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.
In diesem Kapitel 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*

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

sodass $\operatorname{supp}(p) := \{i \in \mathbb{N} \mid p(i) \neq 0\}$ *eine endliche Menge ist. Diese endliche Menge* $\operatorname{supp}(p)$ *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 $n = \max(\operatorname{supp}(p))$, dann heisst n der **Grad** *von p, geschrieben $n = \operatorname{grad}(p)$.*
Häufig schreiben wir ein Polynom in der Form

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

falls $\operatorname{supp}(p) \subseteq \{0, \ldots, n\}$ 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 beschrieben Polynom nicht.)
Für $i \in \mathbb{N}$ heisst $p(i) = p_i$ der **Koeffizient** *von p bei x^i. Ist $p \neq 0$ und $n = \operatorname{grad}(p)$, dann heisst $p(n) = p_n$ der* **führende Koeffizient** *(***leading coefficient***) von p, geschrieben* $\operatorname{lc}(p)$.
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** *"·" für zwei Polynome*

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

folgendermassen:

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

Satz 13.2: *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.*

Beispiel 13.3: 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

$$a(x) \cdot b(x) = c(x) = c_0x^0 + \cdots + c_7x^7 \ ,$$

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 9.5 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);**

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

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

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

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*

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

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 $\operatorname{grad}_r(p) := \max\{i_r \mid (i_1, \ldots, i_r, \ldots, i_m) \in \operatorname{supp}(p)\}$.

Definition 13.5: *Sei $p = p_0 + p_1x + \cdots + p_nx^n \in K[x]$ ein Polynom über dem Körper K. Dann induziert dieses Polynom eine Funktion*

$$\begin{array}{rccc} \overline{p}: & K & \longrightarrow & K \\ & a & \mapsto & p_0 + p_1a + \cdots + p_na^n \end{array}.$$

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 $\operatorname{PF}(K)$ bezeichnen wir alle Polynomfunktionen auf K.
$\operatorname{polfun} : K[x] \to \operatorname{PF}(K)$ *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* $\operatorname{polfun} : K[x] \to \operatorname{PF}(K), p \mapsto \overline{p}$ *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 $\operatorname{grad}(a) > 0$ 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 Lösungsalgorithem 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 $m \geq n$, dann lässt sich a schreiben als

$$a = \frac{\mathrm{lc}(a)}{\mathrm{lc}(b)} x^{m-n} b + r \;,$$

wobei $\mathrm{grad}(r) < \mathrm{grad}(a)$. Ist $\mathrm{grad}(r) \geq \mathrm{grad}(b)$, 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*

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

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 $r(x) = -\frac{17}{25}x - \frac{27}{25}$. $\square$

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. $\square$

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

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

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

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

Somit ist

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

Dieser ggT ist als Linearkombination

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

darstellbar.

In Maple 9.5 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**.

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 9.5:

> 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. $\square$

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:*

$$b | a \quad \text{aber} \quad b^2 \not| a \ .$$

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 9.5:
> 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. □

<u>Resultanten</u>

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) *$\mathrm{grad}(c) \le m - 1$ und $\mathrm{grad}(d) \le l - 1$, 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

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

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

$$(*) \quad \begin{array}{llllllll} a_0 c_0 & & + & b_0 d_0 & & = & 0 & \text{Koeff. von } x^{l+m-1} \\ a_1 c_0 + a_0 c_1 & & + & b_1 d_0 + b_0 d_1 & & = & 0 & \text{Koeff. von } x^{l+m-2} \\ \ddots & & & \ddots & & \vdots & & \\ & a_l c_{m-1} & + & & b_m d_{l-1} & = & 0 & \text{Koeff. von } x^0 \end{array}$$

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*

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

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

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

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

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

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.