

Vorlesungsskript  
Effiziente numerische Algorithmen

Frank Natterer  
*Institut für Numerische  
und instrumentelle Mathematik*

WS 1994/95, Di/Fr 11-13, M 5

This page intentionally left blank.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Schnelle Multiplikation von Zahlen . . . . .	3
1.2	Multiplikation und Inversion von Matrizen . . . . .	7
<b>2</b>	<b>Algebra</b>	<b>11</b>
2.1	Darstellung endlicher Gruppen . . . . .	11
2.2	Charaktere endlicher Gruppen . . . . .	21
2.3	Der Chinesische Restsatz . . . . .	31
2.4	Gruppentheorie . . . . .	36
<b>3</b>	<b>Schnelle Fourier-Transformation</b>	<b>41</b>
3.1	Fourier-Transformation und Faltung . . . . .	41
3.2	Cooley-Tukey . . . . .	43
3.3	Primfaktoren . . . . .	50
3.4	Schnelle Faltung nach Winograd . . . . .	56
3.5	Die schnelle Fourier-Transformation nach Winograd . . .	64
3.6	Schnelle Poisson-Löser . . . . .	69

<b>4</b>	<b>Symmetrie</b>	<b>73</b>
4.1	Matrizen mit Symmetrien . . . . .	73
4.2	Untergruppen . . . . .	88
4.3	Direkte Produkte . . . . .	91
4.4	Die Fourier-Transformation auf Gruppen . . . . .	95
<b>5</b>	<b>Toeplitz-Matrizen</b>	<b>101</b>
5.1	Der Algorithmus von Trench . . . . .	101
5.2	Der Algorithmus von Morf . . . . .	106

# Kapitel 1

## Einleitung

Wir geben einige Beispiele für effiziente Algorithmen, die wir zum Teil später wieder aufgreifen und vertiefen werden. Zunächst geht es nur darum, einen ersten Einblick in die behandelten Probleme und verwendeten Methoden zu geben.

### 1.1 Schnelle Multiplikation von Zahlen

Seien  $x, y$  Zahlen in endlich  $b$ -adischer Darstellung,  $b > 1$ , also

$$\begin{aligned}x &= x_0 + x_1b + \dots + x_{n-1}b^{n-1} \quad , \quad 0 \leq x_i < b \quad , \\y &= y_0 + y_1b + \dots + y_{n-1}b^{n-1} \quad , \quad 0 \leq y_i < b\end{aligned}$$

mit ganzen Zahlen  $x_i, y_i$ . Gesucht ist das Produkt  $z = xy$ . Die Schulmethode soll an Hand eines Beispiels mit  $b = 10$  und  $n = 3$  erläutert werden:

$$\begin{array}{r}214 \cdot 713 \\ \hline 642 \\ 214 \\ 1498 \\ \hline 152582\end{array}$$

Offenbar benötigt die Schulmethode für eine Multiplikation der Länge  $n$   $O(n^2)$  Rechenoperationen. Addiert man, sobald in einer Spalte alle Produkte berechnet sind, so kommt man mit  $O(n)$  Speicherplätzen aus.

Der Schulmethode stellen wir als effizienten Algorithmus die Karatsuba-Multiplikation gegenüber. Sei  $n$  gerade und  $n = 2m$ . Wir teilen  $x$  auf in

$$\xi_0 = x_0 + x_1b + \dots + x_{m-1}b^{m-1}, \quad \xi_1 = x_m + x_{m+1}b + \dots + x_{n-1}b^{m-1}$$

und entsprechend  $y = \eta_0 + b^m\eta_1$ . Dann ist

$$\begin{aligned} xy &= \xi_0\eta_0 + (\xi_0\eta_1 + \xi_1\eta_0)b^m + \xi_1\eta_1b^n \\ &= (1 + b^m)\xi_0\eta - b^m(\xi_1 - \xi_0)(\eta_1 - \eta_0) + (b^m + b^n)\xi_1\eta_1. \end{aligned}$$

Wir können also eine Multiplikation der Länge  $n$  realisieren durch 3 Multiplikationen der Länge  $n/2$  sowie  $O(n)$  zusätzliche Rechenoperationen. Ist also  $T(n)$  die Anzahl der Rechenoperationen, die wir für eine Multiplikation der Länge  $n$  benötigen, so gilt

$$T(n) \leq 3T\left(\frac{n}{2}\right) + cn, \quad T(1) = 1$$

mit einer von  $n$  unabhängigen Konstanten  $c$ . Ist nun  $n$  eine Zweierpotenz, also  $n = 2^p$ , so ist mit  $T_p = T(2^p)$

$$T_p \leq 3T_{p-1} + c2^p, \quad T_0 = 1. \quad (1.1.1)$$

**Lemma 1.1.1** *Seien  $T_p, q, r_p \geq 0$ , und sei*

$$T_{p+1} \leq qT_p + r_p, \quad p = 0, 1, \dots$$

*Dann ist*

$$T_p \leq q^p T_0 + \sum_{j=0}^{p-1} q^{p-1-j} r_j.$$

Der Beweis durch vollständige Induktion ist trivial.

**Satz 1.1.2** Für  $n = 2^p$  kann die Multiplikation der Länge  $n$  in  $O(n^{\log_2 3})$  Rechenoperationen durchgeführt werden.

**Beweis:** Wenden wir Lemma 1.1.1 auf (1.1.1) an, so entsteht

$$\begin{aligned}
 T_p &\leq 3^p + c \sum_{j=0}^{p-1} 3^{p-1-j} 2^{j+1} \\
 &= 3^p + c 3^p \sum_{j=0}^{p-1} \left(\frac{2}{3}\right)^{j+1} \\
 &\leq 3^p + c 3^p \frac{2}{3} \frac{1}{1-2/3} = (1+2c)3^p \\
 &= (1+2c)n^{\log_2 3}.
 \end{aligned}$$

□

Wegen  $\log_2 3 = 1.585 < 2$  ist dies eine Verbesserung gegenüber der  $O(n^2)$ -Abschätzung für die Schulmethode, jedenfalls für große  $n$ . Das Karatsuba-Verfahren kann leicht durch ein rekursives Programm realisiert werden:

```

fmult (n, x, y, z)
{
  if (n == 1) Schulmethode;
  else
  {
    m = n/2;
    ξ₀ = (x₀, ..., x_{m-1}); ξ₁ = (x_n, ..., x_{n-1});
    η₀ = (y₀, ..., y_{m-1}); η₁ = (y_m, ..., y_{n-1});
    fmult (m, ξ₀, η₀, α);
    fmult (m, ξ₁ - ξ₀, η₁ - η₀, β);
    fmult (m, ξ₁, η₁, γ) for (i = 0; i < n; i++) z_i = 0;
    for (i = 0; i < n; i++)
    {
      z_i = α_i + z_i;
      z_{i+m} = α_i - β_i + γ_i + z_{i+m};
      z_{i+n} = γ_i + z_{i+n};
    }
  }
}

```

Der Karatsuba-Algorithmus ist ein typisches Beispiel für die oft verwendete “Divide-and-Conquer-Strategie”: Ein Problem wird in kleinere Teilprobleme zerlegt. Diese werden gelöst und aus den Lösungen die Lösung des ursprünglichen Problems zusammengesetzt. Dieser Prozeß wird in rekursiver Weise wiederholt.

## 1.2 Schnelle Multiplikation und Inversion von Matrizen

Zur Multiplikation zweier  $(n, n)$ -Matrizen  $A, B$  nach der Schulmethode benötigt man bekanntlich  $O(n^3)$  Rechenoperationen. Das gleiche gilt für die Inversion einer  $(n, n)$ -Matrix. Wir wollen den Straßen-Algorithmus vorstellen, der beide Aufgaben in  $O(n^{\log_2 7})$ ,  $\log_2 7 = \ln 7 / \ln 2 = 2.807$ , Rechenoperationen erledigt.

Für eine  $(n, n)$ -Matrix  $A$  mit geradem  $n$  schreiben wir

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

mit  $(\frac{n}{2}, \frac{n}{2})$ -Matrizen  $A_{ij}$ .

**Lemma 1.2.1** *Sei  $C = AB$  mit  $(n, n)$ -Matrizen  $A, B, C$ . Dann gilt*

$$\begin{aligned} C_{11} &= I + IV - V + VII & , & & C_{12} &= III + V & , \\ C_{21} &= II + IV & , & & C_{22} &= I + III - II + VI \end{aligned}$$

mit

$$\begin{aligned} I &= (A_{11} + A_{22})(B_{11} + B_{22}) \\ II &= (A_{21} + A_{22})B_{11} \\ III &= A_{11}(B_{12} - B_{22}) \\ IV &= A_{22}(B_{21} - B_{11}) \\ V &= (A_{11} + A_{12})B_{22} \\ VI &= (A_{21} - A_{11})(B_{11} + B_{12}) \\ VII &= (A_{12} - A_{22})(B_{21} + B_{22}) \end{aligned}$$

**Beweis:** Der Beweis durch einfaches Nachrechnen ist trivial.

Wer Schwierigkeiten hat, sei auf V. Straßen: *Gaussian Elimination ist not optimal*, Numer. Math. **13**, 354-356 (1969), verwiesen.

□

**Satz 1.2.2** Sei  $n = 2^p$ . Dann kann man zwei  $(n, n)$ -Matrizen in  $O(n^{\log_2 7})$  Rechenoperationen multiplizieren.

**Beweis:** Inspektion der Formel von Lemma 1.2.1 zeigt, daß man die Multiplikation zweier  $(n, n)$ -Matrizen durch 7 Multiplikationen und 18 Additionen von  $(\frac{n}{2}, \frac{n}{2})$ -Matrizen ausführen kann. Ist also  $n = m \cdot 2^p$  und  $M_p$  bzw.  $A_p$  die Anzahl der reellen Multiplikation bzw. Additionen, welche man zur Multiplikation zweier  $(n, n)$ -Matrizen benötigt, so gilt nach Lemma 1.2.1

$$\begin{aligned} M_{p+1} &\leq 7M_p & , & \quad M_0 \leq m^3 , \\ A_{p+1} &\leq 7A_p + 18(m \cdot 2^p)^2 & , & \quad A_0 \leq m^3 . \end{aligned}$$

Nach Lemma 1.1.1 erhält man

$$\begin{aligned} M_p &\leq 7^p m^3 \\ A_p &\leq 7^p m^3 + 18m^2 \sum_{j=0}^{p-1} 7^{p-1-j} 2^{2j} \\ &= 7^p m^3 + 18m^2 7^{p-1} \sum_{j=0}^{p-1} \left(\frac{4}{7}\right)^j \\ &\leq 7^p (m^3 + 6m^2) \end{aligned}$$

Für  $m = 1$  folgt wegen  $7^p = n^{\log_2 7}$  die Behauptung.

□

Für  $n = m2^p$  lautet der Straßen-Algorithmus

```

fmamu      (n, A, B, C)
{
  if      (n ≤ m) Schulmethode;
  else
  {
    fmamu (n/2, A11 + A22, B11 + B22, I);
    ⋮
    fmamu (n/2, A12 - A22, B21 + B22, VII);
    C11 = I + IV - V + VII;   C12 = III + V;
    C21 = II + IV;           C22 = I + VI - II + VI;
  }
}

```

Nun zur Matrizeninversion. Anstelle von Lemma 1.2.1 haben wir jetzt

**Lemma 1.2.3** *Sei  $A$  eine invertierbare  $(n, n)$ -Matrix mit geradem  $n$ , und seien die Matrizen  $A_{11}$  und  $A_{21}A_{11}^{-1}A_{12} - A_{22}$  invertierbar. Dann gilt mit*

$$\begin{aligned} I &= A_{11}^{-1} & , & \quad II = A_{21}I & \quad , & \quad III = IA_{12} \\ IV &= A_{21}III & , & \quad V = IV - A_{22} & \quad , & \quad VI = V^{-1} \end{aligned}$$

für  $C = A_{-1}$ :

$$\begin{aligned} C_{12} &= III VI & , & \quad C_{12} = VI II & \quad , & \quad VII = III C_{21} , \\ C_{11} &= I - VII & , & \quad C_{22} = -VI & \quad . \end{aligned}$$

**Beweis:** Durch triviales Nachrechnen.

□

**Satz 1.2.4** *Sei  $n = 2^p$  und  $A$  eine invertierbare  $(n, n)$ -Matrix. Unter der Voraussetzung  $V$  (siehe unten) kann  $A$  mit  $O(n^{\log 7 / \log 2})$  Rechenoperationen invertiert werden.*

**Beweis:** Durch Inspektion der Formeln von Lemma 1.2.3 sehen wir, daß eine  $(n, n)$ -Matrix durch 2 Inversionen, 6 Multiplikationen, und 2 Additionen von  $(\frac{n}{2}, \frac{n}{2})$ -Matrizen invertiert werden kann. Setzen wir wieder  $n = m2^p$  und bezeichnen wir mit  $\delta_p, \mu_p, \alpha_p$  die Anzahl der reellen Divisionen, Multiplikationen und Additionen für die Inversion einer  $(n, n)$ -Matrix, so gilt also

$$\begin{aligned} \delta_{p+1} &\leq 2\delta_p & , & \quad \delta_0 \leq m & , \\ \mu_{p+1} &\leq 2\mu_p + 6M_p & , & \quad \mu_0 \leq m^3 & , \\ \alpha_{p+1} &\leq 2\alpha_p + 6A_p + 2(m2^p)^2 & , & \quad \alpha_0 \leq m^3 & . \end{aligned}$$

Die Ungleichungen für  $p = 0$  gelten, falls man für  $p = 0$  das Eliminationsverfahren verwendet. Auf diese Rekursionen wenden wir wieder Lemma 1.1.1 an und erhalten

$$\begin{aligned}
\delta_p &\leq m^3, \\
\mu_p &\leq 2^p m^3 + 6 \sum_{j=0}^{p-1} M_j 2^{p-j-1} \\
&\leq 2^p m^3 + 6m^3 \sum_{j=0}^{p-1} 7^j 2^{p-j-1} \\
&= 2^p m^3 \left( 1 + 3 \sum_{j=0}^{p-1} \left(\frac{7}{2}\right)^j \right) \\
&= 2^p m^3 \left( 1 + 3 \frac{(7/2)^p - 1}{\frac{7}{2} - 1} \right) \\
&\leq 7^p m^3 \cdot \frac{6}{5}, \\
\alpha_p &\leq \left( \frac{6}{5} m^3 + 5m^2 \right) 7^p.
\end{aligned}$$

Für  $m = 1$  erhält man die Behauptung.

Natürlich können nur solche Matrizen auf diese Weise invertiert werden, für die bei allen Unterteilungen  $n \rightarrow \frac{n}{2} \rightarrow \frac{n}{4} \dots \rightarrow m$  die Voraussetzungen von Lemma 1.2.3 erfüllt sind. Dies ist Inhalt der Voraussetzung V.

□

# Kapitel 2

## Algebra

### 2.1 Darstellung endlicher Gruppen

Wir setzen eine gewisse Vertrautheit mit der elementaren Gruppentheorie voraus. Sei  $G$  eine endliche Gruppe. Wir schreiben alle Gruppen multiplikativ.  $1$  ist das Einselement,  $|G|$  die Ordnung, d.h. die Anzahl der Elemente, von  $G$ .

#### Beispiele:

- 1) Die zyklische Gruppe  $C_n$  der Ordnung  $n$ . Sie wird erzeugt von einem Element  $q$  mit  $q^n = 1$ , so daß also  $C_n = \{1, q, \dots, q^{n-1}\}$ .  $C_n$  ist abelsch.
- 2) Die Gruppe  $S_n$  der Permutationen von  $n$  Elementen. Sie hat die Ordnung  $n!$  und ist nicht abelsch.  $S_n$  heißt die symmetrische Gruppe. Eine Permutation kann gerade oder ungerade sein. Die Untergruppe  $A_n$  der geraden Permutationen heißt alternierende Gruppe.
- 3) Die Diedergruppe  $D_n$ . Sie wird erzeugt von Rotationen  $r$  um den Winkel  $2\pi/n$  und durch eine Spiegelung  $s$  an einer Geraden. Sie besteht also aus den Elementen  $1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$  und hat also die Ordnung  $2n$ . Es ist  $r^n = 1, s^2 = 1$ .  $D_n$  ist nur für  $n = 1, 2$  abelsch.

**Definition 2.1.1** Sei  $G$  eine endliche Gruppe und  $V$  ein  $d$ -dimensionaler Vektorraum über  $\mathbb{C}$ .  $GL(V)$  sei die Gruppe der linearen invertierbaren Abbildungen  $V \rightarrow V$ .

Ein Homomorphismus  $\rho : G \rightarrow GL(V)$  heißt Darstellung von  $G$  in  $V$ . Ist  $\rho$  injektiv, so heißt die Darstellung treu.  $d$  heißt der Grad von  $\rho$ . Zwei Darstellungen  $\rho, \rho'$  von  $G$  in  $V$  bzw.  $V'$  heißen äquivalent, wenn es eine lineare invertierbare Abbildung  $\tau : V \rightarrow V'$  gibt, so daß  $\rho' = \tau\rho\tau^{-1}$ .

**Beispiele:**

- 1)  $\rho(s) = 1$  für alle  $s$  heißt Einheitsdarstellung.
- 2) Die reguläre Darstellung  $\rho_{\text{reg}}$  wird wie folgt definiert. Sei  $\{e_t : t \in G\}$  eine Basis von  $V$ . Dann setzt man

$$\rho_{\text{reg}}(s)e_t = e_{st}$$

(linksreguläre Darstellung). Es ist also

$$\begin{aligned} \rho_{\text{reg}}(s) \sum_{t \in G} x_t e_t &= \sum_{t \in G} x_t \rho_{\text{reg}}(s)e_t \\ &= \sum_{t \in G} x_t e_{st} \\ &= \sum_{t \in G} x_{s^{-1}t} e_t . \end{aligned}$$

$\rho_{\text{reg}}$  übt also auf die Komponenten  $x_t$  die Permutation  $t \rightarrow s^{-1}t$  aus. Der Grad von  $\rho_{\text{reg}}$  ist  $|G|$ .  $\rho_{\text{reg}}$  ist treu.

- 3) Sei  $G = C_n = \{1, q, \dots, q^{n-1}\}$  und  $\omega$  eine  $n$ -te Einheitswurzel, also  $\omega^n = 1$ . Dann ist

$$\rho(q^k) = \omega^k \quad , \quad k = 0, 1, \dots, n-1$$

eine Darstellung von  $C_n$  in  $\mathbb{C}$ , der Grad also 1.  $\rho$  ist genau dann treu, wenn  $\omega$  eine primitive  $n$ -te Einheitswurzel ist, d.h. wenn  $\omega^m \neq 1$  für  $0 < m < n$ . Sind  $\omega_1, \omega_2$  verschiedene  $n$ -te Einheitswurzeln, so sind die zugehörigen Darstellungen nicht äquivalent.

Wir berechnen die reguläre Darstellung von  $C_n$ . Mit  $e_k = e_{q^k}$ ,  $x_k = x_{q^k}$  haben wir

$$\rho_{\text{reg}}(s^\ell) \sum_{k=0}^{n-1} x_k e_k = \sum_{k=0}^{n-1} x_{k-\ell} e_k, \quad \ell = 0, \dots, n-1,$$

wobei  $k - \ell$  modulo  $n$  genommen wird.

4) Sei  $G = S_n$ . Die alternierende Darstellung

$$\rho_{\text{alt}}(\pi) = \begin{cases} 1 & , \pi \text{ gerade} , \\ -1 & , \pi \text{ ungerade} \end{cases}$$

ist vom Grad 1 und für  $n > 2$  nicht treu. Die natürliche Darstellung von  $S_n$  ist wie folgt definiert. Seien  $e_1, \dots, e_n$  die Einheitsvektoren in  $\mathbb{C}$  und  $v = \sum_{i=1}^n x_i e_i$ . Dann ist

$$\rho_{\text{nat}}(\pi)v = \sum_{i=1}^n x_i e_{\pi(i)}.$$

Der Grad von  $\rho_{\text{nat}}$  ist  $n$ , und  $\rho_{\text{nat}}$  ist treu.

5) Sei  $G = D_n$  und  $n$  gerade. Für  $D_n$  haben wir 5 verschiedene Typen von Darstellungen

	$\rho(r^k)$	$\rho(sr^k)$	Grad( $\rho$ )	Bemerkungen
$\rho_1$	1	1	1	Einheitsdarstellung
$\rho_2$	1	-1	1	
$\rho_3$	$(-1)^k$	$(-1)^k$	1	
$\rho_4$	$(-1)^k$	$(-1)^{k+1}$	1	
$\rho_5^h$	$\begin{pmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{pmatrix}$	$\begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix}$	2	$\omega = e^{2\pi i/n}$ , $h = 1, \dots, \frac{n}{2} - 1$ .

Die Beschränkung auf  $h < \frac{n}{2}$  ist sinnvoll, weil  $\rho_5^h, \rho_5^{n-h}$  äquivalent sind. Wegen  $\omega_n = 1$  ist nämlich

$$\begin{aligned}
\rho_5^{n-h}(r^k) &= \begin{pmatrix} \omega^{(n-h)k} & 0 \\ 0 & \omega^{-(n-h)k} \end{pmatrix} = \begin{pmatrix} \omega^{-hk} & 0 \\ 0 & \omega^{hk} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \tau \rho_5^h(r^k) \tau^{-1}, \\
\rho_5^{n-h}(sr^k) &= \begin{pmatrix} 0 & \omega^{(n-h)k} \\ \omega^{-(n-h)k} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega^{hk} \\ \omega^{-hk} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \tau \rho_5^h(sr^k) \tau^{-1}
\end{aligned}$$

für alle  $k$  mit der nichtsingulären Matrix  $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

**Definition 2.1.2** Eine Darstellung  $\rho$  von  $G$  in  $V$  heißt *reduzibel*, wenn es einen echten Unterraum  $V_1$  von  $V$  gibt mit  $\rho(s)V_1 \subseteq V_1$  für alle  $s \in G$ .  $V_1$  heißt dann *invarianter Unterraum* von  $\rho$ .

Ist  $\rho$  nicht reduzibel, so nennt man  $\rho$  *irreduzibel*.

### Beispiele:

- 1) Die Einheitsdarstellung ist für  $d > 1$  reduzibel. Darstellungen vom Grad 1 sind stets irreduzibel.
- 2)  $\rho_{\text{reg}}$  ist für  $|G| > 1$  reduzibel, denn  $(1, \dots, 1)$  spannt einen echten invarianten Unterraum auf.

**Satz 2.1.3** Sei  $V = V_1 \oplus \dots \oplus V_r$ , und seien  $\rho_i$  Darstellungen von  $G$  in  $V_i$ . Dann ist

$$\rho(s)v = \sum_{i=1}^r \rho_i(s)v_i \quad \text{für} \quad v = \sum_{i=1}^r v_i, \quad v_i \in V_i$$

eine Darstellung von  $G$  in  $V$  mit den invarianten Unterräumen  $V_i$ .

**Beweis:** Natürlich ist  $\rho : G \rightarrow GL(V)$  ein Homomorphismus. Ist  $v \in V_i$ , so ist auch  $\rho(s)v \in V_i$ .

□

**Definition 2.1.4** Die Darstellung  $\rho$  aus Satz 2.1.3 heißt direkte Summe von  $\rho_1, \dots, \rho_r$ . Man schreibt  $\rho = \rho_1 + \dots + \rho_r$ .

Wir wollen nun Darstellungen durch Matrizen beschreiben. Sei  $v_1, \dots, v_d$  eine Basis von  $V$ .  $\rho(s)$  wird dann beschrieben durch eine  $(d, d)$ -Matrix  $R(s)$ , d.h.

$$\rho(s)v = \sum_{i=1}^d y_i v_i \quad \text{für} \quad v = \sum_{i=1}^d x_i v_i$$

mit  $y = R(s)x$ . Natürlich gilt  $R(st) = R(s)R(t)$ .  $R$  ist nichts anderes als eine Darstellung von  $G$  in  $\mathbb{C}^d$ .

Sei nun  $V_1$  invarianter Unterraum von  $\rho$  der Dimension  $m$  mit Basis  $v_1, \dots, v_m$ . Dann hat  $R$  die Gestalt

$$R(s) = \begin{pmatrix} R_{11}(s) & R_{12}(s) \\ \text{O} & R_{22}(s) \end{pmatrix}$$

mit einer  $(m, m)$ -Matrix  $R_{11}(s)$  und einer  $(d-m, d-m)$ -Matrix  $R_{22}(s)$ . Ist  $R_{12} = 0$ , so ist  $\rho = \rho_1 + \rho_2$  mit den durch  $R_{11}, R_{22}$  beschriebenen Darstellungen  $\rho_1, \rho_2$ . Sind allgemeiner  $\rho_1, \dots, \rho_r$  Darstellungen von  $G$  in  $V_1, \dots, V_r$ , welche von den Matrizen  $R_1, \dots, R_r$  beschrieben werden, so wird  $\rho = \rho_1 + \dots + \rho_r$  durch die Matrix

$$R = \begin{pmatrix} R_1 & & \text{O} \\ & \ddots & \\ \text{O} & & R_r \end{pmatrix}$$

beschrieben.

**Satz 2.1.5** Sei  $\rho$  eine Darstellung von  $G$  in  $V$ . Dann gibt es ein Skalarprodukt in  $V$ , bezüglich dem  $\rho$  unitär ist.

**Beweis:** Sei  $(\cdot, \cdot)$  irgendein Skalarprodukt in  $V$ , und sei

$$\langle u, v \rangle = \frac{1}{|G|} \sum_{s \in G} (\rho(s)u, \rho(s)v) .$$

Dann ist auch  $\langle \cdot, \cdot \rangle$  ein Skalarprodukt in  $V$ , und es gilt

$$\begin{aligned} \langle \rho(t)u, \rho(t)v \rangle &= \frac{1}{|G|} \sum_{s \in G} \langle \rho(s)\rho(t)u, \rho(s)\rho(t)v \rangle \\ &= \frac{1}{|G|} \sum_{s \in G} \langle \rho(st)u, \rho(st)v \rangle \\ &= \frac{1}{|G|} \sum_{s \in G} \langle \rho(s)u, \rho(s)v \rangle \\ &= \langle u, v \rangle . \end{aligned}$$

Also ist  $\rho$  bezüglich  $\langle \cdot, \cdot \rangle$  unitär.

□

**Satz 2.1.6** *Jede Darstellung einer Gruppe ist eine direkte Summe irreduzibler Darstellungen dieser Gruppe.*

**Beweis:** Sei  $\rho$  eine Darstellung von  $G$  in  $V$ . Ohne Beschränkung der Allgemeinheit können wir annehmen, daß  $\rho$  bezüglich eines Skalarprodukts  $\langle \cdot, \cdot \rangle$  in  $V$  unitär ist. Ist  $\rho$  irreduzibel, sind wir fertig. Andernfalls besitzt  $\rho$  einen invarianten Unterraum  $V_1 \neq \{0\}, \neq V$ . Sei  $V_2$  das orthogonale Komplement von  $V_1$  in  $V$  bezüglich des Skalarprodukts  $\langle \cdot, \cdot \rangle$ . Wir zeigen, daß auch  $V_2$  invarianter Unterraum von  $\rho$  ist. Sei dazu  $v \in V_2$ . Für jedes  $u \in V_1$  ist

$$\begin{aligned} \langle \rho(s)v, u \rangle &= \langle \rho(s)v, \rho(s)\rho(s^{-1})u \rangle = \langle v, \rho(s^{-1})u \rangle \\ &= 0 , \end{aligned}$$

denn mit  $u$  ist auch  $\rho(s^{-1})u \in V_1$ . Also ist  $\rho(s)v \in V_2$ . Es sind also  $V_1, V_2$  invariante Unterräume von  $\rho$ , und es ist  $V = V_1 \oplus V_2$ . Die Restriktionen

$\rho_1, \rho_2$  von  $\rho$  auf  $V_1, V_2$  sind Darstellungen von  $\rho$  in  $V_1, V_2$ , und es gilt  $\rho = \rho_1 + \rho$ .  $\rho_1, \rho_2$  haben kleineren Grad als  $\rho$ .

Sind  $\rho_1, \rho_2$  irreduzibel, so sind wir fertig. Andernfalls zerfallen  $\rho_1, \rho_2$  ihrerseits in Darstellungen noch kleineren Grades. Durch Fortführen dieses Prozesses kommt man nach endlich vielen Schritten bei irreduziblen Darstellungen an.

□

**Definition 2.1.7** Das Zerlegen einer Darstellung in irreduzible Darstellungen nach Satz 2.1.6 nennt man Ausreduzieren der Darstellung.

