31 Polynomringe

31.1 Motivation

Polynome spielen eine wichtige Rolle in vielen Berechnungen, einerseits weil oftmals funktionale Zusammenhänge durch Polynome beschrieben werden, andererseits weil Polynome oft zur Annäherung anderer Funktionen verwendet werden (vgl. Satz von Taylor, MfI 1, Kap. 20).

Polynomringe gehören damit zu den wichtigsten Ringen.

31.2 Definition: Polynomringe

Es sei $(R, +, \cdot)$ ein Ring (z. B. $R = \mathbb{R}$) und $a_0, a_1, \ldots, a_n \in R$. Wir setzen zur Abkürzung

$$x^k := \underbrace{x \cdot x \cdot \ldots \cdot x}_{k \text{ Faktoren}}$$

und verwenden das Summenzeichen analog zur Addition reeller Zahlen auch für die Addition in R.

Dann nennen wir die Abbildung

$$p : R \to R\,, \qquad\qquad x \mapsto \sum_{k=0}^{n} a_k x^k$$

Polynom (über R). $a_0, \ldots, a_n$ heißen **Koeffizienten** von p. Ist $a_n \neq 0$, so heißt n der **Grad** von p, symbolisch $n = \deg(p)$. (Für $p(x) = 0$ definiert man $\deg(p) = -\infty$.)

Beispiel: $p(x) = 5x^3 - 1{,}3x + 6$ ist ein Polynom vom Grad 3 über $\mathbb{R}$.

Die Menge aller Polynome über R nennen wir $R[x]$.

Auf $R[x]$ definieren wir eine Addition und eine Multiplikation „punktweise“ durch

$$\left.\begin{aligned}(p+q)(x) &:= p(x) + q(x)\\ (p \cdot q)(x) &:= p(x) \cdot q(x)\end{aligned}\right\} \quad \forall p, q \in R[x]\,.$$

Dann ist $(R[x], +, \cdot)$ ein Ring, der **Polynomring** über R.

Der Nachweis der Ringeigenschaften ist aufwändig. Man verwendet, dass für

$$p(x) = \sum_{k=0}^{n} a_k x^k \ , \qquad\qquad q(x) = \sum_{k=0}^{n} b_k x^k$$

gilt

$$(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$$

$$(p \cdot q)(x) = \sum_{k=0}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} a_i b_j \right) x^k \ .$$

Dabei wurde $n := \max(\deg(p), \deg(q))$ gesetzt (und ggf. die Koeffizienten des Polynoms niedrigeren Grades mit Nullen ergänzt).

31.3 Das Horner-Schema

Häufig müssen Funktionswerte von Polynomen effizient berechnet werden. Eine *naive* Auswertung eines Polynoms

$$p(x) = 5x^7 + 4x^6 - 3x^5 + 4x^4 + 6x^3 - 7x^2 + 4x - 1$$

erfordert 7 Additionen und $7 + 6 + 5 + 4 + 3 + 2 + 1 = 28$ Multiplikationen.

Wesentlich effizienter ist das **Horner-Schema**, das eine geschickte Klammerung ausnutzt:

$$p(x) = ((((((5x + 4)x - 3)x + 4)x + 6)x - 7)x + 4)x - 1 \ .$$

Arbeitet man die Klammern von innen nach außen ab, so benötigt man nur 7 Additionen und 7 Multiplikationen.

Allgemein benötigt man zur naiven Auswertung eines Polynoms n-ten Grades n Additionen und $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$ Multiplikationen. Das Horner-Schema reduziert den Aufwand auf n Additionen und n Multiplikationen.

In den Abschnitten 31.4–31.13 beschäftigen wir uns ausschließlich mit dem Polynomring $\mathbb{R}[x]$.

31.4 Polynomdivision in $\mathbb{R}[x]$

Im Ring $(\mathbb{Z}, +, \cdot)$ gibt es die Division mit Rest (vgl. 30.4a sowie MfI 1, Kap. 6). Kann man Ähnliches auch im Polynomring $(\mathbb{R}[x], +, \cdot)$ tun? (Achtung: Hier betrachten wir ausschließlich $R = \mathbb{R}$.)

