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*

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

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 $U_1, \ldots, U_r$ ein MIP von G, und zwar sei $U_j : \mathbb{C}^{n_j} \to \mathbb{C}^{n_j}$, 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

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

für alle $s \in G$.

Beispiele:

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

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

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

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

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

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

3) Für die Block-Matrizen

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

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.

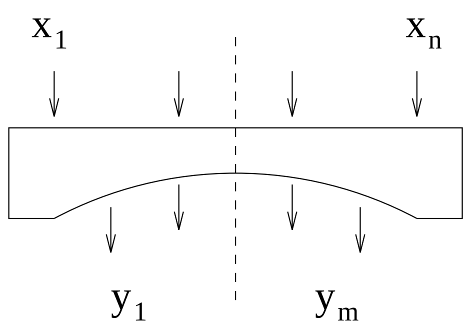
4) Sei die (m, n)-Matrix A die Matrix eines linearen Systems mit n Eingängen und m Ausgängen. Dieses ordnet dem Input $x_1, \ldots, x_n$ den Output $y_1, \ldots, y_n$ zu gemäß $y = Ax$.

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:

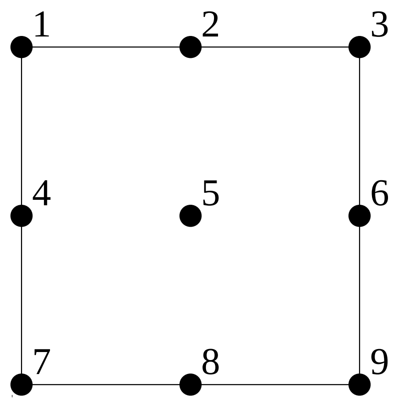


Die x_i bedeuten etwa Belastungen, die y_j Auslenkungen. Seien die (n, n) bzw. (m, m)-Matrizen P, Q erklärt durch

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

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

(b) Die quadratische Platte



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

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

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*

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

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 $B_{jk} = (B_{jk,i\ell})$ mit (n_j, n_k)-Matrizen $B_{jk,i\ell}$, so entsteht

$$B_{jk,i\ell} U_k(s) = U_j(s) B_{ik,i\ell} \ .$$

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

□

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

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

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, $j = 1, \ldots, r$.

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 $1 \le k,\ \ell \le n_j$ 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 $\nu = 1, \dots, c_j$

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

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

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

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

Es folgt

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

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

□

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

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

Insbesondere haben wir

$$T_j^{k\ell}X_{j\nu k} = X_{j\nu\ell} \tag{4.1.7}$$

Als unmittelbare Folgerung aus dem Satz notieren wir: Ist χ_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

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

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 $j = 1, \ldots, r$:

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

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

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

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

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

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 χ, ρ_1, ρ_2 die Charaktere von P, U_1, U_2, also

	1	s
χ	n	$\mathrm{par}(n)$
ρ_1	1	1
ρ_2	1	-1

$$\mathrm{par}(n) = \left\{ \begin{array}{ll} 0 & , \ n \ \text{gerade} \\ 1 & , \ n \ \text{ungerade} . \end{array} \right.$$

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

$$\begin{aligned} c_1 &= \tfrac{1}{2}(\chi(1)\rho_1(1) + \chi(s)\rho_2(s)) &&= \tfrac{1}{2}(n + \mathrm{par}(n)) \\ c_2 &= \tfrac{1}{2}(\chi(1)\rho_1(1) + \chi(s)\rho_2(s)) &&= \tfrac{1}{2}(n - \mathrm{par}(n)) . \end{aligned}$$

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

$$\begin{array}{c} n \ \text{gerade} \ (8) \\ \begin{array}{c|cccc|cccc|} & & & X_1 & & & & X_2 & \\ \hline 1 & 1 & & & & 1 & & & \\ 2 & & 1 & & & & 1 & & \\ 3 & & & 1 & & & & 1 & \\ 4 & & & & 1 & & & & 1 \\ 5 & & & & 1 & & & & -1 \\ 6 & & & 1 & & & & -1 & \\ 7 & & 1 & & & & -1 & & \\ 8 & 1 & & & & -1 & & & \\ \hline \end{array} \end{array} \qquad \begin{array}{c} n \ \text{ungerade} \ (7) \\ \begin{array}{c|cccc|ccc|} & & & X_1 & & & X_2 & \\ \hline 1 & 1 & & & & 1 & & \\ 2 & & 1 & & & & 1 & \\ 3 & & & 1 & & & & 1 \\ 4 & & & & 1 & & & \\ 5 & & & 1 & & & & -1 \\ 6 & & 1 & & & & -1 & \\ 7 & 1 & & & & -1 & & \\ \hline \end{array} \end{array} \tag{4.1.8}$$

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

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

Tatsächlich projeziert 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 χ_j von U_j ist

	r^k	sr^k
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^k$	$(-1)^k$
χ_4	$(-1)^{k+1}$	$(-1)^{k+1}$
χ_5	$i^k + (-i)^k$	0

$k = 0, 1, 2, 3$.

