Komplexität von Polynomidealen I

Quo vadis, Komplexitätstheorie?

Sommerakademie St. Johann 1998

Thorsten Warmt

15. September 1998

Literatur

David Cox, John Little, Donal O'Shea:
Ideals, Varieties, and Algorithms
An Introduction to Computational Algebraic Geometry and Commutative Algebra
Springer 1992

David Eisenbud: *Commutative Algebra* with a View toward Algebraic Geometry
Springer 1995

1 Algebraische Grundlagen

„L'Algébre est une langue bien faite et c'est la seule.“
Condillac

Definition 1.1. Ein *kommutativer Ring mit Eins* ist ein Tripel $(R, +, \cdot)$, kurz R, wobei R eine Menge und $+, \cdot$ innere Verknüpfungen auf R sind, so daß

i) $(R, +)$ ist eine abelsche Gruppe.

ii) $(R, \cdot)$ ist ein kommutativer Monoid, d.h. die Verknüpfung $\cdot$ ist assoziativ und kommutativ und es existiert ein Einselement bezüglich $\cdot$ in R.

Im folgenden sind alle Ringe kommutativ mit Eins.

Beispiel 1.2.

- Es sei R ein Ring. Der Polynomring in einer Variablen x über R ist

$$\begin{aligned} R[x] := R^{(\mathbb{N})} &= \{f : \mathbb{N} \to R | f(i) = 0 \text{ für fast alle } i \in \mathbb{N}\} \\ & \{(a_i)_{i\in\mathbb{N}}, a_i \in R | a_i = 0 \text{ für fast alle } i \in \mathbb{N}\} \end{aligned}$$

mit der Addition als üblicher Addition von Abbildungen und einer Multiplikation

$$(a_i) \cdot (b_i) := (c_i),$$

wobei

$$c_i := \sum_{\mu+\nu=i} a_\mu b_\nu.$$

Ein Element (a_i) des Polynomringes $R[x]$ wird notiert als

$$\sum_{i\in\mathbb{N}} a_i x^i.$$

- Iteration dieser Konstruktion ergibt den Polynomring in mehreren Variablen

$$R[x_1, \ldots, x_n] := (\ldots((R[x_1])[x_2])\ldots)[x_n].$$

Mit Multiindizes sind Elemente aus $R[x_1, \ldots, x_n]$ für $x = (x_1, \ldots, x_n)$ und $\mu = (\mu_1, \ldots, \mu_n)$ zu schreiben als

$$\sum_{\mu \in \mathbb{N}^n} a_\mu x^\mu = \sum_{(\mu_1, \ldots, \mu_n) \in \mathbb{N}^n} a_{\mu_1 \ldots \mu_n} x_1^{\mu 1} \cdots x_n^{\mu_n}.$$

Definition 1.3. Es sei R ein Ring. Eine Teilmenge $I \subset R$ heißt *Ideal* in R, i.Z. $I < R$, wenn gilt:

i) I ist eine additive Untergruppe von R.

ii) Ist $r \in R$ und $a \in I$, so folgt $ra \in I$.

Beispiel 1.4. Es sei k ein Körper. Sind $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, so ist

$$\langle f_1, \ldots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in K[x_1, \ldots, x_n] \right\}$$

das *von* $f_1, \ldots, f_s$ *in* $k[x_1, \ldots, x_n]$ *erzeugte Ideal.* $f_1, \ldots, f_s$ heißt *Basis des Ideals* $\langle f_1, \ldots, f_s \rangle$.

Frage 1.5. *Besitzt jedes Ideal in einem Polynomring eine endliche Basis?*

Satz 1.6: Hilberts Basissatz. *Ist ein Ring R noethersch, so ist auch der Polynomring $R[x]$ noethersch.*

Korollar 1.7. *Jedes Ideal I in $k[x_1, \ldots, x_n]$ besitzt eine endliche Basis, d.h. es gibt Polynome $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ mit $I = \langle f_1, \ldots, f_s \rangle$.*

2 Affine algebraische Geometrie

„Geometry is any branch of mathematics in which you can trace your primary source of information or intuition back to a sensorial experience"
E. Calabi

Ist $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ ein Polynom, so definiert dies durch Substitution eine Abbildung

$$\begin{array}{cccc} f: & k^n & \to & k \\ & (y_1, \ldots, y_n) & \mapsto & \sum_\alpha a_\alpha y^\alpha \end{array}.$$

Definition 2.1. Es sei k ein Körper, $M \subset k[x_1, \ldots, x_n]$ eine Menge von Polynomen, dann heißt

$$\mathcal{V}(M) := \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in M\}$$

die von M definierte *affine Varietät.*

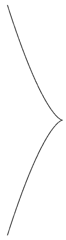
Umgekehrt wird definiert:

Definition 2.2. Sei $V \subset k^n$ eine affine Varietät.

$$\mathcal{I}(V) := \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ für alle } (a_1, \ldots, a_n) \in V\}.$$

$\mathcal{I}(V)$ ist ein Ideal.