Man kann zeigen:

Satz: Zu $a, b \in \mathbb{R}[x]$ mit $b \neq 0$ gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{R}[x]$ mit

$$a = qb + r \qquad \text{und} \quad \deg(r) < \deg(b) \; .$$

Quotient, Rest, Dividend, Divisor werden definiert wie in 30.4a.

Definition: Ist der Rest der Division von a durch b gleich 0, so ist das Polynom a durch das Polynom b teilbar. (b teilt a, b ist Teiler von a.)

31.5 Praktische Durchführung der Polynomdivision

Analog zur schriftlichen Division natürlicher Zahlen

$$\begin{array}{rl} & \overset{\text{7 geht 5}\times \text{ in 36}}{\overset{\curvearrowright}{}} \\ \overline{36}5 & : \; 7 \; = \; \underline{5}2 \quad \text{Rest} \;\; 1 \\ -\underline{35} & \leftarrow 5 \cdot 7 = 35 \\ 15 & \\ -\underline{14} & \\ 1 & \end{array}$$

führt man die Polynomdivision durch:

$$\begin{array}{rl} & \overset{x^4 : x^2 = x^2}{\overset{\curvearrowright}{}} \qquad\qquad \overset{\curvearrowright}{} \\ (\overline{x^4} + 2x^3 + 3x^2 + 4x + 5) & : (x^2+1) = \underline{x^2} + 2x + 2 \quad \text{Rest} \;\; 2x+3 \\ -\underline{(x^4 \quad + \quad x^2)} & \longleftarrow x^2 \cdot (x^2+1) = x^4 + x^2 \\ 2x^3 + 2x^2 + 4x & \\ -\underline{(2x^3 \quad + 2x)} & \\ 2x^2 + 2x + 5 & \\ -\underline{(2x^2 \quad + 2)} & \\ 2x + 3 & \end{array}$$

Satz 31.4 hat zwei wichtige Folgerungen.

31.6 Satz: Abspaltung von Nullstellen

Hat $p \in \mathbb{R}[x]$ die **Nullstelle** x_0 (d. h. $p(x_0) = 0$), so ist p durch das Polynom $x - x_0$ ohne Rest teilbar.

Beweis: Nach Satz 31.4 existieren für $p(x)$ und $b(x) = x - x_0$ die Polynome $q(x), r(x)$ mit

$$p(x) = q(x)b(x) + r(x) \ , \quad \deg(r) < \deg(b) \ .$$

In x_0 gilt dann

$$0 = p(x_0) = q(x_0) \cdot \underbrace{b(x_0)}_{=0} + r(x_0) \ . \qquad (*)$$

Wegen $\deg(r) < \deg(b) = 1$ folgt $\deg(r) \leq 0$, also $r(x) = a_0$. Wegen $(*)$ ist $r(x) = r(x_0) = 0$. □

31.7 Satz: Anzahl der Nullstellen

Ein von 0 verschiedenes Polynom $p \in \mathbb{R}[x]$ vom Grad n hat höchstens n Nullstellen.

Beweis: Angenommen, p hat mehr als n Nullstellen. Sukzessives Abspalten der Nullstellen $x_1, x_2, \ldots, x_n$ (aufgrund der Nullteilerfreiheit des Körpers $\mathbb{R}$) ergibt

$$\exists q \in \mathbb{R}[x] : \quad p(x) = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n)q(x)$$

Dabei hat $q(x)$ den Grad 0, sonst wäre $\deg(p) > n$, also ist $q(x) = a_0$.

Es sei nun x_{n+1} eine weitere Nullstelle, d. h.

$$0 = p(x_{n+1}) = (x_{n+1} - x_1)(x_{n+1} - x_2) \cdot \ldots \cdot (x_{n+1} - x_n) \cdot a_0 \ .$$

Aufgrund der Nullteilerfreiheit von $\mathbb{R}$ ist einer der Faktoren $(x_{n+1} - x_1), \ldots, (x_{n+1} - x_n), a_0$ gleich 0. Wegen $p(x) \neq 0$ kann $a_0 = 0$ nicht gelten.

