13 Polynome

Polynome und Polynomfunktionen

In Beispiel 1.5.29 sowie Beispiel 5.4 haben wir bereits Polynome eingeführt. In diesem Kapitel wollen wir diese wichtige algebraische Struktur genauer untersuchen.
Dabei ist R immer ein kommutativer Ring mit Einselement, und K ein Körper.

Definition 13.1: *Ein* **univariates Polynom** *oder einfach* **Polynom** p *über* R *ist eine Funktion von* $\mathbb{N}$ *nach* R*, welche auf fast allen (d.h. auf allen bis auf endlich viele) Elementen von* $\mathbb{N}$ *die* $0 \in R$ *ergibt. Also*

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

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 $R[x]$ *bezeichnen wir die* **Menge aller Polynome** *über dem Ring* R*.*
Auf $R[x]$ *definieren wir zwei Operationen* **Addition** *"*$+$*" und* **Multiplikation** *"*$\cdot$*" für zwei Polynome*

$$a(x) = \sum_{i=0}^{m} a_i x^i \quad \textit{und} \quad b(x) = \sum_{i=0}^{n} b_i x^i$$

folgendermassen:

$$a(x) + b(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i \quad \textit{und} \quad a(x) \cdot b(x) = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j \cdot b_{i-j} \right) x^i . \qquad \square$$

Beispiel 13.2: Wir betrachten Polynome über dem Körper $\mathbb{R}$. Das Produkt der beiden Polynome

$$a(x) = 2x^0 + 3x^2 - 1x^3 \quad \text{und} \quad b(x) = 1x^1 - 5x^2 + 2x^4$$

errechnet man als

$$a(x) \cdot b(x) = c(x) = c_0 x^0 + \cdots + c_7 x^7 ,$$

wobei etwa

$$c_4 = a_0b_4 + a_2b_2 + a_3b_1 = 4 - 15 - 1 = -12 \ .$$

Insgesamt erhalten wir

$$a(x) \cdot b(x) = 2x - 10x^2 + 3x^3 - 12x^4 + 5x^5 + 6x^6 - 2x^7 \ .$$

In Maple 16 können wir diese Rechnung wie folgt ausführen:
> **a:= 2 + 3*x^2 - x^3;**

$$a := 2 + 3x^2 - x^3$$

> **b:= 1*x - 5*x^2 + 2*x^4;**

$$b := x - 5x^2 + 2x^4$$

> **c:=expand(a*b);**

$$c := 2x - 10x^2 + 3x^3 - 12x^4 + 5x^5 + 6x^6 - 2x^7$$ □

Satz 13.3: *Die Polynome $R[x]$ bilden einen kommutativen Ring mit Einselement. Ist R ein Integritätsbereich, so ist auch $R[x]$ ein Integritätsbereich. Die Polynome $K[x]$ bilden auch einen Vektorraum über K.*

Als Vektorraum über $\mathbb{R}$ hat $\mathbb{R}[x]$ die kanonische Basis

$$1 = x^0, x, x^2, \dots \ .$$

Alle Elemente dieser Basis sind Potenzen des Polynoms $x = 1x$. Somit können wir die Schreibweise

$$a(x) = a_0 + a_1x + \ldots + a_nx^n$$

auch interpretieren als Darstellung des Polynoms a bzgl. der kanonischen Basis. "x" ist dann kein willkürliches syntaktisches Zeichen, sondern einfach das erzeugende Element der Vektorraumbasis.

Definition 13.4: *Sei m eine positive natürliche Zahl. Ein m-***variates Polynom** *p über R ist eine Funktion von $\mathbb{N}^m$ nach R, welche auf fast allen (d.h. auf allen bis auf endlich viele) Elementen von $\mathbb{N}^m$ die $0 \in R$ ergibt. Also*

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

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* $\mathrm{grad}(p) := \max\{i_1 + \cdots + i_m \mid (i_1, \dots, i_m) \in \mathrm{supp}(p)\}$, *während der* **Grad** *von p* **bzgl.** *der Variablen x_r definiert ist als*
$\mathrm{grad}_r(p) := \max\{i_r \mid (i_1, \dots, i_r, \dots, i_m) \in \mathrm{supp}(p)\}$. □

Definition 13.5: *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 13.6: *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 13.7: 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 13.8: *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 beweisen werden konnte. Alle Beweise dieses Fundamentalsatzes der Algebra verwenden analytische Methoden. Wir geben hier keinen Beweis.

