Konstruktive Darstellungstheorie und Algorithmengenerierung

Zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften der Fakultät für Informatik der Universität Karlsruhe (Technische Hochschule)

vorgelegte

Dissertation

von

Markus Püschel

aus Augsburg

Tag der mündlichen Prüfung:	6. Mai 1998
Erster Gutachter:	Prof. Dr. Thomas Beth
Zweiter Gutachter:	Prof. Dr. Heinrich-Wolfgang Leopoldt

13. Juli 1998

Dank

An erster Stelle danke ich Herrn Professor Dr. Beth, der meine Arbeit stets förderte und mit seiner Idee zur Verknüpfung von Signalverarbeitung und Darstellungstheorie bereits vor vielen Jahren den Grundstock für diese Dissertation legte. Mein herzlicher Dank gilt Herrn Professor Dr. Leopoldt für die Übernahme des Korreferats. Unter meinen Mitarbeitern möchte ich an erster Stelle Herrn Dr. Sebastian Egner danken für die freundschaftliche und fruchtbare Zusammenarbeit, die mir viel Freude gemacht hat. Des weiteren danke ich Martin Rötteler für seine Korrekturen und Verbesserungsvorschläge und Volker Baumgarte, Detlef Zerfowski sowie Markus Grassl für die Hilfe bei diversen TeX-Problemen. Außerdem danke ich allen Mitarbeitern des Instituts für Algorithmen und Kognitive Systeme für die offene, freundschaftliche Atmosphäre, die wesentlich zum Gelingen dieser Arbeit beitrug. Zum Schluß danke ich Werner Veit, der dieser Arbeit den letzten Schliff gab.

Inhalt

Einleitung

Effiziente Algorithmen sind in der Signalverarbeitung von zentraler Bedeutung. Allein die schnelle Fouriertransformation war Gegenstand zahlreicher Veröffentlichungen der letzten dreißig Jahre. Wie diese sind auch andere schnelle Signaltransformationen durch Zerlegung der zugehörigen Matrix realisiert. Ziel dieser Arbeit ist die automatische Generierung solcher Zerlegungen.

Hintergrund und Vorgeschichte

Die schnelle Fouriertransformation (Fast Fourier Transform, FFT) gehört zu den nützlichsten Algorithmen der Informatik. Sie entspricht einer effizienten Auswertung der diskreten Fouriertransformation (DFT), was mathematisch nichts anderes bedeutet als die Multiplikation eines Vektors der Länge n mit der Matrix

$$\mathrm{DFT}_n = [\omega_n^{ij} \mid i, j \in \{0, \dots, n-1\}],$$

wobei ω_n eine primitive n-te Einheitswurzel bezeichnet. Die Anwendungen der FFT liegen in der Korrelationsanalyse, Polynominterpolation, der effizienten Berechnung von Faltungen und vor allem in der Signalverarbeitung. Tatsächlich bedeutete die Veröffentlichung der FFT von Cooley/Tukey (1965), [19] einen wesentlichen Schritt in Richtung moderne Signalverarbeitung. Sie zeigten, daß, unter gewissen Voraussetzungen an die Zahl n, die Berechnung der DFT $O(n \log n)$ arithmetische Operationen erfordert, statt $O(n^2)$ wie bis dahin angenommen.

Um so erstaunlicher ist es, daß eine historische Untersuchung (siehe Heidemann/Johnson/Burrus (1985), [34]) ergab, daß genau dieser Algorithmus bereits über 150 Jahre früher gefunden wurde und zwar von niemand anderem als Carl Friedrich Gauß. Dazu bemerkte Huang 1971 (siehe [35]) satirisch, daß dies wohl der 1001-te Algorithmus von Gauß sein muß. Nach heutigem Kenntnisstand benutzte dieser die FFT, um Asteroidenorbits zu interpolieren und schrieb den Algorithmus 1805 nieder. Dieser wurde aber nicht veröffentlicht und findet sich unter dem Titel „Theoria Interpolationis Methodo Nova Tractata“ nur in seinen gesammelten Werken, Gauß (1866), [31].

Weiterentwicklungen der Arbeit von Cooley/Tukey, welche unter anderem die einschränkenden Bedingungen an die Zahl n aufhob, wurden von Rader (1968),

[53] und Bluestein (1970), [10] geleistet. Damit war das Problem einer schnellen Fouriertransformation weitgehend gelöst.

Der Grundstein zu einer tieferen Sichtweise und einer erheblichen Verallgemeinerung der DFT wurde in der Habilitationsschrift von Beth (1984), [6] gelegt. Bereits in Apple/Wintz (1970), [2] und Pichler (1975), [52] wurde erkannt, daß die DFT_n genau die Matrix ist, welche die reguläre Darstellung

$$\phi: \ x \mapsto (1, 2, \ldots, n)$$

einer zyklischen Gruppe $\mathsf{Z}_n = \langle x \mid x^n = 1 \rangle$ der Ordnung n in irreduzible Komponenten zerlegt, das heißt es gilt

$$\phi^{\mathrm{DFT}_n} = \bigoplus_{i=1}^{n} (x \mapsto \omega_n^i).$$

Damit ergibt sich eine natürliche Verbindung zwischen der Fouriertransformation und der Darstellungstheorie endlicher Gruppen. Beth erkannte, daß sich die FFT erklären läßt durch die schrittweise Zerlegung von ϕ entlang einer Untergruppenkette der Z_n und verallgemeinerte die DFT auf beliebige endliche Gruppen. Eine erste Untersuchung zum Aufwand der FFT beliebiger auflösbarer Gruppen findet sich in Beth (1987), [7].

In der Folgezeit wurden schnelle Fouriertransformationen zu gewissen Klassen nichtabelscher Gruppen konstruiert und deren Komplexität untersucht. Als wesentliche Arbeiten sind hierzu Clausen (1988/89), [13, 14], wo unter anderem eine FFT zur symmetrischen Gruppe S_n konstruiert wird, und Diaconis/Rockmore (1990), [23] sowie Rockmore (1994), [55] zu erwähnen. Eine gute Einführung in das Gebiet allgemeiner Fouriertransformationen ist das Buch von Clausen/Baum (1993), [16]. Der Status quo der Forschung ist in dem Übersichtsartikel Maslen/Rockmore (1995), [43] dargestellt. Die Anwendungen allgemeiner FFTs sind noch vergleichsweise dünn gesät und liegen hauptsächlich im Bereich Signalverarbeitung und Statistik. Einen Überblick hierzu liefert Rockmore (1995), [56].

Eine völlig neue Vorgehensweise und Allgemeinheit wurde von Minkwitz im Rahmen seiner Dissertation (1993), [45] entwickelt (siehe auch [46, 48]). Der zentrale Punkt in dieser Arbeit ist die Definition der *Symmetrie* einer Matrix M. Sind ϕ, ψ Darstellungen derselben Gruppe G, dann hat M die Symmetrie (ϕ, ψ), wenn

$$\phi(g) \cdot M = M \cdot \psi(g) \text{ für alle } g \in G.$$

Minkwitz zeigte, daß sich die Matrix M in ein Produkt dünn besetzter Matrizen zerlegen läßt, wenn ϕ eine beliebige Permutationsdarstellung ist und ψ entweder eine direkte Summe irreduzibler Darstellungen (in diese Kategorie fallen die Fouriertransformationen zu beliebigen Gruppen G) oder ebenfalls eine Permutationsdarstellung ist. Die Beschränkung auf reguläre Darstellungen entfiel damit und Minkwitz entwickelte Methoden, um eine beliebige Permutationsdarstellung ϕ einer auflösbaren Gruppe schrittweise in ihre irreduziblen Komponenten zu zerlegen. Diese *schrittweise* Zerlegung führt zu einer Zerlegungsmatrix A_ϕ, die ein Produkt dünnbesetzter Matrizen ist. Besitzt nun M die Symmetrie (ϕ, ψ) und sind A_ϕ bzw. A_ψ die zugehörigen Zerlegungsmatrizen, dann ist die Matrix

$$B = A_\phi^{-1} \cdot M \cdot A_\psi$$

blockdiagonal, was eine Folge des Lemmas von Schur aus der Darstellungstheorie ist. Damit ist durch

$$M = A_\phi \cdot B \cdot A_\psi^{-1}$$

eine Zerlegung von M bestimmt. Der entscheidende Punkt bei dieser Zerlegung ist offenbar, daß A_ϕ und A_ψ in zerlegter Form gewonnen werden können. Die Zerlegung von M repräsentiert dann einen schnellen Algorithmus zur Multiplikation mit M. Später erkannte Minkwitz, daß eine Verallgemeinerung auf monomiale Darstellungen ϕ, ψ möglich ist. Die Vorgehensweise zur Zerlegung einer Matrix M ist demnach wie folgt:

1. Bestimme eine geeignete Symmetrie (ϕ, ψ) von M.
2. Berechne Zerlegungsmatrizen A_ϕ, A_ψ von ϕ bzw. ψ.
3. Berechne die Blockdiagonalmatrix $B = A_\phi^{-1} \cdot M \cdot A_\psi$.

Mit dieser Methode ist es nun möglich, eine *konkret gegebene* Matrix zu zerlegen. Als ein Beispiel bestimmte Minkwitz (per Hand) die Symmetrie der Diskreten Cosinustransformation (DCT) und konnte diese dann zerlegen. Die DCT besaß bis dahin keine darstellungstheoretische Interpretation. Anwendung der Methode auf die DFT lieferte die bekannte Cooley-Tukey- bzw. Rader-Zerlegung.

Der Grundstein zur automatischen Generierung einer Zerlegung einer Matrix mit Symmetrie war somit gelegt. Dem schwierigen Problem der Symmetriefindung widmete sich Egner in seiner Dissertation (1997), [26]. Er benannte die oben erwähnten Symmetrietypen Perm-Irred-Symmetrie, Perm-Perm-Symmetrie und Mon-Mon-Symmetrie und entwickelte unter anderem den ersten Algorithmus zum Finden der Perm-Irred-Symmetrie.

Beitrag dieser Arbeit

In den Veröffentlichungen von Minkwitz werden die Methoden zur Bestimmung von Zerlegungsmatrizen zu Permutationsdarstellungen nur grob skizziert. Die gut untersuchte gewöhnliche Darstellungstheorie endlicher Gruppen liefert zu dieser Problematik nahezu keine Aussagen, da dort Darstellungen nur bis auf Äquivalenz betrachtet werden.

In dieser Arbeit wird daher zunächst ein *konstruktiver* Aufbau der Darstellungstheorie entwickelt, das heißt mit Darstellungen wird bis auf Gleichheit gerechnet, statt nur bis auf Äquivalenz wie in den bekannten Standardwerken. Das bedeutet unter anderem, daß konjugierende Matrizen zu ähnlichen Darstellungen in den Brennpunkt des Interesses rücken. In diesem Sinne werden zuerst bekannte Sätze über das Zusammenspiel von Induktion und anderen Konstruktionen für Darstellungen verfeinert und später auf Permutations- bzw. monomiale Darstellungen angewandt. Ein Stück weit wird eine Theorie der Zerlegungsmatrizen entwickelt. Näher untersucht werden auch Intertwiningräume von Darstellungen, die durch Minkwitz' Symmetriedefinition in natürlicher Weise ins Spiel gebracht werden: Der Intertwiningraum $\mathsf{Int}(\phi, \psi)$ von zwei Darstellungen ϕ und ψ ist genau die Menge aller Matrizen, die (ϕ, ψ) als Symmetrie besitzt. Die Mehrzahl der in dieser Arbeit bewiesenen Resultate ist in der Literatur nicht zu finden. Darauf aufbauend wird ein Algorithmus zur Zerlegung einer großen Klasse monomialer Darstellungen entwickelt und ausführlich präsentiert.
Für eine effiziente Implementierung der Algorithmen wurden in Zusammenarbeit mit Sebastian Egner Datenstrukturen entwickelt, die das Rechnen mit strukturierten Darstellungen und Matrizen überhaupt erst möglich machen (siehe Anhang). Darauf aufbauend wurden dann alle in dieser Arbeit entwickelten Algorithmen implementiert. Durch Kombination dieser Programme mit den Programmen zur Symmetriefindung entstand ein Programm, welches Matrixzerlegungen (für Matrizen mit Symmetrie) automatisch generieren kann.
Schließlich wurde das Programm zur Matrixzerlegung auf die bekanntesten klassischen Signaltransformationen angewandt: Es konnten alle substantiell zerlegt werden. Damit liefert die Darstellungstheorie für die betrachteten Transformationen nicht nur den theoretischen Hintergrund für die Existenz schneller Algorithmen, sie bietet auch die Möglichkeit, diese zu generieren.

Gliederung

Kapitel 1 erklärt zunächst die verwendeten Symbole und Bezeichnungskonventionen. Danach wird der oben erwähnte konstruktive Aufbau der gewöhnlichen Darstellungstheorie entwickelt. Hauptergebnisse betreffen Induktionen von Darstellungen, monomiale Darstellungen, Intertwiningräume und Zerlegungsmatrizen. Die konkrete algorithmische Umsetzung der bewiesenen Resultate steht stets im Vordergrund und wurde auch durchgeführt (siehe Anhang).
Kapitel 2 beinhaltet einen effizienten Algorithmus zur Zerlegung einer großen Klasse von monomialen Darstellungen, welcher auf den Ergebnissen aus Kapitel 1 aufbaut und genau beschrieben wird. Ein ausführliches Beispiel schließt das Kapitel ab.
Kapitel 3 behandelt die Zerlegung von Matrizen mit Symmetrie. Zunächst werden die drei betrachteten Symmetrietypen definiert und jeweils erläutert, wie aus

der Symmetrie einer Matrix eine Zerlegung derselben gewonnen wird. Zum Abschluß wird ein Algorithmus entwickelt, der in der Lage ist, monomiale Symmetrie zu finden.
Kapitel 4 befaßt sich mit konkreten Beispielen aus der Signalverarbeitung. Die bekanntesten klassischen Signaltransformationen werden auf Symmetrie der in Kapitel 3 betrachteten Typen untersucht und jeweils der Isomorphietyp der Symmetriegruppe angegeben. Exemplarisch werden zu den Signaltransformationen *automatisch* generierte Zerlegungen angegeben. Diese entsprechen weitgehend den bekannten Zerlegungen aus der Literatur und machen die Mächtigkeit der entwickelten Methoden deutlich.
Anhang ist ein Manual des Softwarepakets AREP zum Rechnen mit Matrixdarstellungen, welches im Rahmen dieser Dissertation in Zusammenarbeit mit Sebastian Egner entstand. AREP basiert auf den Ergebnissen aus den Kapiteln 1 und 2.

1

Konstruktive Darstellungstheorie

Die Darstellungstheorie endlicher Gruppen gilt als eines der schönsten Teilgebiete der Algebra. Viele der namhaftesten Algebraiker dieses Jahrhunderts haben sich mit ihr befaßt, und so ist es nicht verwunderlich, daß die Grundlagen der Darstellungstheorie nahezu vollständig geklärt sind.

Eine (Matrix-)Darstellung ist gegeben durch einen Homomorphismus ϕ einer endlichen Gruppe G in die Gruppe $\mathsf{GL}_n(\mathbb{K})$ der invertierbaren $(n \times n)$-Matrizen über einem Körper $\mathbb{K}$. Die „Maschke-Bedingung", welche verlangt, daß die Charakteristik von $\mathbb{K}$ die Gruppenordnung $|G|$ nicht teilt, spaltet die Darstellungstheorie in zwei wesentlich unterschiedliche Teilgebiete: die gewöhnliche $(\mathrm{char}(\mathbb{K}) \nmid |G|)$ und die modulare $(\mathrm{char}(\mathbb{K}) \mid |G|)$ Darstellungstheorie. Erstere ist heutzutage weitgehend geklärt, während die zweite Gegenstand aktueller Forschung ist.

Als Literatur zur Darstellungstheorie sind zu empfehlen: James/Liebeck (1993), [38] als einfachste Einführung in das Gebiet, Dornhoff (1971), [25] und Serre (1977), [58], um einen schnellen Überblick zu bekommen sowie Huppert (1967), [36] und vor allem Curtis/Reiner (1962), [21] bzw. (1981), [22] zur Vertiefung. Das Buch von Feit (1982), [29] ist auf hohem Niveau geschrieben. Ebenfalls eine schöne Einführung liefert das leider nicht allgemein erhältliche Skript zu einer Vorlesung über Darstellungstheorie von Leopoldt (1979), [40].

Zur Einführung in die Gruppentheorie seien genannt: das umfassende Buch von Huppert (1967), [36] und das schöne Buch von Marshall Hall jr. (1976), [33]. Der Atlas (1985), [18] gibt einen Überblick über die endlichen einfachen Gruppen. Für die Gruppen bis zur Ordnung 1000 (außer 512 und 768) steht der neue Katalog von Besche und Eick (1996), [5] der kleinen endlichen Gruppen zur Verfügung, welcher in das GAP-System [57] geladen werden kann. Für die Computeralgebra der Gruppen ist der Atkinson (1984), [3] ein Klassiker, wie auch das Buch von Butler (1991), [12] zum Rechnen mit Permutationsgruppen.

In den obengenannten Büchern werden Darstellungen von Gruppen nur bis auf Äquivalenz betrachtet, das heißt bis auf Konjugation $\phi \to \phi^A$ mit einer invertierbaren Matrix A. Die atomaren Objekte der Untersuchungen sind also

Äquivalenzklassen von (irreduziblen) Darstellungen. Zur Entwicklung der Strukturtheorie werden dabei selten Darstellungen, sondern Charaktere von Darstellungen betrachtet. Diese sind invariant unter Konjugation der Darstellung und tragen die wesentliche Information der Äquivalenzklasse in sich. Darüber hinaus sind Charaktere kompakt darstellbar: ein Charakter ist gegeben durch die Werte auf den Konjugationsklassen der Gruppe. Das computergestützte Rechnen mit Charakteren hat wesentlich zur Klassifikation der endlichen einfachen Gruppen beigetragen.

Für viele Anwendungen ist das Rechnen mit Charakteren jedoch nicht ausreichend. Man möchte explizit mit Matrixdarstellungen rechnen und diese unter Bewahrung von Gleichheit transformieren können. Die Zerlegung einer Matrix mit Symmetrie ist ein Beispiel für eine solche Anwendung. Hierbei ist es notwendig, eine monomiale Darstellung schrittweise zu zerlegen und dabei die Zerlegungsmatrix mitzuführen (siehe Einleitung).

Die Entwicklung von Programmen zum Rechnen mit Matrixdarstellungen erfordert also eine Erweiterung der Darstellungstheorie: bekannte Sätze über Äquivalenz von zwei Darstellungen müssen durch explizite Angabe einer konjugierenden Matrix, einer Transversale etc. so verfeinert werden, daß Gleichheit gilt. Es ist beispielsweise bekannt, daß jede transitive monomiale Darstellung μ einer Gruppe G ähnlich ist zur Induktion einer Darstellung λ vom Grad 1 einer Untergruppe $H \leq G$. Wie kann H und λ gefunden werden? Wie ist eine Transversale und eine konjugierende Matrix zu wählen, so daß Gleichheit gilt? Fragen dieser Art werden in diesem Kapitel beantwortet.

Im Rahmen dieser Dissertation entstand in Zusammenarbeit mit Sebastian Egner das Software-Paket AREP zum Rechnen mit Matrixdarstellungen. Dieses ist programmiert in der Sprache GAP (Groups, Algorithms and Programming, [57]) und implementiert eine Termalgebra zum Rechnen mit Darstellungen und Matrizen sowie alle Algorithmen, die in diser Dissertation präsentiert werden. AREP wird ab Mitte 98 als GAP Share Package auf dem GAP Server verfügbar sein.

Die zentralen Objekte in diesem Paket sind die rekursiven Datentypen `ARep` und `AMat`. Eine `ARep` ist ein GAP-Record, das eine Darstellung repräsentiert. Das Record enthält eine Reihe von Feldern, die die Darstellung eindeutig charakterisieren, beispielsweise müssen stets Grad, Charakteristik und dargestellte Gruppe präsent sein. Es gibt nun eine Reihe von elementaren Konstruktoren, welche eine `ARep` konstruieren, zum Beispiel durch Angabe der Bilder auf den Erzeugern der Gruppe (`ARepByImages`) und eine Reihe von Konstruktoren, die aus gegebenen `AReps` eine höher strukturierte `ARep` bauen (z. B. `DirectSumARep`). Die Idee hierbei ist, eine solche Konstruktion, beispielsweise die direkte Summe, nicht gleich auszurechnen, sondern eine `ARep` zu bauen, die diese repräsentiert, das heißt eine `ARep`, welche ein Feld `summands` enthält mit einer Liste der Summanden. Will man zu einer Matrixdarstellung konvertieren, benutzt man die entsprechende Funktion. Auf der anderen Seite gibt es Funktionen, welche aus einer unstrukturierten, z. B. monomialen `ARep`, eine hochstrukturierte `ARep` bauen (z. B. konjugierte Induktion einer Darstellung vom Grad 1), die mathematisch *identisch* zur ursprünglichen ist. Permutationsdarstellungen und monomiale Darstellungen sind bei der Erstellung des Pakets besonders berücksichtigt worden, da sie gut zu speichern und zu handhaben sind und bei der Zerlegung von Matrizen mit Symmetrie die zentrale Rolle spielen.

Nach dem gleichen Prinzip ist der Datentyp `AMat` konzipiert als GAP-Record, das eine Matrix repräsentiert. Es gibt wieder elementare Konstruktoren, beispielsweise baut `AMatPerm` aus einer Permutation mit Grad und evtl. Charakteristik eine `AMat`, die eine Permutationsmatrix repräsentiert. Höhere Konstruktoren (Produkt, direkte Summe, Tensorprodukt etc.) werden erst ausgewertet, wenn die entsprechende Funktion aufgerufen wird. Dies ermöglicht es, strukturierte Matrizen zu bauen, die leichter zu handhaben sind, als die (mathematisch identische) repräsentierte Matrix. Berechnung von Inversen, Determinante, Spur etc. sind mit den meisten Konstruktoren verträglich und ermöglichen eine schnelle Berechnung unter Verwendung mathematischen Wissens. Darüber hinaus sind strukturierte `AMat`s effizienter zu speichern als die entsprechenden Matrizen. Ein Manual zu AREP ist im Anhang zu finden.

Im folgenden sind die Theorie und die Algorithmen präsentiert, welche den Funktionen in AREP zugrunde liegen. Dabei wird auf Ergebnissen von Minkwitz (1993), [45] und Clausen/Baum (1993), [16] aufgebaut. Im Zentrum des Interesses stehen Induktionen und monomiale Darstellungen. Der Algorithmus zur Zerlegung monomialer Darstellungen baut darauf auf und wird im nächsten Kapitel vorgestellt.

Das Kapitel ist wie folgt aufgebaut: In Abschnitt 1.1 werden die wichtigsten verwendeten Begriffe und Symbole, teils tabellarisch, vorgestellt. In Abschnitt 1.2 sind die Sätze präsentiert, die das Zusammenspiel von Induktion und anderen Konstruktoren von Darstellungen (Einschränkung, Tensorprodukt, etc.) klären. Die Sätze sind bekannt, werden aber konstruktiv verfeinert präsentiert, das heißt es gilt stets „$=$“ und nicht „$\cong$“. Speziell mit monomialen Darstellungen beschäftigt sich Abschnitt 1.3, wo unter anderem Algorithmen zur Zerlegung einer transitiven monomialen Darstellung in eine Induktion bzw. in ein konjugiertes äußeres Tensorprodukt vorgestellt wird. Der Erweiterungssatz von Minkwitz ist Gegenstand von Abschnitt 1.4. In Abschnitt 1.5 wird der Intertwiningraum zweier Darstellungen untersucht mit besonderem Augenmerk auf den monomialen Fall. Den Abschluß bildet der Abschnitt 1.6, wo die Grundlagen für den Algorithmus zur Zerlegung von monomialen Darstellungen gelegt werden. Höhepunkt ist dort der Satz zur schrittweisen Berechnung von Zerlegungsmatrizen entlang einer Kompositionsreihe.

Wir betrachten ausschließlich Darstellungen von endlichen Gruppen, für die die Maschke-Bedingung erfüllt ist. Soweit es möglich ist, werden alle Sätze in der Sprache der Matrixdarstellungen formuliert und die Modulsprechweise vermieden.

1.1 Notation und Konstruktionen

Eine Darstellung ϕ vom Grad n ist ein Homomorphismus einer Gruppe G in die Gruppe $\mathsf{GL}_n(\mathbb{K})$ der invertierbaren $(n \times n)$-Matrizen über einem Körper $\mathbb{K}$. Die Gruppe G sei endlich und die Charakteristik von $\mathbb{K}$ sei kein Teiler der Gruppenordnung $|G|$ (Maschke-Bedingung). Jede Darstellung ϕ läßt sich dann mit einer invertierbaren Matrix A in eine Summe irreduzibler Darstellungen ϕ_i zerlegen (Satz von Maschke), jedes ϕ_i heißt irreduzible Komponente von ϕ:

$$\phi^A = \bigoplus_{i=1}^{r} (\underbrace{\phi_i \oplus \ldots \oplus \phi_i}_{n_i}), \text{ mit } \phi_i \text{ irreduzibel, } \phi_i \not\cong \phi_j \text{ für } i \neq j.$$

Eine Darstellung heißt Permutationsdarstellung, wenn alle Bilder Permutationsmatrizen sind. Eine Darstellung heißt monomial, wenn alle Bilder monomiale Matrizen sind. Eine Matrix heißt monomial, wenn in jeder Zeile und in jeder Spalte genau ein Eintrag $\neq 0$ ist. Monomiale Matrizen sind stets invertierbar. Eine Darstellung heißt unitär, wenn alle Bilder unitäre Matrizen sind.
Ist ϕ eine Darstellung über $\mathbb{K}$ vom Grad n, dann operiert G auf dem Vektorraum $V = \mathbb{K}^n$ via ϕ, durch $v \cdot g = v \cdot \phi(g)$, $v \in V$, $g \in G$, wodurch V ein $\mathbb{K}[G]$-Rechtsmodul wird, V nennen wir dann den „Darstellungsraum" von ϕ. Ist ϕ wie oben zerlegt, so heißt der Darstellungsraum zu einem ϕ_i irreduzible Komponente von V und der Darstellungsraum zu $(\phi_i \oplus \ldots \oplus \phi_i)$ homogene Komponente von V. Die Zerlegung der Darstellung entspricht also einer Zerlegung des Darstellungsraums in homogene bzw. irreduzible Komponenten.

Wir verwenden die folgenden Bezeichnungskonventionen:

Matrizen:

$A, B, M, P, \ldots$	Matrizen
$[a_{i,j} \mid i \in \{1, \ldots, n\},$ $j \in \{1, \ldots, m\}]$	oder einfach $[a_{i,j}]_{i,j}$, Matrix mit Einträgen $a_{i,j}$
$\mathrm{diag}(x_k \mid k \in \{1, \ldots, n\})$	Diagonalmatrix mit Einträgen x_k
σ, τ	Permutationen
$[\sigma, n]$	$[\delta_{i^\sigma j} \mid i, j \in \{1, \ldots, n\}]$, $(n \times n)$-Permutationsmatrix zur Permutation σ, es gilt $[\tau, n] \cdot [a_{i,j}]_{i,j} \cdot [\sigma, m] = [a_{i^\tau, j^{\sigma^{-1}}}]_{i,j}$
$[\sigma, (x_1, \ldots, x_n)]$	$[\sigma, n] \cdot \mathrm{diag}(x_k \mid k \in \{1, \ldots, n\})$, monomiale $(n \times n)$-Matrix
ω_n	primitive n-te Einheitswurzel
i	$\sqrt{-1}$
A^*	Adjunktion der Matrix A (transponiert und komplex konjugiert)
DFT_n	$[\omega_n^{ij} \mid i \in \{0, \ldots, n-1\}, j \in \{0, \ldots, n-1\}]$
$\mathbf{1}_n$	Identitätsmatrix vom Grad n
$\mathbf{0}_n$	Nullmatrix vom Grad n

Gruppen:

$G, H, N, \ldots$	Gruppen
$H \backslash G$	Menge der Rechtsnebenklassen von H in G
$H \times N$	direktes Produkt von H mit N
$H \ltimes N$	semidirektes Produkt vom Normalteiler N mit Untergruppe H
$g, h, x, y, s, t, \ldots$	Gruppenelemente
$\langle x, y, \ldots \rangle$	Gruppe bzw. Vektorraum, der von $x, y, \ldots$ erzeugt wird
T, S	Transversalen (= Vertretersysteme von Rechtsnebenklassen)
E	triviale Gruppe
Z_n	zyklische Gruppe der Ordnung n
D_{2n}	Diedergruppe mit $2n$ Elementen
A_n	alternierende Gruppe auf n Punkten
S_n	symmetrische Gruppe auf n Punkten
Q_8	Quaternionengruppe

Darstellungen:

$\phi, \psi, \rho, \ldots$	Darstellungen
μ	monomiale Darstellung
π	Permutationsdarstellung
ϕ_G, μ_G, π_G	Darstellungen der Gruppe G
1_G	Einsdarstellung vom Grad 1 auf G
$\deg(\phi)$	Grad von ϕ
χ_ϕ	Charakter von ϕ

Mengen und Listen:

$\{t_1, \ldots, t_n\}$	Menge der Elemente $t_1, \ldots, t_n$
$(t_1, \ldots, t_n)$	Liste der Elemente $t_1, \ldots, t_n$
$\cup$	Vereinigung von Mengen oder Konkatenation von Listen

Weiter bezeichnen wir mit

$$A \oplus B \;=\; \begin{bmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{bmatrix}$$

die *direkte Summe* der Matrizen $A = [a_{i,j} \mid i,j \in \{0, \ldots, n-1\}]$ und $B = [b_{i,j} \mid i,j \in \{0, \ldots, m-1\}]$ und das *Kroneckerprodukt* (oder Tensorprodukt) durch

$$A \otimes B \;=\; \left[a_{i \operatorname{div} m,\, j \operatorname{div} m} \cdot b_{i \operatorname{mod} m,\, j \operatorname{mod} m} \mid i,j \in \{0, \ldots, nm-1\} \right].$$

Im Kroneckerprodukt $A \otimes B$ bestimmt A die grobe Struktur und B die feine. Zum Beispiel

$$\mathbf{1}_2 \otimes \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \mathbf{1}_3 = \begin{bmatrix}
1 & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
3 & \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 3 & \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 3 & \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 2 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 2 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 3 & \cdot & \cdot & 4 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 3 & \cdot & \cdot & 4 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 3 & \cdot & \cdot & 4
\end{bmatrix}.$$

Eine Matrix M heißt *blockpermutiert* (bzgl. der Blöcke $B_1, \ldots, B_n$), wenn

$$M = P_1 \cdot (B_1 \oplus \ldots \oplus B_n) \cdot P_2 \text{ mit Permutationsmatrizen } P_1, P_2.$$

Für Darstellungen werden die folgenden Konstruktionen benötigt:

- $\phi_G^A = g \mapsto A^{-1} \cdot \phi_G(g) \cdot A$ ist die mit $A \in \mathsf{GL}_n(\mathbb{K})$ konjugierte Darstellung von G. Wir schreiben auch $\phi_G \xrightarrow{A} \phi_G^A$.

