Script **generated by TTT**

Title: Mayr: 2012 ds (27.11.2012)

Date: Tue Nov 27 13:44:54 CET 2012

Duration: 91:05 min

Pages: 32

WS 2012/13

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012WS/ds/

Wintersemester 2012

Division

Für diesen Abschnitt setzen wir voraus, dass der Koeffizientenring ein Körper ist.
Betrachte das Schema

$$2x^4 + x^3 + \quad x + 3 \ \text{div} \ x^2 + x - 1 \ =$$

Division

Für diesen Abschnitt setzen wir voraus, dass der Koeffizientenring ein Körper ist.
Betrachte das Schema

$$\begin{array}{l}
2x^4 + x^3 + \quad x + 3 \ \text{div} \ x^2 + x - 1 \ = \ 2x^2 - x + 3 \\
-\ (2x^4 + 2x^3 - 2x^2) \\
\qquad -x^3 + 2x^2 + x + 3 \\
\qquad -\ (-x^3 - x^2 + x) \\
\qquad\qquad 3x^2 + \quad 3 \\
\qquad\qquad -(3x^2 + 3x - 3) \\
\qquad\qquad\quad - 3x + 6
\end{array}$$

Satz 135

Zu je zwei Polynomen $a(x)$ und $b(x)$, $b \neq 0$, gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, so dass

$$a(x) = q(x)b(x) + r(x) \text{ und } r = 0 \text{ oder } \operatorname{grad}(r) < \operatorname{grad}(b).$$

Beispiel 136

Im vorhergehenden Schema war das

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)} \cdot \underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}$$

Beweis:

Gilt $\operatorname{grad}(a) < \operatorname{grad}(b)$, so kann man $q = 0$ und $r = a$ setzen. Sei also $\operatorname{grad}(a) \geq \operatorname{grad}(b)$.

Induktion über $\operatorname{grad}(a)$:

Ist $\operatorname{grad}(a) = 0$, so folgt aus $\operatorname{grad}(a) \geq \operatorname{grad}(b)$, dass a und b beides konstante Funtionen sind. Also $a(x) = a_0$ und $b(x) = b_0$ mit $b_0 \neq 0$. Wir können daher $q(x) = a_0/b_0$ und $r(x) = 0$ setzen.

Beweis (Forts.):

Ist $\operatorname{grad}(a) = n > 0$ und $\operatorname{grad}(b) = m$, $m \leq n$, und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m)x^{n-m} \cdot b(x)\ .$$

Dann gilt $\operatorname{grad}(\tilde{a}) < \operatorname{grad}(a)$.

Nach Induktionsannahme gibt es daher Polynome $\tilde{q}(x)$ und $\tilde{r}(x)$ mit $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$, mit $\tilde{r}(x) = 0$ oder $\operatorname{grad}(\tilde{r}) < \operatorname{grad}(b)$ (falls $m = n$, wird $\tilde{q}(x) = 0$ und $\tilde{r}(x) = \tilde{a}(x)$). Es gilt

$$a(x) \ = \ (a_n/b_m)x^{n-m}b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \ =: \ q(x)b(x) + r(x)\ .$$

Beweis (Forts.):

Ist $\operatorname{grad}(a) = n > 0$ und $\operatorname{grad}(b) = m$, $m \leq n$, und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m)x^{n-m} \cdot b(x)\ .$$

Dann gilt $\operatorname{grad}(\tilde{a}) < \operatorname{grad}(a)$.

