ist zu zeigen: $\tilde{\varphi} \in \mathrm{Hom}_R({}^{M}\!/_{\mathrm{Ker}(\varphi)}, \mathrm{Im}(\varphi))$ Betrachte

$$\tilde{\varphi}(r \cdot (m + \mathrm{Ker}(\varphi)) = \tilde{\varphi}(rm) = r \cdot \tilde{\varphi}(m) = r\tilde{\varphi}(M + \mathrm{Ker}(\varphi))$$

□

Satz 1.7 *(Isomorphisatz)*
Sei M ein R-Modul und $N_1, N_2 \leq M$ Untermoduln, dann gelten:
(a) Falls $N_1 \leq N_2$: ${}^{M}\!/_{N_1}\!/_{N_2/N_1} \xrightarrow{\sim} {}^{M}\!/_{N_2}$
(b) ${}^{(N_1+N_2)}\!/_{N_2} \xrightarrow{\sim} {}^{N_1}\!/_{N_1 \cap N_2}$

Beweis. Übungsblatt 1, Aufgabe 4

Definition 1.8 *(Komplex, exakte Sequenz)*
Seien M_i für $i \in \mathbb{N}$ gegebene R-Moduln mit $\varphi_i \in \mathrm{Hom}_R(M_i, M_{i+1})$. Eine Folge / Sequenz

$$\ldots \to M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \to \ldots$$

heißt:
- ein Komplex, falls $\mathrm{Im}(\varphi_{i-1}) \subseteq \mathrm{Ker}(\varphi_i)$
- eine exakte Sequenz oder exakt, falls $\mathrm{Im}(\varphi_{i-1}) = \mathrm{Ker}(\varphi_i)$

Bemerkung 1.9 *Seien M, N zwei R-Moduln und $\varphi \in \mathrm{Hom}_R(M,N)$, weiter bezeichne o die Nullabbildung.*
(a) φ ist genau dann injektiv, wenn
$0 \xrightarrow{o} M \xrightarrow{\varphi} N$ *eine exakte Sequenz ist.*
(b) φ ist genau dann surjektiv, wenn
$M \xrightarrow{\varphi} N \xrightarrow{o} 0$ *eine exakte Sequenz ist.*
(c) Eine Sequenz von R-Moduln $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ *ist genau dann exakt, wenn gilt:*
(i) φ ist injektiv und (ii) ψ ist surjektiv und (iii) $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$.

Beweis. zu a) $0 \to M \to N$ ist exakt $\Leftrightarrow \mathrm{Ker}(\varphi) = \mathrm{Im}(o) = 0 \Leftrightarrow \varphi$ ist injektiv.
b) folgt analog. Aus (a) und (b) folgt (c). □

[2] Vgl. L2: Satz 4.8 S.15

Satz 1.10 *(Links-exakte Funktoren)*
Seien M, N, N_i sowie M_i R-Moduln. Weiter seien $\varphi, \bar{\varphi}, \rho, \bar{\rho}$ R-Homomorphismen. Es gelten:
a) Ist $0 \to N_1 \xrightarrow{\varphi} N_2 \xrightarrow{\rho} N_3$ *exakt, dann ist auch*

$$0 \to \mathrm{Hom}_R(M, N_1) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(M, N_2) \xrightarrow{\bar{\rho}} \mathrm{Hom}_R(M, N_3)$$

exakt, mit

$$\begin{aligned} \bar{\varphi} : \mathrm{Hom}_R(M, N_1) &\to \mathrm{Hom}_R(M, N_2) \\ \alpha &\mapsto \varphi \circ \alpha \end{aligned}$$

Analog definieren wir $\bar{\rho}$.
Sprechweise: $\mathrm{Hom}_R(M, \cdot)$ *ist ein links-exakter kovarianter Funktor.*
b)Ist $M_3 \xrightarrow{\varphi} M_2 \xrightarrow{\rho} M_1 \to 0$ *exakt, dann ist auch*

$$0 \to \mathrm{Hom}_R(M_1, N) \xrightarrow{\bar{\rho}} \mathrm{Hom}_R(M_2, N) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(M_3, N)$$

exakt, mit

$$\begin{aligned} \bar{\varphi} : \mathrm{Hom}_R(M_2, N) &\to \mathrm{Hom}_R(M_3, N) \\ \alpha &\mapsto \alpha \circ \varphi \end{aligned}$$

Analog definieren wir $\bar{\rho}$.
Sprechweise: $\mathrm{Hom}_R(\cdot, N)$ *ist ein links-exakter kontravarianter Funktor.*

Beweis. zu a)
Es ist zu zeigen, dass $\bar{\varphi}$ injektiv und $\mathrm{Ker}(\bar{\rho}) = \mathrm{Im}(\bar{\varphi})$ ist.
Sei $\alpha \in \mathrm{Hom}_R(M, N_1)$ mit $\alpha \in \mathrm{Ker}(\bar{\varphi})$.
$\Rightarrow 0 = \bar{\varphi}(\alpha) = \varphi(\alpha)$
Nach (1.9 a) ist φ injektiv, also gilt $\alpha = 0$ und somit ist $\bar{\varphi}$ injektiv.
Sei nun $\alpha \in \mathrm{Hom}_R(M, N_1)$. Da $0 \to N_1 \xrightarrow{\varphi} N_2 \xrightarrow{\rho} N_3$ exakt ist, gilt: $\rho \circ \varphi = 0$. Betrachte:

$$\bar{\rho} \circ \bar{\varphi}(\alpha) = \bar{\rho}(\varphi \circ \alpha) = \rho \circ \varphi \circ \alpha = 0 \circ \alpha = 0$$

Es ist also $\mathrm{Im}(\bar{\varphi})$ in $\mathrm{Ker}(\bar{\rho})$ enthalten. Sei nun $\beta \in \mathrm{Ker}(\bar{\rho})$ also $\beta \in \mathrm{Hom}_R(M, N_2)$ und $\rho \circ \beta = 0$.
Betrachte:

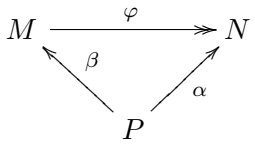
$$\bar{\rho}(\beta)(m) = \rho \circ \beta(m) = 0 \ \forall m \in M$$

Nach Voraussetzung gilt: $\mathrm{Ker}(\rho) = \mathrm{Im}(\varphi)$ also: $\mathrm{Im}(\beta) \subseteq \mathrm{Im}(\varphi)$.
Da φ injektiv ist, gilt insbesondere $\varphi : N_1 \xrightarrow{\sim} Im(\varphi)$.
Betrachte also nun $\varphi^{-1} : \mathrm{Im}(\varphi) \to N_1$ und definiere $\alpha := \varphi^{-1} \circ \beta$.
Es ist klar, dass α ein R-Homomorphismus ist, und somit ist

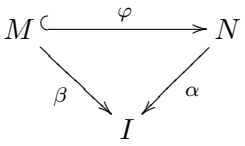
$$\bar{\varphi}(\alpha) = \varphi \circ \alpha = \varphi \circ \varphi^{-1} \circ \beta = \beta$$

Somit ist $\beta \in \mathrm{Im}(\bar{\varphi})$ womit folgt, dass $\mathrm{Ker}(\bar{\rho})$ in $\mathrm{Im}(\bar{\varphi})$ enthalten ist. Es folgt, was zu zeigen war $\mathrm{Ker}(\bar{\rho}) = \mathrm{Im}(\bar{\varphi})$. Der Beweis von (b) wird eine Übungsaufgabe auf einem der kommenden Arbeitsblätter. □

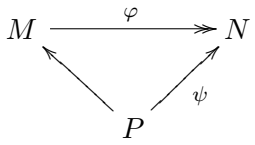
Definition 1.11 *(Projektive und injektive Moduln)*
Seien M, N, I und P R-Moduln. Ein Modul P heißt projektiv, falls die folgende universelle Abbildungseigenschaft (UAE) gilt:
Für alle R-Moduln M, N und für alle surjektiven R-Homomorphismen $\varphi \in \mathrm{Hom}_R(M, N)$ sowie für alle $\alpha \in \mathrm{Hom}_R(P, N)$ gibt es einen Homomorphismus $\beta \in \mathrm{Hom}_R(P, M)$, so dass gilt: $\varphi \circ \beta = \alpha$.



Ein Modul I heißt injektiv, falls die folgende universelle Abbildungseigenschaft (UAE) gilt:
Für alle R-Moduln M, N und für alle injektiven R-Homomorphismen $\varphi \in \mathrm{Hom}_R(M, N)$ sowie für alle $\alpha \in \mathrm{Hom}_R(N, I)$: gibt es ein $\beta \in \mathrm{Hom}_R(M, I)$, so dass gilt: $\beta \circ \varphi = \alpha$.



Beispiel 4 *Sei $P := R \oplus \ldots \oplus R$ ein freier R-Modul , dann ist P ein projektiver Modul.*
Beweis. *Wir haben M, N sowie φ, ψ, so dass*



Wir definieren $e_1 := (1, 0, \ldots, 0)$, $e_2 := (0, 1, 0, \ldots, 0)$ usw.
Die Elemente e_i erzeugen P als R-Modul. Wir definieren weiter: $n_i := \psi(e_i)$ und wählen für jedes i die Urbilder m_i zu n_i unter φ, also: $\varphi(m_i) = n_i$. Definiere nun α dadurch, dass $\alpha(e_i) := m_i$, und verwende lineare Fortsetzung. Dann gilt: $\varphi \circ \alpha(e_i) = \psi(e_i) = n_i$ und somit $\varphi \circ \alpha = \psi$.

Bemerkung 1.12 *Seien A, B zwei R-Moduln und φ, α zwei R-Homomorphismen.*
(a) Sei p ein projektiver Modul, dann zerfällt jede exakte Sequenz von der Form:

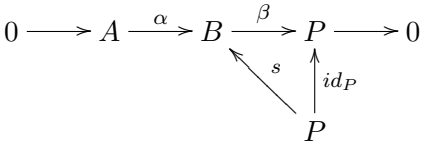
$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\varphi} P \to 0$$

d.h. es exisitert ein $s \in \mathrm{Hom}_R(P, B)$, so dass $\varphi \circ s = id_P$
(b) Sei I ein injektiver Modul, dann zerfällt jede exakte Sequenz von der Form:

$$0 \to I \xrightarrow{\varphi} A \xrightarrow{\alpha} B \to 0$$

d.h. es exisitert $s \in \mathrm{Hom}_R(A, I)$, so dass $s \circ \varphi = id_I$

Beweis. zu a:
Da die Sequenz exakt ist, ist φ surjektiv. Nach Definition 1.11 existiert ein s mit der geforderten Eigenschaft.



Der Beweis zu (b) erfolgt analog. □

Anmerkung Nach der ersten Aufgabe vom zweiten Übungsblatt gilt im Fall (a) $B \cong A \oplus P$ und im Fall (b) $A \cong I \oplus B$

Satz 1.13 *Seien N_1, N_2, N_3, P sowie I R-Moduln und α, β seien R-Homomorphismen.*
(a)P ist genau dann projektiv, wenn für alle kurzen exakten Sequenzen

$$0 \to N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3 \to 0$$

auch die Sequenz

$$0 \to \mathrm{Hom}_R(P, N_1) \xrightarrow{\bar{\alpha}} \mathrm{Hom}_R(P, N_2) \xrightarrow{\bar{\beta}} \mathrm{Hom}_R(P, N_3) \to 0$$

exakt ist.
(b)I ist genau dann injektiv, wenn für alle kurzen exakten Sequenzen

$$0 \to N_3 \xrightarrow{\beta} N_2 \xrightarrow{\alpha} N_1 \to 0$$

auch die Sequenz

$$0 \to \mathrm{Hom}_R(N_1, I) \to \mathrm{Hom}_R(N_2, I) \to \mathrm{Hom}_R(N_3, I) \to 0$$

exakt ist.

Beweis. zu a)
Nach Satz 1.10 genügt es zu zeigen, dass P projektiv, bzw. $\bar{\beta}$ surjektiv ist.Wir beginnen mit der Voraussetzung, das P projektiver R-Modul ist und wollen zeigen, dass $\bar{\beta}$ surjektiv ist. Sei dann $\varphi \in \mathrm{Hom}_R(P, N_3)$, dann gibt es $\psi \in \mathrm{Hom}_R(P, N_2)$ mit $\beta \circ \psi = \varphi$. In Satz 1.10 definierten wir $\bar{\beta}(\psi) := \beta \circ \psi$. Es folgt unmittelbar die surjektivität von $\bar{\beta}$. Nun nehmen wir $\bar{\beta}$ für alle exakten Sequenzen

$$0 \to N_1 \to N_2 \to N_3 \to 0$$

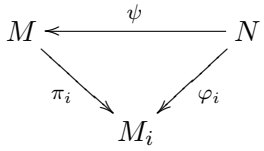
als surjektiv an, und wollen zeigen, dass P ein projektiver R-Modul ist. Wir haben $\beta : N_1 \twoheadrightarrow N_2$ und $\varphi : P \twoheadrightarrow N_2$ gegeben. Da $\bar{\beta}$ surjektiv ist, gibt es $\psi \in \mathrm{Hom}_R(P, N_2)$ so dass $\bar{\beta}(\psi) = \varphi \Rightarrow P$ projektiv ist. Der Beweis zu (b) verläuft analog. □

Anmerkung Sprechweise für (a): $\mathrm{Hom}_R(P, \cdot)$ ist ein exakter Funktor, falls P projektiv ist.

2 Direkte Summen und Produkte

Wir führen direkte Summen und Produkte mittels Universeller Abbildungseigenschaften ein, da die UAE auch in anderen Zusammenhängen dieselben sind, die Konstruktionen der direkten Summen und Produkte aber unterschiedlich sind.

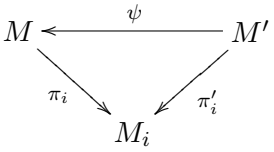
Definition 2.1 *(Das direkte Produkt)*
Seien M_i für $i \in I$ R-Moduln. Ein R-Modul M zusammen mit projektionen $\pi_i \in \mathrm{Hom}_R(M, M_i)$ heißt das direkte Produkt der M_i, falls die folgende universelle Abbildungseigenschaft gilt: Für alle $i \in I$ und für alle R-Moduln N sowie für alle $\varphi_i \in \mathrm{Hom}_R(N, M_i)$ existiert genau ein $\psi \in \mathrm{Hom}_R(N, M)$, derart dass $\pi_i \circ \psi = \varphi_i$ für alle $i \in I$ gilt.



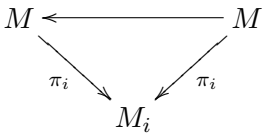
(Notation: $\prod_{i \in I} M_i$)

Satz 2.2 *Das direkte Produkt $\prod M_i$ existiert und ist bis auf (eindeutige) Isomorphie eindeutig.*

Beweis. Es sind zwei Dinge zu zeigen, nämlich die Eindeutigkeit und die Existenz. Wir beginnen mit der Eindeutigkeit. Seien also (M, π_i) und (M', π_i') direkte Produkte.



Die universelle Abbildungseigenschaft von M gibt uns die eindeutige Existenz von $\psi \in \mathrm{Hom}_R(M', M)$ mit $\pi_i \circ \psi = \pi_i'$. Analog liefert uns die universelle Abbildungseigenschaft von M' die eindeutige Existenz von $\psi' \in \mathrm{Hom}_R(M, M')$ mit $\pi_i' \circ \psi' = \pi_i$.
Es folgen daher die Identitäten $\pi_i \circ \psi \circ \psi' = \pi_i' \circ \psi' = \pi_i$



Das obige Diagramm kommutiert für id_M und $\psi \circ \psi'$. Nach der universellen Abbildungseigenschaft von M ist $\psi \circ \psi' = id_M$. Also ist ψ' injektiv und ψ surjektiv. Analog gilt nach der universellen Abbildungseigenschaft von M' $\psi' \circ \psi = id_{M'}$. Daher müssen ψ und ψ' Isomorphismen sein und somit gilt:

$$M \cong M'$$

Nach der universellen Abbildungseigenschaft ist der Isomorphismus zwischen M und M' eindeutig bestimmt. Die Existenz beweisen wir Konstruktiv und definieren

$$M := \prod_{i \in I} M_i = \{\, (x_i)_{i \in I} \mid x_i \in M_i \,\}$$

und

$$\begin{array}{rcl} \pi_j : M & \to & M_j \\ (x_i)_{i \in I} & \mapsto & x_j \end{array}$$

Die universelle Abbildungseigenschaft ist erfüllt, denn mit gegebenem R-Modul N und $\varphi_i \in \mathrm{Hom}_R(N, M_i)$ konstuiere ψ wie folgt: Sei $n \in N$, dann definiere $\psi(n) := \varphi_i(n))_{i\in I}$. Es gilt:

$$\pi_j \circ \psi(n) = \pi_j[\,(\varphi_i(n))_{i\in I}\,] = \varphi_j(n) \qquad \forall j \in I$$

Es folgt, dass $\pi_j \circ \psi = \varphi_j$ ist. Die konstruierte Abbildung ist eindeutig, denn erfülle $\psi' \in \mathrm{Hom}_R(N, M)$ die universelle Abbildungseigenschaft (Also: $\pi_j \circ \psi' = \varphi_j$), dann ist für alle $j \in I$ die j-te Komponente von $\psi' = \varphi_j$ also gilt bereits $\psi' = \psi$. □

Satz 2.3 *(Kriterium für direkte Summen)*
Hier sei R ein - nicht notwendig kommutativer - Ring. Weiter seien M und $M_i \subseteq M$ für $i \in I$ R-Moduln, mit:

$$M = \sum_{i\in I} M_i$$

Genau dann ist M direkte Summe der M_i, wenn für alle $j \in I$ der Schnitt von M_j mit der Summe über die restlichen M_i leer ist, also

$$M \cong \bigoplus_{i\in I} M_i \Leftrightarrow \forall\, j \in I\, : M_j \cap \sum_{\substack{i\in I\\ i\neq j}} M_i = \{0\}$$

Zur Verdeutlichung betrachte folgenden Spezialfall:

$$M = A + B \Rightarrow M \cong A \oplus B \Leftrightarrow A \cap B = \{0\}$$

Beweis. Betrachte

$$\begin{aligned} \varphi :\ \bigoplus_{i\in I} M_i &\ \to\ \sum_{i\in I} M_i = M \\ (m_i)_{i\in I} &\ \mapsto\ \sum_{i\in I} m_i \end{aligned}$$

φ ist trivialer weise surjektiv. Da $\sum m_i$ endlich ist, ist φ auch wohldefiniert. Es gilt:

$$\begin{aligned} \varphi \text{ ist Isomorphismus} &\ \Leftrightarrow\ \mathrm{Ker}(\varphi) = \{0\} \\ &\ \Leftrightarrow\ \left(\text{für } m_i \in M_i : \sum_{i\in I} m_i = 0 \Rightarrow m_i = 0 \quad \forall\, i \in I\right) \\ &\ \Leftrightarrow\ \forall\, j \in I : M_j \cap \sum_{\substack{i\in I\\ i\neq j}} M_i = \{0\} \end{aligned}$$

„⇒“: Sei $x \in M_j \cap \sum_{i\neq j} M_i$, dann können wir x darstellen als

$$x = \sum_{i\neq j} m_i$$

Es gilt

$$0 = -x + \sum_{i\neq j} m_i$$

Also muss $x = 0$ sein.
„$\Leftarrow$“: Es gilt: $\sum_{i \in I} m_i = 0$. Ohne Beschränkung der Allgemeinheit gelte nach Umsortieren: $\sum_{i=1}^{n} m_i = 0$
Damit haben wir eine Darstellung von m_1 als

$$m_1 = -\sum_{i=2}^{n} m_i \in M_1 \cap \sum_{i=2}^{n} M_i$$

Damit ist $m_1 = 0$. Setze nun dieses Verfahren induktiv fort, dann folgt für alle $i = 1, ..., n$, die Identität $m_i = 0$ □

Bemerkung 2.4 *Sei M ein R-Modul und seien $\varphi_1, \ldots, \varphi_n \in \mathrm{End}_R(M)$, die eine Zerlegung der Eins (id_M) bilden, gegeben. Das heißt:*

$$\sum_{i=1}^{n} \varphi_i = id_M \quad \text{und } \varphi_i \circ \varphi_j = 0 \quad \forall i \neq j$$

Dann gelten:
(a) $\varphi_i \circ \varphi_i = \varphi_i$
(b) Die Abbildung

$$\begin{aligned} \phi : M &\to \prod_{i=1}^{n} M_i \\ x &\mapsto (\varphi_i(x))_{i=1\ldots n} \end{aligned}$$

mit $M_i = \varphi_i(M)$ ist R-Isomorphismus.

Beweis. zu (a) betrachte:

$$\varphi_i = \varphi_i \circ id_M = \varphi_i \circ \left(\sum_{j=1}^{n} \varphi_j \right) = \sum_{j=1}^{n} \varphi_i \circ \varphi_j = \varphi_i \circ \varphi_i$$

zu (b): ϕ ist injektiv, denn für alle $i = 1, \ldots, n$ gilt

$$\phi(x) = 0 = (\varphi_i(x))_{i=1\ldots n} \Rightarrow \varphi_i(x) = 0$$

Betrachte:

$$x = id_M(x) = \sum_{j=1}^{n} \varphi_j(x) = 0$$

Also ist $x = 0$. Weiter ist ϕ surjektiv, denn seien $x_i := \varphi_i(y_i) \in M_i$ vorgegeben, dann setze $x := \sum_{i=1}^{n} x_i$ und Betrachte:

$$\begin{aligned} \phi(x) = (\varphi_i(x))_{i=1\ldots n} &= (\varphi_i \left(\sum_{j=1}^{n} \varphi_j(y_j) \right))_{i=1\ldots n} \\ &= \left(\sum_{j=1}^{n} \varphi_i \circ \varphi_j(y_j) \right)_{i=1\ldots n} \\ &= (\varphi_i(y_i))_{i=1\ldots n} \\ &= (x_i)_{i=1\ldots n} \end{aligned}$$

□

Satz 2.5 *Seien für $i \in I$ R-Moduln N_i sowie ein R-Modul M gegeben und $\pi_i : \prod N_i \to N_i$ die Projektionen nach Definition 2.1, dann gilt:*

$$\begin{array}{rcl} \Psi : \mathrm{Hom}_R(M, \prod_{i\in I} N_i) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Hom}_R(M, N_i) \\ \varphi & \mapsto & (\pi_i \circ \varphi)_{i\in I} \end{array}$$

als abelsche Gruppen (bzw. als R-Moduln, falls R kommutativ ist).

Beweis. Die Homomorphieeigenschaft ist klar, da φ und alle π_i Homomorphismen sind.

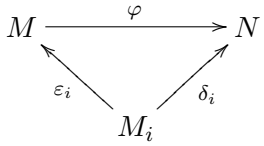
$$\begin{array}{c} M \xrightarrow{\bar\varphi} \prod N_i \\ \pi_i \circ \varphi \searrow \quad \swarrow \pi_i \\ N_i \end{array}$$

Zur Injektivität:
$\Psi(\varphi) = 0 \Rightarrow \pi_i \circ \varphi = 0 \quad \forall\, i \in I$
Nach der universellen Abbildungseigenschaft gibt es eindeutig bestimmtes $\bar\varphi$ mit $\pi_i \circ \bar\varphi = \underline{0}$. Es gilt $\bar\varphi = \underline{0} \wedge \bar\varphi = \varphi \Rightarrow \varphi = \underline{0}$

$$\begin{array}{c} M \xrightarrow{\bar\varphi} \prod N_i \\ \varphi_i \searrow \quad \swarrow \pi_i \\ N_i \end{array}$$

Zur Surjektivität:
Gegeben seien $(\varphi_i)_{i\in I}$ mit $\varphi_i \in \mathrm{Hom}_R(M, N_i)$. Nach der universellen Abbildungseigenschaft gibt es genau ein $\bar\varphi \in \mathrm{Hom}_R(M, \bigotimes N_i)$ mit $(\pi_i \circ \bar\varphi)_{i\in I} = \Psi(\bar\varphi) = (\varphi_i)_{i\in I}$ □

Definition 2.6 *(Die direkte Summe, Koprodukt)*
Für $i \in I$ seien M_i gegebene R-Moduln. Ein R-Modul M zusammen mit Inklusionen $\varepsilon_i \in \mathrm{Hom}_R(M_i, M)$ heißt direkte Summe oder auch Koprodukt der M_i, falls die folgende universelle Abbildungseigenschaft erfüllt ist:



Für alle R-Moduln N und für alle $\delta_i \in \mathrm{Hom}_R(M_i, N)$ existiert genau ein $\varphi \in \mathrm{Hom}_R(M, N)$, so dass $\varphi \circ \varepsilon_i = \delta_i$ ist.
Notation: $M = \bigoplus_{i\in I} M_i$

Satz 2.7 *Die direkte Summe aus Definition 2.6 existiert und ist bis auf eindeutige Isomorphie eindeutig.*

Beweis. Zum Nachweis der Eindeutigkeit betrachte den Beweis zu Satz 2.2 mit „umgedrehten Pfeilen“. Die Existenz beweisen wir wieder konstruktiv. Setze

$$M := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} M_i \,|\, \text{fast alle } 0 = x_i \in (x_i)_{i\in I} \right\}$$

und die natürlichen Inklusionen:

$$\begin{array}{rcl} \varepsilon_j : M_j & \to & M \\ x_j & \mapsto & (x_j)_{i\in I} \text{ mit } x_i = 0 \text{ für } i \neq j \end{array}$$

Seien ein R-Modul N und $\delta_i \in \mathrm{Hom}_R(N, M_i)$ gegeben.
Wir suchen ein $\varphi \in \mathrm{Hom}_R(M, N)$ werlches für alle $i \in I$ die Identität $\varphi \circ \varepsilon_i = \delta_i$ erfüllt, d.h.

$$\forall j \in I: \quad (\varphi \circ \varepsilon_j(x_j)) = \varphi((x_j)_{i\in I}) = \delta_j(x_j) \qquad (1)$$

Definiere also für $m \in M$ mit $m = (m_i)_{i\in I}$ Die Abbildung φ wie folgt:

$$\varphi(m) = \varphi((m_i)_{i\in I} := \sum_{i\in I} \delta_i(m_i)$$

dann erfüllt φ Gleichung (1) und φ ist eindeutig, da die Elemente der Form $(x_j)_{i\in I}$ ein Erzeugendensystem von M bilden. Der Wert von φ auf diesen Elementen ist durch (1) vorgeschrieben. □

Folgerung 2.8 *Seien $M_1, \ldots, M_n$ R-Moduln, dann gilt:*

$$\bigoplus_{i=1}^{n} M_i \cong \prod_{i=1}^{n} M_i$$

und $\varepsilon_i \circ \pi_i$ bilden eine Zerlegung der Eins (id_{M_i}).

Satz 2.9 *Seien für $i \in I$ M_i und N R-Moduln und $\varepsilon_i : \bigoplus M_i \to M_i$ die Inklusionen nach Definition 2.6, dann gilt:*

$$\begin{array}{rccc} \Psi : \mathrm{Hom}_R(\bigoplus_{i\in I} M_i, N) & \tilde{\to} & \prod_{i\in I} \mathrm{Hom}_R(M_i, N) \\ \varphi & \mapsto & (\varphi \circ \varepsilon_i)_{i\in I} \end{array}$$

als abelsche Gruppen (bzw. als R-Moduln, falls R kommutativ ist).

Beweis. Sei: $\underline{0} = \Psi(\varphi) = (\varphi \circ \varepsilon_i)_{i\in I}$. Nach der universellen Abbildungseigenschaft gibt es genau ein $\bar{\varphi}$ mit

$$\bar{\varphi} \circ \varepsilon_i = \varphi \circ \varepsilon_i = \underline{0} \circ \varepsilon_i = \underline{0} \Rightarrow \varphi = \underline{0}$$

Seien $\varphi_i \in \mathrm{Hom}_R(M_i, N)$ gegeben, dann gibt es nach der universellen Abbildungseigenschaft $\bar{\varphi}$ mit

$$\Psi(\bar{\varphi}) = (\bar{\varphi} \circ \varepsilon_i)_{i\in I} = (\varphi_i)_{i\in I}$$

□

Definition 2.10 *(Freie Moduln, Erzeugendensystem und Basen)*
Sei M ein R-Modul mit $B \subseteq M$.
(a) B heißt Erzeugendensystem von M, falls

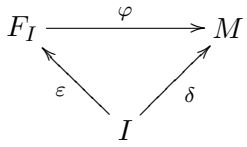
$$\forall\, m \in M\ \exists\, b_1, \ldots, b_n \in B\ \exists\, r_1, \ldots, r_n \in R : m = \sum_{i=1}^{n} r_i b_i$$

(b) B heißt frei, falls für $r_i \in R$ und $b_i \in B$ gilt:

$$\sum_{i=1}^{n} r_i b_i = 0 \Rightarrow r_i = 0 \quad \forall\, i = 1...n$$

(c) B heißt Basis von M, falls B ein freies Erzeugendensystem von M ist.
(d) M heißt freier Modul, falls M eine Basis hat.

Definition 2.11 *(Freier Modul über einer Menge)*
Sei I eine Menge. Ein R-Modul F_I zusammen mit $\varepsilon \in \mathrm{Abb}(I, F_I)$ heißt freier Modul über I, falls folgende universelle Abbildungseigenschaft gilt:



Für alle R-Moduln M und für alle $\delta \in \mathrm{Abb}(I, M)$ existiert genau ein $\varphi \in \mathrm{Hom}_R(F_I, M)$, so dass $\varphi \circ \varepsilon = \delta$erfüllt ist.

Satz 2.12 *Sei I eine Menge, dann existiert ein freier R-Modul F_I über I und dieser ist bis auf (eindeutige) Isomorphie eindeutig bestimmt.*

Beweis. Der Nachweis der Eindeutigkeit ist eine Übungsaufgabe auf dem 2. Blatt.
Zur Existenz definiere

$$F_I := \bigoplus_{i \in I} R \quad \text{und} \quad \varepsilon(i) := e_i$$

Seien ein R-Modul M mit $\delta \in \mathrm{Abb}(I, M)$ gegeben. Es gilt: F_I ist freier Modul, mit Basis $\mathfrak{B} = \{e_i \mid i \in I\}$ und weiter definiert $\varphi(e_i) := \delta(i)$ ein eindeutiges φ mit $\varphi \circ \varepsilon = \delta$. □

Bemerkung 2.13 *Es gelten:*
(a) $\{e_i \mid i \in I\} := \mathfrak{B}$ aus dem Beweis von Satz 2.12 ist eine Basis von F_I.
(b) Seien I, J Mengen mit $\sharp I = \sharp J$, dann gilt: $F_I \cong F_J$. □

Folgerung 2.14 *Jeder R-Modul M ist Quotientenmodul eines freien Moduls.*

Beweis.
$F_E \xrightarrow{\varphi} M$, $\varepsilon \nwarrow \nearrow \iota$, E — Sei $E \subseteq M$ ein Erzeugendensystem von M. Betrachte den freien Modul F_E über E. Nach der universellen Abbildungseigenschaft gibt es φ.Es gilt: $E \subseteq \mathrm{Im}(\varphi)$. Also ist φ surjektiv und wir können den Homomorphiesatz anwenden: $F_E / \mathrm{Ker}(\varphi) \cong M$ □

Definition und Satz 2.15 *(Länge einer Basis)*
(a) Sei M ein freier R-Modul mit Basis $\mathfrak{B}$, dann gilt: $M \cong F_{\mathfrak{B}}$.
(b) Sei R kommutativ und M ein endlich erzeugter freier R Modul mit den Basen $\mathfrak{B}$ und $\mathfrak{B}'$, dann gilt: $\sharp\mathfrak{B} = \sharp\mathfrak{B}'$. Wir nennen $\sharp\mathfrak{B}$ die Länge von $\mathfrak{B}$.

Satz 2.16 *Sei P ein R-Modul. Genau dann ist P projektiv, wenn P direkter Summand eines freien Moduls ist. D.h. es gibt einen R-Modul X, so dass $P \bigoplus X =: F$ mit einem freien Modul F ist.*

Beweis. Zur Vereinfachung beweisen wir zunächst die Behauptung, dass freie Moduln projektiv sind: Seien $F := \bigoplus_{i \in I} R$ und $0 \to A \to B \to C \to 0$ eine exakte Sequenz von R-Moduln. Wenn wir zeigen können, dass

$$0 \to \mathrm{Hom}_R(F, A) \to \mathrm{Hom}_R(F, B) \to \mathrm{Hom}_R(F, C) \to 0$$

exakt ist, dann ist nach Satz 1.13 P projektiv. Es gilt:

$$\mathrm{Hom}_R(\bigoplus_{i\in I}, A) \cong \prod_{iinI} \mathrm{Hom}_R(R, A)$$

analog gilt dies für B, C, betrachte also:

$$\begin{array}{ccccccccc}
0 \to & \mathrm{Hom}_R(F,A) & \to & \mathrm{Hom}_R(F,B) & \to & \mathrm{Hom}_R(F,C) & \to 0 \\
& \wr\shortparallel & & \wr\shortparallel & & \wr\shortparallel & \\
0 \to & \prod_{i\in I}\mathrm{Hom}_R(R,A) & \to & \prod_{i\in I}\mathrm{Hom}_R(R,B) & \to & \prod_{i\in I}\mathrm{Hom}_R(R,C) & \to 0 \\
& \wr\shortparallel & & \wr\shortparallel & & \wr\shortparallel & \\
0 \to & A & \to & B & \to & C & \to 0
\end{array}$$

Die Komponenten dieser Sequenz sind gerade wieder die vorgegebene Sequenz, diese ist aber exakt, also haben wir die Behauptung bewiesen.
„⇒“: P ist projektiv daher gibt es mit Folgerung 2.14 einen freien R-Modul F und hierzu ein surjektives $\pi \in \mathrm{Hom}_R(F, P)$ derart, dass die folgende Sequenz exakt ist

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ker}(\pi) & \longrightarrow & F & \xrightarrow{\pi} & P & \longrightarrow & 0 \\
& & & & & \nwarrow^{s} & \uparrow{\scriptstyle id_P} & & \\
& & & & & & P & &
\end{array}$$

Mit Bemerkung 1.12 gibt es ein $s \in \mathrm{Hom}_R(P, F)$ mit $\pi \circ s = id_P$. Die Aussage der ersten Aufgabe vom zweiten Blatt liefert dann:

$$F \cong s(P) \bigoplus \mathrm{Ker}(\pi) \cong P \bigoplus \mathrm{Ker}(\pi)$$

„⇐“: Nach Voraussetzung ist $F = P \bigoplus X$ ein freier R-Modul. Seien M, N zwei R-Moduln und α, β nach Definition gegeben. Betrachte:

$$\begin{array}{ccccc}
M \bigoplus X & & \xleftarrow{\quad\bar{\alpha}\quad} & & N \bigoplus X \\
& \nwarrow^{\bar{\varphi}} & & \nearrow_{\bar{\beta}} & \\
& & P \bigoplus X & &
\end{array}$$

Hierbei ist

$$\bar{\alpha} : M \bigoplus X \ni (m, x) \mapsto (\alpha(m), id_X(x)) \in N \bigoplus X$$

und $\bar{\beta}$ analog definiert. Nach der zuvor bewiesenen Behauptung ist $P \bigoplus X$ projektiv. Daher gibt es ein $\bar{\varphi} \in \mathrm{Hom}_R\left(P \bigoplus X, M \bigoplus X\right)$ mit $\bar{\alpha} \circ \bar{\varphi} = \bar{\beta}$. Definiere φ wie folgt:

$$\begin{array}{rcccccc}
\varphi : P & \xrightarrow{\iota} & P \bigoplus X & \xrightarrow{\bar{\varphi}} & M \bigoplus X & \xrightarrow{\pi} & M \\
p & \mapsto & (p, 0) & \mapsto & (\bar{\varphi}(p), 0) & \mapsto & \bar{\varphi}(p)
\end{array}$$

Hierbei ist ι die natürliche Inklusion. Betrachte:

$$\alpha \circ \varphi = \alpha \circ \pi \circ \bar{\varphi} = \pi \circ \bar{\alpha} \circ \bar{\varphi} = \beta$$

□

3 Moduln über Hauptidealringen

Ab diesem Kapitel (einschließlich) bezeichne R immer einen kommutativen Intigritätsring.

Definition und Bemerkung 3.1 *(Torsionselement, Torsionsmodul, Annulator)*
Sei M ein R-Modul und $x \in M$, dann heißt...
(a) x Torsionselement, falls es ein $r \in R\backslash\{0\}$ gibt, so dass $r \cdot x = 0_M$ gilt.
(b) $\mathrm{Ann}(x) := \{ r \in R | rx = 0\}$ der Annulator von $x \in M$.
(c) $M_{tor} := \{ x \in M \,|x$ ist Torsionselement $\}$ Torsionsmenge bzw. -modul von M
(d) M torsionsfrei, wenn $M_{tor} = \{0\}$
Es gilt: Der Annulator von $x \in M$ ist ein Ideal in R, und M_{tor} ist ein Untermodul von M.

Beispiel 5 *Sei $R = \mathbb{Z}$, dann ist $\mathrm{Ann}(x) = (n)$ mit $n \in \mathbb{N}$.*
Falls x Torsionselement ist, so ist $n \neq 0$ und n ist die Ordnung von x.

Bemerkung 3.2 *Sei M ein R-Modul, dann ist*

$$\bar{M} := {}^{M}\!/_{M_{tor}}$$

ein torsionsfreier Modul.

Beweis. Sei $\bar{x} \in \bar{M}$ ein Torsionselement, dann gibt es ein $r \in R\backslash\{0\}$ mit $r \cdot \bar{x} = 0$
Also ist $rx \in M_{tor}$ für $x \in M$ mit $\bar{x} = x + M_{tor}$ Damit gibt es aber ein $s \in R\backslash\{0\}$ derart, dass $s(rx) = 0$ gilt. Also ist $x \in M_{tor}$ und somit muss $\bar{x} = 0_{\bar{M}}$ sein. □

Definition und Satz 3.3 *(Rang eines freien Moduls)*
Sei R ein Hauptidealring (HIR) und M ein freier R-Modul. Wir definieren den Rang eines freien Moduls durch

$$\mathrm{rg}(M) := \sharp\mathfrak{B}_M \quad \text{mit } \mathfrak{B}_M \text{ ist Basis von } M$$

Ist M vom Rang $\mathrm{rg}(M) = m$ so ist jeder Untermodul N von M vom Rang $\mathrm{rg}(N) = n \leq m$.

Beweis. Wir führen den Beweis Induktiv über M, und betrachten zunächst den Spezialfall ($m = 0$):

$$M = \{0\} \Rightarrow N = \{0\} \Rightarrow m = n$$

Induktions Anfang ($m = 1$):
Es gilt: $M \cong R \Rightarrow N \trianglelefteq R$, also $N = (a)$, da R ein Hauptidealring ist.
Es folgt: $N = \{0\} \vee N \cong R$. Somit ist N ein freier Modul vom Rang $n = 0 \vee n = 1$
Induktions Schritt ($m - 1 \curvearrowright m$):
Ohne Beschränkung der Allgemeinheit sei M die m-Fache direkte Summe von R, also

$$M \cong \bigoplus_{i=1}^{m} R$$

Betrachte die folgende exakte Sequenz:

$$0 \to \bigoplus_{i=1}^{m-1} R \xrightarrow{\iota} \bigoplus_{i=1}^{m} R \xrightarrow{\pi_m} R \to 0$$

mit ι der natürlichen Inklusion und π_m der Projektion auf die m-te Komponente. Es gilt:

$$\mathrm{Ker}(\pi_m) \cap N = \bigoplus_{i=1}^{m-1} R \cap N$$

daher ist

$$0 \to Ker(\pi_m) \cap N \xrightarrow{\iota} N \xrightarrow{\pi_m} \pi_m(N) \to 0$$

auch eine kurze exakte Sequenz. Wir wissen $\mathrm{Ker}(\pi_m) \cap N$ ist freier Modul vom Rang $m-1$ und es gilt $\pi_m(N) \cong R$ oder $\pi_m(N) = \{0\}$. Ist letzteres der Fall, so ist der Satz bewiesen. Für den ersten Fall wissen wir, dass R projektiv ist, also ist $N \cong R \bigoplus Ker(\pi_m) \cap N$ und damit ist N ein freier R-Modul vom Rang $rg(N) \leq m$ □

Anmerkung Satz 3.3 gilt auch für nicht endlich erzeugte Moduln. Die Voraussetzung, dass R ein Hauptidealring ist haben wir nur in $m = 1$ verwendet. In allen Ringen, in denen der Induktionsanfang wahr ist folgt also die Behauptung.

Generalvorausetzung: Ab jetzt bezeichne R immer einen Hauptidealring (HIR).

Satz 3.4 *Sei M ein endlich erzeugter R-Modul. M ist genau dann frei, wenn M torsionsfrei ist.*

Beweis. Die Richtung „⇒“ ist trivial, da R ein Integritätsring ist. Wir zeigen nur die andere Richtung: Sei $\{x_1, \ldots, x_n\} =: \mathfrak{E}$ ein Erzeugendensystem von M, wobei $\mathfrak{E}' := \{x_1, \ldots, x_m\} \subseteq \mathfrak{E}$ für $m \leq n$ ein maximal freies System bildet. Für alle $m < i \leq n$ gibt es $r_i, r_{i,j} \in R$ mit der Eigenschaft

$$r_i x_i = \sum_{j=1}^{m} r_{i,j} x_j$$

Definiere $r := r_{m+1} \cdot \ldots \cdot r_n$. Da $\mathfrak{E}'$ frei ist gilt dann für alle $i = 1...n$

$$r x_i \in \sum_{j=1}^{m} R x_j \cong \prod_{j=1}^{m} R x_j$$

Und somit ist für alle $m \in M$

$$rm \in \sum_{j=1}^{m} R x_j$$

Betrachte den folgenden R-Homomorphismus

$$\begin{array}{rcl} \varphi : M & \to & \bigoplus_{j=1}^{m} R x_j \\ m & \mapsto & rm \end{array}$$

φ ist wohldefiniert und es gilt: $\mathrm{Ker}(\varphi) \leq M_{tor} = \{0\}$ Damit ist φ injektiv und es ist

$$\mathrm{Im}(\varphi) \cong M \leq \bigoplus_{j=1}^{m} R x_j$$

mit Satz 3.3 ist M dann ein freier R-Modul. □

Satz 3.5 *Sei M ein endlich erzeugter R-Modul, dann gilt:*
$M = M_{tor} \oplus F$ mit einem freien R-Modul F.