- $\phi_G \oplus \psi_G = g \mapsto \phi_G(g) \oplus \psi_G(g)$ ist die direkte Summe der Darstellungen ϕ_G, ψ_G derselben Gruppe G.

- $\phi_G \otimes \psi_G = g \mapsto \phi_G(g) \otimes \psi_G(g)$ ist das innere Tensorprodukt der Darstellungen ϕ_G, ψ_G derselben Gruppe G und ist wieder eine Darstellung von G.

- $\phi_G \,\#\, \psi_H = (g, h) \mapsto \phi_G(g) \,\#\, \psi_H(h)$ ist das äußere Tensorprodukt der Darstellungen ϕ_G von G und ψ_H von H. Das äußere Tensorprodukt ist eine Darstellung des direkten Produkts $G \times H$.

- $\lambda_G \cdot \phi_G = g \mapsto \lambda_G(g) \cdot \phi_G(g)$ ist das lineare Vielfache der Darstellung ϕ_G mit der Darstellung λ_G vom Grad 1. Es ist ein Spezialfall eines inneren Tensorprodukts.

- $\phi_G \downarrow H = h \mapsto \phi_G(h)$ ist die Einschränkung (Restriktion) der Darstellung ϕ_G von G auf die Untergruppe H.

- $\phi_H \uparrow_T G$ bezeichnet die Induktion der Darstellung ϕ_H auf G bezüglich T. Dabei ist H eine Untergruppe von G und $T = (t_1, \ldots, t_n)$ eine Transversale (Vertretersystem der Rechtsnebenklassen) von $H \backslash G$ der Länge $n = (G : H)$. Da die Äquivalenzklasse der Induktion unabhängig ist von der Wahl der Transversalen, kann sie dort, wo es nur auf Äquivalenz ankommt, weggelassen werden. Die Induktion hat den Grad $\deg(\phi_H) \cdot n$. Sie ist definiert durch

$$\begin{aligned} \phi_H \uparrow_T G \;&=\; g \mapsto \left[\dot{\phi}_H(t_i \cdot g \cdot t_j^{-1}) \;\middle|\; i, j \in \{1, \ldots, n\}\right], \quad \text{mit} \\ \dot{\phi}_H(x) &= \begin{cases} \phi_H(x), & x \in H \\ \mathbf{0}_{\deg(\phi_H)}, & \text{sonst} \end{cases} . \end{aligned}$$

Hat ϕ_H den Grad 1, so ist die Induktion monomial, ist sogar $\phi_H = 1_H$, so ist die Induktion eine Permutationsdarstellung.

- Eine reguläre Darstellung einer Gruppe ist eine spezielle Permutationsdarstellung einer Gruppe gegeben durch $1_\mathsf{E} \uparrow G$, wobei E die triviale Gruppe bezeichnet.

- Die Erweiterung (Extension) einer Darstellung ϕ von H auf eine Obergruppe G von H wird mit $\overline{\phi}$ bezeichnet. Im Gegensatz zur Induktion besitzt eine Darstellung einer Untergruppe H im allgemeinen keine Erweiterung.

- $\phi_H^t = g \mapsto \phi_H(t \cdot g \cdot t^{-1})$ ist die innere Konjugierte der Darstellung ϕ_H von H mit einem Element t einer Obergruppe G von H. ϕ_H^t ist eine Darstellung der zu H konjugierten Gruppe $H^t = t^{-1}Ht$. Ist insbesondere H ein Normalteiler, so ergibt sich durch innere Konjugation stets wieder eine Darstellung von H, die aber im allgemeinen nicht äquivalent zur ursprünglichen ist. Diese Definition impliziert die folgende Rechenregel:

$$\left(\phi_H^t\right)^s = \phi_H^{ts} = g \mapsto \phi_H(tsgs^{-1}t^{-1}),$$

  das heißt g wird *zuerst* mit dem Inversen des *äußeren* Exponenten konjugiert.

Eine Übersicht über das Zusammenspiel der eben vorgestellten Konstruktoren für Darstellungen ist in Tabelle 1.1 zusammengestellt. Es bezeichnet $(\cdot)^A$ die Konjugation einer Darstellung mit einer Matrix A und $(\cdot)^t$ die innere Konjugation einer Darstellung mit einem Gruppenelement. Die Tabelle ist folgendermaßen zu lesen. Wird zuerst die Operation, die zu einer Zeile gehört, ausgeführt und dann die Operation zu einer Spalte, dann steht an der entsprechenden Stelle in der Tabelle nichts, wenn es keine allgemeingültige Transformationsregel gibt, ein Kreuz, wenn es eine solche Regel gibt, diese aber trivial ist, die Nummer des Satzes, wenn die Regel nichttrivial ist. Beispielsweise läßt sich $(\phi_1 \oplus \phi_2)^A$ für beliebige Darstellungen ϕ_1, ϕ_2 und Matrix A (der passenden Größe) nicht umformen, also steht in Zeile 2, Spalte 1 der Tabelle nichts. Die Assoziativität von $\oplus, \otimes$ findet sich auf der Hauptdiagonalen an zweiter bzw. dritter Stelle. Die (triviale) Regel $(\phi \downarrow H)^A = \phi^A \downarrow H$ ist durch ein Kreuz an den Stellen $(6,1)$ und $(1,6)$ gekennzeichnet. Der Satz von Mackey, welcher die Restriktion einer Induktion zerlegt, ist in Zeile 5, Spalte 6 zu finden.
Es fällt auf, daß alle nichttrivialen Unformungsregeln mit der Induktion zusammenhängen, was wohl daran liegt, daß diese der einzige nichttriviale Konstruktor für Darstellungen ist. Die genannten Sätze befinden sich alle im folgenden Abschnitt.

	$(\cdot)^A$	$\oplus$	$\otimes$	$\#$	$\uparrow$	$\downarrow$	$(\cdot)^t$
$(\cdot)^A$	$\times$	$\times$	$\times$	$\times$	1.6	$\times$	$\times$
$\oplus$		$\times$	$\times$	$\times$	1.5	$\times$	$\times$
$\otimes$			$\times$			$\times$	$\times$
$\#$				$\times$	1.7		$\times$
$\uparrow$			1.17	1.7	1.4	1.12	1.11
$\downarrow$	$\times$			$\times$	1.15	$\times$	$\times$
$(\cdot)^t$	$\times$			$\times$	1.10	$\times$	$\times$

Tabelle 1.1: Zusammenspiel der Konstruktoren

1.2 Induktion

In diesem Abschnitt sind die wesentlichen Sätze zusammengestellt, die es erlauben, mit beliebigen Induktionen von Darstellungen zu rechnen.

Transversalenwechsel Es ist bekannt, daß die Wahl der Transversale bei der Induktion einer Darstellung ϕ von $H \leq G$ keinen Einfluß auf die Äquivalenzklasse hat, in der diese Induktion liegt, das heißt

$$\phi \uparrow_T G \cong \phi \uparrow_{T'} G.$$

Wir wollen zunächst die zum Paar (T, T') gehörende konjugierende Matrix bestimmen, welche Gleichheit herstellt. Sei dazu ϕ eine Darstellung von H, $n = (G : H)$ und $T = (t_1, \ldots, t_n)$ eine beliebige Transversale von $H \backslash G$. Zuerst betrachten wir zwei Spezialfälle eines Transversalenwechsel. Permutation von T mit $\sigma \in \mathsf{S}_n$ ergibt eine andere Transversale

$$T' = T^\sigma = (t_{1^{\sigma^{-1}}}, \ldots, t_{n^{\sigma^{-1}}})$$

und die Induktion mit T' berechnet sich zu

$$\begin{aligned}
(\phi \uparrow_{T'} G)(x) &= \left[\dot\phi(t'_i x {t'_j}^{-1})\right]_{i,j} \\
&= \left[\dot\phi(t_{i^{\sigma^{-1}}} x t^{-1}_{j^{\sigma^{-1}}})\right]_{i,j} \\
&= \left([\sigma^{-1}, n] \otimes \mathbf{1}_{\deg(\phi)}\right) \cdot \left[\dot\phi(t_i x t_j^{-1})\right]_{i,j} \cdot \left([\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}\right) \\
&= (\phi \uparrow_T G)(x)^{[\sigma,n] \otimes \mathbf{1}_{\deg(\phi)}}.
\end{aligned}$$

Wechsel der Nebenklassenvertreter in T ergibt eine Transversale

$$T' = (h_1 t_1, \ldots, h_n t_n),\ h_i \in H,$$

was sich in der Induktion wie folgt auswirkt:

$$\begin{aligned}(\phi \uparrow_{T'} G)(x) &= \left[\dot{\phi}(t'_i x t'^{-1}_j)\right]_{i,j} \\ &= \left[\dot{\phi}(h_i t_i x t_j^{-1} h_j^{-1})\right]_{i,j} \\ &= \left[\dot{\phi}(t_i x t_j^{-1})\right]_{i,j}^D,\end{aligned}$$

wobei $D = \bigoplus_{i=1}^n \phi(h_i^{-1})$ eine blockdiagonale Matrix mit Blöcken der Größe $\deg(\phi)$ ist. Aus diesen beiden Spezialfällen lassen sich alle Transversalenwechsel zusammensetzen.

1.1 Satz *Sei $H \leq G$ eine Untergruppe und ϕ eine Darstellung von H sowie $T = (t_1, \ldots, t_n)$ und $T' = (t'_1, \ldots, t'_n)$ zwei Transversalen von $H \backslash G$. Weiter sei σ die Permutation aus der S_n, welche die Nebenklassen $(Ht_1, \ldots, Ht_n)$ abbildet auf die Nebenklassen $(Ht'_1, \ldots, Ht'_n)$. Dann gilt*

$$\phi \uparrow_{T'} G = (\phi \uparrow_T G)^M \;\; mit \;\; M = ([\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}) \cdot \bigoplus_{i=1}^n \phi\left(t_{i^{\sigma^{-1}}} \cdot t'^{-1}_i\right).$$

Wir nennen M die Matrix zum Transversalenwechsel $T \to T'$.

Beweis Nach obiger Rechnung ist $\phi \uparrow_{T^\sigma} G = (\phi \uparrow_T G)^{[\sigma,n]\otimes \mathbf{1}_{\deg(\phi)}}$. Der Übergang von T^σ nach T' ist nur noch ein Wechsel der Nebenklassenvertreter und damit gilt $\phi \uparrow_{T'} G = (\phi \uparrow_{T^\sigma} G)^D$ mit $D = \bigoplus_{i=1}^n \phi(t_{i^{\sigma^{-1}}} \cdot t'^{-1}_i)$, woraus die Behauptung folgt. ∎

Der Algorithmus zum Basiswechsel ergibt sich aus dem Beweis.

1.2 Algorithmus (Transversalenwechsel) Gegeben ist eine Induktion $\phi \uparrow_T G$ von einer Darstellung ϕ einer Untergruppe $H \leq G$ und eine zweite Transversale T' von $H \backslash G$. Gesucht ist die Matrix M aus Satz 1.1 zum Transversalenwechsel $T \to T'$.

1. Bestimme die Permutation σ, welche die Nebenklassenliste $(Ht_1, \ldots, Ht_n)$ auf $(Ht'_1, \ldots, Ht'_n)$ abbildet.

2. Werte ϕ an den Stellen $t_{i^{\sigma^{-1}}} \cdot t'^{-1}_i$, $i = 1 \ldots n$, aus.

Dann ist $M = ([\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}) \cdot \bigoplus_{i=1}^n \phi\left(t_{i^{\sigma^{-1}}} \cdot t'^{-1}_i\right)$. ∎

1.3 Korollar Der Algorithmus 1.2 benötigt $O(n \log(n))$ Vergleiche von Nebenklassen und n Auswertungen von ϕ.

Beweis Zur Berechnung von σ sortiert man die Listen $(Ht_1, \ldots, Ht_n)$ und $(Ht'_1, \ldots, Ht'_n)$ und bildet den Quotient der sortierenden Permutationen. Der Rest ist klar. ∎

Der Transversalenwechsel ist der wichtigste Baustein für das Rechnen mit Induktionen. Die Sätze in den folgenden Abschnitten klären, wie das Zusammenspiel der Induktion mit den anderen Operationen auf Darstellungen funktioniert. Gleichheit wird in allen Fällen dadurch erzielt, daß bestimmte Transversalen gewählt werden. Will man eine Transformation ausführen, muß man also nur einen Wechsel von der gegebenen zur geforderten Transversale ausführen und die Darstellung transformiert.

Zweifache Induktion Induktion ist eine transitive Operation. Wenn ϕ eine Darstellung von H ist und $H \leq K \leq G$, dann gilt (vgl. Abbildung 1.1)

$$\phi \uparrow G \cong (\phi \uparrow K) \uparrow G.$$

Hier erreicht man Gleichheit durch geeignete Wahl der Transversalen.

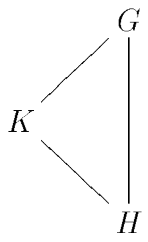

Abbildung 1.1: Situation bei zweifacher Induktion

1.4 Satz *Seien $H \leq K \leq G$ Gruppen und ϕ eine Darstellung von H, außerdem $S = (s_1, \ldots, s_m)$, $T = (t_1, \ldots, t_n)$ Transversalen von $H \backslash K$ bzw. $K \backslash G$. Dann gilt*

$$\phi \uparrow_{TS} G = (\phi \uparrow_T K) \uparrow_S G,$$

wobei $TS = (t_1 s_1, \ldots, t_n s_1, t_1 s_2, \ldots, t_n s_2, \ldots, t_1 s_m, \ldots, t_n s_m)$ das Komplexprodukt der Transversalen S und T ist.

Beweis TS ist eine Transversale von $H \backslash G$ und

$$\begin{aligned}
(\phi \uparrow_T K) \uparrow_S G &= \left(x \mapsto \left[\dot{\phi}(t_i x t_j^{-1})\right]_{i,j}\right) \uparrow_S G \\
&= x \mapsto \left[\dot{\phi}(t_i s_k x s_\ell^{-1} t_j^{-1})\right]_{(k,i),(\ell,j)} \\
&= \phi \uparrow_{TS} G,
\end{aligned}$$

wobei

$$\dot{\phi}(y) = \begin{cases} \phi(y), & y \in H \\ \mathbf{0}_{\deg(\phi_H)}, & \text{sonst} \end{cases} .$$

∎

Der letzte Satz ist wesentlich für die Zerlegung monomialer Darstellungen, er erlaubt es, die Induktion in kleine Schritte entlang einer Untergruppenkette zu zerlegen. Dazu ist es lediglich nötig, einen Transversalenwechsel gemäß Satz 1.1 auszuführen.

Direkte Summe Induktion ist additiv, das heißt ist $H \leq G$ mit Darstellungen ϕ_1 und ϕ_2, dann gilt

$$(\phi_1 \oplus \phi_2) \uparrow G \cong (\phi_1 \uparrow G) \oplus (\phi_2 \uparrow G).$$

Durch eine Permutationsmatrix läßt sich Gleichheit erreichen.

1.5 Satz *Sei $H \leq G$ eine Untergruppe mit Darstellungen ϕ_1 und ϕ_2 der Grade d_1 bzw. d_2 sowie T eine Transversale der Länge n von $H\backslash G$. Zur Abkürzung sei $d = d_1 + d_2$. Ist σ die Permutation, welche die Liste („$\cup$“ = Konkatenation)*

$$\bigcup_{k=0}^{n-1} (k \cdot d + 1, \ldots, k \cdot d + d_1) \ \cup \ \bigcup_{k=0}^{n-1} (k \cdot d + d_1 + 1, \ldots, (k+1) \cdot d)$$

abbildet auf $(1, \ldots, n \cdot d)$, dann gilt

$$((\phi_1 \oplus \phi_2) \uparrow_T G)^{[\sigma, n \cdot d]} = (\phi_1 \uparrow_T G) \oplus (\phi_2 \uparrow_T G).$$

Beweis Die Induktion hat den Grad $n \cdot d$. Die erste Konkatenation entspricht den Indizes der Basisvektoren des Darstellungsraums von $\phi_1 \uparrow G$ in $(\phi_1 \oplus \phi_2) \uparrow G$, entsprechend die zweite Konkatenation. Der zugehörige Basiswechsel zerlegt die Darstellung. ∎

Konjugation Die Induktion äquivalenter Darstellungen ϕ und $\psi = \phi^A$ liefert äquivalente Ergebnisse. Die konjugierende Matrix läßt sich direkt angeben.

1.6 Satz *Sei $H \leq G$ eine Untergruppe vom Index n mit Darstellung ϕ über $\mathbb{K}$ vom Grad d und T eine Transversale von $H\backslash G$. Ist $A \in \mathsf{GL}_d(\mathbb{K})$, dann gilt*

$$(\phi^A \uparrow_T G) = (\phi \uparrow_T G)^{(\mathbf{1}_n \otimes A)}.$$

Beweis Mit $x \in G$ gilt

$$\begin{aligned} (\phi^A \uparrow_T G)(x) &= \left[\dot{\phi^A}(t_i x t_j^{-1})\right]_{i,j} \\ &= \left[A^{-1} \cdot \dot{\phi}(t_i x t_j^{-1}) \cdot A\right]_{i,j} \\ &= (\phi \uparrow_T G)(x)^{(\mathbf{1}_d \otimes A)}, \end{aligned}$$

was zu zeigen war. ∎

Ist insbesondere A eine Zerlegungsmatrix von ϕ, dann läßt sich mit Satz 1.5 eine Permutationsmatrix P bestimmen, so daß $(\mathbf{1}_d \otimes A) \cdot P$ die Darstellung $\phi \uparrow G$ zerlegt (im allgemeinen aber nicht in Irreduzible).

Äußeres Tensorprodukt Seien G_1, G_2 Gruppen und $H_1 \leq G_1$, $H_2 \leq G_2$ Untergruppen mit Darstellungen ϕ_1, ϕ_2. Ein bekannter Satz der Darstellungstheorie (siehe z. B. [21], S. 316) besagt, daß (vgl. Abbildung 1.2)

$$(\phi_1 \uparrow G_1) \#(\phi_2 \uparrow G_2) \cong (\phi_1 \# \phi_2) \uparrow (G_1 \times G_2).$$

Bei geeigneter Wahl der Transversalen läßt sich auch hier Gleichheit erzielen. Der folgende Satz ist eine Grundlage für die konstruktive Zerlegung von monomialen Darstellungen in ein äußeres Tensorprodukt.

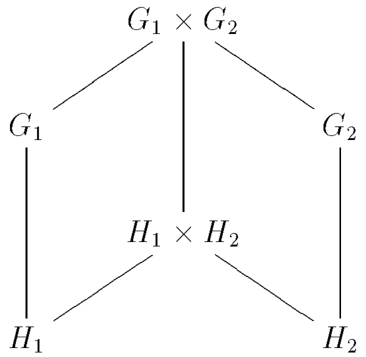

Abbildung 1.2: Situation beim äußeren Tensorprodukt von Induktionen

1.7 Satz *Seien $H_1 \leq G_1$ und $H_2 \leq G_2$ Untergruppen mit Darstellungen ϕ_1 und ϕ_2 sowie $T_1 = (t_1^{(1)}, \ldots, t_n^{(1)})$ und $T_2 = (t_1^{(2)}, \ldots, t_m^{(2)})$ Transversalen von $H_1 \backslash G_1$ bzw. $H_2 \backslash G_2$. Dann gilt*

$$(\phi_1 \uparrow_{T_1} G_1) \#(\phi_2 \uparrow_{T_2} G_2) = (\phi_1 \# \phi_2) \uparrow_{T_1 \times T_2} (G_1 \times G_2),$$

wobei $T_1 \times T_2 = \big((t_1^{(1)}, t_1^{(2)}), (t_1^{(1)}, t_2^{(2)}), \ldots\big)$ das kartesische Produkt der Listen T_1 und T_2 bezeichnet.

Beweis $T_1 \times T_2$ ist eine Transversale von $(H_1 \times H_2) \backslash (G_1 \times G_2)$ und

$$\begin{aligned}
& ((\phi_1 \uparrow_{T_1} G_1) \#(\phi_2 \uparrow_{T_2} G_2))(x_1, x_2) \\
= \; & \left[\dot{\phi}_1(t_i^{(1)} x_1 t_j^{(1)^{-1}})\right]_{i,j} \otimes \left[\dot{\phi}_2(t_k^{(2)} x_2 t_\ell^{(2)^{-1}})\right]_{k,\ell} \\
= \; & \left[(\phi_1 \,\dot{\#}\, \phi_2)\left((t_i^{(1)} x_1 t_j^{(1)^{-1}}), (t_k^{(2)} x_2 t_\ell^{(2)^{-1}})\right)\right]_{(i,k),(j,\ell)} \\
= \; & ((\phi_1 \# \phi_2) \uparrow_{T_1 \times T_2} (G_1 \times G_2))(x_1, x_2),
\end{aligned}$$

woraus die Behauptung folgt. ■

Sind die in Satz 1.7 auftretenden Produkte $H_1 \times H_2$ und $G_1 \times G_2$ innere direkte Produkte, so ist $T_1 \times T_2 = T_1 T_2$ gerade wieder das Komplexprodukt der Transversalen. Um eine Induktion in ein äußeres Tensorprodukt zu zerlegen, genügt es jedoch nicht, daß die dargestellte Gruppe ein direktes Produkt ist. Im Abschnitt 1.3 werden wir für den Spezialfall von monomialen Darstellungen ein notwendiges und hinreichendes Kriterium für die Existenz einer solchen Zerlegung kennenlernen.

Innere Konjugation In diesem Abschnitt wollen wir untersuchen, wie das Zusammenspiel zwischen Induktion und innerer Konjugation funktioniert. Zunächst wollen wir zur Erinnerung noch einmal die Definition der inneren Konjugation angeben.

1.8 Definition *Sei $H \leq G$ eine Untergruppe, ϕ eine Darstellung von H und $s \in G$. Dann ist*

$$\phi^s = x \mapsto \phi(sxs^{-1})$$

eine Darstellung von $H^s = s^{-1}Hs$ und heißt die „innere Konjugierte“ von ϕ mit s.

Wir möchten an dieser Stelle noch einmal darauf hinweisen, daß diese Definition die folgende Rechenregel impliziert:

$$\left(\phi_H^t\right)^s = \phi^{ts} = g \mapsto \phi_H(tsgs^{-1}t^{-1}),$$

das heißt g wird *zuerst* mit dem Inversen des *äußeren* Exponenten konjugiert.

1.9 Beispiel Wir betrachten $\mathsf{S}_3 = \langle x, y \mid x^3 = y^2 = 1,\ x^y = x^{-1} \rangle$ mit Normalteiler $\mathsf{Z}_3 = \langle x \rangle \trianglelefteq \mathsf{S}_3$. Z_3 hat die Darstellung $\lambda :\ x \mapsto \omega_3$ (ω_3 ist eine primitive 3-te Einheitswurzel) und es gilt

$$\lambda^y :\ x \mapsto \lambda(yxy^{-1}) = \lambda(x^{-1}) = \omega_3^{-1},$$

also $\lambda \not\cong \lambda^y = \lambda^{-1}$. ■

Die Induktion einer Darstellung ϕ von $H \leq G$ läßt sich umrechnen in eine Induktion von ϕ^s.

1.10 Satz *Sei $H \leq G$ eine Untergruppe, $s \in G$, ϕ eine Darstellung von H und T eine Transversale von $H \backslash G$. Dann ist*

$$\phi \uparrow_T G = \phi^s \uparrow_{s^{-1}T} G.$$

Beweis Sei $T = (t_1, \ldots, t_n)$ und $x \in G$:

$$\begin{aligned}(\phi \uparrow_T G)(x) &= \left[\dot{\phi}(t_i x t_j^{-1})\right]_{i,j} \\ &= \left[\dot{\phi}^s(s^{-1} t_i x t_j^{-1} s)\right]_{i,j} \\ &= (\phi^s \uparrow_{s^{-1}T} G)(x).\end{aligned}$$

Man beachte, daß $s^{-1}T$ eine Transversale von $H^s \backslash G$ ist. ∎

Insbesondere gilt also $\phi \uparrow G \cong \phi^s \uparrow G$. Was passiert bei innerer Konjugation einer Induktion?

1.11 Satz *Seien $H \leq K \leq G$, ϕ eine Darstellung von H, T eine Transversale von $H \backslash K$ und $s \in G$. Dann gilt*

$$(\phi \uparrow_T K)^s = \phi^s \uparrow_{T^s} K^s,$$

wobei $T^s = (s^{-1}t_1 s, \ldots, s^{-1}t_n s)$ die elementweise Konjugation der Transversalen $T = (t_1, \ldots, t_n)$ mit s bezeichnet.

Beweis Für $x \in K^s$ gilt

$$\begin{aligned}(\phi \uparrow_T K)^s(x) &= (\phi \uparrow_T K)(sxs^{-1}) \\ &= \left[\dot{\phi}(t_i sxs^{-1} t_j^{-1})\right]_{i,j} \\ &= \left[\dot{\phi}^s(t_i^s x (t_j^s)^{-1})\right]_{i,j} \\ &= (\phi^s \uparrow_{T^s} K^s)(x),\end{aligned}$$

was die Behauptung ist. ∎

Einschränkung Der Untergruppensatz von Mackey ermöglicht eine teilweise Zerlegung der Einschränkung einer Induktion auf eine beliebige Untergruppe. Sind $H, K \leq G$ Untergruppen und ϕ eine Darstellung von H, dann ist

$$(\phi \uparrow G) \downarrow K \cong \bigoplus_{s \in S} (\phi^s \downarrow (H^s \cap K)) \uparrow K,$$

wo S ein Vertretersystem der Doppelnebenklassen $H \backslash G / K = \{HgK \mid g \in G\}$ bezeichnet (vgl. Abbildung 1.3). Die Indizes $(K : (H^s \cap K))$, $s \in S$, sind natürlich im allgemeinen verschieden. Wir wollen für die Induktionen Transversalen angeben, so daß Gleichheit gilt.

1.12 Satz (Untergruppensatz von Mackey) *Seien $H, K \leq G$ Untergruppen, ϕ eine Darstellung von H sowie $S = (s_1, \ldots, s_n)$ ein Vertretersystem der Doppelnebenklassen $H \backslash G / K$. Weiter seien $T_i = (t_{i,1}, \ldots, t_{i,r_i})$, $i = 1 \ldots n$, Transversalen von $(H^{s_i} \cap K) \backslash K$. Dann ist die Konkatenation*

$$T = \bigcup_{i=1}^{n} s_i T_i \textit{ eine Transversale von } H \backslash G$$

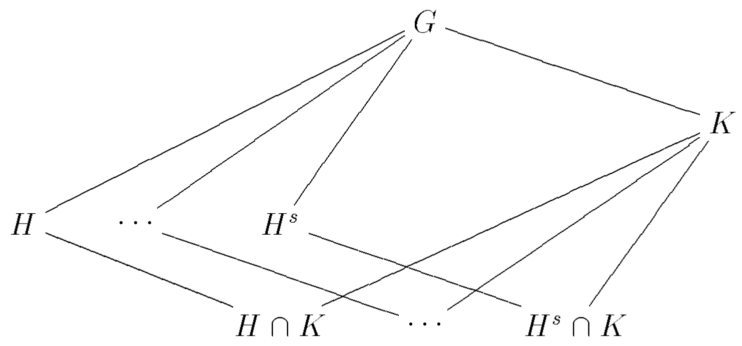

Abbildung 1.3: Situation beim Untergruppensatz von Mackey

und

$$(\phi \uparrow_T G) \downarrow K = \bigoplus_{i=1}^{n} (\phi^{s_i} \downarrow (H^{s_i} \cap K)) \uparrow_{T_i} K.$$

Ist $s \in G$, dann hängt die Äquivalenzklasse der Darstellung $(\phi^s \downarrow (H^s \cap K)) \uparrow K$ nur ab von der Doppelnebenklasse HsK.

