# Kapitel 2

# Polynome

## 2.1 Polynome, Polynomfunktionen und Nullstellen

**Der Polynomring $R[x]$**

**Definition:** Ein *Polynom* mit einer Variablen $x$ über einem kommutativen Ring $R$ ist ein formaler Ausdruck der Form

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

wobei alle $a_k$ Elemente des Rings $R$ sind und $a_n \neq 0$. Die Werte $a_k$ nennt man die Koeffizienten des Polynoms $p(x)$. Der Grad dieses Polynoms ist $n$. Die Menge aller Polynome über dem Ring $R$ wird mit $R[x]$ bezeichnet.

Jedes Polynom bestimmt eine *Polynomfunktion* $R \to R$, die man an jeder Stelle $r \in R$ durch Einsetzen des Wertes $r$ für die Variable $x$ und Auswertung der Operationen im Ring $R$ berechnen kann. Der Wert, der sich bei dieser Auswertung ergibt, wird mit $p(r)$ bezeichnet.

Leider kann diese Notation auch leicht zu Verwechslungen zwischen Polynom und Polynomfunktion führen. Einziges Unterscheidungsmerkmal ist das Argument: ist $x$ eine Variable, so bezeichnet $p(x)$ ein Polynom, für Ringelemente $r$ bezeichnet $p(r)$ den Wert der Polynomfunktion an der Stelle $r$. Soll dieser Unterschied noch deutlicher betont werden, kann die Funktion auch mit $f_p$ bezeichnet werden, der Wert an der Stelle $r$ wäre dann $f_p(r)$.

Zwei Polynome

$$p(x) = \sum_{k=0}^{n} a_k x^k \quad \text{und} \quad q(x) = \sum_{k=0}^{m} b_k x^k$$

sind (syntaktisch) gleich, falls $n = m$ und $a_k = b_k$ für $k = 0, \ldots n$

Durch Einführung einer Addition und einer Multiplikation von Polynomen bildet sich die Struktur des Polynomrings $R[x]$. Die Operationen sind so definiert, dass sie verträglich mit den Operationen auf den Polynomfunktionen (Addition und Multiplikation der Funktionswerte) sind. In der folgenden Formel werden alle nicht in den Operanden definierten Werte

$a_k$ und $b_k$ gleich 0 gesetzt.

$$\begin{aligned}\sum_{k=0}^{n} a_k x^k \pm \sum_{k=0}^{m} b_k x^k &= \sum_{k=0}^{max(n,m)} (a_k \pm b_k) x^k \\ \sum_{k=0}^{n} a_k x^k \cdot \sum_{k=0}^{m} b_k x^k &= \sum_{k=0}^{n+m} (\sum_{j=0}^{k} a_j b_{k-j}) x^k\end{aligned}$$

**Horner-Schema**

Der naive Ansatz zur Auswertung eines Polynoms von Grad $n$ an einer Stelle $r$ erfordert $2n-1$ Multiplikationen (Potenzen von $r$ berechnen und mit den Koeffizienten multiplizieren) und $n$ Additionen. Wesentlich effizienter ist die Polynomauswertung mit dem *Horner-Schema*, für die $n$ Multiplikationen und $n$ Additionen ausreichend sind. Die Grundidee beruht auf der folgenden Beobachtung:

$$\begin{aligned}f(r) &= \sum_{k=0}^{n} a_k r^k \\ &= a_n r^k + a_{n-1} r^{n-1} + \ldots + a_2 r^2 + a_1 r + a_0 \\ &= ((((\underbrace{a_n}_{c_n} r + a_{n-1}) \cdot r \ldots a_3) \cdot r + a_2) \cdot r + a_1) \cdot r + a_0\end{aligned}$$

$$\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{a_n}_{c_n} r + a_{n-1}}_{c_{n-1}} \cdot r \ldots a_3}_{c_3} \cdot r + a_2}_{c_2} \cdot r + a_1}_{c_1} \cdot r + a_0}_{c_0}$$

Offensichtlich ist $c_n = a_n$ und für die Berechnung der Zwischenergebnisse $c_{n-1}, c_{n-2}, \ldots, c_0$ braucht man jeweils eine Multiplikation und eine Addition. Zur Rechnung auf dem Papier verwendet man das folgende Schema:

| $f(x) \mapsto$ | $a_n$ | $a_{n-1}$ | $a_{n-1}$ | $\ldots$ | $a_1$ | $a_0$ |
|---|---|---|---|---|---|---|
| $+$ | | $c_n \cdot r$ | $c_{n-1} \cdot r$ | | $c_2 \cdot r$ | $c_1 \cdot r$ |
| | $c_n$ | $c_{n-1}$ | $c_{n-2}$ | $c_2$ | $c_1$ | $c_0$ |

Der Wert von $c_0$ ist der Funktionswert von $f(x)$.