Beweis. Betrachte die triviale exakte Sequenz:

$$0 \to M_{tor} \xrightarrow{\iota} M \xrightarrow{\pi} \bar{M} \to 0$$

Es gilt nach Bemerkung 3.2, dass $\bar{M} := {}^{M}\!/_{M_{tor}}$ torsionsfrei ist. Mit Satz 3.4 ist $\bar{M}$ dann ein freier R-Modul und mit Satz 2.16 ist $\bar{M}$ dann auch projektiv. Das heißt es gibt ein $s \in \mathrm{Hom}_R(\bar{M}, M)$ derart, dass $s \circ \pi = id_{\bar{M}}$ ist.Nun liefert die erste Aufgabe vom zweiten Übungsblatt: $M = M_{tor} \oplus s(\bar{M})$. Setze also: $F := s(\bar{M})$. □

Definition und Bemerkung 3.6 *(Rang von Moduln, p-primäre Elemente)*
Sei M ein endlich erzeugter R-Modul.
(a) Wir definieren Rang$(M) := \mathrm{rg}(M) := \dim_R(\bar{M})$.
(b) Es sei p ein Primelement[3] *von R.*

(i) $x \in M$ heißt p-primär (oder p-primäres Element), falls es ein $e \in \mathbb{N}$ gibt mit $p^e \cdot x = 0_M \Leftrightarrow p^e \subseteq \mathrm{Ann}(x)$
(ii) $M_{(p)} := \{x \in M \mid x$ ist p-primär $\}$ ist Untermodul der p-primären Elemente. □

Satz 3.7 *Sei $M = M_{tor}$ ein R-Torsionsmodul und bezeichne p Primelemente in R, dann gilt:*

$$M = \bigoplus_{(p) \lhd R} M_{(p)}$$

Bevor wir diesen wichtigen Satz beweisen, zeigen wir zunächst eine Bemerkung, die uns den Beweis von Satz 3.7 vereinfachen wird:

Bemerkung 3.8 *Sei $M = M_{tor}$ ein R-Torsionsmodul.*
(a) Seien $(q), (p_i)$ für $i \in I$ paarweise verschiedene Primideale von R, dann gilt:

$$M_{(q)} \cap \sum_{i \in I} M_{(p_i)} = \{0\}$$

(b) Seien $(p_1), \ldots, (p_n)$ paarweise verschiedene Primideale in R, dann gilt:

$$\begin{aligned} \mathrm{Ann}\left(\sum_{i=1}^{n} M_{(p_i)}\right) &\overset{(a)}{=} \mathrm{Ann}\left(\bigoplus_{i=1}^{n} M_{(p_i)}\right) = \bigcap_{i=1}^{n} \mathrm{Ann}(M_{(p_i)}) \\ &= \prod_{i=1}^{n} (p_i^{e_i}) \text{ mit } \mathrm{Ann}(M_{(p_i)}) = (p_i^{e_i}) \\ &= (p_1^{e_1}, \ldots, p_n^{e_n}) \end{aligned}$$

Beweis. Der Beweis zu (b) ist bereits in der Aussage enthalten, daher zu (a): Sei

$$x \in M_{(q)} \cap \sum_{i=1}^{n} M_{(p_i)}$$

[3] [L2] Kapittel 2.2: p Primelement $\overset{(HIR)}{\Longleftrightarrow}$ p unzerlegbar $\Leftrightarrow$ $(p) \trianglelefteq R$ Primideal

Dann lässt sich x darstellen als

$$x = \sum_{i=1}^{n} m_i \text{ mit } m_i \in M_{(p_i)}$$

Somit ist sowohl (q^e) also auch (m) in $\mathrm{Ann}(x)$ enthalten, wobei $m := \prod p_i^{e_i}$ mit $p_i^{e_i} \cdot m_i = 0$ gilt. Da q^e und m nach Voraussetzung teilerfremd sind, ist die Eins in $\mathrm{Ann}(x)$ enthalten und somit folgt $\mathrm{Ann}(x) = (1) = R$ Also ist $x = 0$. □

Beweis zu 3.7 Sei $x \in M = M_{tor}$ dann ist $(a) := \mathrm{Ann}(x)$ nicht das Nullideal. Zerlege a in Primfaktoren:

$$a = \prod_{i=1}^{n} p_i^{e_i}$$

Hierbei sind die $p_i^{e_i}$ paarweise verschiedene Primelelemente in R. Für $j = 1, ..., n$ setze nun

$$a_j := \frac{a}{p_j^{e_j}}$$

dann gilt: $\mathrm{ggT}(a_1, ..., a_n) = 1$, die a_j sind also Teilerfremd, d.h. es gibt $b_1, ..., b_n \in R$ mit

$$1 = \sum_{i=1}^{n} a_i b_i$$

Damit folgt

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

Es ist zu zeigen, dass $a_i, b_i x \in M_{(p_i)}$. Betrachte dazu:

$$p_i^{e_i} \cdot a_i \cdot b_i \cdot x = a \cdot b_i \cdot x = b_i \cdot a \cdot x = 0$$

Aus der zuvor bewiesenen Bemerkung 3.8 und dem Satz 2.3 folgt nun, dass diese Summe eine direkte Summe ist. □

Anmerkung Sei M ein endlich erzeugter R-Modul und p Primelelemente in R, dann gilt:

$$M = F \bigoplus \bigoplus_{p \lhd R} M_{(p)}$$

Satz 3.9 *Sei p ein Primelelement in R und M ein endlich erzeugter p-primärer R-Modul (Also $M = M_{(p)}$). Dann gibt es $\{x_1, ..., x_n\} =: E \subseteq M$, so dass $M = \bigoplus Rx_i$ mit $\mathrm{Ann}(x_i) = (p^{e_i})$ mit eindeutig bestimmten Exponenten derart, dass $e_1 \leq \ldots \leq e_n$.*

Auch den Beweis dieses Satzes splitten wir wieder in mehrere Bemerkungen auf.

Definition und Bemerkung 3.10 *(Annulator eines Moduls)*
Sei M ein R-Modul mit einem Erzeugendensystem $E := \{x_1, ..., x_n\} \subseteq M$, dann gilt:

$$\mathrm{Ann}(M) := \bigcap_{y \in M} \mathrm{Ann}(y) = \bigcap_{x_i \in E} \mathrm{Ann}(x_i)$$

und $\mathrm{Ann}(M)$ heißt der Annulator von M.

Beweis. „$\subseteq$“ ist trivial, da auf der Linken Seite über mehr Ideale geschnitten wird.
„$\supseteq$“: Sei

$$r \in \bigcap_{x_i \in E} \mathrm{Ann}(x_i)$$

Also ist für alle $i = 1...n$ das Produkt $r \cdot x_i$ Null. Sei nun $y \in M$ mit $y = \sum_{i=1}^{n} r_i x_i$ Dann folgt

$$r \cdot y = r \cdot \sum_{i=1}^{n} r_i x_i \qquad \text{mit } r_i \in R$$

Es gilt: $\sum_{i=1}^{n} r_i \cdot r \cdot x_i = 0$ und somit $r \in \mathrm{Ann}(x)$ □

Bemerkung 3.11 *Sei M ein endlich erzeugter R-Torsionsmodul, also $M = M_{tor}$ und $(a) := \mathrm{Ann}(M)$ mit $a = \prod_{i=1}^{n} p_i^{e_i}$ mit paarweise verschiedenen Primelementen p_i, dann gelten:*
(a) $M = \bigoplus_{i=1}^{n} M_{(p_i)}$ und $\mathrm{Ann}(M_{(p_i)}) = (p_i^{e_i})$
(b) Es gibt ein $y \in M$ derart, dass $\mathrm{Ann}(M) = \mathrm{Ann}(y)$ gilt.

Beweis. Teil (a) folgt aus Satz 3.5 und Bemerkung 3.8 b.
Zu (b):
Sei $\{x_1, ..., x_n\} =: E \subseteq M$ ein Erzeugendensystem von M. Wir wollen zunächst annehmen, dass M für ein Primelelement q ein q-primärer Modul ist. Nach Bemerkung 3.10 gilt:

$$\mathrm{Ann}(M) = \bigcap_{i=1}^{n} \mathrm{Ann}(x_i) = \bigcap_{i=1}^{n} (q^{e_i}) \text{ mit } \mathrm{Ann}(x_i) = (q^{e_i})$$

Sei $e_j := \max_{i=1..n} \{e_i\}$, dann gilt:

$$\bigcap_{i=1}^{n} (q^{e_i}) = (p^{e_j}) = \mathrm{Ann}(x_j)$$

Wir lassen nun die Annahme, dass M q-primär sei, fallen, und betrachten den allgemeinen Fall:
Nach (a) gilt:

$$M = \bigoplus_{i=1}^{n} M_{(p_i)}$$

Im Speziallfall haben wir gezeigt, dass es für alle $i = 1...n$ ein $y_i \in M_{(p_i)}$ gibt, so dass die Behauptung $Ann(y_i) = Ann(M_{(p_i)} = (p_i^{e_i})$ gilt. Setze $y := \sum_{i=1}^{n} y_i$, dann ist $\mathrm{Ann}(y) = (p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}) = \mathrm{Ann}(M)$
□

Anmerkung Sei M eine abelsche Gruppe, dann ist $\mathrm{Ann}(M)$ die kleinste natürliche Zahl, die jedes Element aus der Gruppe annuliert („Exponent von M“)
Beispiel $\mathbb{Z}/(p) \times \mathbb{Z}/(q) \times \mathbb{Z}/(q^2)$ hat Annulator (pq^2)

Definition und Bemerkung 3.12 *Sei M ein endlich erzeugter p-primärer R-Modul, wir definieren:*

$$M_p := \{\, x \in M \mid p \cdot x = 0 \,\}$$

Es gilt: M_p ist ein $R/(p)$-Vektorraum endlicher Dimension.

Beweis. Die Menge M_p ist ein $R/(p)$-Modul, denn (p) operiert trivial auf M_p. Es ist klar, dass M_p ein Vektorraum ist, denn (p) ist ein Primideal, hier[4] also auch ein Maximalideal und somit ist $R/(p)$ ein Körper. □

Beispiel 6 *Sei* $M := \bigoplus_{i=1}^{n} R/(p^{e_i}) = \bigoplus_{i=1}^{n} Rx_i$ *mit* $\mathrm{Ann}(x_i) = (p^{e_i})$*, dann ist*

$$M_p = \bigoplus_{i=1}^{n} R \cdot p^{e_i - 1} \cdot x_i \;\Rightarrow\; \dim_{R/(p)}(M_p) = n$$

Bemerkung 3.13 *Sei M ein endlich erzeugter p-primärer R-Modul. Es gelten:*
(a) Die Aussage $x \in M$ und $y \in Rx$ ist äquivalent zu $\mathrm{Ann}(x) = \mathrm{Ann}(y)$
(b) Ist $\mathrm{Ann}(M) = (p)$ *dann ist $M = M_p$ und dann gibt es $\{x_i, \dots, x_n\} \subseteq M$ mit*

$$M = \bigoplus_{i=1}^{n} Rx_i$$

(c) Sei $x \in M$ mit $\mathrm{Ann}(x) = \mathrm{Ann}(M)$ *und $\bar{y} \in M/Rx$, dann gibt es ein $y \in \bar{y} = y + Rx$ so dass* $\mathrm{Ann}(y) = \mathrm{Ann}(\bar{y})$
(d) Sei $x \in M$ mit $\mathrm{Ann}(x) = \mathrm{Ann}(M)$*, dann gilt:*

$$\dim_{R/(p)}[\left(M/Rx\right)_p] = \dim_{R/(p)}(M_p) - 1$$

Beweis. Zu (a): „⇒“ ist trivial. Für die Gegenrichtung sei $\mathrm{Ann}(x) = (p^e)$ Es gilt:
$y = r \cdot x = p^a \cdot c \cdot x$ mit p, c Teilerfremd und $a \geq 0$, also gibt es $u, v \in R$, so dass

$$1 = up^e + vc \Leftrightarrow x = up^e x + vcx \Leftrightarrow x = vcx$$

damit gilt: $\mathrm{Ann}(y) = (p^{e-a}) \Rightarrow a = 0 \Rightarrow y = c \cdot x$ und somit $\Rightarrow vy = vcx \Rightarrow vy = x \Rightarrow x \in Ry$
Es folgt die Gleichheit von Rx und Ry
Zu (b): Wir machen zur Vereinfachung eine Vorbemerkung:
Seien $N \leq M$, $x \in M \backslash N$, dann gilt:

$$N + Rx = N \bigoplus Rx \leq M$$

Beweis.

$$N \cap Rx = \begin{cases} \{0\} \\ Ry \text{ mit } y \in Rx \wedge y \neq 0 \end{cases}$$

Nach Voraussetzung gilt: $\mathrm{Ann}(M) = (p)$ also $\mathrm{Ann}(x) = (p) = \mathrm{Ann}(y)$. Aus (a) folgt nun
$Rx = Ry \leq N$ also ist $x \in N$ Da dies ein offensichtlicher Widerspruch ist folgt: $N \cap Rx = \{0\}$

[4] Vgl. [L2] Kapitel II §5

Und unsere Vorbemerkung ist bewiesen.
Sei nun $\{y_1, \dots, y_m\} =: E$ ein Erzeugendensystem von M. Setze $M_1 := Ry_1$ und für $i = 2...m$ setze:

$$M_i :== \begin{cases} M_{i-1} & \text{falls } y_i \in M_{i-1} \\ M_{i-1} + Ry_i & \text{falls } y_i \notin M_{i-1} \end{cases}$$

Nach der Vorbemerkung gilt dann für $n \leq m$:

$$M = \bigoplus_{i=1}^{n} M_i = \bigoplus_{i=1}^{n} Ry_i$$

Für den Beweis von (c) sei $y \in \bar{y}$ beliebig aber fest gewählt, dann gelten:

$$\mathrm{Ann}(x) = \mathrm{Ann}(M) = (p^t) \text{ und } \mathrm{Ann}(\bar{y}) = (p^b) \text{ sowie } \mathrm{Ann}(y) = (p^a) \text{ mit } a, b \leq t \text{ und } a \leq b$$

Betrachte: $p^b \cdot \bar{y} = 0$ also $p^b \cdot y = p^s \cdot c \cdot x$ mit zu p Teilerfremden c also $(p, c) = 1$. Weiter gilt:

$$\begin{aligned} & 0 = p^{a-b} \cdot p^b \cdot y = p^{a-b+s} \cdot c \cdot x \\ \Rightarrow \quad & t = a - b + s \Leftrightarrow t - a = s - b \geq 0 \Rightarrow s \geq b \\ \Rightarrow \quad & 0 = p^b(y - p^{s-b}) \cdot c \cdot x \end{aligned}$$

Definiere nun: $\hat{y} := y - p^{s-b} \cdot c \cdot x$ Dann ist $\hat{y} \in \bar{y}$ und es gilt: $\mathrm{Ann}(\hat{y}) = \mathrm{Ann}(\bar{y})$
Zu (d): Sei $\mathrm{Ann}(x) = (p^t)$, dann gilt:

$$\left({}^{M}\!/_{Rx}\right)_p \overset{(b)}{=} \bigoplus_{i=1}^{n} R\bar{X}_i \text{ mit } \bar{x}_i \in {}^{M}\!/_{Rx} \text{ und } \mathrm{Ann}(\bar{x}_i) = (p)$$

Wähle nun für alle i Elemente $x_i \in M$ mit $\mathrm{Ann}(x_i) = (p)$ nach Teil (c) und definiere $x_0 := p^{t-1}x$ dann ist $\mathrm{Ann}(x_0) = (p)$. Es gilt:

$$M_p = \sum_{i=0}^{n} Rx_i \qquad (1)$$

denn sei $m \in M_p$, dann ist

$$\begin{aligned} & \bar{m} = m + Rx \in \left({}^{M}\!/_{Rx}\right)_p \\ & \Rightarrow \bar{m} = \sum_{i=1}^{n} r_i \cdot x_i \Rightarrow m = \sum_{i=1}^{n} r_i \cdot x_i + r \cdot x \\ & \Rightarrow 0 = p \cdot m = \sum_{i=1}^{n} r_i \cdot p \cdot x_i + p \cdot r \cdot x \\ & \Rightarrow 0 = p \cdot r \cdot x \text{ mit } r = p^s \cdot c \text{ so dass } (p, c) = (1) \\ & \Rightarrow 0 = c \cdot p^{s+1}x \Rightarrow r = c \cdot p^s \in (p^{t-1}) \\ & \Rightarrow r \cdot x = r' \cdot p^{t-1} \cdot x = r' \cdot x_0 \text{ für } r' \in R \end{aligned}$$

Nach (b) ist die Summe (1) direkt, also gilt:

$$M_p = \bigoplus_{i=0}^{n} Rx_i$$

□

Anmerkung Sei x ein Torsionselement von M, dann betrachte den R-Hom.

$$\begin{array}{rcl} \varphi : R & \to & Rx \\ r & \mapsto & rx \end{array}$$

Es gilt φ ist surjektiv und $\mathrm{Ker}(\varphi) = \mathrm{Ann}(x)$.
Nach dem Homomorphiesatz gilt also:

$$Rx \cong {}^{R}\!/_{Ann(x)}$$

Wir fassen nun die soeben gemachten Bemerkungen zusammen und können nun Satz 3.9 beweisen:

Satz 3.9 *Sei p ein Primelement in R und M ein endlich erzeugter p-primärer R-Modul ($M = M_{(p)}$). Dann gibt es eine Erzeugendenmenge $\{x_1, \ldots, x_n\} =: E \subseteq M$, so dass $M = \bigoplus Rx_i$ mit $\mathrm{Ann}(x_i) = (p^{e_i})$ mit eindeutig bestimmten Exponenten derart, dass $e_1 \leq \ldots \leq e_n$.*

Beweis. Es sind noch Existenz und Eindeutigkeit zu zeigen. Für die Existenz genügt es

$$M = \bigoplus_{i=1}^{n} Rx_i$$

zu zeigen. Dies werden wir induktiv über $n = \dim_{{R}/{(p)}}(M_p)$ tun. Für den Induktionsanfang $(n = 0)$ gilt: $M = \{0\}$, denn sonst gibt es $0 \neq x \in M$ mit $\mathrm{Ann}(x) = (p^a)$ Also $0 \neq p^{a-1} \cdot x \in M_p$ Dies ist ein Widerspruch, da die Dimension 0 ist. Es gilt also:

$$M = \bigoplus_{i=0}^{0} \varnothing$$

Für den Induktions-Schritt $(n-1 \curvearrowright n)$ wähle $x \in M$ mit $\mathrm{Ann}(x) = \mathrm{Ann}(M)$. Nach Bemerkung 3.13 (b) gilt dann:

$$\dim_{{R}/{(p)}} \left[\left({M}/{Rx} \right)_p \right] = \dim_{{R}/{(p)}}(M_p) - 1 = n - 1$$

Also gibt es $\bar{x}_1, \ldots, \bar{x}_m \in {M}/{Rx}$ derart, dass

$$M/Rx = \bigoplus_{i=1}^{m} Rx_i$$

Wähle nun nach Bemerkung 3.13 (c) Vertreter $x_i \in \bar{x}_i$ mit $\mathrm{Ann}(x_i) = \mathrm{Ann}(\bar{x}_i)$ für alle $i = 1, \ldots, m$. Wir Behaupten, dass dann gilt:

$$M = Rx \bigoplus_{i=1}^{m} Rx_i$$

Beweis. Sei $m \in M \Rightarrow \bar{m} = m + Rx = \sum_{i=1}^{m} r_i x_i$ Wir können nun m schreiben als:

$$m = rx + \sum_{1=i}^{m} r_i x_i$$

Diese Summe ist direkt, denn betrachte:

$$\begin{aligned} & 0 = rx + \sum_{i=1}^{m} r_i x_i \Rightarrow 0 = \sum_{i=1}^{m} r_i \bar{x}_i \\ \Rightarrow \quad & \forall\, i = 1, \ldots, m \quad r_i \bar{x}_i = 0 \\ \Rightarrow \quad & \forall\, i = 1, \ldots, m \quad r_i \in \mathrm{Ann}(\bar{x}_i) = \mathrm{Ann}(x_i) \\ \Rightarrow \quad & \forall\, i = 1, \ldots, m \quad r_i x_i = 0 \\ \Rightarrow \quad & rx = 0 \end{aligned}$$

Zum Nachweis der Eindeutigkeit betrachte:

$$M = \bigoplus_{i=1}^{n} Rx_i \text{ mit } \mathrm{Ann}(x_i) = (p^{e_i}) \quad \forall\, i = 1, \ldots, n$$

Die auftretenden Exponenten e_i sind eindeutig Bestimmt mit $1 \leq e_1 \leq \ldots \leq e_n < \infty$, denn betrachte für $\epsilon \in \mathbb{N}$

$$p^\epsilon M = \bigoplus_{i=1}^{n} Rp^\epsilon x_i = \bigoplus_{\substack{i=1 \\ e_i > \epsilon}}^{n} Rp^\epsilon x_i \qquad (*)$$

Die Anzahl der Summanden ungleich Null in $(*)$ ist gleich der Anzahl der Elemente in $D := \{ e_i \,|\, e_i > \epsilon \}$. Für D gilt aber:

$$\sharp D = \dim_{R/(p)} [(p^\epsilon M)_p]$$

Bemerke, dass die Dimension von $(p^\epsilon M)_p$ als $R/(p)$-Vektorraum ausschließlich von M abhängt, daher hängen auch die e_i ausschließlich von M ab, und sind daher eindeutig bestimmt. □

Satz 3.14 *(Hauptsatz über endlich erzeugte Moduln über Hauptidealringen)*
Sei M ein endlich erzeugter R-Modul. Dann gibt es $r \in \mathbb{N}$ und $x_{i,j} \in M$ mit der Eigenschaft:

$$M = R^r \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} Rx_{i,j}$$

wobei für alle i gilt: $\forall\, j = 1...m_i \;\; Ann(x_{i,j}) = (p_i^{e_{i,j}})$ mit $e_{i,1} \leq \ldots \leq e_{i,m_i}$ und die p_i sind paarweise nicht Assozierte Primelemente in R. Weiter sind die $e_{i,j}$ eindeutig bestimmt.

Beweis. Die Arbeit für diesen Beweis haben wir schon geleistet: In Satz 3.5 haben wir gezeigt, dass Moduln über Hauptidealringen in einen Freien und einen Torsionsmodul zerfallen. Dass wir Torsionsmoduln als direkte Summe von $M_{(p)}$ schreiben können ist die Aussage von Satz 3.7 und im Satz 3.9 haben wir gezeigt, dass p-primäre Moduln als direkte Summe geschrieben werden können. □

Variante zu 3.14
Es gibt eindeutig bestimmte $q_i \in R$ mit $q_1|q_2|\ldots|q_t$, so dass

$$M \cong \bigoplus_{i=1}^{t} {}^{R}\!/\!_{(q_i)}$$

Der Beweis, dass dies wirklich eine Variante zu 3.14 ist, war eine Übungsaufgabe.

Als Folgerungen erhalten wir nun einige schon bekannte Aussagen. Als erstes folgt der Hauptsatz über endlich erzeugte abelsche Gruppen, den wir in Algebra I nicht bewiesen haben:

Folgerung 3.15 *(Hauptsatz über endlich erzeugte abelsche Gruppen)*
Sei G eine endlich erzeugte abelsche Gruppe, dann gibt es eindeutig bestimmte $q_i \in \mathbb{N}$ mit $q_i|q_{i+1}$, so dass

$$G \cong \bigoplus_{i=1}^{n} {}^{\mathbb{Z}}\!/\!_{(q_i)}$$

Beweis. Dieser Satz ist ein Spezialfall von Satz 3.14 mit $R = \mathbb{Z}$. □

Folgerung 3.16 *(Allgemeine Jordansche Normalform)*
Sei K ein Körper und V ein K-Vektorraum mit $\dim_K(V) < \infty$. Weiter seien $\varphi \in \mathrm{End}_K(V)$ ein K-linearer Endomorphismus und $f(X) \in K[X]$ das Minimalpolynom zu φ. Da $K[X]$ ein Hauptidealring ist, faktorisiere $f(X)$:

$$f(X) = \prod_{i=1}^{n} p_i(X)^{e_i}$$

mit paarweise normierten Primpolynomen der Form:

$$p_i(X) = \prod_{j=0}^{d_i} c_{i,j} X^j$$

Setze:

$$B_i := \begin{pmatrix} 0 & 0 & & & -c_{i,0} \\ 1 & 0 & & & -c_{i,1} \\ 0 & 1 & \ddots & & \vdots \\ & & \ddots & & \vdots \\ & & & 1 & 0 & -c_{i,d_i-2} \\ & & & 0 & 1 & -c_{i,d_i-1} \end{pmatrix}$$

Dann gibt es eine Basis $\mathfrak{B}$ von V. Ferner gibt es $t_1, \ldots, t_n \in \mathbb{N}$ sowie $e_{i,j} \in \mathbb{N}$, so dass φ bezüglich der Basis $\mathfrak{B}$ die folgende Form hat:

$$\begin{pmatrix} \boxed{A_1} & & & \\ & \boxed{A_2} & & \\ & & \ddots & \\ & & & \boxed{A_n} \end{pmatrix}$$

mit

$$A_i = \begin{pmatrix} \boxed{D_{i,1}} & & & \\ & \boxed{D_{i,2}} & & \\ & & \ddots & \\ & & & \boxed{D_{i,t_i}} \end{pmatrix}$$

Hierbei ist $D_{i,j}$ von der folgenden Form:

$$D_{i,j} = \begin{pmatrix} \boxed{B_i} & & & & \\ 1 & \boxed{B_i} & & & \\ & 1 & \ddots & & \\ & & \ddots & & \\ & & & 1 & \boxed{B_i} \end{pmatrix}$$

Der Block B_i wird genau $e_{i,j}$-mal wiederholt in $D_{i,j}$. Im Spezialfall $K = \bar{K}$ ist K bereits algebraisch abgeschlossen, daher gilt: $p_i = x - a_i$ und somit ist $B_i = (a_i) \in \mathrm{Mat}_{\bar{K}}(1,1)$

Beweis. V ist ein endlich erzeugter $K[X]$-Torsionsmodul, also gilt nach dem Hauptsatz 3.14:

$$V \cong \bigoplus_{i=1}^{n} V_i$$

mit V_i ist p_i-primärer Modul. Diese Zerlegung liefert die Verteilung der A_i. Weiter gilt:

$$V_i = \bigoplus_{i=1}^{t_i} V_{i,j}$$

mit $\mathrm{Ann}(V_{i,j}) = (p_i^{e_{i,j}})$. Diese Zerlegung liefert die $D_{i,j}$. □

Kapitel II

Zahlringe (I)

4 ganze Zahlen

In diesem Kapitel werden wir ganze Zahlen in Ringen betrachten. Hierbei werden wir viele Parallelen zu den „algebraischen Zahlen“ aus Algebra I feststellen. Beispiele für Zahlringe zu Körpern sind:

Körper	ganze Zahlen	
$\mathbb{Q}$	$\mathbb{Z}$	
$K(X)$	$K[X]$	
$\mathbb{Q}(\zeta_n)$	$\mathbb{Z}[\zeta_n]$	mit $\zeta_n := e^{\frac{2\pi i}{n}}$
Achtung: Im Allgemeinen gilt nicht:		
$\mathbb{Q}(\sqrt{d})$	$\mathbb{Z}[\sqrt{d}]$	mit $d \in \mathbb{Z}$

Definition 4.1 *(Zahlkörper)*
Jede endliche Körpererweiterung (KpErw.) von $\mathbb{Q}$ heißt Zahlkörper.

Bemerkung 4.2 *Sei L/K endliche Galois-Erweiterung und $B \subseteq L$ ein Teilring in L, so dass für alle $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ gilt $\sigma(B) = B$ mit einem algebraische Abschluss $\bar{K}$ von K. Dann hat das Minimalpolynom von jedem $\alpha \in B$ Koeffizienten in $B \cap K$.*

Beweis. Betrachte die Menge: $\{\, \sigma(\alpha) \,|\, \sigma \in \mathrm{Hom}_K(L, \bar{K}) \,\} = \{\, \alpha =: \alpha_1, \ldots, \alpha_n \,\}$. Dann gilt für das zu α gehörige Minimalpolynom f_α die Zerlegung

$$f_\alpha(X) = \prod_{i=1}^{n}(X - \alpha_i) = \sum_{j=0}^{n} c_j X^j$$

Es gilt: $c_j \in L^{\mathrm{Gal}(L/K)} = K$ aber auch $c_j \in B$, denn alle α_i sind Elemente aus B, da $\sigma(B) = B$, daher gilt für alle $j = 1...n$, dass die c_j Elemente von $B \cap K$ sind □

Die Bemerkung 4.2 führt uns auf die Aussage, dass ganze Elemente von L Minimalpolynome in $(B \cap K)[X]$ haben sollten, wenn B die ganzen Zahlen von L sind.

Erinnerung (algebraische Zahlen)
Sei L/K eine Körpererweiterung und $\alpha \in L$, dann heißt α algebraisch, wenn es ein normiertes Polynom $f(X) \in K[X]$ mit $f(\alpha) = 0$ gibt.

Definition 4.3 *(ganzes Element, ganz abgeschlossen, ganze Erweiterung)*
Sei A ein Ring und B ein Erweiterungsring zu A ($A \subseteq B$). Ein Element $\alpha \in B$ heißt ganz über A, wenn es ein normiertes Polynom $f(X) \in A[X]$ mit $f(\alpha) = 0$ gibt.
Die Menge $\tilde{A} = \{ \alpha \in B \mid \alpha \text{ ganz über } A \}$ heißt ganz abgeschlossen bzw. der ganze Abschluss von A in B. Die Erweiterung $B \supseteq A$ (bzw. B/A) heißt ganz, wenn jedes $\alpha \in B$ ganz über A ist.

Anmerkung A priori ist nicht klar, ob $\tilde{A}$ ein Ring ist.

Erinnerung (algebraische Zahlen)
Sei L/K eine Körpererweiterung dann sind die folgenden Aussagen äquivalent:
(1) Das Element $\alpha \in L$ ist algebraisch über K
(2) $K(\alpha)/K$ ist eine endliche Körpererweiterung
(3) Es gibt eine endliche Körpererweiterung T/K mit der Eigenschaft, dass $\alpha \in T$ liegt.
Analoge Äquivalenzen für ganze Elemente folgern wir in Satz 4.5.

Generalvoraussetzung Wir betrachten nun nurnoch kommutative Ringe.

Bemerkung 4.4 *(Gramsche Regel / Laplacescher Entwicklungssatz)*
Sei A ein Ring und $M := (m_{ij}) \in \mathrm{Mat}_A(n,n)$ eine Matrix. Die zu M adjungierte Matrix $M^* = (m^*_{ij}) \in \mathrm{Mat}_A(n,n)$ hat Einträge $m^*_{ij} = \det(M^{ij})$, wobei $M^{ij} = M$ ohne i-te Spalte und j-te Zeile ist. Es gilt: $M \cdot M^* = M^* \cdot M = det(M) \cdot I_n$, wobei I_n die $n \times n$ Einheitsmatrix ist.

Beweis. Der Beweis dieser Regel über Ringen ist Wörtlich der gleiche, wie der aus der linearen Algebra bekannte Beweis über Körpern.

Definition und Satz 4.5 *(Treuer Modul)*
Sei A ein Ring und B ein Erweiterungsring zu A. Sei weiter $\alpha \in B$. Es sind äquivalent:
(i) α ist ganz über A
(ii) $A[\alpha]$ ist endlich erzeugter A-Modul
(iii) Es gibt einen endlich erzeugten A-Modul $T \subseteq B$, der treuer $A[\alpha]$-Modul ist, d.h.

- $\alpha T \subseteq T$
- $xT = 0$ *mit* $x \in A[\alpha] \Rightarrow x = 0$
  ($Ann_{A[\alpha]}(T) = (0)$)

Beweis. per Ringschluss:
„(i) $\Rightarrow$ (ii)“
Nach Voraussetzung ist α ganz über A also gibt es ein normiertes Polynom $f(X) = \sum_{i=0}^{n} c_i X^i \in A[X]$ derart, dass $f(\alpha) = 0$ ist. Also können wir die n-te Potenz von α schreiben als

$$\alpha^n = -(c_{n-1} \cdot \alpha^{n-1} + \ldots + c_0)$$

und somit ist

$$A[\alpha] = \sum_{i=0}^{n-1} A\alpha^i$$

ein endlich erzeugter A-Modul.
„(ii) $\Rightarrow$ (iii)“

Setze $T := A[\alpha]$, dann ist nach Voraussetzung klar, dass T endlich erzeugt ist.
Zur Treuheit: Es gilt $1 \in T$, also folgt aus $xT = 0$ insbesondere $x \cdot 1 = x = 0$
„(iii) $\Rightarrow$ (i)“
Nach Voraussetzung ist T ein endlich erzeugter treuer A-Modul, also

$$T = \sum_{i=1}^{n} At_i \text{ mit } t_1, \dots, t_n \in T$$

Es gilt: $\alpha T \subseteq T$ also

$$\alpha t_j = \sum_{i=1}^{n} m_{ij} t_i \text{ mit } m_i j \in A$$

Setze $M := (m_{ij}) \in \mathrm{Mat}_A(n, n)$ und betrachte:

$$\begin{pmatrix} m_{11} & & & m_{n1} \\ & \ddots & \iddots & \\ & \iddots & \ddots & \\ m_{1n} & & & m_{nn} \end{pmatrix} \begin{pmatrix} t_1 \\ \vdots \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} \alpha t_1 \\ \vdots \\ \vdots \\ \alpha t_n \end{pmatrix} = \begin{pmatrix} \alpha & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \alpha \end{pmatrix} \begin{pmatrix} t_1 \\ \vdots \\ \vdots \\ t_n \end{pmatrix}$$

Setze nun $D := (\alpha \cdot I_n - M) \cdot t = 0$ mit $t := (t_i)_{i=1\dots n}$Nach Bemerkung 4.4 gilt:

$$0 = D^* \cdot D \cdot t = \det(D) \cdot I_n \cdot t = \det(D) \cdot t$$

Da T nach Voraussetzung treu ist, gilt: $\det(D) = 0$. Setze $f(X) := \det(X \cdot I_n - M) \in A[X]$, dann ist $f(X)$ normiert und erfüllt $f(\alpha) = 0$ □

Folgerung 4.6 *Seien $A \subseteq B$ Ringe und $\alpha_1, \dots, \alpha_n \in B$ seien ganz über A, dann ist $A[\alpha_1, \dots, \alpha_n] \subseteq B$ eine ganze Ringerweiterung von A und ist $A[\alpha_1, \dots, \alpha_n]$ als A-Modul endlich erzeugt.*

Beweis. Induktiv über n:
Den Induktionsanfang bei $(n = 1)$ haben wir in Satz 4.5 gezeigt. Wir betrachten nun den Induktionsschritt $(n - 1 \curvearrowright n)$
Nach Annahme ist $T := A[\alpha_1, \dots, \alpha_{n-1}]$ ein endlich erzeugter A-Modul den wir auch durch

$$T = \sum_{i=1}^{r} At_i$$

darstellen können. Weiter ist $A[\alpha_n] = \sum_{i=1}^{m} A\alpha_n^j$ ein endlich erzeugter A-Modul. Insbesondere ist

$$\alpha_n^{m+1} = \sum_{j=1}^{m} a_j \cdot \alpha_n^j \text{ mit } a_j \in A$$

Es gilt:

$$A[\alpha_1, \dots, \alpha_n] = T[\alpha_n] = \left(\sum_{i=1}^{r} At_i \right) [\alpha_n] = \sum_{i=1}^{m} \sum_{i=1}^{r} At_i \alpha_n^j$$

ist ein endlich erzeugter A-Modul.
Sei $\beta \in A[\alpha_1, \dots, \alpha_n]$ und wähle T wie in Satz 4.5 (iii) als $A[\alpha_1, \dots, \alpha_n]$ dann gilt: $\beta T \subseteq T$, und T ist treu, da $1 \in T$ ist. Nach Satz 4.5 ist β dann ganz über A. □

Folgerung 4.7 *Seien $A \subseteq B \subseteq C$ Ringe, dann gilt: Die Ringerweiterung C/A ist genau dann ganz, wenn sowohl C/B als auch B/A ganze Ringerweiterungen sind.*

Beweis. Die Richtung „⇒“ ist trivial. Zum Beweis der gegenrichtung sei $\alpha \in C$. Es gibt dann ein normiertes Polynom $f(X) = \sum_{i=0}^{n} b_i X^i \in B[X]$ mit $f(\alpha) = 0$. Nach Folgerung 4.6 ist $A[b_0, \ldots, b_n]$ als A-Modul endlich erzeugt über A. Somit ist wegen f auch $A[b_0, \ldots, b_n, \alpha]$ endlich erzeugt über A. Mit Satz 4.5 folgt sofort, dass α ganz über A ist. □

Satz 4.8 *Seien B/A (also $A \subseteq B$) Ringe, dann gilt:*

$$\tilde{A} := \{\, \alpha \in B \mid \alpha \text{ ganz über } A \,\} \subseteq B$$

ist ein Ring und jedes $\beta \in B$, das ganz über $\tilde{A}$ ist, liegt bereits in $\tilde{A}$.

Beweis. $\tilde{A}$ ist ein Teilring von B, denn seien $\alpha, \beta \in \tilde{A}$ dann folgt mit Folgerung 4.6, dass $A[\alpha, \beta]$ eine ganze Ringerweiterung von A ist. Daher gilt: $\alpha - \beta, \alpha + \beta, \alpha \cdot \beta \in A[\alpha, \beta]$ sind ganz über A, und somit in $\tilde{A}$ enthalten.
Bemerke: $1 \in \tilde{A}$, denn $f(X) := X - 1$ hat Eigenschaft $f(1) = 0$.
Sei $\alpha \in B$ ganz über $\tilde{A}$ dann gilt mit Folgerung 4.7, dass α ganz über A ist. Somit liegt auch $\alpha \in \tilde{A}$ und der Satz ist bewiesen. □

Definition 4.9 *(Normalisierung, Ring der ganzen Zahlen, ganz abgeschlossen, quadratfrei)*
Sei L ein Körper und $A \subseteq L$ ein Teilring von L.

$$A_L := \{\, x \in L \mid x \text{ ist ganz über } A \,\}$$

heißt die Normalisierung von A in L, die ganz abgeschlossene Hülle bzw. der ganze Abschluss von A in L. Wie in Satz 4.8 bewiesen ist A_L ein Ring.
Sei L ein Zahlkörper (d.h. $[L : \mathbb{Q}] < \infty$), dann heißt $\mathbb{Z}_L$ (Alternative Notation $\mathfrak{O}_L$) Ring der ganzen Zahlen von L.
Sei A ein Integritätsring (IB), dann heißt A ganz abgeschlossen, wenn A ganz abgeschlossen in $\mathrm{Quot}(A) =: K$ ist, also wenn $A_K = A$ gilt.
Sei A ein faktorieller Ring (ZPE), genau dann heißt $d \in A$ quadratfrei, wenn in der Primfaktorzerlegung von d über A keine Primzahl mehrfach vorkommt.

