7 Polynomalgebra

In diesem Kapitel sei K ein Körper.

Polynome und Polynomfunktionen

Definition 7.1: *Ein* **univariates Polynom** *oder einfach* **Polynom** p *über* R *ist eine Funktion von* $\mathbb{N}$ *nach* K*, welche auf fast allen (d.h. auf allen bis auf endlich viele) Elementen von* $\mathbb{N}$ *die* $0 \in K$ *ergibt. Also*

$$\begin{array}{rccc} p: & \mathbb{N} & \longrightarrow & K \\ & i & \mapsto & p(i) \end{array} ,$$

sodass $\mathrm{supp}(p) := \{i \in \mathbb{N} \mid p(i) \neq 0\}$ *eine endliche Menge ist. Diese endliche Menge* $\mathrm{supp}(p)$ *heisst die* **Stützmenge** *bzw.* **Support** *von* p*.*
Das Polynom $0 : \mathbb{N} \to R$ *mit* $0(i) = 0$ *für alle* $i \in \mathbb{N}$ *heisst das* **Nullpolynom***.*
Ist p *verschieden vom Nullpolynom und* $n = \max(\mathrm{supp}(p))$*, dann heisst* n *der* **Grad** *von* p*, geschrieben* $n = \mathrm{grad}(p)$*.*
Häufig schreiben wir ein Polynom in der Form

$$p(x) = \sum_{i=0}^{n} p_i x^i ,$$

falls $\mathrm{supp}(p) \subseteq \{0, \ldots, n\}$ *und* $p_i = p(i)$*. (Dabei ist "*x*" nur ein syntaktisches Konstrukt zur Beschreibung des Polynoms* p*, und kann im Prinzip durch jedes andere Symbol ersetzt werden; dabei ändert sich das beschriebene Polynom nicht.)*
Für $i \in \mathbb{N}$ *heisst* $p(i) = p_i$ *der* **Koeffizient** *von* p *bei* x^i*. Ist* $p \neq 0$ *und* $n = \mathrm{grad}(p)$*, dann heisst* $p(n) = p_n$ *der* **führende Koeffizient** *(***leading coefficient***) von* p*, geschrieben* $\mathrm{fc}(p)$*.*
Ist p *verschieden vom Nullpolynom mit führendem Koeffizienten* 1*, so heisst* p **normiert***.*
Mit $K[x]$ *bezeichnen wir die* **Menge aller Polynome** *über* K*.* □

Satz 7.2: *Die Polynome* $K[x]$ *bilden einen kommutativen Ring mit Einselement ohne Nullteiler; also einen Integritätsbereich. Ausserdem bilden die Polynome* $K[x]$ *auch einen Vektorraum über* K*.*

Definition 7.3: *Sei* m *eine positive natürliche Zahl. Ein* m**-variates Polynom** p *über* K *ist eine Funktion von* $\mathbb{N}^m$ *nach* K*, welche auf fast allen (d.h. auf allen bis auf endlich viele) Elementen von* $\mathbb{N}^m$ *die* $0 \in K$ *ergibt. Also*

$$\begin{array}{rccc} p: & \mathbb{N}^m & \longrightarrow & K \\ & i = (i_1, \ldots, i_m) & \mapsto & p(i) = p(i_1, \ldots, i_m) \end{array} ,$$

sodass $\mathrm{supp}(p) := \{i \in \mathbb{N}^m \mid p(i) \neq 0\}$ *eine endliche Menge ist. Diese endliche Menge* $\mathrm{supp}(p)$ *heisst die* **Stützmenge** *bzw.* **Support** *von* p*.*
Auf analoge Weise wie in Def. 13.1 führt man auch für multivariate Polynome die Begriffe **Nullpolynom** *und* **Koeffizient** *ein.*
Der **(totale) Grad** *von* p *ist* $\mathrm{grad}(p) := \max\{i_1 + \cdots + i_m \mid (i_1, \ldots, i_m) \in \mathrm{supp}(p)\}$*, während der* **Grad** *von* p **bzgl.** *der Variablen* x_r *definiert ist als*
$\mathrm{grad}_r(p) := \max\{i_r \mid (i_1, \ldots, i_r, \ldots, i_m) \in \mathrm{supp}(p)\}$*.* □

