Nulldimensionale Ideale und kommutierende Endomorphismen

(Quelle: Paper von L. Robbiano "Zero-Dimensional Ideals")
gehalten von: Eva Ludwig am 24.6.'03

1 Motivation und Einleitung:

1.1 Definition: Sei I ein Ideal in $P = K[x_1, ..., x_n]$. I heißt nulldimensional genau dann, wenn der K-Vektorraum P/I endlich dimensional ist.
I sei im weiteren immer nulldimensional!

1.2 Beschreibung von I: Dies ist möglich durch eine Menge von Erzeugenden (In $K[x]$ ist jedes Ideal Hauptideal; in $K[x_1, ..., x_n]$ ist jedes Ideal endlich erzeugt, vgl. Hilbert-Basissatz), oder über eine Beschreibung von P/I als K-Vektorraum. I ist allein durch die Vektorraum-Struktur aber noch nicht eindeutig bestimmt.

Beispiel 1: $P = K[x], I = \langle x^4 - 1\rangle, K[x]/I = P/I \cong \langle 1, x, x^2, x^3\rangle$
Aber auch zum z.B. $K[x]/\langle x^4 + 2x^2 - 1\rangle \cong \langle 1, x, x^2, x^3\rangle$
$\Rightarrow$ Keine ausreichende Beschreibung von I.

1.3 Definition: Die Abbildungen
$\Phi_{x_i} : \begin{array}{ccc} P/I & \to & P/I \\ f + I & \mapsto & x_i f + I \end{array}$ für $i \in \{1, ..., n\}$ heißen Multiplikationsendomorphismen. Die zugehörigen Matrizen $\mathcal{M}^{\overline{\mathcal{O}}}_{\Phi_{x_i}}$ bezüglich einer Basis $\overline{\mathcal{O}} = \{\overline{f}_1, ..., \overline{f}_\mu\}$von P/I heißen Multiplikationsmatrizen. Sie sind paarweise kommutierend.
Mit Hilfe dieser Matrizen ist eine eindeutige Beschreibung von I durch $P/I \cong V$ möglich.

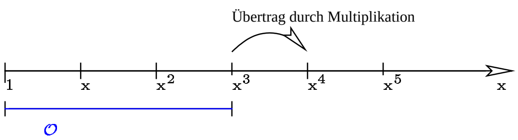
Beispiel 1(Fortsetzung): Wähle eine Basis $\mathcal{O} = \{1, x, x^2, x^3\}$ von P/I.

$$\Phi_x : \begin{array}{ccc} V(\mathcal{O}) & \to & V(\mathcal{O}) \\ a \cdot 1 + bx + cx^2 + dx^3 & \mapsto & ax + bx^2 + cx^3 + d \cdot 1 \end{array} \quad \mathcal{M}^{\mathcal{O}}_{\Phi_x} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Wie sieht I aus? $I = \langle x^4 + p_3x^3 + p_2x^2 + p_1x + p_4\rangle$ Berechne

$$x \cdot x^3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1 \Rightarrow x^4 = 1(modI) \Rightarrow x^4 - 1 \in I$$

x^3 ist der einfachste Fall, der einen Übertrag erzeugt. Andere Überträge gibt es nicht. Also: $J = \langle x^4 - 1\rangle$ und da $dimP/J = 4 = dimP/I$ folgt $J = I$.



Was passiert bei anderen Polynomen?

$$x \cdot (x^2 - x + 1) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 1 \end{pmatrix} = x - x^2 + x^3$$

$\Rightarrow x^3 - x^2 + x = x - x^2 + x^3 (modI) \Rightarrow 0 \in I$

$$x \cdot (x^3 + x - 1) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} = 1 - x + x^2$$

$\Rightarrow x^4 + x^2 - x = 1 - x + x^2 (modI) \Rightarrow x^4 - 1 \in I$

Beispiel 2: $P = K[x,y], I = \langle x^2, y^3 \rangle, \mathcal{O} = \{1, x, xy, xy^2, y, y^2\}$ Basis von $V \cong P/I$.