### Beispiel:

Ausreduzieren der regulären Darstellung  $\rho_{\text{reg}}$  von  $C_n$ . Bezüglich der Basis  $e_0, \dots, e_{n-1}$  in  $V = \mathbb{C}^n$  gilt

$$\rho_{\text{reg}}(s^\ell) \sum_{k=0}^{n-1} x_k e_k = \sum_{k=0}^{n-1} x_{k-\ell} e_k, \quad \ell = 0, \dots, n-1,$$

wobei  $k - \ell$  modulo  $n$  zu verstehen ist. Sei  $\omega_j$  eine  $n$ -te Einheitswurzel und  $x^j = (1, \omega_j, \dots, \omega_j^{n-1})$ . Dann ist

$$\begin{aligned} \rho_{\text{reg}}(s^\ell) x^j &= \sum_{k=0}^{n-1} \omega_j^{k-\ell} e_k = \omega_j^{-\ell} \sum_{k=0}^{n-1} \omega_j^k e_k \\ &= \omega_j^\ell x. \end{aligned}$$

Also ist  $V_j = \text{sp}\langle x^j \rangle$  invarianter Unterraum von  $\rho$ , und  $\rho_j(s^\ell) = \omega_j^\ell$  Darstellung von  $C_n$  in  $V_j$ . Für  $\omega_j = e^{2\pi i j/n}$ ,  $j = 0, \dots, n-1$  gilt  $V = V_0 \oplus \dots \oplus V_{n-1}$ , weil  $x^0, \dots, x^{n-1}$  linear unabhängig sind (Van der Monde'sche Determinante). Also  $\rho = \rho_0 + \dots + \rho_{n-1}$ .

**Satz 2.1.8** (Lemma von Schur) Seien  $\rho_i$  irreduzible Darstellungen einer Gruppe in  $V_i$ ,  $i = 1, 2$ . Sei  $\tau : V_1 \rightarrow V_2$  linear. Es gelte  $\tau \rho_1 = \rho_2 \tau$ . Dann gilt:

(i) Sind  $\rho_1, \rho_2$  nicht äquivalent, so ist  $\tau = 0$ .

(ii) Ist  $\rho_1 = \rho_2$ , so ist  $\tau = \lambda$  mit  $\lambda \in \mathbb{C}$ .

**Beweis:**

(i) Wir zeigen zunächst, daß  $W_1 = \tau^{-1}(0)$  invarianter Unterraum von  $\rho_1$  ist. Ist nämlich  $x \in W_1$ , so ist auch  $\tau\rho_1(s)x = \rho_2(s)\tau x = 0$ .

Da  $\rho_1$  irreduzibel ist, ist also entweder  $W_1 = \{0\}$  oder  $W_1 = V_1$ . Im letzteren Fall sind wir fertig. Im ersten Fall ist  $\tau$  injektiv. Wir zeigen, daß  $W_2 = \tau V_1$  invarianter Unterraum von  $\rho_2$  ist. Für  $y \in W_2$  ist nämlich  $\rho_2(s)y = \rho_2(s)\tau x = \tau\rho_1(s)x \in W_2$ . Da  $\rho_2$  irreduzibel ist, ist entweder  $W_2 = \{0\}$  oder  $W_2 = V_2$ . Im ersten Fall ist  $\tau = 0$ , und wir sind fertig. Im zweiten Fall ist  $\tau$  surjektiv. Da  $\tau$  auch injektiv ist, ist  $\tau$  bijektiv, und das ist nicht möglich, da  $\rho_1, \rho_2$  nicht äquivalent sind.

(ii) Für  $\rho_1 = \rho_2$  ist  $V_1 = V_2 = V$  und  $\tau : V \rightarrow V$  hat mindestens einen Eigenwert  $\lambda$  und Eigenvektor  $x$  zu  $\lambda$ , also  $\tau x = \lambda x$ ,  $x \neq 0$ . Sei  $\tau' = \tau - \lambda$  und  $W'_1 = \tau'^{-1}(0)$ .  $W'_1$  ist invarianter Unterraum von  $\rho$ . Ist nämlich  $v \in W'_1$ , so ist  $\tau'\rho(s)v = (\tau - \lambda)\rho(s)v = \rho(s)(\tau - \lambda)v = \rho(s)\tau'v = 0$ . Also ist wieder entweder  $W'_1 = \{0\}$  oder  $W'_1 = V$ . Das erste ist nicht möglich, weil  $x \in W'_1$ . Also muß  $W'_1 = V$  und damit  $\tau v = \lambda v$  sein für alle  $v \in B$ . Also  $\tau = \lambda$ .

□

**Satz 2.1.9** Seien  $\rho_1, \rho_2$  irreduzible Darstellungen von  $G$  in  $V_1, V_2$ , und sei  $\tau : V_1 \rightarrow V_2$  eine lineare Abbildung. Sei

$$\tau' = \frac{1}{|G|} \sum_{t \in G} \rho_2(t^{-1})\tau\rho_1(t).$$

Dann gilt:

(i) Sind  $\rho_1, \rho_2$  nicht äquivalent, so ist  $\tau' = 0$ .

(ii) Ist  $\rho_1 = \rho_2$ , so ist  $\tau' = d^{-1}$  Spur ( $\tau$ ) mit dem Grad  $d$  von  $\rho_1$ .

**Beweis:** Für jedes  $s \in G$  ist

$$\begin{aligned}
 \rho_2(s)\tau' &= \frac{1}{|G|} \sum_{t \in G} \rho_2(s)\rho_2(t^{-1})\tau\rho_1(t) \\
 &= \frac{1}{|G|} \sum_{t \in G} \rho_2(st^{-1})\tau\rho_1(t) \\
 &= \frac{1}{|G|} \sum_{t \in G} \rho_2(t^{-1})\tau\rho_1(ts) \\
 &= \frac{1}{|G|} \sum_{t \in G} \rho_2(t^{-1})\tau\rho_1(t)\rho_1(s) \\
 &= \tau'\rho_1(s).
 \end{aligned}$$

Sind also  $\rho_1, \rho_2$  nicht äquivalent, so ist nach dem Lemma von Schur  $\tau' = 0$ . Ist  $\rho_1 = \rho_2 = \rho$ , so folgt ebenfalls nach dem Lemma von Schur  $\tau' = \lambda$ . Also gilt

$$\lambda = \frac{1}{|G|} \sum_{t \in G} \rho(t^{-1})\tau\rho(t).$$

Berechnen wir auf beiden Seiten die Spur, so folgt

$$\begin{aligned}
 \lambda d &= \frac{1}{|G|} \sum_{t \in G} \text{Spur } (\rho(t^{-1})\tau\rho(t)) \\
 &= \frac{1}{|G|} \sum_{t \in G} \text{Spur } ((\rho(t)^{-1}\tau\rho(t)) \\
 &= \frac{1}{|G|} \sum_{t \in G} \text{Spur } (\tau) \\
 &= \text{Spur } (\tau).
 \end{aligned}$$

**Satz 2.1.10** (Orthogonalitätsrelationen) Seien  $\rho_1, \rho_2$  irreduzible Darstellungen von  $G$  in  $V_1, V_2$ , und seien  $\rho_1, \rho_2$  bezüglich bestimmter Basen in  $V_1, V_2$  durch die Matrizen  $R^1, R^2$  beschrieben. Dann gilt:

(i) Sind  $\rho_1, \rho_2$  nicht äquivalent, so ist für alle  $i, j, \ell, k$

$$\frac{1}{|G|} \sum_{t \in G} R_{i\ell}^2(t^{-1}) R_{kj}^1(t) = 0$$

(ii) Ist  $\rho_1 = \rho_2$ , so gilt mit  $d = \text{Grad}(\rho_1)$

$$\frac{1}{|G|} \sum_{t \in G} R_{i\ell}^2(t^{-1}) R_{kj}^1(t) = \begin{cases} 1/d & \text{falls } i = j \text{ und } \ell = k, \\ 0 & \text{sonst.} \end{cases}$$

**Beweis:** Sei  $T$  die  $(d_2, d_1)$ -Matrix ( $d_i = \text{Grad}(\rho_i)$ )

$$T_{mn} = \begin{cases} 1 & , \quad m = \ell \text{ und } n = k, \\ 0 & , \quad \text{sonst.} \end{cases}$$

Sei  $\tau$  die lineare Abbildung von  $V_1, V_2$ , die bezüglich der gewählten Basen in  $V_1, V_2$  die Matrix  $T$  hat. Dann hat die lineare Abbildung  $\tau'$  aus Satz 2.1.9 bezüglich dieser Basen die Matrix  $T'$  mit

$$T'_{ij} = \frac{1}{|G|} \sum_{t \in G} R_{i\ell}^2(t^{-1}) R_{kj}^1(t).$$

Sind  $\rho_1, \rho_2$  nicht äquivalent, so ist nach Satz 2.1.9  $T' = 0$  und damit (i) bewiesen. Für  $\rho_1 = \rho_2$  ist nach Satz 2.1.9  $T' = d^{-1} \delta_{\ell k}$ , und daraus folgt (ii).

□

**Beispiel:**  $G = C_n$ . Seien  $\omega_1, \omega_2$   $n$ -te Einheitswurzeln. Dann sind  $\rho_1(q^k) = \omega_1^k, \rho_2(q^k) = \omega_2^k$  irreduzible Darstellungen von  $C_n = \{1, q, \dots, q^{n-1}\}$ , die für  $\omega_1 \neq \omega_2$  nicht äquivalent sind. Nach Satz 2.1.10 (i), (ii) ist dann

$$\frac{1}{n} \sum_{r=0}^{n-1} \omega_2^{-r} \omega_1^r = \begin{cases} 0 & , \quad \omega_1 \neq \omega_2, \\ 1 & , \quad \omega_1 = \omega_2. \end{cases}$$

Dies sind die bekannten Orthogonalitätsrelationen der Exponentialfunktion.

## 2.2 Charaktere endlicher Gruppen

Darstellungen von Gruppen sind recht komplizierte Gebilde. Für viele Fragen genügt es, einfachere Gebilde, nämlich Charaktere zu betrachten.

**Definition 2.2.1** Sei  $\rho$  eine Darstellung von  $G$  in  $V$ . Dann heißt die Abbildung  $\chi : G \rightarrow \mathbf{C}$ , welche durch

$$\chi(s) = \text{Spur}(\rho(s))$$

definiert ist, der Charakter von  $\rho$  und ein Charakter von  $G$ . Charaktere von irreduziblen Darstellungen heißen irreduzible Charaktere.

**Satz 2.2.2** (Eigenschaften von Charakteren):

1. Äquivalente Darstellungen haben den gleichen Charakter.
2.  $\chi(1) = d = \text{Grad}(\rho)$ .
3.  $\chi(a^{-1}sa) = \chi(s)$ .
4. Sind  $\chi_1, \dots, \chi_r$  die Charaktere der Darstellungen  $\rho_1, \dots, \rho_r$ , dann hat  $\rho_1 + \dots + \rho_r$  den Charakter  $\chi_1 + \dots + \chi_r$ .
5.  $\overline{\chi}(s) = \chi(s^{-1})$ .

**Beweis:**

1. Ist  $\rho_1 = \tau\rho_2\tau^{-1}$ , so gilt  $\text{Spur}(\rho_1) = \text{Spur}(\rho_2)$ .
2.  $\text{Spur}(d\text{-dimensionale Einheitsmatrix}) = d$ .
3. Siehe 1.

4. Seien  $\rho_1, \dots, \rho_r$  bezüglich gewisser Basen beschrieben durch Matrizen  $R_1, \dots, R_r$ . Dann hat  $\rho_1 + \dots + \rho_r$  die Matrix

$$\begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_r \end{pmatrix},$$

deren Spur gerade  $\text{Spur}(R_1) + \dots + \text{Spur}(R_r)$  ist.

5. Bezüglich eines geeigneten Skalarproduktes ist die Darstellung  $\rho$  unitär und damit

$$\begin{aligned} \chi(s^{-1}) &= \text{Spur}(\rho(s^{-1})) = \text{Spur}(\rho(s)^*) = \overline{\text{Spur}(\rho(s))} \\ &= \overline{\chi(s)}. \end{aligned}$$

□

In dem linearen Raum der komplexwertigen Funktionen auf  $G$  führen wir nun das Skalarprodukt

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{t \in G} \varphi(t) \overline{\psi(t)}$$

ein. Damit gilt

**Satz 2.2.3** (*Orthogonalität der Charaktere*): Seien  $\chi_1, \chi_2$  die Charaktere der irreduziblen Darstellungen  $\rho_1, \rho_2$  von  $G$ . Dann gilt

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & , \quad \rho_1, \rho_2 \text{ äquivalent} \\ 0 & , \quad \text{sonst.} \end{cases}$$

**Beweis:** Seien  $\chi_1, \chi_2$  die Charaktere der Darstellungen  $\rho_1, \rho_2$  von  $G$ , und seien  $\rho_1, \rho_2$  bezüglich gewisser Basen beschrieben durch die Matrizen  $R^1, R^2$ . Dann ist

$$\begin{aligned} \langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{t \in G} \chi_1(t) \overline{\chi_2(t)} = \frac{1}{|G|} \sum_{t \in G} \chi_1(t) \chi_2(t^{-1}) \\ &= \sum_{k, \ell} \frac{1}{|G|} \sum_{t \in G} R_{kk}^1(t) R_{\ell\ell}^2(t^{-1}). \end{aligned}$$

Die Behauptung folgt aus Satz 2.1.10.

□

Für die direkte Summe von  $c$  zu einer Darstellung  $\rho$  äquivalenten Darstellungen schreiben wir in Zukunft einfach  $c\rho$ . Mit dieser Schreibweise haben wir

**Satz 2.2.4** *Jede Darstellung  $\rho$  einer Gruppe  $G$  läßt sich eindeutig (bis auf die Reihenfolge) als direkte Summe*

$$\rho = c_1\rho_1 + \dots + c_m\rho_m$$

*irreduzibler und paarweise nicht äquivalenter Darstellungen  $\rho_1, \dots, \rho_m$  schreiben. Sind  $\chi, \chi_i$  die Charaktere von  $\rho, \rho_i$ , so gilt*

$$c_i = \langle \chi, \rho_i \rangle .$$

**Beweis:** Nach Satz 2.1.6 gibt es irreduzible Darstellungen  $\rho'_1, \dots, \rho'_r$ , so daß

$$\rho = \rho'_1 + \dots + \rho'_r .$$

Sind  $\chi'_1, \dots, \chi'_r$  die Charaktere von  $\rho'_1, \dots, \rho'_r$ , so ist

$$\langle \chi, \chi_i \rangle = \sum_{k=1}^r \langle \chi'_k, \chi'_k \rangle .$$

Nach 2.1.3 ist dies genau die Anzahl der zu  $\rho'_i$  äquivalenten Darstellungen unter den  $\chi'_1, \dots, \chi'_r$ . Fassen wir jeweils äquivalente Darstellungen zusammen, so folgt die Behauptung.

□

**Definition 2.2.5** *Die Zahlen  $c_i$  in Satz 2.2.4 heißen Vielfachheiten des Auftretens von  $\rho_i$  in  $\rho$ .*

**Satz 2.2.6** *Darstellungen mit gleichem Charakter sind äquivalent.*

**Beweis:** Seien  $\rho^1, \rho^2$  Darstellungen von  $G$ . Nach Satz 2.2.4 gibt es Zahlen  $c_k^1, c_k^2$  mit

$$\rho^1 = \sum_{k=1}^m c_k^1 \rho_k \quad , \quad \rho^2 = \sum_{k=1}^m c_k^2 \rho_k .$$

Dabei sind  $\rho_1, \dots, \rho_m$  irreduzible und paarweise nicht äquivalente Darstellungen von  $G$  und  $\chi_1, \dots, \chi_m$  ihre Charaktere. Haben nun  $\rho^1, \rho^2$  den gleichen Charakter  $\chi$ , so gilt nach Satz 2.2.3

$$c_k^1 = \langle \chi, \chi_k \rangle = c_k^2 .$$

Also sind  $\rho^1, \rho^2$  äquivalent. □

**Folgerung:** Infolge von Satz 2.2.6 lassen sich die Orthogonalitätsrelationen der Charaktere (Satz 2.2.3) einfacher formulieren: Seien  $\chi_1, \chi_2$  irreduzible Charaktere einer Gruppe  $G$ . Dann gilt

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & , \quad \chi_1 = \chi_2 , \\ 0 & , \quad \text{sonst} . \end{cases}$$

**Beispiel:** Die Diedergruppe  $C_n$  besitzt für gerades  $n$  folgende Charaktere:

	$r^k$	$sr^k$	Bemerkungen
$\chi_1$	1	1	$h = 1, \dots, \frac{n}{2} - 1$
$\chi_2$	1	-1	
$\chi_3$	$(-1)^k$	$(-1)^k$	
$\chi_4$	$(-1)^k$	$(-1)^{k+1}$	
$\chi_5$	$2 \cos(2\pi hk/n)$	0	

Neben einer Reihe trivialer Beziehungen erhält man aus Satz 2.2.6 auch die Orthogonalitätsrelationen

$$\sum_{k=0}^{n-1} \cos(2\pi h_1 k/n) \cos(2\pi h_2 k/n) = \begin{cases} \frac{n}{2} & , \quad h_1 = h_2 , \\ 0 & , \quad h_1 \neq h_2 , \end{cases}$$

mit  $1 \leq h_1, h_2 < \frac{n}{2}$ .

**Satz 2.2.7** *Zu einer Gruppe  $G$  gibt es ein maximales endliches System irreduzibler paarweise inäquivalenter Darstellungen  $\rho_1, \dots, \rho_m$ . Jedes  $\rho_i$  ist in  $\rho_{\text{reg}}$  genau so oft enthalten, wie es sein Grad  $d_i$  angibt. Es ist*

$$|G| = \sum_{i=1}^m d_i^2. \quad (2.2.1)$$

**Beweis:** Zunächst berechnen wir den regulären Charakter  $\chi_{\text{reg}}$  der regulären Darstellung  $\rho_{\text{reg}}(s)$ . Ist  $\{e_{t_1}, \dots, e_{t_n}\}$  eine Basis von  $V$ , so wird  $\rho_{\text{reg}}(s)$  beschrieben durch die Permutationsmatrix

$$P(s) = (e_{st_1}, \dots, e_{st_n}),$$

wo  $t_1, \dots, t_n$  die Elemente der Gruppe sind. Für  $s = 1$  ist  $P(1) = I$  und damit  $\chi_{\text{reg}}(1) = \text{Spur}(I) = |G|$ . Für  $s \neq 1$  hat  $P(s)$  in der Diagonale nur Nullen. Also  $\chi_{\text{reg}}(s) = \text{Spur}(P(s)) = 0$  für  $s \neq 1$ .

Sei nun  $\rho_1, \dots, \rho_m$  ein System irreduzibler paarweise inäquivalenter Darstellungen von  $G$  und  $\chi_1, \dots, \chi_m$  die zugehörigen Charaktere. Dann ist

$$\begin{aligned} \langle \chi_{\text{reg}}, \chi_i \rangle &= \frac{1}{|G|} \sum_{t \in G} \chi_{\text{reg}}(t) \overline{\chi_i}(t) \\ &= \frac{1}{|G|} \sum_{t \in G} \chi_{\text{reg}}(t) \chi_i(t^{-1}) \\ &= \chi_i(1) = d_i. \end{aligned}$$

Wir können nach Satz 2.2.4 die  $\rho_i$  so wählen, daß

$$\rho_{\text{reg}} = \sum_{i=1}^m d_i \rho_i.$$

Bilden wir hiervon die Spur, so erhalten wir

$$\begin{aligned} |G| &= \chi_{\text{reg}}(1) = \text{Spur}(\rho_{\text{reg}}(1)) = \sum_{i=1}^m d_i \text{Spur}(\rho_i(1)) \\ &= \sum_{i=1}^m d_i \chi_i(1) = \sum_{i=1}^m d_i^2. \end{aligned}$$

Wäre nun  $\rho_{m+1}$  eine weitere irreduzible Darstellung von  $G$ , welche zu keinem der  $\rho_1, \dots, \rho_m$  äquivalent wäre, so wäre notwendig  $d_{m+1} = 0$ ,  $\rho_{m+1}$  also vom Grade 0. Ein solches  $\rho_{m+1}$  kann es also nicht geben, d.h.  $\rho_1, \dots, \rho_m$  ist maximal.

**Bemerkung:** (2.1) charakterisiert also maximale Systeme paarweise inäquivalenter irreduzibler Darstellungen.

**Satz 2.2.8** *Ein Charakter  $\chi$  ist genau dann irreduzibel, wenn  $\langle \chi, \chi \rangle = 1$ .*

**Beweis:** Sei  $\chi$  der Charakter von  $\rho$  und  $\rho$  irreduzibel. Dann ist  $\langle \chi, \chi \rangle = 1$  nach Satz 2.2.3. Sei umgekehrt  $\langle \chi, \chi \rangle = 1$ . Sei  $\rho_1, \dots, \rho_m$  ein maximales System irreduzibler paarweise inäquivalenter Darstellungen und seien  $\chi_1, \dots, \chi_m$  die zugehörigen Charaktere. Dann gibt es ganze Zahlen  $c_1, \dots, c_m$  mit  $\chi = c_1\chi_1 + \dots + c_m\chi_m$ . Aus Satz 2.2.3 folgt

$$\langle \chi, \chi \rangle = \sum_{i=1}^m c_i^2 \langle \chi_i, \chi_i \rangle.$$

Nun ist  $\langle \chi, \chi \rangle = 1$  und  $\langle \chi_i, \chi_i \rangle = 1$ , weil die  $\chi_i$  irreduzibel sind. Also gilt

$$1 = \sum_{i=1}^m c_i^2.$$

Da die  $c_i$  alle ganz sind, ist genau eines der  $c_i = 1$ , und alle anderen  $c_i$  sind Null.  $\rho$  ist also äquivalent zu einem der  $\rho_i$  und damit wie dieses irreduzibel. Also ist  $\chi$  irreduzibel.

□

**Beispiel:** Wir wollen zeigen, daß das für  $D_n$ ,  $n$  gerade, angegebene System von Darstellungen ein maximales System paarweise inäquivalenter irreduzibler Darstellungen ist.

Die Darstellungen  $\rho_1, \dots, \rho_4$  sind trivialerweise irreduzibel und paarweise nicht äquivalent. Wir haben oben schon nachgerechnet, daß

$$\langle \chi_5^h, \chi_5^h \rangle = \frac{2}{n} \sum_{k=0}^{n-1} \cos^2(2\pi kh/n) = 1$$

ist für  $h = 1, \dots, \frac{n}{2} - 1$ . Wir haben damit

$$d_1 = d_2 = d_3 = d_4 = 1, \quad d_5^h = 2, \quad h = 1, \dots, \frac{n}{2} - 1$$

und damit

$$d_1^2 + d_2^2 + d_3^2 + d_4^2 + \sum_{h=1}^{\frac{n}{2}-1} (d_5^h)^2 = 2n = |G|.$$

Also haben wir ein maximales System.

**Definition 2.2.9**  $a, b \in G$  heißen äquivalent, falls es  $s \in G$  gibt mit  $a = s^{-1}bs$ . Die zugehörigen Äquivalenzklassen seien  $A_1, \dots, A_k$ , und es sei  $s \in A_1$ . Wir setzen  $g_i = |A_i|$  und  $g = |G|$ , also  $g = \sum_{i=1}^k g_i$ . Eine Funktion  $h : G \rightarrow \mathbb{C}$  heißt Klassenfunktion, falls  $h$  auf jeder Äquivalenzklasse konstant ist.

Offenbar ist jeder Charakter von  $G$  eine Klassenfunktion. Der nächste Satz zeigt, daß dies im wesentlichen auch schon alle Klassenfunktionen sind.

**Satz 2.2.10** Sei  $\rho_1, \dots, \rho_m$  ein maximales System irreduzibler und paarweise inäquivalenter Darstellungen von  $G$  und  $A_1, \dots, A_k$  wie in Definition 2.2.9. Dann gilt:

- (i)  $m = k$
- (ii) Jede Klassenfunktion ist Linearkombination von Charakteren von  $G$ .

**Beweis:** Sei  $\chi_j$  der Charakter von  $\rho_j$ . Dann können wir eine Funktion  $\tilde{\chi}_j$  auf  $\{A_1, \dots, A_k\}$  definieren durch

$$\tilde{\chi}_j(A_i) = \sqrt{\frac{g_i}{g}} \chi_j(s), \quad s \in A_i.$$

Auf der Menge der Funktionen auf  $\{A_1, \dots, A_n\}$  definieren wir das Skalarprodukt

$$(u, v) = \sum_{i=1}^k u(A_i) \bar{v}(A_i).$$

Wir zeigen, daß die  $\tilde{\chi}_j$  bezüglich dieses Skalarproduktes ein Orthonormalsystem ist. Es ist mit  $s_i \in A_i$

$$\begin{aligned} \langle \tilde{\chi}_j, \tilde{\chi}_\ell \rangle &= \sum_{i=1}^k \sqrt{\frac{g_i}{g}} \chi_j(s_j) \sqrt{\frac{g_i}{g}} \bar{\chi}_\ell(s_j) \\ &= \frac{1}{g} \sum_{i=1}^k g_i \chi_j(s_i) \bar{\chi}_\ell(s_i) \\ &= \frac{1}{g} \sum_{i=1}^k \sum_{s \in A_i} \chi_j(s) \bar{\chi}_\ell(s) \\ &= \frac{1}{|G|} \sum_{s \in G} \chi_j(s) \bar{\chi}_\ell(s) \\ &= \delta_{j\ell} \end{aligned}$$

nach Satz 2.2.3.

Eine unmittelbare Folgerung ist  $m \leq k$ . Denn  $k$  ist die Dimension des Raumes der Klassenfunktionen, und in diesem Raum gibt es die  $m$  linear unabhängigen Funktionen  $\tilde{\chi}_1, \dots, \tilde{\chi}_m$ .

Es bleibt zu zeigen, daß  $m \geq k$ . Hierzu zeigen wir zunächst einmal: Ist  $\rho$  eine irreduzible Darstellung von  $G$  des Grades  $d$  und  $\chi$  ihr Charakter, so gilt

$$\frac{1}{d} \chi(a) = \chi(b) = \frac{1}{|G|} \sum_{t \in G} \chi(bt^{-1}at). \quad (2.2.2)$$

Aus Satz 2.1.9 mit  $\tau = \rho(a)$  und  $\rho_1 = \rho_2 = \rho$  folgt nämlich

$$\tau' = \frac{1}{|G|} \sum_{t \in G} \rho(t^{-1})\rho(a)\rho(t) = \frac{1}{d} \text{Spur}(\tau) = \frac{\chi(a)}{d}.$$

Linksmultiplikation mit  $\rho(b)$  ergibt

$$\frac{1}{|G|} \sum_{t \in G} \rho(bt^{-1}at) = \frac{\chi(a)}{d} \rho(b).$$

Gehen wir zum Charakter über, so folgt (2.2).

Wir wenden (2.2) an auf  $\chi = \chi_\ell$ ,  $a = s_i \in A_i$ ,  $b^{-1} = s_j \in A_j$ , und summieren über  $\ell$ . Es ergibt sich nach Satz 2.2.7

$$\begin{aligned} \sum_{\ell=1}^m \chi_\ell(s_i)\chi_\ell(s_j^{-1}) &= \frac{1}{|G|} \sum_{\ell=1}^n d_\ell \sum_{t \in G} \chi_\ell(s_j^{-1}t^{-1}s_it) \\ &= \frac{1}{|G|} \sum_{t \in G} \sum_{\ell=1}^n d_\ell \chi_\ell(s^{-1}t^{-1}s_it) \\ &= \frac{1}{|G|} \sum_{t \in G} \chi_{\text{reg}}(s_j^{-1}t^{-1}s_it). \end{aligned}$$

Da für  $i \neq j$  die Elemente  $s_i, s_j$  aus verschiedenen Äquivalenzklassen sind, ist für  $i \neq j$  stets  $s_j^{-1}t^{-1}s_i \neq 1$ . Also

$$\chi_{\text{reg}}(s_j^{-1}t^{-1}s_it) = 0$$

für  $i \neq j$  und damit

$$\sum_{\ell=1}^m \chi_\ell(s_i)\overline{\chi}_\ell(s_j) = 0 \quad (2.2.3)$$

für  $i \neq j$ . Wäre dies auch für  $i = j$  richtig, so wäre

$$\sum_{\ell=1}^m |\chi_\ell(s_i)|^2 = 0 \quad (2.2.4)$$

und damit  $\chi_\ell = 0$  auf  $A_i$  für  $\ell = 1, \dots, m$ . Da  $\rho_1, \dots, \rho_m$  maximal sind, verschwände jeder Charakter auf  $A_i$ . Dies ist z.B. für den Einheitscharakter sicher nicht der Fall. Also kann (2.4) nicht richtig sein.

Zusammen mit (2.3) folgt dann, daß die  $k$ -Spalten der  $(m, k)$ -Matrix

$$\begin{pmatrix} \chi_1(s_1) & , & \cdots & , & \chi_1(s_k) \\ \vdots & & & & \\ \chi_m(s_1) & , & \cdots & , & \chi_m(s_k) \end{pmatrix} \quad (2.2.5)$$

linear unabhängig sind. Diese Matrix muß also mindestens  $k$  Zeilen haben. Damit ist  $m \geq k$  gezeigt.

