Satz 142 (Partialbruchzerlegung)

Seien $f, g \in K[x]$ *(*$K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$*) Polynome mit* $\mathrm{grad}(g) < \mathrm{grad}(f)$*, und es gelte*

$$f(x) = (x - \alpha_1)^{m_1} \cdot \ldots \cdot (x - \alpha_r)^{m_r}$$

mit $\mathbb{N} \ni m_i \geq 1$ *und paarweise verschiedenen* $\alpha_i \in K$ *(*$i = 1, \ldots, r$*). Dann gibt es eindeutig bestimmte Polynome* $g_1, \ldots, g_r \in K[x]$ *mit* $\mathrm{grad}(g_i) < m_i$*, so dass gilt:*

$$\frac{g}{f} = \frac{g_1}{(x - \alpha_1)^{m_1}} + \cdots + \frac{g_r}{(x - \alpha_r)^{m_r}}.$$

Beweis:

Induktion nach r. Für $r = 1$ ist nichts zu zeigen. Es gelte $r > 1$.
Sei $\tilde{f} = (x - \alpha_2)^{m_2} \cdot \ldots \cdot (x - \alpha_r)^{m_r}$. Dann gilt $f = (x - \alpha_1)^{m_1} \tilde{f}$.
Sei $d = \mathrm{grad}(f)$ und $\tilde{d} = \mathrm{grad}(\tilde{f})$. Es genügt nun, Folgendes zu zeigen:

Zwischenbehauptung: Es gibt eindeutig bestimmte Polynome $A, B \in K[x]$ mit $\mathrm{grad}(A) < m_1$, $\mathrm{grad}(B) < \tilde{d}$, so dass

$$\frac{g}{f} = \frac{A}{(x - \alpha_1)^{m_1}} + \frac{B}{\tilde{f}} \tag{1}$$

gilt.
(Wendet man auf $\frac{B}{\tilde{f}}$ die Induktionsbehauptung an, so folgt die Behauptung des Satzes.)

Gleichung (1) ist äquivalent zu

$$A\tilde{f} + B(x-\alpha_1)^{m_1} = g. \tag{2}$$

Wir machen den Ansatz: $A = \sum_{i=0}^{m_1-1} a_i x^i$, $B = \sum_{j=0}^{\tilde{d}-1} b_j x^j$.
Durch Koeffizientenvergleich mit (2) erhalten wir folgendes inhomogene lineare Gleichungssystem bestehend aus d Gleichungen in den Unbestimmten $a_{m_1-1}, \ldots, a_0, b_{\tilde{d}-1}, \ldots, b_0$:

$$M \cdot \begin{pmatrix} a_{m_1-1} \\ \vdots \\ a_0 \\ b_{\tilde{d}-1} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} c_{d-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ c_0 \end{pmatrix}, \tag{3}$$

wobei M eine $d \times d$-Matrix ist, und $g = \sum_{i=0}^{d-1} c_i x^i$. Wir haben die Zwischenbehauptung bewiesen, wenn wir zeigen können, dass die Matrix M invertierbar ($\det M \neq 0$) ist. Dazu benötigen wir das folgende Lemma.

Lemma 143

Seien $\tilde{A}, \tilde{B} \in K[x]$ *Polynome mit* $\operatorname{grad}(\tilde{A}) \geq 1$ *und* $\operatorname{grad}(\tilde{B}) \geq 1$. *Gibt es dann Polynome* $A, B \in K[x]$, $A \neq 0$ *oder* $B \neq 0$, *mit* $\operatorname{grad}(A) < \operatorname{grad}(\tilde{A})$, $\operatorname{grad}(B) < \operatorname{grad}(\tilde{B})$ *und*

$$A\tilde{B} + B\tilde{A} = 0,$$

so sind $\tilde{A}$ *und* $\tilde{B}$ *nicht teilerfremd.*

Beweis:

Dies folgt sofort aus der Eindeutigkeit der Primfaktorzerlegung. □

Beweis (Forts.):

Nun zurück zum Beweis von Satz 142. Angenommen $\det(M) = 0$. Dann würde es einen Vektor $y = (a_{m_1-1}, \ldots, a_0, b_{\tilde{d}-1}, \ldots, b_0)^t \neq 0$ mit $M \cdot y = 0$ geben, d.h. es würde Polynome $A = \sum_{i=0}^{m_1-1} a_i x^i$ und $B = \sum_{j=0}^{\tilde{d}-1} b_j x^j$, $A \neq 0$ oder $B \neq 0$, geben mit $\mathrm{grad}(A) < m_1$, $\mathrm{grad}(B) < \tilde{d} = \mathrm{grad}(\tilde{f})$ und $A\tilde{f} + B(x - \alpha_1)^{m_1} = 0$.