Satz 13.9: (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).*

Der Fundamentalsatz der Algebra besitzt keinen konstruktiven Beweis, in dem Sinn dass man daraus ein Verfahren gewinnen könnte, um eine Nullstelle zu berechnen. Wohl aber gibt es solche konstruktiven Verfahren für endliche Körper $\mathbb{Z}_p$, p eine Primzahl, basierend auf dem Berlekamp-Algorithmus zur Faktorisierung (siehe unten) von Polynomen in $\mathbb{Z}_p[x]$. Ebenso gibt es konstruktive Lösungsalgorithmen für Polynome mit rationalen Koeffizienten, also in $\mathbb{Q}[x]$. Solche Lösungsverfahren werden in der Computeralgebra behandelt.

Beispiel 13.10: Das Polynom

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

hat die Nullstellen $1, 7, 7/4$. Wir können diese Nullstellen in Maple wie folgt bestimmen:
> **a:= 4*x^4 + 27*x^3 - 17*x^2 - 63*x + 49;**

$$a := 4x^4 + 27x^3 - 17x^2 - 63x + 49$$

> **solve(a);**

$$-\frac{7}{4}, -7, 1, 1$$

Daraus sehen wir auch, dass 1 eine "doppelte Nullstelle" ist. □

Teilbarkeit

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 13.11: *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 und Definition 13.12: *Seien $a(x), b(x) \in K[x]$, mit $b \neq 0$. Dann gibt es einen eindeutig bestimmten* **Quotienten** *$q(x)$ und einen eindeutig bestimmten* **Rest** *$r(x)$, sodass*

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

Beispiel 13.13: 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 13.14: *Sei $p \in K[x]$ und $a \in K$. Dann ist a Nullstelle von p gdw. $p = (x-a) \cdot q$ für ein $q \in K[x]$.*

Satz 13.15: *Ein vom Nullpolynom verschiedenes Polynom $a \in K[x]$ mit $n = \mathrm{grad}(a)$ hat höchstens n Nullstellen.*

Satz 13.16: *Die Zuordnung von Polynomen zu Polynomfunktionen* polfun : $K[x] \to \mathrm{PF}(K)$ *ist genau dann ein Isomorphismus, wenn K unendlich ist.*

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 13.17: *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 $\mathrm{ggT}(a,b)$, 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 $\mathrm{ggT}(a,b) = 1$, 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 13.18: *Für $a, b \in K[x]$, $b \neq 0$, gilt:* $\mathrm{ggT}(a,b) = \mathrm{ggT}(\mathrm{rest}(a,b), b)$.

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 $g = \mathrm{ggT}(a,b)$ berechnet.

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

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

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

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

Wegen des obigen Satzes gilt zu jedem Zeitpunkt der Ausführung des Euklidschen Divisionsalgorithmus:

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_{i-1}, r_i).$$

In Schritt (3) gilt offensichlich $r_i = 0$, also ist $g = \mathrm{ggT}(a,b) = \mathrm{ggT}(r_{i-1}, 0) = r_{i-1}$.

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

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

Zu jedem Zeitpunkt der Ausführung des Erweiterten Euklidschen Algorithmus gilt

$$r_i = s_i a + t_i b.$$

In Schritt (3) gilt offensichtlich $g = \mathrm{ggT}(a,b) = sa + tb$.

Erweiterter Euklidscher Divisionsalgorithmus
Für gegebene Polynome $a, b \in K[x]$, $b \neq 0$, wird $g = \mathrm{ggT}(a,b)$ berechnet, sowie Polynome $s, t \in K[x]$ mit der Eigenschaft $g = sa + tb$.