Daß jede Klassenfunktion sich als Linearkombination von Charakteren schreiben läßt, folgt nun unmittelbar aus der Tatsache, daß der Rang der Matrix (2.5)  $m = k$  ist.

□

## 2.3 Der Chinesische Restsatz

Sei  $R$  ein Ring mit Einselement, z.B. der Ring  $\mathbb{Z}$  der ganzen Zahlen oder der Polynomring  $F[z]$  über einem Körper  $F$ . Ein Ring heißt kommutativ, wenn seine Multiplikation kommutativ ist. Ist  $R$  kommutativ, so sagen wir,  $a$  teilt  $b$  ( $a \mid b$ ), falls es ein  $r$  gibt mit  $b = ar$ . Wir sagen  $a \equiv b \pmod{p}$ , falls  $p \mid a - b$ . Die Äquivalenzklassen dieser Äquivalenzrelation nennen wir Restklassen mod  $p$ . Diese bilden den Restklassenring  $R/p$ . Ein Ring heißt nullteilerfrei, wenn  $ab = 0$  zur Folge hat, daß  $a = 0$  oder  $b = 0$ .

### Beispiele:

- 1)  $\mathbb{Z}_p = \mathbb{Z}/p = \{0, 1, \dots, p-1\}$ . In  $\mathbb{Z}_6$  ist z.B.  $2+5 = 1$ ,  $3 \cdot 4 = 0$ . Also ist  $\mathbb{Z}_6$  nicht nullteilerfrei. Aber  $\mathbb{Z}_p$  ist nullteilerfrei für Primzahlen  $p$ .
- 2) Für den Ring  $F[z]$  und  $p = z^n + a_1 z^{n-1} + \dots + a_0$  ist  $F[z]/p$  der Ring der Polynome vom Grade  $< n$ . Für  $p = z^2 - 1$  ist z.B.  $z(z+1) = z^2 + z \equiv 1 + z \pmod{p}$ .
- 3) Der Ring  $M_n[F]$  der  $(n, n)$ -Matrizen über  $F$  ist nicht nullteilerfrei:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

**Definition 2.3.1** *Ein kommutativer nullteilerfreier Ring  $R$  heißt euklidisch, wenn es für jedes  $a \in R$ ,  $a \neq 0$ , eine ganze Zahl  $g(a) \geq 0$  gibt mit*

$$(i) \quad g(ab) \geq g(b)$$

$$(ii) \quad \text{Zu } a, b \in R, a \neq 0 \text{ gibt es } q, r \in R$$

$$b = qa + r,$$

wobei entweder  $r = 0$  oder  $g(r) < g(a)$  ist.

Man nennt  $g$  den Grad.

**Beispiele:**

- 1)  $\mathbb{Z}$  mit  $g(a) = |a|$  ist ein euklidischer Ring.
- 2)  $F[z]$  mit dem Polynomgrad als Grad ist ebenfalls euklidisch. Z.B. ist
 
$$z^3 + 2z^2 + z + 1 = (z + 2)(z^2 - 1) + 2z + 3$$
- 3) Der Ring  $\mathbb{Z} + \sqrt{-3}\mathbb{Z}$  ist nicht euklidisch.

Ein Element  $e \in R$  heißt Einheit, falls ein  $e' \in R$  existiert mit  $ee' = e'e = 1$ . Wir nennen  $e'$  das Inverse zu  $e$  und schreiben  $e' = e^{-1}$ .

**Beispiele:**

- 1)  $\mathbb{Z}$  hat die Einheiten  $+1, -1$ .
- 2)  $F[z]$  hat die Einheiten  $F$  mit Ausnahme der Null.
- 3)  $M_n[F]$  hat als Einheiten die invertierbaren Matrizen.

Ein Element  $p \in R$  heißt prim, falls  $p = p_1 p_2$  nur möglich ist, wenn  $p_1$  oder  $p_2$  Einheit ist.

**Beispiele:**

- 1) In  $\mathbb{Z}$  sind genau die Elemente prim, für welche der Betrag eine Primzahl ist.
- 2) In  $F[z]$  nennt man die Primelemente irreduzibel über  $F$ . Z.B. ist

$$\begin{array}{ll} z^2 - 1 & = (z + 1)(z - 1) \quad \text{nicht prim für beliebiges } F \\ z^2 + 1 & \text{prim für } F = \mathbb{R}, \text{ nicht prim für } F = \mathbb{C} \\ z^2 - 2 & \text{prim für } F = \Gamma = \text{Körper der rationalen Zahlen,} \\ & \text{aber nicht prim für } F = \mathbb{R} \end{array}$$

Folgende Sätze findet man in jedem Lehrbuch der Algebra.

**Satz 2.3.2** *In einem euklidischen Ring gibt es zu jedem Paar  $a, b \neq 0$  einen größten (im Sinne des Grades) gemeinsamen Teiler  $\text{ggT}(a, b)$ . Es gibt  $p, q \in R$  mit  $\text{ggT}(a, b) = ap + bq$ .*

**Satz 2.3.3** *In einem euklidischen Ring ist jedes Element eindeutig (bis auf Reihenfolge und Einheiten) als Produkt von Primelementen darstellbar.*

**Beispiele:** In dem Ring  $\mathbf{Z} + \sqrt{-3}\mathbf{Z}$  gilt  $4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$ . Dieser Ring ist also nicht euklidisch.

Wir suchen nun Lösungen von simultanen Kongruenzen modulo  $p_1, \dots, p_m$ . Seien also  $a_1, \dots, a_m$  gegeben. Gesucht ist ein  $a$  mit

$$a \equiv a_i \pmod{p_i}, \quad i = 1, \dots, m. \quad (2.3.1)$$

Der Chinesische Restsatz gibt ein Kriterium für Existenz und Eindeutigkeit von (3.1).

**Satz 2.3.4** *Sei  $R$  ein euklidischer Ring, und seien  $p_1, \dots, p_m \in R$  paarweise teilerfremd. Dann ist (3.1) für jede Wahl der  $a_1, \dots, a_m \in R$  lösbar. Die Lösung ist mod  $p_1 \dots p_m$  eindeutig bestimmt.*

**Beweis:** Wir zeigen zunächst: Die Gleichung  $ax \equiv b \pmod{p}$  ist genau dann lösbar, wenn  $\text{ggT}(a, p) | b$ . Ist diese Kongruenz nämlich lösbar, so gibt es  $y$  mit  $ax + py = b$ , und es folgt  $\text{ggT}(a, p) | b$ . Sei umgekehrt diese Bedingung erfüllt. Nach Satz 2.3.2 gibt es  $u, v$  mit  $\text{ggT}(a, p) = au + vp$ . Multiplikation mit  $q = b/\text{ggT}(a, p)$  ergibt  $b = aqu + qvp$ . Damit ist  $x = qu$  Lösung der Kongruenz.

Sei  $p = p_1 \dots p_m$ . Dann ist  $\text{ggT}(\frac{p}{p_i}, p_i) = 1$ , und es gibt nach obigem ein  $x_i$  mit  $\frac{p}{p_i} x_i \equiv 1 \pmod{p_i}$ . Wir behaupten, daß

$$a = \sum_{i=1}^m \frac{p}{p_i} a_i x_i$$

Lösung von (3.1) ist. Wir schreiben für ein  $j$

$$\begin{aligned} a &= \sum_{i \neq j} \frac{p}{p_i} a_i x_i + \frac{p}{p_j} a_j x_j \\ &= p_j \sum_{i \neq j} \frac{p}{p_i p_j} a_i x_i + a_j \left( \frac{p}{p_j} x_j \right) \end{aligned}$$

und dies ist kongruent  $a_j \pmod{p_j}$  nach Konstruktion von  $x_j$ .

Sind  $a, a'$  Lösungen von (3.1), so ist  $a - a' \equiv 0 \pmod{p_i}$  für  $i = 1, \dots, m$  und damit  $a \equiv a' \pmod{p}$ .

□

**Beispiel:**  $R = R[z]$ ,  $p_i = z - z_i$ ,  $z_i$  paarweise verschieden. Wir suchen ein  $a \in R$  mit  $a \equiv a_i \pmod{p_i}$ , d.h.

$$a(z_i) = d_i, \quad i = 1, \dots, m.$$

Nach Satz 2.3.4 ist  $a$  modulo  $p = p_1 \dots p_m$  eindeutig bestimmt.  $a$  ist also das Polynom vom Grad  $n - 1$ , das an den Stellen  $z_i$  die Werte  $a_i$  annimmt.  $a$  ergibt sich als

$$a = \sum_{i=1}^m \frac{p}{p_i} a_i x_i, \quad \frac{p}{p_i} x_i \equiv 1 \pmod{p_i}.$$

Mit

$$\omega_i(z) = \frac{p}{p_i} = \prod_{j \neq i} (z - z_j)$$

haben wir  $x_i = \frac{1}{\omega_i(z_i)}$  und damit

$$a = \sum_{i=1}^m \frac{\omega_i(z)}{\omega_i(z_i)} a_i.$$

Dies ist die Lagrange'sche Interpolationsformel.

Seien  $R_1, R_2$  Ringe. Wir definieren dann einen weiteren Ring  $R_1 \otimes R_2$  folgendermaßen.  $R_1 \otimes R_2$  besteht aus den Paaren  $(a_1, a_2)$  mit  $a_i \in R_i$ .

Addition und Multiplikation in  $R_1 \otimes R_2$  sind komponentenweise erklärt, also

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2) \\ (a_1, a_2)(b_1, b_2) &= (a_1 a_2, b_1 b_2) .\end{aligned}$$

$R_1 \otimes R_2$  heißt direktes Produkt von  $R_1$  und  $R_2$ .

**Satz 2.3.5** *Sei  $R$  ein euklidischer Ring und seien  $p_1, \dots, p_m$  paarweise teilerfremd. Sei  $p = p_1 \dots p_m$ . Dann gilt*

$$R/p = R/p_1 \otimes \dots \otimes R/p_m .$$

**Beweis:** Wir definieren eine Abbildung  $\varphi : R/p_1 \otimes \dots \otimes R/p_m \rightarrow R/p$  mit Hilfe des Satzes 2.3.4. Für  $(a_1, \dots, a_m) \in R/p_1 \otimes \dots \otimes R/p_m$  sei  $a$  die Lösung aus (3.1). Diese ist in  $R/p$  wohlbestimmt. Ist  $(b_1, \dots, b_m) \in R/p_1 \otimes \dots \otimes R/p_m$  und  $b$  die zugehörige Lösung von (3.1), so ist

$$\begin{aligned}a + b &\equiv a_i + b_i \pmod{p_i} \\ ab &\equiv a_i b_i \pmod{p_i} .\end{aligned}$$

$\varphi$  ist also ein Ring-Homomorphismus. Ist  $a \in R$  und  $a_i$  ein Repräsentant von  $a \pmod{p_i}$ , so ist  $a = \varphi(a_1, \dots, a_m)$ . Also ist  $\varphi$  surjektiv. Nach der Eindeutigkeitsaussage von Satz 2.3.4 ist  $\varphi$  injektiv. Also ist  $\varphi$  sogar ein Ring-Isomorphismus.

□

## 2.4 Gruppentheorie

Sei  $G$  eine endliche Gruppe und  $H$  eine Untergruppe von  $G$ . Dann können wir in  $G$  die Äquivalenzrelation

$$s \sim t \iff t^{-1}s \in H$$

erklären. Sei  $s_1, \dots, s_r$  ein Repräsentantensystem dieser Äquivalenzrelation, also  $s_1H, \dots, s_rH$  die Äquivalenzklassen. Diese heißen (Links-)Nebenklassen von  $H$ . Es ist  $G = s_1H \cup \dots \cup s_rH$  und  $r|H| = |G|$ .

$H$  heißt Normalteiler in  $G$ , falls  $tH = Ht$  für  $t \in G$ , d.h. falls die Linksnebenklassen gleich den Rechtsnebenklassen sind. Ist  $H$  Normalteiler von  $G$ , dann bilden die Nebenklassen wieder eine Gruppe, die Faktorgruppe  $G/H$ .

Sei  $a \in G$ . Die Ordnung  $m$  ist die kleinste natürliche Zahl  $m \geq 1$ , für welche  $a^m = 1$ . Es bildet dann  $C_m = \{1, a, a^2, \dots, a^{m-1}\}$  eine Untergruppe von  $G$  der Ordnung  $m$ .  $C_m$  heißt zyklische Gruppe der Ordnung  $m$ . Sie ist isomorph der additiven Gruppe  $\mathbb{Z} \bmod m$ .

**Satz 2.4.1** *Sei  $G$  abelsch, und haben  $a_1, \dots, a_r \in G$  die Ordnung  $m_1, \dots, m_r$ . Sei  $\text{ggT}(m_i, m_j) = 1$  für  $i \neq j$ . Dann hat  $a = a_1 \dots a_r$  die Ordnung  $m = m_1 \cdot \dots \cdot m_r$ .*

**Beweis:** Sicher ist  $a^m = 1$ . Gäbe es ein  $n$  mit  $a^n = 1$  und  $n < m$ , so könnten wir unter diesen  $n$ 's das kleinste wählen. Die  $n$  Elemente  $1, \dots, a^{n-1}$  würden dann eine Untergruppe von  $C_m$  bilden, also  $n|m$ . Da die  $m_i$  paarweise teilerfremd sind, wäre sogar  $n|m_i$  für mindestens ein  $i$ , etwa  $i = 1$ . Dann wäre

$$a^n = a_1^n a_2^n \dots a_r^n = a_2^n \dots a_r^n = 1.$$

Hätten wir die Behauptung für  $r-1$  Faktoren schon bewiesen, so würde sie für  $r$  Faktoren folgen. Da  $r = 1$  trivial ist, ist der Satz nach dem Prinzip der vollständigen Induktion bewiesen.

□

Ähnlich wie das direkte Produkt von Ringen ist das direkte Produkt von Gruppen definiert. Seien  $A, B$  Gruppen. Ihr direktes Produkt  $A \otimes B$  besteht aus den Paaren  $(a, b) \in A \times B$  mit komponentenweiser Multiplikation:  $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$ . Die Elemente  $(a, 1)$  bilden eine Untergruppe von  $A \otimes B$ , die isomorph zu  $A$  ist. Wir schreiben  $A$  für diese Untergruppe, identifizieren also  $(a, 1)$  mit  $a$ .  $A$  wird so zu einer Untergruppe von  $A \otimes B$ , und dasselbe gilt für  $B$ . Offenbar sind  $A, B$  sogar Normalteiler in  $A \otimes B$ . Wegen  $(a, b) = (a, 1)(1, b) = (1, b)(a, 1)$  können wir  $ab$  oder  $ba$  für  $(a, b)$  schreiben. Damit haben wir folgende äquivalente Definition des direkten Produkts: Eine Gruppe  $G$  ist direktes Produkt seiner Untergruppen  $A, B$  genau dann, wenn

- (i) Jedes  $g \in G$  sich eindeutig als  $g = ab$  mit  $a \in A, b \in B$  schreiben läßt.
- (ii)  $ab = ba$  für  $a \in A, b \in B$ .

**Satz 2.4.2** *Seien  $n_1, n_2$  teilerfremd und  $n = n_1n_2$ . Dann ist*

$$C_n = C_{n_1} \otimes C_{n_2} .$$

**Beweis:** Wir identifizieren  $C_n$  mit der Gruppe  $\mathbb{Z}$  mit Addition mod  $n$ . Dann können wir die Abbildung  $\varphi : C_{n_1} \otimes C_{n_2} \rightarrow C_n$  erklären durch  $\varphi(m_1, m_2) = m$ , wobei  $m$  die simultanen Kongruenzen  $m \equiv m_i \pmod{n_i}$ ,  $i = 1, 2$  löst. Da  $m \pmod{n}$  eindeutig bestimmt ist, ist  $\varphi$  injektiv. Da  $n_1, n_2$  teilerfremd sind, gibt es Zahlen  $q_1, q_2$  mit  $q_1n_1 + q_2n_2 = 1$ . Also ist  $(q_1m)n_1 + (q_2m)n_2 = m$  und damit  $m = \varphi(q_2mn_2, q_1mn_1)$  für jedes  $m \in C_n$ . Also ist  $\varphi$  surjektiv. Daß  $\varphi$  ein Homomorphismus ist, ist klar.

□

An Hand des Beispiels  $n_1 = n_2 = 2$  macht sich leicht klar, daß die Voraussetzung  $n_1, n_2$  teilerfremd nicht gestrichen werden kann.

Sei  $M_n = \{m \in \mathbf{Z} : 1 \leq m < n, \text{ggT}(m, n) = 1\}$ . Mit der Multiplikation mod  $n$  wird  $M_n$  zur Gruppe. Es ist nämlich  $1 \in M_n$ . Zu jedem  $m \in M_n$  kann man die Kongruenz  $x m \equiv 1 \pmod{n}$  lösen, und es ist  $\text{ggT}(x, n) = 1$ . Also ist  $x \in M_n$  und  $x = m^{-1}$ . Und schließlich ist offenbar  $m_1 m_2 \in M_n$ , falls  $m_1, m_2 \in M_n$ .

Die Ordnung  $\varphi(n) = |M_n|$  heißt Euler'sche  $\varphi$ -Funktion, also

$$\frac{n}{\varphi(n)} = \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{2} \cdot \frac{5}{4} \cdot \frac{6}{3}$$

Offenbar ist  $\varphi(p) = p - 1$  für Primzahlen  $p$ , und  $\varphi(p^r) = p^r - p^{r-1} = (p - 1)p^{r-1}$ .

**Satz 2.4.3** *Sei  $p$  prim. Dann gilt*

$$M_{p^r} = \begin{cases} C_{p^{n-1}(p-1)} & , \quad p > 2, r \geq 1 \\ C_2 \otimes C_{2^{r-2}} & , \quad p = 2, r \geq 2 \end{cases}$$

**Beweis:** Siehe z.B. Hasse, Number Theory, Chapt. 4.5.

Für  $p > 2$  ist  $M_{p^r}$  also zyklisch, d.h. es gibt  $a$  mit  $M_{p^r} = \{1, a, \dots, a^{\varphi(p^r)-1}\}$ . Für  $r = 1$  ist  $a$  die primitive Wurzel mod  $p$ . Diese finden sich für  $p < 10000$  in Abramowitz/Stegun, Handbook of Mathematical Functions, pp. 864-869. Ein kleiner Auszug ist

$$\frac{p}{a} = \frac{3}{2} \cdot \frac{5}{2} \cdot \frac{7}{3} \cdot \frac{11}{2} \cdot \frac{13}{2} \cdot \frac{17}{3} \cdot \frac{19}{2} \cdot \frac{23}{5}$$

**Beispiele:**

1)  $M_5 = \{1, 2, 3, 4\}$ . Die Gruppentafel ist

	1234
1	1234
2	2413
3	3142
4	4321

Nach Satz 2.4.3 ist  $M_5 = C_4 = \{0, 1, 2, 3\}$  mit Addition mod 4. Die Gruppentafel von  $C_4$  ist

	0123
0	0123
1	1230
2	2301
3	3012

Die  $(i + 1)$ -te Zeile entsteht aus der  $i$ -ten durch Links-Ring-Schift.

Nach Satz 2.4.3 sind  $M_5$  und  $C_4$  isomorph. Die Isomorphie wird hergestellt durch ein erzeugendes Element, etwa 2 aus der obigen Tabelle. Danach ist  $M_5 = \{1, 2, 3, 2^2, 2^3\} = \{1, 2, 4, 3\}$ . Dadurch ergibt sich für  $M_5$  auch die Gruppentafel

	1243
1	1243
2	2431
4	4312
5	3124

Diese Tafel ist in der Tat identisch zu der obigen Tafel von  $C_4$ : Die  $(i + 1)$ -te Zeile ergibt sich durch Links-Ring-Schift aus der  $i$ -ten Zeile.

**2)**  $M_9 = \{1, 2, 4, 5, 7, 8\}$  hat als erzeugendes Element die Zahl 5, also  $M_9 = C_6 = \{1, 5, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 7, 8, 4, 2\}$ . Die Gruppentafel von  $M_9$  ist

	157842
1	157842
5	578421
7	784215
8	842157
4	421578
2	215784

# Kapitel 3

## Schnelle Fourier-Transformation

### 3.1 Fourier-Transformation und Faltung

Die diskrete Fouriertransformation, oder Fourier-Transformation der Länge  $n$ , ist definiert durch

$$\hat{y}_k = \sum_{j=0}^{n-1} e^{-2\pi i j k / n} y_j, \quad k = 0, \dots, n-1.$$

Mit Hilfe der Orthogonalitätsrelationen

$$\frac{1}{n} \sum_{j=0}^{n-1} e^{2\pi i j k / n} = \begin{cases} 1 & , \quad k = 0, \pm n, \pm 2n, \dots, \\ 0 & , \quad \text{sonst} \end{cases}$$

zeigt man leicht die Inversionsformel

$$y_j = \frac{1}{n} \sum_{k=0}^{n-1} e^{2\pi i j k / n} \hat{y}_k, \quad j = 0, \dots, n-1.$$

Die Fourier-Transformation ist also eine lineare Abbildung in  $\mathbb{C}^n$  mit der Matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & & & & \\ 1 & \omega^{n-1} & \omega^{(n-1)2} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix}, \quad \omega = e^{2\pi ij/n}.$$

Wegen  $\omega^n = 1$  kann in dem Exponenten in  $W^n$  mod  $n$  gerechnet werden. Die Orthogonalitätsrelationen ergeben

$$W_n W_n^* = nI.$$

Insbesondere ist also  $\frac{1}{\sqrt{n}}W_n$  eine Isometrie.

Für zwei Vektoren  $x, y \in \mathbb{C}^n$ , deren Komponenten wir von 0 bis  $n-1$  numerieren, nennen wir den Vektor  $z$  mit den Komponenten

$$z_k = \sum_{j=0}^{n-1} x_{k-j} y_j, \quad k = 0, \dots, n-1$$

die (zyklische) Faltung von  $x$  und  $y$ . Dabei rechnen wir im Index von  $x$  mod  $n$ . Wir schreiben  $z = x * y$ . In Matrix-Form lautet die Faltung  $z = Xy$

$$X = \begin{pmatrix} x_0 & x_{n-1} & \cdots & x_1 \\ x_1 & x_0 & \cdots & x_2 \\ \vdots & & & \\ x_{n-1} & x_{n-2} & \cdots & x_0 \end{pmatrix}.$$

Die  $(i+1)$ -te Zeile dieser Matrix entsteht also aus der  $i$ -ten durch einen Rechts-Ring-Schift.

**Satz 3.1.1 (Faltungssatz)** Für  $x, y \in \mathbb{Z}^n$  gilt

$$(x * y)_k^\wedge = \hat{x}_k \hat{y}_k, \quad k = 0, \dots, n-1.$$

**Beweis:** Auch dies ist eine unmittelbare Folgerung aus den Orthogonalitätsrelationen. □

## 3.2 Cooley-Tukey

Wir beschreiben nun verschiedene Versionen der schnellen Fourier-Transformation nach Cooley-Tukey. Wir nehmen an, die Länge  $n$  der Fourier-Transformation faktoriere gemäß  $n = mp$ . Den Fall  $p = 2$  haben wir teilweise schon in der Einleitung behandelt.

### 1. Dezimierung in der Zeit

Wir haben auswerten

$$\hat{y}_k = \sum_{j=0}^{n-1} \omega_n^{jk} y_j, \quad k = 0, \dots, n-1,$$

wo  $\omega_n = e^{-2\pi i/n}$  eine  $n$ -te Einheitswurzel ist. Wir fassen in der Summe diejenigen Indizes  $j$  zusammen, welche der gleichen Restklasse mod  $p$  angehören. Dies ergibt

$$\hat{y}_k = \sum_{r=0}^{p-1} \sum_{\ell=0}^{m-1} \omega_n^{(p\ell+r)k} y_{p\ell+r}.$$

Nun ist  $\omega_n^p = \omega_m$ . Also folgt

$$\hat{y}_k = \sum_{r=0}^{p-1} \omega_n^{rk} \sum_{\ell=0}^{m-1} \omega_m^{\ell k} y_{p\ell+r}.$$

Führen wir die Vektoren

$$y^r = \begin{pmatrix} y_r \\ y_{p+r} \\ \vdots \\ y_{(m-1)p+r} \end{pmatrix} \in \mathbb{C}^m, \quad r = 0, \dots, p-1$$

ein, so lautet dies

$$\hat{y}_k = \sum_{r=0}^{p-1} \omega_n^{rk} (\hat{y}^r)_k,$$

wo  $\hat{y}^r$  die Fourier-Transformation der Länge  $m$  von  $y^r$  bedeutet. Diese hat die Periode  $m$ . Also gilt

$$\hat{y}_{k+\ell m} = \sum_{r=0}^{p-1} \omega_n^{(k+\ell m)r} (\hat{y}^r)_k, \quad k = 0, \dots, m-1, \quad \ell = 0, \dots, p-1$$

und wegen  $\omega_n^m = \omega_p$

$$\hat{y}_{k+\ell m} = \sum_{r=0}^{p-1} \omega_p^{\ell r} \omega_n^{k\ell} (\hat{y}^r)_k. \tag{3.2.1}$$

Bis auf die Multiplikation mit  $\omega_n^{k\ell}$  sind dies  $m$  Fourier-Transformationen der Länge  $p$ . Die Fourier - Transformation der Länge  $n$  kann also ausgeführt werden durch  $p$  Fourier-Transformationen der Länge  $m$  und  $m$  Fourier-Transformationen der Länge  $p$ , zuzüglich einiger Multiplikationen mit Einheitswurzeln und Permutationen.

Wir wollen (3.2.1) in Matrixform schreiben. Mit  $W_n, W_m, W_p$  die Fourier-Transformation der Längen  $n, m, p$  und

$$D_n = \begin{pmatrix} 1 & & & \\ & \omega_n & & \\ & & \ddots & \\ & & & \omega_n^{m-1} \end{pmatrix}$$

lautet (3.2.1), wenn wir zunächst die  $m$  Gleichungen für  $\ell = 0$ , dann die  $m$  Gleichungen für  $\ell = 1$  usw. aufschreiben,

$$\hat{y} = \begin{pmatrix} I_m & I_m & \cdots & I_m \\ I_m & \omega_p I_m & \cdots & \omega_p^{p-1} I_m \\ \vdots & \vdots & & \vdots \\ I_m & \omega_p^{p-1} I_m & \cdots & \omega^{(p-1)^2} I_m \end{pmatrix} \begin{pmatrix} D_m^0 & & & \mathbf{0} \\ & D_m^1 & & \\ & & \ddots & \\ \mathbf{0} & & & D_m^{p-1} \end{pmatrix} * \tag{3.2.2}$$

$$* \begin{pmatrix} W_m & & & \mathbf{0} \\ & W_m & & \\ & & \ddots & \\ \mathbf{0} & & & W_m \end{pmatrix} \begin{pmatrix} y^0 \\ y^1 \\ \vdots \\ y^{p-1} \end{pmatrix}.$$

Hier führen wir folgende Schreibweise ein. Ist  $A$  eine  $(m, n)$ -Matrix und  $B$  eine  $(p, q)$ -Matrix, so bezeichnet das Tensorprodukt  $A \otimes B$  die  $(mp, nq)$ -Matrix

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & & & \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

Damit lautet (3.2.2)

$$W_n = (W_p \otimes I_m) \begin{pmatrix} D_m^0 & & & \\ & D_m^1 & & \\ & & \ddots & \\ & & & D_m^{p-1} \end{pmatrix} (I_p \otimes W_m) P_{p,m} \quad (3.2.3)$$

mit einer Permutationsmatrix  $P_{p,m}$ . Ist  $y = (y_0, \dots, y_{n-1})^T$ , so ist  $P_{p,m}y$  der Vektor

$$(y_0, y_p, \dots, y_{(n-1)p}, y_1, y_{p+1}, \dots, y_{(m-1)p+1}, \dots, y_{m-1}, y_{p+m-1}, \dots, y_{(m-1)p+n-1}).$$

Anders ausgedrückt: Ist  $0 \leq i < n$  und  $i = mq + r$  mit ganzen Zahlen  $0 \leq q < p$ ,  $0 \leq r < m$  (Division mit Rest), so ist

$$(Py)_i = y_{rp+q}.$$

Ist  $n$  ein Produkt kleiner Faktoren, so nennt man  $n$  *FT*-freundlich. Wiederholte Anwendungen von (3.2.4) führt dann zu einem effizienten Algorithmus.