$$\begin{array}{cccc} \Phi_x : & V(\mathcal{O}) & \rightarrow & V(\mathcal{O}) \\ & a + bx + cxy + dxy^2 + ey + fy^2 & \mapsto & ax + \underbrace{bx^2 + cx^2y + dx^2y^2}_{=0 \text{ da aus I}} + exy + fxy^2 \end{array}$$

$$\mathcal{M}_{\Phi_x}^{\mathcal{O}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ zu } \Phi_y : \mathcal{M}_{\Phi_y}^{\mathcal{O}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Berechne J:

$$x \cdot x = \mathcal{M}_{\Phi_x}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 0 \Rightarrow x^2 \in J$$

$$x \cdot xy = \mathcal{M}_{\Phi_x}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 0 \Rightarrow x^2y \in J$$

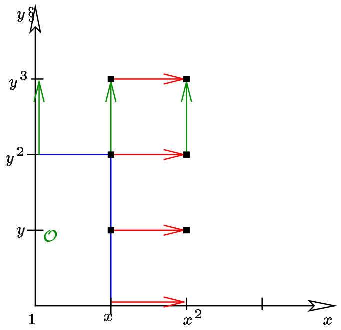
$$x \cdot xy^2 = \mathcal{M}_{\Phi_x}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 0 \Rightarrow x^2y^2 \in J$$

$$y \cdot xy^2 = \mathcal{M}_{\Phi_y}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 0 \Rightarrow xy^3 \in J$$

$$y \cdot y^2 = \mathcal{M}_{\Phi_y}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0 \Rightarrow y^3 \in J$$

$x \cdot (y \cdot xy^2) = x \cdot 0 = 0$ und $y \cdot (x \cdot xy^2) = y \cdot 0 = 0 \Rightarrow x^2y^3 \in J$

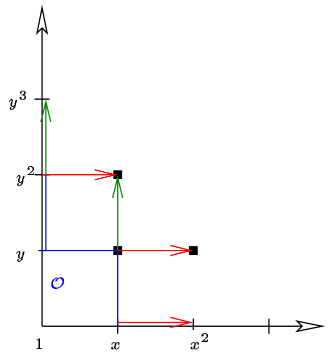
$\Rightarrow J = \langle x^2, x^2y, x^2y^2, xy^3, y^3, x^2y^2 \rangle = \langle x^2, y^3 \rangle = I$



Beispiel 3: $P = K[x,y], I = \langle x^2 - 1, xy^2, y^3 \rangle, \mathcal{O} = \{1, x, y, xy, y^2\}$ Basis von $V \cong P/I$

$$\mathcal{M}_{\Phi_x}^{\mathcal{O}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \mathcal{M}_{\Phi_y}^{\mathcal{O}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Berechne J:



$$x \cdot x = \mathcal{M}_{\Phi_x}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1 \Rightarrow x^2 - 1 \in J$$

$$x \cdot xy = \mathcal{M}_{\Phi_x}^{\mathcal{O}} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = y \Rightarrow x^2y - y \in J$$

$$x \cdot y^2 = \mathcal{M}^{\mathcal{O}}_{\Phi_x} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0 \Rightarrow xy^2 \in J$$

$$y \cdot xy = \mathcal{M}^{\mathcal{O}}_{\Phi_y} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 0 \Rightarrow xy^2 \in J$$

$$y \cdot y^2 = \mathcal{M}^{\mathcal{O}}_{\Phi_y} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0 \Rightarrow y^3 \in J$$

$$y \cdot (x \cdot x) = \mathcal{M}^{\mathcal{O}}_{\Phi_y} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = y \Rightarrow x^2y - y \in J$$

$$y \cdot (x \cdot xy^2) = \mathcal{M}^{\mathcal{O}}_{\Phi_y} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = y^2 \Rightarrow x^2y^2 - y^2 \in J$$