(1) setze $(r_0, r_1, s_0, s_1, t_0, t_1) := (a, b, 1, 0, 0, 1),\ i := 1;$

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

$q_i := \mathrm{quot}(r_{i-1}, r_i);$

$(r_{i+1}, s_{i+1}, t_{i+1}) := (r_{i-1}, s_{i-1}, t_{i-1}) \ - \ q_i \cdot (r_i, s_i, t_i);$

$i := i + 1;$

(3) $(r_i = 0)$ $g := r_{i-1}$ ist der gesuchte ggT, und die Kofaktoren sind $s := s_{i-1}, t := t_{i-1}$. □

Beispiel 13.19: Wir bestimmen den ggT der Polynom

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

Der Euklidsche Divisionsalgorithmus erzeugt die folgende Folge von Resten und Linearkoeffizienten:

$$\begin{aligned} & r_0 = a,\ r_1 = b,\ s_0 = 1,\ t_0 = 0,\ s_1 = 0,\ t_1 = 1; \\ & q_1 = \mathrm{quot}(r_0, r_1) = 1; \\ & r_2 = r_0 - q_1 \cdot r_1 = -2x^5 - 3x^3 - 6x^2 + 2x + 3; \\ & s_2 = s_0 - q_1 \cdot s_1 = 1; \\ & t_2 = t_0 - q_1 \cdot t_1 = -1; \\ & q_2 = \mathrm{quot}(r_1, r_2) = \tfrac{1}{2}(-x - 1); \\ & r_3 = r_1 - q_2 \cdot r_2 = \tfrac{1}{2}(3x^4 + 5x^3 + 6x^2 + 19x + 15); \\ & s_3 = s_1 - q_2 \cdot s_2 = \tfrac{1}{2}(x + 1); \\ & t_3 = t_1 - q_2 \cdot t_2 = \tfrac{1}{2}(-x + 1); \\ & q_3 = \mathrm{quot}(r_2, r_3) = \tfrac{1}{9}(-12x + 20); \\ & r_4 = r_2 - q_3 \cdot r_3 = -\tfrac{41}{9}(x^3 + 2x + 3); \\ & s_4 = s_2 - q_3 \cdot s_3 = \tfrac{1}{9}(6x^2 - 4x - 1); \\ & t_4 = t_2 - q_3 \cdot t_3 = -\tfrac{1}{9}(6x^2 - 16x + 19); \\ & q_4 := \mathrm{quot}(r_3, r_4) = -\tfrac{1}{85}(27x + 45); \\ & r_5 = r_3 - q_4 \cdot r_4 = 0. \end{aligned}$$

Somit ist

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

Dieser ggT ist als Linearkombination

$$\mathrm{ggT}(a,b) = \frac{1}{41}(-6x^2+4x+1)\cdot a + \frac{1}{41}(6x^2-16x+19)\cdot b$$

darstellbar.

In Maple 16 können wir dieses Ergebnis wie folgt berechnen:

> **a:= expand((x^2-x+3)*(x+1)^2*(x^2-2*x+3);**

$$a := x^6 - x^5 + 3x^4 + 4x^3 - x^2 + 9x + 9$$

> **b:= expand((x^2-x+3)*(x+1)*(x^3+x^2+x+2);**

$$b := x^6 + x^5 + 3x^4 + 7x^3 + 5x^2 + 7x + 6$$

> **c:=gcdex(a,b,x,'s','t');**

$$c := x^3 + 2x + 3$$

> **s;**

$$-\frac{6}{41}x^2 + \frac{4}{41}x + \frac{1}{41}$$

> **t;**

$$\frac{6}{41}x^2 - \frac{16}{41}x + \frac{19}{41}$$

Natürlich ist der ggT nicht eindeutig definiert. Maple bestimmt den normierten ggT. □

Definition 13.20: *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.* □

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 13.21: Das Polynom $a = x^4+1 = (x^2+i)(x^2-i)$ ist irreduzibel über dem Körper $K = \mathbb{Q}$, nicht aber wenn K einer der Primkörper $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$ ist. Wir sehen das in folgender Rechnung in Maple 16:

> **a:= x^4 + 1;**

$$a := x^4 + 1$$

> **factor(a);**

$$x^4 + 1$$

> **Factor(a) mod 2;**

$$(x+1)^4$$

> **Factor(a) mod 3;**

$$(x+1)^4$$

> **Factor(a) mod 5;**

$$(x^2+2)(x^2+3)$$

> **Factor(a) mod 7;**

$$(x^2+4x+1)(x^2+3x+1)$$

Tatsächlich ist $a = x^4+1$ über jedem Körper $\mathbb{Z}_p$, p eine Primzahl, reduzibel. □

Satz 13.22: *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.

Es ist i.a. leichter, eine sogenannte "quadratfreie Faktorisierung" eines Polynoms zu berechen als eine vollständige Faktorisierung in irreduzible Faktoren.

Definition 13.23: *Ein nicht-konstantes Polynom $a \in K[x]$ ist* **quadratfrei** *g.d.w. für jeden nicht-konstanten Faktor b von a gilt:*

$$b|a \quad aber \quad b^2 \not| a \ .$$

a hat also keinen nicht-konstanten Faktor, dessen Quadrat a ebenfalls teilt.
Jedes nicht-konstante Polynom a kann geschrieben werden als

$$a = \prod_{i=1}^{r} (a_i)^i \ ,$$

wobei die Polynome a_i jeweils quadratfrei sind und paarweise relativ prim.

Satz 13.24: *Sei $a \in K[x]$ ein nicht-konstantes Polynom und sei* $\mathrm{char}(K) = 0$. *Dann ist a quadratfrei g.d.w.* $\mathrm{ggT}(a, a') = 1$ *(dabei bezeichnet a' die Ableitung von a nach x).*

Mittels dieses Satzes kann durch einige ggT-Berechnungen eine quadratfreie Faktorisierung eines Polynoms hergestellt werden. Wir verweisen dazu auf die Vorlesung "Computeralgebra".

Beispiel 13.25: Wir bestimmen die quadratfreie Faktorisierung des Polynoms

$$a(x) = x^5+6x^4+11x^3+2x^2-12x-8 = \underbrace{(x+1)(x-1)}_{a_1} \cdot (\underbrace{1}_{a_2})^2 \cdot (\underbrace{x+2}_{a_3})^3$$

in $\mathbb{Q}[x]$ mittels Berechung in Maple 16:
> **a:= expand((x+1)*(x-1)*(x+2)^3);**

$$a := x^5+6x^4+11x^3+2x^2-12x-8$$

> **b0:= a;**

$$b0 := x^5 + 6x^4 + 11x^3 + 2x^2 - 12x - 8$$

> **b1 := gcd(b0,diff(b0,x));**

$$b1 := x^2 + 4x + 4$$

> **factor(b1);**

$$(x+2)^2$$

> **c1 := simplify(b0/b1);**

$$c1 := x^3 + 2x^2 - x - 2$$

> **factor(c1);**

$$(x-1)(x+1)(x+2)$$

> **b2 := gcd(b1,diff(b1,x));**

$$b2 := x + 2$$

> **c2 := simplify(b1/b2);**

$$c2 := x + 2$$

> **a1 := simplify(c1/c2);**

$$a1 := x^2 - 1$$

> **b3 := gcd(b2,diff(b2,x));**

$$b3 := 1$$

> **c3 := simplify(b2/b3);**

$$c3 := x + 2$$

> **a2 := simplify(c2/c3);**

$$a2 := 1$$

> **b4 := gcd(b3,diff(b3,x));**

$$b4 := 1$$

> **c4 := simplify(b3/b4);**

$$c3 := 1$$

> **a3 := simplify(c3/c4);**

$$a3 := x + 2$$

Somit haben wir alle quadratfreien Faktoren a_1, a_2, a_3 von a bestimmt. □

Resultanten

Mittels Resultanten kann man bestimmen, ob zwei Polynome in $K[x]$ einen gemeinsamen Faktor haben, also in $\overline{K}$ (dem algebraischen Abschluss von K) eine gemeinsame Nullstelle haben.