Also stimmt x_{n+1} mit einem der $x_1, \ldots, x_n$ überein. □

Im Ring $(\mathbb{Z}, +, \cdot)$ gibt es die Begriffe der Teilbarkeit und des größten gemeinsamen Teilers (vgl. MfI 1, Kap. 6). Diese lassen sich auch für Polynomringe formulieren.

Teilbarkeit wurde bereits in 31.4 eingeführt.

31.8 Definition: größter gemeinsamer Teiler

Es seien $a, b \in \mathbb{R}[x]$. Ein Polynom $p \in \mathbb{R}[x]$ heißt **gemeinsamer Teiler** von a und b, falls p sowohl a als auch b teilt. p heißt **größter gemeinsamer Teiler** von a und b, falls p außerdem durch jeden gemeinsamen Teiler von a und b teilbar ist (Schreibweise: $p = \mathrm{ggT}(a, b)$).

Für eine effiziente Berechnung des ggT nutzen wir folgende Eigenschaften des ggT aus:

Lemma: Eigenschaften des ggT (vgl. MfI 1, Lemma 6.11 für ganze Zahlen)
Es seien $a, b, q \in \mathbb{R}[x]$. Dann gilt:

a) $d = \mathrm{ggT}(a, b)$ genau dann, wenn $d = \mathrm{ggT}(b, a - qb)$.

b) Ist $a = qb$, so gilt $b = \mathrm{ggT}(a, b)$.

31.9 Euklidischer Algorithmus zur ggT-Bestimmung von Polynomen

(Euklidischer Algorithmus für ganze Zahlen: MfI 1, 6.12)

Für die Polynome $a, b \in \mathbb{R}[x]$ mit $\deg(a) \geq \deg(b)$ setzen wir $r_0 := a$, $r_1 := b$ und führen sukzessive Polynomdivisionen aus:

$$\begin{aligned}
r_0 &= q_0 r_1 + r_2 \ , & \deg(r_2) &< \deg(r_1) \ , \\
r_1 &= q_1 r_2 + r_3 \ , & \deg(r_3) &< \deg(r_2) \ , \\
&\vdots & &\vdots \\
r_{n-2} &= q_{n-2} r_{n-1} + r_n \ , & \deg(r_n) &< \deg(r_{n-1}) \ , \\
r_{n-1} &= q_{n-1} r_n \ . &&
\end{aligned}$$

Dann ist $r_n = \mathrm{ggT}(a, b)$.

Beispiel:

$$a(x) = x^4 + x^3 - x^2 + x + 2$$
$$b(x) = x^3 + 2x^2 + 2x + 1$$

Polynomdivisionen:

$$(x^4 + x^3 - x^2 + x + 2) = (x - 1)(x^3 + 2x^2 + 2x + 1) + (-x^2 + 2x + 3)$$
$$(x^3 + 2x^2 + 2x + 1) = (-x - 4)(-x^2 + 2x + 3) + (13x + 13)$$
$$(-x^2 + 2x + 3) = \left(-\frac{1}{13}\,x + \frac{3}{13}\right)(13x + 13)\ .$$

Also ist $\mathrm{ggT}(a(x), b(x)) = 13x + 13$. (Eindeutig nur bis auf Vielfache: Jedes Polynom $c(13x + 13)$ mit einer Konstanten $c \neq 0$ ist ebenfalls ggT.)

Gibt es in Polynomringen eine Entsprechung zu *Primzahlen* und *Primfaktorenzerlegung* in ganzen Zahlen (vgl. MfI 1, 6.3/6.6)?

31.10 Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Ein Polynom $p \in R[x]$ heißt **reduzibel** über R, falls es Polynome $a, b \in R[x]$ mit $\deg(a) > 0$, $\deg(b) > 0$ (nichtkonstante Polynome) gibt mit $p = a \cdot b$. Andernfalls heißt p **irreduzibel** über R.