$\Rightarrow J = \langle x^2 - 1, x^2y - y, xy^2, y^3, x^2y^2 - y^2 \rangle = \langle x^2 - 1, xy^2, y^3 \rangle$
$dim(P/J) = 5 \Rightarrow J = I$

2 Isomorphie und Bedingungen:

2.1 Definition: Es existiert ein eindeutiger K-Algebra-Homomorphismus

$$\begin{array}{lccc} \Theta : & P & \to & End_K(V) \\ & x_i & \mapsto & \Phi_i : V \to V \\ & 1 & \mapsto & Id \\ & \Theta(f(x_1, ..., x_n)) & = & f(\Phi_1, ..., \Phi_n). \end{array}$$

Es gibt eine P-Modulstruktur auf V definiert durch $f(x_1, ..., x_n) \cdot v = f(\Phi_1, ..., \Phi_n)(v)$, wobei $\Phi_1, ..., \Phi_n \in End_K(V)$ paarweise kommutierend sind.

2.2 Satz: i) Θ induziert einen K-Algebra-Isomorphismus $P/kern(\Theta) \cong K[\Phi_1, ..., \Phi_n]$
ii) $kern(\Theta)$ ist ein nulldimensionales Ideal
iii) $kern(\Theta) = Ann_P(V) := \{p \in P \mid p \cdot V = 0\}$

Beweis: i) folgt aus dem Homomorphiesatz: $P/kern(\Theta)$ ist isomorph zum $Bild(\Theta)$
ii) folgt aus i) ($K[\Phi_1, ..., \Phi_n]$ ist Untervektorraum des Endomorphismenringes, also endlich dimensional) und der Definition nulldimensional.
iii) Sei $v \in V$ beliebig: $f \in Ann_P(V) \Leftrightarrow f(x_1, ..., x_n) \cdot v = 0$
$\Leftrightarrow f(\Phi_1, ..., \Phi_n) = 0 \Leftrightarrow V \in kern(\Theta)$

$\square$

<u>2.3 Definition und Satz:</u> Es existiert eine Abbildung $\Theta_w : P \to V, w \in V$ beliebig aber fest, definiert durch $\Theta_w(f) = f(\Phi_1, ..., \Phi_n)(w)$. ($\Theta_w$ ist also eine Auswertung von f an der Stelle w.) $Kern(\Theta_w)$ ist ein nulldimensionales Ideal.

Beweis: $kern(\Theta) \subseteq kern(\Theta_w)$ und $P/kern(\Theta) \supseteq P/kern(\Theta_w)$.
Da $kern(\Theta)$ nulldimensionales Ideal ist, folgt $P/kern(\Theta)$ ist endlich dimensional, und so auch $P/kern(\Theta_w)$. $\Rightarrow kern(\Theta_w)$ ist nulldimensional.

□

<u>2.4 Satz</u> Θ_w ist durch folgende Eigenschaften charakterisiert, d.h. eindeutig festgelegt:
i) Θ_w ist linear
ii) $\Theta_w(1) = w$
iii) $\Theta_w(x_i f) = \Phi_i(\Theta_w(f)) \forall f \in P$

Beweis: Die Eigenschaften folgen aus den Definitionen. Zeige nun: Für eine beliebige Abbildung $\varphi : P \to V$ mit diesen Eigenschaften gilt $\varphi = \Theta_w$. Wegen der Linearität reicht es zu zeigen, daß φ und Θ_w in den Termen übereinstimmen. Mit Induktion über den Grad:
Induktionsanfang: $\Theta_w(1) = w$
Induktionsschluß: Sei t Term vom Grad d und die Terme von φ und Θ_w vom Grad $\leq d-1$ stimmen überein. Schreibe $t = x_i t'$ mit
$grad(t') = d - 1$. Mit der dritten Eigenschaft folgt:
$\varphi(t) = \varphi(x_i t') = \Phi_i(\varphi(t')) = \Phi(\Theta_w(t')) = \Theta_w(t)$.