Das einfachste Beispiel von *FT*-freundlichen Zahlen sind Potenzen von 2. Diesen Fall wollen wir nun etwas ausführlicher betrachten. Wir führen dazu den *butterfly* der Ordnung  $m$  ein als die  $(m, m)$ -Matrix

$$B_m = \begin{pmatrix} I_{m/2} & D_{m/2} \\ I_{m/2} & -D_{m/2} \end{pmatrix}$$

ein. Für  $p = 2$  lautet (3.2.4)

$$\begin{aligned} W_n &= (W_2 \otimes I_{n/2}) \begin{pmatrix} I_{n/2} & \mathbf{O} \\ \mathbf{O} & D_{n/2} \end{pmatrix} (I_2 \otimes W_{n/2}) P_{2,n/2} \\ &= B_n (I_2 \otimes W_{n/2}) P_{2,n/2}. \end{aligned}$$

Rekursive Anwendung ergibt

$$\begin{aligned}
 W_n &= B_n(I_2 \otimes B_{n/2})(I_4 \otimes W_{n/4})(I_2 \otimes P_{2,n/4})P_{2,n/2} \\
 &\vdots \\
 &= (I_1 \otimes B_n)(I_2 \otimes B_{n/2})(I_4 \otimes B_{n/4}) \cdots (I_{n/2} \otimes B_2)P_n \quad (3.2.4) \\
 P_n &= (I_{n/4} \otimes P_{2/2}) \cdots (I_{2,n/4})(I_1 \otimes P_{2,n/2}) . \quad (3.2.5)
 \end{aligned}$$

Dies ist die Radix-2-Version der Cooley-Tukey *FFT*.

Die Permutation  $P_n$  kann durch *bitreversal* angewendet werden. Die *bitreversal*-Funktion  $r_n$  von  $\{0, \dots, n - 1\}$  in sich ist für  $n = 2^t$  wie folgt definiert. Sei  $(b_{t-1}, \dots, b_0)_2$  die Dualdarstellung von  $k$ , also

$$k = b_{t-1}2^{t-1} + \dots + b_12 + b_0$$

mit  $b_i \in \{0, 1\}$ . Dann ist  $r_n(k) = (b_0, \dots, b_{t-1})_2$ .

**Satz 3.2.1** *Die Komponenten von  $x$ ,  $P_n x$  seien von 0 bis  $n - 1$  nummeriert, und  $n = 2^t$ . Dann gilt*

$$(Px)_k = x_{r_n(k)} \quad , \quad k = 0, \dots, n - 1 .$$

**Beweis:** Für  $t = 1$  ist  $P_2 = I_2$  und die Behauptung trivial. Sei die Behauptung richtig für  $t - 1$ , und sei  $m = 2^{t-1}$ .

Nach (3.2.5) ist

$$P_n x = (I_2 \otimes P_m)P_{2,m}x = \begin{pmatrix} P_m \begin{pmatrix} x_0 \\ x_2 \\ \vdots \\ x_{m-2} \end{pmatrix} \\ P_m \begin{pmatrix} x_1 \\ x_3 \\ \vdots \\ x_{m-1} \end{pmatrix} \end{pmatrix} .$$

Nach Induktionsannahme können wir  $P_m$  durch *bitreversal* auswerten. Ist also  $k = (b_{t-2}, \dots, b_0)_2$  und  $k' = (b_0, \dots, b_{t-2})_2$ , so ist

$$\left( P_m \begin{pmatrix} x_0 \\ x_2 \\ \vdots \\ x_{m-1} \end{pmatrix} \right)_k = x_{2k'} \quad , \quad \left( P_m \begin{pmatrix} x_1 \\ x_3 \\ \vdots \\ x_{m-1} \end{pmatrix} \right)_k = x_{2k'+1} \quad .$$

Nun ist aber für  $k = 0, \dots, m-1$

$$k = (0, b_{t-2}, \dots, b_0)_2 \quad , \quad 2k' = (b_{t-2}, \dots, b_0, 0)_2$$

und für  $k = m, \dots, n-1$

$$k = (1, b_{t-2}, \dots, b_0)_2 \quad , \quad 2k' + 1 = (b_{t-2}, \dots, b_0, 1)_2 \quad .$$

In jedem Fall erhält man den Index von  $x$  also durch *bitreversal*.

□

## 2. Dezimierung in der Frequenz

Jetzt fassen wir die Indizes  $k$ , welche zur gleichen Restklasse mod  $m$  gehören, zusammen, schreiben also

$$\begin{aligned} \hat{y}_{m\ell+r} &= \sum_{j=0}^{n-1} \omega_n^{j(m\ell+r)} y_j \\ &= \sum_{j=0}^{n-1} \omega_n^{jr} y_j \\ &= \sum_{k=0}^{m-1} \sum_{j=0}^{p-1} \omega_p^{j+kp} \omega_n^{(j+kp)r} y_{j+kp} \\ &= \sum_{k=0}^{m-1} \omega_m^{kr} \sum_{j=0}^{p-1} \omega_p^{j\ell} \omega_n^{rj} y_{j+kp} \quad , \end{aligned}$$

wobei wir wieder  $\omega_n^p = \omega_m$  und  $\omega_n^m = \omega_p$  benutzt haben. Dieses Mal setzen wir

$$y^k = \begin{pmatrix} y_{kp} \\ y_{kp+1} \\ \vdots \\ y_{kp+p-1} \end{pmatrix} \in \mathbb{C}^p, \quad k = 0, \dots, m-1.$$

Dann können wir schreiben

$$\hat{y}_{m\ell+r} = \sum_{k=0}^{m-1} \omega_m^{kr} \left( D_p^r y^k \right)_\ell,$$

wobei rechts die Fourier-Transformation der Länge  $p$  steht und  $D_p$  entsprechend zu  $D_m$  erklärt ist. Schreiben wir diese Gleichungen erst für  $r = 0$ , dann für  $r = 1$  usw. hin, dann entsteht

$$\begin{aligned} P_{m,p} \hat{y} &= \begin{pmatrix} W_p D_p^0 y^0 & + & W_p D_p^0 y^1 & + & \dots & + & W_p D_p^0 y^{m-1} \\ W_p D_p^1 y^0 & + & \omega_m W_p D_p^1 y^1 & + & \dots & + & \omega_m^{m-1} W_p D_p^1 y^{m-1} \\ \vdots & & & & & & \\ W_p D_p^{m-1} y^0 & + & W_p D_p^{m-1} y^1 & + & \dots & + & \omega^{(m-1)^2} W_p D_p^{m-1} y^{m-1} \end{pmatrix} \\ &= \begin{pmatrix} W_p & & & \\ & W_p & & \\ & & \ddots & \\ & & & W_p \end{pmatrix} \begin{pmatrix} D_p^0 & & & \\ & D_p^1 & & \\ & & \ddots & \\ & & & D_p^{m-1} \end{pmatrix} * \\ &\quad * \begin{pmatrix} I_p & I_p & \dots & I_p \\ I_p & \omega_n I_p & \dots & \omega_m^{m-1} I_p \\ \vdots & \vdots & \ddots & \vdots \\ I_p & \omega_n^{m-1} I_p & \dots & \omega_m^{(m-1)} I_p \end{pmatrix} \begin{pmatrix} y^0 \\ y^1 \\ \vdots \\ y^{m-1} \end{pmatrix} \end{aligned}$$

oder

$$P_{m,p} W_n = (I_m \otimes W_p) \begin{pmatrix} D_p^0 & & & \\ & D_p^1 & & \\ & & \ddots & \\ & & & D_p^{m-1} \end{pmatrix} (W_m \otimes I_p). \quad (3.2.6)$$

Mit Hilfe von

$$P_{m,p}^T = P_{m,p}^{-1} = P_{p,m} \quad (3.2.7)$$

sieht man, daß (3.2.7) unmittelbar aus (3.2.4) folgt. Durch Transposition von (3.2.7) ergibt sich ja

$$W_n P_{m,p}^T = (W_m \otimes I_p) \begin{pmatrix} D_p^0 & & & \\ & D_p^1 & & \\ & & \dots & \\ & & & D_p^{m-1} \end{pmatrix} (I_n \otimes W_p).$$

Wegen (3.2.7) ist dies identisch zu (3.2.3) mit vertauschten  $m, p$ .

### 3.3 Primfaktoren

Die Good'sche oder Primfaktor-FFT benutzt wie Cooley-Tukey auch eine Faktorisierung  $n = mp$  der Länge  $n$ . Die Faktoren  $m, p$  müssen jetzt aber teilerfremd sein. Wir beginnen mit dem Beispiel  $n = G = 2 \cdot 3$ . Wir schreiben  $W_6$  in der Form

$$W_6 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 4 & 0 & 2 & 4 \\ 0 & 3 & 0 & 3 & 0 & 3 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

d.h. wir notieren an der Stelle  $(k, \ell)$  nicht  $\omega_6^{k\ell} = e^{-2\pi i(k+\ell)/6}$ , sondern nur  $k + \ell \bmod 6$ . Ordnen wir die Zeilen von  $W_6$  in der Reihenfolge 0, 3, 4, 1, 2, 5 und die Spalten in der Reihenfolge 0, 3, 2, 5, 4, 1 an, so entsteht

$$W'_6 = \left( \begin{array}{cc|cc|cc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 3 & 0 & 3 \\ \hline 0 & 0 & 2 & 2 & 4 & 4 \\ 0 & 3 & 2 & 5 & 4 & 1 \\ \hline 0 & 0 & 4 & 4 & 2 & 2 \\ 0 & 3 & 4 & 1 & 2 & 5 \end{array} \right) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Bis auf Zeilen- und Spaltenvertauschungen ist  $W_6$ , also das Tensorprodukt von  $W_3$  und  $W_2$ .  $W_6$  kann also ausgeführt werden durch 3 Fourier - Transformation der Länge 2 und 2 Fourier-Transformation der Länge 3.

**Satz 3.3.1** Sei  $n = n_1 n_2$  und  $\text{ggT}(n_1, n_2) = 1$ . Dann gibt es Permutationsmatrizen  $P, Q$ , so daß

$$W_n = Q^T (W_{n_1} \otimes W_{n_2}) P.$$

**Beweis:** Wegen  $\text{ggt}(n_1, n_2) = 1$  können wir zu  $j$  mit  $0 \leq j < n$  Zahlen  $j_1, j_2$  mit  $0 \leq j_1 < n_1, 0 \leq j_2 < n_2$  finden mit  $j = n_1 j_2 + n_2 j_1 \pmod n$ , und ebenso  $k = n_1 k_2 + n_2 k_1 \pmod n$ . Aus

$$\hat{y}_k = \sum_{j=0}^{n-1} \omega^{jk} y_j, \quad \omega = e^{-2\pi i/n}, \quad k = 0, \dots, n-1$$

wird dann

$$\hat{y}_{n_1 k_2 + n_2 k_1} = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \omega^{(n_1 j_2 + n_2 j_1)(n_1 k_2 + n_2 k_1)} y_{n_1 j_2 + n_2 j_1}.$$

Mit  $\omega^{n_1 n_2} = 1, \omega^{n_1} = e^{-2\pi i/n_2} = \omega_2, \omega^{n_2} = e^{-2\pi i/n_1} = \omega_1$  folgt

$$\hat{y}_{n_1 k_2 + n_2 k_1} = \sum_{j_1=0}^{n_1-1} \omega_1^{n_2 j_1 k_1} \sum_{j_2=0}^{n_2-1} \omega_2^{n_1 j_2 k_2} y_{n_1 j_2 + n_2 j_1}.$$

Hier ist  $0 \leq k_1 < n_1, 0 \leq k_2 < n_2$ . Zu jedem solchen Paar  $k_1, k_2$  können wir genau ein Paar  $(k'_1, k'_2)$  finden, so daß

$$n_1 k'_2 \equiv k_2 \pmod{n_2}, \quad n_2 k'_1 \equiv k_1 \pmod{n_1}, \quad (3.3.1)$$

denn  $\text{ggt}(n_1, n_2) = 1$ . Mit diesen Zahlen  $k'_1, k'_2$  gilt dann

$$\hat{y}_{n_1 k'_2 + n_2 k'_1} = \sum_{j_1=0}^{n_1-1} \omega_1^{n_2 j_1 k'_1} \sum_{j_2=0}^{n_2-1} \omega_2^{n_1 j_2 k'_2} y_{n_1 j_2 + n_2 j_1}.$$

Aufgrund der Wahl von  $k'_1, k'_2$  und wegen  $\omega_1^{n_1} = \omega_2^{n_2} = 1$  gilt

$$\omega_1^{n_2 k'_1} = \omega_1^{k_1}, \quad \omega_2^{n_1 k'_2} = \omega_2^{k_2},$$

also

$$\hat{y}_{n_1 k'_2 + n_2 k'_1} = \sum_{j_1=0}^{n_1-1} \omega_1^{j_1 k_1} \sum_{j_2=0}^{n_2-1} \omega_2^{j_2 k_2} y_{n_1 j_2 + n_2 j_1}.$$

Mit den  $n_2$ -Vektoren

$$\begin{aligned} y^{j_1} &= (y_{n_1 j_2 + n_2 j_1})_{0 \leq j_2 < n_2}, \\ \hat{y}^{k_1} &= (\hat{y}_{n_1 k'_2 + n_2 k'_1})_{0 \leq k_2 < n_2} \end{aligned}$$

lautet dies mit  $W_2 = W_{n_2}$

$$(\hat{y}^{k_1})_{k_2} = \sum_{j_1=0}^{n_1-1} \omega_1^{j_1 k_1} (W_2 y^{j_1})_{k_2}$$

oder

$$\begin{pmatrix} \hat{y}^0 \\ \vdots \\ \hat{y}^{n_1-1} \end{pmatrix} = \begin{pmatrix} W_2 & W_2 & \cdots & W_2 \\ W_2 & \omega_1 W_2 & \cdots & \omega_1^{n_1-1} W_2 \\ \vdots & \vdots & \ddots & \vdots \\ W_2 & \omega_1^{n_1-1} W_2 & \cdots & \omega_1^{(n_1-1)^2} W_2 \end{pmatrix} \begin{pmatrix} y^0 \\ \vdots \\ y^{n_1-1} \end{pmatrix}.$$

Also, mit  $W_1 = W_{n_1}$ ,

$$Q\hat{y} = W_1 \otimes W_2 P y,$$

und dies ist die Behauptung. □

Dem Beweis kann man die Permutationen  $P, Q$  entnehmen. Es ist mit  $j = n_2 j_1 + j_2$ ,  $0 \leq j_2 < n_2$  (Division mit Rest)

$$(P y)_j = y_{n_1 j_2 + n_2 j_1}.$$

Entsprechend ist mit  $k = n_2 k_1 + k_2$ ,  $0 \leq k_2 < n_2$ ,

$$(Q \hat{y})_k = \hat{y}_{n_1 k'_2 + n_2 k'_1}.$$

Dabei sind  $k'_1, k'_2$  zu  $k_1, k_2$  gemäß (3.3.1) bestimmt. In jedem Fall ist in den Indizes mod  $n$  zu rechnen.

**Beispiel:**  $n = 2 \cdot 3$ , also  $n_1 = 2, n_2 = 3$ . Wir berechnen  $P$

$$\begin{array}{cccc} j & j_1 & j_2 & n_1 j_2 + n_2 j_1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 4 \\ 3 & 1 & 0 & 3 \\ 4 & 1 & 1 & 5 \\ 5 & 1 & 2 & 1 \end{array}, \quad \text{also } P \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 4 \\ 3 \\ 5 \\ 1 \end{pmatrix}$$

und  $Q$

$$\begin{array}{cccccc}
 k & k_1 & k_2 & k'_1 & k'_2 & n_1 k'_2 + n_2 k'_1 \\
 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 0 & 1 & 0 & 2 & 4 \\
 2 & 0 & 2 & 0 & 1 & 2 \\
 3 & 1 & 0 & 1 & 0 & 3 \\
 4 & 1 & 1 & 1 & 2 & 1 \\
 5 & 1 & 2 & 1 & 1 & 5
 \end{array}
 , \quad \text{also } Q \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 2 \\ 3 \\ 1 \\ 5 \end{pmatrix} .$$

Wir bilden  $QW_6P^T$ , d.h. wir vertauschen die Zeilen gemäß  $Q$  und die Spalten gemäß  $P$ :

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 4 & 0 & 2 & 4 \\ 0 & 3 & 0 & 3 & 0 & 3 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \xrightarrow{Q} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ 0 & 2 & 4 & 0 & 2 & 4 \\ 0 & 3 & 0 & 3 & 0 & 3 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \xrightarrow{P} \left( \begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 & 2 & 4 \\ 0 & 4 & 2 & 0 & 4 & 2 \\ \hline 0 & 0 & 0 & 3 & 3 & 3 \\ 0 & 2 & 4 & 3 & 5 & 1 \\ 0 & 4 & 2 & 3 & 1 & 5 \end{array} \right) = W_2 \otimes W_3$$

Oben haben wir schon den Fall  $n_1 = 3, n_2 = 2$  behandelt.

**Folgerung:** Seien  $M(n), A(n)$  die Anzahl der Multiplikationen bzw. Additionen zur Fourier-Transformation der Länge  $n$ . Sei  $n = n_1 n_2$  mit  $\text{ggT}(n_1, n_2) = 1$ . Dann gilt

$$\begin{aligned}
 M(n) &= n_1 M(n_2) + n_2 M(n_1) \\
 A(n) &= n_1 A(n_2) + n_2 A(n_1)
 \end{aligned}$$

Wir wollen die entsprechenden Überlegungen nun für die Faltung der Länge  $n$ , also

$$z_k = \sum_{j=0}^{n-1} x_{k-j} y_j, \quad k = 0, \dots, n-1 \quad (3.3.2)$$

durchführen. Äquivalent hierzu ist die Anwendung der Matrix

$$X_n = \begin{pmatrix} x_0 & x_{n-1} & \cdots & x_1 \\ x_1 & x_0 & x_{n-1} & \cdots & x_2 \\ \vdots & & & & \\ x_{n-1} & x_{n-2} & \cdots & & x_0 \end{pmatrix}$$

auf den Vektor  $y$ .

**Satz 3.3.2** Sei  $n = n_1, n_2$  und  $\text{ggT}(n_1, n_2) = 1$ . Dann gibt es eine Permutationsmatrix  $P$  und Faltungen  $F_0, \dots, F_{n_1-1}$  der Länge  $n_2$ , so daß

$$X_n = P^T \begin{pmatrix} F_0 & F_{n_1-1} & \cdots & F_1 \\ F_1 & F_0 & F_{n_1-1} & \cdots & F_2 \\ \vdots & & & & \\ F_{n_1-1} & F_{n_1-1} & \cdots & & F_0 \end{pmatrix} P.$$

**Beweis:** Für  $0 \leq k, j < n$  können wir mod  $n$

$$\begin{aligned} k &= k_2 n_1 + k_1 n_2, & j &= j_2 n_1 + j_1 n_2, \\ 0 \leq j_1, k_1 &< n_1, & 0 \leq j_2, k_2 &< n_2 \end{aligned}$$

schreiben, und zwar in eindeutiger Weise. Damit lautet (3.3.1)

$$z_{k_2 n_1 + k_1 n_2} = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} x_{(k_1-j_1)n_2 + (k_2-j_2)n_2} y_{j_1 n_2 + j_2 n_1}.$$

Dabei wird in den Indizes mod  $n$  gerechnet. Die  $j_2$ -Summe ist eine Faltung der  $n_2$ -Vektoren

$$y^{j_1} = (y_{j_1 n_2 + j_2 n_1})_{0 \leq j_2 < n_2}, \quad f^{k_1-j_1} = (x_{(k_1-j_1)n_2 + j_2 n_1})_{0 \leq k_2 < n_2}.$$

Mit dem  $n_2$ -Vektor

$$z^{k_1} = (z_{k_2 n_1 + k_1 n_2})_{0 \leq k_2 < n_2}$$

können wir daher schreiben

$$\begin{pmatrix} z^0 \\ \vdots \\ z^{n_1-1} \end{pmatrix} = \begin{pmatrix} F_0 & F_{n_1-1} & \cdots & F_1 \\ F_1 & F_0 & F_{n_1-1} & \cdots & F_2 \\ \cdots & & & & \\ F_{n_1-1} & F_{n_1-2} & \cdots & & F_0 \end{pmatrix} \begin{pmatrix} y^0 \\ \vdots \\ y^{n_1-1} \end{pmatrix}.$$

Dies ist die Behauptung. □

Der Beweis ergibt eine explizite Darstellung für  $P$ . Setzen wir für  $0 \leq j < n$   $j = j_1 n_2 + j_2$ ,  $0 \leq j_1 < n_1$ ,  $0 \leq j_2 < n_2$ , so ist

$$(Py)_j = y_{j_1 n_2 + j_2 n_1}.$$

**Beispiel:**  $n = 2 \cdot 3$ , also  $n_1 = 2$ ,  $n_2 = 3$ .  $P$  bewirkt die Permutation  $(0, 1, 2, 3, 4, 5) \rightarrow (0, 2, 4, 3, 5, 1)$ . Entsprechende Vertauschungen von Zeilen und Spalten ergibt

$$\begin{aligned} & \begin{pmatrix} 0 & 5 & 4 & 3 & 2 & 1 \\ 1 & 0 & 5 & 4 & 3 & 2 \\ 2 & 1 & 0 & 5 & 4 & 3 \\ 3 & 2 & 1 & 0 & 5 & 4 \\ 4 & 3 & 2 & 1 & 0 & 5 \\ 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 5 & 4 & 3 & 2 & 1 \\ 2 & 1 & 0 & 5 & 4 & 3 \\ 4 & 3 & 2 & 1 & 0 & 5 \\ 3 & 2 & 1 & 0 & 5 & 4 \\ 5 & 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 5 & 4 & 3 & 2 \end{pmatrix} \rightarrow \left( \begin{array}{ccc|ccc} 0 & 4 & 2 & 3 & 1 & 5 \\ 2 & 0 & 4 & 5 & 3 & 1 \\ 4 & 2 & 0 & 1 & 5 & 3 \\ \hline 3 & 1 & 5 & 0 & 4 & 2 \\ 5 & 3 & 1 & 2 & 0 & 4 \\ 1 & 5 & 3 & 4 & 2 & 0 \end{array} \right) \\ & = \begin{pmatrix} F^0 & F^1 \\ F^1 & F^0 \end{pmatrix} \end{aligned}$$

mit Faltungen  $F^\ell$  der Länge 3.

**Folgerung:** Sei  $n = n_1 n_2$  mit  $\text{ggT}(n_1, n_2) = 1$ . Seien  $M(n)$ ,  $A(n)$  die Anzahl der Multiplikationen bzw.  $A(n)$  der Länge  $n$ . Dann gilt

$$\begin{aligned} M(n) &= M(n_1)M(n_2) \\ A(n) &= M(n_1)A(n_2) + n_2 A(n_1) \end{aligned}$$

(Algorithmus von Cooley und Agarwal).

### 3.4 Schnelle Faltung nach Winograd

Wir benutzen nun den Chinesischen Restsatz, um Faltungen schnell auszuführen. Wir wissen, daß wir Faltungen der Länge  $n$  als Multiplikation von Polynomen in  $F[z]$  modulo  $p = z^n - 1$  auffassen können. Es ist ja mod  $p$

$$\begin{aligned} \sum_{k=0}^{n-1} x_k z^k \sum_{\ell=0}^{n-1} y_\ell z^\ell &= \sum_{j=0}^{n-1} \left( \sum_{\ell=0}^j x_{j-\ell} y_\ell \right) z^j + \sum_{j=n}^{2n-2} \left( \sum_{\ell=j-n+1}^{n-1} x_{j-\ell} y_\ell \right) z^j \\ &= \sum_{j=0}^{n-1} \left( \sum_{\ell=0}^j x_{j-\ell} y_\ell + \sum_{\ell=j+1}^{n-1} x_{j-\ell} y_\ell \right) z^j = \sum_{j=0}^{n-1} (x * y)_j z^j, \end{aligned}$$

wenn wir im Index mod  $n$  rechnen.

Ist nun  $p = p_1 p_2$  mit teilerfremden  $p_1, p_2$ , so haben wir nach Satz 2.3.4

$$F[z]/p = F[z]/p_1 \oplus F[z]/p_2 .$$

Dieser Isomorphismus ist leicht hergestellt. Nach Satz 2.3.4 gibt es Polynome  $q_1, q_2$  mit  $q_2 p_1 + q_1 p_2 = 1$ . Also gilt für  $f \in F[z]$  die Beziehung  $q_2 p_1 f + q_1 p_2 f = f$ . Wir definieren nun die Abbildung  $\varphi : F[z]/p \rightarrow F[z]/p_1 \oplus F[z]/p_2$  durch

$$\varphi(f) = (q_1 f, q_2 f) .$$

Dies ist offenbar der gesuchte Isomorphismus. Die Multiplikation zweier Polynome  $f, g$  modulo  $p$  wird nun so ausgeführt: Zunächst ist

$$fg = q_2 p_1 fg + q_1 p_2 fg$$

oder, modulo  $p$  gerechnet,

$$fg = q_2 p_1 (fg \bmod p_2) + q_1 p_2 (fg \bmod p_1) . \quad (3.4.1)$$

Es genügt also, die Multiplikation mod  $p_1$  und mod  $p_2$  auszuführen. Dann läßt sich  $fg \bmod p$  leicht berechnen.

Wir betrachten zunächst den Fall  $n = 2$ . Hier ist  $p_1 = z - 1$ ,  $p_2 = z + 1$ , und wir haben

$$-\frac{1}{2}(z - 1) + \frac{1}{2}(z + 1) = 1 ,$$

also  $q_1 = +\frac{1}{2}$ ,  $q_2 = -\frac{1}{2}$ . Sei  $f = x_0 + x_1z$ ,  $g = y_0 + y_1z$  und  $fg = w_0 + w_1z \pmod{(z^2 - 1)}$ , also  $w_0 = x_0y_0 + x_1y_1$ ,  $w_1 = x_0y_1 + y_1x_0$ .

Wir führen die Multiplikation  $fg \pmod{p_1}$  und  $\pmod{p_2}$  durch. Es ist

$$\begin{aligned} fg \pmod{(z - 1)} &= (fg)(1) = f(1)g(1) = (x_0 + x_1)(y_0 + y_1) , \\ fg \pmod{(z + 1)} &= (fg)(-1) = f(-1)g(-1) = (x_0 - x_1)(y_0 - y_1) . \end{aligned}$$

Nach (3.4.1) haben wir also  $\pmod{(z^2 - 1)}$

$$fg = -\frac{1}{2}(z - 1)(x_0 - x_1)(y_0 - y_1) + \frac{1}{2}(z + 1)(x_0 + x_1)(y_0 + y_1) .$$

Dies liefert den folgenden Algorithmus zur Faltung der Länge 2:

$$\begin{aligned} s_1 &= y_0 + y_1 & , & & s_2 &= y_0 - y_1 \\ m_1 &= \frac{x_0 + x_1}{2} s_1 & , & & m_2 &= \frac{x_0 - x_1}{2} s_2 & (3.4.2) \\ w_0 &= m_1 + m_2 & , & & w_1 &= m_1 - m_2 \end{aligned}$$

Zur Feststellung des Rechenaufwandes legen wir nun fest: Es zählen nicht die Rechnungen, die man auf den Koeffizienten  $x_i$  ausführt. Man stellt sich dazu vor, daß die  $x_i$  ein für allemal gewählt sind, so daß diese Rechnungen ein für allemal durchgeführt werden können. Bei dieser Zählweise erfordert (3.4.2) nur 4 Additionen und zwei Multiplikationen, im Gegensatz zu den 4 Multiplikationen und zwei Additionen der Schulmethode für die Faltung der Länge 2.