Beweis T ist Transversale: Wegen $(G : H) = \sum_{i=1}^{n}(K : (H^{s_i} \cap K))$ hat T die richtige Länge. Seien $x, y \in T, x \neq y$:
1. Fall: $\exists i : x, y \in T_i$, also $x = s_i t_{i,j},\ y = s_i t_{i,k},\ j \neq k$,

$$xy^{-1} \in H \Leftrightarrow s_i t_{i,j} {t_{i,k}}^{-1} s_i^{-1} \in H \Leftrightarrow t_{i,j} {t_{i,k}}^{-1} \in H^{s_i},$$

ein Widerspruch zur Tatsache, daß T_i eine Transversale von $(H^{s_i} \cap K)\backslash K$ ist.
2. Fall: $x = s_i t_{i,k},\ y = s_j t_{j,\ell},\ i \neq j$,

$$xy^{-1} \in H \Leftrightarrow s_i t_{i,k} {t_{j,\ell}}^{-1} s_j^{-1} \in H \Leftrightarrow H s_i \underbrace{t_{i,k} {t_{j,\ell}}^{-1}}_{\in K} = H s_j,$$

ein Widerspruch dazu, daß s_i, s_j in verschiedenen Doppelnebenklassen liegen.
Sei nun $x \in K$:

$$\begin{aligned}
(\phi \uparrow_T G)(x) &= \left[\dot{\phi}(t_i x t_j^{-1}) \,\middle|\, i, j \in \{1, \ldots, \sum_{k=1}^{n} r_k\} \right] \\
&= \bigoplus_{k=1}^{n} \left[\dot{\phi}(s_k t_{k,i} x {t_{k,j}}^{-1} s_k^{-1}) \mid i, j \in \{1, \ldots, r_k\} \right] \\
&= \bigoplus_{k=1}^{n} \left[\dot{\phi^{s_k}}(t_{k,i} x {t_{k,j}}^{-1}) \mid i, j \in \{1, \ldots, r_k\} \right] \\
&= \bigoplus_{k=1}^{n} \left((\phi^{s_k} \downarrow (H^{s_k} \cap K)) \uparrow_{T_k} K \right)(x).
\end{aligned}$$

Es bleibt zu zeigen, daß, für $s \in G$, die Äquivalenzklasse der Induktion $(\phi^s \downarrow (H^s \cap K)) \uparrow K$ nur von der Doppelnebenklasse HsK abhängt. Sei dazu U eine Transversale der Länge n von $H^s \backslash G$. Mit $h \in H$ gilt

$$\begin{aligned}\left(\phi^{hs} \downarrow (H^{hs} \cap K)\right) \uparrow_U K &= (\phi^s \downarrow (H^s \cap K))^{\phi(h^{-1})} \uparrow_U K \\ &= ((\phi^s \downarrow (H^s \cap K)) \uparrow_U K)^{\mathbf{1}_n \otimes \phi(h^{-1})}\end{aligned}$$

nach Satz 1.6. Sei nun $k \in K$ und V eine Transversale von $H^{sk} \backslash G$, dann gilt

$$\begin{aligned}\left(\phi^{sk} \downarrow (H^{sk} \cap K)\right) \uparrow_V K &= (\phi^s \downarrow (H^s \cap K))^k \uparrow_V K \\ &= (\phi^s \downarrow (H^s \cap k)) \uparrow_{kV} K,\end{aligned}$$

nach Satz 1.10. Das war zu zeigen. ∎

Ist $\phi = 1_H$ die Einsdarstellung bzw. $\phi \uparrow G$ eine Permutationsdarstellung, dann liefert der Satz von Mackey genau die Zerlegung von $(1_H \uparrow G) \downarrow K$ in transitive Konstituenten. Zwei Spezialfälle werden eine besondere Bedeutung spielen.

1.13 Korollar Ist $N \trianglelefteq G$, ϕ eine Darstellung von N und T eine Transversale von G/N, dann gilt

$$(\phi \uparrow_T G) \downarrow N = \bigoplus_{t \in T} \phi^t.$$

Beweis Aus $N \backslash G / N = G/N$ und Satz 1.12 folgt die Behauptung. ∎

1.14 Korollar Ist $H \leq G$, $N \trianglelefteq G$ mit $HN = G$, ϕ eine Darstellung von H und T eine Transversale von $(N \cap H) \backslash N$, dann ist T auch eine Transversale von $H \backslash G$ und

$$(\phi \uparrow_T G) \downarrow N = (\phi \downarrow (N \cap H)) \uparrow_T N.$$

Beweis Wegen $H \backslash G / N = HN \backslash G = G \backslash G$ gibt es nur eine Doppelnebenklasse mit Vertreter 1. Der Rest folgt aus Satz 1.12. ∎

Eine Äquivalenz, welche in den genannten Standardwerken selten erwähnt wird, betrachtet die Induktion einer Einschränkung. Für $H \leq G$ und eine Darstellung ϕ von G gilt

$$(\phi \downarrow H) \uparrow G \cong (1_H \uparrow G) \otimes \phi.$$

Dies wird im folgenden Satz konstruktiv bewiesen.

1.15 Satz *Sei $H \leq G$ eine Untergruppe, ϕ eine Darstellung von G und $T = (t_1, \ldots, t_n)$ eine Transversale von $H \backslash G$. Dann gilt*

$$((\phi \downarrow H) \uparrow_T G)^D = (1_H \uparrow_T G) \otimes \phi, \ \textit{mit } D = \bigoplus_{t \in T} \phi(t).$$

Beweis Für $x \in G$ gilt

$$\begin{aligned}((\phi \downarrow H) \uparrow_T G)^D(x) &= \left[\phi(t_i)^{-1}(\phi \dot{\downarrow} H)(t_i x t_j^{-1})\phi(t_j)\right]_{i,j} \\ &= \left[\dot{1}_H(t_i x t_j^{-1}) \cdot \phi(x)\right]_{i,j} \\ &= (1_H \uparrow_T G)(x) \otimes \phi(x).\end{aligned}$$

Das zweite „=“ gilt wegen: ist $t_i x t_j^{-1} \in H$, so ist der Block

$$\phi(t_i)^{-1}(\phi \dot{\downarrow} H)(t_i x t_j^{-1})\phi(t_j) = \phi(x),$$

sonst die Nullmatrix. ∎

Inneres Tensorprodukt Die teilweise Zerlegung eines inneren Tensorprodukts zweier Induktionen wird in dem sogenannten *Tensorproduktsatz* beschrieben. Sind $H_1, H_2 \leq G$ Untergruppen mit Darstellungen ϕ_1, ϕ_2 und S ein Vertretersystem der Doppelnebenklassen $H_1 \backslash G / H_2$, dann gilt

$$(\phi_1 \uparrow G) \otimes (\phi_2 \uparrow G) \cong \bigoplus_{s \in S} (\phi_1^s \downarrow (H_1^s \cap H_2) \otimes \phi_2 \downarrow (H_1^s \cap H_2)) \uparrow G.$$

Um diesen Satz konstruktiv zu formulieren, führen wir zunächst eine Notation ein, welche nur in diesem Abschnitt verwendet wird.

1.16 Definition *Sei G eine Gruppe. Wir bezeichnen mit $\overline{G} = \{(g,g) \mid g \in G\}$ die diagonale Einbettung von G in $G \times G$. Für $H \subseteq G$ ist entsprechend $\overline{H} = \{(h,h) \mid h \in H\}$. Ist ϕ eine Darstellung von G, so bezeichnet*

$$\overline{\phi}: \ (g,g) \mapsto \phi(g)$$

die entsprechende Darstellung von $\overline{G}$.

Das Symbol $\overline{\phi}$ bedeutet im folgenden Satz (und nur dort) also nicht eine Erweiterung von ϕ.

1.17 Satz (Tensorproduktsatz) *Seien $H_1, H_2 \leq G$ Untergruppen mit Darstellungen ϕ_1, ϕ_2 sowie R_i eine Transversale von $H_i \backslash G$, $i = 1, 2$.*
Ist $S = ((x_1, y_1), \ldots, (x_n, y_n))$ ein Vertretersystem der Doppelnebenklassen $(H_1 \times H_2) \backslash (G \times G) / \overline{G}$, dann ist $S' = (x_1 y_1^{-1}, \ldots, x_n y_n^{-1})$ ein Vertretersystem der Doppelnebenklassen $H_1 \backslash G / H_2$ und es gilt

$$(H_1 \times H_2)^{(x_i, y_i)} \cap \overline{G} = \overline{H_1^{x_i} \cap H_2^{y_i}}.$$

Sei weiter T_i eine Transversale von $(H_1^{x_i} \cap H_2^{y_i}) \backslash G$, $i = 1 \ldots n$, und M die (block-permutierte) Matrix zum Transversalenwechsel $(R_1, R_2) \to T = \bigcup_{i=1}^n (x_i, y_i) \cdot \overline{T_i}$ folgender Darstellung (vgl. Satz 1.1):

$$\left((\phi_1 \# \phi_2) \uparrow_{(R_1, R_2)} (G \times G)\right)^M = (\phi_1 \# \phi_2) \uparrow_T (G \times G).$$

Dann gilt (siehe Abbildung 1.4)

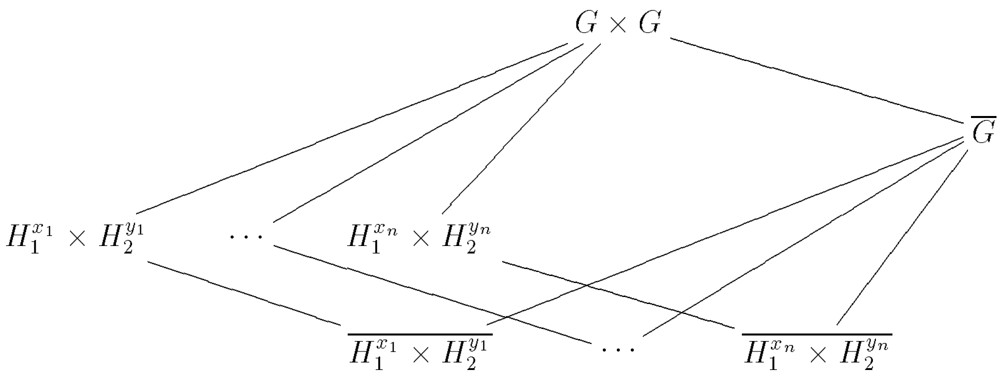

Abbildung 1.4: Situation beim Tensorproduktsatz

$$((\phi_1 \uparrow_{R_1} G) \otimes (\phi_2 \uparrow_{R_2} G))^M =$$

$$\bigoplus_{i=1}^{n} ((\phi_1^{x_i} \downarrow (H_1^{x_i} \cap H_2^{y_i})) \otimes (\phi_2^{y_i} \downarrow (H_1^{x_i} \cap H_2^{y_i}))) \uparrow_{T_i} G.$$

Die Äquivalenzklasse der Darstellung $(\phi_1^{x_i} \downarrow (H_1^{x_i} \cap H_2^{y_i})) \otimes (\phi_2^{y_i} \downarrow (H_1^{x_i} \cap H_2^{y_i}))$ *hängt nur ab von der Doppelnebenklasse* $H_1 \cdot x_i y_i^{-1} \cdot H_2$.

Beweis Wir zeigen zunächst die Korrespondenz zwischen den Doppelnebenklassen $(H_1 \times H_2)\backslash(G \times G)/\overline{G}$ und den Doppelnebenklassen $H_1\backslash G/H_2$.

$$\begin{array}{ll}
& (x_1, x_2), (y_1, y_2) \text{ sind in 2 verschiedenen} \\
& \text{Doppelnebenklassen } (H_1 \times H_2)\backslash(G \times G)/\overline{G} \\
\Leftrightarrow & \forall g \in G: \ (x_1, x_2) \cdot (g, g) \cdot (y_1, y_2)^{-1} \notin (H_1 \times H_2) \\
\Leftrightarrow & \forall g \in G: \ (x_1 g y_1^{-1}, x_2 g y_2^{-1}) \notin (H_1 \times H_2) \\
\Leftrightarrow & x_1^{-1} H_1 y_1 \cap x_2^{-1} H_2 y_2 = \emptyset \\
\Leftrightarrow & H_1 \cap x_1 x_2^{-1} H_2 (y_1 y_2^{-1})^{-1} = \emptyset \\
\Leftrightarrow & x_1 x_2^{-1}, y_1 y_2^{-1} \text{ sind in 2 verschiedenen} \\
& \text{Doppelnebenklassen } H_1\backslash G/H_2.
\end{array}$$

Die Gleichung

$$(H_1 \times H_2)^{(x_i, y_i)} \cap \overline{G} = \overline{H_1^{x_i} \cap H_2^{y_i}}$$

bestätigt man leicht durch Nachrechnen. Sind ψ_1, ψ_2 Darstellungen von G, so läßt sich das innere Tensorprodukt von ψ_1 und ψ_2 interpretieren als Einschränkung des äußeren Tensorprodukts. Genauer gilt für die diagonalen Einbettungen in $G \times G$

$$\overline{\psi_1 \otimes \psi_2} = (\psi_1 \# \psi_2) \downarrow \overline{G}.$$

Damit folgt

$$\begin{aligned}
& \overline{((\phi_1 \uparrow_{R_1} G) \otimes (\phi_2 \uparrow_{R_2} G))}^M \\
= \; & ((\phi_1 \uparrow_{R_1} G) \# (\phi_2 \uparrow_{R_2} G))^M \downarrow \overline{G} \\
= \; & \Big((\phi_1 \# \phi_2) \uparrow_{(R_1,R_2)} G\Big)^M \downarrow \overline{G} \\
& (\text{Satz 1.7}) \\
= \; & ((\phi_1 \# \phi_2) \uparrow_T G) \downarrow \overline{G} \\
& (\text{Satz von Mackey, 1.12}) \\
= \; & \bigoplus_{i=1}^n \Big((\phi_1 \# \phi_2)^{(x_i,y_i)} \downarrow ((H_1 \times H_1)^{(x_i,y_i)} \cap \overline{G})\Big) \uparrow_{\overline{T_i}} \overline{G} \\
= \; & \bigoplus_{i=1}^n \Big((\phi_1 \# \phi_2)^{(x_i,y_i)} \downarrow (\overline{H_1^{x_i} \cap H_2^{y_i}})\Big) \uparrow_{\overline{T_i}} \overline{G} \\
= \; & \bigoplus_{i=1}^n \Big(\overline{(\phi_1^{x_i} \downarrow (H_1^{x_i} \cap H_2^{y_i}))} \otimes \overline{(\phi_2^{y_i} \downarrow (H_1^{x_i} \cap H_2^{y_i}))}\Big) \uparrow_{\overline{T_i}} \overline{G}.
\end{aligned}$$

Weglassen des Überstrichs auf beiden Seiten ergibt die Behauptung. Der Beweis, daß die Darstellung $(\phi_1^{x_i} \downarrow (H_1^{x_i} \cap H_2^{y_i})) \otimes (\phi_2^{y_i} \downarrow (H_1^{x_i} \cap H_2^{y_i}))$ nur von der Doppelnebenklasse $H_1 \cdot x_i y_i^{-1} \cdot H_2$ abhängt, verläuft analog zum Beweis der entsprechenden Behauptung im Satz von Mackey 1.12. ∎

Sind $\phi_1 = 1_{H_1}$ und $\phi_2 = 1_{H_2}$ Einsdarstellungen bzw. $\phi_1 \uparrow G$ und $\phi_2 \uparrow G$ Permutationsdarstellungen, dann liefert der Tensorproduktsatz genau die Zerlegung des inneren Tensorprodukts in transitive Konstituenten.

Kern einer Induktion Der Kern einer Induktion läßt sich wie folgt berechnen.

1.18 Satz *Sei ϕ eine Darstellung von $H \leq G$. Dann ist* $\ker(\phi \uparrow G)$ *der normale Schnitt von* $\mathrm{core}(H)$ *und* $\ker(\phi)$, *das heißt der größte Normalteiler von* $\mathrm{core}(H)$ *und* $\ker(\phi)$ *in G, wobei*

$$\mathrm{core}(H) = \bigcap_{t \in G} H^t \trianglelefteq G$$

der Schnitt aller zu H konjugierten Untergruppen ist.

Beweis Sei $T = (t_1, \ldots, t_n)$ eine Transversale von $H \backslash G$ und $x \in \ker(\phi \uparrow_T G)$. Dann ist $txt^{-1} \in H$ für alle $t \in T$ und $txt^{-1} \in \ker(\phi)$. Ersteres heißt $x \in \mathrm{core}(H)$, die zweite Aussage zeigt $x \in \ker(\phi)$ und da $\ker(\phi \uparrow_T G) \trianglelefteq G$ folgt, daß x im normalen Schnitt von $\mathrm{core}(H)$ und $\ker(\phi)$ liegt.
Sei umgekehrt x im normalen Schnitt von $\mathrm{core}(H)$ und $\ker(\phi)$. Dann ist $txt^{-1} \in H$, $t \in T$ und $txt^{-1} \in \ker(\phi)$ für alle $t \in G$, also insbesondere für alle $t \in T$, woraus $x \in \ker(\phi \uparrow_T G)$ folgt. ∎

Insbesondere ist also der Kern einer Permutationsdarstellung $\pi = 1_H \uparrow G$ gegeben durch core(H).

Unitäre Darstellungen Der folgende Satz zeigt, daß die Induktion einer unitären Darstellung wieder unitär ist.

1.19 Satz *Sei ϕ eine unitäre Darstellung von $H \leq G$ und T eine Transversale von $H \backslash G$. Dann ist $\phi \uparrow_T G$ ebenfalls unitär.*

Beweis Sei $n = \deg(\phi)$ und $m = (G : H)$, $x \in G$. Dann ist $A = (\phi \uparrow_T G)(x) = [\dot{\phi}(t_i x t_j^{-1})]$ blockpermutiert mit m Blöcken der Größe n, $A^* = [\dot{\phi}(t_i x t_j^{-1})]^* = [\dot{\phi}(t_j x t_i^{-1})^*]$ ebenso, also auch $A \cdot A^*$. Wir berechnen den Block $B_{k,\ell}$ von $A \cdot A^*$ an der Stelle $(k, \ell) \in \{1, \ldots, m\} \times \{1, \ldots, m\}$ zu

$$B_{k,\ell} = \sum_{i=1}^{m} \dot{\phi}(t_k x t_i^{-1}) \cdot \dot{\phi}(t_\ell x t_i^{-1})^*.$$

Die Summe ist $= \mathbf{0}_n$, wenn $k \neq \ell$, da einer der beiden Faktoren in der Summe stets $= \mathbf{0}_n$ ist. Für $k = \ell$ gibt es ein j, so daß $t_k x t_j^{-1} \in H$ und

$$B_{k,k} = \sum_{i=1}^{m} \dot{\phi}(t_k x t_i^{-1}) \cdot \dot{\phi}(t_k x t_i^{-1})^* = \phi(t_k x t_j^{-1}) \cdot \phi(t_k x t_j^{-1})^* = \mathbf{1}_n,$$

da ϕ unitär ist. ∎

1.3 Monomiale Darstellungen

Monomiale Darstellungen sind eine natürliche Verallgemeinerung von Permutationsdarstellungen. Eine Darstellung $\phi : G \to \mathsf{GL}_n(\mathbb{K})$ einer Gruppe G heißt monomial, wenn jedes Bild $\phi(g)$, $g \in G$, eine monomiale Matrix ist, das heißt $\phi(g)$ enthält in jeder Spalte und Zeile genau einen Eintrag $\neq 0$. Bildet die Menge aller Permutationsmatrizen in $\mathsf{GL}_n(\mathbb{K})$ noch eine endliche Menge (der Größe $n!$), so gilt dies nicht mehr für die Menge aller monomialen Matrizen (wenn $|\mathbb{K}| = \infty$), auch nicht für die Teilmenge der monomialen Matrizen mit endlicher Ordnung.
Es gibt bedeutend weniger Literatur zu monomialen Darstellungen bzw. Gruppen als für Permutationsgruppen, obwohl sich keineswegs alle Fragestellungen durch Zurückführen auf diese beantworten lassen. Beispielsweise können monomiale Darstellungen vom Grad > 1 durchaus irreduzibel sein, was bei Permutationsdarstellungen unmöglich ist. Darüber hinaus gibt es eine Klasse von Gruppen (sogenannte M-Gruppen), bei denen jede Darstellung ähnlich ist zu einer monomialen Darstellung.
Als Literatur zu monomialen Gruppen sei hier lediglich Ore (1942), [49] und Crouch (1955), [20] genannt, welche aber zu der hier behandelten Problemstellung nichts beitragen.

Im folgenden werden die wichtigsten konstruktiven Ergebnisse zu monomialen Darstellungen zusammengestellt. Da eine monomiale Darstellung im wesentlichen eine direkte Summe von Induktionen von Darstellungen vom Grad 1 ist (vgl. Satz 1.22 und Satz 1.24), finden die Sätze aus dem vorigen Abschnitt eine Anwendung. Zunächst wollen wir einige Begriffe für Permutationsdarstellungen auf monomiale Darstellungen verallgemeinern. Dazu ordnen wir jeder monomialen Darstellung μ in eindeutiger Weise eine Permutationsdarstellung zu.

1.20 Definition *Sei μ eine monomiale Darstellung. Ersetzt man in den Bildmatrizen von μ die Einträge $\neq 0$ durch 1, so erhält man eine Permutationsdarstellung, welche mit $\hat{\mu}$ bezeichnet wird.*

Mittels $\hat{\mu}$ lassen sich viele Begriffe für Permutationsdarstellungen auf monomiale übertragen. Als Literatur zu Permutationsgruppen sei hier genannt: Das schöne Buch von Wielandt (1964), [60] liefert eine sehr gute Einführung, im Buch von Passman (1968), [50] sind manche Aspekte besser dargestellt, das Buch von Dixon/Mortimer (1996), [24] ist das neueste Standardwerk und enthält unter anderem den Satz von O'Nan/Scott zur Klassifikation der primitiven Permutationsgruppen.

1.21 Definition *Eine monomiale Darstellung μ einer Gruppe G heiße transitiv, primitiv, n-fach transitiv, wenn es für $\hat{\mu}$ gilt. Die Orbits von μ auf $\{1, \ldots, \deg(\mu)\}$ seien die Orbits von $\hat{\mu}$ auf dieser Menge. Der Stabilisator* $\mathrm{stab}_\mu(i)$ *eines Punktes i unter μ sei der Stabilisator von i unter $\hat{\mu}$.*

Orbitzerlegung Wie Permutationsdarstellungen lassen sich auch monomiale Darstellungen bzgl. ihrer Orbits in eine direkte Summe von transitiven Konstituenten zerlegen, nötig dazu ist nur eine Permutation. Für eine weitergehende Zerlegung kann man sich dann auf den transitiven Fall beschränken, der in den folgenden Abschnitten untersucht wird.

1.22 Satz *Sei μ eine monomiale Darstellung vom Grad n einer Gruppe G. Die Orbits von μ auf $\{1, \ldots, n\}$ seien gegeben durch die Listen $O_1, \ldots, O_k$. Weiter sei σ die Permutation, welche $L = (\ell_1, \ldots, \ell_n) = O_1 \cup \cdots \cup O_k$ auf $(1, \ldots, n)$ abbildet, das heißt $\ell_i^\sigma = i,\ i = 1 \ldots n$. Dann gilt*

$$\mu^{[\sigma,n]} = \bigoplus_{i=1}^{k} \mu_i,$$

wobei die μ_i transitive, monomiale Darstellungen sind.

Beweis trivial. ∎

Der Algorithmus zur Orbitzerlegung ist demnach wie folgt.

1.23 Algorithmus (Orbitzerlegung) Gegeben sei eine monomiale Darstellung μ vom Grad n einer Gruppe G. μ soll in seine transitiven Konstituenten zerlegt werden.

1. Bestimme die Orbits $O_1, \ldots, O_k$ von μ auf $\{1, \ldots, n\}$.
2. Konkateniere die Orbits zu einer Liste $L = \bigcup_{i=1}^k O_i = (\ell_1, \ldots, \ell_n)$ und bestimme die Permutation $\sigma \in \mathsf{S}_n$ mit $\ell_i^\sigma = i,\ i = 1 \ldots n$.
3. Konjugiere μ mit $[\sigma, n]$ und zerlege in eine direkte Summe von transitiven Darstellungen $\mu_1, \ldots, \mu_k$ mit Graden $|O_1|, \ldots, |O_k|$.

Es gilt $\mu^{[\sigma,n]} = \bigoplus_{i=1}^{k} \mu_i$, die μ_i sind transitiv. ∎

Zerlegung in eine Induktion Jede transitive monomiale Darstellung ist äquivalent zu einer Induktion einer Darstellung λ vom Grad 1 einer Untergruppe H. Diesen Satz werden wir im folgenden konstruktiv beweisen.

1.24 Satz *Sei μ eine transitive monomiale Darstellung einer Gruppe G auf dem Darstellungsraum $V = \langle v_1, \ldots, v_n \rangle$, das heißt*

$$v_i \cdot \mu(g) = v_{i^{\hat{\mu}(g)}} \cdot a_i(g).$$

Dann existiert eine Diagonalmatrix D, eine Untergruppe $H \leq G$ mit einer Darstellung λ vom Grad 1 und eine Transversale T, so daß

$$\mu^D = \lambda \uparrow_T G.$$

Beweis Sei $H = \mathrm{stab}_\mu(1)$ der Stabilisator von 1 unter μ. Da μ transitiv ist, gilt $(G : H) = \deg(\mu) = n$. Sei $T = (t_1, \ldots, t_n)$ eine Transversale von $H \backslash G$ mit $1^{\hat{\mu}(t_i)} = i$. Für $h \in H$ gilt $v_1 \mu(h) = v_1 a_1(h)$, womit durch

$$\lambda : \ h \mapsto a_1(h)$$

eine Darstellung λ von H vom Grad 1 definiert wird. Zu der induzierten Darstellung gehört der Darstellungsraum $V^G = \langle v_1 \otimes t_i \mid i = 1 \ldots n \rangle$. Mit $t_i g = h_i t_{i'},\ h_i \in H$ gilt

$$\begin{aligned}(v_1 \otimes t_i)(\lambda \uparrow_T G)(g) &= v_1 \lambda(h_i) \otimes t_{i'} \\ &= (v_1 \otimes t_{i'}) a_1(h_i).\end{aligned}$$

Wir definieren $w_i = v_1 \mu(t_i) = v_i a_1(t_i)$ für $i = 1 \ldots n$ und berechnen

$$\begin{aligned}w_i \cdot \mu(g) &= v_1 \cdot \mu(t_i g) \\ &= v_1 \cdot \mu(h_i t_{i'}) \\ &= v_1 \cdot a_1(h_i) \mu(t_{i'}) \\ &= w_{i'} \cdot a_1(h_i).\end{aligned}$$

Also liefert der Basiswechsel $v_i \to a_1(t_i)v_i,\ i = 1 \dots n$, den Übergang von μ zu $\lambda \uparrow_T G$. Dazu gehört die Basiswechselmatrix

$$D = \mathrm{diag}(a_1(t_i)^{-1} \mid i = 1 \dots n),$$

da G von *rechts* operiert. ∎

Der Fall einer transitiven Permutationsdarstellung μ verdient besondere Beachtung: hier ist μ sogar gleich einer Induktion.

1.25 Korollar Ist unter den Voraussetzungen von Satz 1.24 μ sogar eine Permutationsdarstellung und $H = \mathrm{stab}_\mu(1)$ der Stabilisator der 1 unter μ, so ist

$$\mu = 1_H \uparrow_T G$$

für jede Transversale $T = (t_1, \dots, t_n)$ von $H \backslash G$ mit der Eigenschaft $1^{\mu(t_i)} = i,\ i = 1 \dots n$.

Beweis Da alle Einträge 1 sind in den Bildern von μ, ist 1_H die Darstellung, von der μ induziert ist. Die Korrekturmatrix D degeneriert damit zur Identität. ∎

Mit dem Beweis von Satz 1.24 ergibt sich der folgende Algorithmus zur Zerlegung einer transitiven monomialen Darstellung in eine konjugierte Induktion.

1.26 Algorithmus (Zerlegung in eine Induktion) Sei μ eine beliebige transitive monomiale Darstellung einer Gruppe G. μ soll in eine konjugierte Induktion einer Darstellung vom Grad 1 einer Untergruppe zerlegt werden.

1. Bestimme den Stabilisator $H = \mathrm{stab}_\mu(1)$ von 1 unter μ.

2. Berechne eine Liste $T = (t_1, \dots, t_n)$ mit $t_i \in G$ und $1^{\hat{\mu}(t_i)} = i$.

3. Bestimme eine Darstellung $\lambda,\ (\deg(\lambda) = 1)$ von H durch

$$\lambda : \ h \mapsto \mu(h)_{1,1},$$

wobei $\mu(h)_{1,1}$ die linke, obere Komponente in der Matrix $\mu(h)$ bezeichnet.

4. Berechne $a_1(t_i)$ für $i = 1 \dots n$, wobei $a_1(t_i)$ definiert ist als der Eintrag $\neq 0$ in der ersten Zeile von $\mu(t_i)$.

Es gilt

$$\mu^D = \lambda \uparrow_T G, \ \text{mit } D = \mathrm{diag}(a_1(t_i)^{-1} \mid i = 1 \dots n).$$

∎

1.27 Beispiel Die folgende monomiale Darstellung der symmetrischen Gruppe $\mathsf{S}_3 = \langle x, y \mid x^3 = y^2 = 1,\ x^y = x^{-1}\rangle$ soll mit Algorithmus 1.26 in eine konjugierte Induktion zerlegt werden.

$$\mu:\ x \mapsto \begin{bmatrix} 0 & 1/2 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{bmatrix},\ y \mapsto \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix},$$

mit zugehöriger Permutationsdarstellung

$$\hat{\mu}:\ x \mapsto [(1,2,3),3],\ y \mapsto [(2,3),3].$$

1. $H = \mathrm{stab}_\mu(1) = \mathrm{stab}_{\hat{\mu}}(1) = \langle y \rangle$.
2. $T = (1, x, x^2)$.
3. $\lambda:\ y \mapsto \mu(y)_{1,1} = -1$.
4. $a_1(1) = 1$, $a_1(x) = 1/2$, $a_1(x^2) = 1/2$
   (Einträge $\neq 0$ in der ersten Zeile von $\mu(1),\ \mu(x),\ \mu(x^2)$).