Lemma 13.26: *Seien $a, b \in K[x]$ mit $\mathrm{grad}(a) = l > 0$ und $\mathrm{grad}(b) = m > 0$. Dann haben a und b einen nicht-trivialen gemeinsamen Faktor (also $\mathrm{ggT}(a,b)$ ist nicht konstant) g.d.w. es Polynome $c, d \in K[x]$ gibt, sodass:*

(i) *c und d sind nicht beide* 0,

(ii) $\operatorname{grad}(c) \leq m-1$ *und* $\operatorname{grad}(d) \leq l-1$, *und*

(iii) $c \cdot a + d \cdot b = 0$.

Um die Existenz solcher Polynome c und d in Lemma 13.26 zu entscheiden, verwenden wir Lineare Algebra. Die Bedingung "$c \cdot a + d \cdot b = 0$" lässt sich nämlich schreiben als System linearer Gleichungen in den Koeffizienten. Dazu sei

$$\begin{aligned} a &= a_0 x^l + \cdots + a_l, \quad a_0 \neq 0, \\ b &= b_0 x^m + \cdots + b_m, \quad b_0 \neq 0, \\ c &= c_0 x^{m-1} + \cdots + c_{m-1}, \\ d &= d_0 x^{l-1} + \cdots + c_{l-1}. \end{aligned}$$

Die Koeffizienten von c, d sind gesucht. Die Bedingung "$c \cdot a + d \cdot b = 0$" führt dann zu folgendem Gleichungssystem in den Koeffizienten:

$$(*) \qquad \begin{array}{lcll} a_0c_0 & + & b_0d_0 & = 0 \quad \text{Koeff. von } x^{l+m-1} \\ a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & = 0 \quad \text{Koeff. von } x^{l+m-2} \\ \ddots & & \ddots & \vdots \\ & a_lc_{m-1} + & b_md_{l-1} & = 0 \quad \text{Koeff. von } x^0 \end{array}$$

Dieses homogene lineare Gleichungssystem besteht aus $l+m$ Gleichungen in $l+m$ Variablen. Es besitzt also eine nichttriviale (nicht beide c, d gleich 0) Lösung g.d.w. die Determinante der Koeffizientenmatrix 0 ist. Diese Überlegungen motivieren die folgende Definition.

Definition 13.27: *Seien $a, b \in K[x]$ mit $\operatorname{grad}(a) = l > 0$ und $\operatorname{grad}(b) = m > 0$, also*

$$\begin{aligned} a &= a_0 x^l + \cdots + a_l, \quad a_0 \neq 0, \\ b &= b_0 x^m + \cdots + b_m, \quad b_0 \neq 0. \end{aligned}$$

Dann ist die **Sylvester-Matrix** *von a und b, in Zeichen $\operatorname{Syl}(a,b)$, die Koeffizientenmatrix des homogenen linearen Gleichungssystems $(*)$. Also $\operatorname{Syl}(a,b)$ ist die folgende $(l+m) \times (l+m)$ Matrix, bestehend aus m Spalten der Koeffizienten von a und l Spalten der Koeffizienten von b:*

$$\operatorname{Syl}(a,b) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}$$

(alle anderen Eintragungen in $\mathrm{Syl}(a,b)$ *sind 0).*
Die **Resultante** *von* a *und* b*, in Zeichen* $\mathrm{Res}(a,b)$*, ist die Determinante der Sylvestermatrix, also*

$$\mathrm{Res}(a,b) \;=\; \det(\mathrm{Syl}(a,b)) \ .$$

Auf analoge Weise erhalten wir die Resultante bzgl x_1 *zweier multivariater Polynome* $a,b \in K[x_1,\ldots,x_n]$ *mit* $\mathrm{grad}_1(a) = l > 0$ *und* $\mathrm{grad}_1(b) = m > 0$*, also*

$$\begin{aligned} a &= a_0(x_2,\ldots,x_n)x_1^l + \cdots + a_l(x_2,\ldots,x_n), \quad a_0 \neq 0, \\ b &= b_0(x_2,\ldots,x_n)x_1^m + \cdots + b_m(x_2,\ldots,x_n), \quad b_0 \neq 0. \end{aligned}$$