Beispiel 7 *Sei $d \in \mathbb{Z} \backslash \{0, 1\}$ weiter sei d quadratfrei. Betrachte $L := \mathbb{Q}(\sqrt{d})$. Es gilt*

$$\mathbb{Z}_L = \mathfrak{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \equiv 2, 3 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{falls } d \equiv 1 \quad (4) \end{cases}$$

Satz 4.10 *Faktorielle Ringe sind ganz abgeschlossen.*

Beweis. Sei A ein faktorieller Ring (ZPE) und bezeichne $K := \mathrm{Quot}(A)$ den Quotientenkörper von A. Weiter sei $y = \frac{b}{c} \in K$ ein Element mit $b, c \in A$, so dass $\mathrm{ggT}(b, c) = 1$ ist. Nimm an, dass y ganz über A ist, d.h. für $a_i \in A$ gilt:

$$\begin{aligned} & 0 = y^n + a_{n-1} y^{n-1} + \ldots + a_1 y + a_0 \\ \Leftrightarrow \quad & 0 = \frac{b^n}{c^n} + a_{n-1} \frac{b^{n-1}}{c^{n-1}} + \ldots + a_0 \\ \Leftrightarrow \quad & 0 = b^n + c \cdot b^{n-1} \cdot a^{n-1} + \ldots + c^{n-1} \cdot b \cdot a_1 + c^n a_0 \\ \Leftrightarrow \quad & b^n = -c \cdot (a_{n-1} b^{n-1} + \ldots + c^{n-1} a_0) \end{aligned}$$

Daher ist c notwendig eine Einheit in A und somit muss y in A liegen. □

Bemerkung 4.11 *Sei A ein ganz abgeschlossener Integritätsring und $K := \mathrm{Quot}(A)$ sein Quotientenkörper. Weiter sei $\bar{K}$ ein algebraischer Abschluss zu K und $y \in \bar{K}$ ein Element. Es gilt: y ist genau dann ganz über A, wenn das Minimalpolynom f_y zu y Koeffizienten in A hat.*

Beweis. Nach Voraussetzung hat das Minimalpolynom zu y Koeffizienten in A. Es gelten: $f_y(y) = 0$ und $f_y(X) \in A[X]$ ist normiert. Nach Voraussetzung ist y nun ganz über A daher gibt es ein normiertes Polynom $g \in A[X]$ mit $g(y) = 0$. Sei $f_y(X) \in K[X]$ das Minimalpolynom zu y, dann teilt f_y das Polynom g, denn $g \in A[X] \subset K[X]$. Betrachte die Menge $M = \{\, \sigma(y) \mid \sigma \in \mathrm{Hom}_K(K(y), \bar{K}) \,\}$ der Konjugierten von y. Alle $z \in M$ sind Nullstellen von g, da es Nullstellen von f_y sind. Daher folgt, dass alle $\sigma(y)$ ganz sind, denn sei $G := \mathrm{Hom}_K(K(y), \bar{K})$, dann

$$f_y(X) = \prod_{\sigma \in G} (X - \sigma(y)) \in K[X] \cap B[X] \quad \text{mit } B = A_{K(y)}$$

Da A ganz abgeschlossen in K ist folgt: $f_y(X) \in A[X]$. □

Satz 4.12 *Sei A ein Integritätsring, $K := \mathrm{Quot}(A)$ sein Quotientenkörper sowie L/K eine endliche Körpererweiterung und $B := A_L$, dann gelten:*

(a) *Jedes $y \in L$ lässt sich schreiben als $y = \frac{b}{a}$ mit $b \in B$ und $a \in A$.*
Insbesondere ist $L = \mathrm{Quot}(B)$

(b) *B ist ganz abgeschlossen*

(c) *Ist A ganz abgeschlossen, dann gilt $B \cap K = A$*

(d) *Ist L/K galoisch, dann ist $\sigma(B) = B$für alle $\sigma \in \mathrm{Gal}(L/K)$ und,*
falls A ganz abgeschlossen ist, dann gilt: $B^{\mathrm{Gal}(L/K)} = A$

Beweis.

zu a) Sei $y \in L$ und $f(X) = \sum_{i=1}^{n} a_i x^i \in K[X]$ das Minimalpolynom von y. Nach Voraussetzung ist $K = \mathrm{Quot}(A)$ also gilt $a_n = 1, a_i = \frac{b_i}{c_i}$ mit $b_i, c_i \in A$ für $i = 1, \ldots, n$ und somit folgt $0 = y^n + \frac{b_{n-1}}{c}{}_{n-1} y^{n-1} + \ldots + \frac{b_0}{c_0}$ Definiere nun $c := \prod_{i=1}^{n-1} c_i$ Dann ist $0 = (cy)^n + c\frac{b_{n-1}}{c_{n-1}}(cy)^{n-1} + \ldots + c^n \frac{b_0}{c_0}$ und somit ist cy ist ganz über A, das heißt $cy = b$ für $b \in B$ und somit gilt $y = \frac{b}{c}$

zu b) Bereits bewiesen in Satz 4.8

zu c) „$\subset$“: Sei $x \in B \cap K \Leftrightarrow x \in B$ ganz über A und $x \in K$.
Da A nach Vor. ganz abgeschlossen in K ist gilt aber: $x \in A_K = A$
„$\supset$“: Sei $x \in A$ ganz $\Rightarrow\ x \in K$ und $x \in A_K \subseteq B \Rightarrow x \in K \cap B$

zu d) Sei $b \in B$ gegeben und $\sigma \in \mathrm{Gal}(L/K)$ und weiter sei $g(X) \in A[X]$ ein normiertes Polynom mit Nullstelle b, also $g(b) = 0$
$\Rightarrow\ 0 = \sigma(0) = \sigma(g(b)) = g(\sigma(b))$
$\Rightarrow\ \sigma(b) \in B\ \Rightarrow\ \sigma(B) \subseteq B\ \Rightarrow\ B = \sigma^{-1}(\sigma(B)) \subseteq \sigma^{-1}(B)$
Sei nun A ganz abgeschlossen, dann gilt:
$B^{\mathrm{Gal}(L/K)} = B \cap L^{\mathrm{Gal}(L/K)} = B \cap K = A$ □

Satz 4.13 *(Elementarteilersatz)*
Sei R ein Hauptidealring und F ein freier R-Modul von endlichem Rang. Sei weiter $M \subseteq F$ ein R-Untermodul von F, dann gibt es eine Basis $\mathfrak{B}$ von F mit $e_1, \ldots, e_m \in \mathfrak{B}$ und es gibt $a_1, \ldots, a_m \in R$, so dass
(i) M die Basis $\{a_1e_1, \ldots, a_me_m\}$ hat.
(ii) $a_1 | \ldots | a_m$
Die Folge der Ideale $(a_1) \supseteq (a_2) \supseteq \ldots \supseteq (a_m)$ ist eindeutig.

Beweis. Die Eindeutigkeit folgt aus dem Hauptsatz über endlich erzeugte Moduln über Hauptidealringen (Satz 3.14). Zum Beweis der Existenz sei $\{b_1, \ldots, b_n\} =: \mathfrak{B}' \subseteq F$ Basis von F. Betrachte die Koordinatenfunktion

$$\begin{array}{rccc} \kappa_i : & F & \to & R \\ & \sum_{j=1}^{n} r_j b_j & \mapsto & r_i \end{array}$$

Für alle i ist $\kappa_i \in \mathrm{Hom}_R(F, R)$ ein Homomorphismus. Betrachte die Abbildung

$$\begin{array}{ccc} \mathrm{Hom}_R(F,R) & \to & \{\mathfrak{a} \,|\, \mathfrak{a} \trianglelefteq R\} \\ \lambda & \mapsto & \lambda(M) \quad \trianglelefteq R \end{array}$$

Wähle $\lambda_1 \in \mathrm{Hom}_R(F, R)$ maximal in dem Sinn, dass aus $\lambda_1(M) \subseteq \mu(M)$ stets $\lambda_1 = \mu$ folgt. Benenne $\lambda_1(M) =: (a_1) \neq (0)$ falls $M \neq (0)$. Es gibt ein $x_1 \in M$ mit der Eigenschaft: $\lambda_1(x_1) = a_1$
Für alle $\lambda \in \mathrm{Hom}_R(F, R)$ ist $\lambda(x_1) \in (a_1)$, denn sonst gelte
$(y) = (\lambda(x_1), (a_1)) \supsetneq (a_1)$ und somit ließe sich y darstellen als $y = r\lambda(x_1) + sa_1$ mit $r, s \in R$
Definiere $\tilde{\lambda} := r\lambda + s\lambda_1$ dann ist $\tilde{\lambda}(x_1) = y$ und somit ist $\tilde{\lambda}(M)$ nicht in $\lambda_1(M)$ enthalten. Dies ist aber ein Widerspruch zur Maximalität von λ_1.
Insbesondere liegt für alle $i = 1, ..., n$ $\kappa_i(x_1)$ wieder in (a_1). Es folgt, dass alle Koordinaten von x_1 bezüglich $\mathfrak{B}'$ durch a_1 teilbar sind, also gibt es $e_1 \in F$ mit der Eigenschaft $a_1e_1 = x_1$. Es gilt: $F = Re_1 \bigoplus \mathrm{Ker}(\lambda_1)$, denn

1. $Re_1 \cap \mathrm{Ker}(\lambda_1) = \{\, ae_1 \,|\, a \in R \wedge \lambda_1(ae_1) = 0 \,\} = (0)$, denn
   $\lambda_1(ae_1) = 0 \Rightarrow 0 = \lambda(aa_1e_1) = a\lambda(x_1) = a \cdot a_1$
2. Sei $x \in F$ so folgt:
   $\lambda_1(x - \lambda_1(x)e_1) = \lambda_1(x) - \lambda_1(\lambda_1(x)e_1) = \lambda_1(x) - \lambda_1(x) \cdot 1 = 0$
   denn $a_1 = \lambda(x_1) = \lambda_1(a_1e_1) = a_1\lambda_1(e_1)$

Bezeichne $F_1 := \mathrm{Ker}(\lambda_1)$ und $M_1 := M \cap F_1$, dann gilt:

$$Rx_1 \bigoplus M_1 = M \subseteq F = Re_1 \bigoplus F_1$$

Fahre nun induktiv fort, dies ist möglich, da $\mathrm{rg}(M_1) = \mathrm{rg}(M) - 1$ ausserdem gilt: $\lambda \in \mathrm{Hom}_R(F_1, R)$ also $\lambda(M_1) \subseteq (a_1)$, denn sonst gelte mit $m \in M_1$: $(y) = (a_1, \lambda(m)) \supsetneq (a_1)$. Damit ließe sich y aber darstellen als $y = ra_1 + s\lambda(m)$ mit $r, s \in R$ Betrachte nun die Abbildung:

$$\begin{array}{rccc} \tilde{\lambda} : & Re_1 \bigoplus F_1 & \to & R_1 \\ & ae_1 + b & \mapsto & ra + s\lambda(b) \end{array}$$

Es gelte $\tilde{\lambda}(a_1e_1 + m) = ra_1 + s\lambda(m) = y$ und somit $\tilde{\lambda}(M) \supsetneq (a_1)$
Dies ist aber ein Widerspruch zur Maximalität von λ_1. □

5 Ideale und die Diskriminante

Motivation Im Allgemeinen ist der Ring der ganzen Zahlen eines Zahlkörpers kein faktorieller Ring.

Beispiel 8 $L := \mathbb{Q}(\sqrt{-5})$ *Es gilt:* $-5 \equiv 3\ (4)$ $\Rightarrow \mathfrak{O}_L = \mathbb{Z}[\sqrt{-5}]$
Betrachte $6 = 2 \cdot 3 = (1-\sqrt{-5}) \cdot (1+\sqrt{-5})$ *Es gilt:* 2 *und* 3 *sind nicht zu* $(1-\sqrt{-5})$, $(1+\sqrt{-5})$ *assoziert. Ausserdem sind* 2, 3, $(1-\sqrt{-5})$, $(1+\sqrt{-5})$ *unzerlegbar in* $\mathbb{Z}[\sqrt{-5}]$. *Damit ist der Ring* $\mathbb{Z}[\sqrt{-5}]$ *nicht faktoriell.*

Ziel ist zu zeigen, dass $\mathbb{Z}_L$ die „eindeutige Primidealfaktorisierung“ gilt.

Satz 5.1 *Sei* $p \neq 2$ *eine Primzahl. Genau dann gibt es natürliche Zahlen* a, b *mit der Eigenschaft* $p = a^2 + b^2$, *wenn* $p \equiv 1\ (4)$ *ist.*

Satz 5.2 *(Eigenschaften von* $\mathbb{Z}\,[i]$*)*

(a) $\mathbb{Z}[i]$ *mit* $i^2 = -1$ *ist der Ring der ganzen Zahlen von* $\mathbb{Q}(i)$

(b) $\mathbb{Z}[i]$ *ist euklidisch und somit faktoriell*

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

(d) *Die Primelemente von* $\mathbb{Z}[i]$ *sind (bis auf assozierte) die folgenden:*

- $1 + i$
- $a + ib$ *mit* $a^2 + b^2 = p$ *(prim)* $\in \mathbb{Z}$ *mit* $p \equiv 1\ (4)$ *und* $a > |b| > 0$
- p *(prim)* $\in \mathbb{Z}$ *mit* $p \equiv 3\ (4)$

Beweis.

zu a) $i = \sqrt{-1}$ und $-1 \equiv 3\ (4)$. Somit ist (a) ein Spezialfall von Aufgabe 1 des 4. Übungsblattes.

zu b) Aus Algebra I ist bekannt, dass $\mathbb{Z}[i]$ euklidisch ist bezüglich
$N : \mathbb{Z}[i] \ni a + ib \mapsto a^2 + b^2 \in \mathbb{N}$

zu c) Es gilt: $N(xy) = N(x) \cdot N(y)$. Sei $x = a + ib \in \mathbb{Z}[i]^*$, dann gibt es ein $y \in \mathbb{Z}[i]^*$ mit $1 = xy$.
Betrachte: $N(1) = 1 = N(x)N(y)$
$\Rightarrow\ N(x) = a^2 + b^2 = 1.$

zu d) Beh. 1: Sei p eine Primzahl in $\mathbb{Z}$. Es gilt: -1 ist Quadrat in $\mathbb{F}_p^* \Leftrightarrow p \equiv 1\ (4)$
Beweis. $\mathbb{F}_p^* \cong \mathbb{Z}(p-1)\mathbb{Z}$ und damit ist -1 genau dann ein Quadrat in $\mathbb{F}_p^*$, wenn es ein $x \in \mathbb{F}_p^*$ mit $\mathrm{Ord}(x) = 4$ gibt. D.h. genau dann, wenn $4|(p-1)$ $\triangle$

Beh. 2: Sei a eine ganze Zahl, dann gilt: $a^2 \equiv 0, 1\ (4)$
Beweis. Sei $p \equiv 1\ (4) \Rightarrow \exists\, x \in \mathbb{F}_p^* : x^2 + 1 = 0$
$\Rightarrow \exists\, y \in \mathbb{Z} : y^2 + 1 \equiv 0\ (p) \Rightarrow p|(y^2+1) = (y+i)(y-i) \in \mathbb{Z}[i]$
$\Rightarrow p$ ist kein Primelement von $\mathbb{Z}[i]$, denn $\frac{y}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$ $\triangle$

Sei p kein Primelement in $\mathbb{Z}[i] \Rightarrow p = \alpha \cdot \beta \in \mathbb{Z}[i]$ mit $\alpha, \beta \notin \mathbb{Z}[i]^*$ Es gilt:
$N(p) = p^2 = N(\alpha)N(\beta) \Rightarrow p = N(\alpha)$ mit $\alpha = a + ib$
$\Rightarrow N(\alpha) = a^2 + b^2 \Rightarrow p \equiv 1, 2\ (4)$
$\Rightarrow p = 2 \vee p \equiv 1\ (4)$
$2 = (1+i)(1-i)$ Es gilt: $1 - i = -i(1+i)$
Sei $p \equiv 3\ (4) \Rightarrow p$ ist Primelement.
Sei $p \equiv 1\ (4) \Rightarrow p$ ist kein Primelement und $\alpha = a + ib$ mit $p = \alpha \cdot \beta$ und $p = a^2 + b^2$ □

Definition 5.3 *(Summen und Produkte von Idealen)*
Sei R ein Ring und $I, J \trianglelefteq R$ Ideale. Wir definieren genau wie in Algebra I

- $I \cdot J := \{ \sum_{i=1}^{n} x_i \cdot y_i \,|\, x_i \in I \wedge y_i \in J \wedge n \in \mathbb{N} \}$
- $I + J := (I, J) = \{ xy \,|\, x_i \in I \wedge y_i \in J \}$
- $I^n := I \cdot \ldots \cdot I$ *n-mal*
- I, J *heißen Teilerfremd, falls* $I + J = R$

Beispiel 9 $R = \mathbb{Z}$
$(a) \cdot (b) = (ab)$, $(a) + (b) = (\, ggT(a,b)\,)$, $(a) \cap (b) = (\, kgV(a,b)\,)$

Anmerkung Sei R ein Ring mit Idealen $I, J \trianglelefteq R$, dann gilt: $I \cap J \supseteq I \cdot J$

Bemerkung 5.4 *Sei R ein Ring mit Idealen $I, J, P, Q \trianglelefteq R$ dann gelten:*
(a) Falls $I + J = R$ gilt, folgt $I \cdot J = I \cap J$
(b) P, Q prim mit P ist Maximalideal und $Q \subsetneq P$, dann sind P, Q Teilerfremd.

Beweis. Zunächst zu Teil (b). Es gilt $P \subsetneq P + Q$. Da P ein Maximalideal ist, folgt: $P + Q = R$
Für den Teil (a) ist die Inklusion „$\subseteq$“ trivial, die andere Inklusion ist auch klar, denn aus $I + J = R$ folgt, dass es ein $x \in I$ und ein $y \in J$ gibt, so dass $1 = x + y$. Sei nun $z \in I \cap J$ dann gilt $z = z \cdot 1 = zx + zy \in I \cdot J$ □

Definition 5.5 *(eindeutige Idealfaktorisierungseigenschaft)*
Sei R ein Ring, dann hat R die eindeutige Idealfaktorisierungseigenschaft (EIFE), falls sich jedes Ideal I mit $(o) \neq I \lhd R$ auf bis auf die Reihenfolge eindeutige Art als Produkt von Primidealen P_i schreiben lässt. (D.h. $I = P_1 \cdot \ldots \cdot P_n$)

Beispiel 10 *(Algebra I)*
Jeder Hauptidealring R hat die eindeutige Idealfaktorisierungseigenschaft, denn sei $a \in R$, dann gilt

$$a = \varepsilon \cdot \prod_{i=1}^{n} p_i^{e_i} \text{ mit } \varepsilon \in R^* \text{ und } p_i \text{ paarweise nicht assozierte Primelemente}$$

Daraus folgt unmittelbar eine bis auf Reihenfolge Eindeutige Zerlegung:

$$(a) = (p_1)^{e_1} \cdot \ldots \cdot (p_n)^{e_n}$$

Satz 5.6 *Sei A ein Hauptidealring mit $K := \mathrm{Quot}(A)$. Sei L eine endliche separable Erweiterung von K, dann hat A_L die eindeutige Idealfaktorisierungseigenschaft.*

Diesen wichtigen Satz können wir noch nicht beweisen, aber wir werden im Folgenden zeigen, dass ein kleinerer Ring als A_L nicht die eindeutige Idealfaktorisierungseigenschaft besitzt.

Beispiel 11 *Der Ring $\mathbb{Z}[\sqrt{5}]$ hat die eindeutige Idealfaktorisierungseigenschaft nicht.*
Bezeichne $L := \mathbb{Q}(\sqrt{5})$, dann gilt:

$$\mathbb{Z}[\sqrt{5}] \subsetneq \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \mathbb{Z}_L$$

Aus Gründen der Lesbarkeit führen wir die Notation g wie goldener Schnitt *für $\frac{1+\sqrt{5}}{2}$ ein. Wir wollen nun ein Gegenbeispiel konstruieren. Wir suchen also ein Ideal, welches sich nicht bis auf die Reihenfolge eindeutig in Primideale zerlegen lässt.*

Behauptung 1 *Sei $Q := 2 \cdot \mathbb{Z}[g]$, dann ist Q Maximalideal.*

Beweis. *Das Minimalpolynom von g ist $X^2 - X - 1$. Betrachte:*

$$\begin{aligned}
\mathbb{Z}[g]/Q &\cong \left(\mathbb{Z}[X]/(X^2 - X - 1)\right)/(2) \cong \mathbb{Z}[X]/(X^2 - X - 1, 2) \\
&\cong \left(\mathbb{Z}[X]/(2)\right)/(X^2 - X - 1) \cong \mathbb{F}_2[X]/(X^2 - X - 1) \\
&\cong \mathbb{F}_2[X]/(X^2 + X + 1) \overset{g \bmod (2)\, irred.}{\cong} \mathbb{F}_4 \\
&\Rightarrow Q \text{ ist Maximalideal}
\end{aligned}$$

□

Behauptung 2 *$g := \frac{1+\sqrt{5}}{2}$ ist eine Einheit, denn $\frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = -1$ also ist $g^{-1} = \frac{\sqrt{5}-1}{2}$.*
Es gilt: $2 \cdot g \in Q \Rightarrow \sqrt{5} - 1 \in Q$.

Behauptung 3 *$P := Q \cap \mathbb{Z}[\sqrt{5}]$ ist Primideal von $\mathbb{Z}[\sqrt{5}]$.*

Beweis. *Betrachte: $\varphi : \mathbb{Z}[\sqrt{5}] \hookrightarrow \mathbb{Z}[g] \to \mathbb{Z}[g]/Q \cong \mathbb{F}_4$ Es gilt: $P = \mathrm{Ker}(\varphi)$, daher gilt nach dem Homomorphiegesetz:*

$$\mathbb{Z}[\sqrt{5}]/P \cong \mathrm{Im}(\varphi) \subseteq \mathbb{F}_4$$

und somit $\mathrm{Im}(\varphi) = \mathbb{F}_4 \vee \mathrm{Im}(\varphi) = \mathbb{F}_2$. Damit haben wir gezeigt, dass P Maximalideal ist, also ist P ein Primideal. □

Behauptung 4 *$P = (2, \sqrt{5} - 1) \trianglelefteq \mathbb{Z}[\sqrt{5}]$.*

Beweis. *Betrachte den folgenden surjektiven Ringhomomorphismus:*

$$\begin{aligned}
\mathbb{Z}[\sqrt{5}]/(2, \sqrt{5} - 1) &\longrightarrow \mathbb{F}_2 \\
\sqrt{5} &\mapsto 1
\end{aligned}$$

Dieser ist aber auch injektiv, denn:

$$\begin{aligned}
\mathbb{Z}[\sqrt{5}]/(2, \sqrt{5}-1) &= \Big(\mathbb{Z}[X]/(X^2-5)\Big)/(2, x-1) \cong \mathbb{Z}[X]/(2, X^2-5, X-1) \\
&\cong \mathbb{F}_2[X]/(X-1, X^2-5) = \mathbb{F}_2[X]/(X+1, (X+1)^2) \\
&\cong \mathbb{F}_2[X]/(x-1) \cong \mathbb{F}_2
\end{aligned}$$

□

Behauptung 5 *Sei $I := 2 \cdot \mathbb{Z}[\sqrt{5}]$, dann gilt: $I \subsetneq P$*

Beweis.

$$\mathbb{Z}[\sqrt{5}]/I = \mathbb{F}_2[X]/(x^2-5) = \mathbb{F}_2[X]/((x+1)^2) \neq \mathbb{F}_2 \cong \mathbb{Z}[\sqrt{5}]/P$$

Behauptung 6 $P^2 = I \cdot P$

Beweis.

$$\begin{aligned}
P^2 &= (2, \sqrt{5}-1) \cdot (2, \sqrt{5}-1) = (4, 2(\sqrt{5}-1), (\sqrt{5}-1)^2) \\
&= (4, 2(\sqrt{5}-1), 5+1-2\sqrt{5}) = (2) \cdot (2, \sqrt{5}-1) \\
&= I \cdot P
\end{aligned}$$

□

Das Ideal P^2 lässt sich also wie folgt faktorisieren: $I \cdot P = P^2 = P \cdot P$, wobei I und P Primideale sind. Habe $\mathbb{Z}[\sqrt{5}]$ nun die eindeutige Idealfaktorisierungseigenschaft, so folgte daraus $I = P$. Dies ist, wie gezeigt, nicht der Fall, also kann $\mathbb{Z}[\sqrt{5}]$ die eindeutige Idealfaktorisierungseigenschaft nicht besitzen.

Definition 5.7 *(Spur und Norm)*[1]
Sei L/K eine endliche Körperweiterung dann gilt: $[L:K] = [L:K]_S \cdot q$. Seien weiter $\alpha \in L$ und $\{\sigma_1, \dots, \sigma_n\} = \mathrm{Hom}_K(L, \bar{K})$. Wir definieren die Spur von α über L/K durch

$$\mathrm{Spur}_{L/K}(\alpha) := \mathrm{Sp}_{L/K}(\alpha) := q \cdot \sum_{i=1}^{n} \sigma_i(\alpha)$$

Und die Norm von α über L/K durch

$$\mathrm{Norm}_{L/K}(\alpha) := \mathrm{N}_{L/K}(\alpha) := \left(\prod_{i=1}^{n} \sigma_i(\alpha) \right)^q$$

Bemerkung 5.8 *Seien $M/L/K$ endliche Körpererweiterungen, dann gelten*

$$\mathrm{Sp}_{M/K} = \mathrm{Sp}_{L/K} \circ \mathrm{Sp}_{M/L} \quad \text{und} \quad \mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$$

[1] Vergleiche [L2] Seite 81, Definition 20.1

Beweis. Auf $\mathrm{Hom}_K(M, \bar{K})$ ist durch $\sigma \sim \tau :\Leftrightarrow \sigma_{|_L} = \tau_{|_L} (\Leftrightarrow (\tau^{-1} \circ \sigma)_{|_L} = id_L)$ eine Äquivalenzrelation definiert. Seien also $\sigma_1, \ldots, \sigma_n$ Repräsentanten der Äquivalenzklassen und numeriere $\{\tau_1, \ldots, \tau_m\} = \mathrm{Hom}_L(M, \bar{K})$, dann gilt:

$$\mathrm{Hom}_K(M, \bar{K}) = \{\, \sigma_i \cdot \tau_j \,|\, 1 \leq i \leq n \wedge 1 \leq j \leq m \,\}$$

Es gilt: $[L : K] = [L : K]_S \cdot q \wedge [M : L] = [M : L]_s \cdot r$. Sei nun $\alpha \in M$, dann gilt:

$$\begin{aligned} \mathrm{Sp}_{L/K}(\alpha) &= q \cdot r \sum_{i=1}^{n} \sum_{j=1}^{m} \sigma_i \circ \tau_j(\alpha) \\ &= q \cdot \sum_{i=1}^{n} \sigma_i \left(r \cdot \sum_{j=1}^{m} \tau_j(\alpha) \right) \\ &= \mathrm{Sp}_{L/K} \cdot \mathrm{Sp}_{M/L}(\alpha) \end{aligned}$$

Der Beweis für diese Eigenschaft der Norm folgt analog. □

Definition 5.9 *(Die Diskriminante)*
Sei L/K endlliche separable Körpererweiterung und $\mathfrak{B} := \{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L. Weiter numeriere $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \bar{K})$. Die Diskriminante der Basis $\mathfrak{B}$ ist definiert als

$$d(\mathfrak{B}) := \det\left((\sigma_i(\alpha_j))_{1 \leq i,j \leq n}\right)^2$$

Bemerkung 5.10 *Wir verwenden die Bezeichnungen aus Definition 5.9. Es gilt:*

$$d(\mathfrak{B}) = \det\left((\mathrm{Sp}_{L/K}(\alpha_i \cdot \alpha_j)_{1 \leq i,j \leq n}\right)$$

Beweis. Setze $M := \big(\sigma_i(\alpha_j)\big)_{1 \leq i,j \leq n}$ und betrachte

$$\begin{aligned} M^T \cdot M &= \left(\sum_{k=1}^{n} \sigma_k(\alpha_i) \cdot \sigma_k(\alpha_j) \right)_{1 \leq i,j \leq n} \\ &= \left(\sum_{k=1}^{n} \sigma_k(\alpha_i \cdot \alpha_j) \right)_{1 \leq i,j \leq n} \\ &= \big(\mathrm{Sp}_{L/K}(\alpha_i \cdot \alpha_j) \big)_{1 \leq i,j \leq n} \end{aligned}$$

Es gilt also:

$$d(\mathfrak{B}) = \det(M)^2 = \det(M^T \cdot M) = \det\left((\mathrm{Sp}_{L/K}(\alpha_i \cdot \alpha_j))_{1 \leq i,j \leq n}\right)$$

□

Sei L/K eine separable Körpererweiterung vom Grad n, dann wissen wir aus Algebra I, dass es ein $a \in L$ gibt, mit $K(a) = L$ und $\mathfrak{B} := \{1, a, a^2, \ldots, a^{n-1}\}$ ist eine K-Basis von L. Bezeichne $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \bar{K})$. Die Matrix $M \in \mathrm{Mat}_K(n, n)$ zu dieser Basis ist die Vandermonde-Matrix

$$V = \begin{pmatrix} \sigma_1(1) & \sigma_1(a) & \cdots & \sigma_1(a)^{n-1} \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(a) & \cdots & \sigma_n(a)^{n-1} \end{pmatrix}$$

Bemerkung 5.11 *Die Determinante der Vandermonde-Matrix ist*

$$\det(V) := \det \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{pmatrix} = \prod_{n \geq j > i \geq 1} (a_j - a_i)$$

□

Anmerkung Die Diskriminante von obigem $\mathfrak{B}$ ist also:

$$d(\mathfrak{B}) = \prod_{j>i} (\sigma_j(a) - \sigma_i(a))^2$$

Satz 5.12 *Sei L/K eine endlich separable Körpererweiterung vom Grad n. Die Bilinearform*

$$\begin{aligned} < \cdot, \cdot >: L \times L &\to K \\ (x, y) &\mapsto < x, y > := \mathrm{Sp}_{L/K}(x \cdot y) \end{aligned}$$

ist nicht ausgeartet. Ausserdem ist die Diskriminante $d(\mathfrak{B}) \neq 0$ für alle K-Basen $\mathfrak{B}$ von L.

Beweis. Sei $\mathfrak{B} := \{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L und $\tilde{M}$ die zu $< \cdot, \cdot >$ gehörige Gramsche-Matrix. D.h. $< x, y >= y^T \cdot \tilde{M} \cdot x$. Mit $x = \alpha_i$ und $y = \alpha_j$ gilt dann

$$y^T \, \tilde{M} \, x = \tilde{m}_{i,j} = \mathrm{Sp}_{L/K}(\alpha_i \, \alpha_j)$$

Behauptung 1 *Jede Bilinearform ist genau dann nicht ausgeartet, wenn die Determinante der Gramschen Matrix nicht Null ist.*

Diese Behauptung beweisen wir noch etwas allgemeiner in folgendem
Lemma *Sei $A \in \mathrm{Mat}_K(n, n)$ symmetrisch, genau dann ist A nicht ausgeartet, wenn* $\det(A) \neq 0$.

Beweis. „⇐“ Sei $x \in L$ derart, dass für alle $y \in L$ gilt: $y^T \, A \, x = 0$.
Wähle eine Basiswechselmatrix $C \in \mathrm{GL}_K(n)$ mit $x = C \cdot e_1$ wobei e_1 den ersten Einheitsvektor bezeichne, dann gilt für alle $y \in L$

$$y^T \, A \, x = y^T \, (AC) C^{-1} \, x = y^T \, (AC) \, e_1 = 0$$

Die 1. Spalte von (AC) besteht also nur aus Nullen, daher gilt: $\det(AC) = \det(A) \cdot \det(C) = 0$. Da $C \in \mathrm{GL}_K(n)$ ist, folgt $\det(A) = 0$.
„⇒“: Sei $\det(A) = 0$, dann hat A keinen vollen Rang, also gibt es invertierbare Matritzen
$C, C^{-1} \in \mathrm{GL}_K(n)$, so dass die 1. Spalte von $D = CAC$ nur aus Nullen besteht. Hieraus folgt aber schon die Ausgeartetheit von A, denn:

$$y^T \, A \, x = y^T C^{-1} D C x$$

Das *Lemma* ist also bewiesen. △
Wir wählen nun zunächst $\mathfrak{B}' := \{1, a, \ldots, a^{n-1}\}$ mit $K(a) = L$. Nach der Anmerkung vom Begin der Vorlesung ist die Determinante von $\tilde{M}$ nicht Null bezüglich $\mathfrak{B}'$, also ist die Spurform nicht ausgeartet. Die nicht Ausgeartetheit einer Bilinearform ist jedoch Basisunabhängig, also folgt die Behauptung. Insbesondere gilt für jede beliebige K-Basis $\mathfrak{B}$ von L:

$$d(\mathfrak{B}) = \det(\mathrm{Sp}_{L/K}(\alpha_i \alpha_j))_{i,j} \neq 0$$

□

Bemerkung 5.13 *Sei A ein ganz abgeschlossener Integritätsring mit $K := \mathrm{Quot}(A)$. Weiter sei L/K eine endliche separable Körpererweiterung und $B := A_L$ bezeichne den ganzen Abschluss von A in L. Für $x \in B$ gelten:*
(a) $\mathrm{Sp}_{L/K}(x) \in A$ *und* $\mathrm{N}_{L/K}(x) \in A$
(b) x ist genau dann eine Einheit von B, wenn $\mathrm{N}_{L/K}(x)$ eine Einheit von A ist.

Beweis. Zu (a) Nach Bemerkung 4.11 hat das Minimalpolynom f_x von x Koeffizienten in A. Weiter ist $\sigma(x)$ für alle $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ eine Nullstelle des Minimalpolynoms f_x also ist $\sigma(x) \in B$. Hieraus folgen nun die beiden Aussagen:

$$\begin{aligned} \mathrm{Sp}_{L/K}(x) &= \sum_{\sigma \in \mathrm{Hom}_K(L,\bar{K})} \sigma(x) \in B \cap K = A \\ \mathrm{N}_{L/K}(x) &= \prod_{\sigma \in \mathrm{Hom}_K(L,\bar{K})} \sigma(x) \in B \cap K = A \end{aligned}$$

Zu (b) Sei $x \in B^*$ dann gibt es ein $y \in B$ so dass $x \cdot y = 1$ gilt. Daher gilt

$$1 = \mathrm{N}_{L/K}(1) = \mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x) \cdot \mathrm{N}_{L/K}(y)$$

Sei nun $\mathrm{N}_{L/K}(x) \in A^*$ dann gibt es ein $a \in A$ so dass $a \cdot \mathrm{N}_{L/K}(x) = 1$ gilt. Daher gilt

$$a \cdot \left(\prod_{\sigma \neq id} \sigma(x) \right) \cdot x = 1 \Rightarrow x \in B^*$$

□

Bemerkung 5.14 *Zusätzlich zu den Voraussetzungen in 5.13 sei $\mathfrak{B} := \{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L und weiter bezeichne $d := d(\mathfrak{B})$ die Diskriminante von $\mathfrak{B}$. Dann gilt:*

$$dB \subseteq A\alpha_1 + \ldots + A\alpha_n$$

Beweis. Sei $\beta \in B := A_L \subseteq L$, dann lässt sich β darstellen als

$$\beta = \sum_{i=1}^{n} r_i \alpha_i$$

wobei alle r_i Elemente aus K sind. Nach Bemerkung 5.13 gilt dann

$$\begin{aligned} \mathrm{Sp}_{L/K}(\alpha_j \beta) &= \mathrm{Sp}_{L/K}\left(\alpha_j \left(\sum_{i=1}^{n} r_i \alpha_i \right) \right) \\ &= \sum_{i=1}^{n} r_i \, \mathrm{Sp}_{L/K}(\alpha_j \alpha_i) \qquad \in A \end{aligned}$$

Schreiben wir diese Gleichung in Matrixform auf, erhalten wir

$$\tilde{M} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} \mathrm{Sp}(\alpha_1\alpha_1) & & \mathrm{Sp}(\alpha_1\alpha_n) \\ & \ddots \quad \iddots & \\ & \iddots \quad \ddots & \\ \mathrm{Sp}(\alpha_1\alpha_n) & & \mathrm{Sp}(\alpha_n\alpha_n) \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$$

Sei $\tilde{M}^*$ die zu $\tilde{M}$ adjungierte Matrix, dann ist

$$\tilde{M}^* \cdot \begin{pmatrix} \mathrm{Sp}(\alpha_1\beta) \\ \vdots \\ \mathrm{Sp}(\alpha_n\beta) \end{pmatrix} = \tilde{M}^* \cdot \tilde{M} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \det(\tilde{M}) \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} d \cdot r_1 \\ \vdots \\ d \cdot r_n \end{pmatrix}$$

Wie wir an dieser Gleichung ablesen können gilt für alle $i = 1, \ldots, n$, dass die Elemente $d \cdot r_i$ bereits in A liegen. □

Definition 5.15 *(Ganzheitsbasis)*
Sei A ein ganz abgeschlossener Integritätsring mit Quotientenkörper $K := \mathrm{Quot}(A)$. Weiter sei L/K eine endliche separable Körpererweiterung und $B := A_L$ bezeichne den ganzen Abschluss von A in L. Ist B ein freier A-Modul vom Rang n, dann heißt $\Omega := \{\omega_1, \ldots, \omega_n\} \subseteq B$ eine Ganzheitsbasis von B/A, falls $B = A\omega_1 + \ldots + A\omega_n$ gilt.

Anmerkung Im Allgemeinen gibt es keine Ganzheitsbasen, da B im Allgemeinen kein freier A-Modul ist. Ist Ω eine Ganzheitsbasis, so bildet Ω auch eine K-Basis von L.

Satz 5.16 *Sei A ein Hauptidealring mit Quotientenkörper $K := \mathrm{Quot}(A)$. Weiter sei L/K eine endliche separable Körpererweiterung und $B := A_L$ bezeichne den ganzen Abschluss von A in L.*
Sei $M \subseteq L$ mit $M \neq \{0\}$ ein endlich erzeugter B-Modul, dann ist M ein freier A-Modul mit $\mathrm{rg}_A(M) = [L : K] = n$

Beweis. Sei $\mathfrak{B} := \{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L. Wir können ohne Einschränkung annehmen, dass alle $\alpha_i \in B$ sind, denn sonst multiplizieren wir alle Elemente aus $\mathfrak{B}$ mit dem Hauptnenner durch. Bezeichne $d := d(\mathfrak{B})$ die Diskriminante von $\mathfrak{B}$, dann gilt nach Bemerkung 5.14:

$$dB \subseteq A\alpha_1 + \ldots + A\alpha_n$$

Sei $E := \{\mu_1, \ldots, \mu_n\} \subseteq L$ ein Erzeugendensystem von M als B-Modul, dann gibt es ein $a \in A$ derart, dass für alle $i = 1, \ldots, n$ die Elemente $a\mu_i$ in B liegen, daher gilt $aM \subseteq B$. Betrachte

$$adM \subseteq dB \subseteq A\alpha_1 + \ldots + A\alpha_n \subseteq B$$

Es gilt: $A\alpha_1 + \ldots + A\alpha_n$ ist ein freier A-Modul, also ist adM als Untermodul eines freien A-Moduls selbst frei und $\mathrm{rg}_A(adM) = \mathrm{rg}_A(M) \leq n$. Sei nun $m \in M \backslash \{0\}$, dann betrachte

$$\begin{array}{rcl} \varphi : B & \to & M \\ b & \mapsto & bm \end{array}$$

φ ist injektiv, also folgt: $\mathrm{rg}_A(M) \geq \mathrm{rg}_A(B) = n$ □

Definition und Folgerung 5.17 *(Diskriminante der ganzen Zahlen)*
Seien K ein Zahlkörper (d.h. $[K : \mathbb{Q}] < \infty$) und $\mathfrak{O}_K = \mathbb{Z}_K$ der Ring der ganzen Zahlen von K. Dann hat $\mathfrak{O}_K$ eine Ganzheitsbasis Ω und die Diskriminante jeder Ganzheitsbasis ist gleich.
Wir nennen $d(\Omega) =: d(\mathfrak{O}_K)$ die Diskriminante der ganzen Zahlen von K.
Allgemeiner gilt: Jeder $\mathfrak{O}_K$-Untermodul M von K ist ein freier $\mathbb{Z}$-Modul mit $\mathrm{rg}(M) = [K : \mathbb{Q}]$ und die Diskriminante aller $\mathbb{Z}$-Basen von M ist gleich.

Beweis. Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealring, also gilt nach Satz 5.16, dass M ein freier $\mathbb{Z}$-Modul mit $\mathrm{rg}(M) = n = [K : \mathbb{Q}]$ ist. Seien $\mathfrak{A} := \{\alpha_1, \ldots, \alpha_n\}$ und $\mathfrak{B} := \{\beta_1, \ldots, \beta_n\}$ zwei $\mathbb{Z}$-Basen von M mit der zugehörigen Basiswechselmatrix $C \in \mathrm{GL}_{\mathbb{Z}}(n)$ D.h. insbesondere gilt:

$$\det(C \cdot C^{-1}) = 1 = \det(C) \cdot \det(C^{-1}) \Rightarrow \det(C) \in \mathbb{Z}^* \Rightarrow \det(C) \in \{\pm 1\}$$

Sei $\tilde{M} := (\mathrm{Sp}_{K/\mathbb{Q}}(\alpha_i \alpha_j))_{i,j}$ dann folgt $C^T \cdot \tilde{M} \cdot C = (\mathrm{Sp}_{K/\mathbb{Q}}(\beta_i \beta_j))_{i,j}$ Es gilt:

$$det(C^T \, \tilde{M} \, C) = \det(C)^2 \det(\tilde{M}) = \det(\tilde{M})$$

□

Folgerung 5.18 *Unter den Voraussetzungen aus Definition und Folgerung 5.17, mit zusätzlich $M_1 \subseteq M_2$ zwei endlich erzeugten $\mathfrak{O}_K$-Moduln von K, gilt:*

$$d(M_1) = d(M_2) \cdot (M_2 : M_1)^2$$

wobei $(M_2 : M_1) = \sharp \left({}^{M_2}\!/_{M_1} \right)$ der Gruppenindex abelscher Gruppen ist[2]*.*

Beweis. Übungsaufgabe.

6 Noethersche Ringe

Motivation In einem Hauptidealring R gilt: Jeder Untermodul eines endlich erzeugten R-Moduls ist selbst endlich erzeugt. $(*)$

Beispiel 12 *Sei K ein Körper und $R := K[X_1, X_2, X_3, \ldots]$ der Polynomring über K in unendlich vielen Variablen. Betrachte $M := R$ als R-Modul, dieser ist endlich erzeugt von 1_R. Jedoch ist $M \geq N := (X_1, X_2, X_3, \ldots)$ nicht endlich erzeugt.*

Das Beispiel zeigt, dass die Aussage $(*)$ etwas besonderes ist und im Allgemeinen nicht gilt.

Beispiel 13 *In $R := K[X_1, \ldots, X_n]$ dem Polynomring über K in endlich vielen Variablen gilt die Aussage $(*)$ nach dem Basissatz von Hilbert.*

Ringe in denen $(*)$ gilt heißen Noethersche Ringe nach Emmy Noether. Wir definieren sie wie folgt:

Definition 6.1 *(Noethersch, Artinsch)*
Sei R ein Ring und M ein R-Modul.

1. *M heißt Noethersch (bzw. Artinsch), falls jede nicht-leere Menge S von Untermoduln von M ein maximales (bzw. minimales) Element enthält.*
   Dabei heißt $N \in S$ maximal (bzw. minimal), falls
   $N \subseteq \tilde{N} \in S \Rightarrow N = \tilde{N}$ (bzw. $N \supseteq \tilde{N} \Rightarrow N = \tilde{N}$) gilt.

2. *R heißt Noethersch (bzw. Artinsch), falls R als R-Modul Noethersch (bzw. Artinsch) ist.*

[2] Vgl. [L2] Def. 2.4 - Seite 5

Bemerkung 6.2 *Sei R ein Ring und M ein R-Modul, dann sind äquivalent:*

(i) *M ist Noethersch (bzw. Artinsch)*

(ii) *Jede aufsteigende (bzw. absteigende) Kette von Untermoduln*
$N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$ *(bzw. $N_1 \supseteq N_2 \supseteq N_3 \supseteq \ldots$)*
wird stationär, d.h. es gibt ein $\hat{n}$, so dass für alle n, die größer sind als $\hat{n}$, die Gleichung $N_{\hat{n}} = N_n$ erfüllt ist.