Nach Lemma 143 wären dann $\tilde{f}$ und $(x - \alpha_1)^{m_1}$ nicht teilerfremd. Dies ist jedoch ein Widerspruch zur Voraussetzung. Damit ist Satz 142 bewiesen. □

3.5 Schnelle Fouriertransformation (FFT, DFT)

3.5.1 Grundlagen

Ein Polynom $P = \sum_i a_i x^i \in \mathbb{C}[x]$ vom Grad $\leq n$ ist eindeutig durch seine Koeffizienten a_i bestimmt, d.h. man hat eine Bijektion

$$\begin{aligned} \{\text{Polynome} \in \mathbb{C}[x] \text{ vom Grad} \leq n\} &\rightarrow \mathbb{C}^{n+1} \\ P_{\vec{a}} = \sum_{i=0}^{n} a_i x^i &\mapsto \vec{a} = (a_0, \ldots, a_n). \end{aligned}$$

Problem: $P_{\vec{a}} \cdot P_{\vec{b}} = P_{\vec{c}}$ mit $\vec{c} = (c_0, \ldots, c_{2n})$, $c_k = \sum_i a_{k-i} b_i$, und die naive Berechnung von $\vec{c}$ benötigt $\Theta(n^2)$ Operationen.

Bemerkung: $\vec{c} = \vec{a} * \vec{b}$ mit $c_k = \sum_i a_{k-i} b_i$ ist die Faltung von $\vec{a}$ und $\vec{b}$.

Es gibt noch eine weitere eindeutige Darstellung eines Polynoms.

Lemma 144

Seien $P = \sum_{i=0}^{n} a_i x^i$ und $Q = \sum_{j=0}^{n} b_j x^j$ Polynome ($\in \mathbb{C}[x]$) vom Grad $\leq n$ und seien $\omega_0, \ldots, \omega_n \in \mathbb{C}$ paarweise verschiedene Elemente. Dann gilt:

$$P = Q \iff P(\omega_i) = Q(\omega_i) \quad \text{für alle } i = 0, \ldots, n.$$

Beweis:

„$\Rightarrow$“: Klar.

„$\Leftarrow$“: Es gelte $P(\omega_i) = Q(\omega_i)$ für $i = 0, \ldots, n$. Dann ist jedes ω_i eine Nullstelle des Polynoms $P - Q$. Da $\operatorname{grad}(P - Q) \leq n$ gilt, folgt $P - Q = 0$ aus Satz 139. □

Man kann leicht zeigen, dass es zu jedem Tupel $(b_0, \ldots, b_n) \in \mathbb{C}^{n+1}$ (genau) ein Polynom $f \in \mathbb{C}[x]$ vom Grad $\leq n$ gibt, mit $f(\omega_i) = b_i$ für $i = 0, \ldots, n$ (z.B. das Newtonsche Interpolationspolynom, benannt nach Sir Isaac Newton (1643–1727)).

Somit erhalten wir eine weitere Bijektion:

$$\begin{aligned} \{\text{Polynome} \in \mathbb{C}[x] \text{ vom Grad} \leq n\} &\to \mathbb{C}^{n+1} \\ P &\mapsto (P(\omega_0), \ldots, P(\omega_n)) \end{aligned}$$

Vorteil:

$$P \times Q \mapsto (P(\omega_0)Q(\omega_0), \ldots, P(\omega_n)Q(\omega_n)) = \\ (P(\omega_0), \ldots, P(\omega_n)) \cdot (Q(\omega_0), \ldots, Q(\omega_n)).$$

Multiplikation benötigt nur $O(n)$ Operationen. „$\cdot$“ auf der rechten Seite bezeichnet hier das komponentenweise (Hadamard) Vektorprodukt (Jacques S. Hadamard (1865–1963)).

Problem: Bijektion i.a. zu komplex.

Definition 145

Ein $\omega \in \mathbb{C}$ heißt primitive n-te Einheitswurzel, wenn $\omega^k \neq 1$ für alle $k = 1, \ldots, n-1$ und $\omega^n = 1$ gilt, d.h. $\mathrm{ord}(\omega) = n$ in $\mathbb{C}^* = \mathbb{C} \setminus 0$.

Bemerkung: Es ist $\omega = e^{2i\pi/n}$ eine primitive n-te Einheitswurzel.

Definition 146

Sei $\omega \in \mathbb{C}$ eine primitive n-te Einheitswurzel, $n \in \mathbb{N}$. Die Abbildung

$$\begin{aligned} \mathcal{F}_{n,\omega} : \quad & \mathbb{C}^n \to \mathbb{C}^n, \\ & \vec{a} = (a_0, \ldots, a_{n-1}) \mapsto (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1})) \end{aligned}$$

heißt diskrete Fouriertransformation; wir schreiben auch kurz $\mathcal{F}$ für $\mathcal{F}_{n,\omega}$.

Die Fouriertransformation ist nach Jean Baptiste Joseph Fourier (1768–1830) benannt.