Definition 7.4: *Sei $p = p_0 + p_1 x + \cdots + p_n x^n \in K[x]$ ein Polynom über dem Körper K. Dann induziert dieses Polynom eine Funktion*

$$\begin{array}{rccc} \overline{p}: & K & \longrightarrow & K \\ & a & \mapsto & p_0 + p_1 a + \cdots + p_n a^n \end{array} .$$

Diese Funktion ist die von p induzierte **Polynomfunktion**. *Das Ergebnis der Anwendung der Polynomfunktion $\overline{p}$ auf a schreiben wir dennoch oft einfach als $p(a)$.*
Mit $\mathrm{PF}(K)$ bezeichnen wir alle Polynomfunktionen auf K.
$\mathrm{polfun} : K[x] \to \mathrm{PF}(K)$ *bezeichne diese Zuordnung von Polynomen zu Polynomfunktionen.*
Auf analoge Weise kann man einem m-variaten Polynom $p(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ eine Polynomfunktion $\overline{p} : K^m \to K$ zuordnen. □

Satz 7.5: *Die Zuordnung von Polynomen zu Polynomfunktionen* $\mathrm{polfun} : K[x] \to \mathrm{PF}(K), p \mapsto \overline{p}$ *über einem Körper K ist ein Ring- und ein Vektorraumepimorphismus. Es gilt also $\overline{p+q} = \overline{p} + \overline{q}, \overline{\lambda p} = \lambda \overline{p}, \overline{p \cdot q} = \overline{p} \cdot \overline{q}$.*

Man kann sich nun fragen, ob diese Zuordnung von Polynomen zu Polynomfunktionen nicht vielleicht ein Isomorphismus ist. Das ist natürlich für endliche Körper sicherlich nicht der Fall. Für unendliche Körper werden wir unten sehen, dass diese Zuordnung tatsächlich ein Isomorphismus ist.

Beispiel 7.6: Über dem endlichen Körper $\mathbb{Z}_3$ gilt offensichtlich

$$\overline{p} = \overline{0}$$

für $p = x(x+1)(x+2)$. Dieses Beispiel ist sofort für jeden Körper $\mathbb{Z}_p$ verallgemeinerbar. □

Definition 7.7: *Sei $p \in K[x]$ und $a \in K$. Dann heisst a eine* **Nullstelle** *oder* **Wurzel** *von p gdw. $p(a) = 0$.*
Analog für ein multivariates Polynom $p \in K[x_1, \ldots, x_m]$ und $a = (a_1, \ldots, a_m) \in K^m$: a heisst **Nullstelle** *oder* **Wurzel** *von p gdw. $p(a) = p(a_1, \ldots, a_m) = 0$.*

Es war ein grosser Erfolg der Mathematik zu Anfang des 19. Jahrhunderts, dass der folgende Fundamentalsatz der Algebra bewiesen werden konnte.

Satz 7.8: (Fundamentalsatz der Algebra) *Jedes Polynom $a(x) \in \mathbb{C}[x]$ mit $\mathrm{grad}(a) > 0$ besitzt in $\mathbb{C}$ eine Nullstelle (der Körper $\mathbb{C}$ ist also algebraisch abgeschlossen).*

Beispiel 7.9: Das Polynom

$$a(x) = 4x^4 + 27x^3 - 17x^2 - 63x + 49 \ \in \ \mathbb{Q}[x]$$

hat die Nullstellen $1, -7, -7/4$. Dabei ist 1 eine "doppelte Nullstelle". Das Polynom lässt sich schreiben als

$$a(x) = 4 \cdot (x-1)^2 \cdot (x+7) \cdot (x + \frac{7}{4}) \ . \qquad \square$$

In $K[x]$ haben wir zwei verwandte Begriffe der Teilbarkeit: die exakte Teilbarkeit und die Teilung mit Quotient und Rest. Diese Begriffe hängen eng miteinander zusammen:

mittels des Euklidschen Algorithmus, der eine Folge von Resten herstellt, können wir den grössten (exakten) gemeinsamen Teiler bestimmen.