**Beispiel:** Bestimme $f(3)$ von $f(x) = 2x^4 - 4x^3 + 3x + 10$. Wichtig ist, dass für alle fehlenden Koeffizienten Nullen eingetragen werden!

| | | | | | |
|---|---|---|---|---|---|
| | 2 | $-4$ | 0 | 3 | 10 |
| $+$ | | 6 | 6 | 18 | 63 |
| | 2 | 2 | 6 | 21 | 73 |

Damit ist $f(3) = 73$.

Das Horner-Schema kann man auch einsetzen, um einige spezielle Polynomdivisionen auszuführen, bei denen ein Polymon $p(x) = \sum_{k=0}^{n} a_k x^k$ durch ein Polynom der Form $(x-a)$ geteilt

wird (der allgemeine Fall wird im nächsten Abschnitt behandelt). Ziel ist die Bestimmung eines Polynoms $q(x) = \sum_{k=0}^{n-1} b_k x^k$ und eines Rests $r' \in R$, so dass

$$p(x) = q(x) \cdot (x - a) + r'.$$

Wertet man das Polynom $p(x)$ an der Stelle $a$ mit dem Horner Schema aus und setzt $b_{n-1} = c_n, b_{n-2} = c_{n-1}, \ldots, b_1 = c_2, b_0 = c_1$ und $r' = c_0$, kann durch einen einfachen Koeffizientenvergleich nachgerechnet werden, dass die geforderte Identität erfüllt ist:
Für $x^n$ steht auf der linken Seite (Polynom $p(x)$) der Koeffizient $a_n$, auf der rechten Seite (bei $q(x) \cdot (x - a) + r'$) der Koeffizient $b_{n-1} = c_n = a_n$.
Für $x^{n-1}$ steht links der Koeffizient $a_{n-1}$, rechts der Koeffizient $b_{n-2} - a \cdot b_{n-1} = c_{n-1} - a \cdot c_n = a_{n-1}$, denn $c_{n-1} = a \cdot c_n + a_{n-1}$.
Analog setzt sich das fort bis zum Koeffizienten von $x^0$: Links steht $a_0$ und auf der rechten Seite $r' - a \cdot b_0 = c_o - a \cdot c_1 = a_0$, denn $c_0 = a \cdot c_1 + a_0$.

### Nullstellen

**Definition:** $a \in R$ ist Nullstelle des Polynoms $p(x) \in R[x]$, falls $p(a) = 0$.

**Satz:** Ist $a$ Nullstelle von $p(x)$, dann existiert ein Polynom $q(x)$, so dass

$$p(x) = (x - a) \cdot q(x)$$

Der Beweis folgt aus der Anwendung des Horner-Schemas zur Polynomdivision: $c_0$ ist einerseits der Rest aus der Polynomdivision durch $(x-a)$, andererseits der Wert der Polynomfunktion an der Stelle $a$. Deshalb ist $a$ genau dann eine Nullstelle, wenn bei der Polynomdivision der Rest verschwindet.

**Definition:** $a$ ist $k$-fache Nullstelle von $p(x)$, wenn ein Polynom $q(x)$ existiert, so dass

$$p(x) = (x - a)^k \cdot q(x)$$

### Zerlegung von komplexen und reellen Polynomen

**Fundamentalsatz der Algebra (Gauss):** Jedes komplexe Polynom $p(x) = \sum_{k=0}^{n} a_k x^k$ mit $a_i \in \mathbb{C}$ hat eine komplexe Nullstelle. Folglich kann $p(x)$ in der Form

$$a_n \cdot \prod_{\mu=1}^{n} (x - z_\mu)$$

dargestellt werden, wobei $z_\mu$ die Nullstellen von $p(x)$ sind.