Nach Induktionsannahme gibt es daher Polynome $\tilde{q}(x)$ und $\tilde{r}(x)$ mit $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$, mit $\tilde{r}(x) = 0$ oder $\operatorname{grad}(\tilde{r}) < \operatorname{grad}(b)$ (falls $m = n$, wird $\tilde{q}(x) = 0$ und $\tilde{r}(x) = \tilde{a}(x)$). Es gilt

$$a(x) \ = \ (a_n/b_m)x^{n-m}b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \ =: \ q(x)b(x) + r(x)\ .$$

Beweis (Forts.):

Um die Eindeutigkeit zu beweisen, nehmen wir an, es gäbe für Polynome a und b zwei Darstellungen wie im Satz angegeben. Also $q \cdot b + r = a = \hat{q} \cdot b + \hat{r}$ und somit auch

$$(q - \hat{q}) \cdot b = (\hat{r} - r).$$

Falls $q \neq \hat{q}$, ist die linke Seite ein Polynom vom Grad $\geq \text{grad}(b)$. Da die rechte Seite aus der Differenz zweier Polynome vom Grad kleiner als $\text{grad}(b)$ besteht, Widerspruch! Also ist $q = \hat{q}$ und damit auch $r = \hat{r}$. □

Beobachtung:
Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 135 wie im Beispiel bestimmen. Da sich der Grad des Polynoms in jeder Zeile verringert, benötigen wir also höchstens n Multiplikationen von Polynomen mit Konstanten und n Subtraktionen von Polynomen vom Grad höchstens n.

Insgesamt ergibt sich:

Die Division zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Beobachtung:
Falls der führende Koeffizient des Divisorpolynoms gleich 1 ist, lässt sich die Division auch über einem Ring R durchführen.

Beobachtung:
Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 135 wie im Beispiel bestimmen. Da sich der Grad des Polynoms in jeder Zeile verringert, benötigen wir also höchstens n Multiplikationen von Polynomen mit Konstanten und n Subtraktionen von Polynomen vom Grad höchstens n.

Insgesamt ergibt sich:

Die Division zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Beobachtung:
Falls der führende Koeffizient des Divisorpolynoms gleich 1 ist, lässt sich die Division auch über einem Ring R durchführen.

3.3 Nullstellen von Polynomen

Definition 137
Eine Nullstelle eines Polynoms p ist ein Wert x_0 mit $p(x_0) = 0$.

Lemma 138
Sei $p \in R[x]$, $x_0 \in R$ eine Nullstelle von p. Dann ist $p(x)$ ohne Rest durch $x - x_0$ teilbar.

Beweis:
Nach Satz 135 gibt es Polynome q und r mit $p(x) = q(x) \cdot (x - x_0) + r(x)$ und $\text{grad}(r) < \text{grad}(x - x_0) = 1$, also $\text{grad}(r) = 0$, d.h. $r(x) = r_0$. Wegen $p(x_0) = q(x_0) \cdot (x_0 - x_0) + r_0 = r_0$ muss also r_0 gleich Null sein. D.h., $p(x) = q(x) \cdot (x - x_0)$. □

Satz 139 (Fundamentalsatz der Algebra)

Jedes Polynom $p \neq 0$ mit Grad n hat höchstens n Nullstellen.

Beweis:
Wir zeigen den Satz durch Induktion über den Grad des Polynoms. Ist p ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme $p \neq 0$ offenbar richtig.

Satz 139 (Fundamentalsatz der Algebra)

Jedes Polynom $p \neq 0$ mit Grad n hat höchstens n Nullstellen.

Beweis:
Wir zeigen den Satz durch Induktion über den Grad des Polynoms. Ist p ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme $p \neq 0$ offenbar richtig.
Ist p ein Polynom mit Grad $n > 0$, so hat p entweder keine Nullstelle (und die Aussage ist somit trivialerweise richtig) oder p hat mindestens eine Nullstelle a. Dann gibt es nach Lemma 138 eine Darstellung $p(x) = q(x) \cdot (x - a)$ mit $\mathrm{grad}(q) = n - 1$. Nach Induktionsannahme hat q höchstens $n - 1$ und somit p höchstens n Nullstellen. □

Satz 139 (Fundamentalsatz der Algebra)

Jedes Polynom $p \neq 0$ mit Grad n hat höchstens n Nullstellen.