Beispiel 2.3. Die Neilsche Parabel $\mathcal{V}(y^2 - x^3)$.



Lemma 2.4. *Es seien $f_1, \ldots, f_s$ Polynome aus $k[x_1, \ldots, x_n]$, dann gilt*

$$\mathcal{V}(\{f_1, \ldots, f_s\}) = \mathcal{V}(\langle f_1, \ldots, f_s \rangle).$$

Satz 2.5. *Es seien V und W affine Varietäten im k^n, dann gilt:*

- $V \subset W \Leftrightarrow \mathcal{I}(V) \supset \mathcal{I}(W)$,
- $V \subsetneq W \Leftrightarrow \mathcal{I}(V) \supsetneq \mathcal{I}(W)$ *und*
- $\mathcal{V}(\mathcal{I}(V)) = V$.

Satz 2.6: (Starker) Hilbertscher Nullstellensatz.
Ist k ein algebraisch abgeschlossener Körper, $I < k[x_1, \ldots, x_n]$ ein Ideal, dann gilt

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = \{r \in R : r^i \in I \text{ für ein } i \in \mathbb{N}\}.$$

3 Probleme

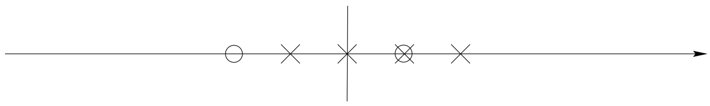
Frage 3.1: PIMP. *Gilt für gegebene Polynome $f, f_1, \ldots, f_s$*

$$f \in \langle f_1, \ldots, f_s \rangle?$$

Die Geometrie der Varietät eines Polynoms in einer Variablen ist sehr einfach, die Frage 3.1 ist in diesem Fall schnell zu beantworten:

Beispiel 3.2.

$$f = (x-1)x(x+1)(x+2) = x^4 + 2x^3 - x^2 - 2x$$
$$f_1 = (x+1)(x-2) = x^2 - x - 2$$



$$\begin{array}{l}
(x^4 + 2x^3 - x^2 - 2x) \quad : (x^2 - x - 2) = x^2 + 3x + 4 + \frac{8x+8}{x^2-x-2} \\
\underline{x^4 - x^3 - 2x^2} \\
\quad 3x^3 + x^2 - 2x \\
\quad \underline{3x^3 - 3x^2 - 6x} \\
\qquad 4x^2 + 4x \\
\qquad \underline{4x^2 - 4x - 8} \\
\qquad\qquad 8x + 8
\end{array}$$

Frage 3.3. *Sind zwei durch Basen gegebene Polynomideale*

$$\langle f_1, \ldots, f_s \rangle$$

und

$$\langle g_1, \ldots, g_t \rangle$$

gleich?

Frage 3.4. *Wie sind beschreibende Gleichungen des Abschlusses einer durch polynomielle Parametrisierung gegebenen Menge zu finden?*
D.h. zu gegeben Polynomen $p_1, \ldots, p_n \in k[x_1, \ldots, x_s]$ sind die beschreibenden Gleichungen der kleinsten affinen Varität gesucht, die das Bild der Abblidung

$$\begin{array}{cccc} P: & k^s & \to & k^n \\ & (x_1, \ldots, x_s) & \mapsto & (p_1(x_1, \ldots, x_s), \ldots, p_n(x_1, \ldots, x_s)) \end{array}$$

enthält.

4 Gröbnerbasics

Definition 4.1. Eine *Monomordnung* auf $k[x_1, \ldots, x_n]$ ist eine Relation $>$ auf $\mathbb{N}_0^n$, für die gilt:

i) $>$ ist eine totale Ordnung auf $\mathbb{N}_0^n$.

ii) Sind $\alpha, \beta, \gamma \in \mathbb{N}_0^n$, so folgt aus $\alpha > \beta$, daß $\alpha + \gamma > \beta + \gamma$.

iii) $>$ ist eine Wohlordnung auf $\mathbb{N}_0^n$.