Es gilt

$$\mu^{\mathrm{diag}(1,2,2)} = \lambda \uparrow_T \mathsf{S}_3.$$

∎

Zur Eindeutigkeit der Zerlegung beweisen wir den folgenden Satz.

1.28 Satz *Sei λ_i eine Darstellung von $H_i \leq G$ vom Grad 1 sowie T_i eine Transversale von $H_i \backslash G$ für $i = 1, 2$. Gilt*

$$\lambda_1 \uparrow_{T_1} G = \lambda_2 \uparrow_{T_2} G,$$

dann sind H_1 und H_2 konjugierte Untergruppen und $\lambda_1,\ \lambda_2$ innere konjugierte Darstellungen in G.

Beweis Sei $\mu = \lambda_1 \uparrow_{T_1} G = \lambda_2 \uparrow_{T_2} G$. Zunächst zeigen wir, daß H_1 Stabilisator eines Punktes unter μ ist. Sei $t \in T_1$ das Element $\in H_1$, etwa an Position i. Dann ist

$$x \in \mathrm{stab}_\mu(i) \Leftrightarrow txt^{-1} \in H_1 \Leftrightarrow x \in H_1,$$

also $H_1 = \mathrm{stab}_\mu(i)$. Entsprechend ist auch H_2 der Stabilisator eines Punktes unter μ. Da μ transitiv ist, folgt $H_1 = H_2^s$ für ein $s \in G$. Nach Satz 1.10 gilt $\mu = \lambda_2 \uparrow_{T_2} G = \lambda_2^s \uparrow_{s^{-1}T_2} G$, wobei λ_2^s eine Darstellung von H_1 ist. Wir betrachten wieder die Transversalenelemente $u \in T_1$ und $v \in s^{-1}T_2$, welche in H_1 liegen, o.B.d.A. an der gemeinsamen Position j. Dann gilt für $x \in H_1$

$$\lambda_1(uxu^{-1}) = \lambda_2^s(vxv^{-1}) \Leftrightarrow \lambda_1(x) = \lambda_2^s(x),$$

also sind λ_1 und λ_2 innere Konjugierte. ∎

Eine Erweiterung von Satz 1.28 werden wir später (Satz 1.53) beweisen. Um mit monomialen Darstellungen gut rechnen zu können, zerlegt man sie zunächst mit dem Algorithmus 1.26 in eine konjugierte Induktion. In dieser Gestalt ist die Darstellung dann besser zu handhaben, beispielsweise ermöglichen die Sätze aus dem letzten Abschnitt eine Anzahl von Manipulationen.

Zerlegung in ein äußeres Tensorprodukt In diesem Abschnitt wird ein notwendiges und hinreichendes Kriterium bewiesen, welches feststellt, ob eine monomiale Darstellung in ein konjugiertes, äußeres Tensorprodukt zerfällt. Ist dies der Fall, wird die Zerlegung konstruktiv durchgeführt. Das Kriterium wurde von Minkwitz gefunden und wird hier mit einem kürzeren Beweis präsentiert.

1.29 Satz *Sei μ eine transitive monomiale Darstellung einer Gruppe G und $G = N_1 \times N_2$ das direkte Produkt von N_1 und N_2. Der Stabilisator* $\mathrm{stab}_\mu(1)$ *der 1 unter μ heiße S. Dann ist μ äquivalent zu einem äußeren Tensorprodukt von zwei Darstellungen μ_1 von N_1 und μ_2 von N_2,*

$$\mu \cong \mu_1 \# \mu_2,$$

genau dann, wenn

$$|S| = |S \cap N_1| \cdot |S \cap N_2|.$$

Ist $\mu^D = \lambda \uparrow_T G$ mit einer Darstellung λ vom Grad 1 von S (siehe Satz 1.24), so ist in diesem Fall

$$\mu^{DM} = ((\lambda \downarrow S \cap N_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow S \cap N_2) \uparrow_{T_2} N_2),$$

wobei T_i eine Transversale von $(S \cap N_i)\backslash N_i$ bezeichnet für $i = 1, 2$ und M die monomiale Matrix ist, die zum Transversalenwechsel $T \to T_1T_2$ gehört (vgl. Satz 1.1).

Beweis Sei $\mu \cong \mu_1 \# \mu_2$ (notwendig sind μ_1 und μ_2 monomial) und $S = \mathrm{stab}_\mu(1)$. In dieser Situation ist $S_1 = \mathrm{stab}_{\mu_1}(1) = S \cap N_1$ (da $1^{\mu(x)} = 1$ und $x \in N_1 \Leftrightarrow 1^{\mu_1(x)} = 1$), analog $S_2 = \mathrm{stab}_{\mu_2}(1) = S \cap N_2$. Gradvergleich der Darstellungen ergibt

$$\begin{aligned} & \deg(\mu) = \deg(\mu_1) \cdot \deg(\mu_2) \\ \Leftrightarrow\ & |G|/|S| = |N_1|/|S \cap N_1| \cdot |N_2|/|S \cap N_2| \\ \Leftrightarrow\ & |S| = |S \cap N_1| \cdot |S \cap N_2|, \end{aligned}$$

was zu zeigen war.

Sei nun $S_i = S \cap N_i,\ i = 1, 2$ und $|S| = |S_1| \cdot |S_2|$. Wegen $S_i \trianglelefteq S,\ i = 1, 2$ und $S_1 \cap S_2 = \{1\}$ ist dann $S = S_1 \times S_2$ und damit

$$\begin{aligned} \lambda \uparrow_T G &= ((\lambda \downarrow S_1) \# (\lambda \downarrow S_2)) \uparrow_T G \\ &\cong ((\lambda \downarrow S_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow S_2) \uparrow_{T_2} N_2), \end{aligned}$$

wobei die erste Gleichheit gilt, da λ als irreduzible Darstellung vom Grad 1 eines direkten Produkts äußeres Tensorprodukt ist (siehe z. B. [25], S. 54). Die zweite Äquivalenz gilt wegen Satz 1.7. Ist weiterhin M die konjugierende Matrix zum Transversalenwechsel $T \to T_1T_2$, so gilt

$$\begin{aligned} \mu^{DM} &= \lambda \uparrow_{T_1T_2} G \\ &= ((\lambda \downarrow S_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow S_2) \uparrow_{T_2} N_2) \end{aligned}$$

nach Satz 1.7. ∎

Bevor wir fortfahren, geben wir ein Beispiel einer Permutationsdarstellung eines direkten Produkts an, die *nicht* in ein äußeres Tensorprodukt zerfällt.

1.30 Beispiel Wir betrachten die Gruppe $\mathsf{S}_3 = \langle x, y \mid x^3 = y^2 = 1, x^y = 1\rangle$. Eine treue, transitive Permutationsdarstellung ϕ von $\mathsf{S}_3 \times \mathsf{S}_3$ ist gegeben durch

$$\begin{aligned} \phi: \quad &(x,1) \mapsto [(1,5,4)(2,3,6),6], \; (y,1) \mapsto [(1,2)(3,4)(5,6),6], \\ &(1,x) \mapsto [(1,4,5)(2,3,6),6], \; (1,y) \mapsto [(1,2)(3,5)(4,6),6]. \end{aligned}$$

Würde ϕ in ein äußeres Tensorprodukt zerfallen, dann hätte einer der Faktoren einen Grad < 3. Da die Faktoren treue Darstellungen von S_3 sein müssen, ist das unmöglich. ∎

1.31 Korollar Ist ϕ eine reguläre Darstellung oder eine Darstellung vom Grad 1 von G, dann zerfällt ϕ in ein äußeres Tensorprodukt genauso wie G in ein direktes Produkt zerfällt.

Beweis ϕ regulär: In diesem Fall ist $|S| = 1$, so daß für beliebige N_1, N_2 mit $G = N_1 \times N_2$ die Bedingung $|S| = |S \cap N_1| \cdot |S \cap N_2|$ erfüllt ist.
$\deg(\phi) = 1$: In diesem Fall ist $S = G$ und mit $G = N_1 \times N_2$ ist die Bedingung aus Satz 1.29 erfüllt. ∎

Man beachte, daß sich dieser Satz nicht ohne weiteres auf Induktionen von Darstellungen beliebigen Grades verallgemeinern läßt, da an entscheidender Stelle benutzt wird, daß eine Darstellung von G vom Grad 1 irreduzibel ist. Ist außerdem G ein direktes Produkt, so ist diese Darstellung *gleich* einem äußerem Tensorprodukt. Diese haben notwendig wieder den Grad 1. Ein Ansatz zur Zerlegung einer Darstellung in ein äußeres Tensorprodukt über die Struktur der Bilder der Erzeuger von G wird in Egner/Püschel/Beth (1997), [27] behandelt, ist aber der hier vorgestellten Methode unterlegen.
Der Beweis des vorigen Satzes liefert auch den Algorithmus zur Zerlegung einer monomialen Darstellung in ein konjugiertes äußeres Tensorprodukt.

1.32 Algorithmus (Zerlegung in ein konjugiertes äußeres Tensorprodukt)
Sei μ eine transitive monomiale Darstellung von G gegeben. μ soll in ein konjugiertes äußeres Tensorprodukt zerlegt werden.

1. Zerlege $\mu^D = \lambda \uparrow_T G$ mit einer Darstellung λ vom Grad 1 von $S \leq G$ (Algorithmus 1.26).

2. Suche eine Zerlegung $G = N_1 \times N_2$ von G mit $|S| = |S \cap N_1| \cdot |S \cap N_2|$. Dazu wird der Normalteilerverband berechnet. Gibt es keine solche Zerlegung, dann ist μ kein konjugiertes äußeres Tensorprodukt.

3. Bestimme T_i als Transversale von $(S \cap N_i)\backslash N_i,\ i = 1, 2$ und die Matrix M zum Transversalenwechsel $T \to T_1 T_2$.

Es gilt

$$\mu^{DM} = ((\lambda \downarrow S \cap N_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow S \cap N_2) \uparrow_{T_2} N_2).$$

■

Abelsche Gruppen In diesem Abschnitt werden wir die transitiven monomialen Darstellungen abelscher Gruppen klassifizieren. Dazu wollen wir uns zunächst in Erinnerung rufen, wie die Darstellungen einer Gruppe G mit den Darstellungen einer Faktorgruppe G/N zusammenhängen.

1.33 Lemma Sei $N \trianglelefteq G$ ein Normalteiler. Dann entsprechen die Darstellungen von G/N genau den Darstellungen von G, für die N im Kern liegt.

Beweis Sei $\kappa: G \to G/N,\ g \mapsto gN$ der kanonische Homomorphismus. Ist ϕ eine Darstellung von G/N, so ist $\phi \circ \kappa$ eine Darstellung von G, die N im Kern enthält ($\phi \circ \kappa$ ist Homomorphismus und $x \in N \Rightarrow (\phi \circ \kappa)(x) = \phi(1 \cdot N) = \mathbf{1}_{\deg(\phi)}$). Ist umgekehrt ϕ eine Darstellung von G mit $N \leq \ker(\phi)$, so wird durch $gN \mapsto \phi(g)$ eine Darstellung von G/N (wohl-)definiert. ■

Wir werden im folgenden gelegentlich Darstellungen von G/N mit den zugehörigen Darstellungen von G identifizieren.
Die Darstellungstheorie abelscher Gruppen ist besonders einfach, da alle Irreduziblen den Grad 1 haben. Das führt dazu, daß jede Darstellung ϕ einer Untergruppe $H \leq G$ einer abelschen Gruppe G eine Erweiterung $\overline{\phi}$ auf G besitzt. Wie das konstruktiv geschieht, wird später in Algorithmus 1.74 erklärt.
Jetzt können wir die monomialen Darstellungen abelscher Gruppen klassifizieren.

1.34 Satz *Sei μ eine transitive monomiale Darstellung einer abelschen Gruppe G mit Zerlegung $\mu^D = \lambda \uparrow_T G$ gemäß Satz 1.24, wobei λ eine Darstellung von $N \leq G$ ist mit Erweiterung $\overline{\lambda}$ auf G. Dann gilt*

$$\mu^{DD_1} = \overline{\lambda} \cdot (1_N \uparrow_T G) \ \mathit{mit}\ D_1 = \mathrm{diag}(\overline{\lambda}(t) \mid t \in T)\ \mathit{und}\ \overline{\lambda} \downarrow N = \lambda,$$

insbesondere ist also μ äquivalent (bzgl. einer Diagonalmatrix) zum Produkt einer Darstellung vom Grad 1 und einer regulären Darstellung einer Faktorgruppe von G. Die irreduziblen Komponenten von μ sind also paarweise verschieden.

Beweis λ läßt sich zu einer Darstellung $\overline{\lambda}$ von G erweitern. Mit Satz 1.15 folgt

$$\mu^{DD_1} = (\lambda \uparrow_T G)^{D_1} = \left((\overline{\lambda} \downarrow N) \uparrow_T G\right)^{D_1} = (1_N \uparrow_T G) \otimes \overline{\lambda} = \overline{\lambda} \cdot (1_N \uparrow_T G).$$

Eine reguläre Darstellung einer abelschen Gruppe enthält paarweise verschiedene Irreduzible. ∎

Reguläre Darstellungen zerfallen nach Korollar 1.31 genau so in ein äußeres Tensorprodukt, wie die dargestellte Gruppe in ein direktes Produkt. Da sich eine abelsche Gruppe bereits anhand einer Kompositionsreihe in ein direktes Produkt zerlegen läßt, ist diese Zerlegung somit schnell durchführbar.

Primzahlgrad In diesem Abschnitt wollen wir die transitiven monomialen Darstellungen μ von Primzahlgrad $\deg(\mu) = p$ prim, charakterisieren. Dazu benötigen wir zunächst den folgenden Satz über transitive Permutationsgruppen von Primzahlgrad, der von Burnside gefunden wurde (siehe [24], S. 91 und 99).

1.35 Satz (Burnside) *Jede transitive Permutationsgruppe von Primzahlgrad p ist zweifach transitiv oder auflösbar mit einem regulären zyklischen p-Sylow-Normalteiler.*

1.36 Satz *Sei μ eine transitive monomiale Darstellung von G mit Grad* $\deg(\mu) = p$, *prim. μ sei nicht zweifach transitiv und habe die Zerlegung $\mu^D = \lambda_H \uparrow_T G$ mit einer Darstellung λ von $H \leq G$ vom Grad 1. Dann trifft genau einer der beiden folgenden Fälle ein:*

i) μ ist irreduzibel

ii) λ_H hat eine Erweiterung λ_G auf G, das heißt

$$\mu^{D \cdot D_1} = \lambda_G \cdot (1_H \uparrow_T G), \ \textit{mit}\ D_1 = \mathrm{diag}(\lambda_G(t) \mid t \in T).$$

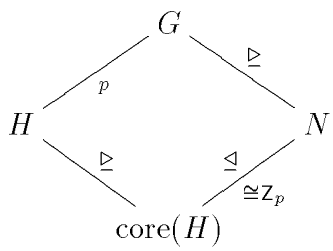

Abbildung 1.5: Situation in Satz 1.36

Beweis $1_H \uparrow G$ ist eine treue Permutationsdarstellung von $G/\operatorname{core}(H)$ (vgl. Satz 1.18) vom Grad p. Nach dem Satz von Burnside (1.35) gibt es einen Normalteiler N von G mit

$$\operatorname{core}(H) \overset{p}{\trianglelefteq} N \trianglelefteq G,$$

also $(N : \operatorname{core}(H)) = p$ (vgl. Abbildung 1.5) und wenn T_1 eine Transversale von $\operatorname{core}(H)\backslash N$ ist, gilt mit Korollar 1.14

$$(\lambda_H \uparrow_{T_1} G) \downarrow N = (\lambda_H \downarrow \operatorname{core}(H)) \uparrow_{T_1} N$$

und $(\lambda_H \uparrow_T G) = (\lambda_H \uparrow_{T_1} G)^M$ mit einer monomialen Matrix M. Sei $\lambda_{\operatorname{core}(H)} = \lambda_H \downarrow \operatorname{core}(H)$. Nach dem Satz von Clifford 1.71 (auf Seite 56) tritt genau einer der beiden folgenden Fälle ein:

1. $\lambda_{\operatorname{core}(H)}$ hat eine Erweiterung λ_N auf N. Dann hat auch λ_H eine Erweiterung λ_G auf G (Schreibe $g \in G$ als $g = ht$, $h \in H$, $t \in T_1$ und definiere $\lambda_G(ht) = \lambda_H(h)\lambda_N(t)$). Wegen Satz 1.15 gilt

$$(\lambda_H \uparrow_T G)^{D_1} = \lambda_G \cdot (1_H \uparrow_T G), \text{ mit } D_1 = \operatorname{diag}(\lambda_G(t) \mid t \in T).$$

2. $\lambda_{\operatorname{core}(H)} \uparrow_{T_1} N$ ist irreduzibel. Dann ist auch $\lambda_H \uparrow_{T_1} G$ als Erweiterung irreduzibel, also auch μ. ∎

M-Gruppen Es gibt Gruppen, bei denen jede Darstellung äquivalent zu einer monomialen Darstellung ist. In diesem Abschnitt wollen wir die wesentlichen Ergebnisse zur Klasse dieser Gruppen zusammenstellen. Wir folgen Huppert, [36], S. 578 ff.

1.37 Definition *Eine Gruppe G heißt M-Gruppe, wenn jede Darstellung von G äquivalent ist zu einer monomialen Darstellung.*

Offensichtlich ist eine Gruppe G genau dann eine M-Gruppe, wenn jede *irreduzible* Darstellung äquivalent ist zu einer monomialen Darstellung.
Die Klasse der M-Gruppen wird durch die folgenden beiden Sätze abgegrenzt.

1.38 Satz *i) Jede überauflösbare Gruppe ist eine M-Gruppe.*

ii) Jede nilpotente Gruppe ist eine M-Gruppe.

iii) Jede auflösbare Gruppe mit lauter abelschen Sylowgruppen ist eine M-Gruppe.

1.39 Satz *Jede M-Gruppe ist auflösbar.*

Damit eine auflösbare Gruppe der Ordnung n eine nicht-abelsche Sylowgruppe enthält, ist es notwendig, daß in n eine Primzahl zur dritten Potenz steckt; damit sie nicht nilpotent ist, muß n mindestens zwei verschiedene Primzahlen enthalten. Die kleinste Ordnung, die beides erfüllt, ist offensichtlich 24. Wir geben ein Beispiel für eine Gruppe der Ordnung 24 an, die keine M-Gruppe ist.

1.40 Beispiel Wir betrachten die Gruppe $\mathsf{SL}(2,3)$ der (2×2)-Matrizen über $\mathbb{F}_3$. Bezeichnet Q_8 die Quaternionengruppe, dann ist

$$\mathsf{SL}(2,3) \cong \mathsf{Z}_3 \ltimes \mathsf{Q}_8 \cong \langle r,s,t \mid r^3 = s^4 = t^4 = 1,\ s^t = s^{-1},\ t^r = st,\ s^r = t^{-1}\rangle.$$

Die Darstellung ρ gegeben durch

$$\rho:\ r \mapsto \frac{1}{2}\cdot \begin{bmatrix} -1+\mathrm{i} & -1-\mathrm{i} \\ 1-\mathrm{i} & -1-\mathrm{i} \end{bmatrix},\ t \mapsto \begin{bmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix},\ s \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

ist treu, irreduzibel und nicht ähnlich zu einer monomialen Darstellung. ∎

1.4 Die Erweiterungsformel von Minkwitz

Der Erweiterungssatz von Minkwitz (siehe [47]) erlaubt es, eine irreduzible Darstellung einer Untergruppe konstruktiv zu erweitern, falls dies möglich ist. Nötig dazu ist nur die Angabe eines Charakters einer erweiternden Darstellung.

1.41 Satz (Minkwitz' Erweiterungsformel) *Sei $H \le G$ eine Untergruppe und ρ eine irreduzible Darstellung von H vom Grad $\deg(\rho) = n$ mit Charakter χ. Es gebe einen Charakter $\overline{\chi}$ von G, der χ erweitert, das heißt $\overline{\chi} \downarrow H = \chi$. Dann ist durch*

$$\overline{\rho}:\ g \mapsto \frac{n}{|H|}\cdot \sum_{h\in H} \overline{\chi}(gh^{-1})\rho(h)$$

eine Darstellung $\overline{\rho}$ definiert, welche ρ auf G erweitert und den Charakter $\chi_{\overline{\rho}} = \overline{\chi}$ hat.

Der kürzeste Beweis wurde von Michael Clausen gefunden und findet sich in [15].

1.5 Intertwiningraum

Der Begriff des Intertwiningraumes wurde bereits in der Einleitung kurz erwähnt und soll hier definiert werden.

1.42 Definition *Seien ϕ, ψ Darstellungen einer Gruppe G über dem Körper $\mathbb{K}$ mit Graden $\deg(\phi) = n,\ \deg(\psi) = m$. Dann nennen wir den Vektorraum*

$$\mathsf{Int}(\phi,\psi) = \{A \in \mathbb{K}^{n\times m} \mid \forall g \in G:\ \phi(g)\cdot A = A\cdot \psi(g)\}$$

den „Intertwiningraum" von ϕ und ψ. Weiter definieren wir mit

$$\langle \phi, \psi \rangle = \dim(\mathsf{Int}(\phi, \psi))$$

die Dimension des Intertwiningraumes oder „Intertwiningzahl" von ϕ und ψ.

In der Strukturtheorie wird nur die Intertwiningzahl benötigt. Sie ist invariant unter Konjugation der Argumente und hängt somit nur von der Äquivalenzklasse der Darstellungen ab. Wir werden gleich sehen, daß die Intertwiningzahl zweier Darstellungen nichts anderes ist, als das Skalarprodukt der zugehörigen Charaktere, wie die obige Notation bereits suggeriert.
Die in diesem Kapitel angestrebte Konstruktivität verlangt auch hier mehr. Wir wollen nicht nur wissen, wie sich die Intertwining*zahl* unter Konjugation, direkter Summe, Induktion etc. der Argumente verändert, sondern untersuchen wie sich der Intertwining*raum* transformiert. Wie in Abschnitt 1.2 werden wir also bekannte Sätze konstruktiv verfeinern.
Dieser Abschnitt gliedert sich in zwei Teile: im ersten geben wir die bekannten Sätze über Intertwiningzahlen an, im zweiten werden diese zu konkreten Aussagen über Intertwiningräume erweitert.

Intertwiningzahl Die Schreibweise $\langle \phi, \psi \rangle$ als Skalarprodukt wird gerechtfertigt durch den folgenden Satz und folgt Clausen/Baum, [16].

1.43 Satz *Seien ϕ, ψ Darstellungen einer Gruppe G. Dann gilt:*

i) Sind ϕ und ψ irreduzibel, so ist

$$\langle \phi, \psi \rangle = \begin{cases} 1, & \phi \cong \psi \\ 0, & \phi \not\cong \psi \end{cases} .$$

ii) $\langle \phi, \psi \rangle = \langle \psi, \phi \rangle$.

iii) $\langle \phi_1 \oplus \phi_2, \psi \rangle = \langle \phi_1, \psi \rangle + \langle \phi_2, \psi \rangle$.

iv) $\langle \phi, \phi \rangle = 1 \Leftrightarrow \phi$ *ist irreduzibel.*

v) $\langle \phi, \psi \rangle = \langle \chi_\phi, \chi_\psi \rangle$.

Für den Beweis verweisen wir auf [21], S. 320/321.

Die Dimension des Intertwiningraumes zweier Darstellungen ist also nichts anderes als das wohlbekannte Skalarprodukt der zugehörigen Charaktere

$$\langle \chi_\phi, \chi_\psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\phi(g) \chi_\psi(g^{-1}),$$

womit sich eine Möglichkeit ergibt, die Intertwiningzahl auszurechnen. Man beachte, daß die Intertwiningzahl invariant ist unter Konjugation der Argumente. Zwei wichtige Sätze erlauben das Rechnen mit der Intertwiningzahl von Induktionen.

1.44 Satz (Frobenius-Reziprozität) *Sei $H \leq G$ eine Untergruppe, ϕ eine Darstellung von H und ψ eine Darstellung von G. Dann gilt*

$$\langle \phi \uparrow G, \psi \rangle = \langle \phi, \psi \downarrow H \rangle.$$

Zum Beweis siehe z. B. [25], S. 48 ff.

1.45 Satz (Intertwiningzahl-Satz) *Seien $H_1, H_2 \leq G$ zwei Untergruppen mit Darstellungen ϕ_1, ϕ_2. Sind $x, y \in G$ dann hängt die Intertwiningzahl*

$$\langle \phi_1^x \downarrow (H_1^x \cap H_2^y), \phi_2^y \downarrow (H_1^x \cap H_2^y) \rangle$$

nur ab von der Doppelnebenklasse $H_1 \cdot xy^{-1} \cdot H_2$. Ist S ein Vertretersystem der Doppelnebenklassen $H_1 \backslash G / H_2$, dann gilt

$$\langle \phi_1 \uparrow G, \phi_2 \uparrow G \rangle = \sum_{s \in S} \langle \phi_1^s \downarrow (H_1^s \cap H_2), \phi_2 \downarrow (H_1^s \cap H_2) \rangle.$$

Zum Beweis siehe [21], S. 327.

Aus dem Intertwiningzahl-Satz ergeben sich einige besonders einfache Formeln für Permutationsdarstellungen.

1.46 Korollar Sind π_1, π_2 zwei transitive Permutationsdarstellungen einer Gruppe G mit $H_i = \mathrm{stab}_{\pi_i}(1),\ i = 1, 2$, so ist

$$\langle \pi_1, \pi_2 \rangle = |H_1 \backslash G / H_2|.$$

Beweis Sei S ein Vertretersystem der Doppelnebenklassen $H_1 \backslash G / H_2$. Nach Korollar 1.25 ist $\pi_i = 1_{H_i} \uparrow G,\ i = 1, 2$ und damit

$$\begin{aligned} \langle \pi_1, \pi_2 \rangle &= \langle 1_{H_1} \uparrow G, 1_{H_2} \uparrow G \rangle \\ &= \sum_{s \in S} \langle 1_{H_1 \cap H_2^s}, 1_{H_1 \cap H_2^s} \rangle \\ &= |H_1 \backslash G / H_2| \end{aligned}$$

nach Satz 1.45, was zu zeigen war. ■

1.47 Korollar Ist π eine transitive Permutationsdarstellung einer Gruppe G, dann gilt:

i) $\langle \pi, 1_G \rangle = 1$.

ii) π ist irreduzibel $\Leftrightarrow \deg(\pi) = 1$.

iii) π ist zweifach transitiv $\Leftrightarrow \langle \pi, \pi \rangle = 2$, das heißt in diesem Fall ist $\pi \cong 1_G \oplus \rho$ mit einer irreduziblen Darstellung ρ.

Beweis Sei $\pi = 1_H \uparrow G$. Wegen $|H \backslash G/G| = 1$ und Korollar 1.46 folgt Behauptung i), Behauptung ii) folgt aus i). Ist π zweifach transitiv, dann gilt $|H \backslash G/H| = 2$ woraus wieder mit Korollar 1.46 iii) folgt. ∎

Intertwiningraum Zunächst ein paar einfache Aussagen, die als Erweiterung von Satz 1.43 betrachtet werden können.

1.48 Satz *Seien $\phi, \phi_1, \phi_2 \ldots, \psi, \psi_1, \psi_2 \ldots$ Darstellungen über $\mathbb{K}$ der Gruppe G mit Graden* $\deg(\phi) = n, \deg(\psi) = m$. *Dann gilt:*

i) Sind $A \in \mathsf{GL}_n(\mathbb{K}), B \in GL_m(\mathbb{K})$, so ist

$$\mathsf{Int}(\phi^A, \psi^B) = A^{-1} \cdot \mathsf{Int}(\phi, \psi) \cdot B.$$

ii)

$$\mathsf{Int}(\phi_1 \oplus \phi_2, \psi_1 \oplus \psi_2) = \left\{ \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} \mid A_{i,j} \in \mathsf{Int}(\phi_i, \psi_j) \right\}.$$

iii) (Schurs Lemma) Sind ϕ, ψ irreduzibel vom Grad n, so ist

$$\mathsf{Int}(\phi, \psi) = \begin{cases} \mathbb{K} \cdot A, \ \textit{für ein } A \in \mathsf{GL}_n(\mathbb{K}), & \phi \cong \psi \\ \mathbf{0}_n, & \phi \not\cong \psi \end{cases}.$$

iv) Sind $\phi = (\mathbf{1}_{n_1} \otimes \phi_1) \oplus \ldots \oplus (\mathbf{1}_{n_k} \otimes \phi_k)$ und $\psi = (\mathbf{1}_{m_1} \otimes \phi_1) \oplus \ldots \oplus (\mathbf{1}_{m_k} \otimes \phi_k)$ zwei vollständig zerlegte Darstellungen mit irreduziblen paarweise inäquivalenten ϕ_i, dann gilt

$$\mathsf{Int}(\phi, \psi) = (\mathbb{K}^{n_1 \times m_1} \otimes \mathbf{1}_{\deg(\phi_1)}) \oplus \ldots \oplus (\mathbb{K}^{n_k \times m_k} \otimes \mathbf{1}_{\deg(\phi_k)}).$$

Jede Matrix $\in \mathsf{Int}(\phi, \psi)$ ist also blockpermutiert bzgl. der homogenen Komponenten von ϕ und ψ.