Auf den (recht anspruchsvollen) Beweis wird hier verzichtet. Stattdessen sollen die Konsequenzen für reelle Polynome genauer untersucht werden:

1. Jedes reelle Polynom hat eine komplexe Nullstelle.
2. Ist $z$ eine komplexe Nullstelle eines reellen Polynoms $p(x) = \sum_{k=0}^{n} a_k x^k$, dann ist auch die konjugiert komplexe Zahl $\overline{z}$ eine Nullstelle von $p(x)$:

$$\begin{aligned} p(\overline{z}) = \textstyle\sum_{k=0}^{n} a_k \overline{z}^k &= \textstyle\sum_{k=0}^{n} \overline{a}_k \overline{z}^k && | a_k \in \mathbb{R} \\ &= \overline{\textstyle\sum_{k=0}^{n} a_k z^k} && | \overline{v} \cdot \overline{w} = \overline{v \cdot w} \\ &= \overline{\textstyle\sum_{k=0}^{n} a_k z^k} && | \overline{v} + \overline{w} = \overline{v + w} \\ &= \overline{p(z)} = \overline{0} = 0. \end{aligned}$$

3. Ist $z \in \mathbb{C} \setminus \mathbb{R}$ eine komplexe Nullstelle eines reellen Polynoms $p(x)$, dann gibt es ein (komplexes) Polynom $q(x)$, so dass

$$p(x) = (x - z)(x - \overline{z})q(x) = (x^2 - (z + \overline{z}) + z\overline{z})q(x) = (x^2 - 2Re(z) + |z|^2)q(x)$$

Da die beiden Linearfaktoren zusammen ein reelles Polynom ergeben, ist auch $q(x)$ ein reelles Polynom. Der folgende Satz fasst die Schlussfolgerungen zusammen.

**Satz:** Jedes reelle Polynom $p(x) \in \mathbb{R}[x]$ kann folgendermaßen zerlegt werden:

$$p(x) = \sum_{k=0}^{n} a_k x^k = a_n \cdot \prod_{i=1}^{l} (x - b_i)^{k_i} \cdot \prod_{i=1}^{m} (x^2 + c_i x + d_i) \qquad \text{mit}$$

- $k_1 + k_2 + \ldots + k_l + 2m = n$ ist Grad des Polynoms $p(x)$.
- $b_1, b_2, \ldots b_l$ sind $k_1$–fache, $k_2$–fache bzw. $k_l$–fache reelle Nullstellen von $p(x)$.
- Die Polynome $x^2 + c_i \cdot x + d_i$ haben keine reelle Nullstellen.

Zum Beweis dieses Satzes genügt es, die vorher aufgelisteten Beobachtungen zusammenzufassen und rekursiv anzuwenden. Den Abschluss dieses Abschnitts bildet ein weiterer Satz, der für unendliche Körper eine Bijektion zwischen Polynomen und Polynomfunktionen postuliert. Es ist wichtig, darauf hinzuweisen, dass die Aussage nicht auf Polynome über endlichen Körper übertragen werden kann.

**Satz:** Zwei Polynome $p(x), q(x) \in \mathbb{R}[x]$ (auch aus $\mathbb{Q}[x]$ oder $\mathbb{C}[x]$) sind genau dann syntaktisch gleich (gleiche Koeffizienten), wenn sie semantisch gleich sind (gleiche Polynomfunktionen).

**Beweis:** Nur die Rückrichtung muss begründet werden. Angenommen zwei Polynome $p(x)$ und $q(x)$ erzeugen die gleiche Polynomfunktion und sei $n$ das Maximum der Grade der beiden Polynome. Das Differenzpolynom $s(x) = p(x) - q(x)$ hat die Eigenschaft, an jeder Stelle $r \in \mathbb{R}$ den Wert 0 anzunehmen: $s(r) = p(r) - q(r) = 0$.
Dann sind die Zahlen $0, 1, \ldots n$ Nullstellen von $s(x)$ und es gibt ein Polynom $t(x)$, so dass

$$s(x) = (x - 0)(x - 1) \ldots (x - n)t(x)$$

Da der Grad von $s(n)$ höchstens $n$ ist, aber die ersten $n + 1$ Faktoren auf der rechten Seite schon ein Polynom vom Grad $n + 1$ erzeugen, bleibt als einzige Konsequenz, dass $t(x)$ das Nullpolynom ist. Damit ist auch $s(x)$ das Nullpolynom und daraus folgt die Gleichheit von $p(x)$ und $q(x)$.