Nun zum Fall  $n = 3$ . Hier haben wir  $z^3 - 1 = (z^2 + z + 1)(z - 1)$ , also  $p_1 = z - 1$ ,  $p_2 = z^2 + z + 1$ . Die Polynome  $q_1$ ,  $q_2$  werden durch Division mit Rest berechnet. Es ist

$$\begin{aligned} p_2 : p_1 &= z^2 + z + 1 : z - 1 = z + z \\ &\quad \frac{z^2 - z}{2z + 1} \\ &\quad \frac{2z - 2}{3} \end{aligned}$$

also

$$z^2 + z + 1 = (z - 1)(z + 2) + 3$$

und daher

$$-\frac{z+2}{3}(z-1) + \frac{1}{3}(z^2+z+1) = 1.$$

Dieser Beziehung entnehmen wir  $q_2 = -(z+2)/3$ ,  $q_1 = 1/3$ . Seien wieder  $f = x_0 + x_1z + x_2z^2$ ,  $g = y_0 + y_1z + y_2z^2$  und  $fg \bmod (z^3 - 1) = w_0 + w_1z + w_2z^2$ . Die Berechnung von  $fg \bmod (z-1)$  und  $\bmod(z^2+z+1)$  ergibt nun

$$\begin{aligned} fg \bmod (z-1) &= (fg)(1) = f(1)g(1) = (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) \\ fg \bmod (z^2 + z + 1) &= f \bmod(z^2 + z + 1) \cdot g \bmod (z^2 + z + 1) \\ &= (x_0 + x_1z - x_2(1+z))(y_0 + y_1z - y_2(1+z)) \\ &= (x_0 - x_2 + (x_1 - x_2)z)(y_0 - y_2 + (y_1 - y_2)z) \\ &= (x_0 - x_2)(y_0 - y_2) + ((x_1 - x_2)(y_0 - y_2) \\ &\quad + (x_0 - x_2)(y_1 - y_2))z - (x_1 - x_2)(y_1 - y_2)(1+z) \\ &= (x_0 - x_2)(y_0 - y_2) - (x_1 - x_2)(y_1 - y_2) \\ &\quad + ((x_1 - x_2)(y_0 - y_2) + (x_0 - x_2)(y_1 - y_2) \\ &\quad - (x_1 - x_2)(y_1 - y_2))z \\ &= m'_1 - m'_2 + (m'_1 - m'_3)z, \end{aligned}$$

$$m'_1 = (x_0 - x_2)(y_0 - y_2),$$

$$m'_2 = (x_1 - x_2)(y_1 - y_2),$$

$$m'_3 = (x_0 - x_1)(y_0 - y_1).$$

Wir setzen auch noch

$$m'_0 = (x_0 + x_1 + x_2)(y_0 + y_1 + y_2).$$

Zusammensetzen dieser Resultate mittels (3.4.1) ergibt

$$\begin{aligned} fg \bmod (z^3 - 1) &= -\frac{z+2}{3}(z-1)(fg \bmod (z^2 + z + 1)) \\ &\quad + \frac{1}{3}(z^2 + z + 1)fg \bmod z - 1 \\ &= -\frac{z+2}{3}(z-1)(m'_1 - m'_2 + (m'_1 - m'_3)z) \\ &\quad + \frac{1}{3}(z^2 + z + 1)(x_0 + x_1 + x_2)(y_0 + y_1 + y_2) \\ &= \frac{2}{3}(m'_1 - m'_2) + (-\frac{1}{3}(m'_1 - m'_2) + \frac{2}{3}(m_1 - m'_3) + \frac{1}{3}m'_0)z \\ &\quad + (-\frac{1}{3}(m'_1 - m'_2) - \frac{1}{3}(m'_1 - m'_3) + \frac{1}{3}m_0)z^2 - \frac{1}{3}(m'_1 - m'_3)z^3. \end{aligned}$$

Dies ergibt den Algorithmus

$$\begin{aligned}
 s_0 &= y_0 + y_1 + y_2, & s_1 &= y_0 - y_2, & s_2 &= y_1 - y_2, & s_3 &= y_0 - y_1, \\
 m_0 &= \frac{x_0 + x_1 x_2}{3} s_0, & m_1 &= \frac{x_0 - x_2}{3} s_1, & m_2 &= \frac{x_1 - x_2}{3} s_2, & m_3 &= \frac{x_0 - x_1}{3} s_3 \\
 w_0 &= m_0 + m_1 - 2m_2 + m_3, & w_1 &= m_0 + m_1 + m_2 - 2m_3, & w_2 &= m_0 - 2m_1 + m_2 + m_3.
 \end{aligned} \tag{3.4.3}$$

Er benötigt 4 Multiplikationen und 17 Additionen (Multiplikationen mit 2 werden durch Additionen realisiert). Die Anzahl der Multiplikationen hat sich gegenüber der Schulmethode für die Faltung der Länge 3 also gewaltig reduziert (von 9 auf 4). Die Anzahl der Additionen ist noch nicht endgültig.

Zur Reduzierung der Anzahl der Additionen führen wir nun das Hilfsmittel der Transposition ein. Es seien  $t$  Bilinearformen

$$w_k = \sum_{i=1}^s \sum_{j=1}^r a_{ijk} x_i y_j, \quad k = 1, \dots, t \tag{3.4.4}$$

auszuwerten. Dafür stehe ein Algorithmus der Form

$$w_k = \sum_{\ell=1}^m \gamma_{\ell k} \left( \frac{1}{f_\ell} \sum_{i=1}^s \alpha_{\ell i} x_i \right) \left( \sum_{j=1}^r \beta_{\ell j} y_j \right) \tag{3.4.5}$$

zur Verfügung mit ganzen Zahlen  $\gamma_{\ell k}, f_\ell, \alpha_{\ell i}, \beta_{\ell j}$ . Zur Zählung der Operationen in (3.4.3) machen wir folgende Konventionen:

- (a) Operationen auf den  $x_i$  werden nicht gezählt. Man stellt sich vor, daß die  $x_i$  immer die gleichen sind, so daß

$$\frac{1}{f_\ell} \sum_{i=1}^s \alpha_{\ell i} x_i, \quad \ell = 1, \dots, m$$

vorberechnet werden kann.

- (b) Die Multiplikationen mit  $\gamma_{\ell k}, \beta_{\ell j}$  werden durch Additionen realisiert.

So gezählt benötigt (3.4.5)  $m$  Multiplikationen.

Faltungen mit festem  $x$  und Fourier-Transformationen sind Beispiele für (3.4.4). Die oben gefundenen Algorithmen für die Faltungen der Länge 2 und 3 sind Beispiele für (3.4.5).

Unter dem zu (3.4.4) transponierten System von Bilinearformen verstehen wir das System

$$\sum_{k=1}^t \sum_{j=1}^r a_{ijk} z_k y_j \quad , \quad i = 1, \dots, s. \quad (3.4.6)$$

Wir erhalten das transponierte System aus (3.4.4), indem wir die  $k$ -te Gleichung (3.4.4) mit  $z_k$  multiplizieren, über  $k$  summieren, und die Koeffizienten der  $x_i$  betrachten.

Wir wollen zeigen, daß (3.4.5) auch einen Algorithmus zur Auswertung des transponierten Systems (3.4.6) liefert, der ebenfalls mit  $m$  Multiplikationen auskommt. Dazu multiplizieren wir (3.4.6) mit  $x_i$  und summieren über  $i$ . Mit (3.4.5) ergibt sich

$$\begin{aligned} \sum_{i=1}^s x_i \sum_{k=1}^t \sum_{j=1}^r a_{ijk} z_k y_j &= \sum_{k=1}^t z_k \sum_{i=1}^s \sum_{j=1}^r a_{ijk} x_i y_j \\ &= \sum_{k=1}^t z_k \sum_{\ell=1}^m \gamma_{\ell k} \left( \frac{1}{f_{\ell}} \sum_{i=1}^s \alpha_{\ell i} x_i \right) \left( \sum_{j=1}^r \beta_{\ell j} y_j \right) \\ &= \sum_{i=1}^s x_i \sum_{\ell=1}^m \alpha_{\ell i} \left( \frac{1}{f_{\ell}} \sum_{k=1}^t \gamma_{\ell k} z_k \right) \left( \sum_{j=1}^r \beta_{\ell j} y_j \right). \end{aligned}$$

Vergleichen wir den Koeffizienten von  $x_i$ , so erhalten wir

$$\sum_{k=1}^t \sum_{j=1}^r a_{ijk} z_k y_j = \sum_{\ell=1}^m \alpha_{\ell i} \left( \frac{1}{f_{\ell}} \sum_{k=1}^t \gamma_{\ell k} z_k \right) \left( \sum_{j=1}^r \beta_{\ell j} y_j \right). \quad (3.4.7)$$

Dies ist ein Algorithmus zur Auswertung des transponierten Systems (3.4.6) mit  $m$  Multiplikationen.

Wir wenden die Transposition an auf die Faltung

$$w_k = \sum_{i=0}^{n-1} x_{i-k} y_k \quad , \quad k = 0, \dots, n-1 .$$

Das dazu transponierte System ist

$$w'_i = \sum_{k=0}^{n-1} y_{k-i} z_k \quad , \quad i = 0, \dots, n-1 ,$$

und dies ist auch eine Faltung. (3.4.7) ist also wieder ein Algorithmus zur Faltung mit  $m$  Multiplikationen, aber einer anderen (und hoffentlich geringeren) Anzahl von Additionen.

Wir führen die Transposition durch für den Algorithmus (3.4.3) zur Faltung der Länge 3. Die Koeffizienten  $f_\ell, \gamma_{\ell k}, \alpha_{\ell i}, \beta_{\ell j}$  sind in folgendem Schema zusammengestellt:

$f$	$\gamma$			$\alpha$			$\beta$		
3	1	1	1	1	1	1	1	1	1
3	1	1	-2	1	0	-1	1	0	-1
3	-2	1	1	0	1	-1	0	1	-1
3	1	-2	1	1	-1	0	1	-1	0
	$w_0$	$w_1$	$w_2$	$x_0$	$x_1$	$x_2$	$y_0$	$y_1$	$y_2$

Die Anwendung von  $\alpha$  und  $\beta$  zeilenweise erfordert jeweils 5 Additionen, die Anwendung von  $\gamma$  spaltenweise aber 12 (Multiplikation mit 2 wird durch Addition realisiert). In dieser Form benötigt der Algorithmus also 17 Additionen. Bei der Transposition wird  $\alpha$  mit  $\gamma$  vertauscht, während  $\beta$  unverändert bleibt.

Die Anwendung von  $\beta$  (zeilenweise) erfordert nach wie vor 5 Additionen, die Anwendung von  $\alpha$  (spaltenweise) aber nur noch 6 Additionen. Der transponierte Algorithmus (3.4.7) kommt also mit 11 (statt 17) Additionen und 5 Multiplikationen aus. Er lautet:

$$s_0 = y_0 + y_1 + y_2 \quad , \quad s_1 = y_0 - y_2 \quad , \quad s_2 = y_1 - y_2 \quad , \quad s_3 = y_0 - y_1 \quad ,$$

$$\begin{aligned}
m_0 &= \frac{z_0 + z_1 + z_2}{3} s_0 \quad , \quad m_1 = \frac{z_0 + z_1 - 2z_2}{3} s_1 \quad , \\
m_2 &= \frac{-2z_0 + z_1 + z_2}{3} \quad , \quad m_3 = \frac{z_0 - 2z_1 + z_2}{3} \quad (3.4.8) \\
w'_0 &= m_0 + m_1 + m_3 \quad , \quad w'_1 = m_0 + m_1 - m_3 \quad , \quad w'_2 = m_0 - m_1 - m_2 \quad .
\end{aligned}$$

Die Winograd-Faltung versucht mit möglichst wenig Multiplikationen auszukommen. Wir wollen eine Aussage über die benötigten Multiplikationen für Faltungen beliebiger Länge herleiten. Sie gilt für einen beliebigen Körper  $F$  der Charakteristik 0, also z.B.  $F = \mathbb{R}, \mathbb{C}$ . Die Kreisteilungspolynome  $\phi_d$  (siehe z.B. Fischer/Sacher: Einführung in die Algebra, S. 172 ff.) in einem solchen Körper sind Polynome mit der Eigenschaft

$$x^n - 1 = \prod_{d|n} \phi_d(x) .$$

Ihre Anzahl  $k$  entspricht also der Anzahl der Teiler von  $n$  (einschließlich 1,  $n$ ). Eine kleine Liste von Kreisteilungspolynomen ist

$$\begin{aligned}
\phi_1 &= x - 1 \\
\phi_2 &= x + 1 \\
\phi_3 &= x^2 + x + 1 \\
\phi_4 &= x^2 + 1 \\
\phi_5 &= x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

Sie haben folgende Eigenschaften:

- (i)  $\phi_d$  hat nur ganzzahlige Koeffizienten
- (ii)  $\phi_d$  ist irreduzibel
- (iii)  $\phi_d, \phi_{d'}$  sind für  $d \neq d'$  teilerfremd.

**Satz 3.4.1** *Sei  $F$  ein Körper der Charakteristik 0 und  $k$  die Anzahl der Teiler von  $n$ , welche  $\leq n$  sind (1 und  $n$  eingeschlossen). Dann kann man die Faltung der Länge  $n$  in  $F$  mit  $2n - k$  Multiplikationen ausführen (Vorberechnungen auf einem der Faktoren werden nicht gezählt).*

**Beweis:** Seien  $p_1, \dots, p_k$  die Kreisteilungspolynome zu  $n$ , also

$$x^n - 1 = p_1 p_2 \cdots p_n .$$

Sei  $P_2 = p_2 \cdots p_k$ . Wir wenden den Chinesischen Restsatz an und bestimmen  $q_1, q_2 \in F[z]$ , so daß

$$1 = q_2 p_1 + q_1 P_2 .$$

Dann ist wie oben für  $f, g \in F[z]$

$$\begin{aligned} fg \bmod (z^n - 1) &= q_2 p_1 ((fg) \bmod P_2) + q_1 P_2 ((fg) \bmod p_1) \\ &= q_2 p_1 (f \bmod P_2)(g \bmod P_2) + q_1 P_2 (f \bmod p_1)(g \bmod p_1) . \end{aligned}$$

Da  $p_1, P_2$  nur ganzzahlige Koeffizienten haben, können  $f$  und  $g \bmod P_2$  bzw.  $\bmod p_1$  durch Additionen berechnet werden. Die Multiplikation zweier Polynome  $q, f$  vom Grade  $k, \ell$  kann mit  $k + \ell + 1$  Multiplikationen ausgeführt werden. man braucht ja nur  $k + \ell + 1$  paarweise verschiedene Punkte  $z_0, \dots, z_{k+\ell}$  aus dem Primkörper von  $F$  zu wählen und für  $fg$  die Lagrange'sche Interpolationsformel hinzuschreiben, also

$$(fg)(z) = \sum_{j=0}^{\ell+k} \omega_j(z) f(z_j) g(z_j) , \quad \omega_j(z) = \prod_{\substack{i=0 \\ i \neq j}}^{k+\ell} \frac{z - z_i}{z_j - z_i} .$$

Da die  $\omega_j$  Koeffizienten aus dem Primkörper von  $F$  haben, können die Koeffizienten von  $fg$  durch Addition berechnet werden, sobald die  $k + \ell + 1$  Produkte  $f(z_j)g(z_j)$  bekannt sind. Also kann  $fg$  tatsächlich mit  $k + \ell + 1$  Multiplikationen berechnet werden.

Sei nun  $M(p)$  die Anzahl der Multiplikationen für die Berechnung von  $fg \bmod p$ , wobei  $p$  irgendein Polynom über dem Primkörper von  $F$  ist. Nach dem Chinesischen Restsatz gilt dann

$$\begin{aligned} M(x^n - 1) &= M(p_1) + M(P_2) \\ &= M(p_1) + M(p_2) + \cdots + M(p_k) . \end{aligned}$$

Wir haben gerade gesehen, daß  $M(p) = 2 \text{ Grad}(p) - 1$ . Also folgt

$$M(x^n - 1) = \sum_{i=1}^k (2 \text{ Grad}(p_i) - 1) = 2n - k .$$

□

### 3.5 Die schnelle Fourier–Transformation nach Winograd

Winograd führt die Fourier-Transformation auf Faltungen zurück. Dazu definieren wir zunächst die Faltung auf einer beliebigen Gruppe  $G$ . Sei  $|G| = n$ , und seien  $x, y \in \mathbb{C}^n$ . Wir interpretieren  $x, y$  als Funktionen auf  $G$ , schreiben also  $x = (x_s)_{s \in G}$ ,  $y = (y_s)_{s \in G}$ . Die Faltung  $z = x * y$  ist dann eine ebensolche Funktion auf  $G$ , und zwar ist

$$\begin{aligned} z_g &= \sum_{\substack{s,t \in G \\ ts=g}} x_s y_t = \sum_{t \in G} x_{t^{-1}g} y_t, \\ &= \sum_{t \in G} x_{tg} y_{t^{-1}}. \end{aligned}$$

In Matrix-Form schreibt sich dies

$$z = X P y \quad , \quad X = (x_{tg})_{g,t \in G}$$

mit einer Permutationsmatrix  $P$ . Anders ausgedrückt: Eine Faltung auf  $G$  wird durch eine Matrix beschrieben, in der die  $n$  Komponenten des Vektors  $x$  entsprechend der Gruppentafel von  $G$  angeordnet sind.

Nun zur Fourier-Transformation  $W_n$  der Länge  $n$ , also

$$W_n = (\omega^{k\ell})_{k,\ell=0,\dots,n-1} \quad , \quad \omega = e^{-2\pi i/n}.$$

Wegen  $\omega_n^n = 1$  kann man die Produkte im Exponenten mod  $n$  berechnen. Streicht man aus  $W_n$  die Zeilen und Spalten  $k$  mit  $k = 0$  oder  $k|n$ , so bleibt übrig eine  $(\varphi(n), \varphi(n))$ -Matrix  $\tilde{W}_n$  ( $\varphi$  ist die Euler'sche  $\varphi$ -Funktion, vgl. 2.4), in welcher die  $\varphi(n)$  Elemente  $\omega^k$ ,  $0 \leq k < n-1$ ,  $k \neq 0$  und  $\text{ggT}(n, k) = 1$  entsprechend der Gruppentafel von  $M_n$  angeordnet sind.

Wir haben eben gesehen, daß eine solche Matrix nichts anderes als eine Faltung auf  $M_n$  darstellt. Ein großer Teil der zur Anwendung von  $W_n$  notwendigen Rechenoperationen kann also als Faltung auf  $M_n$  ausgeführt werden.

### 3.5. DIE SCHNELLE FOURIER-TRANSFORMATION NACH WINOGRAD65

Aus Satz 2.4.3 wissen wir, daß  $M_n$  für  $n = p^r$ ,  $p > 2$ ,  $r > 1$  zyklisch ist. Dann ist also  $\tilde{W}_n$  sogar eine Faltung auf  $C_n$ , und diese können nach den Methoden aus §4 schnell ausgeführt werden. Diese Art der schnellen Fourier-Transformation wird auch Rader FFT genannt. Wir führen dies nun für einige Beispiele durch.

Beginnen wir mit  $n = 3$ . Nach Satz 2.4.3 ist  $M_3 \cong C_2$ . In der Tat sind in

$$W_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \omega = e^{-2\pi i/3}$$

die beiden letzten Zeilen und Spalten eine Faltung der Länge 2. Diese können wir mit 2 Multiplikationen und 4 Additionen ausführen, dazu kommen dann nach 4 Additionen in Zeile und Spalte 0. Von den acht Additionen kann man noch zwei einsparen, wenn man

$$\begin{pmatrix} \hat{y}_1 - \hat{y}_0 \\ \hat{y}_2 - \hat{y}_0 \end{pmatrix} = \begin{pmatrix} \omega - 1 & \omega^2 - 1 \\ \omega^2 - 1 & \omega - 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

schreibt. Ausführung dieser Faltung mit schnellem Algorithmus ergibt

$$\begin{aligned} \hat{y}_1 - \hat{y}_0 &= \frac{\omega + \omega^2 - 2}{2}(y_1 + y_2) + \frac{\omega - \omega^2}{2}(y_2 - y_1) \\ \hat{y}_2 - \hat{y}_0 &= \frac{\omega + \omega^2 - 2}{2}(y_1 + y_2) - \frac{\omega - \omega^2}{2}(y_1 - y_2) \end{aligned}$$

Damit kommen wir zu folgendem Algorithmus mit 2 Multiplikationen und 6 Additionen:

$$\begin{aligned} s_1 &= y_1 + y_2 & , & & s_2 &= y_1 - y_2 \\ m_1 &= \frac{\omega + \omega^2 - 2}{2}s_1, & m_2 &= \frac{\omega - \omega^2}{2}s_2 & & (3.5.1) \\ \hat{y}_0 &= y_0 + s_1 & , & & s_3 &= \hat{y}_0 + m_1 \\ \hat{y}_1 &= s_3 - m_2 & , & & \hat{y}_2 &= s_3 + m_2 . \end{aligned}$$

Wir bemerken, daß

$$\begin{aligned} \frac{\omega + \omega^2 - 2}{2} &= \frac{\omega + \bar{\omega} - 2}{2} = \cos(2\pi/3) - 1 \\ \frac{\omega - \omega^2}{2} &= \frac{\omega - \bar{\omega}}{2} = i \sin(2\pi/3) \end{aligned}$$

reell bzw. rein imaginär sind, so daß sich die beiden Multiplikationen von (3.5.1) in insgesamt 4 reellen Multiplikationen ausführen lassen.

Im Falle  $n = 4$  haben wir nach Satz 2.4.3  $M_4 = \{1, 3\} = C_2$ . Die entsprechende Umordnung von  $W_4$  ist

	0	2	1	3
0	1	1	1	1
2	1	1	-1	-1
1	1	-1	$i$	$-i$
3	1	-1	$-i$	$i$

Ein schneller Algorithmus ist

$$s_2 = y_0 + y_2 \quad s_1 = y_1 + y_3 \quad , \quad s_2 = y_0 - y_2 \quad , \quad s_3 = y_1 - y_3 \tag{3.5.2}$$

$$\hat{y}_0 = s_0 + s_1 \quad \hat{y}_1 = s_2 + is_3 \quad , \quad \hat{y}_2 = s_0 - s_1 \quad , \quad \hat{y}_3 = s_2 - is_3 .$$

Dieser Algorithmus kommt also ganz ohne Multiplikation aus. Die Anzahl der Additionen ist 8.

Als nächstes nehmen wir  $n = 7$ . Dann ist  $M_7 = C_6 = \{1, a, \dots, a^5\}$  mit dem erzeugenden Element  $a = 3$ , vgl. Abschnitt 2.4. Also ist  $M_7 = \{1, 3, 2, 6, 4, 5\}$ . Wir ordnen  $W_7$  so an, daß die Zeilen und Spalten 1, 2, 3, 4, 5, 6 in der Reihenfolge 1, 3, 2, 6, 4, 5 erscheinen. Notieren wir nur die Exponenten, so bedeutet dies

	0	1	2	3	4	5	6			0	1	2	3	4	5	6
0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6		1	0	1	3	2	6	4	5
2	0	2	4	6	1	3	5	→ Zeilen	3	0	3	6	2	5	1	4
3	0	3	6	2	5	1	4		2	0	2	4	6	1	3	5
4	0	4	1	5	2	6	3		6	0	6	5	4	3	2	1
5	0	5	3	1	6	4	2		4	0	4	1	5	2	6	3
6	0	6	5	4	3	2	1		5	0	5	3	1	6	4	2

Es entsteht die Gruppentafel von  $C_6$ , wie es auf Grund der Isomorphie  $M_7 \cong C_6$  zu erwarten ist.

Dies wird in folgender Weise in einen Algorithmus umgesetzt. Die Faltung der Länge 6 realisieren wir durch eine Faltung der Länge 2 auf

### 3.5. DIE SCHNELLE FOURIER-TRANSFORMATION NACH WINOGRAD67

Blöcken, die ihrerseits Faltungen der Länge 3 sind. Die Faltungen der Länge 3 führen wir durch Algorithmus (3.4.8) aus ( $M(3) = 4$ ,  $A(3) = 11$ ), für die Faltungen der Länge 2 ist  $M(2) = 2$ ,  $A(2) = 4$ . Nach 3.4 ist dann  $M(6) = M(2)M(3) = 8$ ,  $A(6) = M(2)A(3) + 3A(2) = 34$ . Die Faltung der Länge 6 läßt sich also mit 8 Multiplikationen und 34 Additionen ausführen. Bei den Faltungen der Länge 3 fallen auch die Summen  $y_1 + y_2 + y_3$  und  $y_4 + y_5 + y_6$  an. Die Addition  $\hat{y}_6 = (y_1 + y_2 + y_3) + (y_4 + y_5 + y_6)$  fällt bei der Blockfaltung an. Jetzt sind nur noch die 6 Additionen mit  $\hat{y}_0$  auszuführen. Nun ist aber jeder der beiden Faltungsalgorithmen für die Faltung der Länge 3 von der Form  $w'_k = m_0 + \dots$ ,  $k = 0, 1, 2$  (vgl. 3.4.8). Also braucht man für jede dieser Faltungen nur  $m_0 + y_0$  zu bilden, kommt also mit 2 Additionen aus. Insgesamt reichen also 36 Additionen und 8 Multiplikationen.

Nehmen wir als weiteres Beispiel  $n = 9 = 3^2$ . Dann ist nach Satz 2.4.3  $M_9 = \{1, 2, 4, 5, 7, 8\} \cong C_6 = \{1, a, \dots, a^5\}$  mit  $a = 5$  (wir könnten ebensogut  $a = 2$  nehmen, nicht aber  $a = 4$ ). Ordnen wir demgemäß  $M_9 = \{1, 5, 7, 8, 4, 2\}$  an und schreiben wir in  $W_9$  erst die (nicht zu  $M_9$  gehörigen) Indizes 0, 3, 6 an, so nimmt  $W_9$  die Form

	0	3	6	1	5	7	8	4	2
0	0	0	0	0	0	0	0	0	0
3	0	0	0	3	6	3	6	3	6
6	0	0	0	6	3	6	3	6	3
1	0	3	6	1	5	7	8	4	2
5	0	6	3	5	7	8	4	2	1
7	0	3	6	7	8	4	2	1	5
8	0	6	3	8	4	2	1	5	7
4	0	3	6	4	2	1	5	7	8
3	0	6	3	2	1	5	7	8	4

Man erkennt die Faltung der Länge 6 in den letzten 6 Zeilen und Spalten.

Für die Winograd-FFT kann man folgende Tabelle verifizieren:

$n$	Multiplikationen	Additionen	Herleitung
2	0	2	--
3	2	6	$M_3 \cong C_2$
4	0	8	$M_4 \cong C_2$
5	5	17	$M_5 \cong C_4$
7	8	36	$M_7 \cong C_2 \otimes C_3$
8	2	26	$M_8 \cong C_2 \otimes C_2$
9	10	45	$M_9 \cong C_6$
16	10	74	$M_{16} \cong C_2 \otimes C_4$

Aus dieser Tabelle kann man nun mittels Primfaktorzerlegung und Tensorprodukten nach §3 Algorithmen für andere Längen  $n$  herleiten.

### 3.6 Schnelle Poisson-Löser

Als Anwendung der schnellen Fourier-Transformation wollen wir nun einen schnellen Algorithmus zur Lösung der Randwertaufgabe

$$\Delta u = f \quad \text{in } \Omega, \quad u = 0 \quad \text{auf } \partial\Omega \quad (3.6.1)$$

für ein Rechteck  $\Omega$  herleiten. Durch Diskretisierung auf einem Gitter der Schrittweite  $h$  wird (3.6.1) angenähert durch

$$\begin{aligned} -4u_{k,\ell} + u_{k+1,\ell} + u_{k-1,\ell} + u_{k,\ell-1} + u_{k,\ell+1} &= h^2 f_{k,\ell}, \quad 0 < k < m, \quad 0 < \ell < n \\ u_{k\ell} &= 0, \quad k = 0 \quad \text{oder } m \quad \text{oder } \ell = 0 \quad \text{oder } n. \end{aligned} \quad (3.6.2)$$

Dabei ist  $u_{k,\ell}$  eine Näherung für  $u$  in dem durch  $k, \ell$  bezeichneten Gitterpunkt, und  $f_{k,\ell}$  ist der dortige Funktionswert von  $f$ . Unser Ziel ist es, (3.6.2) in  $O(mn \log(mn))$  Rechenoperationen zu lösen.