Beweis. „(i) $\Rightarrow$ (ii)“
M ist nach Voraussetzung Noethersch und eine Aufsteigende Kette $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$ ist gegeben, setze $S := \{N_1, N_2, \ldots\}$. Dann hat S ein maximales Element. Bei diesem wird die Kette stationär.
„(ii) $\Rightarrow$ (i)“
Angenommen M sei nicht Noethersch und S eine nicht-leere Menge von M-Untermoduln N_i ohne maximales Element. Konstruiere eine unendliche Kette mit echten Inklusionen wie folgt:
Sei $N_1 \in S$ beliebig, da S nach Annahme kein maximales Element hat gibt es $N_2 \in S$ mit $N_1 \subset N_2$. N_2 ist nicht maximal, also gibt es $N_3 \in S$ mit $N_1 \subset N_2 \subset N_3$ ... und so weiter.
Dies ist ein Widerspruch zur Voraussetzung, dass Jede Kette abbricht!
Analog folgen die Beweise für Artinsch mit absteigenden Ketten. □

Beispiel 14 *(Für Noetersche / Artinsche Ringe)*

- *Körper sind sowohl Noethersch als auch Artinsch.*
- *Hauptidealringe sind Noethersch.*
- *$\mathbb{Z}$ ist nicht Artinsch, denn $(2) \supsetneqq (4) \supsetneqq (8) \ldots$*
- *Jede endliche abelsche Gruppe ist sowohl Noethersch als auch Artinsch als $\mathbb{Z}$-Modul.*
- *$K[X_1, X_2, \ldots]$ ist nicht Noethersch, denn $(X_1) \subsetneqq (X_1, X_2) \subsetneqq \ldots$*

Satz 6.3 *Sei R ein Ring und M sei ein R-Modul. Es sind äquivalent:*
(i) M ist Noethersch und (ii) Jeder Untermodul $N \leq M$ ist endlich erzeugt.

Beweis. „(i) $\Rightarrow$ (ii)“:
Angenommen N ist nicht endlich erzeugt, dann gibt es für $i \in \mathbb{N}$ Elemente $x_i \in N$, so dass

$$< x_1 >_R \subsetneqq < x_1, x_2 >_R \subsetneqq \ldots$$

Dann ist M aber nicht Noehtersch.
„(ii) $\Rightarrow$ (i)“:
Sei $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq \ldots$ eine aufsteigende Kette von Untermoduln von M. Definiere

$$N := \bigcup_{i=1}^{\infty} N_i \leq M$$

Dieser ist endlich erzeugt mit den Erzeugern $x_1, \ldots, x_m$. Es gibt ein $l \in \mathbb{N}$, so dass die $x_1, \ldots, x_m$ im zugehörigen Untermodul N_l liegen. Diese Kette ist also ab l stationär. □

Satz 6.4 *Sei R ein Ring und*

$$0 \to N \overset{\iota}{\hookrightarrow} M \overset{\pi}{\to} {}^{M}\!/_{N} \to 0$$

eine exakte Sequenz von R-Moduln. Es sind äquivalent:
(i) M Noethersch und (ii) sowohl N als auch ${}^{M}\!/_{N}$ sind Noethersch.

Beweis. „(i) $\Rightarrow$ (ii)“:
Sei S eine nicht-leere Menge von Untermoduln von N. Fasse die Elemente von S als Untermoduln von M auf. Da M nach Voraussetzung Noethersch ist, hat S ein maximales Element.
Sei $\bar{M}_1 \subseteq \bar{M}_2 \subseteq \ldots$ eine aufsteigende Kette von ${}^{M}\!/_{N}$ Untermoduln und bezeichne π die Projektionsabbildung von M nach ${}^{M}\!/_{N}$, dann ist

$$\pi^{-1}(\bar{M}_1) \subseteq \pi^{-1}(\bar{M}_2) \subseteq \ldots$$

eine aufsteigende Kette in M. Diese wird stationär, d.h. es gibt ein $n \in \mathbb{N}$, so dass für alle $i \in \mathbb{N}$ gilt: $\pi^{-1}(\bar{M}_{n+i}) = \pi^{-1}(\bar{M}_n)$ Daher folgt

$$\pi\left(\pi^{-1}(\bar{M}_{n+i})\right) = \bar{M}_{n+i} = \bar{M}_n = \pi\left(\pi^{-1}(\bar{M}_n)\right)$$

Zu „(ii) $\Rightarrow$ (i)“:
Sei $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ eine Kette in M. Betrachte $N \cap M_1 \subseteq N \cap M_2 \subseteq \ldots$ diese Kette wird stationär nach Voraussetzung. Betrachte weiter $M_1 + {}^{M}\!/_{N} \subseteq M_2 + {}^{M}\!/_{N} \subseteq \ldots$ auch diese Kette wird nach Voraussetzung stationär. Bezeichne n einen Index, ab dem beide Ketten stationär sind, dann gilt für alle $i \geq 0$

$$M_n + {}^{M}\!/_{N} = M_{n+i} + {}^{M}\!/_{N}$$

Mit den Isomorphiesatz folgt dann:

$$M_n/M_n \cap N \cong M_n + {}^{M}\!/_{N} = M_{n+i} + {}^{M}\!/_{N} \cong M_{n+i}/M_{n+i} \cap N = M_{n+i}/M_n \cap N$$

Weiter lässt sich nun folgern, dass

$$\left(M_{n+i}/M_n \cap N\right)\Big/\left(M_n/M_n \cap N\right) \cong M_{n+i}/M_n = 0$$

und mit $M_{n+i} = M_n$ folgt nun die Behauptung. □

Anmerkung Der soeben bewiesene Satz gilt auch für Artinsche Moduln.

Folgerung 6.5 *Sei R ein Ring und $M_1, \ldots M_n \leq N$ seien R-Moduln. Dann sind äquivalent:*
(i) $M_1, \ldots, M_n$ sind Noethersch und (ii) $\sum_{i=1}^{n} M_i$ ist Noethersch

Beweis. „(ii) $\Rightarrow$ (i)“:
Untermoduln Noeterscher Moduln sind selbst Noethersch nach Satz 6.4.
Zu „(i) $\Rightarrow$ (ii)“:
O.B.d.A. sei $n = 2$, dann betrachte die folgende exakte Sequenz:

$$0 \to M_1 \overset{\iota}{\to} M_1 + M_2 \overset{\pi}{\to} (M_1 + M_2)/M_1 \to 0$$

Es gilt:

$$(M_1 + M_2)/M_1 \cong M_2/M_1 \cap M_2$$

dieser ist Noethersch, da er ein Quotient von Noetherschen Moduln ist. Mit Satz 6.4 folgt dann direkt, dass auch $M_1 + M_2$ Noethersch ist. □

Folgerung 6.6 *Sei R ein Noetherscher Ring und M ein endlich erzeugter R-Modul, dann ist M Noethersch.*

Beweis. Sei $\{x_1, \dots, x_n\} =: E$ ein Erzeugendensystem von M, dann können wir M darstellen als

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

Da Rx_i als Quotient von R Noethersch ist folgt die Aussage aus Folgerung 6.5. □

Anmerkung Die Folgerungen 6.5 und 6.6 gelten ebenso für Artinsche Moduln.

Satz 6.7 *Sei R ein Noetherscher Ring, dann ist $R[X]$ Noethersch.*

Dieser Satz Beweist den Induktionsanfang von Hilberts Basissatz, den wir gleich mit beweisen wollen.

Folgerung 6.8 *(Hilberts Basissatz)*
Sei R ein Noetherscher Ring, dann ist $R[X_1, \dots, X_n]$ Noethersch. Insbesondere sind alle Ideale $\mathfrak{a} \trianglelefteq R[X_1, \dots, X_n]$ endlich erzeugt.

Beweis. Sei $I \trianglelefteq R[X]$ ein Ideal. Wir müssen zeigen, dass I endlich erzeugt ist.
Dazu definieren wir:

$$\begin{aligned} A_0 &:= \{a_0 \,|\, a_0 \in I \wedge a_o \in R\} = I \cap R \trianglelefteq R \\ A_1 &:= \{a_1 \,|\, a_1 X + b_0 \in I \wedge a_1 \in R\} \trianglelefteq R \\ A_2 &:= \{a_2 \,|\, a_2 X^2 + X b_1 + b_0 \in I \wedge a_2 \in R\} \trianglelefteq R \\ &\vdots \end{aligned}$$

Es gilt: $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$. Da R Noethersch ist, wird diese Kette Stationär, also gibt es ein $d \in \mathbb{N}$ derart, dass für alle $i \geq 0$ die Gleichung $A_{d+i} = A_d$ gilt. Da für $0 \leq m \leq d$ die Ideale A_m als Ideale eines Noetherschen Rings endlich erzeugt sind, können wir A_m schreiben als $(a_{m,1}, \dots, a_{m,e_m})$. Für jedes dieser $a_{m,i}$ gibt es

$$f_{m,i}(X) = a_{m,i} X^m + \sum_{i=0}^{m-1} b_j X^j \in I$$

Behauptung 1 $I = (f_{m,i}(X))_{\substack{0 \leq m \leq d \\ 1 \leq i \leq e_m}}$

Wir beweisen für $g(X) \in I$, dass g von den $f_{m,i}$ erzeugt wird, per Induktion über den Grad r von g.
1. Fall ($r \geq d$):
Nun ist $a_r \in A_r = A_d$ daher gibt es Elemente $s_i \in R$ so dass $a_r = \sum_{i=1}^{e_d} s_i \, a_{d_i}$ gilt. Betrachte:

$$h(X) := g(X) - \sum_{i=1}^{e_d} s_i \, f_{d,i}(X) \cdot X^{r-d} \;\in I$$

Es gilt: $\deg(h) < \deg(g) = r$. Diesen Vorgang wiederholen wir solange, bis $\deg(h) < d$ ist, dann gehe zum

2. Fall ($r < d$):
Es gilt: $a_r \in A_r \subseteq A_d$ also gibt es Elemente $s_i \in R$ so dass $a_r = \sum_{i=1}^{e_r} s_i\, a_{d_i}$ gilt. Betrachte nun

$$h(X) := g(X) - \sum_{i=1}^{e_r} s_i\, f_{r,i}(X) \ \in I$$

Es gilt $\deg(h) < r$. Schlussendlich kommen wir zum
3. Fall ($r = 0$), dies ist trivial. □

Satz 6.9 *Sei A ein ganz abgeschlossener Noethersche Integritätsring und bezeichne $K := \mathrm{Quot}(A)$ den Quozientenkörper von A. Weiter sei L/K eine endlich separable Körpererweiterung und $B := A_L$ bezeichne den ganzen Abschluss von A in L. Es gilt: B ist Noethersch und B ist endlich erzeugter A-Modul*

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\} =: \mathfrak{B}$ eine K-Basis von L und $d := d(\mathfrak{B})$ die Diskriminante von $\mathfrak{B}$. Es gilt:

$$\begin{aligned} dB \subseteq \ & A\alpha_1 + \ldots + A\alpha_n \ \subseteq L \\ \Rightarrow\ B \subseteq \ & A\tfrac{\alpha_1}{d} + \ldots + A\tfrac{\alpha_n}{d} \ \subseteq L \end{aligned}$$

Weiter ist $A\frac{\alpha_1}{d} + \ldots + A\frac{\alpha_n}{d}$ Noetherscher A-Modul, daher folgt mit den Sätzen 6.4 und 6.5 sofort, dass B ein endlich erzeugter Noetherscher A-Modul ist. □

7 Ringe der Dimension 1

Definition 7.1 *(Primidealketten, (Krull-)Dimension)*
Sei R ein Ring. Eine Primidealkette in R der Länge n ist eine aufsteigende Kette von $n+1$ Primidealen mit echten Inklusionen:

$$P_n \subsetneq P_{n-1} \subsetneq \ldots \subsetneq P_1 \subsetneq P_0$$

Sei $P \lhd R$ ein Primideal. Die Höhe von P ist definiert als

$$\mathrm{h}(P) := \sup\{ \text{ Länge der Primidealketten mit } P_0 = P \}$$

Die (Krull-)Dimension eines Rings R definieren wir als

$$\dim(R) := \sup\{ \mathrm{h}(P) \mid P\,(prim) \ \lhd R \}$$

Beispiel 15 *(Krulldimensionen)*

- *Sei K ein Körper, dann ist $(0) \lhd K$ das einzige Primideal, also ist $\dim(K) = 0$.*
- *Sei R ein Hauptidealring, aber kein Körper, dann ist $\dim(R) = 1$, denn in Satz 6.4 der Algebra I haben wir gezeigt, dass jedes Primideal $\mathfrak{p} \neq (0)$ ein Maximalideal ist.*
- *Sei K ein Körper und $R := K[X_1, \ldots, X_n]$, dann gilt:*
  $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$, also ist $\dim(R) \geq n$.
  mit dem Noetherschen Maximalisierungssatz lässt sich hier sogar Gleichheit zeigen.

Bemerkung 7.2 *Sei R ein faktorieller Ring und $P \lhd R$ ein Primideal mit $(0) \neq P$, dann sind äquivalent: (i) P ist ein Hauptideal und (ii) Die Höhe von P ist* 1

Beweis. „(ii) $\Rightarrow$ (i)“
Unsere Voraussetzung ist $\mathrm{h}(P) = 1$. Sei $x \in P \backslash \{0\}$, dann ist

$$x = \prod_{i=1}^{n} p_i^{e_i} \quad \text{mit } p_i \, (prim) \in R$$

P ist Primideal und $x \in P$ daher gibt es ein p_i mit $p_i \in P$.
Betrachte die folgenden Inklusionen: $(0) \subsetneqq (p_i) \subsetneqq P$ Da $\mathrm{h}(P) = 1$ ist, gilt $(p_i) = P$
Zu (i) „$\Rightarrow$“ (ii)
Nach Voraussetzung gilt: $P = (p)$. Sei $(0) \subsetneqq Q \subsetneqq (p)$ mit $Q \lhd R$ ein Primideal. Ohne Einschränkung sei $\mathrm{h}(Q) = 1$ dann folgt aus der Implikation von (ii) nach (i), dass $Q = (q) \subseteq (p)$ mit $q \in (p)$ ist, also gilt $q = p \cdot r$ mit $r \in Rp$ und somit liegt $pr \in (q)$ da (q) ein Primideal ist. Also ist entweder $p \in (q)$, dann gilt $(p) = (q)$, oder $r \in (q)$. Angenommen $r \in (q)$, dann gilt

$$\begin{aligned} r &= qs \qquad s \in R \\ \Rightarrow q &= pr = qps \\ \Rightarrow 0 &= q(1 - ps) \\ \Rightarrow 1 &= ps \end{aligned}$$

Also ist $p \in R^*$, dies ist jedoch ein Widerspruch, da p ein Primelement von R ist. □

Erinnerung Aus Algebra I wissen wir, das Hauptidealringe faktorielle Ringe sind[3].

Satz 7.3 *Sei R ein faktorieller, Noetherscher Ring. Es sind äquivalent:*
(i) R ist Hauptidealring, aber kein Körper und (ii) Die (Krull-)Dimension von R ist 1

Beweis: „(i) $\Rightarrow$ (ii)“
Algebra I[4]
„(ii) $\Rightarrow$ (i)“
Sei $I = (a_1, \ldots, a_n) \lhd R$ Wir beweisen die Behauptung nun induktiv über n. Hierbei ist der Induktionsanfang für $(n = 1)$ trivial. Betrachte nun $(n > 1)$:
Sei zunächst $\mathbb{P}$ ein Vertretersystem der Primelemente von R bis auf Assoziertheit, dann faktorisiere die Erzeuger von I:

$$a_1 = \varepsilon_1 \cdot \prod_{p \in \mathbb{P}} p^{e_p} \text{ und } a_2 = \varepsilon_2 \cdot \prod_{p \in \mathbb{P}} p^{f_p} \quad \text{mit } \varepsilon_1, \varepsilon_2 \in R^*$$

$$\text{Sei nun } c := \mathrm{ggT}(a_1, a_2) = \prod_{p \in \mathbb{P}} p^{\min\{e_p, f_p\}}$$

dann definiere $d_1 := \frac{a_1}{c}$, $d_2 := \frac{a_2}{c}$. Es gilt $(d_1, d_2) = (1) = R$, denn sonst gäbe es ein Maximalideal P mit $(d_1, d_2) \subseteq P$. Mit Bemerkung 7.2 gilt dann aber $P = (p)$, also teilt p die Elemente d_1 und d_2. Dies ist ein Widerspruch, denn wir haben bereits alle gemeinsamen Faktoren von $a_1,\ a_2$ herausgeteilt.

[3] [L2] Seite 23 - Korollar 7.8
[4] [L2] Seite 19 - Bemerkung 6.4

Es gilt: $1 = r_1 d_1 + r_2 d_2$ mit $r_1,\ r_2 \in R$, multipliziere die Gleichung mit c und erhalte:

$$c = r_1\, c\, d_1 + r_2\, c\, d_2 = r_1 a_1 + r_2 a_2 \in (a_1, a_2)$$

Folglich gilt $(c) \subseteq (a_1, a_2)$, wir erinnern uns an die Definition $c := \mathrm{ggT}(a_1, a_2)$ also gilt die Inklusion $(a_1, a_2) \subseteq (c)$. Da wir nun beide Inklusionen haben folgt die Gleichheit □

Bemerkung 7.4 *Sei $\varphi : A \to B$ ein Ring-Homomorphismus und $P \lhd B$ ein Primideal in B. Dann ist $\varphi^{-1}(P) \lhd A$ ein Primideal in A.*

Beweis.

$$A/\varphi^{-1}(P) \hookrightarrow B/P$$

ist ein injektiver Ring-Homomorphismus und B/P ist ein Integritätsbereich also ist auch $A/\varphi^{-1}(P)$ ein Integritätsbereich. Dann ist $\varphi^{-1}(P)$ ein Primideal. □

Definition und Bemerkung 7.5 *($\mathfrak{p}$ unter P)*
Sei $A \subseteq B$ eine Ringerweiterung. $A \cap P$ ist ein Primideal, falls $P \lhd B$ ein Primideal ist. Ist $P \lhd B$ ein Primideal und bezeichne $\mathfrak{p} := A \cap P$, dann sagen wir, dass P über $\mathfrak{p}$ liegt, bzw. dass $\mathfrak{p}$ unter P liegt. Notation: $P|\mathfrak{p}$. □

Satz 7.6 *Seien $A \subseteq B$ Integritätsringe und B/A eine ganze Ringerweiterung, dann gelten:*

1. *A ist genau dann ein Körper, wenn B ein Körper ist.*
2. *Seien $\mathfrak{b} \lhd B$ und $\mathfrak{a} := A \cap \mathfrak{b}$, dann ist die Erweiterung $B/\mathfrak{b} \subseteq A/\mathfrak{a}$ ganz.*
3. *$P \lhd B$ sei ein Primideal und $\mathfrak{p} := P \cap A$, genau dann ist P ein Maximalideal, wenn $\mathfrak{p}$ ein Maximalideal ist.*

Beweis. Übung.

Bemerkung 7.7 *Sei $A \subseteq B$ eine ganze Ringerweiterung.*

(a) *Sei $\mathfrak{b} \lhd B$ ein Ideal mit $x \in \mathfrak{b}$ ein Nicht-Nullteiler, dann ist $\mathfrak{a} := \mathfrak{b} \cap A \neq (0)$*

(b) *Seien $P_1 \subsetneq P_2 \lhd B$ Primideale. Dann sind $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \lhd A$ Primideale mit $\mathfrak{p}_i := P_i \cap A$*

Beweis. Zu (a):
Es gilt: x ist ganz über A, also gibt es $a_i \in A$ so dass

$$0 = \sum_{i=0}^{n} x^i a_i$$

Da x kein Nullteiler ist, gibt es ein i, so dass $a_i \neq 0$, denn sonst gelte $0 = x^n$ d.h. x ist nilpotent, also Insbesondere Nullteiler. Sei nun j der kleinste Index mit $a_j \neq 0$, dann ist

$$0 \;=\; x^n + a_{n-1}x^{n-1} + \ldots + a_{j+1}x^{j+1} + a_j x^j \;=\; x^j(x^{n-j} + a_{n+1}x^{n-1-j} + \ldots + a_{j+1}x + a_j)$$

Da x kein Nullteiler ist, ist insbesondere x^j kein Nullteiler, also folgt

$$x^{n-j} + a_{n+1}x^{n-1-j} + \ldots + a_{j+1}x + a_j \;=\; 0$$

Damit gilt:

$$-(x^{n-j} + a_{n+1}x^{n-1-j} + \ldots + a_{j+1}x + a_j) = a_j \in A \cap \mathfrak{b} = \mathfrak{a} \neq (0)$$

Zu (b):
Betrachte

$$A/\mathfrak{p}_1 \hookrightarrow B/P_1$$

Dies ist eine ganze Ringerweiterung. Nach Satz 7.6 Teil (b) ist P_2/P_1 ein Primideal in B/P_1, denn

$$B/P_1/P_2/P_1 \cong B/P_2$$

Angenommen es gelte $\mathfrak{p}_1 = \mathfrak{p}_2$, dann ist $A/\mathfrak{p}_1 \cap P_2/P_1 = (0)$. Nach (a) gilt dann aber $P_2/P_1 = (0)$ denn sonst enthielte P_2/P_1 einen Nicht-Nullteiler, da B/P_1 ein Integritätsbereich ist.
Dies ist aber ein Widerspruch zur Voraussetzung, dass $P_1 \subsetneqq P_2$ gilt. □

Anmerkung Sei B/A eine ganze Ringerweiterung, dann gilt: $\dim(A) \geq \dim(B)$, denn nach Teil (b) der soeben bewiesenen Bemerkung ist die Kette

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n$$

mit $\mathfrak{p}_i = P_i \cap A$ genauso lang, wie die in B vorgegebene Kette

$$P_0 \subsetneqq P_1 \subsetneqq P_2 \subsetneqq \ldots \subsetneqq P_n$$

Erinnerung (Lokalisierung[5])
Sei R ein Ring und $S \subset R$ eine multiplikativ abgeschlossenne Teilmenge, d.h. $1 \in S$ und $0 \notin S$ sowie für alle $s, t \in S$ gilt $s \cdot t \in S$. Auf $R \times S$ definiert man wie folgt eine Äquivalenzrelation:

$$(r, s) \sim (r', s') \Leftrightarrow \exists\, a \in S : a(rs' - r's) = 0$$

Wir bezeichnen die Äquivalenzklassen mit $\frac{r}{s}$, und die Menge der Äquivalenzklassen mit $S^{-1}R$. Es gilt: $S^{-1}R$ ist ein Ring bezüglich

$$\begin{aligned} + : \frac{r}{s} + \frac{r'}{s'} &:= \frac{rs' + r's}{s's} \\ \cdot : \frac{r}{s} \cdot \frac{r'}{s'} &:= \frac{rr'}{ss'} \end{aligned}$$

Beispiel 16 *(Lokalisierung)*

- *Sei R ein Integritätsbereich, dann ist*
  $S := R\backslash\{0\}$ *multiplikativ abgeschlossen und* $S^{-1}R = \mathrm{Quot}(R)$
- *Sei R ein Ring und $\mathfrak{p} \lhd R$ Primideal. Es gilt: $R\backslash\mathfrak{p}$ ist multiplikativ abgeschlossen und der Ring $S^{-1}R =: R_{\mathfrak{p}}$ heißt Lokalisierung von R bei $\mathfrak{p}$*
  Insbesondere ist das erste Beispiel ein Spezialfall des zweiten mit $\mathrm{Quot}(R) = R_{(0)}$.

[5] [L2] Seite 18 - Satz 5.8

Satz 7.8 *Sei R ein Ring und $S \subset R$ multiplikativ abgeschlossen. Die Abbildung*

$$\begin{array}{rcl} \varphi : R & \to & S^{-1}R \\ r & \mapsto & \frac{r}{1} \end{array}$$

liefert eine Bijektion wie folgt:

$$\begin{array}{rcl} \{\, P \lhd R \,|\, P(prim) \,\wedge\, P \cap S = \varnothing \,\} & \rightleftarrows & \{\mathfrak{P} \lhd S^{-1}R \,|\, \mathfrak{P}(prim)\,\} \\ P & \to & S^{-1}P \\ \varphi^{-1}(\mathfrak{P}) & \leftarrow & \mathfrak{P} \end{array}$$

Beweis. Zur Vereinfachung teilen wir den Beweis in vier Schritte auf:

Behauptung 1 *$S^{-1}P$ ist ein Primideal*

Beweis. Sei $\frac{r}{s} \cdot \frac{r'}{s'} \in S^{-1}P$ dann ist $\frac{rr'}{ss'} = \frac{x}{t}$ mit $x \in P$ und $t \in S$. Weiter gibt es ein $a \in S$ mit $atrr' = ass'x \in P$, also $at \in P$ oder $r \in P$ oder $r' \in P$. Die Annahme, dass at in P enthalten sei ist aber widersprüchlich zu $S \cap P = \varnothing$, wir können also folgern, dass $\frac{r}{s} \in S^{-1}P$ oder $\frac{r'}{s'} \in S^{-1}P$ △

Behauptung 2 *Die Abbildung $P \to S^{-1}P$ ist injektiv*

Beweis. Sei $S^{-1}P = S^{-1}P'$ und $\frac{x}{s} \in S^{-1}P$ beliebig, dann gilt $\frac{x}{s} = \frac{x'}{s'}$ mit $x' \in P$ und damit gibt es ein $u \in S$ mit $us'x = usx' \in P'$. Mit der gleichen Begründung wie unter (1) folgt, dass x in P' enthalten ist. Es gilt $P' \subseteq P'$. Analog folgt $P' \subseteq P$. Da wir beide Inklusionen gezeigt haben sind P und P' gleich. △

Behauptung 3 $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$ *ist Wohldefiniert*

Beweis. Es ist zu zeigen, dass aus $\mathfrak{p} \lhd S^{-1}R$ ist Primideal folgt $\varphi^{-1}(\mathfrak{p}) \cap S = \varnothing$
Sei also $s \in S$. Wäre $s \in \varphi^{-1}(\mathfrak{p})$, dann wäre auch $\frac{s}{1} = \varphi(s) \subset \mathfrak{p}$. Daraus folgt: $\frac{1}{s} \cdot \frac{s}{1} = 1 \in \mathfrak{p}$. Also gilt $\mathfrak{p} = S^{-1}R$. Dies ist ein Widerspruch, denn $\mathfrak{p}$ ist ein Primideal. △

Behauptung 4 *$P \to S^{-1}P$ ist surjektiv*

Beweis. Betrachte: $\varphi(\varphi^{-1}(\mathfrak{p})) \subseteq \mathfrak{p}$ daher ist auch $S^{-1}(\varphi^{-1}(\mathfrak{p})) \subseteq \mathfrak{p}$ Sei $\frac{x}{s} \in \mathfrak{p}$, dann ist $s \cdot \frac{x}{s} = \frac{x}{1} \in \mathfrak{p}$, also $x \in \varphi^{-1}(\mathfrak{p})$ Damit gilt $\frac{x}{s} \in S^{-1}(\varphi^{-1}(\mathfrak{g}))$ also $S^{-1}(\varphi^{-1}(\mathfrak{p})) = \mathfrak{p}$ □

Definition und Folgerung 7.9 *(Lokaler Ring)*
Sei R ein Ring und $P \lhd R$ ein Primideal, dann ist R_p ein lokaler Ring, d.h. R_P enthält nur ein einziges Maximalideal, nämlich $S^{-1}P$, wobei $S = R \backslash P$.

Beweis. Sei $Q \lhd R$ ein Primideal. Der Schnitt von $Q \cap S$ ist genau dann leer, wenn $Q \subseteq P$ ist. Die Bijektion aus Satz 7.8 ist Inklusionserhaltend, in dem Sinne, dass aus $Q_1 \subseteq Q_2$ stets folgt $S^{-1}(Q_1) \subseteq S^{-1}(Q_2)$. Daher ist $S^{-1}P$ das einzige Maximalideal von $S^{-1}R = R_P$. □

Bemerkung 7.10 *Sei $A \subseteq B$ eine ganze Ringerweiterung und $S \subset A$ eine multiplikativ abgeschlossenne Teilmenge von A. Dann ist $S^{-1}A \subseteq S^{-1}B$ eine ganze Ringerweiterung.*

Beweis. Sei $\frac{x}{s} \in S^{-1}B$, d.h. $x \in B, s \in S$, dann gibt es $a_i \in A$ derart, dass gilt

$$\sum_{i=0}^{n} a_i x^i = 0$$

Betrachte nun die Äquivalenzklassen zu $\frac{1}{s^n}$:

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{x}{s^n} = 0$$

Es folgt, dass $\frac{x}{s}$ ganz über $S^{-1}A$ ist. □

Satz 7.11 *Sei $A \subseteq B$ eine ganze Ringerweiterung und $\mathfrak{p} \lhd A$ ein Primideal. Dann gibt es $P \lhd B$ Primideal mit $P \cap A = \mathfrak{p}$.*

Beweis. Definiere: $S := A \backslash \mathfrak{p}$, dann ist S multiplikativ abgeschlossen in A und B. Betrachte

$$\begin{array}{ccc} A & \overset{i}{\hookrightarrow} & B \\ \alpha \downarrow & & \downarrow \beta \\ S^{-1}A & \overset{j}{\hookrightarrow} & S^{-1}B \end{array}$$

mit $\alpha(a) = \frac{a}{1}$ und $\beta(b) = \frac{b}{1}$. Nach Voraussetzung ist $A \subseteq B$ ganz, also ist nach Bemerkung 7.10 auch $S^{-1}A \subseteq S^{-1}B$ ganz und das obige Diagramm kommutiert.
Sei $M \lhd S^{-1}B$ ein Maximalideal, dann gilt: $M \cap S^{-1}A = S^{-1}\mathfrak{p}$, denn nach 7.6 Teil (c) ist $M \cap S^{-1}A$ ein Maximalideal, aber $S^{-1}A = A_{\mathfrak{p}}$ hat nach Folgerung 7.9 nur ein einziges Maximnalideal, nämlich $S^{-1}\mathfrak{p}$. Setze $P := \beta^{-1}(M)$, dann ist P ein Maximalideal nach Bemerkung 7.4. Betrachte:

$$\begin{aligned} P \cap A &= \beta^{-1}(M) \cap A = i^{-1}(\beta^{-1}(M)) = (\beta \circ i)^{-1}(M) \\ &= (j \cap \alpha)^{-1}(M) = \alpha^{-1}(j^{-1}(M)) = \\ &= \alpha^{-1}(M \cap S^{-1}A) = \alpha^{-1}(S^{-1}\mathfrak{p}) \overset{(7.8)}{=} \mathfrak{p} \end{aligned}$$

□

Satz 7.12 *(*going up*)*
Sei $A \subseteq B$ eine ganze Ringerweiterung und $\mathfrak{p}^1 \subset \mathfrak{p}_2 \lhd A$ Primideale sowie $P_1 \lhd B$ mit $P_1 \cap A = \mathfrak{p}_1$. Dann gibt es ein Primideal $P_2 \lhd B$ mit $P_1 \subset P_2$ und $P_2 \cap A = \mathfrak{p}_2$.

Beweis. Die Ringerweiterung ${}^{A}\!/_{\mathfrak{p}_1} \subseteq {}^{B}\!/_{P_1}$ ist ganz. Betrachte das Primideal

$${}^{\mathfrak{p}_2}\!/_{\mathfrak{p}_1} \lhd {}^{A}\!/_{\mathfrak{p}_1}$$

Mit Satz 7.11 gibt es dann ein Primideal $\bar{P}_2 \lhd {}^{B}\!/_{P_1}$, so dass gilt

$$\bar{P}_2 \cap {}^{A}\!/_{\mathfrak{p}_1} = {}^{\mathfrak{p}_2}\!/_{\mathfrak{p}_1}$$

Sei $\pi : B \twoheadrightarrow {}^{B}\!/_{P_1}$ die natürliche Projektion, dann setze $P_2 := \pi^{-1}(\bar{P}_2) \lhd B$. Nach Bemerkung 7.4 ist P_2 ein Primideal in B. Betrachte nun:

$${}^{(P_2 \cap A)}\!/_{\mathfrak{p}_1} = {}^{P_2}\!/_{P_1} \cap {}^{A}\!/_{\mathfrak{p}_1} = {}^{\mathfrak{p}_2}\!/_{\mathfrak{p}_1}$$

Es folgt $P_2 \cap A = \mathfrak{p}_2$. □

Folgerung 7.13 *Sei $A \subseteq B$ eine ganze Ringerweiterung, dann gelten:*
(a) $\dim(A) = \dim(B)$
(b) Ist $P \lhd B$ Primideal, so gilt: $\mathrm{h}(P) = \dim(B_P) = \dim(A_{A\cap P}) = \mathrm{h}(A \cap P)$

Beweis. Zu (a):
Nach Bemerkung 7.7 ist $\dim(B) \leq \dim(A)$ somit bleibt nur die andere Ungleichung zu zeigen. Sei $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n$, die längste Primidealkette in A, dann wähle nach Satz 7.11 ein Primideal $P_0 \lhd B$ mit $P_0 \cap A = \mathfrak{p}_0$. Benutze nun mehrfach Satz 7.12 „going up“ und erhalte:

$$P_0 \subsetneqq P_1 \subsetneqq \ldots \subsetneqq P_n$$

B enthält also eine Primidealkette mit der gleichen Länge, wie die in A vorgegebene, daher folgt $\dim(B) \geq \dim(A)$.
Zu (b):
Es gilt: $A_{P\cap A} \subseteq B_P$ ist eine ganze Ringerweiterung, also gilt:

$$\dim(A_{P\cap A}) = \dim(B_P)$$

Sowohl B_P als auch $A_{P\cap A}$ sind lokale Ringe mit dem einzigen Maximalideal $S^{-1}P$ für $S := B\backslash P$ bzw. $S^{-1}(A \cap P)$ für $S := A\backslash(A \cap P)$. Mit Satz 7.8 folgt nun die Behauptung. □

Folgerung 7.14 *Sei A ein Noetherscher Integritätsring der Dimension 1 und bezeichne $K := \mathrm{Quot}(A)$ seinen Quotientenkörper. Weiter sei L/K eine endlich separable Körpererweiterung. Es gilt:*
A_L ist ein ganz abgeschlossener Noetherscher Integritätsring der Dimension 1.
Insbesondere sind die Ringe der ganzen Zahlen von Zahlkörpern ganz abgeschlossene Integritätsringe der Dimension 1. □

Diese Folgerung führt uns zur Definition der Dedekind-Ringe:

Definition 7.15 *(Dedekind-Ringe)*
Ein Noetherscher ganz abgeschlossenner Integritätsring der Dimension 1 heißt ein Dedekind-Ring.

Beispiel 17 *(Dedekind-Ringe)*

- *ganze Zahlen von Zahlkörpern*
- *Der Koordinatenring einer nichtsingulären Kurve über einem Körper*

Satz 7.16 *Sei R ein Noetherscher Integritätsring der Dimension 1, dann sind äquivalent:*
(i) R ist ein Dedekind-Ring
(ii) R hat die Eindeutige Primideal Faktorisierung

Kapitel III

Ebene Kurven

8 Definition und Beispiele

Definition 8.1 *(affine Räume, Hyperflächen und ebene Kurven)*
Es sei K ein Körper und $n \in \mathbb{N}$, dann heißt

$$\mathbb{A}^n(K) := K^n$$

der affine n-Raum mit Koordinaten in K.
Sei $f \in K[X_1, \ldots, X_n]$, dann schreiben wir

$$f(\underline{X}) := F(X_1, \ldots, X_n) = \sum_{i_0,\ldots,i_n \geq 0} a_{i_0,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} =: \sum_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}}$$

und definieren den Grad von F als:

$$\deg(f) := max\,\{i_1 + \ldots + i_n \,|\, a_{i_1,\ldots,i_n}\}$$

Sei nun L/K eine Körpererweiterung, dann heißt

$$V_f(L) := \{\, (x_1, \ldots, x_n) \in \mathbb{A}^n(L) \,|\, f(x_1, \ldots, x_n) = 0 \,\}$$

affine Hyperfläche vom Grad $\deg(f)$ mit Koordinaten in L.
Im Spezialfall $n = 2$ heißt $V_f(L)$ ebene affine Kurve mit Koordinaten in L.

Beispiel 18 *($f(X,Y) = X^2 + Y^2 - 1 \ \in K[X,Y]$)*
Sei $L = K = \mathbb{R}$, dann ist f der Einheitskreis im $\mathbb{R}^2$. Sei nun $L = K = \bar{\mathbb{F}}_2$, dann gilt:

$$\begin{aligned}
(x,y) \in V_f(\bar{\mathbb{F}}_2) \quad &\Leftrightarrow \quad x^2 + y^2 - 1 = 0 \\
&\overset{char(K)=2}{\Longleftrightarrow} \quad (x + y + 1)^2 = 0 \\
&\Leftrightarrow \quad x + y + 1 = 0 \\
&\Leftrightarrow \quad (x,y) \in V_{x+y+1}(\bar{\mathbb{F}}_2)
\end{aligned}$$

Also ist f eine Gerade[1] *in $\bar{\mathbb{F}}_2^2$.*

[1] $f(X,Y) = aX + bY + c \in K[X,Y]$ heißt Gerade, falls $a \cdot b \neq 0$,

Beispiel 19 *($f(X,Y) = X^2 + Y^2 + 1$)*
Ist $K = L = \mathbb{R}$, dann ist $V_f(\mathbb{R}) = \varnothing$
Falls $L = \mathbb{C}$ so ist $V_f(\mathbb{C})$ ein Kreis vom Radius i ($i^2 = -1$)

Bemerkung 8.2 *Sei K ein algebraisch abgeschlossener Körper und $f(X,Y) \in K[X,Y]$ ein Polynom mit Grad $\deg(f) \geq 1$, dann gilt: $\sharp V_f(K) = \infty$.*

Beweis. Fasse f als Element in $(K[X])[Y]$ auf, d.h.

$$f(X,Y) = \sum_{i=1}^{n} a_i(X)Y^i \text{ mit } a_i(X) \in K[X]$$

1.Fall $(n = 0)$: Es gilt: $f(X,Y) = a_0(X)$, sei nun $x \in K$, derart, dass $a_0(x) = 0$, dann ist das Tupel $(x,y) \in V_f(K)$ für alle $y \in K$. Da K algebraisch abgeschlossen ist gilt $\sharp K = \infty$, also auch $\sharp V_f(K) = \infty$.
2.Fall $(n > 0)$: Diesmal gilt: $a_n(x) \neq 0$ für fast alle $x \in K$. Wähle nun zu jedem dieser x ein $y \in K$ derart, dass $a_n(x)y^n + \ldots + a_0(x) = 0$. Es folgt: $\sharp V_f(K) = \infty$. □

Beispiel 20 *($f(X,Y) = X^2 + Y^2 \in K[X,Y]$)*
Ist $(x,0) \in V_f(K)$, dann ist $x^2 = 0$ und also auch $x = 0$.
Sei $y \neq 0$ und $(x,y) \in V_f(K)$ es gilt:

$$\begin{aligned} & x^2 + y^2 = 0 \\ \Leftrightarrow \quad & x^2 = y^2 \\ \Leftrightarrow \quad & \left(\frac{x}{y}\right)^2 = -1 \end{aligned}$$

Aus $(x,y) \in V_f(K)$ folgt also, dass die Gleichung $X^2 + 1 = 0$ eine Lösung in K hat. Weiter gilt:

$$V_f(K) = \{\,(0,0)\,\} \leftrightarrow X^2 + 1 = 0$$

hat keine Lösung in K. Genauer: Sei $K = \mathbb{F}_p$ mit $p \equiv 3(4)$, dann gilt: $V_f(\mathbb{F}_p) = \{\,(0,0)\,\}$. Für $K = \mathbb{F}_2$ gilt. $V_f(\mathbb{F}_2) = \{\,(0,0),\,(1,1)\,\}$

Beispiel 21 *(affine elliptische Kurven)*
$f(X,Y) = Y^2 - g(X) \in K[X,Y]$ wobei $g(X) \in K[X]$ mit $\deg(g) = 3$ heißt affine elliptische Kurve, falls $\triangle(g) \neq 0$ Sei, für eine Primzahl p und $q := p^r$ definiere $K := \mathbb{F}_q$, dann gelten folgende Aussagen:
Hasse-Weil Schranke:

$$|\,\sharp V_f(\mathbb{F}_{q^n}) - q^n\,| \leq 2 \cdot \sqrt{q^n}$$

Zeta-Funktion:

$$Z(T) := \exp\left(\sum_{n=1}^{\infty}(\sharp V_f(\mathbb{F}_{q^n}) + 1) \cdot \frac{T^n}{n}\right) = \frac{1 - aT}{(1-T)(1-qT)}$$

mit $a := q - \sharp V_f(\mathbb{F}_q)$.

9 Koordinatenringe und die Zariski-Topologie

Definition 9.1 *(affine Menge)*
Sei K ein Körper und $S \subseteq K[X_1, \dots, X_n]$ eine Teilmenge. Weiter sei L/K eine Körpererweiterung.

$$V_S(L) := \{ (x_1, \dots, x_n) \in \mathbb{A}^n(L) \mid f(x_1, \dots, x_n) = 0 \ \forall f \in S \}$$

heißt affine (algebraische) Menge mit Koordinaten in L.