Für den Charakter χ 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

$$c_1 = \langle \chi, \chi_1 \rangle = \frac{1}{8}(9 + 1 + 1 + 1 + 3 + 3 + 3 + 3) = 3$$
$$c_2 = 0 , \qquad c_3 = c_4 = 1 , \qquad c_5 = 2 .$$

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

Beispiel (aber etwas mühsamer) durch Suchen nach unter P invarianten Vektoren und Unterräumen.

$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	X_3	X_4	$X_{5,1}$		$X_{5,2}$	
$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{matrix}$	$\begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{matrix}$	$\begin{matrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{matrix}$	$\begin{matrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & -1 \end{matrix}$	$\begin{matrix} 0 & 1 & 0 \\ -1 & 0 & -1 \\ 0 & 1 & 0 \end{matrix}$	$\begin{matrix} 0 & 0 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{matrix}$	$\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & -1 & 0 \end{matrix}$	$\begin{matrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{matrix}$	$\begin{matrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & -1 \end{matrix}$

Die Matrix A zerfällt bezüglich dieser Basis in

$$\begin{pmatrix} A_1 & & & & & & \mathbf{O} \\ & A_1 & & & & & \\ & & A_1 & & & & \\ & & & A_3 & & & \\ & & & & A_4 & & \\ & & & & & A_5 & \\ \mathbf{O} & & & & & & A_5 \end{pmatrix}$$

mit $(1,1)$-Matrizen A_1, A_3, A_4 und einer $(2,2)$-Matrix A_5.

Bleibt noch das Problem der Invertierung von X bzw. Y. Diese wird durch folgenden Satz erleichtert.

3) Das obige Beispiel 1) ist besonders einfach. Die Faltung A hat die Symmetrien der regulären Darstellung P von C_n, und

$$U_j(a^k) = \omega^{kj}\ , \quad \omega = e^{-2\pi i/n}\ , \quad j = 0, \ldots, n-1$$

definiert ein MIP von C_n. Jedes U_j kommt genau einmal in P vor. Wir haben also $c_j = n_j = 1$, $j = 0, \ldots, n-1$ und damit

$$A = X \begin{pmatrix} A_0 & & \\ & \ddots & \\ & & A_{n-1} \end{pmatrix} X^{-1}$$

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

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

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 ϕ_d die Kreisteilungspolynome, und sei X_d die Matrix der Spalten von W_n, welche zu den Nullstellen von ϕ_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

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

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

$$\begin{array}{rcll} x_0 + x_1 + x_2 & = & 0 & , \\ x_1 + x_2 + x_3 & = & 0 & , \\ x_2 + x_3 + x_4 & = & 0 & , \\ x_4 + x_5 + x_6 & = & 06. & \end{array}$$

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 $X'^T X' = \mathrm{diag}\,(6, 6, 4, 12, 4, 12)$ 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, $U_1, \ldots, U_r$ unitär und werden die Vektoren $X'_{j\nu 1}$, $\nu = 1, \ldots, c_j$ 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

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

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 ν, μ. Bleibt noch zu sagen, daß

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

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.

$\square$

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 $h \in H$

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

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*

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

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

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

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

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 $\rho\colon G \to GL(V)$ 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 Repräsentantenssystem von G/H, also $G/H = \{g_1 H, \dots, g_m H\}$. Wir setzen