□

<u>2.5 Folgerung:</u> Sei I ein nulldimensionales Ideal in $P = K[x_1, ..., x_n]$. Mit den Multiplikationsmatrizen $\Phi_{x_1}, ..., \Phi_{x_n} \in End_K(P/I)$ erhalten wir:

$$i)\ \Theta : \begin{array}{ccc} P & \to & End_K(P/I) \\ x_i & \mapsto & \Phi_{x_i} : P/I \to P/I \\ \Theta(f(x_1,...,x_n)) & = & f(\Phi_{x_1},...,\Phi_{x_n}), \end{array}$$

wobei $kern(\Theta) = I$.

$$\Theta_w : \begin{array}{ccc} P & \to & P/I \\ \Theta_w(f) & = & f(\Phi_{x_1},...,\Phi_{x_n})(w) \end{array}$$

ii) Θ induziert einen K-Algebra-Isomorphismus $P/I \cong K[\Phi_{x_1}, ..., \Phi_{x_n}]$.
iii) Der K-Vektorraum P/I ist ein zyklischer P-Modul via $\Phi_{x_1}, ..., \Phi_{x_n}$ und $P/I \cong \langle 1 \rangle$.

Beweis: i) $I \subseteq kern(\Theta)$: Sei $f \in I$. Zeige $f(\Phi_{x_1}, ..., \Phi_{x_n})$ ist die Nullabbildung. Betrachte $f(\Phi_{x_1}, ..., \Phi_{x_n})(\overline{h}) \equiv 0 (mod I)\ \forall h \in P$, da $f \in I$, also $\overline{f} \cdot \overline{h} = \overline{0} \cdot \overline{h}$.
$kern(\Theta) \subseteq I$: Sei $f \in kern(\Theta) \Rightarrow f(\Phi_{x_1}, ..., \Phi_{x_n})$ ist die Nullabbildung. Betrachte $f(\Phi_{x_1}, ..., \Phi_{x_n})(\overline{1}) = \overline{f(x_1, ..., x_n)} \cdot 1 = 0 \Rightarrow f \in I$
ii) für $kern(\Theta) = I$
iii) $f(x_1, ..., x_n) \cdot \overline{1} = f(\Phi_{x_1}, ..., \Phi_{x_n})(\overline{1} = \overline{f(x_1, ..., x_n)} \forall f \in P$
$\Rightarrow 1$ erzeugt P/I.

□

<u>2.6 Satz:</u> Sei V endlich dimensionaler K-Vektorraum, $\Phi_1, ..., \Phi_n \in End_K(V)$ paarweise kommutierend, sei $I = kern(\Theta) = Ann_P(V)$, sei $w \in V$. Folgende

Aussagen sind äquivalent:
i) $\overline{\Theta}_w : P/I \to V$ ist Vektorraum-Isomorphismus.

$$\begin{tikzcd} P \arrow[r, "\Theta_w"] \arrow[d, "\rho \text{ Projektion}"'] & V \\ P/I \arrow[ur, "\overline{\Theta}_w"'] & \end{tikzcd}$$

ii) $\Theta_w : P \to V$ ist surjektiv.
iii) V ist zyklischer P-Modul via $\Phi_1, ..., \Phi_n$ und $V = \langle w \rangle$ als P-Modul.
iv) Es existiert ein Tupel $(h_1, ..., h_\mu)$ von Polynomen dessen Restklassen eine Basis von P/I bilden so, daß das zugehörige Tupel $(\Theta_w(h_1), ..., \Theta_w(h_\mu))$ eine K-Vektorraumbasis von V ist.
v) Für alle Tupel $(h_1, ..., h_\mu)$ von Polynomen deren Restklassen eine Basis von P/I bilden, ist $(\Theta_w(h_1), ..., \Theta_w(h_\mu))$ eine K-Vektorraumbasis von V.