Beweis i) und ii) bestätigt man durch Nachrechnen. Zu iii) seien ϕ, ψ irreduzibel vom Grad n. Verwende Satz 1.43 i): ist $\phi \not\cong \psi$, so $\langle \phi, \psi \rangle = 0$, also $\mathsf{Int}(\phi, \psi) = \{\mathbf{0}_n\}$, ist $\phi \cong \psi$, so existiert eine invertierbare Matrix A mit $\phi^A = \psi$, welche wegen $\langle \phi, \psi \rangle = 1$ den Intertwiningraum erzeugt. iv) folgt aus ii) und iii). ∎

1.49 Beispiel Wir betrachten die Gruppe $\mathsf{Z}_4 = \langle x \mid x^4 = 1 \rangle$, mit den Darstellungen vom Grad 1: $\lambda_k : \ x \mapsto \omega_4^k, \ k = 0 \dots 3$, und der regulären Darstellung $\phi : \ x \mapsto [(1,2,3,4),4]$. Dann ist

$$\mathsf{Int}(\lambda_k, \lambda_\ell) = \langle \delta_{k,\ell} \rangle, \ \mathsf{Int}(\lambda_1, \phi) = \langle [1, -\omega_4, -1, \omega_4] \rangle$$

sowie

$$\mathsf{Int}(\phi,\phi) = \langle \begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{bmatrix}, \begin{bmatrix} 0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0 \end{bmatrix}, \begin{bmatrix} 0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0 \end{bmatrix}, \begin{bmatrix} 0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0 \end{bmatrix} \rangle$$

der Vektorraum der zirkulanten Matrizen, und wenn $\rho = \lambda_0 \oplus \lambda_1 \oplus \lambda_2 \oplus \lambda_3$ bezeichnet, so ist

$$\mathsf{Int}(\phi,\rho) = \langle \begin{bmatrix} 1&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0 \end{bmatrix}, \begin{bmatrix} 0&1&0&0\\0&\omega_4&0&0\\0&-1&0&0\\0&-\omega_4&0&0 \end{bmatrix}, \begin{bmatrix} 0&0&1&0\\0&0&-1&0\\0&0&1&0\\0&0&-1&0 \end{bmatrix}, \begin{bmatrix} 0&0&0&1\\0&0&0&-\omega_4\\0&0&0&-1\\0&0&0&\omega_4 \end{bmatrix} \rangle$$

der Raum, in dem auch die DFT_4 liegt als Summe der Basiselemente. ■

Für unsere Zwecke besonders interessant sind die Intertwiningräume von monomialen Darstellungen, was wir mit Satz 1.48 i) und ii) auf die Frage nach Intertwiningräumen von Induktionen eindimensionaler Darstellungen reduzieren können. Wir werden dazu im folgenden konstruktive Varianten der Frobenius-Reziprozität und des Intertwiningzahl-Satzes beweisen.

1.50 Satz (Frobenius-Reziprozität) *Es sei $H \leq G$ eine Untergruppe vom Index n mit Transversale $T = (t_1, \dots, t_n)$ sowie ϕ eine Darstellung von G und ψ eine von H. Weiter sei $t_i^{-1} = h_i t_{i'}$, $i = 1 \dots n$. Dann ist*

$$\Phi : \begin{cases} \mathsf{Int}(\phi \downarrow H, \psi) & \rightarrow \ \mathsf{Int}(\phi, \psi \uparrow_T G) \\ \qquad A & \mapsto \ [A_1, \dots, A_n] \end{cases}, \ \textit{mit } A_{i'} = \phi(t_i) \cdot A \cdot \psi(h_i)$$

ein Vektorraumisomorphismus.

Beweis Zunächst eine Vorbemerkung. Sind ϕ_1, ϕ_2 Darstellungen (über $\mathbb{K}$) mit Graden n_1, n_2 derselben Gruppe G, dann operiert G von links auf dem Vektorraum $\mathbb{K}^{n_1 \times n_2}$ durch

$$g \bullet M = \phi_1(g) \cdot M \cdot \phi_2(g^{-1}), \ g \in G, \ M \in \mathbb{K}^{n_1 \times n_2}.$$

Die Frage nach einer Matrix M aus dem Intertwiningraum $\mathsf{Int}(\phi_1, \phi_2)$ ist damit äquivalent zur Frage nach unter G bzgl. der Operation $\bullet$ invarianten Matrizen . Zum Beweis von Satz 1.50 sei nun $d = \deg(\phi), e = \deg(\psi)$ und t_j das Transversalenelement $\in H$. Zu einer Matrix $A \in \mathsf{Int}(\phi \downarrow H, \psi) \leq \mathbb{K}^{d \times e}$ definieren wir die Matrix $\overline{A} \in \mathbb{K}^{d \times en}$ durch

$$\overline{A} = [\mathbf{0}_{d\times e}, \dots, \mathbf{0}_{d\times e}, \underset{j}{A \cdot \psi(t_j^{-1})}, \mathbf{0}_{d\times e}, \dots, \mathbf{0}_{d\times e}].$$

Wir zeigen nun, daß $\overline{A} \in \mathsf{Int}(\phi \downarrow H, (\psi \uparrow_T G) \downarrow H)$. Sei $h \in H$. Zur Berechnung von $\overline{A} \cdot (\psi \uparrow_T G)(h)$ genügt es, die j-te Blockzeile von $(\psi \uparrow_T G)(h)$ zu kennen. Diese Blockzeile enthält in der j-ten Blockspalte die Matrix $\psi(t_j h t_j^{-1})$, sonst die Nullmatrix. Wegen $A \cdot \psi(t_j^{-1}) \cdot \psi(t_j h t_j^{-1}) = \phi(h) \cdot A \cdot \psi(t_j^{-1})$ folgt die Behauptung. Anders ausgedrückt ist $\overline{A}$ eine Invariante unter H bzgl. $\bullet$. Um aus $\overline{A}$ eine Invariante unter G, das heißt ein Element $B \in \mathsf{Int}(\phi, \psi \uparrow_T G)$ zu konstruieren, verwenden wir den Reynoldsoperator (siehe z. B. [59]), das heißt wir summieren die Bilder von $\overline{A}$ unter den Nebenklassenvertretern:

$$B = \sum_{i=1}^{n} t_i \bullet \overline{A} = \sum_{i=1}^{n} \phi(t_i) \cdot \overline{A} \cdot (\psi \uparrow_T G)(t_i^{-1}).$$

Um das Produkt $\overline{A} \cdot (\psi \uparrow_T G)(t_i^{-1})$ zu bestimmen, genügt es wieder, die j-te Blockzeile von $(\psi \uparrow_T G)(t_i^{-1})$ zu kennen. Wir verwenden $t_i^{-1} = h_i t_{i'}$ und erhalten

$$t_j t_i^{-1} t_\ell^{-1} \in H \Leftrightarrow t_j h_i t_{i'} t_\ell^{-1} \in H \Leftrightarrow \ell = i'$$

und $\psi(t_j t_i^{-1} t_{i'}^{-1}) = \psi(t_j h_i)$. Es ergibt sich

$$\overline{A} \cdot (\psi \uparrow_T G)(t_i^{-1}) = [\mathbf{0}_{d\times e}, \ldots, \mathbf{0}_{d\times e}, \underset{i'}{A \cdot \psi(h_i)}, \mathbf{0}_{d\times e}, \ldots, \mathbf{0}_{d\times e}],$$

woraus folgt, daß $B = [A_1, \ldots, A_n]$ ist, mit $A_{i'} = \phi(t_i) \cdot A \cdot \psi(h_i)$. Man überzeugt sich leicht, daß die so erhaltende Abbildung Φ einen Vektorraumisomorphismus definiert. ∎

Der folgende Satz ist die konstruktive Erweiterung des Intertwiningzahl-Satzes, 1.45.

1.51 Satz *Es seien $H, K \leq G$ Untergruppen vom Index n bzw. m mit Transversalen $T = (t_1, \ldots, t_n)$ bzw. $S = (s_1, \ldots, s_m)$ und Darstellungen ϕ bzw. ψ der Grade $d = \deg(\phi)$ und $e = \deg(\psi)$. Es gilt:*

i) $H \cdot t_i s_j^{-1} \cdot K = H \cdot t_k s_\ell^{-1} \cdot K \Leftrightarrow \exists g \in G: \; H t_i g = H t_k$ *und* $K s_j g = K s_\ell$.

ii) Durch

$$\Phi_{k,\ell} : \begin{cases} \mathsf{Int}(\phi^{t_k} \downarrow (H^{t_k} \cap K^{s_\ell}), \psi^{s_\ell} \downarrow (H^{t_k} \cap K^{s_\ell})) & \rightarrow \mathsf{Int}(\phi \uparrow_T G, \psi \uparrow_S G) \\ A & \mapsto [A_{i,j}]_{1 \leq i \leq n,\ 1 \leq j \leq m} \end{cases}$$

mit

$$A_{i,j} = \begin{cases} \phi(t_i g t_k^{-1}) \cdot A \cdot \psi(s_\ell g^{-1} s_j^{-1}), & H \cdot t_i s_j^{-1} \cdot K = H \cdot t_k s_\ell^{-1} \cdot K, \\ & g \text{ wie in i) definiert} \\ \mathbf{0}_{d\times e}, & \text{sonst} \end{cases}$$

wird ein injektiver Vektorraumhomomorphismus definiert.

iii) *Das Bild von $\Phi_{k,\ell}$ hängt nur ab von der Doppelnebenklasse $D = H \cdot t_k s_\ell^{-1} \cdot K$ und wird bezeichnet mit V_D. Es gilt*

$$\mathsf{Int}(\phi \uparrow_T G, \psi \uparrow_S G) = \bigoplus_{D \in H \backslash G / K} V_D \quad \textit{(direkte Summe von Vektorräumen).}$$

Beweis Zunächst zeigen wir i):

$$\begin{aligned} H \cdot t_i s_j^{-1} \cdot K = H \cdot t_k s_\ell^{-1} \cdot K \quad &\Leftrightarrow \quad H \cap t_i s_j^{-1} \cdot K \cdot (t_k s_\ell^{-1})^{-1} \neq \emptyset \\ &\Leftrightarrow \quad t_i^{-1} H t_k \cap s_j^{-1} K s_\ell \neq \emptyset \\ &\Leftrightarrow \quad \exists g \in G: \ t_i g t_k^{-1} \in H \text{ und } s_j g s_\ell^{-1} \in K \\ &\Leftrightarrow \quad \exists g \in G: \ H t_i g = H t_k \text{ und } K s_j g = K s_\ell. \end{aligned}$$

Um ii) zu zeigen definieren wir zu $A \in \mathsf{Int}(\phi^{t_k} \downarrow (H^{t_k} \cap K^{s_\ell}), \psi^{s_\ell} \downarrow (H^{t_k} \cap K^{s_\ell}))$ die Matrix $B = [B_{i,j}]$ durch $B_{k,\ell} = A,\ B_{i,j} = \mathbf{0}_{d\times e}$ sonst. Dann gilt $(\phi \uparrow_T G)(h) \cdot B = B \cdot (\psi \uparrow_S G)(h)$ für alle $h \in (H^{t_k} \cap K^{s_\ell})$. Anders ausgedrückt ist B invariant unter $(H^{t_k} \cap K^{s_\ell})$ bzgl. der Operation

$$g \bullet M = (\phi \uparrow_T G)(g) \cdot M \cdot (\psi \uparrow_S G)(g^{-1}),\ g \in G,\ M \in \mathbb{K}^{dn \times em}.$$

Genau wie im Beweis von Satz 1.50 erhalten wir eine Invariante unter ganz G durch Summation über ein Vertretersystem R der Nebenklassen $(H^{t_k} \cap K^{s_\ell}) \backslash G$:

$$C = \sum_{r \in R} r \bullet B.$$

Die Nebenklassen entsprechen bijektiv den Paaren (i,j), für die $H \cdot t_i s_j^{-1} \cdot K = H \cdot t_k s_\ell^{-1} \cdot K$ ist, denn G operiert auf Paaren (Ht_i, Ks_j) von Nebenklassen durch Rechtsmultiplikation $(Ht_i, Ks_j) \cdot g = (Ht_i g, Ks_j g)$. Die Fixgruppe von (Ht_i, Ks_j) ist genau $H^{t_i} \cap K^{s_j}$ und nach i) liegen zwei Paare von Nebenklassen in derselben Bahn genau dann, wenn die Quotienten der Vertreter in der gleichen Doppelnebenklasse liegen. Die Matrix C enthält somit an der Stelle (i,j) einen Block $\neq \mathbf{0}_{d\times e}$ genau dann, wenn $H \cdot t_i s_j^{-1} \cdot K = H \cdot t_k s_\ell^{-1} \cdot K$ (und $A \neq \mathbf{0}_{d\times e}$). Sei nun für ein (i,j) diese Bedingung erfüllt und $r \in G$ so, daß $Ht_i r = Ht_k$ und $Ks_j r = Ks_\ell$. Um den Block $A_{i,j}$ von C an der Stelle (i,j) zu berechnen, genügt es die k-te Blockspalte von $(\phi \uparrow_T G)(r)$ und die ℓ-te Blockzeile von $(\psi \uparrow_S G)(r^{-1})$ zu kennen. Wegen $t_i r t_k^{-1} \in H$ und $s_\ell r^{-1} s_j^{-1} \in K$ hat $A_{i,j}$ die gewünschte Gestalt. Tatsächlich gilt $A_{i,j} \in \mathsf{Int}(\phi^{t_i} \downarrow (H^{t_i} \cap K^{s_j}), \psi^{s_j} \downarrow (H^{t_i} \cap K^{s_j}))$, denn ist C irgendeine Invariante unter G bzgl. $\bullet$, dann erfüllt insbesondere für $h \in (H^{t_i} \cap K^{s_j})$ der Block $A_{i,j}$ an der Stelle (i,j) die Bedingung $\phi(t_i h t_i^{-1}) \cdot A_{i,j} \cdot \psi(s_j h^{-1} s_j^{-1})$. Ist also C eine Invariante unter G bzgl. $\bullet$ und der Block an einer Stelle (k,ℓ) gegeben, dann sind die Blöcke an den Stellen (i,j) mit $H \cdot t_i s_j^{-1} \cdot K = H \cdot t_k s_\ell^{-1} \cdot K$ eindeutig bestimmt. Daraus folgt, daß das Bild der Abbildung $\Phi_{k,\ell}$ nur von der Doppelnebenklasse $H \cdot t_k s_\ell^{-1} \cdot K$ abhängt. Weiter sieht man leicht ein, daß

$\Phi_{k,\ell}$ einen injektiven Vektorraumhomomorphismus definiert. Offensichtlich ist die Summe der Bilder

$$\bigoplus_{D \in H\backslash G/K} V_D \leq \mathsf{Int}(\phi \uparrow_T G, \psi \uparrow_S G)$$

direkt, denn sind $\Phi_{k,\ell}$, $\Phi_{k',\ell'}$ zwei Homomorphismen zu unterschiedlichen Doppelnebenklassen mit Bildmatrizen A_1 bzw. A_2, dann gibt es keine Position, an der A_1 *und* A_2 einen Eintrag $\neq 0$ besitzen. Dimensionsvergleich (Intertwiningzahl-Satz 1.45) zeigt Gleichheit. ∎

Dieser sehr technische Satz erlaubt es uns, einige interessante Folgerungen für monomiale Darstellungen zu beweisen.
Es seien $\mu_1 = \lambda_H \uparrow_T G$ und $\mu_2 = \lambda_K \uparrow_S G$ zwei transitive monomiale Darstellungen, $\deg(\lambda_H) = \deg(\lambda_K) = 1$. Es sei $T = (t_1, \ldots, t_n)$ und $S = (s_1, \ldots, s_m)$. Mit Satz 1.51 können wir uns eine Basis von $\mathsf{Int}(\mu_1, \mu_2)$ beschaffen. Wir wählen dazu aus den Quotienten $t_i s_j^{-1}$, $i = 1 \ldots n$, $j = 1 \ldots m$, ein Vertretersystem der Doppelnebenklassen $H\backslash G/K$. Ein solches finden wir bereits unter den Quotienten $t_1 s_j^{-1}$, $j = 1 \ldots m$ (verwende Satz 1.51, i), mit $g = t_1 t_i^{-1}$), beispielsweise $t_1 s_{j_1}^{-1}, \ldots, t_1 s_{j_d}^{-1}$, $d = |H\backslash G/K|$. Für jeden Quotienten $t_1 s_{j_r}^{-1}$ gibt es nun zwei Möglichkeiten:

1. $\langle \lambda_H^{t_1} \downarrow (H^{t_1} \cap K^{s_{j_r}}), \lambda_K^{s_{j_r}} \downarrow (H^{t_1} \cap K^{s_{j_r}}) \rangle = 0$. In diesem Fall trägt die Doppelnebenklasse $H \cdot t_1 s_{j_r}^{-1} \cdot K$ nichts zum Intertwiningraum $\mathsf{Int}(\mu_1, \mu_2)$ bei.

2. $\langle \lambda_H^{t_1} \downarrow (H^{t_1} \cap K^{s_{j_r}}), \lambda_K^{s_{j_r}} \downarrow (H^{t_1} \cap K^{s_{j_r}}) \rangle = 1$, das heißt der zugehörige Intertwiningraum wird erzeugt von der (1×1)-Matrix $[1]$. Der zugehörige Basisvektor $\Phi_{1,j_r}(1)$ von $\mathsf{Int}(\mu_1, \mu_2)$ ist dann gegeben durch

$$\begin{array}{rcl} \Phi_{1,j_r}(1) & = & [a_{k,\ell} \mid k \in \{1, \ldots, n\},\ \ell \in \{1, \ldots, m\}], \text{ wobei} \\ a_{k,\ell} & = & \begin{cases} \lambda_H(t_k g t_1^{-1}) \cdot \lambda_K(s_{j_r} g^{-1} s_\ell^{-1}), & Ht_i g = Ht_1 \text{ und} \\ & Ks_\ell g = Ks_{j_r} \\ 0, & \text{sonst} \end{cases} . \end{array}$$

Auf diese Weise erhalten wir eine Basis $B = \{B_1, \ldots, B_e\}$ von $\mathsf{Int}(\mu_1, \mu_2)$ der Länge $e \leq d$. Ist $\mu_1' = \mu^{D_1}$ und $\mu_2' = \mu^{D_2}$ mit Diagonalmatrizen D_1, D_2 (was dem allgemeinen Fall transitiver monomialer Darstellungen entspricht), dann ist nach Satz 1.48, i), $B = \{D_1^{-1} B_1 D_2, \ldots, D_1^{-1} B_e D_2\}$ eine Basis von $\mathsf{Int}(\mu_1', \mu_2')$. B hat die folgenden Eigenschaften.

1.52 Lemma Seien μ_1, μ_2 zwei transitive monomiale Darstellungen der Gruppe G mit Zerlegungen $\mu_1 = (\lambda_H \uparrow_T G)^{D_1}$ und $\mu_2 = (\lambda_K \uparrow_S G)^{D_2}$. Es sei $T = (t_1, \ldots, t_n)$ und $S = (s_1, \ldots, s_m)$. D_1, D_2 sind Diagonalmatrizen. Die wie oben konstruierte Basis $B = \{B_1, \ldots, B_e\}$ von $\mathsf{Int}(\mu_1, \mu_2)$ hat die folgenden Eigenschaften:

i) Ist $i \neq j$, dann gibt es keine Stelle, an der B_i *und* B_j einen Eintrag $\neq 0$ besitzen.

ii) Die Basis B ist durch Eigenschaft i) bis auf skalare Multiplikation ihrer Elemente eindeutig bestimmt.

iii) Besitzt die Matrix B_i an der Stelle (k, ℓ) einen Eintrag $\neq 0$, dann besitzt sie in jeder Zeile genau $(H^{t_k} : (H^{t_k} \cap K^{s_\ell}))$ und in jeder Spalte genau $(K^{s_\ell} : (H^{t_k} \cap K^{s_\ell}))$ Einträge $\neq 0$.

Beweis Eigenschaft i) folgt aus der Konstruktion. Da jede andere Basis von $\mathsf{Int}(\mu_1, \mu_2)$ linear kombinierbar in B ist, folgt ii). Zu iii) zeigen wir

$$\begin{aligned}
& B_i \text{ hat Einträge} \neq 0 \text{ an den Stellen } (k,\ell),\ (k,\ell') \\
\Leftrightarrow\ & H \cdot t_k s_\ell^{-1} \cdot K = H \cdot t_k s_{\ell'}^{-1} \cdot K \\
\Leftrightarrow\ & H \cdot t_{k'} \underbrace{t_{k'}^{-1} t_k s_\ell^{-1} K}_{=s_{\ell_1} K} = H \cdot t_{k'} \underbrace{t_{k'}^{-1} t_k s_{\ell'}^{-1} K}_{=s_{\ell'_1} K} \\
\Leftrightarrow\ & B_i \text{ hat Einträge} \neq 0 \text{ an den Stellen } (k',\ell_1), (k',\ell'_1).
\end{aligned}$$

Da die Multiplikation von links mit $t_{k'}^{-1} t_k$ die Nebenklassen G/K permutiert, enthält B_i in jeder Zeile gleich viele Einträge $\neq 0$. Ein analoger Schluß zeigt, das B_i auch in jeder Spalte gleich viele Einträge $\neq 0$ besitzt. Enthält B_i an der Stelle (k, ℓ) einen Eintrag $\neq 0$, dann enthält B_i insgesamt $(G : (H^{t_k} \cap K^{s_\ell}))$ Einträge $\neq 0$ (folgt aus dem Beweis von Satz 1.45). Da B_i eine Matrix mit $n = (G : H) = (G : H^{t_k})$ Zeilen und $m = (G : K) = (G : K^{s_\ell})$ Spalten ist, folgen die Anzahlformeln. ∎

Im Falle von zwei transitiven Permutationsdarstellungen $\mu_1 = 1_H \uparrow G$ und $\mu_2 = 1_K \uparrow G$ läßt sich mit Hilfe von Lemma 1.52 eine Verbindung zur Designtheorie aufzeigen. In diesem Fall hat die Basis B die Länge $e = d = |H \backslash G / K|$ und die Einträge $\neq 0$ in den Basisvektoren sind alle $= 1$, wodurch B eindeutig bestimmt ist. Die Summe der Basisvektoren ist die All-One-Matrix. Lemma 1.52, iii) besagt, daß jeder Basisvektor ein Design beschreibt. Zum Begriff des Designs siehe die Standardwerke von Beth/Jungnickel/Lenz (1985), [9], Buekenhout (1995), [11] und Colbourn (1996), [17].
Das Verständnis für die Struktur der Basis B ist wichtig für den Beweis des folgenden Satzes.

1.53 Satz *Es seien $\mu_1 = (\lambda_H \uparrow_T G)^{D_1} \cong \mu_2 = (\lambda_K \uparrow_S G)^{D_2}$ zwei ähnliche monomiale Darstellungen. Dann gibt es eine monomiale Matrix M mit $\mu_1^M = \mu_2$ genau dann, wenn H und K in G konjugiert sind und λ_H und λ_K innere Konjugierte in G sind.*

Beweis Seien H und K konjugiert in G und $\lambda_K = \lambda_H^g$. Dann gilt

$$\mu_2 = (\lambda_K \uparrow_S G)^{D_2} = (\lambda_H^g \uparrow_S G)^{D_2} = (\lambda_H \uparrow_{gS} G)^{D_2}$$

nach Satz 1.10. Der Übergang von $\mu_2^{D_2^{-1}}$ zu $\mu_1^{D_1^{-1}}$ läßt sich also durch einen Transversalenwechsel erreichen, woraus mit Satz 1.1 die Behauptung folgt.
Für die andere Richtung enthalte der Intertwiningraum $\mathsf{Int}(\mu_1, \mu_2)$ eine monomiale Matrix. Nach Lemma 1.52 enthält dann bereits die oben konstruierte Basis B eine monomiale Matrix M. Abzählen der Einträge $\neq 0$ mit Lemma 1.52, iii), liefert $(H^{t_k} : (H^{t_k} \cap K^{s_\ell})) = (K^{s_\ell} : (H^{t_k} \cap K^{s_\ell})) = 1$, also $H^{t_k} = K^{s_\ell}$ und H und K sind konjugiert in G. Außerdem gilt $\lambda^{t_k} \downarrow (H^{t_k} \cap K^{s_\ell}) = \lambda^{s_\ell} \downarrow (H^{t_k} \cap K^{s_\ell})$, also sind λ_H und λ_K innere Konjugierte, was zu zeigen war. ∎

Für Permutationsdarstellungen folgt sofort das folgende Korollar.

1.54 Korollar Es seien $\pi_1 = (1_H \uparrow_T G) \cong \pi_2 = (1_K \uparrow_S G)$ zwei äquivalente Permutationsdarstellungen. Dann gibt es eine Permutationsmatrix P mit $\pi_1^P = \pi_2$ genau dann, wenn H und K in G konjugiert sind.

Wir geben nun ein Beispiel an für zwei äquivalente Permutationsdarstellungen, die nicht durch Konjugation mit einer Permutationsmatrix auseinander hervorgehen.

1.55 Beispiel Wir betrachten die einfache Gruppe $\mathsf{PSL}(3,2) = \langle x, y \mid x^2 = y^3 = (xy)^7 = 1 \rangle$ der Größe 168 mit den beiden zweifach transitiven Permutationsdarstellungen

$$\pi_1 : \; x \mapsto [(4,5)(6,7),7], \;\; y \mapsto [(1,2,4)(3,6,5),7],$$

und

$$\pi_2 : \; x \mapsto [(1,2)(3,5),7], \;\; y \mapsto [(1,4,7)(2,3,6),7].$$

Es gilt $\pi_1 \cong \pi_2$, $\langle \pi_1, \pi_2 \rangle = 2$ und $\mathsf{Int}(\pi_1, \pi_2) = \langle M_1, M_2 \rangle$ mit

$$M_1 = \begin{bmatrix} 1&1&1&0&1&0&0 \\ 0&0&1&1&1&1&0 \\ 1&1&0&1&0&1&0 \\ 0&1&0&0&1&1&1 \\ 1&0&1&0&0&1&1 \\ 0&1&1&1&0&0&1 \\ 1&0&0&1&1&0&1 \end{bmatrix}, \; M_2 = \begin{bmatrix} 0&0&0&1&0&1&1 \\ 1&1&0&0&0&0&1 \\ 0&0&1&0&1&0&1 \\ 1&0&1&1&0&0&0 \\ 0&1&0&1&1&0&0 \\ 1&0&0&0&1&1&0 \\ 0&1&1&0&0&1&0 \end{bmatrix}.$$

M_1 und M_2 beschreiben zwei komplementäre 2-Designs, welche die kleinste projektive Geometrie, die sogenannte *Fano-Ebene*, beschreiben. In $\mathsf{Int}(\pi_1, \pi_2)$ liegt offenbar keine Permutationsmatrix. ∎

Die Berechnung des Intertwiningraumes im allgemeinen Fall ist aufwendig, spielt aber eine wichtige Rolle in der konstruktiven Darstellungstheorie, zum Beispiel ermöglicht sie die Angabe einer konjugierenden Matrix zu zwei beliebigen äquivalenten Matrixdarstellungen. Die Berechnung erfordert das Lösen eines linearen Gleichungssystems.
Seien ϕ, ψ Darstellungen derselben Gruppe $G = \langle g_1, \ldots, g_n \rangle$. Eine Matrix $A = [a_{i,j}]$ liegt offenbar genau dann in $\mathsf{Int}(\phi, \psi) \subset \mathbb{K}^{\deg(\phi) \times \deg(\psi)}$, wenn die Gleichungen

$$\phi(g_i) \cdot A = A \cdot \psi(g_i) \Leftrightarrow \phi(g_i) \cdot A - A \cdot \psi(g_i) = \mathbf{0}_{\deg(\phi), \deg(\psi)}, \ \ i = 1 \ldots n,$$

erfüllt sind. Für jeden Erzeuger g erhalten wir somit die folgenden $\deg(\phi) \cdot \deg(\psi)$ Gleichungen in ebenso vielen Unbekannten

$$\sum_{i=1}^{\deg(\phi)} \phi(g)_{k,i} \cdot a_{i,\ell} - \sum_{j=1}^{\deg(\psi)} a_{k,j} \cdot \psi(g)_{j,\ell}, \ \ k = 1 \ldots \deg(\phi), \ \ \ell = 1 \ldots \deg(\psi).$$

Das halten wir in dem folgenden Satz fest.

1.56 Satz *Der Intertwiningraum von zwei Darstellungen ϕ, ψ der Gruppe G, welche erzeugt wird von $\{g_1, \ldots, g_n\}$, läßt sich berechnen durch Lösen eines linearen Gleichungssystem mit $n \cdot \deg(\phi) \cdot \deg(\psi)$ Gleichungen in $\deg(\phi) \cdot \deg(\psi)$ Unbekannten.*

Sind die Darstellungen ϕ, ψ monomial, so ist das Gleichungssystem dünn besetzt.