31.11 Beispiele

a) $x^2 - 4$ ist reduzibel über $\mathbb{Z}$:

$$x^2 - 4 = (x + 2)(x - 2)\ .$$

b) $x^2 - 3$ ist irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$, aber reduzibel über $\mathbb{R}$:

$$x^2 - 3 = \left(x + \sqrt{3}\right)\left(x - \sqrt{3}\right)\ .$$

c) $x^2 + 1$ ist irreduzibel über $\mathbb{R}$.

31.12 Irreduzible Polynome als „Primfaktoren“ in $\mathbb{R}[x]$

Irreduzible Polynome in $(\mathbb{R}[x], +, \cdot)$ haben ähnliche Eigenschaften wie Primfaktoren in $(\mathbb{Z}, +, \cdot)$. So existiert z. B. eine „Primfaktorzerlegung“:

Jedes nichtkonstante Polynom $p \in \mathbb{R}[x]$ lässt sich als Produkt irreduzibler Polynome aus $\mathbb{R}[x]$ darstellen. Die Darstellung ist bis auf die Reihenfolge der irreduziblen Polynome und bis auf Multiplikation mit konstanten Polynomen eindeutig.

31.13 Beispiel

$p(x) = x^3 - x^2 + x - 1$ hat in $\mathbb{R}[x]$ die folgende Zerlegung in irreduzible Polynome:

$$p(x) = (x^2 + 1)(x - 1)$$

Äquivalent hierzu sind z. B.

$$p(x) = (x - 1)(x^2 + 1) = (4x - 4)\left(\frac{1}{4}\,x^2 + \frac{1}{4}\right) .$$

Generell kann man zeigen, dass es über $\mathbb{R}$ nur zwei Typen irreduzibler Polynome gibt:

a) lineare Polynome,

b) quadratische Polynome $ax^2 + bx + c$ mit $b^2 - 4ac < 0$.

31.14 Polynomringe über allgemeinen Körpern

Das Horner-Schema (31.3) sowie die in den Abschnitten 31.4–31.13 für $\mathbb{R}[x]$ gewonnenen Resultate

- Polynomdivision
- Abspaltung von Nullstellen
- Anzahl der Nullstellen eines Polynoms n-ten Grades
- Teilbarkeit, gemeinsame Teiler, ggT, Euklidischer Algorithmus

gelten allgemein für jeden Polynomring $K[x]$ über einem Körper K. Die Beweise verlaufen identisch.

31.15 Beispiele

a) Wir betrachten den Polynomring über dem Körper $(\mathbb{Z}_5, +, \cdot)$. Das Polynom

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

hat wegen

$$\begin{aligned}
p([0]) &= [4] \cdot [0]^2 + [3] \cdot [0] - [1] = [4] \\
p([1]) &= [4] \cdot [1]^2 + [3] \cdot [1] - [1] = [1] \\
p([2]) &= [4] \cdot [2]^2 + [3] \cdot [2] - [1] = [1] \\
p([3]) &= [4] \cdot [3]^2 + [3] \cdot [3] - [1] = [4] \\
p([4]) &= [4] \cdot [4]^2 + [3] \cdot [4] - [1] = [0]
\end{aligned}$$

in $\mathbb{Z}_5$ genau eine Nullstelle, nämlich $[4]$.

b) Abspalten der Nullstelle durch Polynomdivision in $(\mathbb{Z}_5, +, \cdot)$:

$$\begin{array}{rl}
([4]x^2 + [3]x - [1]) & : (x - [4]) \quad = [4]x + [4] \\
-(\underline{[4]x^2 - [1]x}\,) & \\
\qquad [4]x - [1] & \\
\qquad -(\underline{[4]x + [4]}) & \\
\qquad\qquad [0] &
\end{array}$$

Also ist

$$[4]x^2 + [3]x - [1] = (x - [4])([4]x + [4]) = [4](x - [4])^2 \quad \text{in } \mathbb{Z}_5.$$

31.16 Anwendung: Fehlerkorrektur in der Datenübertragung

Bei der Übertragung binärer Daten können Bits „umklappen“.