Definition 7.10: *Seien $a(x), b(x) \in K[x]$. Das Polynom a* **teilt** *das Polynom b, in Zeichen $a|b$, gdw. es ein Polynom $c(x) \in K[x]$ gibt, sodass $a \cdot c = b$. In diesem Fall heisst a ein* **Teiler** *oder* **Faktor** *von b.*

Ebenso wie man natürliche Zahlen dividiert mit Quotient und Rest kann man auch Polynome in $K[x]$ dividieren mit Quotient und Rest: sind

$$a = a_m x^m + \ldots + a_0 \quad \text{und} \quad b = b_n x^n + \ldots + b_0$$

verschieden vom Nullpolynom und ist $\text{grad}(a) = m \geq n = \text{grad}(b)$, dann lässt sich a schreiben als

$$a = \frac{\text{fc}(a)}{\text{fc}(b)} x^{m-n} b + r \ ,$$

wobei $\text{grad}(r) < \text{grad}(a)$. Ist $\text{grad}(r) \geq \text{grad}(b)$, so nehmen wir r als unser neues a und wiederholen diesen Prozess. Damit haben wir den folgenden Satz bewiesen.

Satz 7.11: *Seien $a(x), b(x) \in K[x]$, mit $b \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, sodass*

$$a = q \cdot b + r, \quad \textit{und} \quad r = 0 \textit{ oder } \text{grad}(r) < \text{grad}(b).$$

Definition 7.12: *Seien $a(x), b(x) \in K[x]$, mit $b \neq 0$. Die laut Satz 7.11 eindeutig bestimmten Polynome $q(x)$ und $r(x)$ heissen* **Quotient** *und* **Rest** *bei Division von $a(x)$ durch $b(x)$.* □

Beispiel 7.13: In $\mathbb{Q}[x]$ teilen wir die Polynome

$$a(x) = 3x^3 + x^2 - 1 \quad \text{und} \quad b(x) = 5x^2 + x + 1$$

mit Quotient und Rest. Wir erhalten

$$a(x) = \frac{3}{5} \cdot x \cdot b(x) + (\frac{2}{5}x^2 - \frac{3}{5}x - 1) = (\frac{3}{5}x + \frac{2}{25}) \cdot b(x) - (\frac{17}{25}x + \frac{27}{25}).$$

Also $q(x) = \frac{3}{5}x + \frac{2}{25}$, und $r(x) = -\frac{17}{25}x - \frac{27}{25}$. □

Satz 7.14: *Sei $p \in K[x]$ und $a \in K$. Dann ist a Nullstelle von p gdw. $p = (x - a) \cdot q$ für ein $q \in K[x]$.*

Beweis: Lässt sich p schreiben als $p = (x - a)q$, dann ist offensichtlich a eine Nullstelle von p.
Andererseits nehmen wir an, a sei Nullstelle von p. Sei q der Quotient und r der Rest bei Division von p durch $x - a$, also

$$p = (x - a) \cdot q + r \ , \quad \text{und } r = 0 \text{ oder } \text{grad}(r) < \text{grad}(x - a) = 1 \ .$$

r ist also ein konstantes Polynom und es muss gelten $r(a) = 0$. Das geht nur für $r = 0$. □

Daraus sehen wir sofort:

Satz 7.15: *Ein vom Nullpolynom verschiedenes Polynom $a \in K[x]$ mit $n = \text{grad}(a)$ hat höchstens n Nullstellen.*

Über einem algebraisch abgeschlossenen Körper (etwa $\mathbb{C}$) hat ein univariates Polynom genau so viele Nullstellen (mit Vielfachheit gezählt) wie sein Grad angibt.

Satz 7.16: *Die Zuordnung von Polynomen zu Polynomfunktionen* polfun : $K[x] \to \text{PF}(K)$ *ist genau dann ein Isomorphismus, wenn K unendlich ist.*

Beweis: Aus Beispiel 13.6 wissen wir schon, dass polfun kein Isomorphismus ist, falls K endlich ist.
Sei nun K unendlich. polfun : $K[x] \to \text{PK}(K)$ ist linear, laut Satz 13.5. Ist $p \in \text{kern}(\text{polfun})$, so hat p unendlich viele Nullstellen. Das geht nur für $p = 0$. □

Für Polynome $a(x) \in \mathbb{C}[x]$ vom Grad ≤ 4 gibt es explizite Lösungsformeln mittels Wurzelausdrücken (Radikale). Dass es eine solche Lösungsformel für Polynome höheren Grades nicht mehr geben kann, ist Inhalt der Galois-Theorie (Évariste Galois, 1811–1832).