Definition 4.2. Sei $f = \sum_\alpha a_\alpha x^\alpha \not\equiv 0$ ein Polynom in $k[x_1, \ldots, x_n]$ und $>$ eine Monomordnung.

i) Der *Multigrad* von f bezüglich $>$ ist

$$\text{multideg}(f) = \max_{<}(\alpha \in \mathbb{N}_0^n : a : \alpha \neq 0).$$

ii) Der *Leitkoeffizient* von f bezüglich $>$ ist

$$\text{LK}(f) = a_{\text{multideg}(f)}.$$

iii) Das *Leitmonom* von f bezüglich $>$ ist

$$\text{LM}(f) = x^{\text{multideg}(f)}.$$

iv) Der *Leitterm* von f bezüglich $>$ ist

$$\text{LT}(f) = \text{LK}(f) \cdot \text{LM}(f).$$

Analoge Definitionen werden für Ideale und allgemeiner Mengen von Polynomen vorgenommen.

Beispiel 4.3: Lexikographische Ordnung. Es seien $\alpha, \beta \in \mathbb{N}_0^n$.
$\alpha >_{lex} \beta :\Leftrightarrow$ Der erste Vektoreintrag des Vektors $\alpha - \beta$ von links ungleich Null ist positiv.
Ist $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$, so gilt

- $\text{multideg}(f) = (3, 0, 0)$
- $\text{LK}(f) = -5$
- $\text{LM}(f) = x^3$
- $\text{LT}(f) = -5x^3$.

Beispiel 4.4: Graduierte lexikographische Ordnung. Es seien $\alpha, \beta \in \mathbb{N}_0^n$.
$\alpha >_{grlex} \beta :\Leftrightarrow$

$$|\alpha| > |\beta| \text{ oder } |\alpha| = |\beta| \text{ und } \alpha >_{lex} \beta.$$

Algorithmus 4.5: Divisionsalgorithmus.
Eingabe: $f_1, \dots, f_s, f$
Ausgabe: $a_1, \dots, a_s, r$, so daß

$$f = a_1 f_1 + \dots + a_s f_s + r,$$

$a_1 := 0; \dots a_s := 0; r := 0;$
$p := f;$
WHILE $p \neq 0$ DO
    $i := 1;$
    division:=false
    WHILE $i \leq s$ AND *division*=false DO
        IF $\mathrm{LT}(f_i)$ teilt $\mathrm{LT}(p)$ THEN
            $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
            $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
            $division := true$
        ELSE
            $i := i + 1$
    IF $division = false$ THEN
        $r := r + \mathrm{LT}(p)$
        $p := p - \mathrm{LT}(p)$

p ist der aktuelle Divident, r der aktuelle Rest.
Um die Korrektheit einzusehen zeigt man, daß nach jedem Schritt gilt

$$f = a_1 f_1 + \dots + a_s f_s + p + r :$$

- Nach einem Divisionsschritt bleibt $a_i f_i + p$ unverändert.
- Nach einem Restschritt bleibt $p + r$ unverändert.

Der Algorithmus hält, wenn $p = 0$, dann gilt also

$$f = a_1 f_1 + \dots + a_s f_s + r.$$

Der Multigrad von p fällt in jedem Schritt echt, $<$ ist eine Wohlordnung, also terminiert der Algorithmus.
Zu den Multigraden: Zu geeigneten Zeitpunkt ist jedes Monom von p von der Form $\mathrm{LT}(p)/\mathrm{LT}(f_i)$.

Beispiel 4.6. $f_1 = x^2y - z$, $f_2 = xy - 1$
$I = \langle f_1, f_2 \rangle$
$f = x^3 - x^2y - x^2z + xy + x - 1$
Lexikographische Ordnung.

$$\begin{array}{r|rl}
 & a_1 : & \\
 & a_2 : & \qquad\qquad r \\
\hline
 & x^3 - x^2y - x^2z + xyz + x - z & \longrightarrow x^3 \\
x^2y - z & -x^2y - x^2z + xyz + x - z & \\
xy - 1 & &
\end{array}$$

$$\begin{array}{r|rl}
 & a_1 : -1 & \\
 & a_2 : z & \qquad\qquad r \\
\hline
 & x^3 - x^2y - x^2z + xyz + x - z & \longrightarrow x^3 \\
x^2y - z & -x^2y - x^2z + xyz + x - z & \\
xy - 1 & \underline{-x^2y + z} & \\
 & -x^2z + xyz + x - 2z & \longrightarrow -x^2z \\
 & xyz + x - 2z &
\end{array}$$

$$
\begin{array}{l|rl}
 & a_1 : -1 & \\
 & a_2 : z & \qquad r \\
\hline
 & x^3-x^2y-x^2z+xyz+x-z & \longrightarrow x^3 \\
x^2y-z & -x^2y-x^2z+xyz+x-z & \\
xy-1 & \underline{-x^2y+z} & \\
 & -x^2z+xyz+x-2z & \longrightarrow -x^2z \\
 & xyz+x-2z & \\
 & \underline{xyz-z} & \\
 & x-z & \longrightarrow x-z
\end{array}
$$