Bemerkung 9.2 *Sei L/K eine Körpererweiterung und bezeichne $\underline{X} := X_1, \dots, X_n$ dann gelten:*

(a) *Sei $S \in K[\underline{X}]$ eine Teilmenge und $A := (S) \trianglelefteq K[\underline{X}]$, dann gilt: $V_S(L) = V_A(L)$.*

(b) *Seien $A, B \trianglelefteq K[\underline{X}]$ mit $A \subseteq B$, dann gilt: $V_B(L) \subseteq V_A(L)$.*

(c) *Seien für $i \in I$ $A_i \triangleleft K[\underline{X}]$, dann ist $V_{\bigcup\limits_{i\in I} A_i}(L) = \bigcap\limits_{i\in I} V_{A_i}(L)$*

(d) *Seien $A, B \triangleleft K[\underline{X}]$, dann gilt: $V_{AB}(L) = V_A(L) \cup V_B(L)$.*

(e) *Es gelten: $V_{(0)}(L) = \mathbb{A}^n(L)$ und $V_{(1)}(L) = \varnothing$.*

Beweis. Zu a):
Sei $f \in A$, dann können wir f darstellen als

$$f = \sum_{i=1}^{n} h_i g_i \text{ mit } g_i \in S,\ h_i \in K[\underline{\mathrm{X}}]$$

Für $\underline{\mathrm{x}} \in V_S(L)$ ist dann $g_i(\underline{\mathrm{x}}) = 0$ für alle $i = 1, \dots, n$ daher ist auch $f(\underline{\mathrm{x}}) = 0$ und somit muss $\underline{\mathrm{x}}$ ein Element aus $V_A(L)$ sein. Gilt nun $S \subseteq A$ so folgt sofort, dass $V_A(L) \subseteq V_S(L)$ gilt.
Der Teil (b) ist klar.Zum Beweis von (c)

$$\begin{aligned}
\text{Sei } \underline{\mathrm{x}} \in V_{\bigcup\limits_{i\in I} A_i}(L) \quad &\Leftrightarrow \quad \forall f \in \bigcup_{i\in I} A_i :\ f_i(\underline{\mathrm{x}}) = 0 \\
&\Leftrightarrow \quad \forall i \in I\ \forall f \in A_i :\ f(\underline{\mathrm{x}}) = 0 \\
&\Leftrightarrow \quad \forall i \in I :\ \underline{\mathrm{x}} \in V_{A_i}(L) \\
&\Leftrightarrow \quad \underline{\mathrm{x}} \in \bigcap_{i\in I} V_{A_i}(L)
\end{aligned}$$

zu d): Es gilt $AB \subseteq A$ also ist mit (a) $V_A(L) \subseteq V_{AB}(L)$. Analog gilt $V_B(L) \subseteq V_{AB}(L)$ Damit gilt nun, dass $V_A(L) \cap V_B(L) \subseteq V_{AB}(L)$ ist. Weiter gilt für $\underline{\mathrm{x}} \in \mathbb{A}^n(L)$ und $\underline{\mathrm{x}} \notin V_A(L) \cap V_B(L)$, dass es ein $f \in A$ mit der Eigenschaft $f(\underline{\mathrm{x}}) \neq 0$ sowie ein $g \in B$ mit der Eigenschaft $g(\underline{\mathrm{x}}) \neq 0$ gibt. Mit diesen ist $f(\underline{\mathrm{x}}) \cdot g(\underline{\mathrm{x}}) \neq 0$ also folgt $\underline{\mathrm{x}} \notin V_{AB}(L)$, denn $f \cdot g \in A \cdot B$ und wir haben beide Inklusionen gezeigt. Der Teil (e) ist trivial. □

Definition 9.3 *(Topologie)*
Sei $\mathfrak{X}$ eine Menge. Eine Menge $\mathfrak{O}$ von Teilmengen von $\mathfrak{X}$ (d.h. $\mathfrak{O} \subseteq P(\mathfrak{X})$) heißt Topologie auf $\mathfrak{X}$ (bzw. $(\mathfrak{X}, \mathfrak{O})$ heißt Topologischer Raum), falls

(TOP 1) Die leere Menge und der Raum selber in $\mathfrak{O}$ liegen ($\varnothing, \mathfrak{X} \in \mathfrak{O}$)
(TOP 2) Beliebige Vereinigungen von Mengen aus $\mathfrak{O}$ wieder in $\mathfrak{O}$ liegen ($A_i \in \mathfrak{O} \Rightarrow \bigcup A_i \in \mathfrak{O}$)
(TOP 3) Endliche Schnitte von Mengen aus $\mathfrak{O}$ wieder in $\mathfrak{O}$ liegen ($A, B \in \mathfrak{O} \Rightarrow A \cap B \in \mathfrak{O}$)

Die Elemente von $\mathfrak{O}$ heißen die offenen (Teil-)Mengen von $\mathfrak{X}$. Eine Menge $M \in \mathfrak{X}$ heißt abgeschlossen, falls $\mathfrak{X} \backslash M \in \mathfrak{O}$ ist.

Definition und Bemerkung 9.4 *(Zariski Topologie)*
Die Zariski-Topologie auf $\mathbb{A}^n(K)$ ist wie folgt gegeben:

$$\mathfrak{O} := \{\mathbb{A}^n(K) \backslash V_S(K) \mid S \subseteq K[\underline{X}]\}$$

sei die Menge der offenen Mengen auf $\mathbb{A}^n(K)$, d.h. insbesondere die abgeschlossenen Teilmengen sind grade die $V_S(K)$.

Beweis. $\mathfrak{O}$ erfüllt (TOP 1) - (TOP 3), denn (TOP 1) gilt unmittelbar nach Bemerkung 9.2 (e). Nach den De Morganschen Regeln gilt:

$$\bigcup_{i \in I} \mathbb{A}^n(K) \backslash V_{S_i}(K) \;=\; \mathbb{A}^n(K) \backslash \bigcap_{i \in I} V_{S_i}(K) \;=\; \mathbb{A}^n(K) \backslash V_{\bigcup_{i \in I} S_i}(K) \quad \in \mathfrak{O}$$

damit folgt (TOP 2) und zum Nachweis von (TOP 3) seien $A, B \lhd K[\underline{X}]$, dann betrachte:

$$\begin{aligned} \mathbb{A}^n(K) \backslash V_a(K) \cap \mathbb{A}^n(K) \backslash V_B(K) \quad &= \quad \mathbb{A}^n(K) \backslash (\, V_A(K) \cup V_B(K)\,) \\ &\overset{9.2\,d}{=} \quad \mathbb{A}^n(K) \backslash V_{AB}(K) \quad \in \mathfrak{O} \end{aligned}$$

□

Bemerkung 9.5 *Die abgeschlossenen Mengen von $\mathbb{A}^n(K)$ bzgl. der Zariski-Topologie sind grade die endlichen Mengen und $\mathbb{A}^n(K)$.*

Beweis. Übungsaufgabe.

Definition 9.6 *(stetigkeit und Teilraumtopologie)*
Seien $(\mathfrak{X}, \mathfrak{O}_\mathfrak{X})$ und $(\mathfrak{Y}, \mathfrak{O}_\mathfrak{Y})$ topologische Räume. Eine Abbildung $f : \mathfrak{X} \to \mathfrak{Y}$ heißt stetig, falls für alle $U \in \mathfrak{O}_\mathfrak{Y}$ gilt $f^{-1}(U) \in \mathfrak{O}_\mathfrak{X}$ (d.h. Urbilder von offenen Mengen sind offen unter f)
Notation: $C(\mathfrak{X}, \mathfrak{Y}) := \{\, f : \mathfrak{X} \to \mathfrak{Y} \mid f \text{ stetig} \,\}$.
Sei $(\mathfrak{X}, \mathfrak{O}_\mathfrak{X})$ ein topologischer Raum und $\mathfrak{Y} \subseteq \mathfrak{X}$ eine Teilmenge, dann ist:

$$\mathfrak{O}_\mathfrak{Y} := \{U \cap \mathfrak{Y} \mid U \in \mathfrak{O}_\mathfrak{X}\}$$

die von $\mathfrak{X}$ induzierte Teilraumtopologie auf $\mathfrak{Y}$.

Definition und Bemerkung 9.7 *(Verschwindungsideal, Koordinatenring)*
Sei $\mathfrak{X} \subseteq \mathbb{A}^n(K)$ eine Teilmenge, versehen mit der, von der Zariski-Topologie auf $\mathbb{A}^n$ induzierten, Teilraumtopologie. Die Abbildung

$$\begin{array}{rcl} \varphi : K[\underline{X}] & \longrightarrow & \mathrm{Abb}(\mathfrak{X} \to \mathbb{A}^1(K)) \\ f & \mapsto & (\underline{x} \mapsto f(\underline{x})) \end{array}$$

ist ein Ring-Homomorphismus, wobei $\mathrm{Abb}(\mathfrak{X},\, \mathbb{A}^1(K))$ *punktweise zum Ring wird. Der Kern von* φ *heißt das Verschwindungsideal von* $\mathfrak{X}$*. Notation:* $I(\mathfrak{X})$
Es gilt: $I(\mathfrak{X}) = \{\, f \in K[\underline{X}] \mid f(\underline{x}) = 0 \ \forall\, \underline{x} \in \mathfrak{X} \,\}$ *und*

$$K[\mathfrak{X}] := {}^{K[\underline{X}]}\!/_{I(\mathfrak{X})}$$

heißt der Koordinatenring von $\mathfrak{X}$*. Weiter gilt:*

$$K[\mathfrak{X}] \overset{\varphi}{\hookrightarrow} C(\mathfrak{X}, \mathbb{A}^1(K)) \subseteq \mathrm{Abb}(\mathfrak{X}, \mathbb{A}^1(K))$$

Beweis. Sei $f \in K[\mathfrak{X}]$. Zu zeigen: $\varphi(f) : \mathfrak{X} \to \mathbb{A}^1(K)$ ist stetig.
Hierzu zeigen wir: $(\varphi(f))^{-1}$ ist abgeschlossen, nach Bemerkung 9.5 genügt es dazu zu zeigen, dass $(\varphi(f))^{-1}(\{a\})$ für $a \in K$ abgeschlossen in $\mathfrak{X}$ ist.

$$\begin{aligned}(\varphi(f))^{-1}(\{a\}) &= \{\, \underline{\mathrm{x}} \in \mathfrak{X} \mid f(\underline{\mathrm{x}}) = a \,\} \\ &= \{\, \underline{\mathrm{x}} \in \mathfrak{X} \ < \ f(\underline{\mathrm{x}}) - a = 0 \,\} \\ &= \mathfrak{X} \cap V_{f-a}(K) \text{ ist abgeschlossen in } \mathfrak{X}\end{aligned}$$

□

Anmerkung $K[\mathfrak{X}]$ enthält die Koordinatenfunktionen:

$$\begin{aligned}x_i : \quad \mathfrak{X} \quad &\to \quad \mathbb{A}^1(K) \\ (a_1, \ldots, a_n) \quad &\mapsto \quad a_i\end{aligned}$$

insbesondere erzeugen diese Funktionen $K[\mathfrak{X}]$.

Bemerkung 9.8 *(Eigenschaften von Verschwindungsidealen)*

1. $\mathfrak{X} \subseteq \mathfrak{Y} \subseteq \mathbb{A}^n(K) \subseteq \mathfrak{Y} \ \Rightarrow\ I(\mathfrak{X}) \supseteq I(\mathfrak{Y})$
2. $I(\varnothing) = K[\underline{X}]$*, falls* $\sharp K = \infty$*, dann* $I(\mathbb{A}^n(K)) = (0)$
3. $S \subseteq K[\underline{X}] \Rightarrow I(V_S(K)) \supseteq S$
   $\mathfrak{X} \subseteq \mathbb{A}^n(K) \ \Rightarrow\ V_{I(\mathfrak{X})}(K) \supseteq \mathfrak{X}$
4. $S \subseteq K[\underline{X}] \ \Rightarrow\ V_{I(V_S(K))}(K) = V_S(K)$
   $\mathfrak{X} \subseteq \mathbb{A}^n(K) \ \Rightarrow\ I(V_{I(\mathfrak{X})}(K)) = I(\mathfrak{X})$

Beweis. Übungsaufgabe

Definition 9.9 *(reduzibel, irreduzibel)*
Sei $\mathfrak{X}$ *ein topologischer Raum.* $\mathfrak{Y} \subseteq \mathfrak{X}$ *heißt reduzibel, falls es abgeschlossene, nicht-leere Teilmengen* $\mathfrak{Y}_1, \mathfrak{Y}_2$ *von* $\mathfrak{Y}$ *mit der Eigenschaft*

$$\mathfrak{Y}_1 \cup \mathfrak{Y}_2 = \mathfrak{Y}$$

gibt. Eine irreduzible affine algebraische Menge heißt affine Varietät.

Satz 9.10 *Sei* $\mathfrak{X} \subseteq \mathbb{A}^n(K)$ *eine affine algebraische Menge, dann sind äquivalent:*
(i) $\mathfrak{X}$ *ist eine Varietät (d.h. insbesondere irreduzibel)*
(ii) $I(\mathfrak{X}) \lhd K[\underline{X}]$ *ist Primideal*
(iii) $K[\mathfrak{X}]$ *ist ein Integritätsbereich.*

Beweis. „(ii) $\Leftrightarrow$ (iii)“ folgt direkt aus der Definition 9.9 und der Primeigenschaft von Idealen.
„(i) $\Rightarrow$ (ii)“: Annahme: $I(\mathfrak{X}) \lhd K[\underline{X}]$ sei kein Primideal, dann gäbe es $f_1, f_2 \in K[\underline{X}] \backslash I(\mathfrak{X})$, so dass $f_1 \cdot f_2 \in I(\mathfrak{X})$ liegen. Also ließe sich $\mathfrak{X}$ darstellen als

$$\mathfrak{X} = (\mathfrak{X} \cap V_{f_1}(K)) \cup (\mathfrak{X} \cap V_{f_2}(K))$$

Es gilt: $\mathfrak{X} \cap V_{f_i}(K) \neq \mathfrak{X}$, denn $f_i \notin I(\mathfrak{X})$ für $i \in \{1, 2\}$. Weiter ist

$$V_{f_1}(K) \cup V_{f_2}(K) = V_{f_1 f_2}(K) \supseteq \mathfrak{X}$$

dies impliziert aber, dass $\mathfrak{X}$ reduzibel ist und das ist ein Widerspruch zur Voraussetzung.
„(ii) $\Rightarrow$ (i)“: Annahme: Sei $\mathfrak{X} = \mathfrak{X}_1 \cup \mathfrak{X}_2$ mit $\mathfrak{X}_1 \neq \mathfrak{X} \neq \mathfrak{X}_2$ und $\mathfrak{X}_i$(abges.) $\in \mathfrak{X}$. Dann ist wegen Bemerkung 9.8 (d) $I(\mathfrak{X}) \subsetneqq I(\mathfrak{X}_1)$. Wähle $f_i \in I(\mathfrak{X}_i) \backslash I(\mathfrak{X})$ für $i \in \{1, 2\}$, dann gilt: $f_1 \cdot f_2 \in I(\mathfrak{X})$, also ist $I(\mathfrak{X})$ kein Primideal. Dies ist aber ein Widerspruch zur Voraussetzung. □

Satz 9.11 *(schwacher Hilbertscher Nullstellensatz)*
Sei K ein Körper und $A \lhd K[\underline{X}] := K[X_1, \dots, X_n]$ ein Ideal mit $A \neq K[\underline{X}]$, dann gilt $V_A(\bar{K}) \neq \varnothing$

Satz 9.12 *(schwacher Hilbertscher Nullstellensatz, Körpertheoretische Form)*
Sei L/K eine Körpererweiterung, so dass es $a_1, \dots, a_n \in L$ gibt mit $L = K[a_1, \dots, a_n] =: K[\underline{a}]$, dann ist L/K eine endliche algebraische Körpererweiterung.

Wir werden zunächst zeigen, dass die Aussagen der Sätze 9.11 und 9.12 äquivalent sind und anschließend mit dem Beweis von Satz 9.12 (Körpertheoretische Form) beide Sätze beweisen.

Bemerkung 9.13 *Die Aussagen der Sätze 9.11 und 9.12 sind äquivalent.*

Beweis. „9.12 $\Rightarrow$ 9.11“:
Sei $A \lhd K[\underline{X}] := K[X_1, \dots, X_n]$ mit $A \neq K[\underline{X}]$ ein Ideal. Weiter sei $M \lhd K[\underline{X}]$ ein Maximalideal mit $A \subseteq M$, dann definiere:

$$L := \bar{K}[\underline{X}] \big/ M$$

Dann ist L eine Körpererweiterung von $\bar{K}$, wir definieren weiter:
$a_i := X_i + M$, dann gilt: $L = \bar{K}[a_1, \dots, a_n]$. Mit Satz 9.12 folgt nun, dass $L/\bar{K}$ eine endliche algebraische Körpererweiterung ist. Da $\bar{K}$ algebraisch abgeschlossen ist, heißt dies $L = \bar{K}$ und somit gilt für alle $i = 1, \dots, n$, dass $a_i \in \bar{K}$ sind. Es gilt nun:

$$\underline{a} := (a_1, \dots, a_n) \in V_M(\bar{K})$$

denn für alle i gilt: $X_i - a_i \in M \subseteq \bar{K}[\underline{X}]$. Also ist das von den $X_i - a_i$ erzeugte Maximalideal in M enthalten. Da beides Maximalideale sind gilt: $(X_1 - a_1, \dots, X_n - a_n) = M$. Wir dürfen also folgern

$$V_A(\bar{K}) \supseteq V_M(\bar{K}) \ni \{\underline{a}\}$$

Daher kann $V_A(\bar{K})$ nicht leer sein.
„ 9.11 $\Rightarrow$ 9.12“:
Sei L/K eine Körpererweiterung mit $L = K[a_1, \dots, a_n]$ für $a_i \in L$, betrachte:

$$\begin{aligned} \psi : K[\underline{X}] &\to L \\ X_i &\mapsto a_i \end{aligned}$$

Definiere: $M := \mathrm{Ker}(\psi)$, dann ist M ein Maximalideal. Es gibt einen Vektor $\underline{b} \in V_M(\bar{K})$ nach Satz 9.11. Mit diesem betrachte

$$\begin{aligned} \varphi : K[\underline{X}] &\to \bar{K} \\ x_i &\mapsto b_i \end{aligned}$$

Es gilt: $M = \mathrm{Ker}(\psi) \subseteq \mathrm{Ker}(\varphi)$, denn Sei $f \in M$, dann ist $f(\underline{b}) = 0$ also ist $f \in \mathrm{Ker}(\varphi)$. Da $M \lhd K[\underline{X}]$ ein Maximalideal ist, gilt $M = \mathrm{Ker}(\varphi)$, damit folgt:

$$K \subseteq L \cong {}^{K[\underline{X}]}\!/_{M} \subseteq \bar{K}$$

Dies heißt L/K ist eine Teilerweiterung von $\bar{K}/K$, also ist L/K algebraisch und wird insbesondere von den $a_1, \ldots, a_n$ endlich erzeugt. □

Beweis. Zu Satz 9.12 *(schwacher Hilbertscher Nullstellensatz, Körpertheoretische Form)*
Sei L/K eine Körpererweiterung mit $L = K[a_1, \ldots, a_n]$. Wir nehmen an, dass L/K nicht algebraisch ist, dann gibt es eine Transzendenzbais $\mathfrak{T} := \{e_1, \ldots, e_t\}$ so dass

$$K \subseteq K(\mathfrak{T}) \subseteq L = K[a_1, \ldots, a_n] \text{ mit } L/K(\mathfrak{T}) \text{ ist algebraisch}$$

insbesondere ist L ein endlich dimensionaler $K(\mathfrak{T})$-Vektorraum.

Mit den folgenden Bemerkungen 9.14 und 9.15 wollen wir dies nun zum Widerspruch führen.

Definition und Bemerkung 9.14 *(R-Algebra)*
Seien R, A Ringe und $\varphi \in \mathrm{Hom}(R, A)$ ein Homomorphismus, dann heißt das Tupel (A, φ) eine R-Algebra. Die Skalarmultiplikation von A mit R ist wie folgt gegeben:

$$\begin{aligned} \cdot : R \times A &\to A \\ (r, a) &\mapsto \varphi(r) \cdot a \end{aligned}$$

Seien $R \subseteq S \subseteq T$ Ringe mit folgenden Eigenschaften:
- R ist Noetherscher Ring.
- T ist als R-Algebra wie auch als S-Modul endlich erzeugt.
Dann gilt: S ist eine endlich erzeugte R-Algbra

Beweis. Sei $\mathfrak{X} := \{x_1, \ldots, x_n\}$ ein Erzeugendensystem von T als R-Algebra, dann wähle ein Erzeugendensystem $E := \{t_1, \ldots, t_m\}$ von T als S-Modul, so dass $\mathfrak{X} \subseteq E$. Betrachte:

$$t_i \cdot t_j = \sum_{l=1}^{m} a_{i,j,l} \cdot t_l \quad \text{mit } a_{i,j,l} \in S$$

Definiere nun eine endlich erzeugte R-Algebra wie folgt:

$$S' := R[a_{i,j,l} \,|\, 1 \leq i, j, l \leq n]$$

Da für alle i, j, l gilt: $a_{i,j,l} \in S$ folgt unmittelbar $S' \subseteq S$. Da $\mathfrak{X} \subseteq E$ wird T zum S'-Modul durch $T = S't_1 + \ldots S't_m$, insbesondere ist also T als S'-Modul endlich erzeugt, weiter ist S' als Quotient von $R[X_{i,j,l} \,|\, 1 \leq i, j, l \leq n]$ Noethersch, also ist auch T als endlich erzeugter S'-Modul Noethersch.
Es gilt: $S' \subseteq S \subseteq T$, daher ist S insbesondere ein endlich erzeugter S'-Modul.
Sei also $\{s_1, \ldots, s_r\} \subseteq S$ ein Erzeugendensystem von S als S'-Modul, dann ist S als R-Algebra von $\{s_1, \ldots, s_r\} \cup \{a_{i,j,l} \,|\, 1 \leq i, j, l \leq n\}$ endlich erzeugt. □

Bemerkung 9.15 *Für $t > 0$ ist $K(X_1, \ldots, X_t) := \mathrm{Quot}(K[X_1, \ldots, X_t])$ als K-Algebra nicht endlich erzeugt.*

Beweis. Zur besseren Lesbarkeit bezeichne wieder $\underline{X} := (X_1, \ldots, X_t)$. Wir nehmen die gegenteilige Aussage an, dann ist

$$E := \left\{ \frac{f_i(\underline{X})}{g_i(\underline{X})} \mid i = 1, \ldots, n \; n \in \mathbb{N} \right\}$$

ein Erzeugendensystem von $K(\underline{X})$ als K-Algebra. Seien dann $p_1(\underline{X}), \ldots, p_m(\underline{X})$ bis auf Assoziertheit alle irreduziblen Polynome derart, dass es für alle $i = 1, \ldots, n$ ein $j \in \{1, \ldots, m\}$ mit der Eigenschaft $p_j(\underline{X})$ teilt $g_i(\underline{X})$, gibt. Nimm nun ein irreduzibles Polynom $p(\underline{X})$, dass zu keinem der $p_i(\underline{X})$ Assoziert ist. Da es nach Euklid unendlich viele irreduzible Polynome in $K(\underline{X})$ gibt, ist diese Wahl zulässig.
Es gilt: $\frac{1}{p(\underline{X})}$ ist nicht durch E darzustellen. Dies ist ein Widerspruch dazu, dass E ein Erzeugendensystem ist, also ist $K(\underline{X})$ nicht endlich erzeugt. □

Fortsetzung des Beweises von Satz 9.12
Nach Bemerkung 9.14 ist $K(\mathfrak{T}$ als K-Algebra endlich erzeugt, was nach Bemerkung 9.15 nicht möglich ist. Wir haben unsere Annahme L/K wäre nicht algebraisch also widerlegt und den Satz bewiesen. □

Folgerung 9.16 *Sei K ein Körper und $M \lhd K[\underline{X}] := K[X_1, \ldots, X_n]$ ein Maximalideal, dann ist*

$$L := {}^{K[\underline{X}]}\!/_{M}$$

eine endlich erzeugte Körpererweiterung von K. Ist K algebraisch abgeschlossen, dann gibt es $a_1, \ldots, a_n \in K$, so dass $M = (X_i - a_i | i = 1 \ldots n)$.

Beweis. Diese Folgerung haben wir bereits in Bemerkung 9.13 im Teil „9.11 $\Rightarrow$ 9.12“ bewiesen. □

Folgerung 9.17 *Sei K algebraisch abgeschlossen und $\mathfrak{X} \subseteq \mathbb{A}^n(K)$ eine affine algebraische Menge, dann gelten:*
(a) Für $\underline{a} \in \mathbb{A}^n(K)$ gilt: $\underline{a} \in \mathfrak{X} \Leftrightarrow I(\mathfrak{X}) \subseteq (X_1 - a_1, \ldots, X_n - a_n)$
(b) Die Maximalideale von $K[\mathfrak{X}]$ sind von der Form:

$$(X_1 - a_1, \ldots, X_n - a_n) + I(\mathfrak{X}) \text{ für } \underline{a} \in \mathfrak{X}$$

Beweis. Der Nachweis von (b) erfolgt direkt durch Folgerung 9.16 und die Ergebnisse aus Algebra I. Zum Nachweis von (a) betachte:

$$\begin{aligned} \underline{a} \in \mathfrak{X} &\Leftrightarrow \{\underline{a}\} \subseteq \mathfrak{X} \Leftrightarrow I(\{\underline{a}\}) \supseteq I(\mathfrak{X}) \\ &\Leftrightarrow (X_1 - a_1, \ldots, X_n - a_n) \supseteq I(\mathfrak{X}) \end{aligned}$$

□

10 Die Resultante und Schnitte von Kurven

Definition 10.1 *(Resultante)*
Sei R ein kommutativer Ring und die Polynome

$$f(X) := \sum_{i=0}^{m} a_i X^{m-1}, g(X) := \sum_{i=0}^{n} b_i X^{n-i} \in R[X]$$

Die Resultante zum formalen Grad n, m ist die Daterminante der folgenden $n+m \times n+m$-Matrix

$$S_{(f,g)} := \begin{pmatrix} a_0 & a_1 & \dots & \dots & a_m & & & \\ & a_0 & a_1 & \dots & \dots & a_m & & \\ & & \ddots & & & & \ddots & \\ & & & a_o & a_1 & \dots & \dots & a_m \\ b_0 & \dots & \dots & b_n & & & & \\ & b_0 & \dots & \dots & b_n & & & \\ & & \ddots & & & \ddots & & \\ & & & b_o & \dots & \dots & b_n & \end{pmatrix}$$

Also $\operatorname{res}(f,g) := \det(S_{(f,g)})$.

Anmerkung Die Matrix $S_{(f,g)}$ heißt Sylvestermatrix nach James J. Sylvester

Bemerkung 10.2 *Unter Verwendung der Bezeichnungen aus Definition 10.1 gelten:*

1. $\operatorname{res}(f,g) = (-1)^{nm} \operatorname{res}(g,f)$
2. *Seien $\alpha, \beta \in R$, dann gilt* $\operatorname{res}(\alpha f, \beta g) = \alpha^n \cdot \beta^m \cdot \operatorname{res}(f,g)$
3. *Sei $\varphi : R \to S$ ein Ringhomomorphismus, dann ist* $\operatorname{res}(\varphi(f), \varphi(g)) = \varphi(\operatorname{res}(f,g))$

Beweis. Die Ergebnisse erhalten wir aus der Linearen Algebra. In (1) durch Zeilenvertauschung, in (2) durch Skalarmultiplikation und in (3) durch ausnützen der Homomorphieeigenschaft von φ. □

Beispiel 22 *(Resultante)*
Sei $f(X) := X - a$ und $g(X) := X - b$, dann gilt

$$\mathrm{res}(f,g) = \det \begin{pmatrix} 1 & -a \\ 1 & -b \end{pmatrix} = a - b$$

Sei $f(X) := X - a$ und $g(X) := \sum_{i=1}^{n} b_i \cdot X^{n-i}$, dann gilt

$$\begin{aligned}
\mathrm{res}(f,g) &= \det \begin{pmatrix} 1 & -a & & & & \\ & 1 & -a & & & \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \\ & & & & 1 & -a \\ b_0 & b_1 & b_2 & \dots & \dots & b_n \end{pmatrix} \\
&= b_0 \cdot (-1)^{n+2} \cdot \det \begin{pmatrix} -a & & & \\ 1 & -a & & \\ & \ddots & \ddots & \\ & & 1 & -a \end{pmatrix} + \dots \\
&\quad \dots + b_n \cdot (-1)^{2n+1} \cdot \det \begin{pmatrix} 1 & -a & & \\ & \ddots & \ddots & \\ & & 1 & -a \\ & & & 1 \end{pmatrix} \\
&= b_0 \cdot a^n + b_1 \cdot a^{n-1} + \dots + b_n \cdot a^0 \;=\; g(a)
\end{aligned}$$

Bemerkung 10.3 *Sei R ein kommutativer Ring und die Polynome f, g wie in Definition 10.1 gegeben. Weiter Bezeichne*

$$R[X]_{<n} := \{\, f \mid f \in R[X] \wedge \deg(f) < n \,\}$$

Die Menge der Polynome in $R[X]$ mit Grad kleiner n und

$$\begin{aligned}
\mathfrak{B}_n &:= \{X^{n-1}, X^{n-2}, \dots, X^0 = 1\} \text{ Basis von } R[X]_{<n} \\
\mathfrak{B}_m &:= \{X^{m-1}, X^{m-2}, \dots, X^0 = 1\} \text{ Basis von } R[X]_{<m} \\
\mathfrak{B}_{m+n} &:= \{X^{m+n-1}, X^{m+n-2}, \dots, X^0 = 1\} \text{ Basis von } R[X]_{<m+n}
\end{aligned}$$

Dann wird der R-Modulhomomorphismus

$$\begin{aligned}
S : R[X]_{<n} \times R[X]_{<m} &\to R[X]_{<n+m} \\
(u(X), v(X)) &\mapsto u(X) \cdot f(X) + v(X) \cdot g(X)
\end{aligned}$$

von der Matrix ${S_{(f,g)}}^T$ beschrieben.

Beweis. Das Matrix-Vektor-Produkt der Transformierten Matrix von $S_{(f,g)}$ und dem Vektor

$$(u_o, \dots, u_{n-1}, v_o, \dots, v_{m-1})^T$$

wobei die u_i die Koeffizienten von $u(X)$ und die v_i die Koeffizienten von $v(X)$ sind, ergibt den Koeffizientenvektor von $u(X) \cdot f(X) + v(X) \cdot g(X)$. □

Satz 10.4 *Sei R ein kommutativer Ring und $f, g \in R[X]$ Polynome. Dann gibt es weitere Polynome $u, v \in R[X]$ mit $\deg(u) < \deg(g)$ und $\deg(v) < \deg(f)$, so dass*

$$\operatorname{res}(f,g) = u(X) \cdot f(X) + v(X) \cdot g(X)$$

Beweis. Sei $S := {S_{(f,g)}}^T$ die Matrix zur Abbildung aus Bemerkung 10.3, und S^* die zu S adjungierte Matrix. Weiter bezeichne $I := id \in \operatorname{Mat}_R(n+m, n+m)$. Es gilt

$$S \cdot S^* = \det(S) \cdot I = \operatorname{res}(f,g) \cdot I$$

also folgt

$$S \left(S^* \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \det(S) \end{pmatrix} \in \operatorname{Im}(S)$$

Mit den Basen aus Bemerkung 10.3 ist also $\det(S) \in \operatorname{Im}(S)$. Ebenfalls in Bemerkung 10.3 haben wir errechnet, dass $\det(S) = u(X) \cdot f(X) + v(X) \cdot g(X)$ ist. □

Bemerkung 10.5 *Seien R, f, g wie in Definition 10.1 gegeben. Zusätzlich sei f normiert. Es gelten*

(a) *Neben $\mathfrak{B}_{n+m}$ aus Bemerkung 10.3 ist auch*

$$\mathfrak{B}'_{n+m} := \{ f(X)X^{n-1}, \ldots, f(X) \cdot X^0, X^{m-1}, \ldots, X^0 \}$$

eine Basis von $R[X]_{<n+m}$ und die Basiswechselmatrix hat die Determinante 1.

(b) *Für den im Folgenden definierten R-Endomorphismus Φ' gilt $\operatorname{res}(f,g) = \det(\Phi')$*

$$\begin{array}{rcl} \Phi' : R[X]_{<n+m} & \to & R[X]_{<n+m} \\ f(X) \cdot X^i & \mapsto & f(X) \cdot X^i \text{ für } 0 \le i \le n \\ X^j & \mapsto & g(X) \cdot X^j \text{ für } 0 \le j \le m \end{array}$$

Beweis. Zu (a):
Stelle $\mathfrak{B}' := \mathfrak{B}'_{n+m}$ in der Basis $\mathfrak{B} := \mathfrak{B}_{n+m}$ dar

$$M_{\mathfrak{B}}^{\mathfrak{B}'} = \begin{pmatrix} a_0 & & & & & & \\ \vdots & a_0 & & & & & \\ a_m & \vdots & \ddots & & & & \\ & a_m & & a_0 & & & \\ & & \ddots & \vdots & 1 & & \\ & & & a_m & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

Nach Voraussetzung ist f normiert, das heißt a_0, der höchste Koeffizient von f, ist 1 daher folgt $\det(M_{\mathfrak{B}}^{\mathfrak{B}'}) = 1$

Zu (b):
Die Darstellungsmatrix von Φ' bezüglich $\mathfrak{B}'$ und $\mathfrak{B}$ ist gegeben durch ${S_{(f,g)}}^T$. Nach (a) gilt dann

$$\mathrm{res}(f,g) = \det({S_{(f,g)}}^T) = 1 \cdot \det({S_{(f,g)}}^T) = \det(M_{\mathfrak{B}}^{\mathfrak{B}'}) \cdot \det({S_{(f,g)}}^T) = \det(\Phi')$$

□

Definition und Satz 10.6 *(Norm)*
Sei R ein kommutativer Ring und $f \in R[X]$ ein normiertes Polynom mit $\deg(f) = m$. Es gelten:
(a) Der Ring $A := {R[X]}/{(f)}$ ist ein freier R-Modul vom Rang m mit der Basis $\{x^{m-1}, \ldots, x^0\}$, wobei $x := X + (f)$ ist.
(b) Sei $g \in R[X]$ mit $\deg(g) \leq n$, dann bezeichne $g(x) := g(X) + (f) \in A$.
Die Norm $\mathrm{N}_{A/R}(\, g(x)\,)$ ist definiert als die Determinante der R-linearen Abbildung

$$\begin{array}{rcl} \psi : A & \to & A \\ a & \mapsto & a \cdot g(x) \end{array}$$

Es gilt $\mathrm{N}_{A/R}(\, g(x)\,) := \det(\psi) = \mathrm{res}(f,g)$. Insbesondere ist $\mathrm{res}(f,g)$ unabhängig vom formalen Grad von g.

Beweis. Zum Teil a): Da f nach Voraussetzung normiert ist können wir die Division mit Rest durchführen. Hierbei ist der Rest eindeutig bestimmt.
zu (b):
Sei $\iota : \mathrm{Ker}(\pi) \to R[X]_{<n+m}$ die Inklusion, wobei $\pi : R[X]_{<n+m} \to {R[X]}/{(f)}$ die natürliche Projektion ist. Nach (a) ist π surjektiv. Betrachte:

$$\begin{array}{ccc} \mathrm{Ker}(\pi) & \xrightarrow{id} & \mathrm{Ker}(\pi) \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ R[X]_{<n+m} & \xrightarrow{\Phi'} & R[X]_{<n+m} \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ A & \xrightarrow{\psi} & A \end{array}$$

Dieses Diagramm ist kommutativ, denn nach Definition von Φ' gilt
$\pi \circ \Phi' = \psi \circ \pi$. Weiter gilt $\mathrm{Ker}(\pi) = f \cdot R[X]_{<n}$. Betrachte

$$\Phi'(\mathrm{Ker}(\pi)\,) = \Phi'(f \cdot R[X]_{<n}) = f \cdot R[X]_{<n} = \mathrm{Ker}(\pi)$$

Es folgt also: $\Phi' \circ \iota = \iota \circ id$. Und daher gilt

$$\mathrm{res}(f,g) = \det(\Phi') = \det(id) \cdot \det(\psi) = \mathrm{N}_{A/R}(\, g(x)\,)$$

□

Folgerung 10.7 *Sei R ein faktorieller Integritätsring mit $K := \mathrm{Quot}(R)$, dann fixiere $\bar{K}$ einen algebraischen Abschluss von K. Weiter seien $f, g \in R[X]$ normierte Polynome. Es sind äquivalent*
(i) $\mathrm{res}(f,g) \neq 0$
(ii) f und g haben keine gemeinsamen Nullstellen in $\bar{K}$
(ii) f und g haben keine gemeinsamen Faktoren in $R[X]$

Beweis. „(i) $\Rightarrow$ (iii)“:
Nach Voraussetzung ist $\mathrm{res}(f,g) \neq 0$ damit ist mit $A, g(x)$ wie in Satz 10.6 $\mathrm{N}_{A/K}(\, g(x)\,) \neq 0$. Es gilt $g(x) \in A^*$, denn die Determinante der zur Multiplikation mit $g(x)$ gehörigen Matrix ist nicht Null. Also gibt es $h \in K[X]$ derart, dass $1 = h(x) \cdot g(x) \in A$ gilt und somit gibt es $p \in K[X]$ so dass wir die Darstellung zu $1 = h(X)g(X) + p(X)f(X)$ verändern können also ist der $\mathrm{ggT}(f,g) = 1$ in $K[X]$. Damit haben f, g keinen gemeinsamen Faktor in $R[X]$.
„(iii) $\Rightarrow$ (ii)“:
Hätten f, g gemeinsame Nullstelle in $\bar{K}$, dann hätten f und g einen gemeinsamen Faktor in $K[X]$, nämlich das Minimalpolynom der gemeinsamen Nullstelle. Mit dem Satz von Gauß hätten f, g dann einen gemeinsamen Faktor in $R[X]$, dies ist jedoch ein Widerspruch.
„(ii) $\Rightarrow$ (i)“:
Gibt es kein $k \in \bar{K}$ mit $f(k) = g(k) = 0$, dann haben f und g keinen gemeinsamen Faktor in $K[X]$, also gilt $\mathrm{ggT}(f,g) = 1$. Es folgt, dass es $h, p \in K[X]$ gibt, so dass $1 = h(X)g(X) + p(X)f(X)$. Daher ist $g(x) \in A^*$. Es gilt $\mathrm{res}(f,g) = \mathrm{N}_{A/R}(\, g(x)\,) \neq 0$ □

Folgerung 10.8 *Sei R ein kommutativer Ring.*

(a) *Seien $f, g_1, g_2 \in R[X]$ und f normiert, dann ist*

$$\mathrm{res}(f, g_1 g_2) = \mathrm{res}(f, g_1) \cdot \mathrm{res}(f, g_2)$$

(b) *Seien $f_1, f_2, g \in R[X]$ und g normiert, dann ist*

$$\mathrm{res}(f_1 f_2, g) = \mathrm{res}(f_1, g) \cdot \mathrm{res}(f_2, g)$$

Beweis. Teil (a) folgt direkt aus Satz 10.6. Zu (b) betrachte

$$\begin{aligned}
\mathrm{res}(f_1 f_2, g) &= (-1)^{\deg(f_1 f_2)\cdot\deg(g)}\, \mathrm{res}(g, f_1 f_2) \\
&\overset{(a)}{=} (-1)^{\deg(f_1)\cdot\deg(g)} \cdot (-1)^{\deg(f_2)\cdot\deg(g)} \cdot \mathrm{res}(g, f_1) \cdot \mathrm{res}(g, f_2) \\
&= \left((-1)^{\deg(f_1)\cdot\deg(g)}\right)^2 \cdot \mathrm{res}(f_1, g) \cdot \left((-1)^{\deg(f_2)\cdot\deg(g)}\right)^2 \mathrm{res}(f_2, g)
\end{aligned}$$

□

Folgerung 10.9 *Sei R ein kommutativer Ring und*

$$f(X) := \prod_{i=1}^{m} (X - \alpha_i) \;\text{ und }\; g(X) := \prod_{j=1}^{n} (X - \beta_j)$$

Dann ist die Resultante von f und g

$$res(f,g) = \prod_{i=1}^{m} g(\alpha_i) = \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

Beweis. $\mathrm{res}(X - \alpha, g) = g(\alpha)$ nach Beispiel 22. Mit Folgerung 10.8 folgt die Aussage. □

Folgerung 10.10 *(Diskriminantenformel)*
Sei R ein kommutativer Ring und $f \in R[X]$ normiert vom Grad m mit Ableitung f', dann gilt

$$(-1)^{\frac{m(m-1)}{2}} \cdot \triangle_f \;=\; \mathrm{res}(f, f')$$

Zerfällt f in Linearfaktoren, mit Nullstellen α_i, dann gilt sogar

$$\mathrm{res}(f, f') \;=\; \prod_{i=1}^{m} f'(\alpha_i) = \prod_{i=1}^{m}\prod_{j=1}^{m}(\alpha_i - \alpha_j)$$

Beweis. Nach einer Übungsaufgabe gibt es eine Ringerweiterung R' von R sowie $\alpha_i \in R'$, so dass

$$f(X) = \prod_{i=1}^{m}(X - \alpha_i)$$

Betrachte

$$\begin{aligned}
\mathrm{res}(f, f') &= \prod_{i=1}^{m} f'(\alpha_i) = \prod_{i=1}^{m}\prod_{j=1}^{m}(\alpha_i - \alpha_j) \\
&= (-1)^{\frac{m(m-1)}{2}} \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2 \\
&= (-1)^{\frac{m(m-1)}{2}} \cdot \triangle_f
\end{aligned}$$

□

Satz 10.11 *Sei K ein algebraisch abgeschlossener Körper und $f, g \in K[X, Y]$ zwei teilerfremde Polynome, dann gilt*

$$\sharp\,(V_f(K) \cap V_g(K)) < \infty$$

Beweis. Zunächst werden wir den Beweis darauf reduzieren, dass f irreduzibel ist, denn sei

$$f(X, Y) = \prod_{i=1}^{n} f_i(X, Y)^{r_i}$$

die Zerlegung von f in irreduzible Elemente, dann gilt

$$V_F(K) = \bigcup_{i=1}^{n} V_{f_i}(K)$$

demnach genügt es zu zeigen, dass für alle diese i gilt $\sharp\,(V_{f_i}(K) \cap K) < \infty$. Sei f also o.B.d.A. irreduzibel. Wir werden nun die Behauptung in zwei Fällen zeigen:
1. Fall: Sei $f(X, Y) = c \cdot (X - a) \in K[X, Y]$ mit $a, c \in K$. Dann betrachte

$$\begin{aligned}
\sharp\,(V_f(K) \cap V_g(K)) &= \sharp\{\,(x, y) \in \mathbb{A}^2(K) \mid x = a \wedge g(a, y) = 0\,\} \\
&= \sharp\{\,y \in K \mid g(a, y)\,\}
\end{aligned}$$

Diese Menge hat nur dann unendlich viele Elemente, wenn $g(a, Y)$ das Nullpolynom ist. Dies wollen wir im folgenden annehmen. Weiter fassen wir $g(X, Y)$ als Polynom in $(K[Y])[X]$ auf, d.h.

$$g(X, Y) = \sum_{i=0}^{n} \beta_i(Y) X^i \text{ mit } \beta_i(Y) \in K[Y]$$

Es gilt: a ist Nullstelle von $g(X, Y)$ in $K[Y][X]$, also teilt $(X - a)$ das Polynom $g(X, Y)$, dies ist jedoch ein Widerspruch zur Teilerfremdheit, also kann $g(a, Y)$ nicht das Nullpolynom sein.
2. Fall: Nun im Allgemeinen. Wir fassen dazu $f(X, Y), g(X, Y)$ als Polynome in $K[X][Y]$ auf, d.h.

$$f(X, Y) = \sum_{1=0}^{m} \alpha_i(X) Y^i \text{ und } g(X, Y) = \sum_{j=0}^{n} \beta_j(X) y^j \text{ mit } \alpha_i(X), \beta_j(X) \in K[X]$$

Betrachte nun die Resultante von f, g als Polynome in Y:

$$r(X) := \operatorname{res}(f, g) \in K[X]$$

Es gilt $R(a) = \operatorname{res}(f(a, Y), g(a, Y))$ für alle $a \in K$. Wir wollen nun zeigen, dass

$$x\left(V_f(K) \cap V_g(K)\right) \subseteq \{\, a \in K \mid r(a) \cdot \alpha_m(a) = 0 \,\}$$

Betrachte die Koordinatenabbildung

$$\begin{aligned} x : \mathbb{A}^2(K) &\to K \\ (x, y) &\mapsto x \end{aligned}$$

und sei $a \in x\left(V_f(K) \cap V_g(K)\right)$, dann gibt es ein $b \in K$ dearart, dass
$f(a, b) = g(a, b) = 0$. Es ist b eine gemeinsame Nullstelle von $f(a, Y)$ und $g(a, Y)$ daher ist mit Folgerung 10.7

$$r(a) = 0 \vee \alpha_m(a) = 0$$

Insgesamt gilt: Es kommen nur endlich viele X-Koordinaten vor. Zu jeder dieser X-Koordinaten gibt es nur endlich viele Y-Koordinaten. □

Anmerkung Genauer gilt nach dem Satz von Bezout:

$$\sharp\left(V_f(K) \cap V_g(K)\right) \leq \deg(f) \cdot \deg(g)$$

Bemerkung 10.12 *Sei K ein alebraisch abgeschlossener Körper und $f \in K[X, Y]$ ein irreduzibles Polynom. Es gilt:*

$$I\left(V_f(K)\right) = (f)$$

Beweis. Nach Definition ist klar, dass (f) in $I\left(V_f(K)\right)$ enthalten ist, wir müssen uns also nur um die andere Inklusion kümmern. Dazu sei $g \in I\left(V_f(K)\right)$ mit $f \nmid g$, dann folgt mit dem soeben bewiesenen Satz 10.11

$$\sharp\left(V_f(K) \cap V_g(K)\right) < \infty$$

Aus $g \in I\left(V_f(K)\right)$ folgt aber auch:

$$V_g(K) \supseteq V_f(K)$$

und somit, da K algebraisch abgeschlossen ist, folgt $\sharp V_g(K) = \infty$, dies ist aber ein Widerspruch dazu, dass der Schnitt nur endlich viele Punkte enthählt. □

Definition 10.13 *(Funktionenkörper von $\mathfrak{X}$)*
Sei K ein Körper und $\mathfrak{X} \subseteq \mathbb{A}^n(K)$ eine affine Varietät über K (d.h. insbesondere irreduzibel, und $K[\mathfrak{X}]$ ist ein Integritätsbereich).

$$K(\mathfrak{X}) := \text{Quot}\,(K[\mathfrak{X}])$$

heißt der Funktionenkörper von $\mathfrak{X}$.