Definition 7.17: *Seien $a(x), b(x) \in K[x]$. Dann heisst $c(x) \in K[x]$ ein* **gemeinsamer Teiler** *von a und b g.d.w. $c|a$ und $c|b$.*
$g(x)$ heisst ein **grösster gemeinsamer Teiler** *von a und b, in Zeichen $\text{ggT}(a, b)$, g.d.w. g ein gemeinsamer Teiler von a und b ist, und für jeden gemeinsamen Teiler d von a und b gilt $d|g$ (der ggT ist bis auf Multiplikation mit einer Konstanten eindeutig bestimmt; oft nimmt man deshalb einfach nur den normierten ggT).*
Ist $\text{ggT}(a, b) = 1$, dann nennt man a und b **relativ prim**.

Offensichtlich wird 0 von jedem Polynom geteilt. Der ggT ist also auf dem Paar $(0, 0)$ nicht definiert.

Satz 7.18: *Für $a, b \in K[x]$, $b \neq 0$, gilt:* $\text{ggT}(a, b) = \text{ggT}(\text{rest}(a, b), b)$.

Beweis: Wenn c sowohl a als auch b teilt, so teilt c auch $\text{rest}(a, b) = a - qb$ und b und umgekehrt. Damit haben die Paare (a, b) und $(b, \text{rest}(a, b))$ die gleichen Teiler, und somit auch den gleichen grössten gemeinsamen Teiler. □

Somit kann der ggT von a und b mit dem Euklidschen Divisionsalgorithmus berechnet werden.

Euklidscher Divisionsalgorithmus
Für gegebene Polynome $a, b \in K[x]$, $b \neq 0$, wird $g = \text{ggT}(a, b)$ berechnet.

(1) setze $r_0 := a,\ r_1 := b,\ i := 1$;

(2) solange $r_i \neq 0$ ist, führe aus:

$$r_{i+1} := \text{rest}(r_{i-1}, r_i),\ i := i + 1;$$

(3) $(r_i = 0)$ $g := r_{i-1}$ ist der gesuchte ggT. □

Der Euklidsche Divisionsalgorithmus kann unschwer dahingehend erweitert werden, dass neben dem grössten gemeinsamen Teiler auch sogenannte Bézout-Kofaktoren $s, t \in$

$K[x]$ berechnet werden, sodass

$$\mathrm{ggT}(a,b) = sa + tb \ .$$

Beispiel 7.19: Wir bestimmen den ggT der Polynome

$$\begin{array}{rcl} a & = & x^6 - x^5 + 3x^4 + 4x^3 - x^2 + 9x + 9 \quad = \quad (x^2 - x + 3)(x+1)^2(x^2 - 2x + 3) \ , \\ b & = & x^6 + x^5 + 3x^4 + 7x^3 + 5x^2 + 7x + 6 \quad = \quad (x^2 - x + 3)(x+1)(x^3 + x^2 + x + 2) \ . \end{array}$$

Der Euklidsche Divisionsalgorithmus erzeugt die folgende Folge von Resten:

$$\begin{array}{l} r_0 = a, \ r_1 = b, \\ q_1 = \mathrm{quot}(r_0, r_1) = 1; \\ r_2 = r_0 - q_1 \cdot r_1 = -2x^5 - 3x^3 - 6x^2 + 2x + 3; \\ q_2 = \mathrm{quot}(r_1, r_2) = \frac{1}{2}(-x - 1); \\ r_3 = r_1 - q_2 \cdot r_2 = \frac{1}{2}(3x^4 + 5x^3 + 6x^2 + 19x + 15); \\ q_3 = \mathrm{quot}(r_2, r_3) = \frac{1}{9}(-12x + 20); \\ r_4 = r_2 - q_3 \cdot r_3 = -\frac{41}{9}(x^3 + 2x + 3); \\ q_4 := \mathrm{quot}(r_3, r_4) = -\frac{1}{85}(27x + 45); \\ r_5 = r_3 - q_4 \cdot r_4 = 0. \end{array}$$

Somit ist $r_4(x)$ ein grösster gemeinsamer Teiler von $a(x)$ und $b(x)$. Wenn wir diesen nun normieren, so erhalten wir

$$-\frac{9}{41} \cdot r_4 = x^3 + 2x + 3 = \mathrm{ggT}(a,b) \ . \qquad \square$$

Definition 7.20: *Sei $a \in K[x]$ ein nicht-konstantes Polynom, also $\mathrm{grad}(a) > 0$. Dann heisst a* **reduzibel** *g.d.w. es Polynome $a_1, a_2 \in K[x]$ gibt, sodass*

$$a = a_1 \cdot a_2 \quad \textit{und} \quad \mathrm{grad}(a_1), \mathrm{grad}(a_2) < \mathrm{grad}(a).$$