Wir beginnen mit dem eindimensionalen Fall, also

$$u'' = f \quad \text{in } 0 < x < a, \quad u(0) = u(a) = 0. \quad (3.6.3)$$

Durch Diskretisierung geht dies über in

$$\begin{aligned} u_{k+1} - 2u_k + u_{k-1} &= h^2 f_k, \quad 0 < k < m \\ u_0 &= u_m = 0. \end{aligned} \quad (3.6.4)$$

Führen wir die Vektoren und Matrizen

$$U = \begin{pmatrix} u_1 \\ \vdots \\ u_{m-1} \end{pmatrix}, \quad F = h^2 \begin{pmatrix} f_1 \\ \vdots \\ f_{m-1} \end{pmatrix}, \quad T_{m-1} = \begin{pmatrix} -2 & 1 & & & \mathbf{0} \\ 1 & -2 & 1 & & \\ & 1 & -2 & 1 & \\ & & & \ddots & \\ \mathbf{0} & & & 1 & -2 \end{pmatrix}$$

ein, so schreibt sich (3.6.4) als

$$T_{m-1}U = F. \quad (3.6.5)$$

Da  $T_{m-1}$  tridiagonal ist, kann man dies durch Elimination in  $O(m)$  Rechenoperationen lösen. Wir gehen komplizierter vor und berechnen zunächst die Eigenwerte und Eigenvektoren von  $T_m$ . Dazu setzen wir

$$c_k = \cos(\theta) , \quad s_k = \sin(k\theta)$$

und bekommen dann aus den Additionstheoremen

$$\begin{aligned} s_{k-1} &= c_1 s_k - s_1 c_k , & s_{k+1} &= c_1 s_k + s_1 c_k , \\ c_{k-1} &= c_1 c_k + s_1 s_k , & c_{k+1} &= c_1 s_k - s_1 s_k . \end{aligned}$$

Daraus folgt weiter

$$s_{k-1} - 2c_1 s_k + s_{k+1} = 0 , \quad c_{k-1} - 2c_1 c_k + c_{k+1} = 0 .$$

Die erste Beziehung schreiben wir in der Form

$$s_{k-1} - 2s_k + s_{k+1} = -2(1 - c_1)s_k = -4 \sin^2\left(\frac{\theta}{2}\right)s_k ,$$

wobei wir  $1 - \cos \theta = 2 \sin^2(\theta/2)$  benutzt haben. Setzen wir hier  $\theta = \theta_j = \pi j/m$  und bezeichnen wir mit  $s^j$  den zugehörigen Vektor  $(s_1, \dots, s_{m-1})$ , so ist  $s_m = 0$  und damit  $s^j$  Eigenvektor zu  $T_{m-1}$  zum Eigenwert  $\lambda_j = -4 \sin^2(\pi j/2m)$ . Mit den Matrizen

$$S_{m-1} = (s^1, \dots, s^{m-1}) , \quad \Lambda_{m-1} = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_{m-1} \end{pmatrix}$$

hat man als

$$S_{m-1}^{-1} T_{m-1} S_{m-1} = \Lambda_{m-1} . \quad (3.6.6)$$

Nun behandeln wir den zweidimensionalen Fall (3.6.2). Wir ordnen die  $u_{kl}$  zeilenweise an, definieren also einen  $(n-1)(m-1)$ -Vektor  $U$  mit den Komponenten ( $m=4, n=5$ )

$$u_{11}, u_{12}, u_{13}, u_{14}, u_{21}, u_{22}, u_{23}, u_{24}, u_{31}, u_{32}, u_{33}, u_{34} .$$



$M_m$ . Dann gilt

$$M^{-1} = (V_m \otimes U_n)(I_m \otimes \Lambda_n + M_m \otimes I_n)^{-1}(V_m^{-1} \otimes U_n^{-1}) .$$

**Beweis:** Dies folgt sofort aus den Rechenregeln

$$(A \otimes B)(C \otimes D) = AC \otimes BD , \quad (A \otimes B)^{-1} = A^{-1} \otimes B^{-1} .$$

□

Sind  $\Lambda_n$ ,  $M_m$  diagonal, so auch  $I_n \otimes \Lambda_n + M_n \otimes I_n$  und damit leicht zu invertieren. In der Anwendung auf (3.6.7) sind  $U_n$ ,  $V_m$  die Sinus-Transformation, die  $n \log n$  bzw.  $m \log m$  Operationen erfordern.  $V_m \otimes U_n$  verlangt also  $m$  Sinus-Transformationen der Länge  $n$  und  $n$  Sinus-Transformationen der Länge  $m$ , also

$$mn \log n + nm \log m = mn \log(mn)$$

Operationen. Das gleiche gilt für  $V_m^{-1} \otimes U_n^{-1}$ , und die Anwendung von  $(I_m \otimes \Lambda_n + M_m \otimes I_n)^{-1}$  verlangt  $mn$  Operationen. Also kann (3.6.2) in  $O(mn \log(mn))$  Operationen gelöst werden.

# Kapitel 4

## Symmetrie

### 4.1 Matrizen mit Symmetrien

Wir haben schon in der Einleitung gesehen, daß effiziente Algorithmen für Matrizen möglich sind, die gewisse Vertauschbarkeitsrelationen erfüllen. Dies wollen wir nun systematisch verfolgen.

**Definition 4.1.1** Sei  $A$  eine  $(m, n)$ -Matrix, und seien  $P, Q$  Darstellungen einer Gruppe  $G$  in  $\mathbb{C}^m$  bzw.  $\mathbb{C}^n$ . Wir sagen,  $A$  besitze die Symmetrien von  $P, Q$ , falls

$$AP(s) = Q(s)A \quad , \quad \forall s \in G . \quad (4.1.1)$$

Ist  $P = Q$ , so sagen wir,  $A$  besitze die Symmetrien von  $P$ .

Ein maximales System irreduzibler paarweise inäquivalenter Darstellungen nennen wir in Zukunft kurz MIP.

Sei  $U_1, \dots, U_r$  ein MIP von  $G$ , und zwar sei  $U_j : \mathbb{C}^{n_j} \rightarrow \mathbb{C}^{n_j}$ , also vom Grade  $n_j$ . Die Vielfachheit von  $U_j$  in  $P, Q$  sei  $c_j$  bzw.  $d_j$ . Dann gibt es  $(m, m)$  bzw.  $(n, n)$ -Matrizen  $X, Y$ , so daß

$$\begin{aligned}
 P(s) &= X \begin{pmatrix} I_{c_1} \otimes U_1(s) & & \\ & \ddots & \\ & & I_{c_r} \otimes U_r(s) \end{pmatrix} X^{-1}, \\
 Q(s) &= Y \begin{pmatrix} I_{d_1} \otimes U_1(s) & & \\ & \ddots & \\ & & I_{d_r} \otimes U_r(s) \end{pmatrix} Y^{-1}
 \end{aligned} \tag{4.1.2}$$

für alle  $s \in G$ .

**Beispiele:**

1) Faltungen. Sei  $X$  die  $(n, n)$ -Matrix aus 3.3.1, und sei  $P = (e_1, \dots, e_{n-1}, e_0)$  mit dem  $i$ -ten Einheitsvektor  $e_i$  in  $\mathbb{R}^n$  (Komponenten von 0 bis  $n-1$  numeriert). Dann ist  $PX = XP$  und damit  $P^k X = X P^k$ . Sei nun  $C_n = \{1, a, \dots, a^{n-1}\}$ . Die Abbildung

$$P(a^k) = P^k, \quad k = 0, \dots, n-1$$

ist eine Darstellung von  $C_n$  in  $\mathbb{C}^n$ .  $X$  besitzt also die Symmetrien von  $P$ .

2) Fourier-Transformation. Mit der Matrix  $P$  aus i) und

$$Q = \begin{pmatrix} 1 & & & \\ & \omega & & \\ & & \ddots & \\ & & & \omega^{n-1} \end{pmatrix}, \quad \omega = e^{-2\pi i/n}$$

gilt für die Fourier-Transformation  $W_n$  der Länge  $n$  (vgl. III.3.1) die Beziehung  $W_n P = Q W_n$  und damit  $W_n P^k = Q^k W_n$ .  $W_n$  hat also die Symmetrien der gleichen Darstellung  $P$  von  $C_n$  wie in i) und der Darstellung

$$Q(a^k) = Q^k, \quad k = 0, 1, \dots, n-1.$$

3) Für die Block-Matrizen

$$A = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}, \quad P = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

gilt  $AP = PA$ . Definieren wir also eine Darstellung  $P$  von  $C_2 = \{1, a\}$  durch  $P(a^k) = P^k$ ,  $k = 0, 1$ , so hat  $A$  die Symmetrie dieser Darstellung.

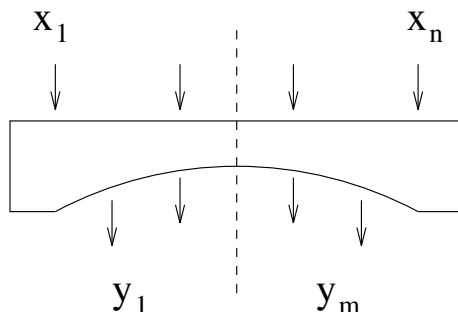
4) Sei die  $(m, n)$ -Matrix  $A$  die Matrix eines linearen Systems mit  $n$  Eingängen und  $m$  Ausgängen. Dieses ordnet dem Input  $x_1, \dots, x_n$  den Output  $y_1, \dots, y_m$  zu gemäß  $y = Ax$ .

Wir wollen nun annehmen, das lineare System besitze Symmetrien, d.h. Input  $Px$  entspreche der Output  $Qy$  mit gewissen Permutationsmatrizen  $P, Q$ . Dann gilt für alle  $x$

$$QAx = APx$$

und damit  $AP = QA$ . Als Beispiele haben wir

(a) Eine spiegelsymmetrische Brücke:

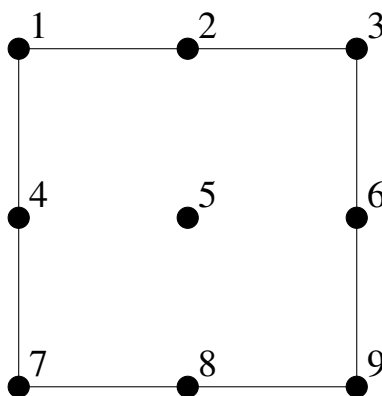


Die  $x_i$  bedeuten etwa Belastungen, die  $y_j$  Auslenkungen. Seien die  $(n, n)$  bzw.  $(m, m)$ -Matrizen  $P, Q$  erklärt durch

$$P = \begin{pmatrix} & & & 1 \\ 0 & & 1 & \\ & \ddots & & \\ 1 & & & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} & & & 1 \\ 0 & & 1 & \\ & \ddots & & \\ 1 & & & 0 \end{pmatrix}.$$

Diese Matrizen beschreiben die Symmetrie des Systems. Die Symmetriegruppe ist  $C_2 = \{1, a\}$ ,  $a^2 = 1$ .

(b) Die quadratische Platte



hat als Symmetriegruppe  $D_4$ . Die Belastungen in den 9 Knoten seien  $x_1, \dots, x_9$ , und die zugehörigen Dehnungen  $y_1, \dots, y_9$ . Wieder ist  $y = Ax$ . Für  $g \in D_4$  sei  $\pi(g)$  die Permutation von  $1, \dots, 9$ , die von der Anwendung von  $g$  auf die Platte bewirkt wird. Dann ist

$$P(g) \begin{pmatrix} x_1 \\ \vdots \\ x_9 \end{pmatrix} = \begin{pmatrix} x_{\pi(g)1} \\ \vdots \\ x_{\pi(g)9} \end{pmatrix}, \quad g \in D_4$$

eine Darstellung von  $D_4$  in  $\mathbb{C}^9$  definiert, und  $A$  hat die Symmetrie von  $P$ .

**Satz 4.1.2** *A besitze die Symmetrien von  $P, Q$ . Dann gibt es  $(d_j, c_j)$ -Matrizen  $A_j$  mit*

$$A = Y \begin{pmatrix} A_1 \otimes I_{n_1} & & \\ & \ddots & \\ & & A_r \otimes I_{n_r} \end{pmatrix} X^{-1}. \quad (4.1.3)$$

**Beweis:** Mit  $B = Y^{-1}AX$  lautet (1.1)

$$B \begin{pmatrix} I_{c_1} \otimes U_1(s) & & \\ & \ddots & \\ & & I_{c_r} \otimes U_r(s) \end{pmatrix} = \begin{pmatrix} I_{d_1} \otimes U_1(s) & & \\ & \ddots & \\ & & I_{d_r} \otimes U_r(s) \end{pmatrix} B .$$

Schreiben wir  $B = (B_{jk})$  mit  $(d_j n_j, c_k n_k)$ -Matrizen  $B_{jk}$ , so geht dies über in

$$B_{jk}(I_{c_k} \otimes U_k(s)) = (I_{d_j} \otimes U_j(s))B_{jk} .$$

Schreiben wir weiter  $B_{jk} = (B_{jk,il})$  mit  $(n_j, n_k)$ -Matrizen  $B_{jk,il}$ , so entsteht

$$B_{jk,il}U_k(s) = U_j(s)B_{ik,il} .$$

Für  $k \neq j$  sind  $U_k, U_j$  nicht äquivalent und irreduzibel. Nach Satz 2.1.8 folgt also  $B_{jk,il} = 0$  für  $k \neq j$ . Für  $k = j$  folgt nach dem gleichen Satz  $B_{jj,il} = \lambda_{jil}$  mit gewissen Zahlen  $\lambda_{jil}$ . Insgesamt ist also  $B_{jk} = 0$  für  $j \neq k$  und  $B_{jj} = A_j \otimes I_{n_j}$  mit  $(A_j)_{il} = \lambda_{jil}$ .

□

**Bemerkung:** Für das praktische Rechnen ist es bequemer,  $Y^{-1}AX$  in der Form

$$\begin{pmatrix} I_{n_1} \otimes A_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & I_{n_r} \otimes A_r \end{pmatrix}$$

zu haben. Dies kann durch eine Permutation von Zeilen und Spalten erreicht werden. Ignoriert man einmal die Matrizen  $X, Y$ , so bietet diese Form von  $A$  folgende Vorteile:

Statt der Anwendung der  $(m, n)$ -Matrix  $A$  hat man nur  $n_j$  mal die  $(d_j, c_j)$ -Matrix  $A_j$  anzuwenden,  $j = 1, \dots, r$ .

Ist  $P = Q$  (also  $n = m$  und  $c_j = d_j$ ), so hat man statt des Gleichungssystems  $Ax = b$  der Dimension  $n$  nur  $n_j$  mal ein Gleichungssystem  $A_j x_j = b_j$  der Dimension  $c_j$  (also immer mit gleicher Matrix  $A_j$ ) zu

lösen,  $j = 1, \dots, r$ . Ebenso reduziert sich das  $(n, n)$ -Eigenwertproblem auf  $n_j$  Eigenwertprobleme der Dimension  $c_j$ ,  $j = 1, \dots, r$ , für die Matrizen  $A_j$  (mit Konsequenzen für die Vielfachheiten der Eigenwerte von  $A$ ).

Wir wollen uns nun Gedanken darüber machen, was (4.1.2) bedeutet und wie man diese Faktorisierung von  $P$ ,  $Q$  herstellt. Sei zunächst  $X = (X_1, \dots, X_r)$  eine entsprechende Zerlegung von  $X$ , d.h.  $X_j$  hat  $c_j n_j$  Spalten, und sei  $V_j$  der von diesen Spalten aufgespannte Teilraum der Dimension  $c_j n_j$ . Dann ist

$$PX_j = X_j(I_{c_j} \otimes U_j) \quad , \quad j = 1, \dots, r .$$

Ist also  $x \in V_j$ , d.h.  $x = X_j v$  mit  $v \in \mathbb{C}^{c_j n_j}$ , so ist

$$Pv = PX_j v = X_j(I_{c_j} \otimes U_j)v \in V_j .$$

$V_j$  ist also invarianter Unterraum von  $P$ , und in der Basis  $X_j$  von  $V_j$  ist  $P$  gegeben durch  $I_{c_j} \otimes U_j$ .  $V_j$  zerfällt also noch weiter in invariante Unterräume  $V_{j,1}, \dots, V_{j,c_j}$  der Dimension  $n_j$ , und es ist  $X_j = (X_{j,1}, \dots, X_{j,c_j})$  mit Matrizen  $X_{j,\nu}$  von  $n_j$  Spalten, welche eine Basis von  $V_{j,\nu}$  bilden. Es ist

$$PX_{j,\nu} = X_{j,\nu} U_j . \tag{4.1.4}$$

Wie oben sieht man, daß  $V_{j,\nu}$  invariante Unterräume von  $P$  sind, und daß  $P$  in der Basis  $X_{j,\nu}$  in  $V_{j,\nu}$  durch  $U_j$  gegeben ist.

Das Auffinden von  $X$  für gegebenes  $P$  wird durch folgenden Satz ermöglicht.

**Satz 4.1.3** Sei für  $1 \leq k, \ell \leq n_j$  mit dem  $k, \ell$ -Element  $U_j^{k\ell}$  von  $U_j$

$$T_j^{k\ell} = \frac{n_j}{|G|} \sum_{g \in G} u_j^{k\ell}(g^{-1}) P(g) .$$

Dann ist für  $\nu = 1, \dots, c_j$

$$T_j^{k\ell} X_{j\nu} = \begin{cases} X_{j\nu} I_{n_j}^{\ell k} & , \quad i = j \quad , \\ 0 & , \quad \text{sonst} \quad , \end{cases}$$

wo  $I_{n_j}^{\ell k}$  an der Stelle  $(\ell, k)$  eine 1 und sonst nur Nullen hat.

**Beweis:** Wir erinnern an die Orthogonalitätseigenschaften von Darstellungen (Satz 2.1.10). Danach gilt

$$\frac{n_j}{|G|} \sum_{g \in G} U_j^{k\ell}(g^{-1}) U_i^{mn}(g) = \begin{cases} 1 & , \quad i = j, \quad k = n \quad \text{und} \quad \ell = m, \\ 0 & , \quad \text{sonst.} \end{cases}$$

Es folgt

$$\frac{n_j}{|G|} \sum_{g \in G} U_j^{k\ell}(g^{-1}) U_i(g) = \begin{cases} I_{n_j}^{\ell k} & , \quad i = j, \\ 0 & , \quad \text{sonst.} \end{cases} \quad (4.1.5)$$

(4.1.2) bedeutet

$$T_j^{k\ell} X = X \frac{n_j}{|G|} \sum_{g \in G} U_j^{k\ell}(g^{-1}) \begin{pmatrix} I_{c_1} \otimes U_1(g) & & \\ & \ddots & \\ & & I_{c_r} \otimes U_r(g) \end{pmatrix}.$$

Mit  $X = (X_1, \dots, X_r)$  und  $X_j = (X_{j,1}, \dots, X_{j,c_j})$  folgt der Satz direkt aus (4.1.5).

□

Ist also  $X_{j\nu i}$  die  $i$ -te Spalte von  $X_{j\nu}$ , so gilt

$$T_j^{k\ell} X_{j\nu i} = \begin{cases} X_{j\nu \ell} & , \quad i = k, \\ 0 & , \quad \text{sonst.} \end{cases} \quad (4.1.6)$$

Insbesondere haben wir

$$T_j^{k\ell} X_{j\nu k} = X_{j\nu \ell} \quad (4.1.7)$$

Als unmittelbare Folgerung aus dem Satz notieren wir: Ist  $\chi_j$  der Charakter von  $U_j$  und

$$T_j = \frac{n_j}{|G|} \sum_{g \in G} \chi_j(g^{-1}) P(g),$$

so ist

$$T_j X_k = \begin{cases} X_j & , \quad j = k, \\ 0 & , \quad \text{sonst.} \end{cases}$$

Insbesondere ist also  $T_j$  eine Projektion auf  $V_j$ .

Nun können wir einen Algorithmus zur Berechnung einer Matrix  $X$  aufstellen, die (4.1.2) erfüllt.

Für  $j = 1, \dots, r$ :

Finde Basis für  $\ell = 1, \dots, n_j$

$$X'_{j\nu\ell} = T_j^{1\ell} X'_{j\nu 1}, \quad \nu = 1, \dots, c_j.$$

Setze  $X'_{j\nu} = (X'_{j\nu 1}, \dots, X'_{j\nu n_j})$ ,  $X'_j = (X'_{j1}, \dots, X'_{jc_j})$ ,  $X' = (X_1, \dots, X_r)$ .

**Satz 4.1.4** Für die Matrix  $X'$  gilt (4.1.2).

**Beweis:** Wir haben nur (4.1.4) für  $X'$  nachzuweisen.

Wegen (4.1.6) ist  $X'_{j\nu 1}$  eine Linearkombination der  $X_{j\mu 1}$ , etwa

$$X'_{j\nu 1} = \sum_{\mu=1}^{c_j} \alpha_{j\nu\mu} X_{j\mu 1}.$$

Nach (4.1.7) folgt

$$X'_{j\nu\ell} = \sum_{\mu=1}^{c_j} \alpha_{j\nu\mu} X_{j\mu\ell}.$$

Für die Matrizen  $X'_{j\nu}$  bedeutet dies

$$X'_{j\nu} = \sum_{\mu=1}^{c_j} \alpha_{j\nu\mu} X_{j\mu}.$$

Nun folgt nach (4.1.4)

$$\begin{aligned} PX'_{j\nu} &= \sum_{\mu=1}^{c_j} \alpha_{j\nu\mu} PX_{j\mu} \\ &= \sum_{\mu=1}^{c_j} \alpha_{j\nu\mu} X_{j\mu} U_j \\ &= X'_{j\nu} U_j \end{aligned}$$

und dies ist (4.1.4) für  $X'$ .

□

**Beispiele:**

1) Wir greifen das obige Beispiel 4a) auf. Dort ist  $G = C^2 = \{1, s\}$ ,  $P(s^k) = P^k$ ,  $k = 0, 1$ , mit

$$P = \begin{pmatrix} & & & 1 \\ 0 & & 1 & \\ & \ddots & & \\ 1 & & & 0 \end{pmatrix}.$$

Ein MIP ist gegeben durch  $U_1(s^k) = 1$ ,  $U_2(s^k) = (-1)^k$ ,  $k = 0, 1$ . Also ist  $P = c_1 u_1 + c_2 U_2$ . Seien  $\chi$ ,  $\rho_1$ ,  $\rho_2$  die Charaktere von  $P$ ,  $U_1$ ,  $U_2$ , also

	1	s
$\chi$	$n$	$\text{par}(n)$
$\rho_1$	1	1
$\rho_2$	1	-1

$$\text{par}(n) = \begin{cases} 0 & , \quad n \text{ gerade} \\ 1 & , \quad n \text{ ungerade} . \end{cases}$$

Nach Satz 2.2.4 gilt  $c_j = \langle \chi, \chi_j \rangle$ , also

$$c_1 = \frac{1}{2}(\chi(1)\rho_1(1) + \chi(s)\rho_2(s)) = \frac{1}{2}(n + \text{par}(n))$$

$$c_2 = \frac{1}{2}(\chi(1)\rho_1(1) + \chi(s)\rho_2(s)) = \frac{1}{2}(n - \text{par}(n)) .$$

Die Zerlegung von  $X$  lautet  $X = (X_1, X_2)$ , wobei  $X_j$   $c_j$  Spalten hat, welche den invarianten Unterraum  $V_j$  von  $P$  aufspannen.  $V_1, V_2$  sind hier leicht zu erraten: Je nachdem  $n$  gerade oder ungerade ist, hat man die Basen von  $V_1, V_2$

$$\begin{matrix} n \text{ gerade (8)} \\ X_1 & X_2 \end{matrix}$$

$$\begin{matrix} n \text{ ungerade (7)} \\ X_1 & X_2 \end{matrix}$$

1	1							1						
2		1								1				
3			1									1		
4				1									1	
5					1									-1
6						1								
7							1							
8	1													-1

1	1							1						
2		1								1				
3			1									1		
4				1									1	
5					1									-1
6						1								
7							1							
7	1													-1

(4.1.8)

Die Anzahl der gefundenen linear unabhängigen Vektoren entspricht jeweils genau der Dimension von  $V_1, V_2$ . Jeder der gefundenen Vektoren spannt einen eindimensionalen invarianten Unterraum von  $P$  auf, auf denen  $P$  durch  $U_1$  oder  $U_2$  gegeben ist, je nachdem er zu  $V_1$  oder  $V_2$  gehört. Das ist aber gerade das, was (4.1.2) für die Spalten von  $X_1, X_2$  aussagt. Wir können also für  $X$  die gefundenen Vektoren (4.1.8) nehmen. Zur Bestätigung bilden wir noch

$$T_1 = \frac{1}{2}(I + P), \quad T_2 = \frac{1}{2}(I - P).$$

Tatsächlich projiziert  $T_1$  auf  $V_1, T_2$  auf  $V_2$ .

2) Im obigen Beispiel 4b) ist  $G = D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ .  $D_4$  hat das MIP  $U_1, U_2, U_3, U_4, U_5$  mit den Geraden 1, 1, 1, 1, 2. Die Tabelle der Charaktere  $\chi_j$  von  $U_j$  ist

	$r^k$	$sr^k$	
$\chi_1$	1	1	$k = 0, 1, 2, 3.$
$\chi_2$	1	-1	
$\chi_3$	$(-1)^k$	$(-1)^k$	
$\chi_4$	$(-1)^{k+1}$	$(-1)^{k+1}$	
$\chi_5$	$i^k + (-i)^k$	0	

Für den Charakter  $\chi$  von  $P$  gilt

$$\chi(g) = \text{Anzahl der Knoten, die bei } g \text{ fest bleiben.}$$

Damit erhält man ohne Mühe

$g$	1	$r$	$r^2$	$r^3$	$s$	$sr$	$sr^2$	$sr^3$
$\chi(g)$	9	1	1	1	3	3	3	3

Für die Vielfachheiten  $c_j$ , mit denen  $U_j$  in  $P$  enthalten ist, ergibt sich

$$c_1 = \langle \chi, \chi_1 \rangle = \frac{1}{8}(9 + 1 + 1 + 1 + 3 + 3 + 3 + 3) = 3$$

$$c_2 = 0, \quad c_3 = c_4 = 1, \quad c_5 = 2.$$

Die invarianten Unterräume  $V_1, V_2, V_3, V_4, V_5$  haben damit der Reihe nach die Dimensionen 3, 0, 1, 1, 4. Basen findet man wie beim ersten



mit komplexen Zahlen  $A_0, \dots, A_{n-1}$ . Die Spalten der Matrix

$$X = W_n = (\omega^{kj})_{k,j=0,\dots,n-1}$$

sind invariante Unterräume von  $P$ .  $A$  wird also durch  $W_n$  diagonalisiert. Dies haben wir in Satz 3.3.1 schon gesehen.

Man kann eine rationale Form von  $X$  erhalten, wenn man die invarianten Unterräume geeignet zusammenfaßt. Seien  $\phi_d$  die Kreisteilungspolynome, und sei  $X_d$  die Matrix der Spalten von  $W_n$ , welche zu den Nullstellen von  $\phi_d$  gehören. Da die Kreisteilungspolynome ganzzahlige Koeffizienten haben, gibt es in dem von  $X_d$  aufgespannten invarianten Unterraum  $V_d$  eine ganzzahlige Basis  $X'_d$ . Setzen wir  $X' = (X'_d)_{d|n}$ , so ist

$$A = X' \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix} (X')^{-1}.$$

Dabei gehört jede Matrix  $A_j$  zu einem Teiler von  $n$ , und die Dimension von  $A_j$  entspricht dem Grad des zugehörigen Kreisteilungspolynoms.

Wir führen dies für den Fall  $n = 6$  durch. Es ist

$$z^6 - 1 = \phi_1 \phi_2 \phi_3 \phi_6$$

mit

$$\phi_1 = z - 1, \quad \phi_2 = z + 1, \quad \phi_3 = z^2 + z + 1, \quad \phi_6 = z^2 - z + 1.$$

Ganzzahlige Basen der eindimensionalen invarianten Unterräume  $V_1, V_2$  sind leicht gefunden, nämlich

$$X'_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad X'_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}.$$

Sei  $(x_0, \dots, x_5) \in V_3$ . Er ist eine Linearkombination von Vektoren  $(1, \omega, \dots, \omega^5)$  mit  $\phi_3(\omega) = \omega^2 + \omega + 1 = 0$ . Also gilt

$$\begin{aligned} x_0 + x_1 + x_2 &= 0 & , \\ x_1 + x_2 + x_3 &= 0 & , \\ x_2 + x_3 + x_4 &= 0 & , \\ x_4 + x_5 + x_6 &= 0 & . \end{aligned}$$

Dieses System besitzt zwei linear unabhängige ganzzahlige Lösungen, nämlich

$$X'_3 = \begin{pmatrix} 1 & -1 \\ 0 & 2 \\ -1 & -1 \\ 1 & -1 \\ 0 & 2 \\ -1 & -1 \end{pmatrix} .$$

Für  $V_4$  findet man auf die gleiche Art eine Basis

$$X'_4 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \\ 0 & 2 \\ -1 & 1 \\ -1 & -1 \\ 0 & -2 \end{pmatrix} .$$

Man berechnet  $X'^T X' = \text{diag}(6, 6, 4, 12, 4, 12)$  und hat damit

$$A = X'^T \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & A_3 & \\ & & & A_4 \end{pmatrix} X'$$

mit  $(1, 1)$ -Matrizen  $A_1, A_2$  und  $(2, 2)$ -Matrizen  $A_3, A_4$ . Die Faltung der Länge 6 läßt sich also durch  $1 + 1 + 4 + 4 = 10$  Multiplikationen realisieren.