1.6 Zerlegungsmatrizen

Als Zerlegungsmatrix einer Darstellung ϕ einer Gruppe G bezeichnen wir jede Matrix A, welche ϕ in eine direkte Summe irreduzibler Darstellungen zerlegt, das heißt

$$\phi^A = (x \mapsto A^{-1} \cdot \phi(x) \cdot A) = \bigoplus_{i=1}^{n} \rho_i, \ \ \rho_i \text{ irreduzibel für } i = 1 \ldots n.$$

In der Literatur über Darstellungstheorie spielen Zerlegungsmatrizen keine Rolle, ihre bloße Existenz ist ausreichend für die dortigen Zwecke. In dieser Arbeit sind sie jedoch von zentraler Bedeutung. Zum einen werden sie benötigt, um Darstellungen konstruktiv zerlegen zu können: eine Funktion, die eine monomiale Darstellung ϕ zerlegt sollte nicht nur die ρ_i liefern, sondern eine Darstellung, welche identisch zu ϕ ist und lediglich eine andere Struktur besitzt, nämlich $(\rho_1 \oplus \ldots \oplus \rho_n)^{A^{-1}}$. Zum anderen sind Zerlegungsmatrizen wichtigster Baustein bei der Zerlegung von Matrizen mit Symmetrie (siehe Einleitung).
In diesem Abschnitt soll ein Stück weit eine Theorie der Zerlegungsmatrizen für monomiale Darstellungen entwickelt werden. Da monomiale Darstellungen im wesentlichen direkte Summen von Induktionen sind (vgl. die Sätze 1.22, 1.24), wird

die Induktion hierbei wieder eine zentrale Rolle spielen. Unter anderem wird ein Satz präsentiert, der es erlaubt, aus einer Zerlegungsmatrix einer Darstellung ϕ eines Normalteilers $N \trianglelefteq G$ von Primzahlindex eine Zerlegungsmatrix der Induktion $\phi \uparrow G$ zu konstruieren. Damit wird es beispielsweise möglich sein, reguläre Darstellungen auflösbarer Gruppen im obigen Sinne zu zerlegen. Der Algorithmus in Kapitel 2 verwendet im wesentlichen die Ergebnisse dieses Abschnitts. Es sei noch einmal daran erinnert, daß wir ausschließlich Darstellungen mit Maschke-Bedingung betrachten. Der Begriff der Zerlegungsmatrix, wie er am Anfang dieses Abschnitts eingeführt wurde, läßt sich in der Sprechweise der Intertwiningräume neu definieren.

1.57 Definition *Sei ϕ eine Darstellung einer Gruppe G und ρ eine beliebige Zerlegung von ϕ in Irreduzible ρ_i, das heißt $\phi \cong \rho = \bigoplus_{i=1}^{n} \rho_i$. Dann heißt jede invertierbare Matrix $A \in \mathsf{Int}(\phi, \rho)$ eine „Zerlegungsmatrix" für ϕ. Wir schreiben auch*

$$\phi \xrightarrow[\text{dec}]{A} \rho.$$

Ist ϕ die reguläre Darstellung von G, so nennen wir $A = \mathrm{DFT}_G$ eine „Diskrete Fouriertransformation" zu G.

Die Definition ist nicht ganz sauber, da die reguläre Darstellung einer Gruppe nur bis auf Konjugation mit einer Permutation bestimmt ist (die Transversale besteht aus den Elementen von G in irgendeiner Reihenfolge), also müßte es eigentlich DFT_ϕ heißen. Wir werden hier davon ausgehen, daß immer eine konkrete reguläre Darstellung gegeben ist. Der Zusammenhang zu der bekannten DFT_n definiert durch

$$\mathrm{DFT}_n = [\omega_n^{ij} \mid i, j \in \{0, \ldots, n-1\}],\ \omega_n \text{ primitive } n\text{-te Einheitswurzel},$$

ist dadurch gegeben, daß diese eine Zerlegungsmatrix ist für eine spezielle reguläre Darstellung ϕ der $\mathsf{Z}_n = \langle x \mid x^n = 1 \rangle$, nämlich

$$\phi = 1_{\mathsf{E}} \uparrow_T \mathsf{Z}_n,\ T = (x^0, x^1, \ldots, x^{n-1}),\ \mathsf{E} = \langle 1 \rangle,$$

was das gleiche ist wie

$$\phi :\ x \mapsto [(1, \ldots, n), n]$$

und es gilt die wohlbekannte Gleichung

$$\phi^{\mathrm{DFT}_n} = \bigoplus_{i=0}^{n-1} (x \mapsto \omega_n^i).$$

Eine beliebige reguläre Darstellung, die durch irgendeine Konjugierte von ϕ gegeben ist, wird nicht direkt durch DFT_n zerlegt.
Die DFT ist der wichtigste Baustein bei der Zerlegung monomialer Darstellungen auflösbarer Gruppen. Es stellt sich heraus, daß der DFT_p, p prim, bei der Zerlegung der regulären Darstellung einer auflösbaren Gruppe G eine ähnliche Rolle zukommt, wie der Z_p beim Aufbau von G.

Reduktion auf Permutationsdarstellung Man könnte glauben, daß sich das Problem der Zerlegung monomialer Darstellungen zurückführen läßt auf die Zerlegung von Permutationsdarstellungen. Dies ist aber nicht so, wofür die Tatsache, daß eine monomiale Darstellung beliebigen Grades irreduzibel sein kann, ein Indiz liefert. Satz 1.15 liefert uns einen Spezialfall, in dem es möglich ist.

1.58 Satz *Sei μ eine transitive monomiale Darstellung von G mit Zerlegung $\mu^D = \lambda \uparrow_T G$, λ ist Darstellung von H vom Grad 1. Besitzt λ eine Erweiterung $\overline{\lambda}$ auf G, dann gilt*

$$\mu^{D \cdot D_1} = \overline{\lambda} \cdot (1_H \uparrow_T G), \;\; D_1 = \mathrm{diag}(\overline{\lambda}(t) \mid t \in T).$$

Ist A eine Zerlegungsmatrix für die Permutationsdarstellung $1_H \uparrow_T G$, dann ist $D \cdot D_1 \cdot A$ eine Zerlegungsmatrix für μ.

Beweis Siehe Beweis von Satz 1.15. ∎

Sätze zur Zerlegung von Permutationsdarstellungen, welche im folgenden präsentiert werden, lassen sich stets mit Satz 1.58 (leicht) verallgemeinern.

Konstruktoren und Zerlegungsmatrizen Es wäre wüschenswert, eine Reihe von Sätzen zu haben, die zu jeder Konstruktionsmethode von Darstellungen (Induktion, Erweiterung, Tensorprodukt, etc.) eine entsprechende Konstruktion für die zugehörigen Zerlegungsmatrizen liefert. Dies ist jedoch nur in einigen Fällen möglich, denen wir uns jetzt zuwenden.

1.59 Satz *Seien ϕ_1, ϕ_2 Darstellungen von G mit Zerlegungsmatrizen A_1, A_2. Dann ist $A_1 \oplus A_2$ eine Zerlegungsmatrix für $\phi_1 \oplus \phi_2$.*

Beweis trivial. ∎

1.60 Satz *Seien ϕ_1, ϕ_2 Darstellungen von N_1 bzw. N_2 mit Zerlegungsmatrizen A_1 bzw. A_2. Dann ist $A_1 \otimes A_2$ eine Zerlegungsmatrix für $\phi_1 \# \phi_2$.*

Beweis Folgt aus der Distributivität von „#“ und der Tatsache, daß das äußere Tensorprodukt zweier irreduzibler Darstellungen irreduzibel ist. ∎

Man beachte, daß die entsprechende Aussage für das innere Tensorprodukt nicht gilt. Sind nämlich ϕ, ψ irreduzible Darstellungen von G, dann ist $\phi \otimes \psi$ im allgemeinen nicht irreduzibel. Die Zerlegung von $\phi \otimes \psi$ in Irreduzible ist in der Literatur auch unter dem Namen *Clebsch-Gordan-Problem* bekannt. Siehe dazu zum Beispiel das Buch von Fulton/Harris (1991), [30].
Der Zusammenhang zwischen der Zerlegungsmatrix einer Darstellung und der Zerlegungsmatrix ihrer Einschränkung auf eine Untergruppe wird im folgenden Satz aus Minkwitz, [45] geklärt.

1.61 Satz *Sei $H \leq G$ eine Untergruppe, ϕ_G eine Darstellung von G und $\phi_H = \phi_G \downarrow H$. dann ist aus jeder Zerlegungsmatrix A_H von ϕ_H eine Zerlegungsmatrix A_G von ϕ_G konstruierbar durch*

$$A_G = A_H \cdot C,$$

wobei C eine blockpermutierte Matrix ist. Die Blockgrößen entsprechen den Größen der homogenen Komponenten von ϕ_H. Die Blöcke, die zu irreduziblen homogenen Komponenten gehören, sind die Identität.

$$\begin{tikzcd}
G \arrow[d, dash] & \phi_G \arrow[rrr, "A'_G", "\mathrm{dec}"'] \arrow[d, "\mathrm{res}"'] & & & \rho_G \arrow[d, "\mathrm{res}"'] \\
H & \phi_H \arrow[r, "A_H", "\mathrm{dec}"'] & \rho_H \arrow[r, "C"] & \sigma_H & (\rho_G \downarrow H) \arrow[l, "B"', "\mathrm{dec}"]
\end{tikzcd}$$

Abbildung 1.6: Situation in Satz 1.61

Beweis Sei A'_G eine Zerlegungsmatrix von ϕ_G, das heißt $\phi_G^{A'_G} = \rho_G$. Dann wird $\rho_G \downarrow H = \phi_H^{A'_G}$ zerlegt durch eine Matrix B, das heißt $\phi_H^{A'_G \cdot B} = \sigma_H$, wobei B nur die irreduziblen Komponenten von ρ_G zerlegt, die bei Einschränkung reduzibel geworden sind (vgl. Abbildung 1.6). Insbesondere ist $A_G = A'_G \cdot B$ auch wieder eine Zerlegungsmatrix für ϕ_G. Ist A_H eine Zerlegungsmatrix von ϕ_H, dann ist $C = A_H^{-1} \cdot A_G \in \mathsf{Int}(\rho_H, \sigma_H)$, also blockpermutiert bzgl. der homogenen Komponenten von ρ_H. ∎

Ein besonders schöner Fall liegt vor, wenn die Zerlegungsmatrix der Einschränkung ϕ_H auch ϕ_G zerlegt.

1.62 Korollar Es gelten die gleichen Voraussetzungen wie in Satz 1.61. Sind die irreduziblen Komponenten von ϕ_H paarweise inäquivalent, dann gibt es zu jeder Zerlegungsmatrix A_H von ϕ_H eine Permutationsmatrix P, so daß $A_H \cdot P$ eine Zerlegungsmatrix für ϕ_G ist.

Beweis In diesem Fall haben alle homogenen Komponenten von ϕ_H den Grad 1 und nach Satz 1.61 ist $P = C$ als Permutationsmatrix wählbar. ∎

Die Situation in Korollar 1.62 tritt beispielsweise ein, wenn ϕ monomial ist und die durch ϕ dargestellte Gruppe G einen abelschen Normalteiler H besitzt, der transitiv dargestellt wird (vgl. 1.34), das heißt $\phi \downarrow H$ ist transitiv. In diesem Fall besitzt ϕ ebenfalls paarweise inäquivalente irreduzible Komponenten. Die Permutationsmatrix P in Korollar 1.62 konjugiert die irreduziblen Darstellungen von $\phi \downarrow H$, welche in einer irreduziblen Komponente von ϕ liegen, nebeneinander.

Diese Beobachtung werden wir im folgenden ausnutzen, um Darstellungen mit regulärem abelschen Normalteiler zu zerlegen. Es zeigt sich, daß insbesondere primitive Permutationsdarstellungen auflösbarer Gruppen in diese Kategorie fallen.

Regulärer abelscher Normalteiler Ist N ein Normalteiler von G, dann operiert G auf den irreduziblen Darstellungen von N (bis auf Äquivalenz) durch innere Konjugation. Der Stabilisator einer irreduziblen Darstellung unter dieser Operation ist eine Gruppe zwischen N und G. Dieser spielt eine wichtige Rolle in der Beziehung zwischen den irreduziblen Darstellungen von N und G. Der Satz von Clifford in seiner allgemeinsten Form (siehe z. B. [22], S. 259 ff) untersucht diese Beziehung. Wir werden hier nur einige Aspekte dieser Untersuchung benötigen und den Satz von Clifford später (Satz 1.71) nur für einen Spezialfall ($(G : N)$ prim) formulieren. Man beachte, daß der Kern einer Permutationsdarstellung $\pi = 1_H \uparrow_T G$ durch $\mathrm{core}(H) = \bigcap_{x \in G} H^x$ gegeben ist (vgl. Satz 1.18).

1.63 Definition *Sei $N \trianglelefteq G$ ein Normalteiler und ϕ eine Darstellung von N. Dann nennen wir*

$$G_\phi = \{x \in G \mid \phi^x \cong \phi\}$$

die „Trägheitsgruppe" von ϕ. Es gilt

$$N \leq G_\phi \leq G.$$

1.64 Lemma Ist G eine Permutationsgruppe mit regulärem Normalteiler N und H der Stabilisator der 1 unter G, dann gilt

$$G = H \ltimes N.$$

Beweis Sei $x \in G$ und $1^x = i$. Da N transitiv ist, gibt es ein $y \in N$ mit $1^y = i$, also ist $xy^{-1} = h \in H$, also $x \in HN$. Da N regulär ist, folgt $H \cap N = \langle 1 \rangle$. ∎

1.65 Lemma Sei $G = H \ltimes N$, N abelsch mit irreduzibler Darstellung λ. Dann gilt:

i) $G_\lambda = (G_\lambda \cap H) \ltimes N$.

ii) λ hat eine Erweiterung $\overline{\lambda}$ auf G_λ.

Beweis i) ist klar. Zu ii) definiere $\overline{\lambda}(hn) = \lambda(n)$ für $h \in G_\lambda \cap H$, $n \in N$. Wir zeigen, daß so ein Homomorphismus definiert wird.

$$\begin{aligned}
\overline{\lambda}(hn)\overline{\lambda}(h_1n_1) &= \lambda(n)\lambda(n_1) \\
\overline{\lambda}(hnh_1n_1) &= \overline{\lambda}(hh_1n^{h_1}n_1) \\
&= \lambda(n^{h_1}n_1) \\
&= \lambda(n^{h_1})\lambda(n_1) \\
&= \lambda(n)\lambda(n_1).
\end{aligned}$$

Das letzte Gleichheitszeichen gilt, weil λ den Grad 1 hat. ∎

Jetzt können wir den Satz formulieren, der es uns erlauben wird, Permutationsdarstellungen mit regulärem abelschen Normalteiler zu zerlegen. In diese Kategorie fallen insbesondere alle primitiven Permutationsdarstellungen auflösbarer Gruppen.

1.66 Satz *Sei* $\pi = 1_H \uparrow_T G$ *eine Permutationsdarstellung vom Grad* n *von* G *mit Kern* $\mathrm{core}(H)$. $N \trianglelefteq G$ *sei ein Normalteiler, so daß* $N/\mathrm{core}(H)$ *abelsch ist und von* π *regulär dargestellt wird (siehe Abbildung 1.7).* A *sei eine Zerlegungsmatrix von* $\pi \downarrow N$*, das heißt*

$$(\pi \downarrow N)^A = \bigoplus_{i=1}^{n} \lambda_i,\ \deg(\lambda_i) = 1,\ i = 1 \ldots n,\ \lambda_i \textit{ paarweise verschieden.}$$

G *operiert auf* $\{\lambda_1, \ldots, \lambda_n\}$ *durch innere Konjugation. Seien* $O_1, \ldots, O_k$ *die Orbits unter dieser Operation,* $O_i = \{\lambda_{i,1}, \ldots, \lambda_{i,r_i}\}$ *mit Konjugationen* $T_i = \{t_{i,1}, \ldots, t_{i,r_i}\}$*, das heißt* $\lambda_{i,1}^{t_{i,j}} = \lambda_{i,j}$, $j = 1 \ldots r_i$. *Weiter sei* $\overline{\lambda}_{i,1}$ *eine Erweiterung von* $\lambda_{i,1}$ *auf* $G_{\lambda_{i,1}}$, $i = 1 \ldots k$. *Dann gilt*

i) T_i *ist Transversale von* $G_{\lambda_{i,1}} \backslash G$ *und* $\overline{\lambda}_{i,1} \uparrow_{T_i} G$ *ist irreduzibel.*

ii) Ist σ *die Permutation, welche* $\lambda_1, \ldots, \lambda_n$ *abbildet auf die Konkatenation* $O_1 \cup \cdots \cup O_k$*, so ist* $A \cdot [\sigma, n]$ *eine Zerlegungsmatrix für* π *und*

$$\pi^{A \cdot [\sigma,n]} = \bigoplus_{i=1}^{k} \overline{\lambda}_{i,1} \uparrow_{T_i} G.$$

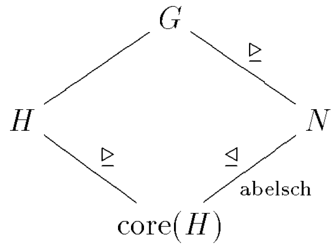

Abbildung 1.7: Situation in Satz 1.66

Beweis Zu i): T_i ist offensichtlich Transversale von $G_{\lambda_{i,1}} \backslash G$. Zum Beweis, daß $\overline{\lambda}_{i,1} \uparrow_{T_i} G$ irreduzibel ist, verweisen wir auf [22], S. 265. Zu ii): Es ist $G_{\lambda_{i,1}} \backslash G/N = G_{\lambda_{i,1}} N \backslash G = G_{\lambda_{i,1}} \backslash G$ und $G_{\lambda_{i,1}}^t \cap N = N$ für alle $t \in T_i$. Mit Mackeys Untergruppensatz (1.12) gilt

$$\begin{aligned}
(\overline{\lambda}_{i,1} \uparrow_{T_i} G) \downarrow N &= \bigoplus_{t \in T_i} (\overline{\lambda}^t_{i,1} \downarrow \underbrace{G^t_{\lambda_{i,1}} \cap N}_{=N}) \uparrow_{(1)} N \\
&= \bigoplus_{t \in T_i} \overline{\lambda}^t_{i,1} \downarrow N \\
&= \bigoplus_{t \in T_i} \lambda^t_{i,1} \\
&= \bigoplus_{j=1}^{r_i} \lambda_{i,j}
\end{aligned}$$

und mit Korollar 1.62 folgt die Behauptung. ∎

Es ist leicht zu zeigen, daß $A \cdot P$ eine Zerlegungsmatrix für π ist. Die Hauptaussage von Satz 1.66 liegt in der Angabe der dazugehörigen irreduziblen Komponenten. Dies ist algorithmisch von großem Wert, da es die explizite Ausführung der (teuren) Konjugation $\pi^{A \cdot P}$ unnötig macht. Anschaulich gesprochen erklärt der Satz, wie die eindimensionalen Darstellungen von N zusammengefaßt werden müssen, damit sie auf G erweitert werden können (siehe Abbildung 1.8) und konstruiert diese Erweiterung. Anders gesagt: die eindimensionalen Darstellungen von N „verschmelzen“ bei der Erweiterung auf G vermöge der Operation (innere Konjugation) von G auf den λ_i.

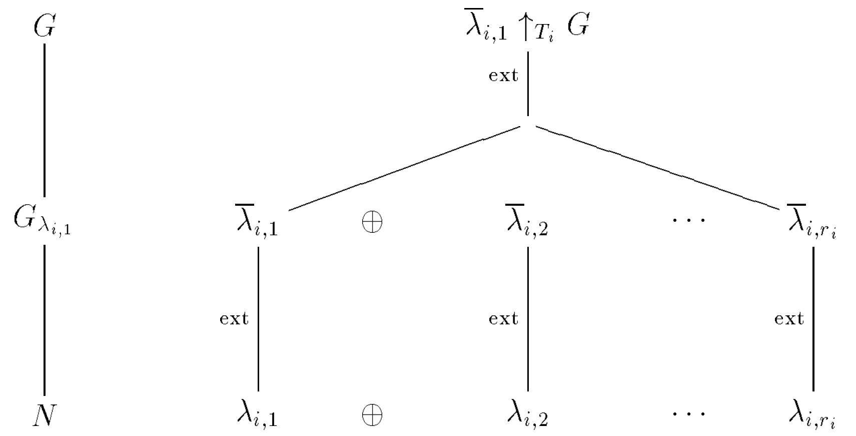

Abbildung 1.8: Erweiterung eines Orbits eindimensionaler Darstellungen von N

Ein algorithmisches Problem ist die Bestimmung des regulär dargestellten Normalteilers N, falls es ihn gibt. Im schlimmsten Fall müssen alle Normalteiler von $G/\ker(\pi)$ der entsprechenden Größe getestet werden. Speziell bei einer großen Klasse von primitiven Permutationsdarstellungen ist ein solcher Normalteiler durch seine Größe jedoch schon eindeutig bestimmt. Der Fall einer monomialen Darstellung von Primzahlgrad läßt sich nun sogar fast vollständig erledigen.

Primzahlgrad Die Charakterisierung der monomialen Darstellungen μ von Primzahlgrad $\deg(\mu) = p$ in Satz 1.36 liefert ein Klasse von Darstellungen auf die sich Satz 1.66 anwenden läßt.

1.67 Satz *Sei μ eine transitive monomiale Darstellung von G mit Grad $\deg(\mu) = p$, prim. μ sei nicht zweifach transitiv und habe die Zerlegung $\mu^D = \lambda_H \uparrow_T G$ mit einer Darstellung λ von $H \leq G$ vom Grad 1. Dann trifft genau einer der beiden folgenden Fälle ein:*

i) μ ist irreduzibel.

ii) λ_H hat eine Erweiterung λ_G auf G, das heißt

$$\mu^{D \cdot D_1} = \lambda_G \cdot (1_H \uparrow_T G), \;\; D_1 = \mathrm{diag}(\lambda_G(t) \mid t \in T).$$

Die p-Sylowgruppe von $G/\operatorname{core}(H)$ ist $\cong \mathsf{Z}_p$ und wird regulär dargestellt durch $1_H \uparrow_T G$. Insbesondere gibt es eine monomiale Matrix M und eine Permutationsmatrix P, so daß $M \cdot \mathrm{DFT}_p \cdot P$ eine Zerlegungsmatrix für μ ist.

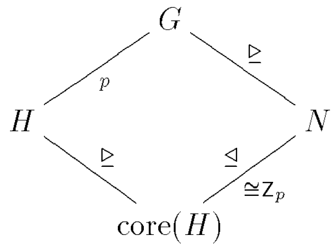

Abbildung 1.9: Situation in Satz 1.67

Beweis Nach dem Satz 1.35 von Burnside besitzt $G/\operatorname{core}(H)$ eine normale p-Sylowgruppe $\cong \mathsf{Z}_p$. Diese wird regulär dargestellt durch $1_H \uparrow_T G$. Der Rest folgt aus Satz 1.36 und Satz 1.66. ∎

Der Fall, daß μ zweifach transitiv ist, wird im folgenden behandelt.

Zweifach Transitive Darstellungen Ist $\mu \cong \lambda_H \uparrow G$ eine zweifach transitive monomiale Darstellung, so gibt es nur zwei Doppelnebenklassen $H\backslash G/H$ mit Vertretern $1, s$, und aus dem Intertwiningzahl-Satz (1.45) folgt, daß

$$\begin{aligned} \langle \lambda_H \uparrow G, \lambda_H \uparrow G \rangle &= \langle \lambda_H, \lambda_H \rangle + \langle \lambda_H^s \downarrow (H^s \cap H), \lambda_H \downarrow (H^s \cap H) \rangle \\ &= 1 + \langle \lambda_H^s \downarrow (H^s \cap H), \lambda_H \downarrow (H^s \cap H) \rangle, \end{aligned}$$

also ist μ entweder irreduzibel oder enthält 2 irreduzible Komponenten. Besitzt λ_H eine Erweiterung auf G, dann ist nach Satz 1.58 die Induktion im wesentlichen eine Permutationsdarstellung, und wir können die Induktion zerlegen.

1.68 Satz *Sei μ eine zweifach transitive monomiale Darstellung vom Grad n von G mit Zerlegung $\mu^D = \lambda_H \uparrow_T G$ und λ_G eine Erweiterung von λ_H auf G. Sei außerdem die $(n \times n)$-Matrix* SOR_n *(* SOR = *Split OneRep) wie folgt definiert*

$$\mathrm{SOR}_n = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 1 & 0 & 0 & & -1 \end{bmatrix}.$$

Dann gibt es eine Diagonalmatrix A, so daß $A \cdot \mathrm{SOR}_n$ μ zerlegt.

Beweis Nach Satz 1.15 gilt

$$\mu^{D \cdot D_1} = \lambda_G \cdot (1_H \uparrow_T G), \text{ mit } D_1 = \mathrm{diag}(\lambda_G(t) \mid t \in T).$$

$1_H \uparrow_T G$ ist ebenfalls zweifach transitiv und zerfällt nach Satz 1.47 in $1_G \oplus \rho$ mit einer irreduziblen Darstellung ρ. Der Darstellungsraum zur enthaltenden Einsdarstellung ist genau der Eigenraum zum Eigenwert 1, erzeugt von $v = (1, \ldots, 1)$. Da Permutationsmatrizen orthogonal sind, bildet das orthogonale Komplement W von $\langle v \rangle$ den Darstellungsraum von ρ. W wird aber erzeugt von den Zeilen $2, \ldots, \deg(\mu)$ von SOR_n, also ist SOR_n eine Zerlegungsmatrix von $1_H \uparrow_T G$, und $D \cdot D_1 \cdot \mathrm{SOR}_n$ eine von μ. ∎

Aus dem Beweis ist ersichtlich, daß eine zweifach transitiven Permutationsdarstellung $1_H \uparrow_t G$ vom Grad n von jeder $(n \times n)$-Matrix M zerlegt wird, die die folgenden beiden Eigenschaften hat:

1. Die erste Zeile von M enthält nur Einsen.
2. Die Zeilen $2, \ldots, n$ spannen das orthogonale Komplement zur ersten Zeile auf.

Diese Eigenschaften erfüllt beispielsweise auch die DFT_n. Der Grund für die Definition der Matrix SOR_n liegt in der Tatsache, daß sie die Matrix mit den wenigsten Einträgen $\neq 0$ ist, die beide Eigenschaften erfüllt.

Primitive Darstellungen Die Zerlegung einer großen Klasse von primitiven Permutationsdarstellungen erlaubt uns der folgende Satz, der schon von Galois gefunden wurde (siehe [36], S. 159).

1.69 Satz (Galois) *Sei G eine primitive Permutationsgruppe vom Grad n, G_1 der Stabilisator der 1 und N ein minimaler Normalteiler von G. Ist N auflösbar, dann gilt:*

i) *N ist regulär und elementar-abelsch, insbesondere ist n eine Primzahlpotenz.*

ii) *$G = G_1 \ltimes N$.*

iii) *N ist der einzige minimale Normalteiler von G.*

Übertragen auf Permutationsdarstellungen bedeutet das:

1.70 Satz *Sei $\pi = 1_H \uparrow_T G$ eine primitive Permutationsdarstellung von G. $G/\operatorname{core}(H)$ habe einen minimalen auflösbaren Normalteiler $N/\operatorname{core}(H)$. Dann ist $\deg(\pi) = (N : \operatorname{core}(H)) = p^n$, p prim, und $N/\operatorname{core}(H) \cong \mathsf{Z}_p^n$ und wird regulär dargestellt durch π (siehe Abbildung 1.10).*

$$\begin{tikzcd}
& G \arrow[dl, dash, "p^n"'] \arrow[dr, dash, "\trianglerighteq"] & \\
H \arrow[dr, dash, "\trianglerighteq"'] & & N \arrow[dl, dash, "\trianglelefteq"', "\cong \mathsf{Z}_p^n"] \\
& \operatorname{core}(H) &
\end{tikzcd}$$

Abbildung 1.10: Situation in Satz 1.70

Beweis Folgt aus Satz 1.69. ∎

Mit Satz 1.66 können wir also insbesondere primitive Darstellungen auflösbarer Gruppen zerlegen. Notwendig ist, daß der Grad eine Primzahlpotenz ist. Der Normalteiler $N \cong \mathsf{Z}_p^n$ kann aufgrund seiner Größe identifiziert werden, da er nach Satz 1.69 der *einzige* minimale Normalteiler ist.
Ein weitaus mächtigeres Werkzeug zur Zerlegung liefert uns der Satz von Clifford, den wir für einen wichtigen Spezialfall im folgenden konstruktiv formulieren werden.

Eine Rekursionsmethode Die Transitivität der Induktion (vgl. Satz 1.4)

$$\phi \uparrow_{TS} G = (\phi_H \uparrow_T K) \uparrow_S G,$$

erlaubt es, diese schrittweise auszuführen, zum Beispiel entlang einer Kette von Untergruppen $G = K_1 \geq K_2 \geq \cdots \geq K_n = H$, wobei K_i eine maximale Untergruppe in K_{i-1} ist ($i = 2 \ldots n$). Ein naheliegender Gedanke ist es, die Zerlegung einer monomialen Darstellung ebenfalls entlang dieser Kette auszuführen. Dabei sind zwei Fragen zu klären:

1. Wie entstehen aus den irreduziblen Komponenten von $\phi_H \uparrow K_i$ die von $\phi_H \uparrow K_{i-1}$?

2. Wie berechnet man eine Zerlegungsmatrix von $\phi_H \uparrow K_{i-1}$ aus einer von $\phi_H \uparrow K_i$?

Die Antworten auf diese Fragen existieren im allgemeinen leider nicht. Ist die obengenannte Kette jedoch das Anfangsstück einer Kompositionsreihe, so liefert uns der Satz von Clifford eine genaue Antwort auf Frage 1. Die im folgenden präsentierte Version dieses Satzes ist erweitert um die Antwort auf Frage 2. Der Satz von Clifford beschäftigt sich in seiner allgemeinsten Form (siehe z. B. [21], S. 345) mit der Einschränkung einer irreduziblen Darstellung einer Gruppe G auf einen Normalteiler $N \trianglelefteq G$. In Hinblick auf eine Kompositionsreihe betrachten wir hier lediglich den Fall, daß $(G : N) = p$, eine Primzahl ist.