Ist das nicht der Fall, so heisst a **irreduzibel**.
$a(x)$ heisst **prim** *gdw gilt: teilt $a(x)$ ein Produkt $b(x) \cdot c(x)$, so teilt a einen der Faktoren b oder c.* $\square$

Im Polynomring sind die Begriffe "irreduzibel" und "prim" äquivalent. Das gilt aber nicht in jedem Ring. So haben wir etwa in $\mathbb{Z}[\sqrt{-5}]$:

$$2 \cdot 3 \ = \ 6 \ = \ (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \ .$$

Jeder dieser Faktoren ist irreduzibel, aber offensichtlich nicht prim.

Beispiel 7.21: Das Polynom $a = x^4 + 1 = (x^2 + i)(x^2 - i)$ ist irreduzibel über dem Körper $K = \mathbb{Q}$, nicht aber wenn K ein Primkörper $\mathbb{Z}_p$, p Primzahl, ist. So etwa gilt modulo 7, also über $\mathbb{Z}_7$:

$$a = (x^2 + 4x + 1)(x^2 + 3x + 1) \ . \qquad \square$$

Satz 7.22: *Jedes nicht-konstante Polynom $a \in K[x]$ kann geschrieben werden als Produkt endlich vieler irreduzibler Polynome $a_1, \ldots, a_r$, also*

$$a = \prod_{i=1}^{r} a_i \ .$$

Diese Faktorisierung von a ist im wesentlichen eindeutig. Ist $a'_1, \ldots, a'_s$ eine andere Faktorisierung von a, dann ist $r = s$ und die a'_i können so umgeordnet (permutiert) werden, dass jedes a'_i ein Produkt von a_i mit einer Konstanten ist.

Gröbnerbasen für Polynomideale

In Kapitel 4.3 haben wir gesehen, wie man mittels Resultanten feststellen kann, ob zwei univariate Polynome $a(x), b(x)$ eine gemeinsame Nullstelle haben. Wir haben die Idee der Resultanten auch auf multivariate Polynome angewandt, um gemeinsame Nullstellen zu bestimmen.

Eine moderne Methode zur Lösung polynomialer Gleichungssysteme in mehreren Variablen ist die Methode der Gröbnerbasen. Sie kann gesehen werden als Verallgemeinerung sowohl des Euklidschen Algorithmus als auch des Gaußschen Eliminationsverfahrens. Hier können hier nur einführende Erläuterungen gegeben werden. Betreffend Details sei verwiesen auf das Buch

F. Winkler,
Polynomial Algorithms in Computer Algebra,
Springer-Verlag Wien New York (1996).

Definition 7.23: *Ein* **Ideal** *I in einem kommutativen Ring R mit 1 (wie etwa $K[x_1, \ldots, x_n]$) ist eine Teilmenge von R, welche abgeschlossen ist bzgl. der Bildung von Linearkombinationen über R; also für alle $a, b \in I$ und alle $u, v \in R$ muss gelten: $u \cdot a + v \cdot b \in I$.* □

Definition 7.24: Seien $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$, also Polynome in den Variablen $x_1, \ldots, x_n$ und Koeffizienten in K. Dann heisst die Menge

$$I \;:=\; \text{ideal}(f_1, \ldots, f_m) \;:=\; \{a_1 \cdot f_1 + \cdots + a_m \cdot f_m \mid a_i \in K[x_1, \ldots, x_n]\}$$

das von $f_1, \ldots, f_m$ **erzeugte (Polynom-)Ideal**.
Die Menge $\{f_1, \ldots, f_m\}$ heisst eine **(Ideal-)Basis** für I. □

Offenbar ist ideal$(f_1, \ldots, f_m)$ ein Ideal im Sinne von Definition 7.23.

Beispiel 7.25: Betrachte die Polynome

$$f_1 = x^2y^2 + y - 1, \quad f_2 = x^2y + x \quad \text{in } \mathbb{Q}[x, y] \; .$$

Dann ist

$$f = -xy + y - 1 = f_1 - y \cdot f_2 \in \text{ideal}(f_1, f_2) \; . \qquad \square$$

Für den Fall univariater Polynome f_1, f_2 wissen wir, dass der ggT g dasselbe Ideal erzeugt:

$$\text{ideal}(f_1, f_2) \;=\; \text{ideal}(g) \; .$$

Um also zu entscheiden, ob ein Polynom h im Ideal ist, müssen wir nur prüfen, ob der ggT das Polynom h teilt.