## 2.2 Rationale Funktionen

In diesem Abschnitt werden nur Polynome über den reellen Zahlen behandelt. Man kann aber alle Betrachtungen problemlos auf Polynome über einem beliebigen Körper verallgemeinern, wenn man die Division von Zahlen durch die Multiplikation mit inversen Elementen ersetzt ($a \cdot b^{-1}$ anstelle von $\frac{a}{b}$).

**Definitionen:**

- Eine *ganz rationale Funktion* ist eine Polynomfunktion $p(x)$.

- Eine *(gebrochen) rationale Funktion* ist ein Quotient aus zwei Polynomen $\frac{p(x)}{q(x)}$.
- Eine *echt gebrochen rationale Funktion* ist ein Quotient von zwei Polynomen $\frac{p(x)}{q(x)}$ mit $\text{Grad}(p(x)) < \text{Grad}(q(x))$.

**Satz:** Jede rationale Funktion $\frac{p(x)}{q(x)}$ lässt sich darstellen in der Form

$$\frac{p(x)}{q(x)} = h(x) + \frac{r(x)}{q(x)}$$

wobei $h(x)$ ganz rational und $\frac{r(x)}{q(x)}$ echt gebrochen rational ist.

**Beweis:** Dieser Beweis zeigt, warum und wie *Polynomdivision* funktioniert. Eine entscheidende Rolle spielen die Grade $n$ und $m$ und die führenden Koeffizienten $a_n$ und $b_m$ der Polynome

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

Für $n < m$ ist die Behauptung trivialerweise erfüllt, indem man für $h(x)$ das Nullpolynom und $r(x) = p(x)$ setzt. Ist $n \geq m$, wird der Satz mit vollständiger Induktion nach $d = n - m$ bewiesen:

**Induktionsanfang:** $d = 0$, d.h. $n = m$

Man setzt $h(x) = \frac{a_n}{b_n}$ und $r(x) = p(x) - \frac{a_n}{b_n} \cdot q(x)$.

Zu zeigen ist $\text{Grad}(r(x)) < n$ und $\frac{p(x)}{q(x)} = h(x) + \frac{r(x)}{q(x)}$

Dazu untersucht man den Koeffizienten von $x^n$ im Polynom $r(x)$, das ist $a_n - \frac{a_n}{b_n} \cdot b_n = 0$. Folglich ist der Grad von $r(x)$ kleiner als $n$.
Für die zweite Behauptung geht man von der Identität $p(x) = \frac{a_n}{b_n} q(x) + p(x) - \frac{a_n}{b_n} q(x) = h(x)q(x) + r(x)$ aus. Die Behauptung folgt, wenn man beide Seiten durch $q(x)$ teilt.

**Induktionsschritt:** $d \to d + 1$

Sei $n = m + d + 1$. Man beginnt mit einem ähnlichen Ansatz wie beim Induktionsanfang:

$$p_1(x) = p(x) - \frac{a_n}{b_m} \cdot x^{n-m} \cdot q(x) \text{ und folglich } \frac{p(x)}{q(x)} = \frac{a_n}{b_m} \cdot x^{n-m} + \frac{p_1(x)}{q(x)}$$

Der Koeffizient von $x^n$ im Polynom $p_1(x)$ ist 0, d.h. der Grad von $p_1(x)$ ist kleiner als $n$ und folglich kann für die rationale Funktion $\frac{p_1(x)}{q(x)}$ die Induktionsvoraussetzung angewendet werden. Bezeichnet man die Polynome aus der Induktionsvoraussetzung mit $h_1(x)$ und $r_1(x)$, so ergibt sich

$$\begin{aligned} \frac{p(x)}{q(x)} &= \frac{a_n}{b_m} \cdot x^{n-m} + \frac{p_1(x)}{q(x)} \\ &= \frac{a_n}{b_m} \cdot x^{n-m} + h_1(x) + \frac{r_1(x)}{q(x)} \\ &= h(x) + \frac{r_1(x)}{q(x)} \end{aligned}$$

Die Polynomdivision spielt im Polynomring $\mathbb{R}[x]$ eine ähnliche Rolle wie die ganzzahlige Division mit Rest im Ring der ganzen Zahlen. Insbesondere kann man die Definitionen vom größten

gemeinsamen Teiler (ggT) und kleinsten gemeinsamen Vielfachen (kgV) auf den Polynomring übertragen und den Euklidischen Algorithmus zur Berechnung des ggT verwenden.