Satz 10.14 *Sei K ein algebraisch abgeschlossener Körper und $f \in K[X,Y]$ ein irreduzibles Polynom. Definiere $\mathfrak{X} := V_f(K)$ und sei weiter $\alpha \in K(\mathfrak{X})^*$. Dann gibt es endlich viele Punkte $p_1, \ldots, p_s \in \mathfrak{X}$, so dass α eine stetige Funktion auf $\mathfrak{X}\backslash\{p_1, \ldots, p_s\} \to \mathbb{A}^1(K)$ induziert.*

Beweis. Es gibt $g, h \in K[X,Y]$, derart dass $\alpha = \frac{\bar{h}}{\bar{g}}$ ist, wobei $\bar{h}, \bar{g}$ die Restklassen von h, g in $K[\mathfrak{X}] := {}^{K[X,Y]}\!/_{(f)}$ sind. Definiere

$$\{p_1, \ldots, p_s\} := V_f(K) \cap V_g(K)$$

dann gilt: Ist $(x,y) \in \mathfrak{X}\backslash\{p_1, \ldots, p_s\}$, so ist $\bar{g}(x,y) \neq 0$. D.h. $\alpha(x,y) := \frac{\bar{h}(x,y)}{\bar{g}(x,y)}$ ist wohldefiniert und gibt uns die gewünschte Abbildung. Die Stetigkeit sieht man durch Nachrechnen ein. □

11 Morphismen von Kurven

Definition 11.1 *(Morphismus von Kurven)*
Sei K ein Körper und $f, g \in K[X,Y]$ zwei Polynome, dann setze $C := V_f(K)$ und $D := V_g(K)$. Eine Abbildung

$$\begin{array}{rccc} \varphi: & C & \to & D \\ & (a,b) & \mapsto & (\,\varphi_1(a,b), \varphi_2(a,b)\,) \end{array}$$

heißt Morphismus von Kurven, falls es Polynome $\alpha, \beta \in K[X,Y]$ gibt, so dass für alle $(a,b) \in C$ gilt:

$$\varphi_1(a,b) = \alpha(a,b) \text{ und } \varphi_2(a,b) = \beta(a,b)$$

Anmerkung Diese Definition verallgemeinert sich auf nicht triviale Weise auf Varietäten höherer Dimension.

Beispiel 23 *(Potenzieren)*
Sei K ein Körper und $f(X,Y) := X^n + Y^n - 1$, $g(X,Y) := X + Y - 1 \in K[X,Y]$, dann ist

$$\begin{array}{rccc} \varphi: V_f(K) & \to & V_g(K) \\ (a,b) & \mapsto & (a^n, b^n) \end{array}$$

ein Morphismus von Kurven, mit $\alpha(X,Y) = X^n$ und $\beta(X,Y) = Y^n$.

Beispiel 24 *(Projektion auf die X-Achse)*
Sei K ein Körper und $f \in K[X,Y]$. Setze $C := V_f(K)$.
Die X-Achse ist die Kurve $D := V_g(K)$ mit $g(X,Y) = Y$. Es gilt

$$\begin{array}{rccc} \varphi: V_f(K) & \to & V_g(K) \\ (a,b) & \mapsto & (a,0) \end{array}$$

ist Morphismus von Kurven mit $\alpha(X,Y) = X$ und $\beta(X,Y) = 0$.

Bemerkung 11.2 *Sei K ein Körper und $f, g \in K[X,Y]$ zwei irreduzible Polynome, dann definiere $C := V_f(K)$ und $D := V_g(K)$. Weiter sei $\varphi : C \to D$ ein Morphismus von Kurven, dann ist φ stetig bezüglich der Zariski-Topologie.*

Beweis. Seien $\alpha, \beta \in K[X,Y]$ wie in Definition 11.1 gegeben, dann ist zu zeigen, dass für jede abgeschlossene Menge $A \subseteq D$ auch $\varphi^{-1}(A)$ abgeschlossen ist. Die abgeschlossenen Mengen von D haben die Form

$$D \cap V_{\mathfrak{a}}(K) \text{ mit } \mathfrak{a} \lhd K[X,Y]$$

Nach Satz 10.11 sind dies die Mengen $D, \varnothing, M$ mit $\sharp M < \infty$
Wir müssen die Abgeschlossenheit von φ^{-1} also nur noch für einelementige Mengen zeigen, denn endliche Vereinigungen abgeschlossener Mengen sind abgeschlossen. Betrachte also für $(a,b) \in D$:

$$\begin{aligned} \varphi^{-1}((a,b)) &= \{\, (x,y) \in C \mid \varphi_1(x,y) = a \wedge \varphi_2(x,y) = b \,\} \\ &= \{\, (x,y) \in C \mid \alpha(x,y) - a = 0 \wedge \beta(x,y) - b = 0 \,\} \\ &= C \cap V_{\alpha(X,Y)-a}(K) \cap V_{\beta(X,Y)-b}(K) \end{aligned}$$

Dies ist per Definition eine abgeschlossene Menge. □

Definition 11.3 *(Iso-, Automorphismus von Kurven)*
Sei K ein Körper und $f, g \in K[X,Y]$ Polynome. Setze $C := V_f(K)$ und $D := V_g(K)$. Ein Morphismus von Kurven

$$\varphi : C \to D$$

heißt Isomorphismus, wenn es einen Morphismus von Kurven

$$\psi : D \to C$$

gibt, so dass $\varphi \circ \psi = id_D$ und $\psi \circ \varphi = id_C$
Ist $C = D$, dann heißt ein Isomorphismus von C in sich selbst auch Automorphismus.

Anmerkung Die Automorphismen einer Kurve bilden eine Gruppe. Je mehr Automorphismen eine Kurve hat, desto mehr Symmetrien hat sie, d.h. desto Spezieller ist sie.

Beispiel 25 *(hyperelliptische Kurven)*
Sei K ein Körper und $g \in K[X]$ irreduzibel, dann definiere $f(X,Y) := Y^2 - g(X) \in K[X,Y]$. Die Kurve $C := V_f(K)$ heißt hyperelliptische Kurve. Der Morphismus

$$\begin{aligned} h : C &\to C \\ (a,b) &\mapsto (a,-b) \end{aligned}$$

heißt hyperelliptsiche Involution (d.h. $h^2 = id_C$).

Definition und Bemerkung 11.4 *Seien $\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$ topologische Räume und $\varphi : \mathfrak{X} \to \mathfrak{Y}$ stetig, dann definiere*

$$\begin{aligned} \varphi^* : C(\mathfrak{Y}, \mathfrak{Z}) &\to C(\mathfrak{X}, \mathfrak{Z}) \\ \psi &\mapsto \psi \circ \varphi \end{aligned}$$

Sei nun K ein Körper und $f, g \in K[X,Y]$ Polynome, dann setze $C := V_f(K)$ und $D := V_g(K)$. Weiter sei $\varphi : C \to D$ eine stetige Abbildung, dann Betrachte

$$\begin{array}{ccc} K[X,Y]/I(D) = K[D] & & K[C] = K[X,Y]/I(C) \\ i_D \downarrow & & \downarrow i_C \\ C\big(D, \mathbb{A}^1(K)\big) & \xrightarrow{\varphi^*} & C\big(C, \mathbb{A}^1(K)\big) \end{array}$$

mit

$$\begin{array}{rcl} i_C : K[C] & \to & C\big(D, \mathbb{A}^1(K)\big) \\ p & \mapsto & \Big((a,b) \mapsto p(a,b)\Big) \end{array}$$

Es ist φ genau dann ein Morphismus von Kurven, wenn $\varphi^*\Big(i_D\Big(K[D]\Big)\Big) \subseteq i_C\Big(K[C]\Big)$ ist.

Beweis. Sei φ ein Morphismus von Kurven mit $\varphi_1 = \alpha$ und $\varphi_2 = \beta$ für $\alpha, \beta \in K[X,Y]$. Weiter sei $P \in K[D]$, dann betrachte für $a, b \in C$

$$\begin{array}{rcl} \varphi^*\big(i_D\big(P(X,Y)\big)\big)(a,b) & = & i_D\big(P(X,Y)\big) \circ \big(\varphi_1(a,b), \varphi_2(a,b)\big) \\ & = & P\big(\alpha(a,b), \beta(a,b)\big) \\ & = & i_C\Big(P\big(\alpha(X,Y), \beta(X,Y)\big)\Big)(a,b) \end{array}$$

Folglich ist $P\big(\alpha(X,Y), \beta(X,Y)\big) \in K[C]$. Beweisen wir nun die andere Inplikation, dazu betrachte die X-Koordinate und die Y-Koordinate. Wähle $P(X,Y) := X \in K[D]$. Es gilt:

$$\begin{array}{rcl} \varphi^*\Big(i_D\big(P(X,Y)\big)\Big)(a,b) & = & P\big(\varphi_1(a,b), \varphi_2(a,b)\big) \\ & = & \varphi_1(a,b) \in i_C\big(K[C]\big) \end{array}$$

Also gibt es $\alpha \in K[X,Y]$, so dass für alle $(a,b) \in C$ gilt $\alpha(a,b) = \varphi_1(a,b)$. Mit $P'(X,Y) := Y$ erhalte, dass auch φ_2 durch ein Polynom $\beta(X,Y) \in K[X,Y]$ gegeben ist. □

Bemerkung 11.5 *Sei K ein Körper und $C, D \subseteq \mathbb{A}^2(K)$ seien Kurven. Weiter sei $\varphi : C \to D$ ein Morphismus von Kurven mit $\varphi(a,b) = \big(\alpha(a,b), \beta(a,b)\big)$. Dann ist*

$$\begin{array}{rcccl} \varphi^* : & K[D] & \to & K[C] \\ & P + I(D) & \mapsto & P\Big(\alpha(X,Y), \beta(X,Y)\Big) + I(C) \end{array}$$

ein K-Algebra-Homomorphismus.

Anmerkung Achtung: Die „Pfeilrichtung“ dreht sich um!

Beweis. Wir beweisen hier nur, dass φ^* wohldefiniert ist, denn die (Ring-)Homomorphieeigenschaft rechnet sich leicht nach. Zur Wohldefiniertheit ist zu Zeigen, dass Elemente aus $I(D)$ auf Elemente in $I(C)$ abgebildet werden.
Sei also $P(X,Y) \in I(D)$, dann ist $P\Big(\alpha(a,b), \beta(a,b)\Big) = 0$, denn das Element $\Big(\alpha(a,b), \beta(a,b)\Big)$ liegt in D. Dann ist aber für $(a,b) \in C$ auch

$$P\Big(\alpha(X,Y), \beta(X,Y)\Big)(a,b) = 0$$

also ist $P\Big(\alpha(X,Y), \beta(X,Y)\Big) \in I(C)$ □

Bemerkung 11.6 *Seien K ein Körper, $C, D \subseteq \mathbb{A}^2(K)$ Kurven und $\psi : K[D] \to K[C]$ ein K-Algebra-Homomorphismus. Weiter seien $\alpha, \beta \in K[X,Y]$, so dass $\psi\big(X + I(D)\big) = \alpha(X,Y) + I(C)$ und $\psi\big(Y + I(D)\big) = \beta(X,Y) + I(C)$. Dann definiert*

$$\begin{array}{rccc} \varphi: & C & \to & D \\ & (a,b) & \mapsto & \big(\alpha(a,b), \beta(a,b)\big) \end{array}$$

einen Morphismus von Kurven und es gilt: $\varphi^* = \psi$.

Beweis. Nachrechnen!

12 Singuläre Punkte

Definition 12.1 *(Taylorentwicklung, singulärer Punkt, singuläre Kurve, Tangente)*
Sei K ein Körper und $f \in K[X,Y]$ ein Polynom, dann setze $C := V_f(K)$. Weiter sei $(a,b) \in C$, dann betrachte die ersten Terme der Taylorentwicklung von f:

$$T_f(a,b) := \left.\frac{\partial f}{\partial X}\right|_{(a,b)} \cdot (X-a) + \left.\frac{\partial f}{\partial Y}\right|_{(a,b)} \cdot (Y-b)$$

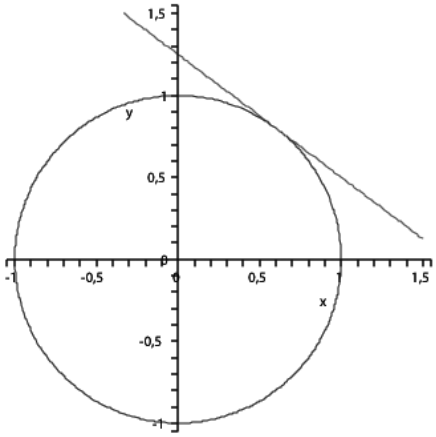
Der Punkt $(a,b) \in C$ heißt singulär, falls $T_f(a,b) = 0$ ist. Andernfalls heißt (a,b) nicht-singulär (oder glatt, regulär)
Sei nun $(a,b) \in C$ regulär, dann heißt die zu $T_f(a,b)$ gehörige Grade ($V_{T_f(a,b)}(K)$) Tangente an C im Punkt (a,b).
Die Kurve C heißt nicht singulär (glatt), falls jeder Punkt in C regulär ist.

Anmerkung Die Tangente an C ist diejenige Grade, die C nahe (a,b) am besten approximiert.

Beispiel 26 *(Tangente an den Einheitskreis)*
Sei $K = \mathbb{Q}$ und $f(X,Y) := X^2 + Y^2 - 1 \in \mathbb{Q}[X,Y]$. Betrachte den Punkt $(\frac{3}{5}, \frac{4}{5})$, dann ist

$$\begin{aligned} T_f(\frac{3}{5}, \frac{4}{5}) &= \left.\frac{\partial f}{\partial X}\right|_{(\frac{3}{5},\frac{4}{5})} \cdot (X - \frac{3}{5}) + \left.\frac{\partial f}{\partial Y}\right|_{(\frac{3}{5},\frac{4}{5})} \cdot (Y - \frac{4}{5}) \\ &= \frac{6}{5} \cdot (X - \frac{3}{5}) + \frac{8}{5} \cdot (Y - \frac{4}{5}) \\ &= \frac{1}{5} \cdot (6X + 8Y - \frac{50}{5}) \\ &= \frac{1}{5} \cdot (6X + 8Y - 10) \end{aligned}$$

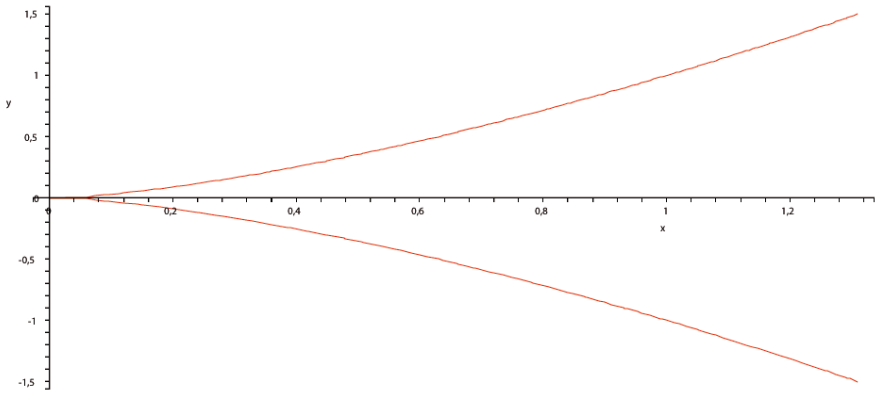
Eine Tangente an den Einheitskreis.



Beispiel 27 *(Singulärer Punkt: „Spitze“)*
Sei $f(X,Y) = Y^2 - X^3$, dann sind die partiellen Ableitungen

$$\frac{\partial f}{\partial X} = -3X^2 \quad \text{und} \quad \frac{\partial f}{\partial Y} = 2Y$$

Beide partiellen Ableitungen verschwinden im Punkt (0,0) , also hat $f(X,Y)$ im Punkt (0,0) eine Singularität.

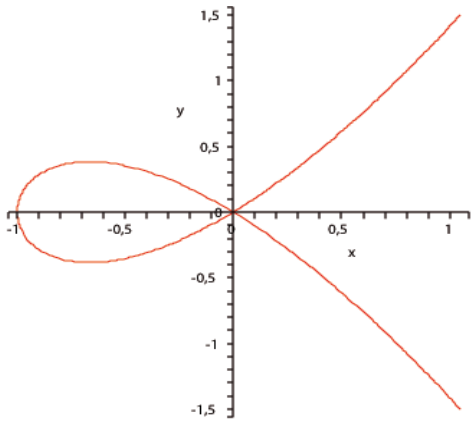


*Diese Art von Singularität heißt „*Spitze*“. Die Tangenten an die beiden Zweige stimmen im Limes gegen Null überein.*

Beispiel 28 *(singulärer Punkt: „gewöhnlicher Doppelpunkt“)*
Sei $f(X,Y) = Y^2 - X^3 - X^2$*, dann sind die partiellen Ableitungen*

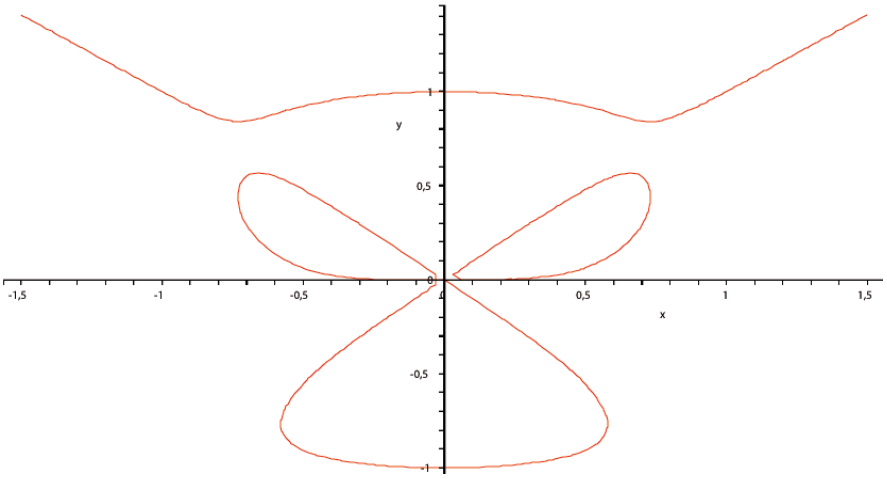
$$\frac{\partial f}{\partial X} = -3X^2 \quad \text{und} \quad \frac{\partial f}{\partial Y} = 2Y$$

Auch hier verschwinden die beiden partiellen Ableitungen im Nullpunkt.



*Diese Art von Singularität heißt „*gewöhnlicher Doppelpunkt*“. Die Tangenten an die beiden Zweige haben in* $(0,0)$ *eine unterschiedliche Steigung.*

Beispiel 29 *(singulärer Punkt)*
$f(X,Y) := Y(Y-X)(Y+X) + X^6 + Y^7$ *hat eine Singularität im Nullpunkt.*



Beispiel 30 *(hyperelliptische Kurven)*
Seien K *ein Körper und* $g(X) \in K[X]$ *ein Polynom, dann heißt die zu* $f(X,Y) := Y^2 - g(X)$ *gehörige Kurve eine „*hyperelliptische Kurve*“. Die partiellen Ableitungen sind:*

$$\frac{\partial f}{\partial X} = -g'(X) \quad \text{und} \quad \frac{\partial f}{\partial Y} = 2Y$$

Also hat $f(X,Y)$ *eine Singularität in* $(x,0)$*, wenn* $g'(x) = 0$*. Weiter gilt, dass* $(x,0) \in V_f(K)$*, also folgt* $g(x) = 0$*. Wir können nun schließen, dass genau dann* $V_f(K)$ *nicht-singulär ist, wenn* $(0,x)$ *ist eine mehrfache Nullstelle von g ist, also genau dann, wenn* $\triangle_g \neq 0$ *ist.*

Motivation Sei K ein algebraisch abgeschlossener Körper und $f(X,Y) \in K[X,Y]$ ein irreduzibles Polynom. Setze $C := V_f(K)$. Im letzten Abschnitt haben wir den Koordinatenring

$$K[C] := {}^{K[X,Y]}\!/_{(f)}$$

und den zugehörigen Quotientenkörper $K(C) := \mathrm{Quot}(K[C])$ definiert. Betrachte

$$\begin{array}{rccc} x: & C & \to & \mathbb{A}^1(K) \\ & (a,b) & \mapsto & a \end{array}$$

Hierzu gehört nach dem vorhergehenden Abschnitt ein K-Algebra-Homomorphismus

$$\begin{array}{rcl} x^*: K[X] & \to & K[C] \\ X & \mapsto & X + (f) \end{array}$$

O.B.d.A. ist x^* injektiv (sonst nimmt die X-Koordinate nur endlich viele Werte an, dann vertausche X und Y). Es gilt $K[X] \subseteq K[C] \subseteq K(C)$. Betrachte nun den ganzen Abschluss von $K[X]$ bzw. $K[C]$ in $K(C)$.
Unser Ziel ist es in den nächsten Abschnitten zu Zeigen, dass $K[C]$ genau dann ganz abgeschlossen ist, wenn C keine Singularitäten hat.

Beispiel 31 *Sei K ein Körper und $f(X,Y) = Y^2 - X^3$ ein Polynom in $K[X,Y]$, weiter sei x^* wie oben injektiv, dann ist $K[C]$ nicht abgeschlossen.*
Beweis. *Im ersten Schritt Behaupten wir, dass $\frac{X}{Y} \in K[C]$ ganz ist über $K[X]$, denn in $K[C]$ gilt*

$$\begin{array}{rcl} 0 & = & Y^2 - X^3 = X^2 \cdot \left(\left(\dfrac{X}{Y} \right)^2 - X \right) \\ \Rightarrow 0 & = & \left(\dfrac{X}{Y} \right)^2 - X \quad \text{in } K(C) \end{array}$$

Es gilt $\frac{X}{Y}$ ist Nullstelle von $T^2 - X \in (K[X])[T]$
Im zweiten Schritt zeigen wir, dass $\mathfrak{X}Y$ kein Element in $K[C]$ ist, denn sonst gäbe es ein Polynom $g(X,Y) \in K[X,Y]$, so dass

$$\frac{Y + (f)}{X + (f)} = g(X,Y) + (f)$$

Es folgte dann, dass $Y = X \cdot g(X,Y) + (f) \in K[C]$, also existierte ein Polynom $h(X,Y) \in K[X,Y]$, so dass

$$Y = X \cdot g(X,Y) + (Y^2 - X^3) \cdot h(X,Y) \ \in K[X,Y]$$

Dies ist jedoch ein Widerspruch.
Aus diesen beiden Schritten folgt nun unmittelbar, das $K[C]$ nicht ganz abgeschlossen in $K(C)$ ist. Weiter gilt, dass $K[\frac{X}{Y}]$ mit $\frac{X}{Y} \in K(C)$ der ganze Abschluss von $K[C]$ in $K(C)$ ist. Auch diese Behauptung beweisen wir in mehreren Schritten:
Zunächst zeigen wir, dass $K[C] \subseteq K[\frac{X}{Y}]$ ist. In $K(C)$ gelten die folgenden Gleichungen: $\left(\frac{X}{Y}\right)^2 = X$ und $\frac{X}{Y} \cdot X = Y$. Die Elemente $X + (f)$ und $Y + (f)$ liegen also in $K[\frac{X}{Y}]$.
Aus der Definition des Koordinatenrings $K[C]$ als Quotientenring von $K[X,Y]$ modulo dem von f erzeugten Ideal folgt unmittelbar, dass $K[C]$ von den Elementen $X + (f)$ und $Y + (f)$ erzeugt wird.

Beim zweiten Schritt ist nichts zu zeigen, denn es ist klar, dass $\mathrm{Quot}\left(K[\frac{X}{Y}]\right) = \mathrm{Quot}(K[C]) = K(C)$ *ist. Weiter gilt:* $K[\frac{X}{Y}]$ *ist isomorph zu einem Polynomring über* K *in einer Variablen, somit ist* $K[\frac{X}{Y}]$ *ein Hauptidealring. Daher ist* $K[\frac{X}{Y}]$ *ganz abgeschlossen.*
Als drittes werden wir nun zeigen, dass $\frac{X}{Y}$ *nicht algebraisch über* K*ist.*
Angenommen, dem wäre so, dann wäre $K[\frac{X}{Y}]$ *eine endliche Körpererweiterung von* K*. Im ersten Schritt haben wir festgestellt, dass* $K[\frac{X}{Y}]$ *den Koordinatenring* $K[C]$ *enthält. Dieser wiederum enthält nach der ersten Behauptung den Polynomring* $K[X]$*. Dies ist ein Widerspruch, denn* X *ist ein transzendentes Element über* K*.*
Zum Schluss betrachten wir noch das Minimalpolynom $F(T) := T^2 - X \in (K[X])[T]$ *von* $\frac{X}{Y}$*.*
Definiere $\tilde{C} := V_F(K)$*, dann ist*

$$K[\tilde{C}] := {}^{K[X,Y]}\!\diagup_{(F)} \cong K[\frac{X}{Y}] \subset K(C)$$

Es gelten folglich die Inklusionen

$$K[X] \subseteq K[C] \subseteq K[\tilde{C}] \subset K(C)$$

und $K[\tilde{C}]$ *ist der ganze Abschluss von* $K[C]$ *in* $K(C)$*.*

Die Verallgemeinerung dieser Motivation ist der folgende Satz 12.2, den wir aber erst später beweisen können:

Satz 12.2 *Sei* K *ein algebraisch abgeschlossener Körper und* $f(X,Y) \in K[X,Y]$ *ein irreduzibles Polynom. Setze* $C := V_f(K)$*. Es gilt:* C *ist genau dann nicht singulär, wenn* $K[C]$ *ganz abgeschlossen ist.*

Kapitel IV

Moduln über Ringen (II)

13 Das Tensorprodukt

In diesem Abschnitt bezeichne R wieder einen, nicht notwendig kommutativen, Ring.

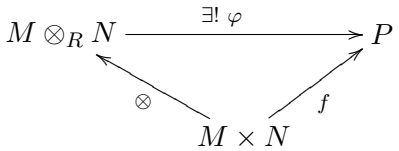
Definition 13.1 *(ausgeglichene Abbildung, - Produkt, Homomorphismus und Tensorprodukt)*
Seien M ein R-Rechtsmodul und N ein R-Linksmodul, sowie P ein $\mathbb{Z}$-Modul. Eine Abbildung $f : M \times N \to P$ heißt ausgeglichen, falls f eine $\mathbb{Z}$-bilineare Abbildung ist, die die folgende Eigenschaft erfüllt.

$$\forall x \in M \ \forall y \in N \ \forall r \in R : \quad f(xr, y) = f(x, ry)$$

In diesem Fall heißt das Paar (P, F) ein ausgeglichenes Produkt von M und N.
Seien (P, f) und (Q, g) zwei ausgeglichene Produkte von M und N. Eine $\mathbb{Z}$-lineare Abbildung $\varphi : P \to Q$ heißt Homomorphismus ausgeglichener Produkte, falls für alle $x \in M$ und für alle $y \in N$ gilt, dass $\varphi\big(f(x, y)\big) = g(x, y)$ ist.
Ein ausgeglichenes Produkt der Moduln M und N heißt Tensorprodukt von M und N über R, mit der Notation $(M \otimes_R N, \otimes)$, falls die folgende universelle Abbildungseigenschaft gilt: Für die ausgeglichenen Produkte (P, f) von M und N gibt es genau einen Homomorphismus

$$\varphi : (M \otimes_R N, \otimes) \to (P, f)$$

von ausgeglichenen Produkten, so dass das folgende Diagramm kommutiert, d.h. $\varphi \circ \otimes = f$.



Anmerkung Solange der Kontext den Ring über dem wir das Tensorprodukt bilden eindeutig bestimmt, vereinfachen wir die Schreibweise von $\otimes_R$ zu $\otimes$.

Satz 13.2 *Seien M, N wie in Definition 13.1 gegeben, dann gilt:*
Das Tensorprodukt $M \otimes N$ existiert und ist bis auf Isomorphie eindeutig.

Beweis. Zunächst konstruieren wir das Tensorprodukt. Setze dazu $F := \mathbb{Z}[M \times N]$ als den freien $\mathbb{Z}$-Modul auf der Menge $M \times N$, d.h. die Elemente von F sind $\mathbb{Z}$-Linearkombinationen mit Symbolen $x \in M$ und $y \in N$. Weiter setze G als den von den Elementen

$$\left\{ \begin{array}{c|c} \begin{array}{c} (x_1 + x_2, y) - (x_1, y) - (x_2, y) \\ (x, y_1 + y_2) - (x, y_1) - (x, y_2) \\ (xr, y) - (x, ry) \end{array} & \begin{array}{c} x, x_1, x_2 \in M \\ y, y_1, y_2 \in N \\ r \in R \end{array} \end{array} \right\}$$

erzeugten $\mathbb{Z}$-Untermodul von F. Definiere

$$\begin{array}{rcl} M \otimes N & := & {}^{F}\!/_{G} \\ \text{und } x \otimes y & := & (x, y) + G = \overline{(x, y)} \end{array}$$

Die zu beweisende Behauptung ist nun:

$$\begin{array}{rcl} \otimes : M \times N & \to & M \otimes N \\ (x, y) & \mapsto & x \otimes y \end{array}$$

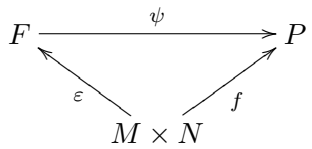
ist eine ausgeglichende Abbildung. Dazu zeigen wir zunächst die $\mathbb{Z}$-Bilinearität. Es genügt diese Eigenschaften für die Erzeuger von $M \otimes N$ zu zeigen.

$$\begin{array}{rcl} x_1 + x_1 \otimes y & := & \otimes\big((x_1 + x_2, y)\big) := (x_1 + x_2, y) + G \\ & = & (x_1, y) + (x_2, y) + G = \otimes(x_1, y) + \otimes(x_2, y) \end{array}$$

Die Linearität in der 2. Variable folgt analog. Betrachte nun die Multiplikation mit Elementen aus R.

$$\begin{array}{rcl} xr \otimes y & := & \otimes(xr, y) = (xr, y) + G \\ & = & (x, ry) + G = \otimes(x, ry) \end{array}$$

Nach dem wir das Tensorprodukt konstruiert haben, müssen wir noch zeigen, dass dieses die universelle Abbildungseigenschaft erfüllt. Hierzu werden wir die uns bereits bekannte universelle Abbildungseigenschaft von freien Moduln verwenden. Sei also ein $\mathbb{Z}$-Modul P vorgegeben, dann betrachte das folgende kommutative Diagramm



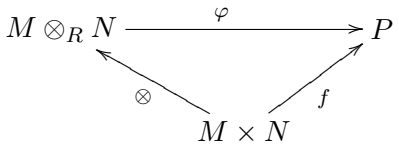
Wir wissen, dass ψ eindeutig bestimmt ist. Betrachte für $x_1, x_2 \in M$ und $y \in N$

$$\begin{array}{rcl} \psi(x_1 + x_2, y) & = & \psi\big(\varepsilon(x_1 + x_2, y)\big) = f(x_1 + x_2, y) \\ & \overset{f \text{ bil.}}{=} & f(x_1, y) + f(x_2, y) \end{array}$$

Folglich ist $(x_1 + x_2, y) - (x_1, y) - (x_2, y) \in \mathrm{Ker}(\psi)$. Analog folgt, dass auch die die anderen Erzeuger von G im Kern von ψ liegen. Somit ist G in $\mathrm{Ker}(\psi)$ enthalten. Definiere nun

$$\begin{array}{rcl} \varphi : {}^{F}\!/_{G} & \to & P \\ a + G & \mapsto & \psi(a) \end{array}$$

damit erhalten wir das gewünschte, kommutative Diagramm wie folgt



Die Eindeutigkeit von φ ist durch $f(x, y)$ bereits gegeben.
Die Eindeutigkeit bis auf Isomorphie von $M \otimes N$ folgt mit dem gleichen Argument wie bei freien Moduln (Vergleiche Satz 2.12), direkten Summen (Vergleiche Satz 2.7) und direkten Produkten (Vergleiche Satz 2.2) direkt aus der universellen Abbildungseigenschaft. □

Beispiel 32 *(Tensorprodukt)*
(T1) *Seien $n, m \in \mathbb{N}$ Teilerfremd, dann gilt*

$$T := \mathbb{Z}/_{m\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}/_{n\mathbb{Z}} = \underline{0}$$

Da n und m Teilerfremd sind, finden wir eine Darstellung der 1, so dass $1 = am + bn$ mit $a, b \in \mathbb{Z}$. Sei nun $r \otimes s \in T$, dann betrachte

$$\begin{aligned} r \otimes s &= r \cdot 1 \otimes s = r(am + bn) \otimes s \\ &= ram \otimes s + rbn \otimes s = ram \otimes s + r \otimes bns \\ &= 0 \otimes s + r \otimes 0 \qquad \text{denn } \bar{r} \cdot \bar{m} = 0 \bmod m \end{aligned}$$

Es gilt $0 \otimes s = 0 + 0 \otimes s = 0 \otimes s + 0 \otimes s$, ziehen wir nun $0 \otimes s$ auf beiden Seiten der Gleichung ab erhalten wir $0 = 0 \otimes s$. Betrachten wir nun ein allgemeines Element aus T, so betrachten wir eine $\mathbb{Z}$-Linearkombination von Nullen, also folgt die Behauptung.

(T2) *Sei G eine abelsche Gruppe und $n \in \mathbb{N}$ derart, dass $nG = \underline{o}$ ist. Mit anderen Worten: G ist ein $\mathbb{Z}$-Torsionsmodul und $n \in Ann(G)$. Es gilt:*

$$T := \mathbb{Q} \otimes_{\mathbb{Z}} G = \underline{0}$$

Denn für $\frac{r}{s} \in \mathbb{Q}$ und $a \in G$ gilt

$$\frac{r}{s} \otimes a = \frac{r}{ns} \cdot n \otimes a = \frac{r}{ns} \otimes n \cdot a = \frac{r}{ns} \otimes 0$$

(T3) *Sei G eine abelsche Gruppe, dann ist $T := \mathbb{Q} \otimes_{\mathbb{Z}} G$ ein $\mathbb{Q}$-Vektorraum via*

$$\frac{r}{s}\left(\frac{t}{u} \otimes a\right) := \frac{rt}{su} \otimes a \quad \text{mit } \frac{r}{s}, \frac{t}{u} \in \mathbb{Q}, a \in G$$

(T4) *Sei S ein Ring und $\varphi : R \to S$ ein Ringhomomorphismus. Weiter sei N ein R-Linksmodul, dann ist $S \otimes_R N$ ein S-Linksmodul via*

$$s(t \otimes n) := st \otimes n \quad \text{mit } s, t \in S, n \in N$$

Dieser heißt Skalar- oder Konstantenerweiterung bzw. Basiswechsel.

Bemerkung 13.3 *Seien $M, \tilde{M}$ zwei R-Rechtsmoduln und $f \in \mathrm{Hom}_R(M, \tilde{M})$. Weiter seien $N, \tilde{N}$ zwei R-Linksmoduln mit $g \in \mathrm{Hom}_R(N, \tilde{N})$. Dann gibt es einen Homomorphismus*

$$f \otimes g : M \otimes_R N \longrightarrow \tilde{M} \otimes_R \tilde{N}$$

Beweis. Betrachte das erweiterte Diagramm der universellen Abbildungseigenschaft:

$$\begin{array}{ccc} M \otimes N & \overset{f \otimes g}{\dashrightarrow} & \tilde{M} \otimes \tilde{N} \\ {\scriptstyle\otimes}\uparrow & \overset{h}{\nearrow} & \uparrow{\scriptstyle\otimes} \\ M \times N & \xrightarrow[f,g]{} & \tilde{M} \times \tilde{N} \end{array}$$

Definiere $h := \otimes \circ (f, g)$, dann ist h eine ausgeglichene Abbildung. Die Existenz von $f \otimes g$ folgt nun sofort aus der universellen Abbildungseigenschaft. □

Bemerkung 13.4 *Seien M, M_1, M_2 drei R-Rechtsmoduln und N, N_1, N_2 drei R-Linksmoduln mit*

$$M \xrightarrow{f} M_1 \xrightarrow{\tilde{f}} M_2 \text{ und } N \xrightarrow{g} N_1 \xrightarrow{\tilde{g}} N_2$$

Dann gilt:

$$(\tilde{f} \otimes \tilde{g}) \circ (f \otimes g) = (\tilde{f} \circ f) \otimes (\tilde{g} \otimes g)$$

Beweis. Für alle $x \otimes y \in M \otimes N$ gilt:

$$\begin{aligned} \tilde{f} \otimes \tilde{g}\Big(f \otimes g(x \otimes y)\Big) &= \tilde{f} \otimes \tilde{g}\Big(f(x) \otimes g(x)\Big) \\ &= \tilde{f}\big(f(x)\big) \otimes \tilde{g}\big(g(x)\big) \end{aligned}$$

□

Folgerung 13.5 *Seien $M, \tilde{M}$ zwei R-Rechtsmoduln und $f \in \mathrm{Hom}_R(M, \tilde{M})$. Weiter seien $N, \tilde{N}$ zwei R-Linksmoduln mit $g \in \mathrm{Hom}_R(N, \tilde{N})$. Dann ist das folgende Diagramm kommutativ:*

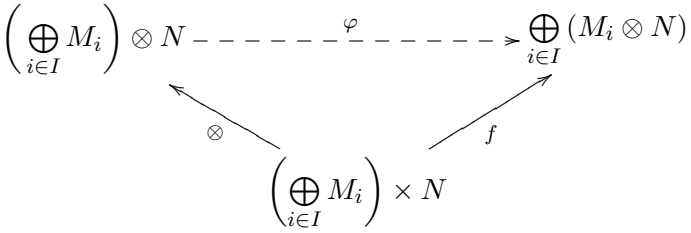
$$\begin{array}{ccccc} & & \tilde{M} \otimes N & & \\ & {\scriptstyle f \otimes id_N}\nearrow & & \searrow{\scriptstyle id_{\tilde{M}} \otimes g} & \\ M \otimes N & & \xrightarrow{f \otimes g} & & \tilde{M} \otimes \tilde{N} \\ & {\scriptstyle id_M \otimes g}\searrow & & \nearrow{\scriptstyle f \otimes id_{\tilde{N}}} & \\ & & M \otimes \tilde{N} & & \end{array}$$

Beweis. Folgt direkt aus Bemerkung 13.4. □

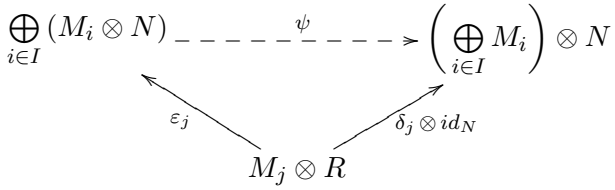
Bemerkung 13.6 *Sei I eine Menge, für $i \in I$ seien M_i R-Rechtsmoduln. Weiter sei N ein R-Linksmodul. Dannn gibt es genau einen Isomorphismus*

$$\begin{aligned} \varphi : \left(\bigoplus_{i \in I} M_i\right) \otimes N &\xrightarrow{\sim} \bigoplus_{i \in I} (M_i \otimes N) \\ (x_i)_{i \in I} \otimes y &\mapsto (x_i \otimes y)_{i \in I} \end{aligned}$$

Beweis. Als erstes schließen wir die Existenz von φ aus der universellen Abbildungseigenschaft des Tensorproduktes. Betrachte dazu das folgende Diagramm:



Definiere f durch $f\left((x_i)_{i\in I}, y\right) := (x_i \otimes y)_{i\in I}$, dann ist f eine ausgeglichene Abbildung. Die Existenz von φ folgt nun sofort. Im zweiten Schritt nutzen wir die universelle Abbildungseigenschaft der direkten Summe aus, um die Umkehrabbildung von φ zu bestimmen. Betrachte dazu dieses Diagramm:



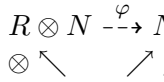
Hierbei sind ε_j die Einbettung von $M_j \otimes N$ auf die j-te Komponente von $\bigoplus(M_i \otimes N)$ und δ_j die Einbettung von M_j auf die j-te Komponente von $\bigoplus M_i$. Nach der universellen Abbildungseigenschaft existiert genau ein ψ mit $\psi \circ \varepsilon_j = \delta_j \otimes id_N$. Zuletzt zeigt man durch Nachrechnen $\varphi = \psi^{-1}$. □

Bemerkung 13.7 *Sei N ein R-Linksmodul dann definiert die Abbildung*

$$\begin{aligned} \varphi : R \otimes N &\to N \\ r \otimes n &\mapsto rn \end{aligned}$$

Einen Isomorphismus von R-Linksmoduln via Skalarerweiterung auf $R \otimes N$.