Im multivariaten Fall muss aber ein Ideal nicht eine Basis aus nur einem Polynom besitzen; wohl aber hat jedes Ideal in $K[x_1, \ldots, x_n]$ eine endliche Basis (Hilbertscher Basissatz). Wir wollen also eine Basis bestimmen, mittels welcher wir durch Division (bzw. Reduktion) einfach bestimmen können, ob ein Polynom im Ideal enthalten ist.

Definition 7.26: *Dazu brauchen wir zunächst eine lineare Ordnung $<$ der Terme, welche verträglich ist mit der Multiplikation auf dem Monoid der Terme:*

(1) $1 = x_1^0 \dots x_n^0$ *ist das kleinste Element bzgl.* $<$*, und*

(2) *falls* $s < t$ *und* u *ein beliebiger Term ist, dann gilt auch* $u \cdot s < u \cdot t$*.*

Eine solche Ordnung nennen wir eine **zulässige Ordnung**. □

Beispiel 7.27: So ist etwa die lexikographische Ordnung auf Termen in den Variablen x, y (mit $x < y$) so eine zulässige Ordnung:

$$1 < x < x^2 < \ldots < y < xy < x^2y < \ldots < y^2 < \ldots$$

Ebenso ist die graduiert-lexikographische Ordnung zulässig:

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < y^3 < \ldots$$ □

Definition 7.28: *Ist* $<$ *eine zulässige Ordnung auf den Termen über* $x_1, \dots, x_n$*, so besitzt jedes vom Nullpolynom verschiedene Polynom* $f \in K[x_1, \dots, x_n]$ *einen höchsten Term bzgl.* $<$*, genannt der* **führende Term** *von* f*, geschrieben* $\mathrm{ft}(f)$*.*
Der (von 0 *verschiedene) Koeffizient von* $\mathrm{ft}(f)$ *heisst der* **führende Koeffizient** *von* f*, geschrieben* $\mathrm{fk}(f)$*.* □

Nun sind wir vorbereitet, um die Reduktion von Polynomen zu beschreiben. Dabei handelt es sich um eine Verallgemeinerung des Begriffs der Division.

Definition 7.29: *Seien* $f, g, h \in K[x_1, \dots, x_n]$*. Dann ist* g **reduzierbar** *zu* h *modulo* f*, wenn es in* g *einen Term gibt von der Form* $c \cdot t \cdot \mathrm{ft}(f)$*, wobei* $c \in K \setminus \{0\}$*,* t *ein Term, und* $h = g - c \cdot t \cdot f$*. Wir schreiben dafür*

$$g \longrightarrow_f h \ .$$

Bei der Reduktion wird also der Term $c \cdot t \cdot \mathrm{ft}(f)$ *in* g *eliminiert und ersetzt durch kleinere Terme bzgl. der Ordnung* $<$*.*
Diese Reduktion lässt sich sofort erweitern zu einer Reduktion modulo einer Menge von Polynomen F*:* $g \longrightarrow_F h$ *gdw. es* $f \in F$ *gibt, sodass* $g \longrightarrow_f h$*.* □

Beispiel 7.30: Seien die Polynome in $\mathbb{Q}[x, y]$ lexikographisch geordnet mit $x < y$. Dann haben wir

$$f = 2x^2y^2 + x^7y - 4 \quad \longrightarrow_{h=x^3y+y+x} \quad g = 2x^2y^2 - x^4y - x^5 - 4 \ .$$ □

Führt man nun diese Reduktion $\longrightarrow_F$, ausgehend von einem Polynom f, in mehreren Schritten hintereinander aus, so kommt man immer nach endlich vielen Schritten zu einem nicht mehr weiter reduzierbaren Ergebnis $\underline{f}$; man nennt $\underline{f}$ eine **Normalform** von f bzgl. F. Die Reduktion $\longrightarrow_F$ ist aber im allgemeinen nicht eindeutig, d.h. es kann verschiedene Normalformen für f geben.