**Satz 4.1.5** *Sind  $P, U_1, \dots, U_r$  unitär und werden die Vektoren  $X'_{j\nu 1}$ ,  $\nu = 1, \dots, c_j$  orthonormal gewählt, so ist  $X'$  unitär.*

**Beweis:** Wir schreiben  $X$  für  $X'$ . Ist  $P$  unitär, so gilt für alle  $g \in G$

$$X_{j\nu}^* X_{i\mu} = (P(g)X_{j\nu})^* P(g)X_{i\mu}$$

und damit

$$\begin{aligned} X_{j\nu}^* X_{i\mu} &= \frac{1}{|G|} \sum_{g \in G} (P(g)X_{j\nu})^* P(g)X_{i\mu} \\ &= \frac{1}{|G|} \sum_{g \in G} (X_{j\nu} U_j(g))^* X_{i\mu} U_i(g) \end{aligned}$$

wegen (4.1.4). Da die  $U_j$  unitär sind, ist  $U_j^*(g) = U_j(g^{-1})$ , also

$$\begin{aligned} X_{j\nu}^* X_{i\mu} &= \frac{1}{|G|} \sum_{g \in G} U_j^*(g) X_{j\nu}^* X_{i\mu} U_i(g) \\ &= \frac{1}{|G|} \sum_{g \in G} U_j(g^{-1}) X_{j\nu}^* X_{i\mu} U_i(g). \end{aligned}$$

Aus den Orthogonalitätsrelationen (Satz 2.1.10) folgt nun

$$X_{j\nu}^* X_{i\mu} = 0, \quad i \neq j.$$

Für  $i \neq j$  sind also alle Spalten von  $X_j$  orthogonal zu allen Spalten von  $X_i$ . Für  $i = j$  setzen wir  $S = X_{j\nu}^* X_{j\mu}$ . Dann gilt

$$S_{k\ell} = \frac{1}{|G|} \sum_{g \in G} \sum_{m,n=1}^{n_j} U_j^{km}(g^{-1}) S_{mn} U_j^{n\ell}(g).$$

Wieder nach den Orthogonalitätsrelationen folgt  $S_{k\ell} = 0$  für  $k \neq \ell$ . Also sind  $X_{j\nu\ell}$ ,  $X_{j\mu k}$  orthogonal für  $\ell \neq k$  und alle  $\nu, \mu$ . Bleibt noch zu sagen, daß

$$X_{j\nu\ell}^* X_{j\mu\ell} = \delta_{\nu\mu}, \quad \nu, \mu = 1, \dots, c_j.$$

Nach (4.1.7) ist

$$\begin{aligned} X_{j\nu\ell} X_{j\mu\ell} &= (T_j^{1\ell} X_{j\nu 1})^* X_{j\mu\ell} \\ &= X_{j\nu 1}^* (T_j^{1\ell})^* X_{j\mu\ell}. \end{aligned} \tag{4.1.9}$$

Da  $P$  und  $U_j$  unitär sind, gilt

$$\begin{aligned}
 (T_j^{1\ell})^* &= \frac{n_j}{|G|} \sum_{g \in G} \overline{U_j^{1\ell}}(g^{-1}) P^*(g) \\
 &= \frac{n_j}{|G|} \sum_{g \in G} \overline{U_j^{1\ell}}(g^{-1}) P(g^{-1}) \\
 &= \frac{n_j}{|G|} \sum_{g \in G} \overline{U_j^{1\ell}}(g) P(g) \\
 &= T_j^{\ell 1} .
 \end{aligned}$$

Nach (4.1.7) folgt also schließlich aus (4.1.9)

$$\begin{aligned}
 X_{j\nu\ell}^* X_{j\mu\ell} &= X_{j\nu 1}^* T_j^{\ell 1} X_{j\mu\ell} \\
 &= X_{j\nu 1}^* X_{j\mu 1} = \delta_{\nu\mu} ,
 \end{aligned}$$

weil die  $X_{j\nu 1}$  ja als Orthonormalsystem konstruiert wurden.

□

## 4.2 Untergruppen

Seien  $P, Q$  wieder Darstellungen der Gruppe  $G$ . Wir betrachten nun den Fall, daß  $G$  eine Untergruppe  $H$  besitzt. Seien  $U_1, \dots, U_r$  ein MIP für  $H$ . Dann gilt also mit gewissen Matrizen  $X, Y$  und gewissen natürlichen Zahlen  $c_j, d_j$  für  $h \in H$

$$\begin{aligned} P(h) &= X \begin{pmatrix} I_{c_1} \otimes U_1(h) & & \\ & \ddots & \\ & & I_{c_r} \otimes U_r(h) \end{pmatrix} X^{-1}, \\ Q(h) &= Y \begin{pmatrix} I_{d_1} \otimes U_1(h) & & \\ & \ddots & \\ & & I_{d_r} \otimes U_r(h) \end{pmatrix} Y^{-1}. \end{aligned} \quad (4.2.1)$$

**Satz 4.2.1** *A besitze die Symmetrien von  $P, Q$ . Die Untergruppe  $H$  von  $G$  liege im Zentrum von  $G$ . Dann gibt es Darstellungen  $P_1, \dots, P_r$  der Grade  $c_1, \dots, c_r$  und  $Q_1, \dots, Q_r$  der Grade  $d_1, \dots, d_r$  von  $G$ , so daß*

$$A = Y \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix} X^{-1} \quad (4.2.2)$$

mit  $(c_j, d_j)$ -Matrizen  $A_j$ , welche die Symmetrien von  $P_j, Q_j$  besitzen. Auf  $H$  sind  $P_j, Q_j$  Vielfache der Einheitsmatrix.

**Beweis:**  $A$  besitzt die Symmetrien der Restriktionen  $P_H, Q_H$  von  $P, Q$  auf  $H$ . Deshalb ist (4.2.2) eine unmittelbare Folgerung aus Satz 4.1.2. Da  $H$  im Zentrum von  $G$  liegt, ist  $gh = hg$  für  $h \in H$  und  $g \in G$ , also  $P(g)P(h) = P(h)P(g)$ , und entsprechend für  $Q$ . Es besitzt also jede Matrix  $P(g)$  die Symmetrien von  $P_H$ , jede Matrix  $Q(g)$  diejenigen von  $Q_H$ . Wieder nach Satz 4.1.2 folgt

$$P(g) = X \begin{pmatrix} P_1(g) & & \\ & \ddots & \\ & & P_r(g) \end{pmatrix} X^{-1},$$

$$Q(g) = Y \begin{pmatrix} Q_1(g) & & \\ & \ddots & \\ & & Q_r(g) \end{pmatrix} Y^{-1} \quad (4.2.3)$$

mit  $(c_j, c_j)$ -Matrizen  $P_j(g)$  und  $(d_j, d_j)$ -Matrizen  $Q_j(g)$ . Offenbar sind  $P_j, Q_j$  Darstellungen von  $G$ . Vergleich mit (4.2.1) ergibt, daß für  $h \in H$

$$P_j(h) = I_{c_j} \otimes U_j(h), \quad Q_j(h) = I_{d_j} \otimes U_j(h)$$

ist. Da  $H$  im Zentrum von  $G$  liegt, ist  $H$  abelsch. Also hat  $U_j$  den Grad 1, und wir haben sogar

$$P_j(h) = U_j(h)I_{c_j}, \quad Q_j(h) = U_j(h)I_{d_j}.$$

$P_j, Q_j$  sind also auf  $H$  Vielfache der Einheitsmatrix. Daß  $A_j$  die Symmetrien von  $P_j, Q_j$  hat, rechnet man mit Hilfe von (4.2.2), (4.2.3) und  $AP = QA$  unmittelbar nach.

□

Betrachten wir den Satz auf der Faktorgruppe  $G/H$ , so gewinnt er einen weiteren Aspekt. Dazu müssen wir allerdings den Begriff der Darstellung etwas erweitern.

**Definition 4.2.2** *Sei  $G$  eine endliche Gruppe und  $V$  ein Vektorraum über  $\mathbb{C}$ . Eine Abbildung  $\rho: G \rightarrow GL(V)$  heißt projektive Darstellung von  $G$  in  $V$ , falls*

$$\rho(st) = \alpha(s, t)\rho(s)\rho(t) \quad , \quad s, t \in G$$

mit  $\alpha(s, t) \in \mathbb{C}$ .

Projektive Darstellungen verhalten sich für die von uns diskutierten Fragen genau so wie Darstellungen. Satz 4.2.1 kann jetzt eleganter formuliert werden.

**Satz 4.2.3** *A besitze die Symmetrien von  $P, Q$ . Die Untergruppe  $H$  von  $G$  liege im Zentrum von  $G$ . Dann gibt es projektive Darstellungen  $P_1, \dots, P_r$  der Grade  $c_1, \dots, c_r$  und  $Q_1, \dots, Q_r$  der Grade  $d_1, \dots, d_r$  von  $G/H$ , so daß*

$$A = Y \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix} X^{-1}$$

mit  $(c_j, d_j)$ -Matrizen, welche die Symmetrien von  $P_j, Q_j$  besitzen.

**Beweis:** Seien  $P_j, Q_j$  die Darstellungen von  $G$  aus Satz 4.2.1. Sei  $g_1, \dots, g_m$  ein Repräsentantensystem von  $G/H$ , also  $G/H = \{g_1H, \dots, g_mH\}$ . Wir setzen

$$\tilde{P}_j(g_kH) = P_j(g_k)$$

und zeigen, daß  $\tilde{P}_j$  eine projektive Darstellung von  $G/H$  ist. Zu  $k, \ell$  gibt es  $i$  mit  $g_k g_\ell H = g_i H$ , d.h. es gibt  $h \in H$  (abhängig von  $g_k, g_\ell$ ) mit  $g_k g_\ell h = g_i$ . Also ist

$$\begin{aligned} \tilde{P}_j(g_k H g_\ell H) &= \tilde{P}_j(g_i H) = P_j(g_i) \\ &= P_j(g_k g_\ell H) \\ &= P_j(g_k g_\ell) P_j(h) \\ &= P_j(g_k) P_j(g_\ell) P_j(h) \\ &= \tilde{P}_j(g_k H) \tilde{P}_j(g_\ell H) P_j(h) . \end{aligned}$$

Auf  $H$  ist  $P_j$  ein Vielfaches der Einheitsmatrix, also  $P_j(h) = \alpha_j(h) I_{c_j}$ . Damit haben wir schließlich

$$\tilde{P}_j(g_k H g_\ell H) = \alpha_j(h) \tilde{P}_j(g_k H) \tilde{P}_j(g_\ell H) ,$$

d.h.  $\tilde{P}_j$  ist eine projektive Darstellung von  $G/H$ . Entsprechend definiert man die projektive Darstellung  $\tilde{Q}_j$  von  $G/H$ . Für  $\tilde{P}_j, \tilde{Q}_j$  gilt

$$A_j \tilde{P}_j(g_k H) = A_j P_j(g_k) = Q_j(g_k) A_j = \tilde{Q}_j(g_k H) A_j ,$$

d.h.  $A_j$  hat die Symmetrien von  $\tilde{P}_j, \tilde{Q}_j$ .

□

### 4.3 Direkte Produkte

Sei  $G$  das direkte Produkt der Gruppen  $G_1, G_2$ , also  $G = G_1 \otimes G_2$ . Sind  $R_i, Q_i$  Darstellungen von  $G_i$  der Grade  $n_i, m_i$ , so sind

$$P(st) = P_1(s) \otimes P_2(t), \quad Q(st) = Q_1(s) \otimes Q_2(t), \quad s \in G_1, \quad t \in G_2$$

Darstellungen von  $G$  der Grade  $n = n_1 n_2, m = m_1 m_2$ .

**Satz 4.3.1** *Die  $(m, n)$ -Matrix  $A$  hat genau dann die Symmetrien von  $P, Q$ , wenn  $A$  eine  $(m_1, n_1)$ -Matrix von  $(m_2, n_2)$ -Matrizen  $A_{j,k} = (A_{j,k}^{\nu,\mu})$  ist mit folgenden Eigenschaften:  $A_{j,k}$  hat die Symmetrien von  $P_2, Q_2$ , und die  $(m_1, n_1)$ -Matrizen  $A^{\nu,\mu} = (A_{j,k}^{\nu,\mu})$  haben die Symmetrien von  $P_1, Q_1$ .*

**Beweis:** Wegen der Rechenregeln des Tensorproduktes gilt  $A(P_1 \otimes P_2) = (Q_1 \otimes Q_2)A$  genau dann, wenn  $A(I_{n_1} \otimes P_2) = (I_{m_1} \otimes Q_2)A$  und  $A(P_1 \otimes I_{n_2}) = (Q_1 \otimes I_{m_2})A$  gilt. Die erste dieser Beziehungen bedeutet  $A_{j,k} P_2 = Q_2 A_{j,k}$ , d.h.  $A_{j,k}$  hat die Symmetrien von  $P_2, Q_2$ . Die zweite Beziehung lautet ausführlich geschrieben

$$\begin{aligned} & \begin{pmatrix} A_{11}, \dots, A_{1,n_1} \\ \vdots \\ A_{n_1,1}, \dots, A_{m_1,n_1} \end{pmatrix} \begin{pmatrix} p_1^{1,1} I_{n_2}, \dots, p_1^{1,n_1} I_{n_2} \\ \vdots \\ p_1^{n_1,1} I_{n_2}, \dots, p_1^{n_1,n_1} I_{n_2} \end{pmatrix} \\ &= \begin{pmatrix} q_1^{1,1} I_{m_2}, \dots, q_1^{1,m_1} I_{m_2} \\ \vdots \\ q_1^{m_1,1} I_{m_2}, \dots, q_1^{m_1,m_1} I_{m_2} \end{pmatrix} \begin{pmatrix} A_{1,1}, \dots, A_{1,n_1} \\ \vdots \\ A_{m_1,1}, \dots, A_{m_1,n_1} \end{pmatrix}, \end{aligned}$$

wo natürlich  $P_1 = (P_1^{i\ell}), Q_1 = (q_1^{i\ell})$  ist. Dies bedeutet

$$\sum_{k=1}^{n_1} A_{j,k} P_1^{k,\ell} = \sum_{k=1}^{m_1} q_1^{j,k} A_{k,\ell}, \quad j = 1, \dots, m_1, \quad \ell = 1, \dots, n_1,$$

oder, elementweise

$$\sum_{k=1}^{n_1} A_{j,k}^{\nu,\mu} P_1^{k,\ell} = \sum_{k=1}^{m_1} q_1^{j,k} A_{k,\ell}^{\nu,\mu}.$$

Dies bedeutet aber gerade  $A^{\nu,\mu} P_1 = Q_1 A^{\nu,\mu}$ , d.h.  $A^{\nu,\mu}$  hat die Symmetrien von  $P_1, Q_1$ .

□

Diesen Satz wollen wir auf Faltungen auf  $G$  anwenden.

Diese haben wir schon in III.3.5 eingeführt durch

$$(x \star y)_g = \sum_{\substack{u,s \in G \\ us=g}} x_s y_u = \sum_{u \in G} x_{u^{-1}g} y_u .$$

Sei  $P$  die reguläre Darstellung von  $G$ , d.h.

$$P(t)x = \sum_{g \in G} x_{t^{-1}g} e_g \quad \text{für} \quad x = \sum_{g \in G} x_g e_g$$

mit einer Basis  $(e_g)_{g \in G}$  des Darstellungsraumes von  $P$ . Dann ist

$$\begin{aligned} P(t)(x \star y) &= \sum_{g \in G} (x \star y)_{t^{-1}g} e_g = \sum_{g \in G} \sum_{us=t^{-1}g} x_s y_u e_g \\ &= \sum_{g \in G} \sum_{vs=g} x_s y_{t^{-1}v} e_g = x \star P(t)y . \end{aligned}$$

Die Faltung  $X = (x_{u^{-1}t})_{t,u \in G}$  hat also die Symmetrien von  $\rho$ , und umgekehrt ist jede  $(|G|, |G|)$ -Matrix  $X$  mit dieser Eigenschaft eine Faltung.

Diesen Satz wollen wir auf Faltungen auf  $G$  anwenden.

Sei  $P$  die reguläre Darstellung von  $G$ . Diese läßt sich aus den regulären Darstellungen  $P_1, P_2$  von  $G_1, G_2$  leicht gewinnen.

**Satz 4.3.2** *Seien  $P_1, P_2$  die reguläre Darstellungen von  $G_1, G_2$ . Dann gilt für die reguläre Darstellung  $P$  von  $G_1 \otimes G_2$*

$$P(st) = P_1(s) \otimes P_2(t) , \quad s \in G_1 , \quad t \in G_2 .$$

**Beweis.** Sei  $G_1 = \{s_1, \dots, s_n\}$ ,  $G_2 = \{t_1, \dots, t_m\}$  und  $G = \{s_1 t_1, \dots, s_1 t_m, s_2 t_1, \dots, s_2 t_m, \dots, s_n t_1, \dots, s_n t_m\}$ . Es ist nach Definition der regulären Darstellung

$$P_1(s_j) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\pi_j(1)} \\ \vdots \\ x_{\pi_j(n)} \end{pmatrix} , \quad P_2(t_k) \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_{\sigma_k(1)} \\ \vdots \\ x_{\sigma_k(m)} \end{pmatrix} ,$$

wobei  $\pi_j$  die Permutation mit  $s_j^{-1}s_\ell = s_{\pi_j(\ell)}$  ist; entsprechend ist  $\sigma$  die Permutation mit  $t_k^{-1}t_i = t_{\sigma_k(i)}$ . Sei nun  $x \in \mathbb{C}^{nm}$  aufgespalten in

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^m.$$

Der Vektor  $P_1(s_j) \otimes P_2(t_k)x$  entsteht dann aus  $x$  durch zwei Operationen.

1. Man übt auf die Komponenten jedes  $x_i$  der Permutation  $\sigma_k$  aus.

2. Man übt auf  $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  die Permutation  $\pi_j$  aus.

Genau diese Permutation übt aber auch  $P(s_j t_k)$  aus, denn es ist

$$\begin{aligned} (s_j t_k)^{-1} s_\ell t_i &= t_k^{-1} s_j^{-1} s_\ell t_i \\ &= s_j^{-1} s_\ell t_k^{-1} t_i \\ &= s_{\pi_j(\ell)} t_{\sigma_k(i)}. \end{aligned}$$

Also ist  $P(s_j t_k) = P_1(s_j) \otimes P_2(t_k)$ .

□

**Bemerkung:** Diese Formel gilt nur, wenn  $G$  so angeordnet wird (lexikographisch), wie es im Beweis gemacht wurde.

**Satz 4.3.3** *Sei  $A$  die Faltung auf  $G$  und  $G = G_1 \otimes G_2$ . Die Faltung auf  $G_1$  werden beschrieben durch die Permutation  $\pi_j$ , d.h. sie sind von der Gestalt*

$$\begin{pmatrix} x_{\pi_1(1)} & \cdots & x_{\pi_1(n)} \\ \vdots & & \\ x_{\pi_n(1)} & \cdots & x_{\pi_n(n)} \end{pmatrix}$$

Dann gibt es Faltungen  $A_1, \dots, A_n$  auf  $G_2$ , so daß

$$A = \begin{pmatrix} A_{\pi_1(1)} & \cdots & A_{\pi_1(n)} \\ \vdots & & \\ A_{\pi_n(1)} & \cdots & A_{\pi_n(n)} \end{pmatrix}.$$

**Beweis:** Folgt sofort aus den beiden vorigen Sätzen.

□

## 4.4 Die Fourier-Transformation auf Gruppen

Sei  $G$  eine endliche Gruppe und  $\hat{G}$  ein MIP von  $G$ . Ist  $G$  abelsch, so ist  $\hat{G}$  wieder eine Gruppe, der Dual von  $G$ .

**Definition 4.4.1** Sei  $f$  eine komplexwertige Funktion auf  $G$ . Dann heißt die Funktion  $\hat{f}$  auf  $\hat{G}$ , welche durch

$$\hat{f}(\xi) = \frac{1}{n} \sum_{g \in G} f(g) \rho(g), \quad \rho \in \hat{G}$$

definiert ist, Fourier-Transform von  $f$ .

### Bemerkungen:

1) Da  $\hat{G}$  durch  $G$  nicht eindeutig bestimmt ist, gibt es in Wahrheit viele Fourier-Transformationen auf  $G$ . Wir ignorieren diese Mehrdeutigkeit, denken uns  $\hat{G}$  also ein für allemal gewählt.

2) Ist  $d_\rho$  der Grad von  $\rho$ , so gilt nach Satz 2.2.7  $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$ .

Da  $\hat{f}(\rho)$  für jedes  $\rho$  durch  $d_\rho^2$  Matrix-Element bestimmt ist, enthält  $\hat{f}$  die gleiche Anzahl von Freiheitsgraden wie  $f$ , nämlich  $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$ . Wir können die Fourier-Transformation ansehen als lineare Abbildung von  $\mathbb{C}^n$ ,  $n = |G|$  in  $\bigoplus_{\rho \in \hat{G}} \mathbb{C}^{d_\rho^2}$ , oder aber als lineare Abbildung von  $\mathbb{C}^n$  in  $\mathbb{C}^n$ .

3) Die Anzahl der Rechenoperationen (= 1 komplexe Multiplikation + 1 komplexe Addition) für die Fourier-Transformation ist offenbar

$$\sum_{\rho \in \hat{G}} |G| d_\rho^2 = |G|^2.$$

**Bespiele:**

1)  $G = C_n = \{1, a, \dots, a^{n-1}\}$ ,  $a^n = 1$ ,  $\hat{G} = \{\rho_0, \dots, \rho_{n-1}\}$  mit  $\rho_j(a^k) = \omega^{jk}$ ,  $\omega = e^{-2\pi i/n}$ . Dann ist  $\hat{f}$  die gewöhnliche Fourier-Transformation der Länge  $n$ .

2) Sei  $G = C_{n_1} \otimes \dots \otimes C_{n_p} = \{a_1^{k_1} a_p^{k_p} : 0 \leq k_r < n_r\}$ ,  $a_r^{n_r} = 1$ , und  $\hat{G} = \{\rho_{j_1, \dots, j_p} : 0 \leq j_r < n_r, r = 1, \dots, p\}$ ,

$$\rho_{j_1, \dots, j_p}(a_1^{k_1} \dots a_p^{k_p}) = \omega_1^{j_1 k_1} \dots \omega_p^{j_p k_p}$$

mit  $\omega_r = e^{-2\pi i/n_r}$ . Dann ist

$$\hat{f}(\rho_{j_1, \dots, j_p}) = \frac{1}{n_1 \dots n_p} \sum_{k_1=0}^{n_1-1} \dots \sum_{k_p=0}^{n_p-1} f(a_1^{k_1} \dots a_p^{k_p}) \omega_1^{j_1 k_1} \dots \omega_p^{j_p k_p} .$$

Dies ist die  $p$ -dimensionale Fourier-Transformation.

3)  $G = C_2 \otimes \dots \otimes C_2$  ( $p$  mal). Dann erhalten wir aus Beispiel 2 - in geringfügig geänderter Notation -

$$\hat{f}_{j_1, \dots, j_p} = 2^{-p} \sum_{0 \leq k_1, \dots, k_p \leq 1} f_{k_1, \dots, k_p} (-1)^{j_1 k_1 + \dots + j_p k_p} .$$

Dies ist die Hadamard-Walsh-Transformation.

**Satz 4.4.2** Die Fourier-Transformation ist injektiv, und es gilt

$$f(g) = \sum_{\rho \in \hat{G}} d_\rho \operatorname{tr}(\hat{f}(\rho) \rho(g^{-1})) ,$$

wobei  $d_\rho$  der Grad von  $\rho$  ist.

**Beweis:** Es ist

$$\begin{aligned}
\sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr}(\hat{f}(\rho)) \rho(g^{-1}) &= \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr} \left( \sum_{t \in G} f(t) \rho(t) \rho(g^{-1}) \right) \\
&= \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr} \left( \sum_{t \in G} f(t) \rho(tg^{-1}) \right) \\
&= \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr} \left( \sum_{s \in G} f(sg) \rho(s) \right) \\
&= \frac{1}{|G|} \sum_{s \in G} f(sg) \sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr}(\rho(s)) \\
&= \frac{1}{|G|} \sum_{s \in G} f(sg) \chi_{\text{reg}}(s) ,
\end{aligned}$$

mit dem regulären Charakter  $\chi_{\text{reg}}$ , vgl. II.2. Nun ist aber

$$\chi_{\text{reg}}(s) = \begin{cases} |G| & , \quad s = 1 , \\ 0 & , \quad \text{sonst} . \end{cases}$$

Also folgt

$$\sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr}(\hat{f}(\rho)) \rho(g^{-1}) = f(g) .$$

□

**Bemerkung:** Auch die inverse Fourier-Transformation erfordert

$$|G| \sum_{\rho \in \hat{G}} d_{\rho}^2 = |G|^2$$

Rechenoperationen.

**Satz 4.4.3** Sei  $f \star g$  die Faltung von  $f, g$  auf  $G$ . Dann gilt

$$(f \star g)^{\wedge}(\rho) = |G| \hat{f}(\rho) \hat{g}(\rho) .$$

**Beweis:** Es ist

$$\begin{aligned}
 (f \star g)^\wedge(\rho) &= \frac{1}{|G|} \sum_{t \in G} (f \star g)(t) \rho(t) \\
 &= \frac{1}{|G|} \sum_{t \in G} \sum_{s \in G} f(s^{-1}t) g(s) \rho(t) \\
 &= \frac{1}{|G|} \sum_{s \in G} g(s) \rho(s) \sum_{t \in G} \rho(s^{-1}t) f(s^{-1}t) \\
 &= \frac{1}{|G|} \sum_{s \in G} g(s) \rho(s) \sum_{t \in G} f(t) \rho(t) \\
 &= |G| \hat{g}(\rho) \hat{f}(\rho).
 \end{aligned}$$

□

Aus 4.3 wissen wir, daß die  $(n, n)$ -Matrix  $A$  ( $n = |G|$ ) genau dann eine Faltung auf  $G$  ist, wenn sie mit der regulären Darstellung  $P$  von  $G$  vertauschbar ist. Nach Satz 4.1.2 zerfällt  $A$  also in  $|\hat{G}|$  Matrizen  $I_{d_\rho} \otimes A_\rho$  mit  $(d_\rho, d_\rho)$ -Matrizen  $A_\rho$ . Die Anwendung von  $A$  auf einen Vektor  $x$  der Länge  $n = |G|$  ist also äquivalent der Anwendung der Matrizen  $A_\rho$  auf  $d_\rho$  Vektoren der Länge  $d_\rho$ ,  $\rho \in \hat{G}$ . Die Komplexität von  $x \rightarrow Ax$  fällt also von  $|G|^2$  auf

$$\sum_{\rho \in \hat{G}} d_\rho^3 \leq |G| \max_{\rho \in \hat{G}} |d_\rho|.$$

Dabei haben wir die Matrix  $X = Y$  in (4.1.3) noch nicht berücksichtigt. Den gleichen Rechenaufwand erhält man, wenn man  $Ax$  nach Satz 4.4.3 berechnet.  $X$  wird also - wie im Falle  $G = C_n$  - durch die Fourier-Transformation geliefert.

Nun zur Fourier-Transformation. Wir berechnen

$$\begin{aligned}
 (P(g)f)^\wedge(\rho) &= \frac{1}{|G|} \sum_{t \in G} (P(g)f)(t) \rho(t) \\
 &= \frac{1}{|G|} \sum_{t \in G} f(g^{-1}t) \rho(t) = \frac{1}{|G|} \sum_{s \in G} f(s) \rho(gs) \\
 &= \rho(g) \hat{f}(\rho).
 \end{aligned}$$

Ist also  $W_G : \mathbb{C}^n \rightarrow \bigotimes_{\rho \in \hat{G}} \mathbb{C}^{d_\rho^2}$  die Fourier-Transformation auf  $G$  und  $Q(g) = \bigotimes_{\rho \in \hat{G}} \rho(g)$ , so ist

$$W_G P(g) = Q(g) W_G, \quad \forall g \in G$$

d.h.  $W_G$  hat die Symmetrien von  $P, Q$ . Damit können wir alle Methoden zur Konstruktion schneller Fourier-Transformationen, die wir für zyklische Gruppen kennengelernt haben, auf allgemeine Gruppen übertragen. Wir wollen dies am Beispiel von direkten Produkten durchführen.

**Satz 4.4.4** Sei  $G = G_1 \otimes \dots \otimes G_r$ . Dann läßt sich die Fourier-Transformation auf  $\mathbb{C}$  in

$$|G| \sum_{j=1}^p |G_j|$$

Rechenoperationen durchführen.

**Beweis:** Wir zeigen den Satz für  $G = A \otimes B$ . Sind  $\hat{A}, \hat{B}$  MIP's für  $A, B$ , so ist durch

$$\rho(ab) = \sigma(a) \otimes \tau(b), \quad \sigma \in \hat{A}, \quad \tau \in \hat{B}, \quad a \in A, \quad b \in B$$

ein MIP  $\hat{G}$  für  $G$  definiert, und es ist

$$\begin{aligned} \hat{f}(\sigma \otimes \tau) &= \frac{1}{|A||B|} \sum_{\substack{a \in A \\ b \in B}} f(ab) \sigma(a) \otimes \tau(b) \\ &= \frac{1}{|A||B|} \sum_{a \in A} \sigma(a) \otimes \sum_{b \in B} f(ab) \tau(b). \end{aligned}$$

Die Auswertung der  $b$ -Summe für ein  $a$  benötigt  $|B|d_\tau^2$  Rechenoperationen, die Ausführung des Tensorprodukts für ein  $a$  deren  $d_\sigma^2 d_\tau^2$  ( $d_\sigma, d_\tau$  sind natürlich die Grade von  $\sigma, \tau$ ). Damit verlangt  $\hat{f}$

$$\begin{aligned} |A| \sum_{\tau \in \hat{B}} |B| d_\tau^2 + \sum_{\sigma \in \hat{A}} \sum_{\tau \in \hat{B}} |A| d_\sigma^2 d_\tau^2 \\ = |A| |B|^2 + |A|^2 |B| = |G|(|A| + |B|) \end{aligned}$$

Rechenoperationen.

□



# Kapitel 5

## Toeplitz-Matrizen

### 5.1 Der Algorithmus von Trench

Im letzten Abschnitt haben wir effiziente Algorithmen zur zyklischen Faltung definiert. Wir hatten gezeigt, daß die Faltung zweier Vektoren der Anwendung einer Matrix  $A$  entspricht mit  $A = P^t A P$  und  $P = (e_2, e_3, \dots, e_n, e_1)$ . Hierbei bewirkt die Rechtsmultiplikation mit  $P$  eine zyklische Verschiebung der Spalten nach links, eine Linksmultiplikation mit  $P^t$  eine zyklische Verschiebung der Zeilen nach oben.