Beweis: i)$\Rightarrow$ii) $\Theta_w = \overline{\Theta}_w \circ \rho$, Surjektivität bleibt erhalten(ρ aus dem Bild).
ii)$\Rightarrow$iii) $\forall v \in V : v = \Theta_w(f)$ für ein $f \in P$ (da Θ_w surjektiv) und $v = \Theta_w(f) = f(x_1, ..., x_n) \cdot w \Rightarrow V = \langle w \rangle$
iii)$\Rightarrow$v) Sei $(h_1, ..., h_\mu)$ eine Basis vonP/I.

$$v = f(x_1, ..., x_n) \cdot w = (\sum_{i=1}^{\mu} a_i h_i(\Phi_1, .., \Phi_n))(w) = \sum_{i=1}^{\mu} a_i \Theta_w(h_i)$$

$\Rightarrow (\Theta_w(h_1), ..., \Theta_w(h_\mu))$ erzeugt V.
Angenommen $\sum_{i=1}^{\mu} a_i \Theta_w(h_i) = 0 \Rightarrow \sum_{i=1}^{\mu} a_i h_i(\Phi_1, .., \Phi_n)$ verschwindet auf V
$\Rightarrow \sum_{i=1}^{\mu} a_i \overline{h_i(x_1, ..., x_n)} \equiv 0(mod I)$, also $a_i = 0 \forall i = 1, ..., \mu$ da $(h_1, ..., h_\mu)$ Basis.
v)$\Rightarrow$iv) Spezialisierung (etwas gilt für alle, also gibt es auch ein bestimmtes so, daß das gilt)
iv)$\Rightarrow$i) Θ_w bildet Basis auf Basis ab, also auch $\overline{\Theta}_w$

$\square$

<u>Zusatz:</u> Unter diesen Bedingungen ist $I = kern(\Theta_w)$.
(aus i) mit $\Theta_w = \overline{\Theta}_w \circ \rho, kern(\rho) = I, \overline{\Theta}_w$ surjektiv)

<u>2.7 Satz:</u> Sei $\varphi : P \to V$ K-lineare surjektive Abbildung mit $kern(\Theta)$ ist ein Ideal und $\varphi(1) = w$.
i) Es folgt: $\Phi_i(\varphi(f)) = \varphi(\Phi_{x_i}(f))$ definiert paarweise kommutierende Endomorphismen $\Phi_i \in End_K(V), i = 1, ..., n$, so daß: $\varphi = \Theta_w$
und $\varphi(f) = f(\Phi_1, ..., \Phi_n)(w)$
ii) Für $V = \langle w \rangle$ als P-Modul via $\Phi_1, ..., \Phi_n$ gilt: $\Phi_i = \overline{\Theta}_w \Phi_{x_i} \overline{\Theta}_w^{-1}$.

Beweis: i) Wohldefiniertheit: $\varphi(f)$ bildet ganz$V$ da φ surjektiv.
Seien $f \neq g \in P$ mit $\varphi(f) = \varphi(g)$. Zu zeigen: $\varphi(\Phi_{x_i}(f)) = \varphi(\Phi_{x_i}(g))$.
$\varphi(f) = \varphi(g) \Rightarrow \varphi(f - g) = 0$
$\Rightarrow f - g \in kern(\varphi)$

$\Rightarrow x_i(f-g) \in kern(\varphi)$
$\Rightarrow \varphi(x_i(f-g)) = 0$
$\Rightarrow \varphi(x_i f) = \varphi(x_i g)$
φ induziert einen Isomorphismus $\overline{\varphi} : P/I \to V$, benutze 2.6
ii) $\forall v \in V$ existiert $f(x_1, ..., x_n) \in P$:
$v = f(x_1, ..., x_n) w \overline{\varphi} \Phi_{x_i} \overline{\varphi}^1(v) = \overline{\varphi}\Phi_{x_i}(f(x_1, ..., x_n) \cdot w)$
$= \overline{\varphi}(x_i(f(x_1, ..., x_n) \cdot w)) = \Phi_i f(\Phi_1, ...; \Phi_n)(w)$
$= \Phi_i(f(x_1, ..., x_n) \cdot w) = \Phi_i(v)$