Ist ein Polynom f mittels $\longrightarrow_F$ in mehreren Schritten zu 0 reduzierbar, dann lässt es sich offensichtlich als Linearkombination der Elemente in F darstellen, ist also in $\mathrm{ideal}(F)$. Die Umkehrung gilt aber i.a. nicht; man sieht das etwa aus Beispiel 7.25. Dort ist $f \in \mathrm{ideal}(f_1, f_2)$, aber offensichtlich ist f bereits in Normalform.

Wir wollen also nun versuchen, eine Idealbasis F dahingehend zu modifizieren zu einer neuen Basis G, sodass $\text{ideal}(F) = \text{ideal}(G)$, und G eindeutige Normalformen erzeugt. Eine solche Basis nennt man eine Gröbnerbasis für das gegebene Ideal.

Definition 7.31: *Sei G eine Teilmenge von $K[x_1, \ldots, x_n]$. Dann heisst G eine* **Gröbnerbasis** *(für $\text{ideal}(G)$), wenn jedes Polynom $f \in K[x_1, \ldots, x_n]$ eine eindeutige Normalform bzgl. $\longrightarrow_G$ hat.* □

Um eine beliebige Idealbasis F in eine Gröbnerbasis zu transformieren, betrachtet man Divergenzen in der Reduktion modulo F. Sind etwa $f_1, f_2 \in F$, so lässt sich das kleinste gemeinsame Vielfache (kgV) der führenden Terme sowohl mittels f_1 als auch mittels f_2 reduzieren. Sind diese Ergebnisse verschieden, so haben wir eine Divergenz in der Reduktion vorliegen.

Definition 7.32: *Seien f_1, f_2 zwei Polynome. Seien g_1, g_2 so, dass*

$$\text{kgV}(\text{ft}(f_1), \text{ft}(f_2)) \longrightarrow_{f_1} g_1, \quad \text{und} \quad \text{kgV}(\text{ft}(f_1), \text{ft}(f_2)) \longrightarrow_{f_2} g_2 \ .$$

Dann heisst $\text{spol}(f_1, f_2) := g_1 - g_2$ das **S-Polynom** *(Subtraktionspolynom) von f_1, f_2.* □

Satz 7.33: (Buchberger) *Sei $F \subseteq K[x_1, \ldots, x_n]$. Dann ist F eine Gröbnerbasis g.d.w. jedes S-Polynom von Elementen von F sich mittels $\longrightarrow_F$ (in endlich vielen Schritten) zu 0 reduzieren lässt.* □

Daraus ergibt sich unmittelbar ein Algorithmus, GB-CHECK, um zu prüfen, ob eine gegebene endliche Menge von Polynomen eine Gröbnerbasis ist. Wir müssen nur die endlich vielen S-Polynome zu Normalformen reduzieren, und prüfen, ob alle diese Normalformen 0 sind.

Dieser Algorithmus lässt sich auch offensichtlich erweitern zu einem Algorithmus GB-CONSTRUCT, der eine Gröbnerbasis für ein gegebenes Ideal herstellt. Sollte nämlich die Normalform eines S-Polynoms verschieden von 0 sein, etwa $h \neq 0$, dann fügen wir einfach h zur Basis hinzu. Dadurch ändert sich das Ideal nicht. Wir haben allerdings nun zusätzliche S-Polynome zu prüfen. Man kann aber zeigen (etwa in der Vorlesung Computeralgebra), dass dieser Vorgang immer abbricht und eine Gröbnerbasis erzeugt.

Offenbar sind die gemeinsamen Nullstellen aller Polynome eines Ideals I identisch mit den gemeinsamen Nullstellen einer (jeder) Basis von I. Sind also etwa

$$F = \{f_1, \ldots, f_k\} \quad \text{und} \quad G = \{g_1, \ldots, g_l\}$$

zwei verschiedene Basen für dasselbe Ideal I, so haben die beiden Gleichungssysteme

$$\begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_k(x_1, \ldots, x_n) & = & 0 \end{array} \qquad \text{und} \qquad \begin{array}{rcl} g_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ g_l(x_1, \ldots, x_n) & = & 0 \end{array}$$

dieselben Lösungen. Ist etwa G eine Gröbnerbasis bzgl. einer lexikographischen Termordnung, so lässt sich aus G die Lösungsmenge relativ leicht ablesen.