Also $f = -f_1 + zf_2 + (x^3 - x^2z + x - z)$.
Division durch (f_2, f_1) ergibt $f = (-x + z)f_2 + (x^3 - x^2z)$.
Im Beispiel $f_1 = xy + 1$, $f_2 = y^2 - 1$, $f = xy^2 - x$ mit lexikographischer Ordnung ist der Rest einmal ungleich Null, einmal gleich Null.

Definition 4.7. Es sei $>$ eine Monomordnung auf $k[x_1, \ldots, x_n]$, $I < k[x_1, \ldots, x_n]$ ein Ideal. Eine endliche Teilmenge $G = \{g_1, \ldots, g_t\} \subset I$ heißt *Gröbnerbasis* von I, falls

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle .$$

Satz 4.8. *Eine Gröbnerbasis von I ist eine Basis von I.*

Beweis. Der Divisionsalgorithmus für ein $f \in I$ liefert

$$f = a_1g_1 + \cdots + a_tg_t + r,$$

wobei r durch keinen der $\mathrm{LT}(g_i)$ teilbar ist. Es gilt $r = 0$, denn:

$$r = f - a_1g_1 - \cdots - a_tg_t \in I$$

Wäre $r \neq 0$, dann folgte $\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ und $\mathrm{LT}(r)$ wäre teilbar durch ein $\mathrm{LT}(g_1)$. ⊡

Satz 4.9. *Es sei $G = (g_1, \ldots, g_t)$ eine Gröbnerbasis eines Ideals*

$$I < k[x_1, \ldots, x_n].$$

Dann existiert zu jedem Polynom $f \in I$ ein eindeutiges $r \in k[x_1, \ldots, x_n]$ mit

i) Kein Term von r ist durch eines der $\mathrm{LT}(g_i)$ teilbar.

ii) Es gibt $g \in I$, so daß $f = g + r$.

Insbesondere ist r der Rest im Divisionsalgorithmus angewendet auf G, f unabhängig von der Anordnung der g_i.

Beweis. Eindeutigkeit: $f = h_1 + r_1 = h_2 + r_2$.
$r_2 - r_1 = h_1 - h_2 \in I$, also $\mathrm{LT}(r_2 - r_1) \in \langle g_1, \ldots, g_t \rangle$. Damit ist $\mathrm{LT}(r_2 - r_1)$ teilbar durch ein $\mathrm{LT}(g_i)$. Aus der Eigenschaft i) folgt $r_2 - r_1 = 0$. ⊡

Korollar 4.10. *Sei $G = \{g_1, \ldots, g_t\}$ eine Gröbnerbasis eines Ideals*

$$I < k[x_1, \ldots, x_n]$$

und $f \in k[x_1, \ldots, x_n]$. Dann ist $f \in I$, genau dann wenn der Rest bei Division von f durch G Null ist.

Beweis.

- Ist der Rest Null, so folgt nach Definition von $\langle \ldots \rangle$ die Behauptung.
- Umgekehrt, ist $f \in I$, so erfüllt $r = 0$ die Anforderungen.

$\boxdot$

Damit ist PIMP berechenbar. Das Beispiel 4.6 nochmals aufgegriffen:
$f_1 = x^2y - z$, $f_2 = xy - 1$
$I = \langle f_1, f_2 \rangle$
$f = x^3 - x^2y - x^2z + xy + x - 1$
Singular-Skript:
```
ring r=0,(x,y,z),lp;
ideal i=(x2y-z,xy-1);
ideal j=groebner(i);
reduce(x3-x2y-x2z+xy+x-1,j);
```
ergibt Null als Ergebnis.