□

3 Algorithmen

3.1 Algorithmus: Gegeben: V endlich dimensionaler K-Vektorraum, $\Phi_1, ..., \Phi_n \in End_K(V)$ paarweise kommutierend, $P = K[x_1, ..., x_n]$
Wähle Basis $\mathcal{E}$ von V und betrachte den Homomorphismus

$$\begin{array}{lccc} \Theta : & P & \to & K[\mathcal{M}^{\mathcal{E}}_{\Phi_1}, ..., \mathcal{M}^{\mathcal{E}}_{\Phi_n}] \\ & x_i & \mapsto & \mathcal{M}^{\mathcal{E}}_{\Phi_i} \end{array}$$

Wir wissen: $J = kern(\Theta)$!
Berechne $Ann_P(V) = J$!
Benutze hierzu eine Variante des Buchberger-Möller-Algorithmus. Dieser wurde im Vortrag "Berechnung von Verschwindungsidealen" explizit angegeben(Alg.2.3). Nenne $\mathcal{G} = J$ und ändere Schritt C3 wie folgt:
$t \in L$. Berechne $\Theta(t) = (\mathcal{M}^{\mathcal{E}}_{\Phi_1})^{\alpha_1} \cdot ... \cdot (\mathcal{M}^{\mathcal{E}}_{\Phi_n})^{\alpha_n}$ und erhalte eine Matrix mit den Einträgen (a^t_{kl}). Schreibe diese nun als Zeile $a^{(t)}_{11}, a^{(t)}_{12}, ..., a^{(t)}_{ss}$. Fahre mit dieser Zeile wie im Algorithmus beschrieben fort. Man erhält in C4 als Polynom eine Kombination von Elementen aus S, die man sowohl als Kombination der Multiplikationsmatrizen als auch als Kombination der zugehörigen Multiplikationen mit $x_1, ..., x_n$ aufschreiben kann.

Beispiel 4: $V = \mathbb{Q}^3, \mathcal{E} = (e_1, e_2, e_3)$ Basis von V

$$\Phi_1 : \mathcal{M}^{\mathcal{E}}_{\Phi_1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} =: M_1, \Phi_2 : \mathcal{M}^{\mathcal{E}}_{\Phi_2} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix} =: M_2$$

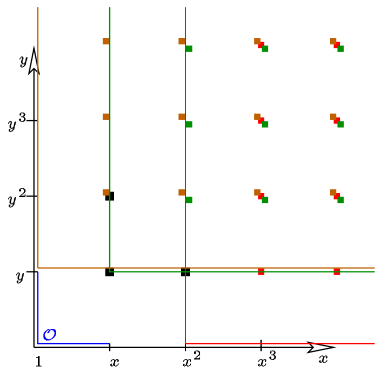
Berechne Erzeugende von J, wobei $P/J \cong \mathbb{Q}[\Phi_1, \Phi_2]$ und $P = \mathbb{Q}[x, y]$. Benutze nun die Variante des Buchberger-Möller-Algorithmus mit einer gradkompatiblen Termordnung. Es reicht $M_1{}^2 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}, M_1 M_2 = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 2 & 1 \end{pmatrix}, M_2{}^2 = \begin{pmatrix} 0 & 3 & 2 \\ 0 & 5 & 3 \\ 0 & 3 & 2 \end{pmatrix}$ zu berechnen, da man diese schon als Linearkombination der Matrizen vom Grad 1 schreiben lassen. Dann liegen folgende Relationen im $kern(\Theta)$: $\Theta(t) = M_1^{\alpha}{}_1 \cdot M_2^{\alpha}{}_2 = 0$ für $M_1{}^2 - M_2, M_1 M_2 - M_1 - M_2, M_2{}^2 - M_1 - 2M_2$, bzw. als Terme geschrieben: $\{x^2 - y, xy - x - y, y^2 - x - 2y\}$ ist eine Gröbner-Basis von J.