Beweis.



Betrachte das nebenstehende Diagramnm. Mit $f(r,n) := rn$ existiert φ mit der offensichtlichen Umkehrabbildung:
$\psi : N \ni n \mapsto 1 \otimes n \in R \otimes N$ □

Anmerkung Die Bemerkungen 13.6 und 13.7 gelten mit einem analogen Beweis auch in den folgenden Formen:

$$M \otimes \left(\bigoplus_{i\in I} N_i\right) \cong \prod_{i\in I} (M \otimes N_i)$$

und

$$\varphi : M \otimes R \ni m \otimes r \mapsto mr \in M$$

Beispiel 33 *Sei G eine endlich erzeugte abelsche Gruppe. Dann ist*

$$\dim_{\mathbb{Q}} \left(\mathbb{Q} \otimes_{\mathbb{Z}} G\right) \;=\; \mathrm{rg}(G) := r$$

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen sind G und $\mathbb{Z}^r \bigoplus G_{tor}$ Isomorph. Somit gilt die folgende Isomorphie

$$\begin{aligned}
\mathbb{Q} \otimes_{\mathbb{Z}} G &\cong \mathbb{Q} \otimes_{\mathbb{Z}} \left(\Big(\bigoplus_{i=1}^{r} \mathbb{Z} \Big) \bigoplus G_{tor} \right) \\
&\cong \Big(\bigotimes_{i=1}^{r} (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}) \Big) \;\bigoplus\; \Big(\mathbb{Q} \otimes_{\mathbb{Z}} G_{tor} \Big) \\
&\cong \bigoplus_{i=1}^{r} \mathbb{Q} \bigoplus \underline{0} \quad \cong \quad \bigoplus_{i=1}^{r} \mathbb{Q}
\end{aligned}$$

Bemerkung 13.8 *Sei R ein kommutativer Ring und M, N seien R-Moduln, dann gilt*

$$M \otimes N \cong N \otimes M$$

Beweis. Übung!

Beispiel 34 *Sei K ein Körper und L/K eine Körpererweiterung, dann ist*

$$L \otimes_K K[X] \;\cong\; L[X]$$

Bemerkung 13.9 *Seien M ein R-Rechtsmodul und N ein R-Linksmodul weiter sei P ein $\mathbb{Z}$-Modul. Fasse $\mathrm{Hom}_{\mathbb{Z}}(N, P)$ als R-Rechtsmodul auf via $(f, r) := f(rn)$ für $f \in \mathrm{Hom}_{\mathbb{Z}}(N, P), r \in R$ und $n \in N$. Dann gibt es einen Isomorphismus, so dass*

$$\mathrm{Hom}_R \Big(M,\, \mathrm{Hom}_{\mathbb{Z}}(N, P) \Big) \;\cong\; \mathrm{Hom}_{\mathbb{Z}} \left(M \otimes N, P \right)$$

Beweis. (ohne Rechnungen)
Zunächst muss nachgerechnet werden, dass es eine Bijektion zwischen den Mengen

$$\begin{aligned}
A := \{\, f : M \times N \to P \mid f \text{ausgeglichen} \,\} \quad &\leftrightarrow \quad \mathrm{Hom}_R \left(M, \mathrm{Hom}_{\mathbb{Z}}(N, P) \right) \\
f \qquad &\mapsto \quad \Big(m \mapsto \big(n \mapsto f(m, n) \big) \Big) \\
\Big((m, n) \mapsto \big(g(m) \big)(n) \Big) \quad &\leftarrow\!\shortmid \quad g
\end{aligned}$$

gibt, dann gibt die universelle Abbildungseigenschaft des Tensorproduktes genau eine Bijektion von A und $\mathrm{Hom}_{\mathbb{Z}}(M \otimes N, P)$. Nun kann nachgerechnet werden, dass diese Bijektion ein Isomorphismus ist. □

Beispiel 35 *(Skalarerweiterung eines freien Moduls)*
Seien R, S Ringe und I eine Menge, dann bezeichne F den freien R-Modul auf der Menge I. Wir wissen, dass

$$F = \bigoplus_{i \in I} R$$

gilt. Sei weiter $\varphi \in \mathrm{Hom}_R(R, S)$, dann fasse S als R-Modul auf via $rs := \varphi(r) \cdot s$. Es gilt

$$S \otimes_R F = S \otimes_R \left(\bigoplus_{i \in I} R \right) \overset{13.6}{\cong} \bigoplus_{i \in I} (S \otimes_R R) \overset{13.7}{\cong} \bigoplus_{i \in I} S$$

Mit anderen Worten: $S \otimes_R F$ ist freier S-Modul auf der Menge I.

Bemerkung 13.10 *Es gelten*
(a) *Sei N ein R-Linksmodul und sei $M_1 \to M_2 \to M_3 \to 0$ eine exakte Sequenz von R-Rechtsmoduln, dann ist auch*

$$M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

eine exakte Sequenz von $\mathbb{Z}$-Moduln.
(b) *Sei M ein R-Rechtsmodul und sei $N_1 \to N_2 \to N_3 \to 0$ eine exakte Sequenz von R-Linksmoduln, dann ist auch*

$$M \otimes N_1 \to M \otimes N_2 \to M \otimes N_3 \to 0$$

eine exakte Sequenz von $\mathbb{Z}$-Moduln.

Beweis. zu (a):
Nach Satz 1.10 gilt für alle $\mathbb{Z}$-Moduln P

$$0 \to \mathrm{Hom}_R\Big(M_3, \mathrm{Hom}_{\mathbb{Z}}(N, P)\Big) \to \mathrm{Hom}_R\Big(M_2, \mathrm{Hom}_{\mathbb{Z}}(N, P)\Big) \to \mathrm{Hom}_R\Big(M_1, \mathrm{Hom}_{\mathbb{Z}}(N, P)\Big)$$

ist eine exakte Sequenz. Mit Bemerkung 13.9 erhalten wir hieraus die exakte Sequenz

$$0 \to \mathrm{Hom}_{\mathbb{Z}}\big(M_3 \otimes N, P\big) \to \mathrm{Hom}_{\mathbb{Z}}\big(M_2 \otimes N, P\big) \to \mathrm{Hom}_{\mathbb{Z}}\big(M_1 \otimes N, P\big)$$

In einer Übungsaufgabe wurde gezeigt, dass die Umkehrung von Satz 1.10 ebenfalls gilt, somit ist

$$M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

eine exakte Sequenz. Der Beweis von (b) erfolgt analog mit vertauschten Rollen. □

Definition 13.11 *(Flache und treu-flache Moduln)*
Ein R-Rechtmodul M heißt flach, falls für alle injektiven R-Homomorphismen $\varphi : N_1 \hookrightarrow N_2$ von R-Linksmoduln der induzierte Homomorphismus

$$id_M \otimes \varphi : M \otimes N_1 \to M \otimes N_2$$

auch injektiv ist. Entsprechend heißt ein R-Linksmodul N flach, falls für alle injektiven R-Homomorphismen $\psi : M_1 \hookrightarrow M_2$ von R-Rechtsmoduln der induzierte Homomorphismus $id_N \otimes \psi$ auch injektiv ist.
Ein R-Rechtsmodul M heißt treu-flach, falls M flach ist und die Injektivität aller R-Homomorphismen $\varphi : N_1 \hookrightarrow N_2$ von R-Linksmoduln aus der Injektivtät von $id_M \otimes \varphi$ folgt.
Entsprechend heißt ein R-Linksmodul N treu-flach.

Beispiel 36 *(Flache und treu-flache Moduln)*
1) Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist flach:
$G := \mathbb{Z}^r \bigoplus G_{tor}$ und $H := \mathbb{Z}^s \bigoplus H_{tor}$ seien $\mathbb{Z}$-Moduln und $\varphi : G \hookrightarrow H$ sei ein injektiver $\mathbb{Z}$-Homomorphismus, dann gilt

$$\begin{array}{ccc} \mathbb{Q} \otimes_{\mathbb{Z}} H & \longrightarrow & \mathbb{Q} \otimes_{\mathbb{Z}} G \\ \downarrow \wr & & \downarrow \wr \\ \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^s & \longrightarrow & \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^r \\ \downarrow \wr & & \downarrow \wr \\ \mathbb{Q}^s & \longrightarrow & \mathbb{Q}^r \end{array}$$

ist injektiv, da $\varphi(\mathbb{Z}^s) \subseteq \mathbb{Z}^r$ gilt.

2) $\mathbb{F}_p$ ist als $\mathbb{Z}$-Modul nicht flach:
Sei p eine Primzahl, dann ist

$$\begin{array}{rccc} \cdot p : \mathbb{Z} & \to & \mathbb{Z} \\ z & \mapsto & z \cdot p \end{array}$$

injektiv aber $\cdot p \otimes id_{\mathbb{F}_p}$ ist die Nullabbildung, denn

$$\cdot p \otimes id_{\mathbb{F}_p}\big(z \otimes x\big) = (zp \otimes x) = (z \otimes px) = (z \otimes 0) = (z \otimes 0 \cdot 0) = (0 \otimes 0)$$

Bemerkung 13.12 *(Tensorieren mit flachen Moduln erhält Exaktheit)*
(a) Sei M ein R-rechtsmodul, genau dann erhält

$$M \otimes_R \cdot$$

exakte Sequenzen, wenn M flach ist. Das heißt ist $0 \to N_1 \to N_2 \to N_3 \to 0$ eine exakte Sequenz so folgt genau dann, dass $0 \to M \otimes N_1 \to M \otimes N_2 \to M \otimes N_3 \to 0$ exakt ist, wenn M flach ist.
(b) Sei N ein R-Linksmodul, genau dann erhält

$$\cdot \otimes_R N$$

exakte Sequenzen, wenn N flach ist.

Beweis. Diese Bemerkung gilt unmittelbar nach Bemerkung 13.10 und Definition 13.11. □

Bemerkung 13.13 *Es gelten (a) Ist M ein R-Modul und $\mathfrak{a} \lhd R$ ein Ideal, dann gilt*

$$M \otimes_R {}^{R}\!/_{\mathfrak{a}} \cong {}^{M}\!/_{M\mathfrak{a}}$$

(b) Sei M ein flacher R-Modul. M ist genau dann treu-flach, wenn für alle R-Moduln $N \neq 0$ gilt

$$M \otimes_R N \neq 0$$

Beweis. zu (a):
Nach dem Homomorphiesatz ist

$$0 \to \mathfrak{a} \to R \to {}^{R}\!/_{\mathfrak{a}} \to 0$$

eine exakte Sequenz. Mit Bemerkung 13.10 ist dann auch

$$M \otimes \mathfrak{a} \xrightarrow{\psi} M \otimes R \cong M \xrightarrow{\varphi} M \otimes {}^{R}\!/_{\mathfrak{a}} \to 0$$

eine exakte Sequenz. Dies heißt, dass insbesondere $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$ ist. Es gilt

$$\psi : M \otimes \mathfrak{a} \to M \otimes R \cong M$$

und $\mathrm{Im}(\psi) \cong M\mathfrak{a}$. Aus dem Homomorphiesatz folgt nun die Behauptung.
zu (b):
Sei M treu-flach, dann betrachte $N \to 0$. Falls $M \otimes N \to M \otimes 0 \to 0$ injektiv ist, dann ist - wegen der Treuflachheit - auch $N \to 0$ und somit folgt $N = 0$.
Sie nun für alle $N \neq 0$ das Tensorprodukt $M \otimes N \neq 0$ und sei weiter $\varphi : N_1 \to N_2$ ein R-Homomorphismus von R-Linksmoduln, dann definiere $K := \mathrm{Ker}(\varphi)$ und betrachte die folgende exakte Sequenz

$$0 \to K \to N_1 \xrightarrow{\varphi} N_2$$

Da M flach ist, ist nach Bemerkung 13.12 auch

$$0 \to M \otimes K \to M \otimes N_1 \xrightarrow{id_M \otimes \varphi} M \otimes N_2$$

eine exakte Sequenz. Ist nun $id_M \otimes \varphi$ injektiv, dann folgt, dass $M \otimes K = 0$ ist. Nach Voraussetzung ist dann $K = 0$, also ist φ injektiv. □

Bemerkung 13.14 *Sei N ein flacher R-Modul, genau dann ist N treu-flach, wenn für alle Maximalideale $P \lhd R$ gilt $PN \neq N$.*

Beweis. Sei N treuflach, dann betrachte die exakte Sequenz

$$0 \to P \to R \to {}^{R}\!/_{P} \to 0$$

Da N treu-flach - also insbesondere flach - ist, ist auch

$$0 \to P \otimes N \xrightarrow{\alpha} R \otimes N \cong N \xrightarrow{\beta} {}^{R}\!/_{P} \otimes N \to 0$$

eine exakte Sequenz ist. Da α injektiv ist, folgt

$$P \otimes N \cong PN$$

Wäre nun $PN = N$, dann wäre nach Bemerkung 13.13 (a) der Modul

$${}^{N}\!/_{PN} \cong {}^{R}\!/_{P} \otimes N = 0$$

und wir könnten schließen, dass dann ${}^{R}\!/_{P}$ der Nullmodul ist. Dies ist aber ein Widerspruch, da P nach Voraussetzung ein Maximalideal und somit ungleich R ist.
Sei nun $PN \neq N$ für alle Maximalideale $P \lhd R$. Für alle echten Ideale $\mathfrak{a} \lhd R$ gilt dann $\mathfrak{a}N \neq N$, da jedes Ideal in einem Maximalideal enthalten ist. Weiter ist dann für alle echten Ideale $\mathfrak{a} \lhd R$ der Modul ${}^{N}\!/_{\mathfrak{a}N}$ nicht der Nullmodul. Sei nun M ein beliebiger R-Modul mit der Eigenschaft, dass $M \otimes N = 0$ ist. Wir wollen nun Teil (b) von Bemerkung 13.13 anwenden. Dazu müssen wir zeigen,

dass M der Nullmodul ist. Nehmen wir nun an, dies wäre nicht der Fall, dann wähle ein $0 \neq m \in M$ und definiere

$$\begin{aligned} \varphi : R &\to M \\ r &\mapsto mr \end{aligned}$$

dann ist der Kern von φ das Annulatorideal $\mathrm{Ann}_R(m) \lhd R$ von m ein echtes Ideal in R. Definiere nun $M' := mR = \mathrm{Im}(\varphi)$, dies ist nicht der Nullmodul, denn $1_R \cdot m$ ist nicht 0, weiter gilt nach dem Homomorphiesatz

$$M' \cong {}^{R}\!/_{\mathrm{Ann}_R(m)}$$

Es gilt

$$M' \otimes N \cong {}^{R}\!/_{\mathrm{Ann}_R(m)} \otimes N \cong {}^{N}\!/_{\mathrm{Ann}_R(m) \cdot N} \neq 0$$

Betrachte die Inklusionskette $0 \hookrightarrow M' \hookrightarrow M$, dann gilt wegen der Flachheit von N auch folgende Inklusionskette $0 \hookrightarrow M' \otimes N \hookrightarrow M \otimes N$ also ist $M \otimes N$ nicht der Nullmodul, womit wir einen Widerspruch haben. □

Bemerkung 13.15 *Seien M_i für $i \in I$ R-Rechtsmoduln, dann gilt*

$$M_i \text{ flach} \iff \bigoplus_{i \in I} M_i \text{ flach}$$

Beweis. Seien N_1, N_2 zwei R-Linksmoduln, und $\varphi : N_1 \hookrightarrow N_2$ ein injektiver R-Homomorphismus. Betrachte das folgende, kommutative Diagramm:

$$\begin{array}{ccc} \left(\bigoplus_{i \in I} M_i\right) \otimes_R N_1 & \xrightarrow{id_{\bigoplus M_i} \otimes \varphi} & \left(\bigoplus_{i \in I} M_i\right) \otimes_R N_2 \\ \downarrow \wr & & \downarrow \wr \\ \bigoplus_{i \in I} \left(M_i \otimes N_1\right) & \xrightarrow{id_{M_i} \otimes \varphi} & \bigoplus_{i \in I} \left(M_i \otimes N_2\right) \end{array}$$

Hiernach gilt:

$$\begin{aligned} \bigoplus_{i \in I} M_i \text{ flach} &\Leftrightarrow id_{\bigoplus M_i} \otimes \varphi \text{ injektiv} \\ &\Leftrightarrow \forall\, i \in I \quad id_{M_i} \otimes \varphi \text{injektiv} \\ &\Leftrightarrow \forall\, i \in I \quad M_i \text{ flach} \end{aligned}$$

□

Satz 13.16 *Es gelten*
(a) Projektive Moduln sind flach.
(b) Freie Moduln, die nicht der Nullmodul sind, sind treuflach.

Beweis. Zunächst können wir feststellen, dass Freie Moduln flach sind, denn nach Bemerkung 13.7 ist R als R-Modul flach und Freie Moduln sind direkte Simmen von R. Nach Bemerkung 13.15 sind direkte Summen flach, wenn alle Komponenten flach sind. Nun sei P ein projektiver R-Modul. Nach

Satz 2.16 gibt es einen R-Modul X, so dass $X \prod P$ ein freier Modul ist. Mit Bemerkung 13.15 ist P dann ein flacher Modul. Betrachte

$$F := \bigoplus_{i \in I} R \qquad \text{mit } I \neq R$$

Nach obiger Überlegung ist F als freier R-Modul flach. Sei nun $N \neq 0$ ein R-Modul, dann ist

$$F \otimes N = \left(\bigoplus_{i \in I} R \right) \otimes N = \bigoplus_{i \in I} \left(R \otimes N \right) = \bigoplus_{i \in I} N \neq 0$$

Nach Teil (b) der Bemerkung 13.13 ist F dann treu-flach. □

Folgerung 13.17 *Seien M ein flacher, sowie T ein treu-flacher R-Modul, dann ist $M \bigoplus T$ ein treu-flacher R-Modul.*

Beweis:
Nach Bemerkung 13.15 ist $M \otimes T$ ein flacher R-Modul. Sei N ein beliebiger R-Modul, mit $N \neq 0$. Nach Voraussetzung ist T treu-flach und mit Bemerkung 13.13 ist dann $N \otimes T \neq 0$, also gilt:

$$N \otimes \left(M \bigoplus T \right) \cong \left(N \otimes M \right) \bigoplus \left(N \otimes T \right) \neq 0$$

□

Satz 13.18 *Sei R ein kommutativer, lokaler Ring und M ein R-Modul, dann sind äquivalent:*
- M ist ein freier Modul.
- M ist ein projektiver Modul.
- M ist ein flacher Modul.

Beweis. Nach Satz 2.16 sind freie Moduln projektiv, mit Teil (a) von Satz 13.16 sind projektive Moduln flach und vermittels *Nakayanas Lemma* und dem *Schlangenlemma* (beide waren Übungsaufgaben) folgt aus der Flachheit eines Moduls dessen Freiheit. □

Bemerkung 13.19 *(Assoziativität des Tensorproduktes)*
Seien S, R Ringe, M ein R-Rechtsmodul und P ein S-Lnksmodul weiter sei N ein R-Linksmodul der gleichzeitig ein S-Rechtsmodul ist, mit der Eigenschaft, dass für alle $r \in R, s \in S, n \in N$ gilt $(rn)s = r(ns)$.
Fasse $R \otimes_R N$, via $(m \otimes n)s := m \otimes ns$, als S-Rechtsmodul und $N \otimes_S P$, via $r(n \otimes p) := rn \otimes p$, als R-Linksmodul auf. Dann gilt:

$$\Big(M \otimes_R N \Big) \otimes_S P \cong M \otimes_R \Big(N \otimes_S P \Big)$$

Beweis. Übung!

Definition und Satz 13.20 *(Treu-flacher Ringhomomorphismus)*
Seien R, S Ringe. Ein Ringhomomorphismus $\varphi : R \to S$ heißt (treu-)flach, falls S als R-Modul (treu-)flach ist.

(a) *Sei $\varphi : R \to S$ (treu-)flacher Ringhomomorphismus und M ein (treu-) flacher S-Modul. Fasse M als R-Modul auf, via $r \cdot m := \varphi(r) \cdot m$ für $r \in R$ und $m \in M$. Dann ist M ein (treu-)flacher R-Modul*

(b) *Sei $\varphi : R \to S$ ein Ringhomomorphismus und M ein (treu-)flacher R-Modul, dann ist $S \otimes_R M$ ein (treu-)flacher S-Modul.*

Beweis. zu (a):
Sei $\phi : N \hookrightarrow N'$ ein injektiver Homomorphismus von R-Moduln. Da nach Voraussetzung φ flach ist, ist $id_S \otimes \phi : S \otimes_R N \hookrightarrow S \otimes_R N'$ ein injektiver Homomorphismus von S-Moduln und weil M ein flacher Modul ist, ist auch

$$M \otimes_S \Big(S \otimes_R N\Big) \hookrightarrow M \otimes_S \Big(S \otimes_R N'\Big)$$

ein Injektiver Homomorphismus. Mit der Assoziativität des Tensorproduktes[1] folgt die Injektivität von

$$\Big(M \otimes_S \Big) \otimes_R N \hookrightarrow \Big(M \otimes_S S\Big) \otimes_R N'$$

Nach Folgerung 13.17 gilt, dass $M \otimes_S S \cong M$ ist, und somit folgt schließlich die Injektivität von

$$M \otimes_R N \hookrightarrow M \otimes_R N'$$

Sind φ und M treu-flach, dann lies die obige Argumentation rückwerts.
zu (b):
Sei nun $\phi : N \hookrightarrow N'$ ein injektiver Homomorphismus von S-Moduln, dann folgt aus der Flachheit von M, dass

$$N \otimes_R M \hookrightarrow N' \otimes_R M$$

eine injektive Abbildung ist. Mit Bemerkung 13.7 folgt die Isomorphie der Moduln $(N \otimes_S S) \otimes_R M$ und $N \otimes_R M$. Mit Bemerkung 13.7 und der Assoziativität der Tensorprodukte können wir nun auf die Injektivität von

$$N \otimes_S \Big(S \otimes_R M\Big) \hookrightarrow N' \otimes_S \Big(S \otimes_R M\Big)$$

schließen. Zum Beweis der Treuflachheit lies die obigen Schritte rückwerts. □

Definition und Satz 13.21 *(Lokalisierung von Moduln I)*
Sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge von R, weiter sei M ein R-Modul, dann definiert

$$(m, s) \sim (m', s') \ :\Leftrightarrow\ \exists t \in S :\ t(s'm - sm') = 0$$

eine Äquivalenzrelation auf $M \times S$. Die zugehörigen Äquivalenzklassen werden mit $\frac{m}{s}$ und die Menge dieser mit $S^{-1}M := {}^{M \times S}\!/_{\sim}$ bezeichnet. Weiter ist $S^{-1}M$ ein $S^{-1}R$ Modul via

$$\frac{r}{s} \cdot \frac{m}{s'} := \frac{rm}{ss'} \quad \text{und} \quad \frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'} \qquad \text{für } r \in R;\ s, s' \in S;\ m, m' \in M$$

Außerdem ist

$$\begin{array}{rccc} \mu_S : & M & \to & S^{-1}M \\ & m & \mapsto & \dfrac{m}{1} \end{array}$$

ein R-Modulhomomorphismus mit $\mathrm{Ker}(\mu_S) = \{m \in M | S \cap \mathrm{Ann}(m) \neq \varnothing\}$

[1] Assoziativität des Tensorproduktes nach Bemerkung 13.19

Beweis. Das Nachrechnen der Äquivalenzklassen-, Modul-, und Homomorphieeigenschaften erfolgt ähnlich wie beim Nachweis der Eigenschaften von lokalen Ringen. □

Definition 13.22 *(Lokalisierung von Moduln II)*

- $S^{-1}M$ *heißt Quotientenmodul von* M *bzgl.* S.
- *Sei* $\mathfrak{p} \lhd R$ *ein Primideal. Setze* $S := R\backslash\{\mathfrak{p}\}$, *dann heißt* $M_{\mathfrak{p}} := S^{-1}M$ *die Lokalisierung von* M *bei* $\mathfrak{p}$.

Bemerkung 13.23 *Sei* R *ein kommutativer Ring und* M, N *seien* R*-Moduln. Es seien weiter* $S \subset R$ *eine multiplikativ abgeschlossene Teilmenge von* R *und* $\varphi : M \to N$ *ein* R*-Homomorphismus.*
(a) Dann ist folgende Abbildung ein $S^{-1}R$*-Homomorphismus:*

$$\begin{array}{rcl} \varphi_S : S^{-1}M & \to & S^{-1}N \\ \dfrac{m}{s} & \mapsto & \dfrac{\varphi(m)}{s} \end{array}$$

(b) Ist φ *injektiv (bzw. surjektiv), so ist auch* φ_S *injektiv (bzw. surjektiv).*

Beweis. Zu (a): Nachrechnen der Wohldefiniertheit
Zu (b): Sei φ injektiv, dann betrachte

$$\begin{array}{rcl} \varphi_S\left(\dfrac{m}{s}\right) & := & \dfrac{\varphi(m)}{s} = \dfrac{0}{1} \\ & \Rightarrow & \exists\, t \in S :\ t \cdot \varphi(m) = 0 \\ & \Rightarrow & \varphi(tm) = 0 \Rightarrow tm = 0 \\ & \Rightarrow & \dfrac{m}{s} = \dfrac{0}{1} \end{array}$$

somit ist φ_S injektiv. Sei φ nun surjektiv und $\frac{n}{s} \in S^{-1}N$ gegeben. Nach Voraussetzung gibt es ein $m \in M$, so dass $\varphi(m) = n$ ist. es folgt

$$\varphi_S\left(\frac{m}{s}\right) = \frac{\varphi(m)}{s} = \frac{n}{s}$$

somit ist φ_S surjektiv. □

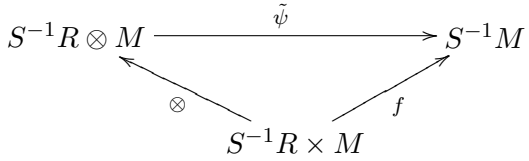
Bemerkung 13.24 *Seien* R *ein kommutativer Ring,* $S \subset R$ *eine multiplikativ abgeschlossene Teilmenge von* R *und* M *ein* R*-Modul, dann ist*

$$\begin{array}{rcl} \psi : S^{-1}M & \to & S^{-1}R \otimes M \\ \dfrac{m}{s} & \mapsto & \dfrac{r}{s} \otimes m \end{array}$$

ein $S^{-1}R$*-Isomorphismus.*

Beweis. In zwei Schritten:
1) Nachrechnen, dass ψ ein $S^{-1}R$-Homomorphismus ist.

2) Benutze die universelle Abbildungseigenschaft des Tensorproduktes um eine Umkehrabbildung $\tilde{\psi}$ zu erhalten



Definiere hierzu eine ausgeglichene Abbildung f durch

$$f\left(\left(\frac{r}{s}, m\right)\right) := \frac{rm}{s}$$

Aus der oben bezeichneten universellen Abbildungseigenschaft folgt nun bereits die eindeutige Existenz von $\tilde{\psi}$ mit $\tilde{\psi} \circ \otimes = f$. Nun kann nachgerechnet werden, dass $\tilde{\psi}$ und ψ invers zueinander sind. □

Folgerung 13.25 *Sei R ein kommutativer Ring, $S \subset R$ eine multiplikativ abgeschlossene Teilmenge von R und M ein (treu-)flacher R-Modul, dann ist $S^{-1}M$ gleichzeitig (treu-)flacher $S^{-1}R$-Modul und flacher R-Modul.*

Beweis. Zuerst zeigen wir, dass $S^{-1}M$ ein (treu-)flacher $S^{-1}R$-Modul ist:
Nach den vorhergegangenen Sätzen gilt für einen $S^{-1}R$-Modul N die folgende Isomorphie

$$\begin{aligned} N \otimes_{S^{-1}R} S^{-1}M &\overset{13.24}{\cong} N \otimes_{S^{-1}R} \left(S^{-1}R \otimes_R M\right) \\ &\overset{13.19}{\cong} \left(N \otimes_{S^{-1}R} S^{-1}R\right) \otimes_R M \\ &\overset{13.7}{\cong} N \otimes_R M \end{aligned}$$

Nun zeigen wir, dass $S^{-1}M$ ein flacher R-Modul ist:

Behauptung 1 *$S^{-1}R$ ist flach als R-Modul.*

Beweis. Sei $M \hookrightarrow M'$ ein injektiver R-Homomorphismus, dann betrachte

$$\begin{array}{ccc} S^{-1}R \otimes_R M & \longrightarrow & S^{-1}R \otimes_R M' \\ \downarrow \wr & & \downarrow \wr \\ S^{-1}M & \xrightarrow{\varphi_S} & S^{-1}M' \end{array}$$

Nach Teil (b) von Bemerkung 13.23 ist φ_S injektiv, und somit die Behauptung bewiesen. △
Da $\varphi : R \to S^{-1}R$ nach obiger Behauptung ein flacher R-Homomorphismus ist, folgt die Aussage aus Satz 13.20 Teil (a). □

Satz 13.26 *Sei R ein kommutativer Ring und $\varphi : M \to N$ ein R-Modulhomomorphismus. Für Primideale $\mathfrak{p} \lhd R$ sei $\varphi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ die Lokalisierung von φ aus Bemerkung 13.23 (a). Es gilt: φ ist genau dann surjektiv (injektiv), wenn für alle Maximalideale $\mathfrak{p} \lhd R$ die Lokalisierung $\varphi_\mathfrak{p}$ surjektiv (injektiv) ist. In Worten heißt dies: Bijektivität von Modul-Homomorphismen ist eine lokale Eigenschaft.*

Beweis. Die Implikation von φ auf $\varphi_\mathfrak{p}$ haben wir in Teil (b) der Bemerkung 13.23 gezeigt, zum Beweis der Gegenrichtung bezeichne P die Menge der Maximalideale von R und seien für alle $\mathfrak{p} \in P$ die Lokalisierungen $\varphi_\mathfrak{p}$ surjektiv (injektiv) dann sind folgende isomorphe Homomorphismen surjektiv (injektiv)

$$\begin{array}{ccc}
\bigoplus_{\mathfrak{p}\in P} M_\mathfrak{p} & \xrightarrow{(\varphi_\mathfrak{p})_{\mathfrak{p}\in P}} & \bigoplus_{\mathfrak{p}\in P} N_\mathfrak{p} \\
\downarrow\wr & & \downarrow\wr \\
\bigoplus_{\mathfrak{p}\in P} \left(R_\mathfrak{p} \otimes_R M\right) & \longrightarrow & \bigoplus_{\mathfrak{p}\in P} \left(R_\mathfrak{p} \otimes_R N\right) \\
\downarrow\wr & & \downarrow\wr \\
\left(\bigoplus_{\mathfrak{p}\in P} R_\mathfrak{p}\right) \otimes_R M & \longrightarrow & \left(\bigoplus_{\mathfrak{p}\in P} R_\mathfrak{p}\right) \otimes_R N
\end{array}$$

Definiere nun

$$T := \bigoplus_{\mathfrak{p}\in P} R_\mathfrak{p}$$

T ist treu-flacher R-Modul, denn T ist flach als R-Modul, weil nach Folgerung 13.25 jedes $R_\mathfrak{p}$ flach ist und nach Folgerung 13.5 direkte Summen von flachen Moduln flach sind. Sei nun $Q \lhd R$ ein Maximalideal, dann ist $QR_Q \neq R_Q$ also folgt, dass $QT \neq T$ ist. Mit Bemerkung 13.4 ist T dann treu-flach. Der Homomorphismus

$$T \otimes_R M \xrightarrow{(\varphi_\mathfrak{p})_{\mathfrak{p}\in P}} T \otimes_R N$$

ist in jeder Komponente surjektiv (injektiv), also folgt, wegen der Treuflachheit von T, dass die Abbildung $\varphi : M \to N$ surjektiv (injektiv) ist. Die injektivität folgt direkt aus der Definition, zum Nachweis der surjektivität nimm an, dass φ nicht surjektiv sei, dann betrachte die exakte Sequenz

$$M \to N \to K \to 0 \qquad \text{mit } K := \mathrm{Cokern}(\varphi)$$

dann ist auch

$$T \otimes_R M \to T \otimes_R N \to T \otimes_R K \to 0$$

eine exakte Sequenz mit $T \otimes_R K \neq 0$. Wir können schließen, dass

$$T \otimes_R M \to T \otimes_R N$$

keine surjektive Abbildung ist, dies haben wir weiter oben jedoch gezeigt und haben somit einen Widerspruch. □

Bemerkung 13.27 *Es seien R ein kommutativer Ring, M ein R-Modul und $P \lhd R$ ein Maximalideal, dann gilt*

$$M/PM \cong M_P/PR_PM_P$$

Beweis. Erinnerung: R_P ist ein lokaler Ring mit dem einzigen Maximalideal PR_P. Es genügt die folgende Isomorphie zu zeigen

$$R/P \cong R_P/PR_P$$

Betrachte hierzu die natürliche Projektion

$$\varphi : R \to {}^{R_P}\!/_{PR_P}$$

Wir wissen, dass $P = R \cap PR_P \subseteq \mathrm{Ker}(\varphi)$ enthalten ist, betrachte nun $r := \frac{x}{s} \in R$ mit $s \in P$ und $x \in R \backslash P$, dann ist $r \cdot s = x \in P$ und somit muss R bereits in P liegen, also ist $\mathrm{Ker}(\varphi) = P$. Weiter ist φ surjektiv, denn sei $s \in R \backslash P$, dann genügt es zu zeigen, dass $\frac{1}{s} - PR_P \in im(\varphi)$ gilt. Da P ein Maximalideal ist, muss das Ideal (P, s) das Einselement enthalten. Also existieren $a, b \in R$ und $x \in P$, so dass wir mit $1 = as + bx$ eine Darstellung der Eins erhalten. Nun folgt $\frac{1}{s} = a + \frac{bx}{s} \in im(\varphi)$ und somit die Surjektivität von φ. Mit dem *Homomorphiesatz* folgt nun die obige Isomorphie, um mit dieser auf die Aussage der Bemerkung zu schließen betrachte

$$\begin{aligned} {}^{M}\!/_{PM} &\overset{13.19\,(a)}{\cong} {}^{R}\!/_{P} \otimes_R M \cong {}^{R_P}\!/_{PR_P} \otimes_R M \\ &\overset{13.7}{\cong} \left({}^{R_P}\!/_{PR_P} \otimes_{R_P} R_P\right) \otimes_R M \cong {}^{R_P}\!/_{PR_P} \otimes_{R_P} \left(R_P \otimes_R M\right) \\ &\cong {}^{R_P}\!/_{PR_P} \otimes_{R_P} M_P \cong {}^{M_P}\!/_{PR_PM_P} \end{aligned}$$

□

Satz 13.28 *(Flachheit ist eine lokale Eigenschaft)*
Seien R ein kommutativer Ring und M ein R-Modul, dann sind äquivalent
(i) M ist (treu-)flach.
(ii) M_P ist (treu-)flach für alle Maximalideale $P \lhd R$.

Beweis. Den Schluss von (i) auf (ii) haben wir bereits in Folgerung 13.25 bewiesen. Wir zeigen für den Schluss von (ii) auf (i) zunächst die Flachheit. Sei also $\varphi : N \hookrightarrow N'$ ein injektiver R-Modulhomomorphismus. Nach Voraussetzung ist M_P flach über R_P und im Beweis zu Folgerung 13.25 haben wir die Flachheit von R_P über R gezeigt, daher ist M_P flach über R. Betrachte also das folgende Diagramm injektiver Homomorphismen:

$$\begin{array}{ccc} N \otimes_R M_P & \longrightarrow & N' \otimes_R M_P \\ \downarrow \wr & & \downarrow \wr \\ \left(N \otimes_R M\right) \otimes_R R_P & \longrightarrow & \left(N' \otimes_R M\right) \otimes_R R_P \\ \downarrow \wr & & \downarrow \wr \\ \left(M \otimes_R M\right)_P & \longrightarrow & \left(N' \otimes_R M\right)_P \end{array}$$

Mit Satz 13.26 folgt nun die Injektivität von

$$N \otimes_R M \hookrightarrow N' \otimes_R M$$

Zur Treuflachheit: Nach Bemerkung 13.14 ist $PR_PM_P \neq M_P$ somit gilt mit Bemerkung 13.27:

$$0 \neq {}^{M_P}\!/_{PR_PM_P} \overset{13.27}{\cong} {}^{M}\!/_{PM}$$

Wir können schließen, dass $M \neq PM$ und somit ist M nach Bemerkung 13.14 treu-flach. □

14 Noetherscher Normalisierungssatz und lokale Charakterisierung der Ganzabgeschlossenheit

Satz 14.1 *(Nagatas Normalisierungslemma)*
Sei K ein Körper und $f \in R := K[X_1, \ldots, X_n]$ ein nicht konstantes Polynom, dann gibt es $m_2, \ldots, m_n \in \mathbb{N}$, so dass R ganz über $S := K[f, Y_2, \ldots, Y_n]$ mit $Y_i := X_i - X_1^{m_i}$ ist.

Beweis. Es gilt $R = S[X_1]$, wir müssen also zeigen, dass X_1 ganz über S ist. Hierzu werden wir versuchen ein Polynom $h \in S[T]$ zu konstruieren das X_1 als Nullstelle hat und dessen höchster Koeffizient bereits in K liegt. Definiere also

$$h(T) := f(T, Y_2 + T^{m_2}, \ldots, Y_n + T^{m_n}) - f(X_1, \ldots, X_n) \ \in S[T]$$

Dieses Polynom erfüllt $h(X_1) = 0$ für alle Wahlen der m_i. Bezeichne d den Grad von f, dann gilt

$$f(X_1, \ldots, X_n) = \sum_{|\alpha| \leq d} a_\alpha X^\alpha \qquad \text{mit einem Multiindex } \alpha := (\alpha_1, \ldots, \alpha_n) \text{ und } |\alpha| := \sum_{i=1}^{n} \alpha_i$$

Damit gilt für $h(T)$

$$\begin{aligned} h(T) &= \sum_{|\alpha| \leq d} a_\alpha \cdot T^{\alpha_1} \cdot (Y_2 + T^{m_2})^{\alpha_2} \ldots (Y_n + T^{m_n})^{\alpha_n} - f(X_1, \ldots, X_n) \\ &= \sum_{|\alpha| = d} a_\alpha \cdot T^\zeta + \text{Terme niedrigeren Grades in T} \qquad \text{mit } \zeta := \sum_{i=1}^{n} \alpha_i m_i \end{aligned}$$

Wähle die m_i nun so, dass alle $\alpha_i \cdot m_i$ verschieden sind (zum Beispiel $m_i := (d+1)^i$), dann ist der hoechste Koeffizient von h ein Element aus K. □

Definition und Satz 14.2 *(Noetherscher Normalisierungssatz)*
Seien K ein Körper und R ein endlich erzeugter Integritätsring über K, dann gibt es $y_1, \ldots, y_r \in R$, so dass $\{y_1, \ldots, y_r\}$ algebraisch unabhängig über K sind und $R/K[y_1, \ldots, y_r]$ eine ganze Ringerweiterung ist.
Der Ring $K[y_1 \ldots, y_r]$ heißt Noetersche-Normalisierung von R.

Anmerkung $K[y_1, \ldots, y_r]$ ist isomorph zum Polynomring über K in r Variablen.