Ein allgemeineres Konzept ist die *Normalform*:

Definition 4.11. Es bezeichne $\mathcal{G}$ die Menge aller endlichen geordneten Teilmengen $G \subset (k[x])^r$. Eine Abbildung

$$\begin{array}{rccc} NF: & (k[x])^r \times \mathcal{G} & \to & (k[x])^r \\ & (f,G) & \mapsto & NF(f|G) \end{array}$$

heißt *Normalform* auf $(k[x])^r$, wenn für alle f, G gilt:

i) $NF(f|G) \neq 0 \Rightarrow \mathrm{LM}(NF(f|G)) \notin \langle \mathrm{LM}(G) \rangle$.

ii) $f - NF(f|G) \in \langle G \rangle$.

Ist G eine Gröbnerbasis eines Ideals I, so ist

$$NF(f|G) = 0 \Leftrightarrow f \in I$$

Satz 4.12. *Jedes nicht-triviale Ideal in $k[x_1, ldots, x_n]$ besitzt eine Gröbnerbasis.*

Definition 4.13: Das S-Polynom. Seien $f, g \in k[x_1, \ldots, x_n]$ mit $\mathrm{multideg}(f) = \alpha$ und $\mathrm{multideg}(g) = \beta$. Die Komponenten von γ seien $\gamma_i := \max\{\alpha_i, \beta_i\}$.
Das *S-Polynom* von f und g ist

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g.$$

Beispiel 4.14. $f = x^3y^2 - x^2y^3 + x$, $3x^4y - y^2$

$$\begin{array}{rcl} S(f,g) & = & \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g \\ & = & xf - \frac{1}{3} yg \\ & = & -x^3y^3 + x^2 - \frac{1}{3} y^3 \end{array}$$

Satz 4.15: Kriterium von Buchberger. *Sei $I < k[x_1 \ldots, x_n]$ ein Ideal. Eine Basis $G = (g_1, \ldots, g_t)$ von I ist eine Gröbnerbasis von I, falls für jedes Paar (i,j) mit $i \neq j$ der Rest bei Division von $S(g_i, g_j)$ durch G gleich Null ist.*

Algorithmus 4.16: Buchbergers Algorithmus.
Eingabe: $F = (f_1, \ldots, f_s)$
Ausgabe: Eine Gröbnerbasis $G = (g_1, \ldots, g_t)$ für $\langle f_1, \ldots, f_s \rangle$ mit $F \subset G$.

$G := F$;
REPEAT
    $G' := G$
    FOR jedes Paar $p, q, p \neq q$ in G' DO
        $S := \overline{S(p,q)}^{G'}$
        IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$

Beweis. Es gilt zu jeder Zeit $G \subset I$: $p, q \in I$, $S(p,q) \in I$ also $\overline{S(p,q)}^{G'} \in I$.
G enthält die Basis F, ist also selbst Basis.
Der Algorithmus terminiert: Es gilt jeweils $\langle \text{LT}(G') \rangle \subsetneq \langle \text{LT}(G) \rangle$, mit Hilberts Basissatz folgt die Behauptung. ⊡

Die so entstandene Basis ist nicht eindeutig und enthält eventuell überflüssige Elemente.

Definition 4.17. Eine *minimale Gröbnerbasis* für ein Polynomideal I ist eine Gröbnerbasis I, für die gilt:

i) $\text{LK}(p) = 1$ für alle $p \in G$.

ii) Für jedes $p \in G$ gilt $\text{LT}(p) \notin \langle \text{LT}(G - \{p\}) \rangle$.

Eine solche Basis kann durch Elimination entsprechender Elemente aus einer Gröbnerbasis berechnet werden.

Definition 4.18. Eine *reduzierte Gröbnerbasis* für ein Polynomideal I ist eine Gröbnerbasis I, für die gilt:

i) $\text{LK}(p) = 1$ für alle $p \in G$.

ii) Für jedes $p \in G$ liegt kein Monom von p in $\langle \text{LT}(G - \{p\}) \rangle$.

Eine reduzierte Gröbnerbasis ist zu gegebener Monomordnung und gegebenem Ideal eindeutig. Dies macht den Vergleich zweier Ideale möglich.
Berechnet kann eine reduzierte Gröbnerbasis werden, indem man setzt

$$g' = \overline{g}^{G-\{g\}},\ G' = (G - \{g\}) \cup \{g'\}.$$

Eindeutigkeit: Seien $G, \tilde{G}$ reduzierte Gröbnerbasen. Reduzierte Gröbnerbasen haben dieselben Leitterme. Also jeweils $\text{LT}(g) = \text{LT}(\tilde{g})$. Daraus folgt schon $g = \tilde{g}$: $g - \tilde{g} \in I$ daher $\overline{g - \tilde{g}}^{G} = 0$. Die Leitterme heben sich weg, die übrigen sind nicht teilbar durch $\text{LT}(G) = \text{LT}(\tilde{G})$, da die Basen reduziert sind. Also ist $0 = \overline{g - \tilde{g}}^{G} = g - \tilde{g}$.