Wir definieren nun die Toeplitz-Matrizen als Erweiterung des Matrizenraums der zyklischen Faltung.

**Definition 5.1.1** *Eine  $(n, n)$ -Matrix der Form*

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{-1} & \ddots & \ddots & & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{-(n-2)} & & \ddots & \ddots & a_1 \\ a_{-(n-1)} & a_{-(n-2)} & \cdots & a_{-1} & a_0 \end{pmatrix}$$

*heißt Toeplitz-Matrix. A ist symmetrische Faltung genau dann, wenn a periodisch ist mit Periode n.*

**Bemerkung:** Für alle Toeplitz-Matrizen  $A$  gilt  $\text{rang}(A - P^tAP) \leq 2$ , denn

$$A - P^tAP = \begin{pmatrix} 0 & \cdots & 0 & a_{n-1} - a_{-1} \\ \vdots & & \vdots & \vdots \\ 0 & & 0 & a_1 - a_{n+1} \\ a_{-(n-1)} - a_1 & \cdots & a_{-1} - a_{n-1} & 0 \end{pmatrix}.$$

Der Rang ist also zwar nicht mehr unbedingt 0, aber klein.

**Satz 5.1.2** Für eine  $(n, n)$  Toeplitz-Matrix  $A$  und einen Vektor  $x$  kann  $Ax$  durch eine zyklische Faltung der Länge  $M \geq 2n - 1$  berechnet werden.

**Beweis:** Wir erweitern  $A$  sinnvoll so, daß sich eine zyklische Faltung ergibt. Sei  $A$  definiert durch den Vektor  $a_k$ ,  $k = -n - 1 \dots n - 1$ . Definiere den Vektor  $\alpha_k$  aus  $\mathbb{C}^M$ ,  $k = -M - 1 \dots M - 1$ , durch

$$\alpha_k := \begin{cases} a_k & -n - 1 \leq k \leq n - 1 \\ a_{k-M} & k > M - n \\ a_{k+M} & k < n - M \\ 0 & \text{sonst.} \end{cases}.$$

Der so definierte Vektor ist periodisch mit der Periode  $M$ .  $\alpha$  definiert eine  $(M, M)$ -Toeplitz-Matrix  $A'$ , die eine zyklische Faltung ist, und deren linke obere  $(n, n)$ -Untermatrix mit  $A$  übereinstimmt. Wir wenden  $A'$  auf den Vektor

$$x' = \begin{pmatrix} x \\ 0 \end{pmatrix} \in \mathbb{C}^M$$

an. Da  $A_{i,k} = A'_{i,k}$  für  $i = 1 \dots n$ ,  $k = 1 \dots n$  gilt

$$A'x' = \begin{pmatrix} Ax \\ y \end{pmatrix}$$

und wir haben  $Ax$  berechnet. Dieses Vorgehen heißt aus naheliegenden Gründen "zero-padding".

**Beispiel:** Wir betrachten ein Beispiel mit  $n = 3$  und  $M = 6$ . Dann gilt

$$A = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_{-1} & a_0 & a_1 \\ a_{-2} & a_{-1} & a_0 \end{pmatrix}$$

und

$$A' = \begin{pmatrix} a_0 & a_1 & a_2 & 0 & a_{-2} & a_{-1} \\ a_{-1} & a_0 & a_1 & a_2 & 0 & a_{-2} \\ a_{-2} & a_{-1} & a_0 & a_1 & a_2 & 0 \\ 0 & a_{-2} & a_{-1} & a_0 & a_1 & a_2 \\ a_2 & 0 & a_{-2} & a_{-1} & a_0 & a_1 \\ a_1 & a_2 & 0 & a_{-2} & a_{-1} & a_0 \end{pmatrix}.$$

**Bemerkung:** Wir haben insbesondere gezeigt, daß sich jede zyklische Faltung der Länge  $n$  auch als zyklische Faltung der Länge  $M$  mit  $M > n$  berechnen läßt. Daher beschränken sich viele Bibliotheken auf die Betrachtung von Faltungen z.B. der Länge  $2^p$ .

**Bemerkung:** Fouriertransformationen von der Ordnung  $p^n$  mit  $p \neq 2$  prim lassen sich im wesentlichen als Faltungen schreiben. Der Satz liefert uns damit auch Verfahren zur schnellen Durchführung von Fouriertransformationen, wenn nur wenige Faltungsalgorithmen implementiert sind.

**Bemerkung:** Toeplitz-Matrizen tauchen zum Beispiel in der Computertomographie auf. Es muß das Gleichungssystem  $Ax = b$  mit einer Toeplitz-Matrix  $A$  gelöst werden. Wir untersuchen daher jetzt den Aufwand zur Lösung dieses Gleichungssystems.

**Satz 5.1.3** Sei  $A$  eine  $(n, n)$  Toeplitz-Matrix. Alle Hauptminoren von  $A$  seien ungleich null (z.B.  $A$  positiv definit). Dann kann das Gleichungssystem  $Ax = b$  mit  $\frac{13}{4}n^2 + O(n)$  Operationen gelöst werden.

**Beweis:** Wir definieren eine Hierarchie von Matrizen  $A_k$  für  $k = -(n-1) \dots (n-1)$ ,  $A_0 := A$ . Für  $k > 0$  sind  $k$  Nebendiagonalen oberhalb der

Hauptdiagonalen 0, für  $k < 0$  sind  $k$  Nebendiagonalen unterhalb der Hauptdiagonalen 0. Es gilt also für  $k > 0$

$$A_k = \begin{pmatrix} * & 0 & \cdots & 0 & * & \cdots & * \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & * \\ \vdots & & & \ddots & \ddots & & 0 \\ \vdots & & & & \ddots & \ddots & \vdots \\ \vdots & & & & & \ddots & 0 \\ * & \cdots & \cdots & \cdots & \cdots & \cdots & * \end{pmatrix}.$$

$A_{-k}$  hat die transponierte Gestalt, aber nicht notwendig mit denselben Einträgen für die Elemente mit  $*$ .

Wir beschreiben den Algorithmus für  $n = 4$ , indem wir elementare Zeilenumformungen von  $A$  angeben, die  $A_k$  erzeugen. Wir starten mit der Matrix  $A = A_0$  und konstruieren  $A_{-1}$  und  $A_1$  gleichzeitig.

$$A_0 = \begin{pmatrix} a_0^0 & a_1^0 & a_2^0 & a_3^0 \\ a_{-1}^0 & a_0^0 & a_1^0 & a_2^0 \\ a_{-2}^0 & a_{-1}^0 & a_0^0 & a_1^0 \\ a_{-3}^0 & a_{-2}^0 & a_{-1}^0 & a_0^0 \end{pmatrix}, \quad A_0 = \begin{pmatrix} a_0^0 & a_1^0 & a_2^0 & a_3^0 \\ a_{-1}^0 & a_0^0 & a_1^0 & a_2^0 \\ a_{-2}^0 & a_{-1}^0 & a_0^0 & a_1^0 \\ a_{-3}^0 & a_{-2}^0 & a_{-1}^0 & a_0^0 \end{pmatrix}.$$

Aus der linken Matrix konstruieren wir  $A_{-1}$ . Die oberste Zeile hat bereits die richtige Form. Für  $k > 1$  ziehen wir von Zeile  $k$  das  $\frac{a_{-1}^0}{a_0^0}$ -fache der  $k-1$ . Zeile der rechten Matrix ab. In der rechten Matrix ziehen wir für  $k < n$  von Zeile  $k$  das  $\frac{a_0^0}{a_1^0}$ -fache der  $k+1$ . Zeile der linken Matrix ab. Dadurch erhalten wir folgende Matrizen:

$$A_{-1} = \begin{pmatrix} a_0^0 & a_1^0 & a_2^0 & a_3^0 \\ 0 & a_0^{-1} & a_1^{-1} & a_2^{-1} \\ a_{-2}^{-1} & 0 & a_0^{-1} & a_1^{-1} \\ a_{-3}^{-1} & a_{-2}^{-1} & 0 & a_0^{-1} \end{pmatrix}, \quad A_1 = \begin{pmatrix} a_0^1 & 0 & a_2^1 & a_3^1 \\ a_{-1}^1 & a_0^1 & 0 & a_2^1 \\ a_{-2}^1 & a_{-1}^1 & a_0^1 & 0 \\ a_{-3}^0 & a_{-2}^0 & a_{-1}^0 & a_0^0 \end{pmatrix}.$$

Die Operation ist durchführbar, denn  $a_0^0$  ist der erste Hauptminor der Matrix  $A$  und damit nicht Null. Zur Durchführung dieses Schritts müssen wir einmal dividieren und links und rechts  $2n - 2$  Elemente neu berechnen. Da dieselbe Rechnung auch auf der rechten Seite ( $b$ ) durchgeführt werden muß, benötigen wir insgesamt  $2(3n - 3)$  Rechenoperationen und eine Division.

Im nächsten Schritt bringen wir die nächste Diagonale auf Null. Man sieht schnell, daß dies nicht durch elementare Zeilenumformungen innerhalb der Matrizen möglich ist. Da wir aber wissen, daß gleichzeitig  $A_{-1}x = b_{-1}$  und  $A_1x = b_1$ , können wir auch Zeilen der rechten Matrix auf die linke addieren und umgekehrt. Für  $k \leq 2$  hat  $A_{-1}$  bereits die richtige Form. Für  $k > 2$  addieren wir zu Zeile  $k$  der linken Matrix das  $\frac{a_{-2}^1}{a_0^1}$ -fache der  $(k - 2)$ . Zeile der rechten Matrix. Für  $k < n + 1 - 2$  addieren wir zur Zeile  $k$  der rechten Matrix das  $\frac{a_2^1}{a_0^1}$ -fache der  $(k + 2)$ . Zeile der linken Matrix. Wir erhalten

$$A_{-2} = \begin{pmatrix} a_0^0 & a_1^0 & a_2^0 & a_3^0 \\ 0 & a_0^{-1} & a_1^{-1} & a_2^{-1} \\ 0 & 0 & a_0^{-2} & a_1^{-2} \\ a_{-3}^{-2} & 0 & 0 & a_0^{-2} \end{pmatrix}, \quad A_2 = \begin{pmatrix} a_0^2 & 0 & 0 & a_3^2 \\ a_{-1}^2 & a_0^2 & 0 & 0 \\ a_{-2}^1 & a_{-1}^1 & a_0^1 & 0 \\ a_{-3}^0 & a_{-2}^0 & a_{-1}^0 & a_0^0 \end{pmatrix}.$$

Die Divisionen sind wieder ausführbar. Die obere linke  $(2, 2)$ -Teilmatrix von  $A_1$  ist durch elementare Zeilenumformungen aus der oberen linken  $(2, 2)$ -Teilmatrix von  $A$  hervorgegangen (genauer Beweis in den Aufgaben). Diese ist invertierbar, denn der zweite Hauptminor ist nicht Null, also ist  $a_0^2$  nicht Null. Der Rechenaufwand für diesen Schritt ist eine Division und  $2(3n - 6)$  Operationen.

Wir beschreiben nun Schritt  $j$ . Seien also  $A_{j-1}$  und  $A_{-(j-1)}$  bereits berechnet. Addiere für  $j + 1 \leq k \leq n$  auf die  $k$ . Zeile der linken Matrix das  $\frac{a_{-j}^{j+1}}{a_0^{j+1}}$ -fache der  $(k - j)$ . Zeile der rechten Matrix. Addiere für  $1 \leq k \leq n - j$  das  $\frac{a_j^{j-1}}{a_0^{j-1}}$ -fache der  $(k + j)$ . Zeile der linken Matrix auf die  $k$ . Zeile der rechten Matrix.

Der Aufwand zur Umformung einer Matrix und seiner rechten Seite beträgt damit  $3(n-j)$  für Schritt  $j$ . Insgesamt erhalten wir einen Aufwand von

$$\sum_{j=1}^{n-1} 2(3n-j) = 3n^2 + O(n).$$

Wir müssen das Gleichungssystem nun noch lösen durch Rückwärts- und Vorwärtseinsetzen. Für die ersten  $\frac{n}{2}$  Variablen benutzen wir  $A_{-(n-1)}$  und Vorwärtseinsetzen, für den Rest  $A_{n-1}$  und Rückwärtseinsetzen, macht noch einmal  $2\frac{1}{2} \left(\frac{n}{2}\right)^2$  Operationen, insgesamt also  $13\frac{n^2}{4}$  Rechenoperationen.

## 5.2 Der Algorithmus von Morf

Wir wollen den Begriff der Toeplitz-Matrix noch einmal verallgemeinern. Wir hatten oben bereits gesehen, daß für den Rang  $d$  der Matrix  $A - P^t A P$  einer Toeplitz-Matrix  $A$  immer  $d \leq 2$  gilt. Wir definieren den  $+-$  und  $--$ -Verschiebungsrang.

**Definition 5.2.1** Sei  $M$  die  $(n, n)$ -Matrix  $(e_2, e_3, \dots, e_n, 0)$ . Für eine  $(n, n)$ -Matrix  $A$  nennen wir

$$\alpha_+(A) := \text{rk}(A - MAM^t)$$

$$\alpha_-(A) := \text{rk}(A - M^t A M)$$

den  $+-$  bzw.  $--$ -Verschiebungsrang von  $A$ .

Sei  $A = (a_{ik})$ ,  $i = 1, \dots, n$ ,  $k = 1, \dots, n$ . Dann ist

$$MAM^t = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{pmatrix}$$

und

$$M^t A M = \begin{pmatrix} a_{2,2} & \cdots & a_{2,n} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n,2} & \cdots & a_{n,n} & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

**Beispiel:** Toeplitz-Matrizen haben den Veriebungsrang  $\alpha_+(A) = \alpha_-(A) \leq 2$ .

**Satz 5.2.2** Für invertierbare Matrizen gilt:

$$\alpha_+(A) = \alpha_-(A^{-1}).$$

**Beweis:** Wir zeigen zunächst den Hilfssatz:

Für beliebige  $(n, n)$ -Matrizen  $A$  und  $B$  gilt:

$$\text{rk}(I - AB) = \text{rk}(I - BA)$$

**Beweis des Hilfssatzes:** Sei  $(x_1, \dots, x_m)$  eine Basis des Kerns von  $(I - AB)$ , und  $y_i := Bx_i$ . Die  $y_i$  sind linear unabhängig, denn sonst wären die  $Ay_i = ABx_i = x_i$  linear abhängig. Außerdem gilt

$$(I - BA)y_i = (I - BA)Bx_i = B(I - AB)x_i = 0$$

und die  $y_i$  sind im Kern von  $(I - BA)$  enthalten. Die Dimension des Kerns von  $(I - BA)$  ist also mindestens so groß wie die Dimension des Kerns von  $(I - AB)$  und es gilt

$$\text{rk}(I - BA) \leq \text{rk}(I - AB).$$

Durch Vertauschen von  $A$  und  $B$  erhält man den Hilfssatz.

**Beweis des Satzes:**

$$\begin{aligned}
\alpha_+(A) &= \text{rk}(I - MAM^t) \\
&= \text{rk}((I - MAM^t A^{-1})A) \\
&= \text{rk}(I - MAM^t A^{-1}) \\
&= \text{rk}(I - M^t A^{-1}MA) \quad \text{nach dem Hilfssatz} \\
&= \text{rk}(A^{-1} - M^t A^{-1}MAA^{-1}) \\
&= \text{rk}(A^{-1} - M^t A^{-1}M) \\
&= \alpha_-(A^{-1}).
\end{aligned}$$

Für unsere weiteren Betrachtungen ist fundamental, daß sich Matrizen mit kleinem Verschiebungsrang als Summe einfacher Matrizen darstellen lassen. Wir definieren zunächst die unteren und oberen Dreiecks-Toeplitz-Matrizen durch

**Definition 5.2.3** Sei  $x \in \mathbb{C}^n$ ,  $x = (x_i)$ ,  $i = 0, \dots, n-1$ . Dann definieren wir die zugehörige untere  $(n, n)$  Dreiecks-Toeplitz-Matrix durch

$$L(x)_{i,i-l} := \begin{cases} x_l, & l \geq 0 \\ 0, & \text{sonst} \end{cases}, \text{ also } L(x) = \begin{pmatrix} x_0 & & 0 \\ \vdots & \ddots & \\ x_{n-1} & \cdots & x_0 \end{pmatrix}$$

und die zugehörige obere  $(n, n)$  Dreiecks-Toeplitz-Matrix durch

$$U(x) := L(x)^t.$$

Die Bezeichnungen  $U$  und  $L$  stehen natürlich für Upper und Lower.

**Satz 5.2.4** Seien  $x^j, y^j \in \mathbb{C}^n$ ,  $j = 1, \dots, \alpha$ ,  $\alpha > 0$ . Dann ist äquivalent:

1.  $A - MAM^t = \sum_{j=1}^{\alpha} x^j (y^j)^t$
2.  $A = \sum_{j=1}^{\alpha} L(x^j)U(y^j)$

**Beweis:** Wir zeigen zunächst  $2 \Rightarrow 1$ . Sei  $A = (a_{i,j}), i = 0, \dots, n-1, j = 0, \dots, n-1$ . Dann gilt

$$\begin{aligned} a_{k,l} &= \sum_{j=1}^{\alpha} \sum_i L(x^j)_{k,i} U(y^j)_{i,l} \\ &= \sum_{j=1}^{\alpha} \sum_{i=0}^{n-1} x_{k-i}^j y_{l-i}^j \end{aligned}$$

mit der Definition  $x_i = y_i = 0$  für  $i < 0$ . Wir definieren weiter  $a_{k,l} = 0$  für  $k < 1$  oder  $l < 1$ . Dann gilt

$$\begin{aligned} (A - MAM^t)_{k,l} &= a_{k,l} - a_{k-1,l-1} \\ &= \sum_{j=1}^{\alpha} \sum_{i=0}^{n-1} x_{k-i}^j y_{l-i}^j - x_{k-1-i}^j y_{l-1-i}^j \\ &= \sum_{j=1}^{\alpha} x_k^j y_l^j \\ &= \sum_{j=1}^{\alpha} (x^j (y^j)^t)_{k,l} \end{aligned}$$

und  $A - MAM^t = \sum_{j=1}^{\alpha} x^j (y^j)^t$ .

Die umgekehrte Richtung folgt sofort (Übungen).

**Satz 5.2.5** *Zu jeder  $(n, n)$  Matrix  $A$  gibt es Vektoren  $x^j, y^j, j = 1, \dots, \alpha_+(A)$ , und Vektoren  $\tilde{x}^j, \tilde{y}^j, j = 1, \dots, \alpha_-(A)$ , so daß*

$$A = \sum_{j=1}^{\alpha_+(A)} L(x^j)U(y^j) \text{ und } A = \sum_{j=1}^{\alpha_-(A)} U(\tilde{y}^j)L(\tilde{x}^j).$$

**Beweis:** Für die Matrix  $B := A - MAM^t$  vom Rang  $\alpha_+(A)$  gibt es Vektoren  $x_0, \dots, x_{k-1}$  und  $y_0, \dots, y_{k-1}$  mit

$$B = \sum_{j=1}^{\alpha} x^j (y^j)^t.$$

Nach Satz (??) folgt die Behauptung für  $A - MAM^t$ .

**Satz 5.2.6** Seien  $A, B$   $(n, n)$ -Matrizen mit festem von  $n$  unabhängigem Verschiebungsrang  $\alpha = \alpha_+(A)$ . Dann kann man die  $LU$ -Zerlegung von  $AB$  mit  $n \log n$  Operationen berechnen.

**Beweis:**

1. Die  $LU$ -Zerlegung von  $A$  kann nach dem Beweis von Satz ?? in  $O(n)$  berechnet werden. (Anmerkung: Mit hoher Wahrscheinlichkeit? nachfragen!) Das Bestimmen der l.u. Vektoren kann  $O(n^2)$  Operationen kosten.
2. Das Produkt von unteren oder oberen Toeplitz-Dreiecksmatrizen ist  $O(n \log n)$ . **Beweis der Zwischenbehauptung:**

$$\begin{aligned} (L(x)L(y))_{kl} &= \sum_{i=l}^k x_{k-i}y_{i-l}, \quad k \geq l \\ &= \sum_{j=0}^{k-l} x_j y_{k-l-j} =: z_i \end{aligned}$$

Die  $z_i$  können durch schnelle Faltungen berechnet werden in Zeit  $O(n \log n)$ .

3. Sei  $U$  eine obere,  $L$  eine untere Dreiecks-Toeplitz-Matrix. Dann kann man in  $O(n)$  untere bzw. obere Dreiecks-Toeplitz-Matrizen  $L_i, U_i$  berechnen mit

$$UL = \sum_{i=1}^3 L_i U_i$$

**Beweis:** Erweitere  $U$  und  $L$  wie im Beweis zu Satz ?? zu zyklischen Faltungen der Länge  $2n$ . Die Matrizen  $\tilde{U}$  und  $\tilde{L}$  haben dann die Form

$$\tilde{U} = \begin{pmatrix} \tilde{U} & \tilde{L}_1 L \\ \tilde{L}_2 & \tilde{U}_3 \end{pmatrix}, \quad \tilde{L} = \begin{pmatrix} L & \tilde{U}_1 \\ \tilde{U}_2 & \tilde{L}_3 \end{pmatrix}, \quad \tilde{U}\tilde{L} = \begin{pmatrix} UL + \tilde{L}_1 \tilde{U}_1 & * \\ * & * \end{pmatrix}.$$

Das Produkt dieser zyklischen Faltung ist wieder eine zyklische Faltung. Also ist es mit  $O(n \log n)$  Operationen berechenbar. Außerdem ist die Matrix  $LU - U_1 L_1$  Toeplitz, also  $LU - U_1 L_1 = \sum_{i=1}^3 L_i U_i$ , und die Zerlegung ist in  $O(n)$  berechenbar.

Wir setzen diese Ergebnisse nun zusammen. Gesucht sei das Produkt von  $A$  und  $B$ . Nach i) gilt

$$A = \sum_{i=1}^{\alpha} L_i U_i, \quad B = \sum_{i=1}^{\alpha} \tilde{L}_i \tilde{U}_i.$$

Damit gilt

$$AB = \sum_{i,j=1}^{\alpha} L_i U_i \tilde{L}_j U_j.$$

Nach Punkt iii) finden wir Matrizen mit

$$U_i \tilde{L}_j = \sum_{k=1}^3 L_k^{i,j} U_k^{i,j}$$

und

$$AB = \sum_{i,j,k=1}^3 L_i L_k^{i,j} U_k^{i,j} \tilde{U}_j = \sum_{j=1}^{3\alpha^2} \hat{L}_l \hat{U}_l.$$

Nach einem Satz ist die Multiplikation von Matrizen ungefähr so aufwendig wie die Inversion. Wir erwarten also, daß es einen schnellen Algorithmus auch zur Inversion von Matrizen mit kleinem Verschiebungsrang gibt.

Sei nun

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

mit  $(\frac{n}{2}, \frac{n}{2})$ -Matrizen  $A_{i,k}$ . In Lemma 2.3 zum Strassen-Algorithmus wurde diese Matrix bereits invertiert. Zur Blockinversion sind einige Produkte von Matrizen  $A_{i,k}$  und die Inversen der Matrizen  $A_{1,1}$  und  $A_{2,2} - A_{2,1} A_{1,1}^{-1} A_{1,2}$  zu berechnen. Wenn wir zeigen können, daß alle diese Matrizen kleinen Verschiebungsrang haben, können wir einen schnellen Algorithmus definieren.

**Satz 5.2.7** *Sei  $A$   $(n, n)$ -Matrix mit  $n = 2m$  wie oben aufgeteilt. Dann gilt:*

- $\alpha_+(A_{1,1}) \leq \alpha_+(A)$ .
- $\alpha_-(A_{2,2}) \leq \alpha_-(A)$ .
- $\alpha_+(A_{2,2}) \leq \alpha_+(A) + 2$ .
- $\alpha_+(A_{1,2}) \leq \alpha_+(A) + 1$ .
- $\alpha_+(A_{2,1}) \leq \alpha_+(A) + 1$ .
- $\alpha_+(A_{2,2} - A_{2,1}A_{1,1}^{-1}A_{1,2}) \leq \alpha_+(A)$ .

**Beweis:** Sei  $A = \sum L_i U_i$ . Spalte  $L_i$  und  $U_i$  auf wie  $A$  in Matrizen

$$L_j = \begin{pmatrix} L_j^{1,1} & 0 \\ L_j^{2,1} & L_j^{2,2} \end{pmatrix}, \quad U_j = \begin{pmatrix} U_j^{1,1} & U_j^{1,2} \\ 0 & U_j^{2,2} \end{pmatrix}, \quad L_j U_j = \begin{pmatrix} L_j^{1,1} U_j^{1,1} & L_j^{1,1} U_j^{1,2} \\ L_j^{2,1} U_j^{1,1} & L_j^{2,1} U_j^{1,2} + L_j^{2,2} U_j^{2,2} \end{pmatrix}$$

mit Dreiecks-Toeplitz-Matrizen  $L_j^{1,1}$ ,  $U_j^{1,1}$ ,  $L_j^{2,2}$  und  $U_j^{2,2}$  sowie mit Toeplitz-Matrizen  $L_j^{2,1}$  und  $U_j^{1,2}$ . Es gilt  $A = \sum_{j=1}^{\alpha_+(A)} L_j U_j$ . Aus dieser Darstellung folgt Punkt 1. Aus der entsprechenden  $UL$ -Darstellung folgt Punkt 2 und hieraus Punkt 3. Die Toeplitz-Matrizen kann man als Summe von Dreiecks-Toeplitz-Matrizen schreiben. Hieraus folgen 4 und 5. Die Matrix in Punkt 6 ist untere Teilmatrix von  $A^{-1}$ , also gilt

$$\alpha_+(A_{2,2} - A_{2,1}A_{1,1}^{-1}A_{1,2}) = \alpha_-(C_{2,2}) \leq \alpha_-(A^{-1}) \leq \alpha_+(A).$$

**Satz 5.2.8** *Die Inversion einer Matrix mit festem, von  $n$  unabhängigem Verschiebungsrang  $\alpha$  kann mit  $O(n(\log n)^2)$  Operationen durchgeführt werden.*

**Beweis:** Seien  $T(n)$  die benötigten Operationen zur Inversion einer  $(n, n)$ -Matrix. Dann gilt  $T(n) = 2T(n/2) + O(n \log n)$ . Nach Satz 1.1 der Vorlesung gilt damit auch  $T(n) = O(n(\log n)^2)$ .

# Literaturverzeichnis

- [1] **Baum, U.:** Existenz und effiziente Konstruktion schneller Fouriertransformationen auf überauflösbaren Gruppen, Dissertation Bonn 1991.
- [2] **Beth, T.:** Verfahren der schnellen Fourier-Transformation, Teubner Studienbücher, Informatik, 1984, ISBN 3-519-02363-6.
- [3] **Brigham, Oran E.:** FFT Schnelle Fourier-Transformation, R. Oldenbourg Verlag München Wien 1987, 3. verbesserte Aufl., ISBN 3-486-20347-9.
- [4] **Elliott, Douglas F. and K. Ramamohan Rao:** FAST TRANSFORMS Algorithms, Analysis, Applications, Academic Press, Inc., 1982, ISBN 0-12-237080-5.
- [5] **Knuth, D.E.:** The Art of Computer Programming, Vol. 2, Addison-Wesley 1969.
- [6] **Van Loan, Charles:** Computational Frameworks for the Fast Fourier Transform, SIAM *FRONTIERS in Applied Mathematics*, Philadelphia 1992, ISBN 0-89871-285-8.
- [7] **Mehlhorn, K.:** Effiziente Algorithmen, Teubner Verlag 1977.
- [8] **Meinel, C.:** Effiziente Algorithmen, Fachbuchverlag Leipzig, 1991.
- [9] **Müller, W.:** Darstellungstheorie von endlichen Gruppen, Teubner Verlag 1980.

- [10] **Nussbaumer, H.J.:** Fast Fourier Transform and Convolution Algorithms, Springer 1982.
- [11] **Pan, V.Ya.:** Methods of Computing Values of Polynomials, *Russian Math. Surveys* **21**, 105-136 (1966).
- [12] **Quinn, M.J.:** Designing Efficient Algorithms for Parallel Computer, McGraw-Hill 1987.
- [13] **Fässler, A. and E. Stiefel.:** Group Theoretical Methods and Its Applications, Birkhäuser Verlag 1992.
- [14] **Stiefel, E. und A. Fässler:** Gruppentheoretische Methoden und ihre Anwendung, Teubner Studienbücher, Mathematik, Bd. 46, 1979. ISBN 3-519-02348-2.
- [15] **Winograd, S.:** Arithmetic Complexity of Computations, SIAM, Philadelphia 1980.