Beweis. Sei $\mathfrak{E} := \{x_1, \ldots, x_n\}$ ein Erzeugendensystem von R über k. Wir wollen den Satz induktiv über n die Anzahl der Erzeuger von R beweisen. Hierbei ist der Induktionsanfang trivial, denn für $n = 0$ gilt $R = K$. Für den Induktionsschritt von $n-1$ auf n definiere

$$\begin{aligned} \varphi : K[X_1, \ldots, X_n] &\twoheadrightarrow R \\ X_i &\mapsto x_i \end{aligned}$$

Die so definierte Abbildung φ ist ein surjektiver Ringhomomorphismus und es gilt

$$P := \mathrm{Ker}(\varphi) \lhd K[X_1, \ldots, X_n]$$

ist ein Primideal. Ist nun $P = (0)$ so folgt mit dem Homomorphiesatz $R \cong K[X_1, \ldots, X_n]$ und somit die Aussage des Satzes. Andernfalls ($P \neq (0)$) sei $f \in P$ ein nicht konstantes Polynom, also insbesondere nicht das Nullpolynom. Dann gibt es mit Satz 14.1 Elemente $y_2, \ldots, y_n$ in $K[X_1, \ldots, X_n]$ derart, dass $K[X_1, \ldots, X_n]$ ganz über $K[f, y_2, \ldots, y_n]$ ist. Definiere

$$R' := \varphi(K[f, y_2, \ldots, y_n]) = K[\varphi(y_2), \ldots, \varphi(y_n)]$$

Nach Induktionsannahme ist R' über $K[Y_1, \ldots Y_{n-1}]$ ganz, dann ist aber auch $R/K[Y_1, \ldots, Y_{n-1}]$ eine ganze Ringerweiterung. □

Bemerkung 14.3 *Sei R ein normaler Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge von R, dann ist auch $S^{-1}R$ ein normaler Ring.*

Beweis. Bezeichne $K := \mathrm{Quot}(R) = \mathrm{Quot}(S^{-1}R)$ und sei $\alpha := \frac{a}{b} \in K$ ganz über $S^{-1}R$, d.h. α ist insbesondere eine Nullstelle eines Polynoms aus $S^{-1}R[X]$. Betrachte

$$\left(\frac{a}{b}\right)^n + \frac{c_{n-1}}{s} \cdot \left(\frac{a}{b}\right)^{n-1} + \cdots + \frac{c_0}{s} = 0$$

Nach Erweitern der Koeffizienten auf den Hauptnenner erhalten wir

$$\left(\frac{a \cdot s}{b}\right)^n + c_{n-1} \cdot \left(\frac{a \cdot s}{b}\right)^{n-1} + \cdots + c_0 \cdot s^{n-1} = 0$$

Damit ist aber $\frac{as}{b}$ Nullstelle eines normierten Polynoms aus R und somit ganz über R. Da R normal ist folgt sofort, dass $\frac{as}{b} \in R$ ist und somit $\frac{a}{b} = \alpha \in S^{-1}R$. □

Bemerkung 14.4 *Seien R ein Integritätsring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Weiter bezeichne $K := \mathrm{Quot}(R)$. Dann gilt*

$$S^{-1}\tilde{R} = \widetilde{S^{-1}R}$$

Hierbei bezeichne $\tilde{R}$ die ganz abgeschlossene Hülle von R in K.

Beweis. Wir wissen $\tilde{R}$ ist normal, damit ist nach Bemerkung 14.3 auch $S^{-1}\tilde{R} \subset K$ normal. Weiter ist $\tilde{R}/R$ eine ganze Ringerweiterung, also ist nach Bemerkung 7.10 auch $S^{-1}\tilde{R}$ ganz über $S^{-1}R$. □

Satz 14.5 *(Lokale Charakterisierung der Normalität)*
Sei R ein Integritätsring, dann sind äquivalent
(i) R ist normal und (ii) R_P ist für alle Maximalideale $P \lhd R$ normal.

Beweis. Der Schluss von (i) auf (ii) ist die Aussage von Bemerkung 14.3, für die Gegenrichtung sei $\tilde{R}$ die normalisierung des ganzen Abschlusses von R. Nach Bemerkung 14.4 gilt

$$\widetilde{R_P} = \left(\tilde{R}\right)_P$$

Betrachte nun die Einbettung $\varphi : R \hookrightarrow \tilde{R}$. Diese ist nach Satz 13.26 genau dann surjektiv, wenn R ein normaler Ring ist, d.h. wenn $R = \tilde{R}$ ist. Also genau dann, wenn $\varphi_P : R_P \to \tilde{R}_P = \widetilde{R_P}$ surjektiv ist, also wenn R_P ein normaler Ring ist. □

15 Allgemeiner Hilbertscher Nullstellensatz

Definition 15.1 *(Radikalideal, Jacobson-Radikal)*
Sei R ein Ring und $\mathfrak{a} \lhd R$ ein Ideal, dann heißt

$$\sqrt{\mathfrak{a}} := \{r \in R \,|\, \exists n \in \mathbb{N} : r^n \in \mathfrak{a}\} \lhd R$$

das Radikal(ideal) von $\mathfrak{a}$. Weiter heißtn $\mathfrak{a}$ Radikalideal, falls $\mathfrak{a} = \sqrt{\mathfrak{a}}$ gilt.
Bezeichne $\mathbb{M}$ die Menge der Maximalideale von R, dann heißt

$$\mathrm{Rad}(R) := \mathrm{Jac}(R) := \bigcap_{P \in \mathbb{M}} P$$

das (Jacobson-)Radikal von R. Analog heißt

$$\mathrm{Rad}(\mathfrak{a}) := \mathrm{Jac}(\mathfrak{a}) := \bigcap_{\substack{P \in \mathbb{M} \\ \mathfrak{a} \subseteq P}} P$$

das (Jacobson-)Radikal von $\mathfrak{a}$.
Sei $P \lhd R$ ein Primideal und $f \in R$ ein Ringelement, dann heißt P Nullstelle von f, wenn

$$\frac{f}{1} = 0 \qquad \text{in } {}^{R_P}\!/_{PR_P}$$

Wir schreiben dann $f(P) = 0$.

Anmerkung Betrachte die natürliche Projektion $\pi : R \to {}^{R}\!/_{\mathfrak{a}}$, dann ist

$$\pi^{-1}\left(\mathrm{Jac}\left({}^{R}\!/_{\mathfrak{a}}\right)\right) = \mathrm{Jac}(\mathfrak{a})$$

Beispiel 37 *Sei R ein Ring und P ein Primideal von R, dann ist $\sqrt{P} = P$.*

Bemerkung 15.2 *Sei R ein Ring, $P \lhd R$ ein Primideal und $f \in R$, dann gilt*

$$\begin{aligned} f(P) = 0 \quad &\Leftrightarrow \quad \frac{f}{1} \in PR_P \\ &\Leftrightarrow \quad \exists\, q \in P,\ \exists\, t \in R \backslash P \quad \frac{f}{1} = \frac{q}{t} \\ &\Leftrightarrow \quad \exists\, t, s \in R \backslash P\ \exists q \in P \quad stf = sq \\ &\Leftrightarrow \quad f \in P \end{aligned}$$

□

Satz 15.3 *(Abstrakter Nullstellensatz)*
Sei R ein kommutativer Ring und $\mathfrak{a} \lhd R$ ein Ideal sowie $f \in R$ ein Element, genau dann gilt für alle Maximalideale $P \lhd R$ die $\mathfrak{a}$ enthalten, dass $f(P) = 0$ ist, wenn $f \in \mathrm{Rad}(\mathfrak{a})$ ist.

Beweis. Folgt sofort aus Bemerkung 15.2. □

Satz 15.4 *(Allgemeiner Hilbertscher Nullstellensatz)*
Sei K ein Körper und R/K eine endlich erzugte K-Algebra. Weiter sei $\mathfrak{a} \lhd R$ ein Ideal, dann gelten:

a) $\sqrt{\mathfrak{a}} = \mathrm{Rad}(\mathfrak{a}) = \mathrm{Jac}(\mathfrak{a})$

b) *Für alle Maximalideale $P \lhd R$ die $\mathfrak{a}$ enthalten gilt genau dann $f(P) = 0$, wenn $f \in \sqrt{\mathfrak{a}}$ ist.*

Beweis. Teil b) der Aussage folgt unmittelbar aus Satz 15.3 und Teil a). Für den Teil a) müssen wir zwei Inklusionen zeigen, sei also zunächst $f \in \sqrt{\mathfrak{a}}$ (d.h. es gibt ein $n \in \mathbb{N}$ so dass $f^n \in \mathfrak{a}$ ist) und weiter sei $P \lhd R$ ein Maximalideal, dass $\mathfrak{a}$ enthält, dann ist $f^n \in P$. Da P insbesondere ein Primideal ist folgt $f \in P$ und damit $f \in \mathrm{Rad}(\mathfrak{a})$.
Für die andere Inklusion zeigen wir, dass aus $f \notin \sqrt{\mathfrak{a}}$ folgt, dass $f \notin \mathrm{Rad}(\mathfrak{a})$ ist.
Sei nun also $f \notin \sqrt{\mathfrak{a}}$ das heißt, dass keine natürliche Potenz von f in $\mathfrak{a}$ enthalten ist. Definiere

$$\bar{R} := {}^{R}\!/_{\mathfrak{a}} \quad \text{und} \quad S := \{\bar{f}^n | n \in \mathbb{N}\} \quad \text{mit } \bar{f} := f + \mathfrak{a}$$

Dann ist S eine multiplikativ abgeschlossene Teilmenge von $\bar{R}$ mit $0 \notin S$. Sei $\bar{Q} \lhd S^{-1}R$ ein Maximalideal, dann ist $\bar{f} \notin \bar{Q}$, da $\bar{f}$ eine Einheit ist und damit ist

$$L := {}^{S^{-1}R}\!/_{\bar{Q}}$$

eine Körpererweiterung von K, die nach Voraussetzung an R als K-Algebra endlich erzeugt ist. Mit Satz 9.12 ist L/K eine endliche Körpererweiterung. Es gelten die folgenden Inklusionen

$$K \subseteq {}^{\bar{R}}\!/_{\bar{Q} \cap \bar{R}} \subseteq L$$

Also ist $\bar{Q} \cap \bar{R} \lhd \bar{R}$ ein Maximalideal, aber $\bar{f} \notin \bar{Q}$. Betrachte die natürliche Projektion

$$\pi : R \to {}^{R}\!/_{\mathfrak{a}} =: \bar{R}$$

und definiere

$$Q := \pi^{-1}\big(\bar{Q} \cap \bar{R}\big)$$

Es gilt: $Q \lhd R$ ist ein Maximalideal mit $\mathfrak{a} \subset Q$ aber $f \notin Q$ daher folgt $f \notin \mathrm{Rad}(\mathfrak{a})$. □

Folgerung 15.5 *(Klassischer Hilbertscher Nullstellensatz)*
Sei K ein algebraisch abgeschlossener Körper und $\mathfrak{a} \lhd K[X_1, \ldots X_n] := K[\underline{X}]$ ein Ideal, dann gilt

$$I\big(V_{\mathfrak{a}}(K)\big) = \sqrt{\mathfrak{a}}$$

Insbesondere entsprechen sich die affinen algebraischen Mengen und die Radikalideale von $K[\underline{X}]$ bijektiv.

Beweis. Sei $f \in I\big(V_{\mathfrak{a}}(K)\big)$ also gilt für alle $\underline{x} \in V_{\mathfrak{a}}(K)$ die Gleichung $f(\underline{x}) = 0$ und auch $f(X_1 - x_1, \ldots, X_n - x_n) = 0$. Dies heißt aber, dass für alle Maximalideale $P \lhd K[X]$ die $\mathfrak{a}$ enthalten $f(P) = 0$ ist und somit folgt nach Satz 15.4 die Behauptung. Zum „Insbesondere“ betrachte

$$\mathfrak{X} = V_{\mathfrak{a}}(K) \mapsto I(\mathfrak{X}) = I\big(V_{\mathfrak{a}}(K)\big) = \sqrt{a} \mapsto V_{\sqrt{\mathfrak{a}}}(K) = V_{\mathfrak{a}}(K) = \mathfrak{X}$$

und

$$\mathfrak{a} = \sqrt{\mathfrak{a}} \mapsto V_{\sqrt{\mathfrak{a}}}(K) \mapsto I\big(V_{\sqrt{\mathfrak{a}}}(K)\big) = \mathfrak{a}$$

□

16 Dimension von Ringen

Bemerkung 16.1 *Sei R ein Ring, M ein endlich erzeugter R-Modul und $\mathfrak{a} \lhd R$ ein Ideal. Weiter sei $\phi : M \to M$ ein R-Homomorphismus mit $\phi(M) \subseteq \mathfrak{a}M$. Dann gibt es ein $n \in \mathbb{N}$ und Elemente $a_0, \dots a_{n-1} \in \mathfrak{a}$ derart, dass gilt*

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 \;=\; 0$$

Beweis. Seien $x_1, \dots x_n \in M$ die Erzeuger von M. Betrachte die Darstellung der Erzeuger bzgl. ϕ

$$\phi(x_i) \;=\; \sum_{j=1}^{n} a_{i,j}x_j \quad \text{mit } a_{i,j} \in \mathfrak{a}$$

Und definiere die Matrix

$$D := D(T) := \begin{pmatrix} T & 0 & \dots & 0 \\ 0 & T & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & T \end{pmatrix} - (a_{i,j})_{0\le i,j\le n} \quad \in \mathrm{Mat}_{R[T]}(n,n)$$

Es gilt $D * D \;=\; \det(D) \cdot E_n$ mit E_n ist die $n \times n$-Einheitsmatrix. Daher folgt für alle i, dass $D(\phi)(x_i) \;=\; 0$ ist. d.h. $D(\phi) \cdot (x_1, \dots, x_n)^T$ mit $D(\phi) \in \mathrm{Mat}_{R[\phi]}(n,n)$ ist der Nullvektor. Daher folgt

$$\det(D)(\phi) = \phi^n + a_{n-1}\phi^{n-1} + \ldots + a_0 = 0$$

□

Definition 16.2 *(Ganz über einem Ideal)*
Sei R/S eine Ringerweiterung und $a \lhd R$ ein Ideal, dann heißt $x \in S$ ganz über $\mathfrak{a}$,
falls es Elemente $a_i \in \mathfrak{a}$ mit der Eigenschaft $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ gibt und die Menge $\bar{\mathfrak{a}} := \{x \in S | x \text{ ganz über } \mathfrak{a}\}$ heißt der ganze Abschluss von $\mathfrak{a}$ in S.

Bemerkung 16.3 *Seien $R \subset S$ Ringe und $C := R_S$ der ganze Abschluss von R in S. Weiter seien $\mathfrak{a} \lhd R$ ein Ideal und $\mathfrak{a}^l = \mathfrak{a}C$ das von $\mathfrak{a}$ erzeugte Ideal in C. Dann ist $\sqrt{\mathfrak{a}^l}$ der ganze Abschluss von $\mathfrak{a}$ in C und Insbesondere ein Ideal.*

Beweis. Wir müssen zwei Inklusionen zeigen. Sei zunächst $x \in S$ ganz über $\mathfrak{a}$, dann gibt es Elemente $a_i \in \mathfrak{a}$ derart, dass die Gleichung $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ erfüllt ist. Dann ist aber $x \in C$ und somit $x^n \in \mathfrak{a}^l$. Es folgt sofort: $x \in \sqrt{\mathfrak{a}^l}$
Sei nun $x \in \sqrt{\mathfrak{a}^l}$, dann gibt es eine natürliche Zahl n, so dass $x^n \in \mathfrak{a}^l$ ist. Wir können also Elemente $a_i \in \mathfrak{a}$ und Elemente $x_i \in C$ finden, so dass wir x^n darstellen können als

$$x^n = \sum_{i=1}^{m} a_i x_i$$

Da C der ganze Abschluss von R in S ist sind alle x_i ganz über R und daher ist $R[x_1, \dots, x_m] =: M$ ein endlich erzeugter R-Modul. Es folgt $x^n M \subseteq \mathfrak{a}M$. Betrachte nun

$$\begin{aligned} \phi : M &\to M \\ y &\mapsto x^n y \end{aligned}$$

Mit Bemerkung 16.1 gilt nun, dass x^n ganz über $\mathfrak{a}$ ist und somit ist auch x ganz über $\mathfrak{a}$. □

Bemerkung 16.4 *Seien $R \subseteq S$ Integritätsringe und R normal. Weiter seien $\mathfrak{a} \lhd R$ ein Ideal und $K := \mathrm{Quot}(R)$ der Quotientenkörper von R. Ist $x \in S$ ganz über $\mathfrak{a}$, dann gelten:*
(a) x ist algebraisch über K.
(b) Das Minimalpolynom $f_x = X^n + a_1 X^{n-1} + \ldots + a_n \in K[X]$ von x erfüllt $a_i \in \sqrt{\mathfrak{a}}$ für alle i.

Beweis. Teil (a) ist trivial. Zu (b) zerlege das Minimalpolynom

$$f_x(X) = \prod_{i=1}^{n} (X - x_i)$$

Es gilt $\{x = x_1, \ldots, x_n\} = \{\sigma(x) | \sigma \in \mathrm{Aut}(K)\}$ damit sind alle x_i ganz über $\mathfrak{a}$, denn sie haben das selbe Minimalpolynom. Nach Bemerkung 16.3 gilt nun für alle i, dass $x_i \in \sqrt{\mathfrak{a}}$ sind. Da die a_i elementarsymmetrische Funktionen in $x_1, \ldots, x_n$ sind folgt nun $a_1, \ldots, a_n \in \sqrt{\mathfrak{a}}$. □

Satz 16.5 *(Going down)*
Seien $R \subseteq S$ Integritätsringe, R normal, S/R eine ganze Ringerweiterung und bezeichne $K := \mathrm{Quot}(R)$ den Quotientenkörper von R. Weiter seien eine Primidealkette $\mathfrak{y}_n \subsetneq \cdots \subsetneq \mathfrak{y}_1$ in R und eine Primidealkette $P_m \subsetneq \cdots \subsetneq P_1$ in S mit $m \leq n$ und $R \cap P_i = \mathfrak{y}_i$ für alle $i = 1...m$ gegeben. Dann gibt es eine Fortsetzung $P_n \subsetneq \cdots \subsetneq P_{m-1} \subsetneq P_m$ von Primidealen in S mit $R \cap P_i = \mathfrak{y}_i$ für alle $i = 1...n$.
In Worten: Jede absteigende Primidealkette in S über eine Primidealkette in R kann verlängert werden.

Beweis. Wir reduzieren auf den Fall $0 \in \mathfrak{y}_2 \subsetneq \mathfrak{y}_1$ und $P_1 \cap R = \mathfrak{y}_1$

Behauptung 1 *Es gilt: $R \cap \mathfrak{y}_2 S_{P_1} = \mathfrak{y}_2$*

Beweis. Sei zunächst $\frac{y}{t} \in \mathfrak{y}_2 S_{P_1}$ also $t \in S \backslash P_1$ und $y \in \mathfrak{y}_2 S$, dann ist y mit Bemerkung 16.3 ganz über $\mathfrak{y}_2$, denn $\sqrt{\mathfrak{y}_2 S}$ ist der ganze Abschluss vonm $\mathfrak{y}_2$ in S. Das Minimalpolynom von y ist mit Bemerkung 16.4

$$f_y(y) = y^r + a_1 y^{r-1} + \cdots + a_r = 0 \qquad \text{mit } a_i \in \mathfrak{y}_2$$

Sei nun $\frac{y}{t} := x \in \mathfrak{y}_2 S_{P_1} \cap R$, dann teile die obige Gleichung durch x^r und erhalte

$$(*) \qquad t^r + \frac{a_1}{x} t^{r-1} + \cdots + \frac{a_r}{x^r} = 0$$

Definiere $v_i := \frac{a_i}{x^i}$, dann ist $x^i v_i = a_i \in \mathfrak{y}_2$. Da t in S ist, ist t ganz über R und somit gilt für alle i: $v_i \in R$, denn $(*)$ ist das Mimimalpolynom von t. Sei nun angenommen, dass $x \notin \mathfrak{y}_2$ dann müssten, wegen der Primidealeigenschaft von $\mathfrak{y}_2$, alle v_i in $\mathfrak{y}_2$ liegen. Damit wäre wegen $(*)$ aber auch $t \in \mathfrak{y}_2$ und dies ist ein Widerspruch, da $\mathfrak{y}_2 \subset \mathfrak{y}_1 \subset P_1$ und $t \in S \backslash P_1$. Also muss $x \in \mathfrak{y}_2$ gelten. △

Behauptung 2 *Es gibt ein Primideal $P_2 \subsetneq P_1$ von S mit $P_2 \cap R = \mathfrak{y}_2$*

Beweis. Definiere $T := R \backslash \mathfrak{y}_2$ dann gilt

$$\mathfrak{y}_2 S_{P_1} \cap T = \left(\mathfrak{y}_2 S_{P_1} \cap R\right) \cap T \overset{\text{1. Beh.}}{=} \mathfrak{y}_2 \cap T = \varnothing$$

Also ist $T^{-1}\mathfrak{y}_2 S_{P_1} = \mathfrak{y}_2 T^{-1} S_{P_1} \lhd T^{-1} S_{P_1}$ ein nicht-triviales Ideal. Sei nun $m \lhd T^{-1} S_{P_1}$ ein Maximalideal, dass $T^{-1}\mathfrak{y}_2 S_{P_1}$ enthält und definiere

$$P_2 := m \cap S$$

Das Ideal P_2 ist in P_1 enthalten, da $m \cap S_{P_1}$ ein Ideal in S_{P_1} ist. Da m ein echtes Ideal ist, muss $m \cap T = \varnothing$ gelten, also folgt

$$m \cap T = (m \cap S) \cap T = P_2 \cap (R \backslash \mathfrak{y}_2) = \varnothing$$

Damit haben wir die Inklusion $P_2 \cap R \subset \mathfrak{y}_2$ gezeigt. Für die andere Inklusion betrachte

$$\mathfrak{y}_2 \subseteq \mathfrak{y}_2 T^{-1} S_{P_1} \cap R \subseteq m \cap R = P_2 \cap R$$

□

Folgerung 16.6 *Seien $R \subset S$ Integritätsringe, R normal und S/R eine ganze Ringerweiterung. Weiter sei $P \lhd S$ ein Primideal, dann gilt*

$$\mathrm{h}(P) = \mathrm{h}(P \cap R)$$

Beweis. Die Relation $\mathrm{h}(P) \leq \mathrm{h}(P \cap R)$ folgt sofort aus Bemerkung 7.7. Nach Satz 16.5 „going down“ kann jede mit $P \cap R$ endende Kette in R zu einer in P endenden Kette von S hochgehoben werden. Damit folgt $\mathrm{h}(P) \geq \mathrm{h}(P \cap R)$. □

Definition 16.7 *(affine Algebra)*
Sei K ein Körper. Eine endlich erzeugte K-Algebra heißt auch affine K-Algebra.

Satz 16.8 *Seien K ein Körper und R eine affine K-Algebra, die ein Integritätsbereich ist. Nach Noether Normalisierung gibt es algebraisch unabhängige Elemente $y_1, \ldots, y_d \in R$, so dass $R/K[y_1, \ldots, y_d]$ eine ganze Ringerweiterung ist. Es gelten*
(a) $\dim(R) = d$
(b) Jede maximale Primidealkette in R hat die Länge d

Beweis. In Folgerung 7.13 (a) haben wir gezeigt, dass $\dim(R) = \dim(K[y_1, \ldots, y_d])$ gilt, daher genügt es zu zeigen, dass die Dimension des Polynomrings in d Variablen d ist. Wir wissen bereits, dass $\dim(K[X_1, \ldots, X_d]) = m \geq d$ ist. Sei also

$$(1) \qquad 0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_m$$

eine Primidealkette in $K[X_1, \ldots, X_d]$ und $f \in P_1$ ein nichtkonstantes Polynom. Finde hierzu mit Satz 16.5 „going down“ und Nagatas Lemma 14.1 eine Primidealkette

$$(2) \qquad 0 \subsetneq \mathfrak{y}_1 = (f) \subsetneq \mathfrak{y}_2 \subsetneq \cdots \subsetneq \mathfrak{y}_m$$

in $K[f, y_2, \ldots, y_d] \subseteq K[X_1, \ldots X_d]$ mit $\mathfrak{y}_i := P_i \cap K[f, y_2, \ldots y_d]$ Betrachte diese Kette modulo (f) und erhalte

$$(3) \qquad 0 \subsetneq \mathfrak{y}_2 \diagup (f) \subsetneq \cdots \subsetneq \mathfrak{y}_m \diagup (f) \quad \text{in } K[y_2, \ldots y_d] \cong K[f, y_2, \ldots, y_d] \diagup (f)$$

Nach Bemerkung 7.7 bleiben die Inklusionen erhalten und nach Folgerung 7.13 (a) gilt:

$$m = \dim\big(K[X_1, \ldots, X_d]\big) = \dim\big(K[f, y_1, \ldots, y_d]\big)$$

Daher muss die Kette der $\mathfrak{y}_i$ maximal sein. Für $i = 2, \ldots, m$ sind die $\mathfrak{y}_i/(f)$ paarweise verschiedene Primideale, daher gilt nach dem Isomorphiesatz für alle i

$$K[f, y_2, \ldots, y_d]/(f)/\mathfrak{y}_i/(f) \cong K[f, y_2, \ldots, y_d]/\mathfrak{y}_i$$

Den Teil (a) beweisen wir nun induktiv über d. Der Anfang für $d = 0$ ist trivial. Für den Schritt von $d-1$ auf d gilt nach Induktionsannahme, dass $\dim(K[y_2, \ldots, y_d]) = d-1$ ist. Daher folgt $m - 1 \leq d - 1$ und $m \leq d$. Es muss also $m = d$ gelten.
Zum Beweis von (b) sei die Kette (1) nicht zu verfeinern. Erhalte Kette (3) wie beschrieben. Ließe sich nun in (3) ein Ideal q einschieben, so wäre mit der natürlichen Projektion $\pi^{-1}(q)$ ein neues Ideal in (2). Damit folgt dann $\mathrm{h}(\mathfrak{y}_m) > m$. Nach Folgerung 16.6 gilt aber $\mathrm{h}(P_m) = \mathrm{h}(\mathfrak{y}_m)$. Die Existens von q liefert also einen Widerspruch. □

Folgerung 16.9 *Seien K ein Körper und R eine affine K-Algebra. Weiter seien R ein Integritätsbereich und $P \supset Q$ Primideale von R, dann gilt: Alle maximalen Primidealketten, die mit P beginnen und mit Q enden, haben die Länge*

$$\dim R/P - \dim R/Q$$

Beweis. Sei die Primidealkette

$$P = P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_m = Q$$

nicht zu verfeinern, dann ist diese Kette auch modulo P nicht zu verfeinern. Daher ist

$$(0) = P_0/P \subsetneq \ldots \subsetneq P_m/P = Q/P \subsetneq R_1 \subsetneq \ldots \subsetneq R_s/P \subsetneq R/P$$

eine Kette maximaler Länge somit ist

$$(0) \subsetneq R_1/Q \subsetneq \ldots \subsetneq R_s/Q$$

eine maximale Primidealkette in R/Q, hat also die Länge $\dim R/Q$. Fügen wir nun diese Ergebnisse zusammen erhalten wir $m + \dim R/Q = R/P$ □

Folgerung 16.10 *Seien K ein Körper und R eine affine K-Algebra. Weiter seien R ein Integritätsbereich und $Q \lhd R$ ein Primideal, dann gilt folgende Dimensionsformel für R:*

$$\dim R = \mathrm{h}(Q) + \dim R/Q$$

Beweis. Folgt sofort aus Folgerung 16.9 mit $P = (0)$ und $Q = Q$. □

Definition 16.11 *(Dimension von $\mathfrak{X}$)*
Sei K ein Körper und $\mathbb{A}^n(K)$ eine affine Varietät. Für eine Teilmenge $\mathfrak{X} \subset \mathbb{A}^n(K)$ heißt

$$\dim \mathfrak{X} := \dim K[\mathfrak{X}]$$

die Dimension von $\mathfrak{X}$.

Folgerung 16.12 *Sei K ein Körper und $\mathbb{A}^n(K)$ eine affine Varietät, dann gelten*
(1) $\dim\left(K[X_1,\ldots,X_d]\right) = d$*, also* $\dim \mathbb{A}^n(K) = n$
(2) Sei $f \in K[X,Y]$ ein irreduzibles, nicht konstantes Polynom und K algebraisch abgeschlossen, dann gilt

$$\dim\Big(V_f(K)\Big) = 1$$

Beweis. Teil (1) haben wir bereits in Satz 16.8 beiwesen für Teil (2) gilt $(f) \neq (0)$ ist ein ein Primideal. Nach Bemerkung 7.2 ist $\mathrm{h}\left((f)\right) = 1$, denn in faktoriellen Ringen haben ausser dem Nullideal alle Hauptideale, die Primideale sind, die Höhe 1. Nach Folgerung 16.10 gilt

$$2 = \dim(K[X,Y]) = \mathrm{h}\left((f)\right) + \dim\left(K[X,Y]/(f)\right) = 1 + \dim\left(V_f(K)\right)$$

□

17 Dedekind-Ringe

Bemerkung 17.1 *Sei R ein lokaler Noetherscher Integritätsring der Dimension 1 mit Maximalideal $\mathfrak{m}$. Ist $I \lhd R$ nicht das Nullideal, dann gibt es ein $n \in \mathbb{N}$ derart, dass $\mathfrak{m}^n \subset I$ ist.*

Beweis. Betrachte die Menge

$$\Sigma := \{\, I \lhd R \,|\, \forall n : \mathfrak{m}^n \nsubseteq I \,\} \ni (0)$$

Da R Noethersch ist enthält Σ ein maximales Element I. Nehmen wir nun an $I \neq (0)$ dann ist I kein Primideal, da $0 \neq I \neq \mathfrak{m}$ gilt, also gibt es $x, y \in R$, so dass $xy \in I$ aber $x \notin I$ und $y \notin I$ ist. Dann ist aber weder (I,x) noch (I,y) in I enthalten und somit gibt es $n_1, n_2 \in \mathbb{N}$ derart, dass $\mathfrak{m}^{n_1} \subseteq (I,x)$ und $\mathfrak{m}^{n_2} \subseteq (I,y)$ gelten. Damit gilt aber

$$\mathfrak{m}^{n_1+n_2} \subseteq (I,x)(I,y) \subseteq I$$

Dies ist ein Widerspruch, daher muss das maximale Element von Σ das Nullideal sein. □

Bemerkung 17.2 *Sei R ein lokaler Noetherscher Ring mit Maximalideal $\mathfrak{m}$, dann gelten:*
(a) $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ *ist ein* $R/\mathfrak{m}$*-Vektorraum mit der natürlichen Operation.*
(b) $\dim_{R/\mathfrak{m}}\left(\mathfrak{m}/\mathfrak{m}^2\right)$ *ist die minimale Anzahl von Erzeugern für das Ideal $\mathfrak{m}$*
(c) Ist $\dim_{R/\mathfrak{m}}\left(\mathfrak{m}/\mathfrak{m}^2\right) = 1$*, dann gibt es keine Ideale $\mathfrak{a}$ mit* $\mathfrak{m}^n \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}^{n-1}$

Beweis. Teil (a) ist klar. Für (b) seien $e_1,\ldots,e_r$ Erzeuger von $\mathfrak{m}$. Dann sind $e_1+\mathfrak{m}^2,\ldots e_r+\mathfrak{m}^2$ die $R/\mathfrak{m}$-Erzeuger von $\mathfrak{m}/\mathfrak{m}^2$ daher muss $\dim_{R/\mathfrak{m}}\left(\mathfrak{m}/\mathfrak{m}^2\right) \leq r$ gelten. Nach Nakayamas Lemma kann $\mathfrak{m}$ als R-Modul, also als Ideal, von $d = \dim_{R/\mathfrak{m}}\left(\mathfrak{m}/\mathfrak{m}^2\right)$ Elementen erzeugt werden.
Zu Teil (c): Es gilt $\mathfrak{a}/\mathfrak{m}^n$ ist Untervektorraum von $\mathfrak{m}^{n-1}/\mathfrak{m}^n$ aber $\dim_{R/\mathfrak{m}}\left(\mathfrak{m}^{n-1}/\mathfrak{m}^n\right) = 1$ □

Definition 17.3 *(Regulärer Ring)*
Ein Noetherscher lokaler Ring mit Maximalideal $\mathfrak{m}$ heißt regulär, falls bezüglich der Krull-Dimension von R gilt:

$$\dim_{R/\mathfrak{m}}\left(\mathfrak{m}/\mathfrak{m}^2\right) = \dim(R)$$

Bemerkung 17.4 *Ein regulärer Ring der Dimension 1 ist automatisch ein Integritätsbereich und alle echten Ideale, die nicht das Nullideal sind, sind von der Form (x^n) mit $(x) = \mathfrak{m}$ für ein $x \in R$.*

Beweis. $\mathfrak{m} = (x)$ ist ein Hauptideal. Nach Definition 17.3 und Bemerkung 17.2 gilt $\mathfrak{m}M = M$ mit

$$M := \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n$$

Mit Nakayamas Lemma ist $M = 0$. Da jede Nicht-Einheit in einem Maximalideal, also $\mathfrak{m}$, liegt, ist

$$R = \mathfrak{m} \cup R^\times$$

eine disjunkte Vereinigung. Sei $0 \neq r \in R$ dann gibt es ein $n \in \mathbb{N}$ und ein $u \in R^\times$ derart, dass r als $r = x^n \cdot u$ dargestellt werden kann, denn sei n das Maximum[2], so dass $r = x^n \cdot v$ mit $v \in R$, gilt, dann ist $r \in R^\times$ sonst wäre $r \in (x)$, was ein Widerspruch zur Maximalität von n wäre.
Also ist jedes Ideal von R, das nicht das Nullideal ist, von der Form (x^n). Diese sind keine Primideale für $n > 1$, also ist (0) das minimale Primideal. □

Anmerkung Bemerkung 17.4 gilt für reguläre Ringe beliebiger Dimension

Satz 17.5 *Sei R ein lokaler Noetherscher Ring der Dimension 1 mit Maximalideal $\mathfrak{m}$, dann sind äquivalent:*
(1) R ist normal (d.h. ganz abgeschlossener Integritätsring)
(2) R ist regulär
(3) R ist ein Hauptidealring

Beweis. Den Schluss von (2) nach (3) haben wir in Bemerkung 17.4 gezeigt. Der Schluss von (3) auf (1) ist trivial, denn Hauptidealrinnge sind faktoriell und faktorielle Ringe sind normal. Für (1) nach (2) zeige: $\mathfrak{m}$ ist ein Hauptideal.
Sei $0 \neq a \in \mathfrak{m}$ dann gibt es nach Bemerkung 17.1 ein $n \in \mathbb{N}$ derart, dass $\mathfrak{m}^n \subseteq (a)$ und $\mathfrak{m}^{n-1} \nsubseteq (a)$ gelten. Sei nun b ein Element aus $\mathfrak{m}^{n-1}$, das nicht in (a) liegt, dann definiere $x := \frac{a}{b} \in K = \mathrm{Quot}(R)$. Es gelten:

- $x^{-1} \notin R$, denn sonst wäre $\frac{b}{a} = r \in R$, also $b = ra \in (a)$, was einen Wiederspruch lieferte.
- Da R normal ist, kann x^{-1} nicht ganz über R sein.
- Es gilt $x^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$, denn sonst wäre, wegen $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, die Abbildung

  $$\phi : \mathfrak{m} \xrightarrow{\cdot x^{-1}} \mathfrak{m}$$

  ein Homomorphismus von R-Moduln. Da R Noethersch ist, ist $\mathfrak{m}$ endlich erzeugt, daher gäbe es dann $a_i \in R$, so dass nach Bemerkung 16.1

  $$(x^{-r} + a_{r-1} \cdot x^{-(r-1)} + \cdots + a_0)\mathfrak{m} = 0$$

  gelte. Da R ein Integritätsring ist folgte die Ganzheit von x^{-1} über R. Dies ist ein Widerspruch.
- $x^{-1}\mathfrak{m} = \frac{b}{a}\mathfrak{m} \subseteq R$, denn $b \cdot \mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$

[2] Dieses Maximum existiert sonst wäre $r \in \bigcap \mathfrak{m}^n$

Insgesamt folgt also $x^{-1}\mathfrak{m} = R$ und damit gilt $\mathfrak{m} = Rx = (x)$ □

Folgerung 17.6 *Sei R ein Noetherscher Integritätsring der Dimension 1, dann sind äquivalent:*
(1) R ist ein Dedekind-Ring
(2) R ist normal
(3) Für alle Maximalideale $\mathfrak{m} \lhd R$ ist $R_{\mathfrak{m}}$ normal
(4) Für alle Maximalideale $\mathfrak{m} \lhd R$ ist $R_{\mathfrak{m}}$ regulär
(5) Für alle Maximalideale $\mathfrak{m} \lhd R$ ist $R_{\mathfrak{m}}$ ein Hauptidealring

Beweis. Die Äquivalenz zwischen (1) und (2) ist die Definition 17.3, die Äquivalent zwischen (2) und (3) haben wir in Satz 14.5 gezeigt und der Rest folgt unmittelbar aus Satz 17.5. □

Bemerkung 17.7 *(Anschauung zur Lokalisierung)*
Sei K ein algebraisch abgeschlossener Körper und $f \in K[X,Y]$ ein irreduzibles, nicht konstantes Polynom. Bezeichne $C := V_f(K)$ und $K[C] = {}^{K[X,Y]}\!/_{(f)}$ den zugehörigen Koordinatenring sowie $K(C) := \mathrm{Quot}(K[C])$ den Funktionenkörper. Sei weiter $\mathfrak{m} = (X-a, Y-b)$ ein Maximalideal von $K[C]$ mit $f((a,b)) = 0$, also $(a,b) \in C$, dann ist

$$K[C]_{\mathfrak{m}} = \left\{ \frac{g}{h} \in K(C) \;\middle|\; h\big((a,b)\big) \neq 0 \right\}$$

Beweis. Es gilt

$$\begin{aligned} \mathfrak{m} &= \mathrm{Ker}\left(\phi : K[C] \xrightarrow{(X,Y)\mapsto(a,b)} K\right) \\ &\cong \{\, h \in K[C] \,|\, h(a,b) = 0 \,\} \end{aligned}$$

□

In Worten Die Lokalisierung des Koordinatenrings am Maximalideal zum Punkt (a,b) der Kurve ist die Menge aller Funktionen im Funktionskörper des Koordinatenrings, die im Punkte (a,b) definiert sind, d.h. es sind genau diejenigen Funktionen, die in einer Umgebung von (a,b) definiert sind.

Bemerkung 17.8 *Sei K ein algebraisch abgeschlossener Körper und $f \in K[X,Y]$ ein irreduzibles, nicht konstantes Polynom. Bezeichne $C := V_f(K)$ und $K[C] = {}^{K[X,Y]}\!/_{(f)}$ den zugehörigen Koordinatenring sowie $K(C) := \mathrm{Quot}(K[C])$ den Funktionenkörper. Sei weiter $\mathfrak{m} = (X-a, Y-b)$ ein Maximalideal von $K[C]$ mit $f((a,b)) = 0$, also $(a,b) \in C$, dann sind äquivalent*
(1) Der Punkt $(a,b) \in C$ ist nicht singulär
(2) $K[C]_{\mathfrak{m}}$ ist ein regulärer, lokaler Ring

Beweis. Ohne Beschränkung der Allgemeinheit kann $(a,b) = (0,0)$ vorausgesetzt werden, sonst führe Variablentrasformation durch. Damit ist $\mathfrak{m} := (X,Y) + (f) \lhd K[C]_{\mathfrak{m}}$. Wir wissen

$$f(X,Y) = \alpha X + \beta Y + \text{ höhere Terme}$$

Zu (1) $\Rightarrow$ (2): Der Punkt $(a,b) = (0,0)$ ist nach Voraussetzung nicht singulär, daher gilt $\alpha \neq 0$ oder $\beta \neq 0$. Ohne Einschränkung sei $\alpha \neq 0$, dann gilt

$$\begin{aligned} X &= \frac{1}{\alpha}\Big(f(X,Y) - \beta Y - \text{ höhere Terme }\Big) \\ &= -\frac{\beta}{\alpha} Y \big(\mathfrak{m}^2\big) \end{aligned}$$

Also ist $\dim_{K[C]/\mathfrak{m}} \left(\mathfrak{m}/\mathfrak{m}^2\right) = 1$ und somit folgt die Regularität von $K[C]_\mathfrak{m}$, denn $K[C]_\mathfrak{m}$ hat, weil $K[C]$ Dimension 1 hat und die Höhe von $\mathfrak{m}$ ebenfalls 1 ist, die Dimension 1.
Zu (2) $\Rightarrow$ (1): Sei (a, b) ein singulärer Punkt, dann gilt $\alpha = \beta = 0$. Es folgt

$$\dim_{K[C]_\mathfrak{m}/K[C]_\mathfrak{m} R} \left(\mathfrak{m}/\mathfrak{m}^2\right) = 2$$

denn $\mathfrak{m}$ wird von X und Y erzeugt. Dann ist $K[C]_\mathfrak{m}$ aber nicht regulär. □

Folgerung 17.9 *Seien K ein algebraisch abgeschlossener Körper, $f \in K[X, Y]$ in irreduzibles, nicht konstantes Polynom und bezeichne $C = V_f(K)$, dann sind äquivalent:*
(1) $K[C]$ ist ein Dedekind-Ring
(2) C ist nicht-singulär

Beweis. Nach Folgerung 16.12 ist $K[C]$ ein Ring der Dimension 1 und Noethersch. Die Aussage folgt nun aus Folgerung 17.6 und Bemerkung 17.8. □

Anhang

Literaturverzeichnis

[L1] **S. Bosch**, Algebra, Springer-Verlag
[L2] **G. Wiese**, Algebra I WS 08/09
http://www.uni-due.de/∼hx0037/notes/AlgebraI.pdf
[L3] **J. Neukirch**, Algebraische Zahlentheorie, Springer-Verlag