Diese Resultante $\mathrm{Res}_{x_1}(a,b)$ *hängt also nur von den Variablen* $x_2,\ldots,x_n$ *ab.* □

Satz 13.28: *Die Polynome* $a,b \in K[x]$ *haben einen nicht-trivialen gemeinsamen Faktor, also* $\mathrm{ggT}(a,b) \neq 1$*, g.d.w.* $\mathrm{Res}(a,b) = 0$*.*

Satz 13.29: *Zu gegebenen Polynomen* $a,b \in K[x]$ *mit positivem Grad gibt es* $c,d \in K[x]$*, sodass*

$$\mathrm{Res}(a,b) = c \cdot a + d \cdot b.$$

Weiters hängen sowohl $\mathrm{Res}(a,b)$ *als auch die Koeffizienten von* c *und* d *ganzzahlig polynomial von den Koeffizienten von* a *und* b *ab.*

Satz 13.30: *Sei* K *ein algebraisch abgeschlossener Körper. Seien*

$$a(x_1,\ldots,x_n) = \sum_{i=1}^{k} a_i(x_1,\ldots,x_{n-1})x_n^i, \qquad b(x_1,\ldots,x_n) = \sum_{i=1}^{l} b_i(x_1,\ldots,x_{n-1})x_n^i$$

n-variate Polynome in $K[x_1,\ldots,x_n]$ *vom Grad* k *bzw.* l*, für* $k,l \geq 0$*. Sei*

$$r(x_1,\ldots,x_{n-1}) = \mathrm{Res}_{x_n}(a,b).$$

(Die Resultante wird also bzgl. der Variablen x_n *berechnet.)*
Ist $(\alpha_1,\ldots,\alpha_n) \in K^n$ *eine gemeinsame Nullstelle von* a *und* b*, dann ist* $(\alpha_1,\ldots,\alpha_{n-1})$ *eine Nullstelle von* r*.*
Ist andererseits $(\alpha_1,\ldots,\alpha_{n-1})$ *eine Nullstelle von* r*, dann ist entweder*
(i) $a_k(\alpha_1,\ldots,\alpha_{n-1}) = b_l(\alpha_1,\ldots,\alpha_{n-1}) = 0$*, oder*
(ii) es gibt $a_n \in K$*, sodass* $(\alpha_1,\ldots,\alpha_n)$ *eine gemeinsame Nullstelle von* a *und* b *ist.*

Beispiel 13.31: Wir betrachten das folgende System polynomialer (algebraischer) Gleichungen:

$$a_1(x,y,z) = a_2(x,y,z) = a_3(x,y,z) = 0 \ ,$$

wobei

$$\begin{aligned} a_1 &= 2xy + yz - 3z^2 \ , \\ a_2 &= x^2 - xy + y^2 - 1 \ , \\ a_3 &= yz + x^2 - 2z^2 \ . \end{aligned}$$

Die Resultante bzgl. y von a_1 und a_3 können wir etwa berechnen als

$$\mathrm{Res}_y(a_1,a_3) = \begin{vmatrix} 2x+z & z \\ -3z^2 & x^2-2z^2 \end{vmatrix} = 2x^3 + x^2z - 4xz^2 + z^3.$$

Wie im Satz 13.30 beschrieben, eliminieren wir einige Variable aus den Gleichungen:

$$\begin{aligned} b(x) &= \mathrm{Res}_z(\mathrm{Res}_y(a_1,a_3),\mathrm{Res}_y(a_2,a_3)) \\ &= x^6(x-1)(x+1)(127x^4-167x^2+4)\ , \\ c(y) &= \mathrm{Res}_z(\mathrm{Res}_x(a_1,a_3),\mathrm{Res}_x(a_2,a_3)) \\ &= (y-1)^3(y+1)^3(3y^2-1)(127y^4-216y^2+81)(457y^4-486y^2+81)\ , \\ d(z) &= \mathrm{Res}_y(\mathrm{Res}_x(a_1,a_2),\mathrm{Res}_x(a_1,a_3)) \\ &= 5184\,z^{10}(z-1)(z+1)(127z^4-91z^2+16)\ . \end{aligned}$$