**Definition:** Seien $p(x)$ und $q(x)$ Polynome, dann ist der *größte gemeinsame Teiler* $\text{ggT}(p(x), q(x))$ das Polynom $d(x)$ maximalen Grades, so dass Zerlegungen

$$p(x) = d(x) \cdot h(x) \quad \text{und} \quad q(x) = d(x) \cdot g(x)$$

existieren und der führende Koeffizent von $d(x)$ gleich 1 ist.
Das *kleinste gemeinsame Vielfache* $\text{kgV}(p(x), q(x))$ ist das Polynom $s(x)$ minimalen Grades, so dass Zerlegungen

$$s(x) = p(x) \cdot h(x) \quad \text{und} \quad s(x) = q(x) \cdot g(x)$$

existieren und der führende Koeffizent von $s(x)$ gleich 1 ist.

**Euklidischer Algorithmus**

Voraussetzung: $p(x)$ und $q(x)$ sind zwei Polynome deren führende Koeffizenten 1 sind und $\text{Grad}(p(x)) \geq \text{Grad}(q(x))$.

```
procedure ggT(p(x), q(x))
    s(x) = p(x)
    t(x) = q(x)
    while (t(x) != 0)
       r(x) = Rest von s(x) / t(x)
       s(x) = t(x)
       t(x) = r(x)
    return s(x)
```

Mit Hilfe des größten gemeinsamen Teilers kann auch das kleinste gemeinsame Vielfache leicht berechnet werden:

$$kgV(p(x), q(x)) \;=\; \frac{p(x) \cdot q(x)}{ggT(p(x), q(x))}$$

**Definition:** Zur Bestimmung der Definitionsbereichs von rationalen Funktionen $\frac{p(x)}{q(x)}$ wird vorausgesetzt, dass $\text{ggT}(p(x), q(x)) = 1$. Ist diese Voraussetzung noch nicht erfüllt, muss zuerst eine gekürzte Darstellung erzeugt werden, indem man beide Polynome durch ihren größten gemeinsamen Teiler teilt. Der Definitionsbereich besteht dann aus allen reellen Zahlen mit Ausnahme der Nullstellen des Polynoms $q(x)$ in der gekürzten Darstellung.

**Beispiel:** $\frac{x^2-1}{x-1} = \frac{x+1}{1}$ ist definiert auf ganz $\mathbb{R}$.

**Definition (Polstelle):** Ist $\text{ggT}(p(x), q(x)) = 1$ und ist $b$ eine $k$-fache Nullstelle von $q(x)$, dann nennt man $b$ einen $k$-fachen *Pol* der rationalen Funktion $\frac{p(x)}{q(x)}$.

## 2.3 Polynominterpolation

Viele Zusammenhänge in realen Prozessen und verschiedene physikalische Gesetze lassen sich durch Polynome beschreiben (z.B der Zusammenhang zwischen elektrischer Spannung und Leistung in einem Stromkreis oder das Fallgesetz). Ist solch ein Zusammenhang bekannt

(d.h. kennt man das Polynom, das ein bestimmtes Gesetz beschreibt), kann man durch Einsetzen von Werten auch Aussagen zu Situationen machen, die nicht experimentell untersucht wurden. Häufig will man aber den umgekehrten Weg gehen: Man kennt den Zusammenhang noch nicht und versucht, eine Reihe von Messwerten als Funktionswerte eines Polynoms (kleinen Grades) zu interpretieren. Ein erster Schritt dazu ist die *Polynominterpolation*, bei der es darum geht, ein Polynom zu finden, dass die Messwerte genau wiedergibt (nicht zu verwechseln mit der Polynomapproximation, bei der kleine Fehler erlaubt sind, aber dafür der Grad stärker beschränkt ist).

**Aufgabenstellung:** Gegeben sind $n+1$ reelle Wertepaare $(x_0, y_0), (x_1, y_1), \ldots (x_n, y_n)$, wobei $x_0 < x_1 < \ldots < x_n$ vorausgesetzt wird. Gesucht ist ein Polynom $p(x)$ vom Grad $\leq n$, so dass $p(x_i) = y_i$ für alle $i = 0, 1, \ldots, n$. Die $x$–Werte bezeichnet man auch als Stützstellen des gesuchten Polynoms.