Damit ist Frage 3.3 nach der Gleichheit zweier durch Basen gegebener Ideale beantwortet: Einfach die reduzierte Gröbnerbasis berechnen und vergleichen.

5 Eine Aufgabe

Zunächst etwas Theorie:

Satz 5.1: Das Eliminationstheorem. *Sei $I < k[x_1, \ldots, x_n]$ ein Ideal mit Gröbnerbasis G bezüglich lexikographischer Ordnung mit $x_1 < \cdots x_n$. Für $0 \leq k \leq n$ gilt*

$$G_k = G \cap k[x_{k+1}, \ldots, x_n]$$

ist eine Gröbnerbasis des k-ten Eliminationsideals

$$I_k = I \cap k[x_{k+1}, \ldots, x_n].$$

Satz 5.2: Das Abschlußtheorem. *$\mathcal{V}(I_k)$ ist der Abschluß von $\pi_k(\mathcal{V}(I))$ in der Zariski-Topologie, d.h. sie kleinste affine Varietät, die $\pi_k(\mathcal{V}(I))$ enthält.*

Damit können die Gleichungen der Zariski-Abschlüße polynomiell parametrisierter Mengen berechnet werden:
Gegeben: Polynome $p_1, \ldots, p_n \in k[t_1, \ldots, t_m]$, die eine Menge parametrisieren.
Gesucht: Beschreibende Gleichungen für den Abschluß der Bildes von $P = (p_1, \ldots, p_n)$.

- Die Punkte der Varietät $\mathcal{V}(x_1 - p_1, \ldots, x_n - p_n)$ sind von der Form

  $$(t_1, \ldots, t_m, p_1(t_1, \ldots, t_m), \ldots, p_n(t_1, \ldots, t_m)),$$

  sie beschreibt also den Graphen der Abbildung P.

- Mit der Abbildung

$$
\begin{array}{lccc}
i: & k^m & \to & k^{m+n} \\
 & (t_1,\ldots,t_m) & \mapsto & (t_1,\ldots,t_m,p_1(t_1,\ldots,t_m),\ldots,p_n(t_1,\ldots,t_m))
\end{array}
$$

  und der Projektion π_m auf die letzten n Komponenten ist das Diagramm

$$
\begin{tikzcd}
 & k^{n+m} \arrow[dr, "\pi_m"] & \\
k^m \arrow[ur, "i"] \arrow[rr, "P"] & & k^n
\end{tikzcd}
$$

  kommutativ, das Bild der Parametrisierung ist also die Projektion des Graphen.

Aufgabe 5.3.
Finden Sie die Gleichung der kleinsten Varietät im $\mathbb{R}^3$, die alle Geraden durch den Punkt $(2,2,2) \in \mathbb{R}^3$ enthält, die die in der xy-Ebene eingebettete Neilsche-Parabel schneiden!

Lösung: Die Neilsche Parabel wird parametrisiert durch $t \mapsto (t^2, t^3)$. Der Kegel wird somit parametrisiert durch

$$\begin{pmatrix} s \\ t \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} + s\left(\begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} - \begin{pmatrix} t^2 \\ t^3 \\ 0 \end{pmatrix}\right).$$

Projektion des Graphen mittels des *Singular*-Skriptes

```
ring r=0,(s,t,x,y,z),lp;
poly f1=2+s*(2-t2);
poly f2=2+s*(2-t3);
poly f3=2+2s;
ideal i=(x-f1,y-f2,z-f3);
groebner(i);
```

ergibt

$$
\begin{array}{rl}
gb1 = & 2x^3 - 6x^2z + 6xz^2 + y^2z - 2y^2 - 2yz^2 + 4yz - z^3 - 2z^2 \\
gb2 = & tyz - 2ty - tz^2 + 2tz + 2x^2 - 4xz + 2z^2 \\
gb3 = & tx - tz - y + z \\
gb4 = & t^2z - 2t^2 + 2x - 2z \\
gb5 = & 2s - z + 2
\end{array},
$$

d.h. beschreibende Gleichung ist

$$2x^3 - 6x^2z + 6xz^2 + y^2z - 2y^2 - 2yz^2 + 4yz - z^3 - 2z^2.$$