3.2 Bemerkung: Der Algorithmus ist auf den Modulfall übertragbar. Sei V ein K-Vektorraum mit Basis $\mathcal{W} = (w_1, ..., w_\mu)$, also $V = \langle w_1, ..., w_\mu \rangle$ als P-Modul. $\Theta_{\mathcal{W}} : P^\mu \to V$ ist definiert durch $\Theta_{\mathcal{W}}(f_1, ..., f_\mu) = \sum_{i=1}^{\mu} \Theta_{wi}(f).\Theta_{\mathcal{W}}$ ist

surjektive Abbildung von P-Moduln und $P^\mu / kern(\Theta_{\mathcal{W}}) \cong V$.
$(\Theta_{wi}(f) = \Theta(f)(w_i) = f(x_1, ..., x_n) \cdot w_i)$ Auch in diesem Fall läßt sich $kern(\Theta_{\mathcal{W}})$ mit einer Variante des Buchberger-Möller-Algorithmus berechnen.

3.3 Algorithmus: Gegeben: V endlich dimensionaler K-Vektorraum, $\Phi_1, ..., \Phi_n \in End_K(V)$ paarweise kommutierend, $J = kern(\Theta)$.
Überprüfe ob V zyklisch ist!
1. Führe Algorithmus 1 durch und erhalte Gröbner-Basis von J und Basis $\mathcal{O} = (t_1, ..., t_\mu)$ von P/J. Übernehme $\mathcal{E}, \mathcal{M}^{\mathcal{E}}_{\Phi_1}, ..., \mathcal{M}^{\mathcal{E}}_{\Phi_n}$.
2. Abbruch für $dim(V) \neq \mu$: V ist kein zyklischer P-Modul via $\Phi_1, ..., \Phi_n$
3. Führe ein Tupel $u = (u_1, ..., u_\mu)$ neuer Unbestimmter ein. Definiere
$\mathcal{A}_u := (t_1(\mathcal{M}^{\mathcal{E}}_{\Phi_1}, ..., \mathcal{M}^{\mathcal{E}}_{\Phi_n}) \cdot u, ..., t_\mu(\mathcal{M}^{\mathcal{E}}_{\Phi_1}, ..., \mathcal{M}^{\mathcal{E}}_{\Phi_n}) \cdot u) \in K[\mathcal{M}^{\mathcal{E}}_{\Phi_1}(u), ..., \mathcal{M}^{\mathcal{E}}_{\Phi_n}(u)]$ und berechne $det(\mathcal{A}_u)$.
4. Abbruch für:
es existiert kein $u = (u_1, ..., u_\mu)$ mit $det(\mathcal{A}_u) \neq 0$: V ist kein zyklischer P-Modul via $\Phi_1, ..., \Phi_n$.
5. Wähle ein $w = (w_1, ..., w_\mu)$ mit $det(\mathcal{A}_u) \neq 0$: $V = \langle w \rangle$.

Beispiel 4(Fortsetzung): 1. Nach Algorithmus 1:
$\{x^2 - y, xy - x - y, y^2 - x - 2y\}$ Gröbner-Basis von J, $\mathcal{O} = \{1, x, y\}$ Basis von P/J.



2. $dim(V) = 3 = dim(P/J) \Rightarrow$ kein Abbruch
3. Sei $u = (u_1, u_2, u_3)$.
$\mathcal{A}_u = (1(M_1, M_2) \cdot u, x(M_1, M_2) \cdot u, y(M_1, M_2) \cdot u) = (Iu, M_1 u, M_2 u)$
$= \begin{pmatrix} u_1 & u_2 & u_2 + u_3 \\ u_2 & u_2 + u_3 & 2u_2 + u_3 \\ u_3 & u_2 & u_2 + u_3 \end{pmatrix}$
$det(\mathcal{A}_u) = ... = (u_1 - u_3)({u_3}^2 - {u_2}^2 + u_2 u_3)$
4. kein Abbruch
5. Alle $w = (w_1, w_2, w_3)$ mit $w_1 \neq w_3$ erzeugen $\mathbb{Q}^3$ als zyklischen P-Modul via Φ_1, Φ_2 mit Basis $\{w, \Phi_1(w), \Phi_2(w)\}$. (Wähle z.B. $w = (1, 1, 0)$)