Alle gemeinsamen Nullstellen von a_1, a_2, a_3 haben Koordinaten, welche Nullstellen von b, c, d sind, etwa $(1, 1, 1)$. Aber nicht jede Nullstelle von c, etwa $1/\sqrt{3}$, lässt sich erweitern zu einer gemeinsamen Nullstelle von a_1, a_2, a_3. □

Die Methode der Resultanten ist eine von mehreren konstruktiven Zugängen zur Eliminationstheorie von multivariaten Polynomen, also der Lösung von polynomialen (algebraischen) Gleichungssystemen in mehreren Variablen. Eine andere sehr potente Methode beruht auf Gröbner-Basen. Davon lernt man in der Computeralgebra.

Gröbnerbasen für Polynomideale

Wir wollen die Idee des Euklidschen Divisionsalgorithmus verallgemeinern von univariaten Polynomen auf multivariate Polynome. Hier können 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 13.32: *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 13.33: 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

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

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 $\mathrm{ideal}(f_1, \ldots, f_m)$ ein Ideal im Sinne von Definition 13.32.

Beispiel 13.34: 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

$$f = -xy + y - 1 = f_1 - y \cdot f_2 \in \mathrm{ideal}(f_1, f_2)\ .$$ □

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

(1) $1 = x_1^0 \ldots x_n^0$ *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 13.36: 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 13.37: *Ist $<$ eine zulässige Ordnung auf den Termen über $x_1, \ldots, x_n$, so besitzt jedes vom Nullpolynom verschiedene Polynom $f \in K[x_1, \ldots, x_n]$ einen höchsten Term bzgl. $<$, genannt der* **führende Term** *von f, geschrieben* $\text{ft}(f)$.
Der (von 0 verschiedene) Koeffizient von $\text{ft}(f)$ *heisst der* **führende Koeffizient** *von f, geschrieben* $\text{fk}(f)$. □

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

Definition 13.38: *Seien $f, g, h \in K[x_1, \ldots, x_n]$. Dann ist g* **reduzierbar** *zu h modulo f, wenn es in g einen Term gibt von der Form $c \cdot t \cdot \text{ft}(f)$, 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 $c \cdot t \cdot \text{ft}(f)$ 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 13.39: 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 ideal(F). Die Umkehrung gilt aber i.a. nicht; man sieht das etwa aus Beispiel 13.34. Dort ist $f \in \text{ideal}(f_1, f_2)$, aber offensichtlich ist f bereits in Normalform.

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

Definition 13.40: *Sei G eine Teilmenge von $K[x_1, \ldots, x_n]$. Dann heisst G eine* **Gröbnerbasis** *(für* 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 13.41: *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 spol$(f_1, f_2) := g_1 - g_2$ *das* **S-Polynom** *(Subtraktionspolynom) von f_1, f_2.* □

Satz 13.42: (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 13.43: (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 13.44: Wie schon in Beispiel 13.34 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.

In Maple 16 berechnen wir diese Gröbnerbasis wie folgt:

```
> with(Groebner):
> f1 := x^2*y^2 + y - 1;
```

$$f1 := x^2y^2 + y - 1$$

```
> f2 := x^2*y + x;
```

$$f2 := x^2y + x$$

```
> F := [f1,f2];
```

$$F := \{x^2y^2 + y - 1, x^2y + x\}$$

```
> G := Basis(F,plex(y,x));
```

$$G := \{x, y - 1\}$$

Die Lösungen des Gleichungssystems

$$f_1(x, y) \;=\; f_2(x, y) \;=\; 0$$

sind also die Lösungen des Systems

$$x \;=\; 0 \;=\; y - 1 \; ,$$

also $x = 0, y = 1$. □

Beispiel 13.45: 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

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

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

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

□