Es gibt eine Reihe verschiedener Ansätze zur Lösung dieses Problems. Der naive Ansatz geht von einem Polynom $p(x) = \sum_{k=0}^{n} a_k x^k$ aus, wobei die Koeffizienten Variable sind. Bei der Auswertung des Polynoms an der Stelle $x_i$ (das ist eine konkrete Zahl) entsteht die Gleichung $\sum_{k=0}^{n} x_i^k a_k = y_i$, die in den Variablen $a_k$ linear ist. Insgesamt entsteht ein System von $n+1$ linearen Gleichungen mit $n+1$ Variablen. Wie später gezeigt wird, gibt es eine eindeutige Lösung des Gleichungssystems, die man mit den bekannten Verfahren (z.B. Gauß-Elemination) ausrechnen kann.

Wesentlich eleganter ist aber die folgende *Interpolation mit Lagrange-Polynomen.*

**Satz:** Für die in der Aufgabenstellung gegebenen Wertepaare gibt es genau ein Polynom $p(x)$ vom Grad $\leq n$, dass die Forderung $p(x_i) = y_i$ für alle $i = 0, 1, \ldots, n$ erfüllt. Dieses Polynom hat die Form

$$p(x) := \sum_{j=1}^{n} y_j \cdot \left( \prod_{i \in \{1,2,\ldots,n\} \setminus \{j\}} \frac{x - x_i}{x_j - x_i} \right)$$

**Beweis:** Man betrachtet zuerst die in der Summe zusammengefassten Hilfspolynome, die offensichtlich alle vom Grad $n$ sind:

$$p_j(x) = \prod_{i \in \{1,2,\ldots,n\} \setminus \{j\}} \frac{x - x_i}{x_j - x_i}$$

Wie man leicht überprüfen kann, tritt bei der Auswertung von $p_j(x)$ an einer Stelle $x_i$ der folgende Effekt auf:

$$p_j(x_i) \;=\; \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

Durch die Multiplikation der Hilfspolynome $p_j$ mit den vorgegebenen Funktionswerten $y_j$ zeigt das Polynom $p(x) = \sum_{j=0}^{n} y_j \cdot p_j(x)$ das gewünschte Verhalten.
Zum Eindeutigkeitsbeweis geht man wieder davon aus, dass zwei Polynome $p(x)$ und $q(x)$ den Satz erfüllen. Der Grad des Differenzpolymons $s(x) = p(x) - q(x)$ ist kleiner oder gleich $n$, aber es hat mindestens $n+1$ Nullstellen, nämlich $x_0, x_1, \ldots, x_n$. Somit muss $s(x)$ das Nullpolynom sein und daraus folgt mit $p(x) = q(x)$ die Eindeutigkeit. □

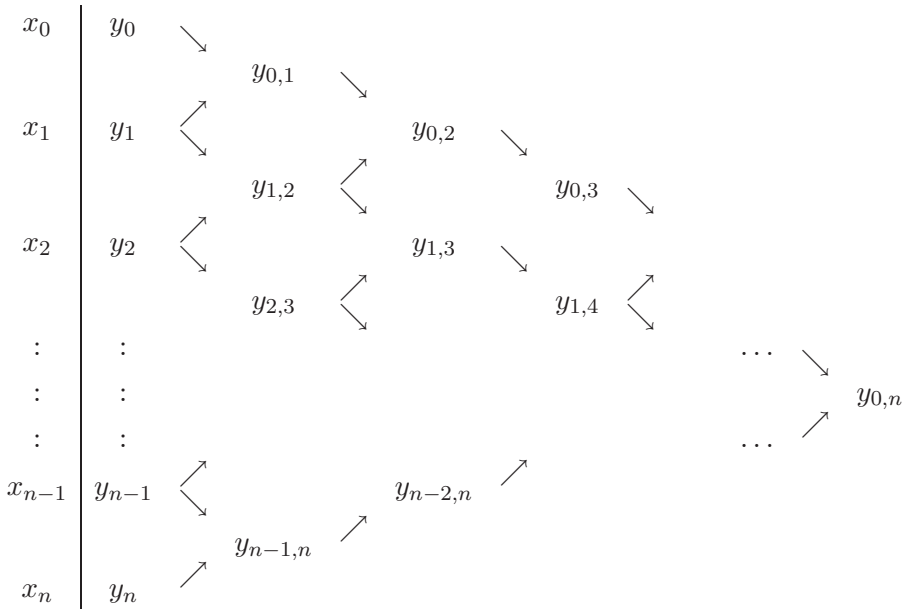
Eine dritte Methode zur Polynominterpolation geht auf Newton zurück. Sie geht von dem folgenden Ansatz aus.