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

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

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

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 Symmetien von P, Q, wenn A eine (m_1,n_1)-Matrix von (m_2,n_2)-Matrizen $A_{j,k} = (A^{\nu,\mu}_{j,k})$ ist mit folgenden Eigenschaften: $A_{j,k}$ hat die Symmetrien von P_2, Q_2, und die (m_1,n_1)-Matrizen $A^{\nu,\mu} = (A^{\nu,\mu}_{j,k})$ 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

$$\begin{pmatrix} A_{11}, \ldots, A_{1,n_1} \\ \vdots \\ A_{n_1,1}, \ldots, A_{m_1,n_1} \end{pmatrix} \begin{pmatrix} p_1^{1,1} I_{n_2}, \ldots, p_1^{1,n_1} I_{n_2} \\ \vdots \\ p_1^{n_1,1} I_{n_2}, \ldots, p_1^{n_1,n_1} I_{n_2} \end{pmatrix}$$

$$= \begin{pmatrix} q_1^{1,1} I_{m_2}, \ldots, q_1^{1,m_1} I_{m_2} \\ \vdots \\ q_1^{m_1,1} I_{m_2}, \ldots, q_1^{m_1,m_1} I_{m_2} \end{pmatrix} \begin{pmatrix} A_{1,1}, \ldots, A_{1,n_1} \\ \vdots \\ A_{m_1,1}, \ldots, A_{m_1,n_1} \end{pmatrix} ,$$

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

$$\sum_{k=1}^{n_1} A_{j,k} p_1^{k,\ell} = \sum_{k=1}^{m_1} q_1^{j,k} A_{k,\ell}\ , \quad j = 1, \ldots, m_1, \quad \ell = 1, \ldots, n_1\ ,$$

oder, elementweise

$$\sum_{k=1}^{n_1} A^{\nu,\mu}_{j,k} p_1^{k,\ell} = \sum_{k=1}^{m_1} q_1^{j,k} A^{\nu,\mu}_{k,\ell}\ .$$

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 ρ, 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 $G_1 = \{s_1, \ldots, s_n\}$, $G_2 = \{t_1, \ldots, t_m\}$ und $G = \{s_1 t_1, \ldots, s_1 t_m, s_2 t_1, \ldots, s_2 t_m, \ldots, s_n t_1, \ldots, s_n t_m\}$. 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 π_j die Permutation mit $s_j^{-1}s_\ell = s_{\pi_j(\ell)}$ ist; entsprechend ist σ die Permutation mit $t_k^{-1}t_i = t_{\sigma_k(i)}$. Sei nun $x \in \mathbb{C}^{nm}$ aufgespaltet 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 σ_k aus.
2. Man übt auf $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ die Permutation π_j aus.

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

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

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

□

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 π_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 $A_1, \ldots, A_n$ 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_ρ der Grad von ρ, so gilt nach Satz 2.2.7 $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$.

Da $\hat{f}(\rho)$ für jedes ρ durch d_ρ^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 $G = C_{n_1} \otimes \cdots \otimes C_{n_p} = \{a_1^{k_1} a_p^{k_p} : 0 \le k_r < n_r\}$, $a_r^{n_r} = 1$, und $\hat{G} = \{\rho_{j_1,\dots,j_r} : 0 \le j_r < n_r,\ r = 1, \dots, p\}$,

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

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

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

Dies ist die p-dimensionale Fourier-Transformation.

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

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

Dies ist die Hadamard-Walsh-Transformation.

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

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

wobei d_ρ der Grad von ρ ist.

Beweis: Es ist

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

mit dem regulären Charakter χ_{reg}, vgl. II.2. Nun ist aber

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

Also folgt

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

□

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

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

□

Aus 4.3 wissen wir, daß die (n,n)-Matrix $A \quad (n = |G|)$ 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_ρ, d_ρ)-Matrizen A_ρ. Die Anwendung von A auf einen Vektor x der Länge $n = |G|$ ist also äquivalent der Anwendung der Matrizen A_ρ auf d_ρ Vektoren der Länge $d_\rho, \;\; \rho \in \hat{G}$. Die Komplexität von $x \to Ax$ fällt also von $|G|^2$ auf

$$
\sum_{\rho \in \hat{G}} d_\rho^3 \leq |G| \underset{\rho \,\in\, \hat{G}}{\operatorname{Max}} |d_\rho| \, .
$$

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

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

Ist also $W_G : \mathbb{C}^n \to \bigotimes_{\rho\in\hat{G}} \mathbb{C}^{d_\rho^2}$ 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 $G = G_1 \otimes \cdots \otimes G_r$. Dann läßt sich die Fourier-Transformation auf 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_σ, d_τ sind natürlich die Grade von σ, τ). Damit verlangt $\hat{f}$

$$\begin{aligned} |A| \sum_{\tau\in\hat{B}} |B| d_\tau^2 \quad &+ \quad \sum_{\sigma\in\hat{A}} \sum_{\tau\in\hat{B}} |A| d_\sigma^2 d_\tau^2 \\ &= \quad |A|\ |B|^2 + |A|^2 B = |G|(|A| + |B|) \end{aligned}$$

Rechenoperationen.

$\square$