Satz 7.34: (Eliminationssatz) *Sei $G \subset K[x_1, \ldots, x_n]$ eine Gröbnerbasis bzgl. der lexikographischen Termordnung mit $x_1 < \cdots < x_n$. Dann ist für alle $i \in \{1, \ldots, n\}$*

$$\text{ideal}(G) \cap K[x_1, \ldots, x_i] \ = \ \text{ideal}(G \cap K[x_1, \ldots, x_i]) \ .$$

Dabei wird das Ideal auf der rechten Seite im Polynomring $K[x_1, \ldots, x_i]$ gebildet. □

Durch Berechnung einer solchen Gröbnerbasis können wir also ein gegebenes Gleichungssystem triangulieren, ganz ähnlich wie es das Eliminationsverfahren von Gauss für lineare Gleichungssysteme macht.

Beispiel 7.35: Wie schon in Beispiel 7.25 betrachten wir das Polynomideal $I = \text{ideal}(f_1, f_2) \subseteq \mathbb{Q}[x, y]$, wobei

$$f_1 = x^2y^2 + y - 1 \ , \quad f_2 = x^2y + x \ .$$

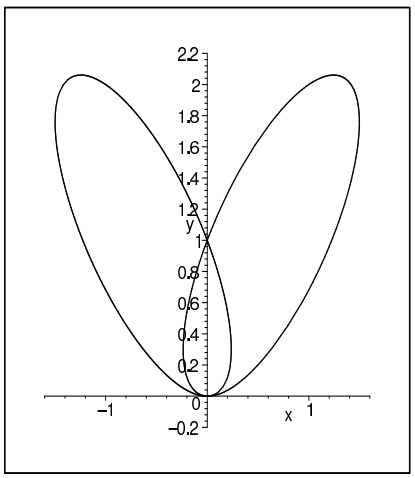
Wir ordnen die Terme lexikographisch mit $x < y$. Dann erzeugt GB-CONSTRUCT sukkzessive folgende Polynome:
$\text{spol}(f_1, f_2) = f_1 - yf_2 = -xy + y - 1 =: f_3$, ist bereits irreduzibel,
$\text{spol}(f_2, f_3) = f_2 + xf_3 = xy \longrightarrow_{f_3} y - 1 =: f_4$,
$\text{spol}(f_3, f_4) = f_3 + xf_4 = y - x - 1 \longrightarrow_{f_4} -x =: f_5$,
Alle anderen S-Polynome sind zu 0 reduzierbar. Damit haben wir folgende Gröbnerbasis bestimmt:

$$G \ = \ \{ \ x^2y^2 + y - 1, \ x^2y + x, \ -xy + y - 1, \ y - 1, \ -x \ \}.$$

Schliesslich brauchen wir in der Gröbnerbasis nur x und $y - 1$, da sich die anderen Basiselemente dadurch darstellen lassen. □

Beispiel 7.36: Wir betrachten die algebraische Kurve $\mathcal{C} = \{(x, y) | f(x, y) = 0\} \subseteq \mathbb{R}^2$, wobei

$$f(x, y) \ = \ 2x^4 - 3x^2y + y^4 - 2y^3 + y^2 \ .$$



Die Kurve $\mathcal{C}$ hat einen sogenannten singulären Punkt dort, wo die Tangente an $\mathcal{C}$ nicht eindeutig definiert ist; wo also beide partiellen Ableitung verschwinden. Wir wollen die singulären Punkte von $\mathcal{C}$ bestimmen. Dazu müssen wir das Gleichungssystem

$$\begin{array}{rcrcl} f(x,y) & = & 2x^4 - 3x^2y + y^4 - 2y^3 + y^2 & = & 0 \\ \frac{\partial f}{\partial x}(x,y) & = & 8x^3 - 6xy & = & 0 \\ \frac{\partial f}{\partial y}(x,y) & = & 4y^3 - 3x^2 - 6y^2 + 2y & = & 0 \end{array}$$

lösen. Wir berechnen für dieses Ideal eine Gröbnerbasis bzgl. der lexikographischen Termordnung mit $x < y$, schreiben die so gewonnene Basis wieder als Gleichungssystem

an

$$\begin{aligned} 2y^2 - 2y + 3x^2 &= 0 \\ xy &= 0 \\ x^3 &= 0 \end{aligned}$$

und lesen die Lösungen, also die singulären Punkte der Kurve $\mathcal{C}$, ab:

$$\mathrm{Sing}(\mathcal{C}) \;=\; \{\ (0,0),\ (0,1)\ \}\ . \qquad \square$$