$$p(x) = \alpha_0 + \alpha_1(x - x_0) + \alpha_2(x - x_0)(x - x_1) + \ldots + \alpha_n(x - x_0)(x - x_1)\ldots(x - x_{n-1})$$

Zunächst ist nicht klar, ob man auf diesem Weg überhaupt ein Polyynom erhalten kann, das alle Forderungen erfüllt. Durch schrittweises Einsetzen der Werte $x_0, x_1, \ldots, x_n$ ergibt sich aber das Gleichungssystem

$$\begin{aligned}
y_0 &= \alpha_0 \\
y_1 &= \alpha_0 + \alpha_1(x - x_0) \\
y_2 &= \alpha_0 + \alpha_1(x - x_0) + \alpha_2(x - x_0)(x - x_1) \\
&\vdots \\
&\vdots \\
y_n &= \alpha_0 + \alpha_1(x - x_0) + \alpha_2(x - x_0)(x - x_1) + \ldots + \alpha_n(x - x_0)(x - x_1)\ldots(x - x_{n-1})
\end{aligned}$$

Daraus kann man schrittweise von oben nach unten die Werte von $\alpha_0, \alpha_1, \ldots \alpha_{n-1}$ berechnen und das Polynom $p(x)$ zusammensetzen. Die Berechnung der $\alpha$-Werte kann durch die Nutzung des sogenannten Schemas der dividierten Differenzen noch weiter vereinfacht werden:




Dabei werden die Einträge $y_{i,j}$ spaltenweise von links nach rechts nach der folgenden Formel berechnet:

$$y_{i,i+1} = \frac{y_{i+1} - y_i}{x_{i+1} - x_i} \quad \text{und für alle } j > i+1 \quad y_{i,j} = \frac{y_{i+1,j} - y_{i,j-1}}{x_j - x_i}$$

**Anwendung: Polynommultiplikation mit schneller Fourier-Transformation**

Bei der Multiplikation von zwei Polynomen $p(x) = \sum_{k=0}^{n-1} a_k x^k$ und $q(x) = \sum_{k=0}^{n-1} b_k x^k$ vom Grad $n-1$ entsteht das Polynom

$$s(x) = p(x) \cdot q(x) = \sum_{k=0}^{2n-2} c_k x^k, \quad \text{wobei} \quad c_k = \sum_{j=0}^{k} a_j b_{k-j}$$

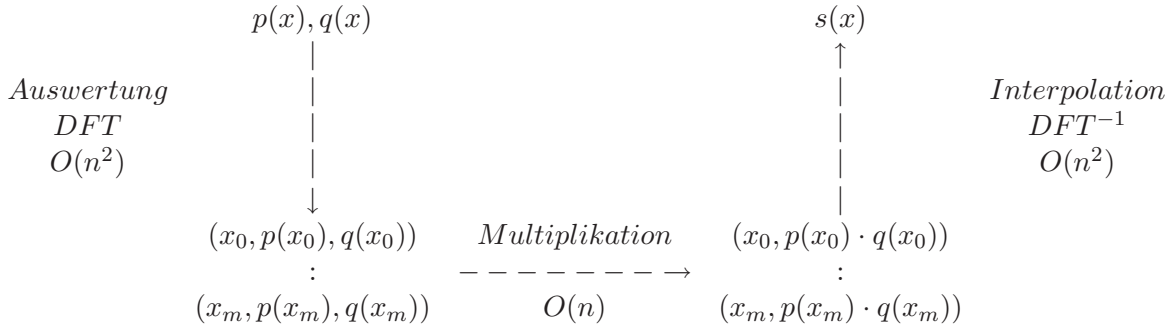
Zur (naiven) Berechnung der Koeffizienten nach dieser Formel sind $n^2$ Multiplikationen und annähernd $n^2$ Additionen notwendig. Mit einer Teile-und-Herrsche-Strategie kann man die Laufzeit wesentlich verbessern. Dazu zerlegt man die Ausgangspolynome jeweils in die Summe

von zwei Teilpolynomen (gleicher Größe) für die niedrigen und für die hohen Potenzen von $x$ und führt die Multiplikation auf die folgende Art und Weise aus:

$$\begin{aligned} p(x) &= p_0(x) + x^{n/2} p_1(x) \\ q(x) &= q_0(x) + x^{n/2} q_1(x) \\ s(x) &= p_0(x)q_0(x) + x^{n/2}\left(p_0(x)q_0(x) + p_1(x)q_1(x) - (p_1(x) - p_0(x))(q_1(x) - q_0(x))\right) \\ &\quad + x^n p_1(x)q_1(x) \end{aligned}$$

Obwohl diese Formel unnötig kompliziert erscheint, hat sie den Vorteil, dass auf Grund von Termwiederholungen nur drei Polynommultiplikationen notwendig sind. Bei rekursiver Anwendung führt das zu drei rekursiven Aufrufen bei Halbierung der Problemgröße und damit zu einer Laufzeit von $O(n^{\log_2 3}) = O(n^{1.586})$.