Einfachste Abhilfe zur Fehlererkennung: Einführung von zusätzlichen Prüfbits.

Beispiel: Ein Datenblock von 1 Byte wird übertragen; es wird ein Prüfbit angehängt, das die Summe der Bits modulo 2 angibt:

$$\underbrace{1\ 1\ 0\ 0\ 1\ 1\ 0\ 1}_{\text{Byte (Daten)}}\ \Big|\ \underbrace{1}_{\text{Prüfbit}}$$

Empfängt man beispielsweise 11011101|1, muss ein Fehler aufgetreten sein.

Nachteile:

- Man muss 1/8 mehr Daten übertragen.
- Kein Fehler wird festgestellt, wenn 2 Bits umklappen.

Sicherung mittels Polynomdivision in $\mathbb{Z}_2$: Alternativ kann man wie folgt vorgehen:

a) Interpretiere die Bits eines zu übertragenden Datenblocks als Koeffizienten eines Polynoms $f(x) \in \mathbb{Z}_2[x]$.

Beispiel: Byte als Datenblock: 11001101
Polynom: $f(x) = x^7 + x^6 + x^3 + x^2 + 1$

b) Ein festes „Generatorpolynom“ $g(x) \in \mathbb{Z}_2[x]$ mit $\deg(g) = n$ dient als Divisor. Typischerweise ist $\deg(g) \ll \deg f$.

c) Betrachte statt $f(x)$ das Polynom $h(x) = x^n \cdot f(x)$.

(Das heißt: an die Bitfolge zu $f(x)$ werden n Nullen angehängt.)

Beispiel ($n = 4$):

$$\overbrace{\underbrace{1\ 1\ 0\ 0\ 1\ 1\ 0\ 1}_{f(x)}\ |\ \underbrace{0\ 0\ 0\ 0}_{\cdot x^n}}^{h(x)}$$

d) Berechne die Polynomdivision $h(x) : g(x)$ in $\mathbb{Z}_2[x]$:

$$h(x) = q(x)g(x) + r(x) \ , \quad \deg(r) < n \ .$$

e) Sende $h(x) - r(x) = q(x)g(x)$. (In $\mathbb{Z}_2[x]$ ist dies auch gleich $h(x) + r(x)$.)

Wegen $\deg(r) < n$ unterscheiden sich $h(x) - r(x)$ und $h(x)$ höchstens in den letzten n Bits:

$$\overbrace{\underbrace{1\,1\,0\,0\,1\,1\,0\,1}_{f(x)} \mid \underbrace{?\,?\,?\,?}_{r(x)}}^{h(x)-r(x)}$$

$r(x)$ dient der Fehlererkennung.

f) Der Empfänger erhält das Polynom $p(x)$.

Tritt bei Division durch $g(x)$ ein Rest auf, so ist $p(x) \neq h(x) - r(x)$, es ist also ein Übertragungsfehler aufgetreten.

Bei geschickter Wahl von $g(x)$

- ist es sehr unwahrscheinlich, dass bei einem Übertragungsfehler die Division $p(x) : g(x)$ ohne Rest aufgeht
- kann man anhand des Divisionsrestes den Fehler lokalisieren und korrigieren.

Konkrete Spezifikation im X.25-Übertragungsprotokoll:

- Datenblock: 4 096 Byte = 32 768 Bit
  $\Rightarrow \deg(f) = 32\,767$.
- Generatorpolynom: $g(x) = x^{16} + x^{12} + x^5 + 1$
  $\Rightarrow \deg(g) = 16$ (2 Byte zur Fehlerkorrektur)

Es werden nur $\frac{2}{4096} \approx 0{,}49$ Promille zusätzliche Daten übertragen. Erkannt werden unter Anderem alle 1-, 2- und 3-Bit-Fehler sowie alle Fehler mit ungerader Anzahl umgeklappter Bits.

Die Algorithmen zur Polynomdivision in $\mathbb{Z}_2[x]$ lassen sich effizient in Soft- und Hardware realisieren.