1.71 Satz (Satz von Clifford) *Sei $N \overset{p}{\trianglelefteq} G$ ein Normalteiler von Primzahlindex p, $T = (t^0, t^1, \ldots, t^{p-1})$ eine Transversale von G/N und ρ eine irreduzible Darstellung von N. Dann tritt genau einer der folgenden beiden Fällen ein:*

1. *(siehe Abbildung 1.11) $\rho \cong \rho^{t^i}$ für $i = 0 \ldots p-1$. Dann besitzt ρ genau p paarweise inäquivalente Erweiterungen auf G. Ist $\overline{\rho}$ eine von diesen und $\lambda: \ t \mapsto \omega_p$ (ω_p primitive p-te Einheitswurzel) eine Darstellung von G/N, dann sind alle Erweiterungen gegeben durch $\lambda^i \cdot \overline{\rho}$, $i = 0 \ldots p-1$. Die Induktion zerfällt gemäß*

$$(\rho \uparrow_T G)^A = \bigoplus_{i=0}^{p-1} \lambda^i \cdot \overline{\rho},$$

mit

$$A = \mathrm{diag}(\overline{\rho}(t)^i \mid i \in \{0, \ldots, p-1\}) \cdot (\mathrm{DFT}_p \otimes \mathbf{1}_{n/p}),$$

in Irreduzible.

2. *(siehe Abbildung 1.12) $\rho \not\cong \rho^{t^i}$ für $i = 0 \ldots p-1$. Dann ist die Induktion $\rho \uparrow G$ irreduzibel und*

$$(\rho \uparrow_T G) \downarrow N = \bigoplus_{i=0}^{p-1} \rho^{t^i}$$

sowie

$$\rho^{t^i} \uparrow_T G = (\rho \uparrow_T G)^B,$$

mit

$$B = \left([(1, \ldots, p)^{-i}, p] \otimes \mathbf{1}_{\deg(\rho)}\right) \cdot \left(\mathbf{1}_{(p-i)\cdot\deg(\rho)} \oplus (\mathbf{1}_i \otimes \rho(t^p))\right).$$

$$\begin{tikzcd}
G \arrow[d, dash, "p"'] & \lambda^0 \cdot \overline{\rho} \arrow[drr, dash, "\mathrm{ext}"'] & \oplus & \lambda^1 \cdot \overline{\rho} \arrow[d, dash, "\mathrm{ext}"'] & \cdots & \lambda^{(p-1)} \cdot \overline{\rho} \arrow[dll, dash, "\mathrm{ext}"'] & \cong & \rho \uparrow G \\
N & & & \rho & & & &
\end{tikzcd}$$

Abbildung 1.11: Satz von Clifford, Fall: $\rho \cong \rho^{t^i}$

$$\begin{tikzcd}
G \arrow[d, dash, "p"'] & & & \rho \uparrow G \arrow[dll, dash, "\mathrm{ind}"'] \arrow[d, dash, "\mathrm{ind}"'] \arrow[drr, dash, "\mathrm{ind}"] & & & & \\
N & \rho^{t^0} & \oplus & \rho^{t^1} & \cdots & \rho^{t^{(p-1)}} & \cong & (\rho \uparrow G) \downarrow N
\end{tikzcd}$$

Abbildung 1.12: Satz von Clifford, Fall: $\rho \not\cong \rho^{t^i}$

Beweis Der Beweis ist z. B. in [16], S. 88 ff ausführlich präsentiert. Wir wollen nur die drei Gleichungen beweisen. Gleichung in 1.: Mit Satz 1.15 gilt

$$(\rho \uparrow_T G)^D = (1_N \uparrow_T G) \otimes \overline{\rho}, \ D = \mathrm{diag}(\overline{\rho}(t)^i \mid i \in \{0, \ldots, p-1\}).$$

Die Darstellung $1_N \uparrow_T G$ ist eine reguläre Darstellung $t \mapsto [(1, \ldots, p), p]$ von $G/N \cong \mathsf{Z}_p$ und wird von DFT_p zerlegt in p Darstellungen $t \mapsto \omega_p^i, \ i = 0 \ldots p-1$ vom Grad 1, woraus die erste Gleichung folgt.
Erste Gleichung in 2.: folgt aus Korollar 1.13. Zweite Gleichung in 2.: Nach Satz 1.10 gilt $\rho^{t^i} \uparrow_T G = \rho \uparrow_{t^iT} G$. Multiplikation von T mit t^i permutiert die Nebenklassen wie $\sigma = (1, \ldots, p)^{-i}$. Der Übergang von T^σ nach t^iT,

$$T^\sigma = (t^i, \ldots, t^{(p-1)}, t^0, \ldots, t^{(i-1)}) \to t^iT = (t^i, \ldots, t^{(p-1)}, t^p, \ldots, t^{(p-i+1)}),$$

bedeutet eine Multiplikation der letzten i Transversalenelemente mt t^p. Mit Satz 1.1 folgt die Behauptung. ∎

1.72 Beispiel Wir betrachten $G = \mathsf{S}_3 = \langle x, y \mid x^3 = y^2 = 1, \ x^y = x^{-1} \rangle$ mit Normalteiler $N = \mathsf{Z}_3 = \langle x \rangle \trianglelefteq G$ vom Index 2. N besitzt 3 verschiedene irreduzible Darstellungen vom Grad 1:

$$\lambda_1 = 1_N, \quad \lambda_2 : \ x \mapsto \omega_3, \quad \lambda_3 : \ x \mapsto \omega_3^{-1}.$$

λ_1 ist offensichtlich gleich seiner inneren Konjugierten und besitzt demnach 2 Erweiterungen

$$\mu_1 = 1_G, \quad \mu_2 : \; x \mapsto 1, \; y \mapsto -1.$$

In Beispiel 1.9 haben wir gesehen, daß $\lambda_2^y = \lambda_3 \not\cong \lambda_2$, also ist die Induktion $\mu_3 = \lambda_2 \uparrow G \cong \lambda_3 \uparrow G$ irreduzibel:

$$\mu_3 = \lambda_2 \uparrow_{(1,y)} G : \; x \mapsto \begin{bmatrix} \omega_3 & 0 \\ 0 & \omega_3^{-1} \end{bmatrix}, \; y \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Es folgt, daß $\mu_1, \; \mu_2, \; \mu_3$ (bis auf Äquivalenz) alle irreduziblen Darstellungen von G sind. ■

Im Fall $\rho \cong \rho^t$ besitzt ρ eine Erweiterung auf G. Diese läßt sich zum Beispiel mit der Erweiterungsformel von Minkwitz (Satz 1.41) berechnen. Die Formel erfordert die Bestimmung eines erweiternden Charakters und die Auswertung von ρ für alle $h \in H$. In der speziellen Situation im Satz von Clifford gibt es noch eine andere Methode, welche bei dem Beweis in [16] verwendet wird und das folgende Lemma ([16], S. 92) benutzt.

1.73 Lemma Es gelten die Voraussetzungen von Satz 1.71. Im Fall $\rho \cong \rho^t$ definiert $\rho(t) = A$ eine Erweiterung von ρ auf G genau dann, wenn:

i) $A \in \mathsf{Int}(\rho^t, \rho)$ und

ii) $A^p = \rho(t^p)$.

Ist der Grad von ρ klein und $|N|$ groß, dann liefert dieses Lemma eine bessere Möglichkeit die Erweiterung zu berechnen, als die Erweiterungsformel von Minkwitz. Ein weiterer Vorteil gegenüber dieser ist die Tatsache, daß man keinen erweiternden Charakter berechnen muß. Selbstverständlich ist die Minkwitz-Erweiterung aber wesentlich allgemeiner.
In der Situation von Lemma 1.73 ist A eindeutig bestimmt bis auf einen skalaren Faktor, da $\mathsf{Int}(\rho^t, \rho)$ die Dimension 1 hat. Ist $A \in \mathsf{Int}(\rho^t, \rho)$ beliebig, dann unterscheiden sich A^p und $\rho(t^p)$ nur um einen skalaren Faktor α, also

$$\alpha \cdot A^p = \rho(t^p).$$

Ist β eine p-te Wurzel von α, dann wird durch $t \mapsto \beta \cdot A$ eine Erweiterung von ρ definiert.

1.74 Algorithmus (Erweiterung ohne Charakter) Gegeben ist eine irreduzible Darstellung vom Grad n von $N \overset{p}{\trianglelefteq} G$, t erzeugt die Faktorgruppe G/N und $\rho \cong \rho^t$. Es soll eine Erweiterung $\overline{\rho}$ von ρ auf G berechnet werden.

1. Berechne eine beliebige Matrix $\mathbf{0}_n \neq A \in \mathsf{Int}(\rho^t, \rho)$.

2. Berechne eine p-te Wurzel β aus der Zahl an Position $(1,1)$ der Matrix $\rho(t^p) \cdot A^{-p}$.

Die Erweiterung ist gegeben durch $t \mapsto \beta \cdot A$. Alle möglichen Erweiterungen sind gegeben durch die p verschiedenen Wurzeln von α. ∎

Ist insbesondere $\deg(\rho) = 1$, so ist eine Erweiterung definiert durch $\rho(t) = \sqrt[p]{\rho(t^p)}$. Der Satz von Clifford beantwortet, wie die irreduziblen Darstellungen von G aus denen von N entstehen. Entsprechend zeigt der folgende Satz, wie aus einer Zerlegungsmatrix einer Darstellung ϕ von N eine Zerlegungsmatrix von $\phi \uparrow G$ entsteht.

1.75 Satz *Sei $N \overset{p}{\trianglelefteq} G$ ein Normalteiler von Primzahlindex p mit Transversale $T = (t^0, t^1, \ldots, t^{(p-1)})$. Weiter sei ϕ eine Darstellung von N vom Grad n mit Zerlegungsmatrix A, so daß $\phi^A = \bigoplus_{i=1}^k \rho_i$ und $\rho_1, \ldots, \rho_j$ genau die unter den ρ_i sind, welche eine Erweiterung $\overline{\rho}_i$ auf G besitzen (Satz 1.71, Fall 1). Bezeichnet $d = \deg(\rho_1) + \ldots + \deg(\rho_j)$ den Gesamtgrad der erweiterbaren ρ_i und $\overline{\rho} = \overline{\rho}_1 \oplus \ldots \oplus \overline{\rho}_j$, dann existiert eine Permutationsmatrix P, so daß*

$$M = (\mathbf{1}_p \otimes A) \cdot P \cdot \left(\bigoplus_{t \in T} \overline{\rho}(t) \oplus \mathbf{1}_{p(n-d)} \right) \cdot \left((\mathrm{DFT}_p \otimes \mathbf{1}_d) \oplus \mathbf{1}_{p(n-d)} \right)$$

eine Zerlegungsmatrix für $\phi \uparrow_T G$ ist. Bezeichnet $\lambda_i : \ t \mapsto \omega_p^i, \ i = 0 \ldots p-1$, die p eindimensionalen Darstellungen von G/N, dann ist

$$(\phi \uparrow_T G)^M = \bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^{j} \lambda_i \cdot \overline{\rho}_\ell \oplus \bigoplus_{i=j+1}^{k} \rho \uparrow_T G$$

die zugehörige Zerlegung in Irreduzible.

Beweis Satz 1.6 zeigt, daß

$$(\phi \uparrow_T G)^{(\mathbf{1}_p \otimes A)} = \phi^A \uparrow_T G = \left(\bigoplus_{i=1}^{k} \rho_i \right) \uparrow_T G.$$

Wir verwenden Satz 1.5 bzgl. der Blockzerlegung $\rho = \rho_1 \oplus \ldots \oplus \rho_j, \rho_{j+1}, \ldots, \rho_k$, um eine Permutationsmatrix P zu bestimmen, so daß

$$(\phi \uparrow_T G)^{(\mathbf{1}_p \otimes A) \cdot P} = \rho \uparrow_T G \oplus \rho_{j+1} \uparrow_T G \oplus \ldots \oplus \rho_k \uparrow_T G.$$

Da ρ eine Erweiterung $\overline{\rho}$ auf G besitzt, ist nach Satz 1.15

$$(\rho \uparrow_T G)^{\bigoplus_{t \in T} \overline{\rho}(t)} = (1_N \uparrow_T G) \otimes \overline{\rho}.$$

Die Darstellung $(1_N \uparrow_T G)$ wird zerlegt von DFT_p in $\bigoplus_{i=0}^{p-1} \lambda_i$ mit $\lambda_i : \ t \mapsto \omega_p^i$. Damit ist $\bigoplus_{t \in T} \overline{\rho}(t) \cdot (\mathrm{DFT}_p \otimes \mathbf{1}_d)$ eine Zerlegungsmatrix für $\rho \uparrow_T G$ mit zugehöriger Zerlegung $\bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^{j} \lambda_i \cdot \overline{\rho}_\ell$. Die Induktionen der $\rho_i, \ i = j+1 \ldots k$ sind nach Voraussetzung bereits irreduzibel, woraus die Behauptung folgt. ∎

Die Bedingung, daß ϕ von A so zerlegt wird, daß die erweiterbaren Irreduziblen vorne stehen, stellt keine Einschränkung dar, da sich das stets durch eine Permutation erreichen läßt. Es sei weiter erwähnt, daß die angegebene Matrix zwar $\phi \uparrow_T G$ zerlegt, daß aber äquivalente irreduzible Komponenten von $\phi \uparrow_T G$ bei dieser Zerlegung nicht notwendig gleich sind. Für algorithmische Zwecke ist das jedoch sehr wichtig. In Kapitel 2 werden wir darauf eingehen und erklären, wie man die einzelnen Faktoren der Zerlegungsmatrix günstig bestimmt. Man beachte, daß mit Satz 1.75 sowohl die Zerlegungsmatrix, als auch die irreduziblen Komponenten rekursiv konstruiert werden, das heißt eine Konjugation wird niemals ausgeführt. Das ist eine Grundvoraussetzung, um Darstellungen höheren Grades (> 100) überhaupt behandeln zu können.
Allein mit diesem Satz lassen sich alle monomialen Darstellungen einer auflösbaren Gruppe zerlegen, die durch Induktion von einer subnormalen Untergruppe aus entstehen. Eine Untergruppe $H \leq G$ einer auflösbaren Gruppe G heißt subnormal, wenn es eine Kompositionsreihe von G gibt, die H enthält.
Die Zerlegungsmatrix M erinnert stark an die bekannte Cooley-Tukey-Zerlegung einer DFT_{2^n} (siehe Cooley/Tukey (1965), [19]) und in der Tat stellt dieser Satz eine Verallgemeinerung dieser Zerlegung dar. Ist nämlich G eine abelsche Gruppe, dann sind alle irreduziblen Komponenten von ϕ erweiterbar (da $\phi \uparrow G$ nur irreduzible Komponenten vom Grad 1 hat) und $d = n$. Die Permutationsmatrix entfällt, da die erweiterbaren Irreduziblen als ein Block behandelt werden. Das wollen wir in dem folgenden Korollar festhalten.

1.76 Korollar Ist in der Situation von Satz 1.75 G abelsch, dann ist $d = n$ und

$$M = (\mathbf{1}_p \otimes A) \cdot \left(\bigoplus_{t \in T} \overline{\rho}(t) \right) \cdot (\mathrm{DFT}_p \otimes \mathbf{1}_n).$$

Die Diagonalelemente der Matrix $\bigoplus_{t \in T} \overline{\rho}(t)$ sind in der Literatur unter dem Namen *Twiddle-Faktoren* bekannt.
Unter einer gewissen Voraussetzung läßt sich eine Zerlegungsmatrix einer Induktion auch anders bestimmen. Diese Variante findet sich in Minkwitz, [46], [48], liefert aber im allgemeinen suboptimale Zerlegungen. Wir wollen sie trotzdem in einem Satz festhalten, da die Formel gefälliger ist.

1.77 Satz *Sei $H \leq G$ eine Untergruppe vom Index k mit Darstellung ϕ vom Grad n, die eine Erweiterung $\overline{\phi}$ auf G besitzt und T eine Transversale von $H \backslash G$. Weiter sei A eine Matrix, die ϕ in Irreduzible zerlegt, also $\phi^A = \rho$ und $\overline{\rho}$ eine Erweiterung von ρ auf G (vgl. Abbildung 1.13). Dann gilt*

$$(\phi \uparrow_T G)^{(\mathbf{1}_k \otimes A) \cdot D} = (1_H \uparrow_T G) \otimes \overline{\rho}, \ \ mit\ D = \bigoplus_{t \in T} \overline{\rho}(t).$$

Ist insbesondere $H \trianglelefteq G$, G/H abelsch und $\overline{\rho}$ ebenfalls in Irreduzible zerlegt, dann ist

$$(\mathbf{1}_k \otimes A) \cdot D \cdot (\mathrm{DFT}_{G/H} \otimes \mathbf{1}_n)$$

eine Zerlegungsmatrix für $\phi \uparrow_T G$.

$$\begin{tikzcd} G \arrow[d, dash] & \overline{\phi} & \overline{\rho} \\ H & \phi \arrow[u, "\mathrm{ext}"] \arrow[r, "A", "\mathrm{dec}"'] & \rho \arrow[u, "\mathrm{ext}"'] \end{tikzcd}$$

Abbildung 1.13: Situation in Satz 1.75

Beweis Wegen Satz 1.6 ist

$$(\phi \uparrow_T G)^{\mathbf{1}_k \otimes A} = \phi^A \uparrow_T G = \rho \uparrow_T G$$

und mit Satz 1.15 folgt $(\rho \uparrow_T G)^D = (1_H \uparrow_T G) \otimes \overline{\rho},\ D = \bigoplus_{t \in T} \overline{\rho}(t)$.
Ist nun $H \trianglelefteq G$ und G/H abelsch, dann ist $1_H \uparrow_T G$ eine reguläre Darstellung von G/H, die von $\mathrm{DFT}_{G/H}$ in $(G:H) = k$ Irreduzible $\lambda_1, \ldots, \lambda_k$ vom Grad 1 zerlegt wird. Sei $M = (\mathbf{1}_n \otimes A) \cdot D \cdot (\mathrm{DFT}_{G/H} \otimes \mathbf{1}_{\deg(\phi)})$, dann gilt

$$(\phi \uparrow_T G)^M = \left(\bigoplus_{i=1}^{k} \lambda_i \right) \otimes \overline{\rho} = \bigoplus_{i=1}^{k} (\lambda_i \cdot \overline{\rho}),$$

was in Irreduzible zerlegt ist. ∎

Die zusätzliche Bedingung, daß ρ eine Erweiterung $\overline{\rho}$ auf G besitzt, ist im abelschen Fall sicher erfüllt. Ist außerdem $H \trianglelefteq G$ ein Normalteiler von Primzahlindex p, dann erhalten wir das gleiche Ergebnis wie in Korollar 1.76. In allen anderen Fällen ist die Zerlegung in Satz 1.77 jedoch schlechter als die Zerlegung in Satz 1.75, da in der ersten n viele DFT_p auftreten, in der zweiten nur $d \leq n$ (Anzahl der erweiterbaren Irreduziblen).
Wir wollen trotzdem noch kurz auf die Frage eingehen, wann eine beliebige Darstellung eines Normalteilers von Primzahlindex eine Erweiterung besitzt.

1.78 Satz *Sei $N \overset{p}{\trianglelefteq} G$ ein Normalteiler von Primzahlindex p mit Darstellung ϕ sowie $T = (t^0, t^1, \ldots, t^{(p-1)})$ eine Transversale von G/N. Genau dann besitzt ϕ eine Erweiterung $\overline{\phi}$ auf G, wenn $\phi^t \cong \phi$.*

Beweis Ist $\overline{\phi}$ eine Erweiterung von ϕ, dann gilt

$$\phi^t(x) = \phi(txt^{-1}) = \phi(x)^{\overline{\phi}(t^{-1})},$$

also $\phi^t \cong \phi$. Für die andere Richtung bemerken wir zunächst, daß eine Darstellung genau dann eine Erweiterung besitzt, wenn dies für eine beliebige Konjugierte gilt.

Sei nun $\phi^t \cong \phi$ und $\rho = \bigoplus_{i=1}^n \rho_i \cong \phi$ eine Zerlegung von ϕ in Irreduzible. Dann operiert G/N auf den Summanden ρ_i durch innere Konjugation (ρ_i irreduzibel $\Leftrightarrow \rho_i^t$ irreduzibel) bis auf Äquivalenz. Nach dem Satz von Clifford gibt es zwei Möglichkeiten für die Orbits: entweder ein Orbit hat die Länge 1 ($\rho_i \cong \rho_i^t$) oder die Länge p ($\rho_i^{t^0}, \rho_i^{t^1}, \ldots, \rho_i^{t^{(p-1)}}$). Im ersten Fall besitzt ρ_i eine Erweiterung, im zweiten Fall läßt sich das ganze Orbit (nach entsprechender Konjugation) simultan erweitern durch $\rho_i \uparrow_T G$ nach Korollar 1.13. Also besitzt ρ eine Erweiterung und damit auch ϕ. ∎

1.79 Korollar Ist in der Situation von Satz 1.78 $\phi = 1_{\mathsf{E}} \uparrow_S N$ eine reguläre Darstellung von N, dann besitzt ϕ eine Erweiterung auf G.

Beweis Es gilt

$$\phi^t = (1_{\mathsf{E}} \uparrow_S N)^t = (1_{\mathsf{E}} \uparrow_{S^t} N) \cong \phi$$

nach Satz 1.11 und mit Satz 1.78 folgt die Behauptung. ∎

Reguläre Darstellungen auflösbarer Gruppen lassen sich also mit Satz 1.77 zerlegen. An dieser Stelle wird es Zeit für ein kleines Beispiel.

1.80 Beispiel Sei $\mathsf{Z}_4 = \langle x \mid x^4 = 1 \rangle$ mit trivialer Untergruppe E. Wir wollen die reguläre Darstellung

$$\phi = 1_{\mathsf{E}} \uparrow_T \mathsf{Z}_4,\ T = (1, x, x^2, x^3),$$

über $\mathbb{C}$ zerlegen. Selbstverständlich wird dies von DFT_4 geleistet, wir wollen aber entlang der Kompositionsreihe

$$\mathsf{E} \trianglelefteq \mathsf{Z}_2 \trianglelefteq \mathsf{Z}_4,\ \mathsf{Z}_2 = \langle x^2 \rangle$$

zerlegen, um somit auch eine Zerlegung der DFT_4 zu erhalten. Zunächst wird die Induktion zerlegt, $T_1 = (1, x^2)$ ist eine Transversale von $\mathsf{E}\backslash\mathsf{Z}_2$ und $T_2 = (1, x)$ eine von $\mathsf{Z}_2\backslash\mathsf{Z}_4$, $T_2T_1 = (1, x^2, x, x^3)$. Transversalenwechsel gemäß Satz 1.1 ergibt

$$(1_{\mathsf{E}} \uparrow_{T_1} \mathsf{Z}_2) \uparrow_{T_2} \mathsf{Z}_4 = 1 \uparrow_{T_2T_1} \mathsf{Z}_4 = (1 \uparrow_T \mathsf{Z}_4)^{[(2,3),4]}.$$

Die Darstellung $1_{\mathsf{E}} \uparrow_{T_1} \mathsf{Z}_2$ wird von der DFT_2 zerlegt und es gilt

$$\rho = (1_{\mathsf{E}} \uparrow_{T_1} \mathsf{Z}_2)^{\mathrm{DFT}_2} = 1_{\mathsf{Z}_2} \oplus (x^2 \mapsto -1).$$

Beide irreduziblen Summanden sind erweiterbar: 1_{Z_2} wird offensichtlich erweitert durch 1_{Z_4} und $(x^2 \mapsto -1)$ durch $(x \mapsto i)$, also

$$\rho = 1_{\mathsf{Z}_2} \oplus (x^2 \mapsto -1) \xrightarrow{\text{ext}} \overline{\rho} = 1_{\mathsf{Z}_4} \oplus (x \mapsto i).$$

Auswertung von $\overline{\rho}$ an der Transversalen T_2 ergibt die Twiddle-Faktoren

$$\overline{\rho}(1) = \mathbf{1}_2,\ \overline{\rho}(x) = \mathrm{diag}(1, i),$$

und die Zerlegungsmatrix M ist gegeben durch

$$M = [(2,3),4] \cdot (\mathbf{1}_2 \otimes \mathrm{DFT}_2) \cdot \mathrm{diag}(1,1,1,i) \cdot (\mathrm{DFT}_2 \otimes \mathbf{1}_2).$$

Da ϕ von M genauso zerlegt wird, wie von DFT_4, gilt $\mathrm{DFT}_4 = M$. ∎

Abelsche Darstellungen Die bekannten Zerlegungen der DFT_n lassen sich aus den Sätzen der vorigen Abschnitte herleiten. Die sogenannte Good-Thomas-Zerlegung (siehe Agarwal (1977), [1]) entspricht der Zerlegung der regulären Darstellung einer Z_n in ein äußeres Tensorprodukt. Die Cooley-Tukey-Zerlegung resultiert aus der iterierten Anwendung von Korollar 1.76. Da in diesen Fällen explizite Formeln bekannt sind, macht es Sinn, diese direkt in das Programm zu integrieren, um die Berechnung zu beschleunigen.
Jede abelsche Gruppe zerfällt in ein direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung. Nach Satz 1.34 sind monomiale Darstellungen abelscher Gruppen im wesentlichen reguläre Darstellungen. Nach Korollar 1.31 zerfallen reguläre Darstellungen in ein äußeres Tensorprodukt genau wie die dargestellte Gruppe in ein direktes Produkt. Damit ist der zentrale Baustein bei der Zerlegung einer abelschen monomialen Darstellung die DFT_{p^e}, p prim. Eine Formel zur Zerlegung dieser findet sich z. B. in der Dissertation von Egner (1997), [26]. Von dort zitieren wir das folgende Lemma.

1.81 Lemma Sei $n = p^e$, p prim und $e > 1$. Dann gilt

$$\begin{aligned}
\mathrm{DFT}_n \;=\; & (\mathbf{1}_1 \otimes \mathrm{DFT}_p \otimes \mathbf{1}_{p^{e-1}}) \cdot \mathrm{diag}\left(\omega_n^{t(e-1,k)} \mid k \in \{0,\dots,n-1\}\right) \cdot \\
& (\mathbf{1}_p \otimes \mathrm{DFT}_p \otimes \mathbf{1}_{p^{e-2}}) \cdot \mathrm{diag}\left(\omega_n^{t(e-2,k)} \mid k \in \{0,\dots,n-1\}\right) \cdot \\
& \qquad\qquad\vdots \\
& (\mathbf{1}_{p^{e-2}} \otimes \mathrm{DFT}_p \otimes \mathbf{1}_p) \cdot \mathrm{diag}\left(\omega_n^{t(1,k)} \mid k \in \{0,\dots,n-1\}\right) \cdot \\
& (\mathbf{1}_{p^{e-1}} \otimes \mathrm{DFT}_p \otimes \mathbf{1}_1) \cdot [\sigma, n],
\end{aligned}$$

wobei die Exponenten $t(\alpha, k)$ der Twiddle-Faktoren und die Permutation σ von $\{0,\dots,n-1\}$ bestimmt sind durch

$$\begin{aligned}
t(\alpha,k) &= \left((k \bmod p^{\alpha+1}) \operatorname{div} p^{\alpha}\right) \cdot (k \bmod p^{\alpha}) \cdot p^{(e-1)-\alpha} \quad \text{und} \\
k^{\sigma} &= \sum_{\ell=0}^{e-1} \left((k \operatorname{div} p^{\ell}) \bmod p\right) p^{(e-1)-\ell}, \\
& \quad k \in \{0,\dots,n-1\},\ \alpha \in \{1,\dots,e-1\}.
\end{aligned}$$

(Die Permutation σ invertiert die Wertigkeit der einzelnen Stellen von k, dargestellt im Zahlensystem zur Basis p.)