Die Grundidee zur Polynommultiplikation mit der diskreten Fourier-Transformation (DFT) beruht auf der oben bewiesenen Tatsache, dass ein Polymom vom Grad $m-1$ bereits eindeutig durch seine Werte an $m$ Stellen bestimmt ist. Für $s(x)$ braucht man also die Werte an $m = 2n-1$ Stellen $x_0, x_1, \ldots x_m$.




Wie bereits in der schematischen Darstellung angedeutet, bedeutet dieser Ansatz noch keinen Fortschritt bei der Laufzeit, aber diese kann entscheidend verbessert werden, wenn man auch wieder eine Teile-und-Herrsche-Strategie verwendet und darüber hinaus eine günstige Auswahl der Stützstellen trifft. Besonders geeignet sind die komplexen $n$-ten Einheitswurzeln.

Im Folgenden gehen wir davon aus, dass $n = 2^k$ eine Zweierpotenz ist, das Produktpolynom $s(x)$ vom Grad $< n$ ist und die Koeffizienten aller beteiligten Polynome durch Auffüllung mit führenden Nullen bis $n-1$ laufen. Damit sind alle beteiligten Polynome durch ihre Werte auf den $n$-ten Einheitswurzeln $\zeta_{0,n}, \zeta_{1,n}, \ldots, \zeta_{n-1,n}$ definiert.
Die Abbildung des Koeffiziententupels eines Polynoms $p(x)$ auf das Wertetupel nennt man die diskrete Fourier-Transformation:

$$(a_0, a_1, \ldots, a_{n-1}) \overset{DFT}{\longmapsto} (y_0, y_1, \ldots, y_{n-1}) \quad \text{wobei} \quad y_k = p(\zeta_{k,n}) = \sum_{i=1}^{n-1} a_i \zeta_{k,n}^i$$

Für die Rekursion zur schnellen Fourier-Transformation wird das Koeffiziententupel nach geraden und ungeraden Indizes unterteilt und damit zwei neue Polynome von Grad $\frac{n}{2} - 1$ definiert:

$$\begin{aligned} p^{even}(x) &= \sum_{k=0}^{\frac{n}{2}-1} a_{2k} x^k \\ p^{odd}(x) &= \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} x^k \\ p(x) &= p^{even}(x^2) + x \cdot p^{odd}(x^2) \end{aligned}$$

Die Berechnung der Werte $y_k$ wird auch in zwei Teilaufgaben zerlegt, zuerst für alle $k < \frac{n}{2}$ und dann für alle $l \geq \frac{n}{2}$, wobei letztere als $l = \frac{n}{2} + k$ dargestellt werden:

$$\begin{aligned} y_k &= p^{even}(\zeta_{k,n}^2) + \zeta_{k,n} \cdot p^{odd}(\zeta_{k,n}^2) \\ &= y_k^{even} + \zeta_{k,n} \cdot y_k^{odd} \\ y_{\frac{n}{2}+k} &= p^{even}(\zeta_{\frac{n}{2}+k,n}^2) + \zeta_{\frac{n}{2}+k,n} \cdot p^{odd}(\zeta_{\frac{n}{2}+k,n}^2) \\ &= y_k^{even} + \zeta_{\frac{n}{2}+k,n} \cdot y_k^{odd} \end{aligned}$$

Durch diesen Ansatz braucht man zur Reduktion auf die halbe Größe nur zwei rekursive Aufrufe und kann die Berechnung deshalb in $O(n \log n)$ Zeit ausführen.

Die inverse DFT kann man mit einem ähnlichen Ansatz beschleunigen, wenn man mit der folgenden Formel arbeitet (auf deren Beweis hier verzichtet wird):

$$a_k = \frac{1}{n} \sum_{j=0}^{n-1} y_j \cdot e^{\frac{2jk\pi}{n} i}$$