3.4 Spezialfall: Betrachte $\Phi \in End_K(V)$ und $P = K[x]$. $kern(\Theta) = \langle m(\Phi) \rangle$, wobei $m(\Phi)$ das Minimalpolynom von Φ (da $m(\Phi) \in kern(\Theta)$ im Hauptidealring).
$\Rightarrow K[x]/\langle m(\Phi) \rangle \cong K[\Phi]$
Sei $m(\Phi) = a_0 + a_1 x + ... + a_{d-1} x^{d-1} + x^d$, $\overline{\mathcal{O}} = (\overline{1}, \overline{x}, ..., \overline{x^{d-1}})$ Basis von

$K[x]/\langle m(\Phi)\rangle \cong K[\Phi]$.

$\Rightarrow \mathcal{M}_x^{\overline{\mathcal{O}}} = \begin{pmatrix} 0 & & & -a_0 \\ 1 & & 0 & \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$ ist die Multiplikationsmatrix zu Φ_x. $\mathcal{M}_x^{\overline{\mathcal{O}}}$ ist genau die Frobenius Begleitmatrix von $m(\Phi)$.

Es gilt: Satz 2.6 $\Leftrightarrow dim_K(V) = d$

"$\Rightarrow$" 2.6iv) $\Rightarrow dim_K(V) = dim(K[x]/\langle m(\Phi)\rangle) = d$

"$\Leftarrow$" $dim_K(V) = d \Rightarrow m(\Phi) = \chi_\Phi \Rightarrow V$ ist zyklisch.

Beispiel 5: Für den Abbruch in 2.: $\Phi \in End_K(K^4) M = \mathcal{M}_\Phi^{\mathcal{E}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

$\chi_\Phi = x^4, M^2 = (0) \Rightarrow m(\Phi) = x^2$

$\Rightarrow 4 = dim(K^4) > deg(m(\Phi)) \Rightarrow K^4$ ist kein zyklischer $K[x]$-Modul via Φ.

Beispiel 6: Für Abbruch in 4.:

Alg.1:

1. $\mathcal{E} = (e_1, e_2, e_3)$ Basis des $\mathbb{Q}^3$.

$\Phi_1 : \mathcal{M}_{\Phi_1}^{\mathcal{E}} = M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in Mat_3(\mathbb{Q})$,

$\Phi_2 : \mathcal{M}_{\Phi_2}^{\mathcal{E}} = M_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in Mat_3(\mathbb{Q})$

2. ${M_1}^2 = M_1 M_2 = {M_2}^2 = (0)$ Dies sind die Relationen aus dem $kern(\Theta)$.

3. Mit einer Variante des Buchberger-Möller-Algorithmus folgt: $P/J \cong \mathbb{Q}[\Phi_1, \Phi_2]$ mit $J = (x^2, xy, y^2)$

Alg.2:

1. $\mathcal{O} = \{1, x, y\}$ Basis von P/J.

2. $dim(P/J) = dim(\mathbb{Q}^3)$

3. Sei $u = (u_1, u_2, u_3)$.

$\mathcal{A}_u = (1(M_1, M_2) \cdot u, x(M_1, M_2) \cdot u, y(M_1, M_2) \cdot u) = (Iu, M_1 u, M_2 u)$

$= \begin{pmatrix} u_1 & 0 & 0 \\ u_2 & u_1 & u_3 \\ u_3 & 0 & 0 \end{pmatrix}$

$det(\mathcal{A}_u) = u_1(u_1 \cdot 0 - 0 \cdot u_3) = 0$

$\Rightarrow$ Abbruch in 4., V ist kein zyklischer P-Modul via Φ_1, Φ_2.