Beweis:
Wir zeigen den Satz durch Induktion über den Grad des Polynoms. Ist p ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme $p \neq 0$ offenbar richtig.
Ist p ein Polynom mit Grad $n > 0$, so hat p entweder keine Nullstelle (und die Aussage ist somit trivialerweise richtig) oder p hat mindestens eine Nullstelle a. Dann gibt es nach Lemma 138 eine Darstellung $p(x) = q(x) \cdot (x - a)$ mit $\mathrm{grad}(q) = n - 1$. Nach Induktionsannahme hat q höchstens $n - 1$ und somit p höchstens n Nullstellen. □

Beispiele 140

- Das Polynom $x^2 - 1 = (x + 1)(x - 1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

Beispiele 140

- Das Polynom $x^2 - 1 = (x+1)(x-1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

3.4 Partialbruchzerlegung

Beispiel 141

Finde zu $\frac{g}{f} = \frac{x^2+1}{(x-1)^2(x-2)}$ Polynome p, q mit $\text{grad}(p) < 2$, $\text{grad}(q) < 1$ und

$$\frac{x^2+1}{(x-1)^2(x-2)} = \frac{p}{(x-1)^2} + \frac{q}{x-2}. \qquad (*)$$

Die r.S. von (*) heißt Partialbruchzerlegung von $\frac{g}{f}$.

Ansatz: $p(x) = ax + b$, $q(x) = c$.

$$\frac{p}{(x-1)^2} + \frac{q}{x-2} = \frac{(x-2)\cdot p + (x-1)^2 \cdot q}{(x-1)^2(x-2)}.$$

Durch Vergleich mit (*) erhält man

$$\begin{aligned} x^2+1 &= (ax+b)(x-2) + c(x-1)^2 \\ &= (a+c)x^2 + (b-2a-2c)x + c - 2b. \end{aligned}$$

Koeffizientenvergleich liefert folgendes lineares Gleichungssystem:

$$\begin{aligned} a + c &= 1 \\ b - 2a - 2c &= 0 \\ c - 2b &= 1 \end{aligned}$$

Dieses hat die eindeutige Lösung $a = -4$, $b = 2$, $c = 5$. Somit gilt:

$$\frac{x^2+1}{(x-1)^2(x-2)} = \frac{-4x+2}{(x-1)^2} + \frac{5}{x-2}.$$

Satz 142 (Partialbruchzerlegung)

Seien $f, g \in K[x]$ ($K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$) Polynome mit $\text{grad}(g) < \text{grad}(f)$, 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 $\text{grad}(g_i) < m_i$, 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 $d = \operatorname{grad}(f)$ und $\tilde{d} = \operatorname{grad}(\tilde{f})$. Es genügt nun, Folgendes zu zeigen:
Zwischenbehauptung: Es gibt eindeutig bestimmte Polynome $A, B \in K[x]$ mit $\operatorname{grad}(A) < m_1$, $\operatorname{grad}(B) < \tilde{d}$, 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.)

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 $d = \operatorname{grad}(f)$ und $\tilde{d} = \operatorname{grad}(\tilde{f})$. Es genügt nun, Folgendes zu zeigen:
Zwischenbehauptung: Es gibt eindeutig bestimmte Polynome $A, B \in K[x]$ mit $\operatorname{grad}(A) < m_1$, $\operatorname{grad}(B) < \tilde{d}$, 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 $a_{m_1-1}, \ldots, a_0, b_{\tilde{d}-1}, \ldots, b_0$:

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

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 $\text{grad}(A) < m_1$, $\text{grad}(B) < \tilde{d} = \text{grad}(\tilde{f})$ 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:

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

Beweis:

„⇒“: Klar.

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:

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

Beweis:

„⇒“: Klar.

„⇐“: 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 $\text{grad}(P - Q) \leq n$ 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)).

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. $\text{ord}(\omega) = n$ 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.

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. $\text{ord}(\omega) = n$ 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.

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.