2

Zerlegung monomialer Darstellungen

Das Hauptergebnis dieser Arbeit ist der im folgenden präsentierte Algorithmus zur Zerlegung einer großen Klasse monomialer Darstellungen. Die in Kapitel 1 bewiesenen konstruktiven Sätze erlauben es, ohne weiteres einen Algorithmus in Makro-Operationen zu formulieren. Wir werden darüber hinaus an den kritischen Stellen sehr genau auf die tatsächliche Umsetzung des Algorithmus eingehen. Die aktuelle Implementierung ist durch ständige Verbesserung, hauptsächlich durch besseres Verständnis der zugrundeliegenden Mathematik, etwa um den Faktor 100 schneller als die erste Version.
Zunächst wollen wir erklären, was wir unter der Zerlegung einer Darstellung in bezug auf den Algorithmus verstehen. Ist eine monomiale Darstellung μ vom Grad n einer Gruppe G gegeben, so wollen wir eine $(n \times n)$-Matrix A bestimmen, so daß

$$\mu^A = A^{-1} \cdot \mu \cdot A = \bigoplus_{i=1}^{k} \rho_i, \text{ wobei } \rho_i \text{ irreduzibel ist für } i = 1 \dots k.$$

Darüber hinaus sollen ähnliche Irreduzible gleich sein, das heißt

$$\rho_i \cong \rho_j \Rightarrow \rho_i = \rho_j.$$

Außerdem sollen gleiche Irreduzible nebeneinander stehen, und alle Irreduziblen sollen nach Grad geordnet sein. Die Einführung einer Totalordnung auf den Irreduziblen, z. B. über den Charakter, hat sich als nicht rentabel erwiesen, da die Berechnung des Charakters in vielen Fällen für die Zerlegung der Darstellung nicht notwendig ist. Das Gleichmachen und Zusammenfassen der Irreduziblen bringt dagegen eine erhebliche Ersparnis bei der rekursiven Zerlegung: alle Berechnungen (z. B. Induktion einer Irreduziblen) müssen nur für eine Darstellung aus einer Gruppe Gleicher ausgeführt werden.
Entscheidend für die Algorithmengenerierung (siehe Kapitel 3) ist, daß die Zerlegungsmatrix A in faktorisierter Form zurückgegeben wird, das heißt A ist ein

Produkt dünn besetzter Matrizen. Dieses Produkt entspricht einem schnellen Algorithmus für die Multiplikation mit A.
Ein weiterer wichtiger Punkt ist die Tatsache, daß sowohl die Zerlegungsmatrix A als auch die Zerlegung $\bigoplus_{i=1}^k \rho_i$ berechnet wird, da sich keineswegs das eine aus dem anderen leicht berechnen läßt. Ist nur A gegeben, so muß die Zerlegung durch explizite Konjugation μ^A bestimmt werden, was bei großem Grad ($n > 100$) teuer ist. Ist nur die Zerlegung $\bigoplus_{i=1}^k \rho_i$ von μ gegeben, so läßt sich eine Zerlegungsmatrix nach Satz 1.56 (Berechnung des Intertwiningraums, S. 46) über ein lineares Gleichungssystem mit n^2 Unbekannten bestimmen, das Ergebnis ist aber nicht faktorisiert.
Das Hauptinstrument zur Zerlegung von μ liefert Satz 1.75 auf S. 59. Ist $\mu^D = \lambda_H \uparrow_T G$ zerlegt in eine Induktion, so erlaubt es dieser Satz, die Zerlegung der Induktion entlang einer Kompositionsreihe von H nach G rekursiv zu bestimmen. Die Konstruktion entlang dieser Kompositionsreihe bestimmt die Faktorisierung der Zerlegungsmatrix A. Die Tatsache, daß eine solche Kompositionsreihe im allgemeinen nicht existiert, stellt die einzige Einschränkung dieser Methode dar.
Eine andere Methode, welche in Satz 1.66 auf S. 51 beschrieben wird, löst die Zerlegung einer Permutationsdarstellung π mit regulär dargestelltem abelschen Normalteiler N. In diesem Fall liefert die Zerlegung der Einschränkung $\pi \downarrow N$ bereits im wesentlichen eine Zerlegung von π. In diese Klasse von Darstellungen fallen insbesondere alle primitiven Permutationsdarstellungen auflösbarer Gruppen.
Ein besonderes Merkmal des Zerlegungsalgorithmus ist die Tatsache, daß er fast immer ohne die Charaktertafel der dargestellten Gruppe auskommt.

2.1 Der Algorithmus

Es sei noch einmal daran erinnert, daß nur Darstellungen mit Maschke-Bedingung betrachtet werden. Zunächst werden wir den Algorithmus angeben, der eine transitive Permutationsdarstellung π von G zerlegt, wenn es einen regulär dargestellten abelschen Normalteiler gibt. Der Algorithmus folgt dem Beweis von Satz 1.66 auf S. 51.

2.1 Algorithmus (Zerlegung bei regulärem abelschen Normalteiler)
Gegeben ist eine transitive Permutationsdarstellung π von G mit Kern $\ker(\pi)$ sowie ein Normalteiler $N \trianglelefteq G$, so daß $N/\ker(\pi)$ abelsch ist und regulär dargestellt wird. π soll zerlegt werden.

1. Zerlege $\pi = 1_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29).

2. Zerlege $\pi \downarrow N$ mit einer Matrix B, das heißt

$$(\pi \downarrow N)^B = \bigoplus_{i=1}^{n} \lambda_i, \ \deg(\lambda_i) = 1.$$

3. Bestimme die Orbits $O_1, \ldots, O_k$ von $L = \{\lambda_1, \ldots, \lambda_n\}$ unter der Operation von G durch innere Konjugation mit zugehörigen Konjugationen $T_1, \ldots, T_k$, das heißt $O_i = \{\lambda_{i,1}, \ldots, \lambda_{i,r_i}\}$, $T_i = \{t_{i,1}, \ldots, t_{i,r_i}\}$ und es gilt $\lambda_{i,1}^{t_{i,j}} = \lambda_{i,j}, \ j = 1 \ldots r_i$. Bestimme außerdem die Stabilisatoren $G_{\lambda_{i,1}}, \ i = 1 \ldots k$.

   Man beachte daß $G = H \ltimes N$ ist, wenn H der Stabilisator eines Punktes unter π ist. Die Operation von G auf den Irreduziblen entspricht daher der Operation von H. Zur Berechnung der Orbits können die Charakterwerte der λ_i vorberechnet werden. H besitzt eine Permutationsdarstellung auf den (einelementigen) Konjugationsklassen von N. Zwei Irreduzible λ_i, λ_j sind äquivalent genau dann, wenn die zugehörigen Listen der Charakterwerte durch eine Permutation in H auseinander hervorgehen.

4. Berechne eine Permutationsmatrix P_1, welche L abbildet auf die Konkatenation $O_1 \cup \cdots \cup O_k$.

5. Erweitere $\lambda_{i,1}$ auf $G_{\lambda_{i,1}}$ durch $\overline{\lambda}_{i,1}(hn) = \lambda_{i,1}(n), \ h \in H, \ n \in N$.

6. Berechne die Induktionen

$$\rho_i = \overline{\lambda}_{i,1} \uparrow_{T_i} G, \ i = 1 \ldots k.$$

7. Sortiere die ρ_i nach Grad mit einer Permutationsmatrix P_2. Man beachte, daß die ρ_i paarweise inäquivalent sind.

Es ist $A = B \cdot P_1 \cdot P_2$ eine Zerlegungsmatrix für π und $\pi^A = \bigoplus_{i=1}^{k} \rho_i$. ∎

Die rekursiv aufgerufene Zerlegung von $\pi \downarrow N$ wird durch den folgenden Algorithmus als Spezialfall geleistet. Man beachte, daß dem Algorithmus 2.1 der Normalteiler N übergeben wird, das heißt er wird nicht im Algorithmus berechnet.
Jetzt können wir uns dem allgemeinen Fall zuwenden.

2.2 Algorithmus (Zerlegung monomialer Darstellungen)
Gegeben ist eine monomiale Darstellung μ vom Grad n einer Gruppe G. Zu μ soll eine (in ein Produkt) zerlegte Matrix A und irreduzible Darstellungen $\rho_i, \ i = 1 \ldots k$ bestimmt werden, so daß die folgenden Bedingungen erfüllt sind:

1. $\rho_i \cong \rho_j \Rightarrow \rho_i = \rho_j$.

2. $i < j \Rightarrow \deg(\rho_i) \leq \deg(\rho_j)$.

3. Gleiche Irreduzible folgen aufeinander.

Fall 1: μ ist irreduzibel

Die Irreduzibilität wird über den Charakter von μ getestet. Man beachte, daß eine Permutationsdarstellung vom Grad > 1 niemals irreduzibel ist.
$A = \mathbf{1}_n$ ist eine Zerlegungsmatrix zur Zerlegung $\rho = \mu$.

Fall 2: μ ist nicht transitiv

1. Zerlege μ mit Algorithmus 1.23 (Orbitzerlegung, S. 28) entsprechend der Orbits mit einer Permutationsmatrix P_1:

$$\mu^{P_1} = \bigoplus_{i=1}^{k} \mu_i, \ \ \mu_i \text{ transitiv.}$$

2. Zerlege rekursiv die μ_i für $i = 1 \ldots k$, das heißt

$$\mu_i^{A_i} = \bigoplus_{j=1}^{r_i} \rho_{i,j}.$$

3. Bestimme eine blockdiagonale Matrix D, welche ähnliche Irreduzible zu verschiedenen μ_i auf Gleichheit konjugiert. Dazu werden gemäß Satz 1.56 (Berechnung des Intertwiningraums, S. 46) lineare Gleichungen gelöst. Beachte, daß ähnliche Irreduzible, welche zu einem μ_i gehören, bereits gleich sind. Die Blöcke in D entsprechen (gröbstens) den Graden der $\rho_{i,j}$.

4. Bestimme eine Permutationsmatrix P_2, welche die $\rho_{i,j}$ nach Grad sortiert und gleiche nebeneinander konjugiert.

$A = P_1 \cdot \bigoplus_{i=1}^{k} A_i \cdot D \cdot P_2$ zerlegt μ.

Fall 3: μ ist eine 2-fach transitive Permutationsdarstellung

Die Matrix

$$A = \mathrm{SOR}_n = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 1 & 0 & 0 & & -1 \end{bmatrix}$$

zerlegt μ in $1_G \oplus \rho$. In diesem Fall werden die beiden Irreduziblen durch Konjugation von μ mit der dünn besetzten ($3n-2$ Einträge) Matrix A bestimmt. Man beachte, daß die beiden Irreduziblen bereits nach Grad geordnet sind.

Fall 4: $\deg(\mu) = p$ **ist eine Primzahl und** μ **ist nicht zweifach transitiv**

Fall 4a: μ ist keine Permutationsdarstellung

1. Zerlege $\mu^{D_1} = \lambda_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29). D_1 ist eine Diagonalmatrix.
2. Erweitere λ_H durch λ_G auf G mit Algorithmus 1.74 (Erweiterung ohne Charakter, S. 58).
3. Berechne $D_2 = \operatorname{diag}(\lambda_G(t) \mid t \in T)$.
4. Zerlege rekursiv $1_H \uparrow_T G$ mit der Matrix B, das heißt

$$(1_H \uparrow_T G)^B = \bigoplus_{i=1}^{k} \rho_i.$$

Es ist $A = D_1 \cdot D_2 \cdot B$ eine Zerlegungsmatrix für μ und $\mu^A = \bigoplus_{i=1}^{k} \lambda_G \cdot \rho_i$. Man beachte, daß mit den ρ_i auch die $\lambda_G \cdot \rho_i$ geordnet sind. λ_H besitzt eine Erweiterung nach Satz 1.36 auf S. 34, die sich mit Algorithmus 1.74 (Erweiterung ohne Charakter, S. 58) berechnen läßt, da nach Satz 1.35 von Burnside auf S. 34 G und damit auch $G/N \cong H$ auflösbar ist.

Fall 4b: μ ist eine Permutationsdarstellung

1. Zerlege $\mu = 1_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29) und bestimme $\ker(\mu) = \operatorname{core}(H)$.
2. Berechne die p-Sylowgruppe N von $G/\operatorname{core}(H)$. Diese ist ein abelscher, von μ regulär dargestellter Normalteiler.
3. Zerlege μ mit Algorithmus 2.1 bzgl. N.

Fall 5: μ **ist eine primitive Permutationsdarstellung mit auflösbarem minimalen Normalteiler**

Nach Satz 1.70 auf S. 55 ist es notwendig in diesem Fall, daß $\deg(\mu)$ eine Primzahlpotenz ist.

1. Zerlege $\mu = 1_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29) und bestimme $\ker(\mu) = \operatorname{core}(H)$.
2. Berechne den kleinsten nichttrivialen Normalteiler N von $G/\operatorname{core}(H)$.
3. Ist N nicht auflösbar, so kann μ nicht zerlegt werden. Sonst ist $N \cong \mathsf{Z}_p^k$ abelsch und wird von μ regulär dargestellt. Zerlege μ mit Algorithmus 2.1 bzgl. N.

Fall 6: $G/\ker(\mu)$ **ist abelsch**

Fall 6a: μ ist keine Permutationsdarstellung

1. Zerlege $\mu^{D_1} = \lambda_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29). D_1 ist eine Diagonalmatrix.
2. Erweitere λ_H durch λ_G auf G mit Algorithmus 1.74 (Erweiterung ohne Charakter, S. 58).
3. Berechne $D_2 = \mathrm{diag}(\lambda_G(t) \mid t \in T)$.
4. Zerlege rekursiv $1_H \uparrow_T G$ durch B, das heißt

$$(1_H \uparrow_T G)^B = \bigoplus_{i=1}^{k} \rho_i, \ \deg(\rho_i) = 1, \ i = 1 \dots k.$$

Es ist $A = D_1 \cdot D_2 \cdot B$ eine Zerlegungsmatrix für μ und $\mu^A = \bigoplus_{i=1}^{k} \lambda_G \cdot \rho_i$. Man beachte, daß mit den ρ_i auch die $\lambda_G \cdot \rho_i$ geordnet sind.

Fall 6b: $G_1 = G/\ker(\mu)$ ist eine zyklische Gruppe von Primzahlpotenzordnung p^k

1. Bestimme ein $g \in G$, welches G_1 erzeugt. Aufgrund der Voraussetzung muß ein solches g in dem Erzeugendensystem von G enthalten sein, μ ist eine reguläre Darstellung von G_1. Berechne $\mu(g)$.
2. Bestimme eine Permutationsmatrix P, welche $\mu(g)$ auf $[(1, \dots, p^k), p^k]$ konjugiert.
3. Berechne eine Zerlegungsmatrix B der Darstellung μ^P gegeben durch $g \mapsto [(1, \dots, p^k), p^k]$ mit der Formel in Lemma 1.81 auf S. 63.

Es ist $A = P \cdot B$ eine Zerlegungsmatrix für μ mit Zerlegung

$$\mu^A = \bigoplus_{i=0}^{p^k-1} \rho_i, \ \rho_i : \ g \mapsto \omega_{p^k}^i.$$

Fall 6c: μ ist eine Permutationsdarstellung

1. Zerlege $\mu = 1_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29). Nach Satz 1.34 auf S. 33 ist μ eine reguläre Darstellung der Faktorgruppe $G_1 = G/H$.
2. Zerlege G_1 in ein direktes Produkt $G_1 = N_1 \times \cdots \times N_k$ von zyklischen Gruppen von Primzahlpotenzordnung, $N_i = \langle x_i \rangle$.
3. Berechne die Permutationsmatrix P zum Transversalenwechsel $T \to T_1 \cdot T_2 \cdots T_k$, wobei $T_i = (x_i^0, x_i^1, x_i^2, \dots)$ eine Liste der Elemente von N_i ist.
4. Zerlege rekursiv $1_{\mathsf{E}} \uparrow_{T_i} N_i$ durch A_i

$$(1_{\mathsf{E}} \uparrow_{T_i} N_i)^{A_i} = \bigoplus_{j=1}^{r_i} \rho_{i,j}.$$

Es ist $A = P \cdot \bigotimes_{i=1}^{k} A_i$ eine Zerlegungsmatrix von μ mit Zerlegung

$$\mu^A = \bigoplus_{j_1=1}^{r_1} \cdots \bigoplus_{j_k=1}^{r_k} (\rho_{1,j} \# \ldots \# \rho_{k,j}).$$

Fall 7: μ ist ähnlich zu einem konjugierten äußeren Tensorprodukt

1. Zerlege μ in ein konjugiertes äußeres Tensorprodukt mit Algorithmus 1.32 (Zerlegung in ein äußeres Tensorprodukt, S. 32)

$$\mu^M = \mu_1 \# \ldots \# \mu_k,$$

wobei M eine monomiale Matrix ist.

2. Zerlege rekursiv die Darstellungen $\mu_i,\ i = 1 \ldots k$

$$\mu_i^{A_i} = \bigoplus_{j=1}^{r_i} \rho_{i,j}.$$

3. Bestimme eine Permutationsmatrix P, so daß

$$(\bigoplus_{j=1}^{r_1} \rho_{1,j} \# \ldots \# \bigoplus_{j=1}^{r_k} \rho_{k,j})^P = \bigoplus_{j_1=1}^{r_1} \cdots \bigoplus_{j_k=1}^{r_k} (\rho_{1,j} \# \ldots \# \rho_{k,j}).$$

P hängt nur ab von den Graden der $\rho_{i,j}$. Die Berechnung ist ein einfaches kombinatorisches Problem.

Es ist $A = M \cdot \bigotimes_{i=1}^{k} A_i \cdot P$ eine Zerlegungsmatrix für μ und

$$\mu^A = \bigoplus_{j_1=1}^{r_1} \cdots \bigoplus_{j_k=1}^{r_k} (\rho_{1,j} \# \ldots \# \rho_{k,j}).$$

Fall 8: Ist $\mu^D = \lambda_H \uparrow_T G$, dann gibt es einen Normalteiler N mit $H \leq N \overset{p}{\trianglelefteq} G$ und p prim

1. Zerlege $\mu^{D_1} = \lambda_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29). D_1 ist eine Diagonalmatrix.

2. Bestimme N mit $H \leq N \overset{p}{\trianglelefteq} G$. Bilde dazu den normalen Abschluß $\overline{H}$ von H in G und berechne eine Kompositionsreihe von $G/\overline{H}$.

3. Zerlege $\lambda_H \uparrow_T G$ mit einer monomialen Matrix M in eine zweifache Induktion

$$(\lambda_H \uparrow_T G)^M = (\lambda_H \uparrow_{T_1} N) \uparrow_{T_2} G,$$

so daß $T_2 = (t^0, t^1 \ldots t^{(p-1)})$. M ist nach Satz 1.4 auf S. 16 die Matrix zum Transversalenwechsel $T \to T_1 T_2$ und wird bestimmt mit Algorithmus 1.2 (Transversalenwechsel, S. 15).

4. Zerlege rekursiv $\lambda_H \uparrow_{T_1} N$ mit B, das heißt
$$(\lambda_H \uparrow_{T_1} N)^B = \bigoplus_{i=1}^{k} \rho_i.$$

5. Fasse die ρ_i bzgl. Gleichheit zusammen. Alle folgenden Berechnungen müssen dann nur noch für jeweils eine Irreduzible einer Gruppe Gleicher ausgeführt werden. Permutationen zum Umsortieren der ρ_i werden dann auf diesen Gruppen ausgeführt.

6. Bestimme die ρ_i, welche eine Erweiterung $\overline{\rho}_i$ auf G besitzen (vgl. Satz 1.71 von Clifford, S. 56). Diese nennen wir η_ℓ und bezeichnen die direkte Summe dieser mit η:
$$\eta = \bigoplus_{\ell=1}^{k} \eta_\ell.$$
Verwende dabei, daß ρ_i genau dann eine Erweiterung besitzt, wenn $\rho_i \cong \rho_i^t$. Um das zu entscheiden, werden die Charakterwerte der ρ_i vorberechnet sowie die Permutation, die von t auf den Konjugationsklassen von N induziert wird. Es gilt genau dann $\rho_i \cong \rho_i^t$, wenn die Liste der Charakterwerte von ρ_i invariant ist unter dieser Permutation.

7. Bestimme für die ρ_i, welche keine Erweiterung besitzen, ob sie innere Konjugierte sind bzgl. einer Potenz t^j, $j = 1 \dots p-1$.
Verwende hierzu wieder die Liste der Charakterwerte und die von t^j induzierte Permutation auf diesen. Beachte, daß zwei solche inneren Konjugierten dies nur bis auf Äquivalenz sind.

8. Berechne eine Permutationsmatrix P_1, welche die ρ_i so sortiert, daß zuerst die erweiterbaren kommen und dann die anderen, sortiert nach innerer Konjugation in Gruppen (nur bis auf Äquivalenz!) der Form
$$\rho, \dots, \rho, \rho^t, \dots, \rho^t, \dots, \rho^{t^{(p-1)}}, \dots, \rho^{t^{(p-1)}}.$$

9. Berechne eine Blockdiagonalmatrix D_2, welche die Irreduziblen in obigen Gruppen so konjugiert, daß Gleichheit gilt (das bedeutet: eine Darstellung, welche $\cong \rho^t$ ist, wird so konjugiert, daß sie danach $= \rho^t$ ist). Hierzu werden nach Satz 1.56 (Berechnung des Intertwiningraums, S. 46) lineare Gleichungen gelöst. Auf den erweiterbaren ρ_i ist D_2 die Identität. Die direkte Summe einer Gruppe von inneren Konjugierten bezeichnen wir mit ν_ℓ, $\ell = 1 \dots m$:
$$\nu_\ell = \rho \oplus \dots \oplus \rho \oplus \rho^t \oplus \dots \oplus \rho^t \oplus \dots \oplus \rho^{t^{(p-1)}} \oplus \dots \oplus \rho^{t^{(p-1)}}.$$
Die Matrix $B \cdot P_1 \cdot D_2$ ist nun ebenfalls eine Zerlegungsmatrix für $\lambda_H \uparrow_{T_1} N$ und es gilt
$$(\lambda_H \uparrow_{T_1} N)^{B \cdot P_1 \cdot D_2} = \eta \oplus \nu_1 \oplus \dots \oplus \nu_m$$

und

$$((\lambda_H \uparrow_{T_1} N) \uparrow_{T_2} G)^{\mathbf{1}_p \otimes B \cdot P_1 \cdot D_2} = (\eta \oplus \nu_1 \oplus \ldots \oplus \nu_m) \uparrow_{T_2} G$$

nach Satz 1.6 auf S. 17.

10. Berechne eine Permutationsmatrix P_2 nach Satz 1.5 auf S. 17, welche die Induktion der direkten Summe in obiger Gleichung zerlegt in eine direkte Summe von Induktionen. Hierbei wird η als ein Summand betrachtet und die irreduziblen Summanden der ν_ℓ als die weiteren.

11. Erweitere η durch $\overline{\eta}$ auf G. Erweitere hierzu die einzelnen Summanden mit Algorithmus 1.74 (Erweiterung ohne Charakter, S. 58) oder mit der Erweiterungsformel 1.41 von Minkwitz auf S. 36.

12. Werte $\overline{\eta}$ an der Stelle t aus und berechne die Blockdiagonalmatrix

$$D_3 = \bigoplus_{i=0}^{p-1} \overline{\eta}(t)^i.$$

Es gilt $(\eta \uparrow_{T_2} G)^{D_3} = (1_N \uparrow_{T_2} G) \otimes \overline{\eta}$ nach Satz 1.15 auf S. 22. Die Darstellung $1_N \uparrow_{T_2} G$ ist eine reguläre Darstellung von $G/N \cong \mathsf{Z}_p$. D_3 hat den Grad $p \cdot \deg(\eta)$.

13. Berechne die p eindimensionalen Darstellungen $\lambda^0, \lambda^1, \ldots, \lambda^{p-1}$ von G/N. Es gilt

$$((1_N \uparrow_{T_2} G) \otimes \overline{\eta})^{\mathrm{DFT}_p \otimes \mathbf{1}_{\deg(\eta)}} = \bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^{k} \lambda^i \cdot \eta_\ell,$$

was in Irreduzible zerlegt ist.

14. Bestimme eine Blockdiagonalmatrix D_4, welche die Induktionen der Summanden der ν_ℓ auf Gleichheit konjugiert.

Die Induktionen der irreduziblen Summanden der ν_ℓ sind bereits irreduzibel. Die Summanden eines ν_ℓ liefern bei Induktion äquivalente Ergebnisse, das heißt $\rho \uparrow G \cong \rho^{t^i} \uparrow G$. Diese können nach dem Satz 1.71 von Clifford mit einer Matrix D_4 auf Gleichheit mit $\rho \uparrow_T G$ konjugiert werden. D_4 hat den Grad $n - p \cdot \deg(\eta)$.

15. Sortiere die Irreduziblen mit einer Permutationsmatrix P_3.

Beachte, daß gleiche Irreduzible bereits nebeneinander stehen.

Es ist

$$A = D_1 \cdot M \cdot (\mathbf{1}_p \otimes B \cdot P_1 \cdot D_2) \cdot P_2 \cdot ((D_3 \cdot (\mathrm{DFT}_p \otimes \mathbf{1}_{\deg(\eta)})) \oplus D_4) \cdot P_3$$

eine Zerlegungsmatrix für μ mit Zerlegung

$$\mu^A = \left(\bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^{k} \lambda^i \cdot \eta_\ell \oplus \bigoplus_{\ell=1}^{m} \underbrace{(\nu_{\ell,1} \uparrow_{T_2} G \oplus \ldots \oplus \nu_{\ell,1} \uparrow_{T_2} G)}_{N_\ell} \right)^{P_3},$$

wobei N_ℓ die Anzahl der Summanden von ν_ℓ und $\nu_{\ell,1}$ den ersten Summanden von ν_ℓ bezeichnet.

Fall 9: $\boldsymbol{\mu}$ ist eine Permutationsdarstellung und es gibt einen regulär dargestellten abelschen Normalteiler von $\boldsymbol{G/\ker(\mu)}$

1. Berechne einen Normalteiler N, $\ker(\mu) \leq N \trianglelefteq G$, so daß $N/\ker(\mu)$ abelsch ist und von μ regulär dargestellt wird. Notwendig ist, daß $|N| = \deg(\mu)$.
2. Zerlege μ mit Algorithmus 2.1 bzgl N.

Fall 10: Ist $\boldsymbol{\mu^D = \lambda_H \uparrow_T G}$, dann besitzt $\boldsymbol{\lambda_H}$ eine Erweiterung auf $\boldsymbol{G}$

1. Zerlege $\mu^{D_1} = \lambda_H \uparrow_T G$ mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29). D_1 ist eine Diagonalmatrix.
2. Erweitere λ_H durch λ_G auf G. λ_G ist ein Charakter von G vom Grad 1. Man beachte, daß dazu nicht die ganze Charaktertafel berechnet werden muß, sondern nur die Charaktere der abelschen Gruppe G/G' (G' ist die Kommutatorgruppe von G).
3. Berechne $D_2 = \operatorname{diag}(\lambda_G(t) \mid t \in T)$.
4. Zerlege rekursiv $1_H \uparrow_T G$ durch B, das heißt

$$(1_H \uparrow_T G)^B = \bigoplus_{i=1}^{k} \rho_i,\ \deg(\rho_i) = 1,\ i = 1 \ldots k.$$

Es ist $A = D_1 \cdot D_2 \cdot B$ eine Zerlegungsmatrix für μ und $\mu^A = \bigoplus_{i=1}^{k} \lambda_G \cdot \rho_i$. Man beachte, daß mit den ρ_i auch die $\lambda_G \cdot \rho_i$ geordnet sind. ∎

Der weitaus mächtigste Teil von Algorithmus 2.2 ist gegeben durch Fall 8. Er allein erlaubt es, eine monomiale Darstellung $\mu = \lambda_H \uparrow_T G$ der auflösbaren Gruppe G zu zerlegen, wenn H subnormal in G ist, das heißt wenn es eine Kompositionsreihe von G gibt, die H enthält.
Die Zerlegung einer Permutationsdarstellung mit abelschem, regulär dargestellten Normalteiler ist eine weitere Methode, die unter anderem einen Teil der primitiven Permutationsdarstellungen erledigt. Im folgenden Lemma werden wir zeigen, daß die beiden Methoden nicht kollidieren, das heißt besitzt eine Permutationsdarstellung $\pi = 1_H \uparrow_T G$ einen abelschen, regulär dargestellten Normalteiler und einen Normalteiler $N \trianglelefteq G$ von Primzahlindex p, dann besitzt auch $1_H \uparrow N$ einen abelschen, regulär dargestellten Normalteiler.

2.3 Lemma Sei $\pi = 1_H \uparrow G$ eine Permutationsdarstellung von G mit Kern $\ker(\pi) = \operatorname{core}(H)$. Es gebe einen Normalteiler N, so daß $N/\operatorname{core}(H)$ abelsch ist und von π regulär dargestellt wird sowie einen Normalteiler K mit $H \leq K \trianglelefteq G$. Nach Lemma 1.64 auf S. 50 ist dann $H \cap N = \operatorname{core}(H)$ und $HN = G$.
Die abelsche Gruppe $(K \cap N)/\operatorname{core}(H)$ wird von $1_H \uparrow K$ regulär dargestellt.

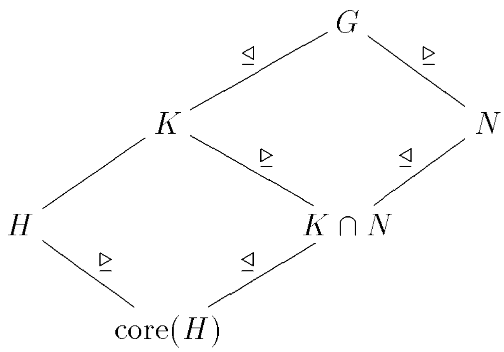

Abbildung 2.1: Situation in Lemma 2.3

Beweis Es gilt $(N : (K \cap N)) = (NK : K) = (G : K)$, $(H \cap (K \cap N)) = \mathrm{core}(H)$ und $H(K \cap N) = K$ (vgl. Abbildung 2.1). Daraus folgt mit Korollar 1.14 auf S. 22

$$(1_H \uparrow K) \downarrow (K \cap N) \cong 1_{\mathrm{core}(H)} \uparrow (K \cap N),$$

was regulär ist. ∎

Wird eine monomiale Darstellung $\mu = \lambda_H \uparrow_T G$ ausschließlich mit Fall 8 in Algorithmus 2.2 zerlegt, das heißt $\mu^A = \rho = \bigoplus_{i=1}^n \rho_i$, dann gibt es eine Kette $\mathcal{T}$ von Normalteilern

$$H = N_{k+1} \trianglelefteq N_k \trianglelefteq \ldots \trianglelefteq G = N_1, \ (N_i : N_{i+1}) \text{ ist prim}, \ i = 1 \ldots k,$$

die bei der Zerlegung gewählt worden sind. In diesem Fall besitzt die Zerlegung zwei zusätzliche Eigenschaften. Zum einen ist sie nach Konstruktion $\mathcal{T}$-adapted im Sinne von Clausen/Baum, das heißt es gilt (vgl. [16], S. 96):

1. Die Einschränkungen $\rho \downarrow N_i$, $i = 1 \ldots k+1$, sind *gleich* einer Summe von irreduziblen Darstellungen.

2. Ähnliche irreduzible Komponenten in $\rho \downarrow N_i$ sind gleich.

Das Konzept von $\mathcal{T}$-adapted Zerlegungen wird in [16] verwendet, um Aussagen zur Komplexität schneller Fouriertransformationen zu gewinnen.
Eine weitere Eigenschaft der gewonnenen Zerlegung ist, daß jede Irreduzible ρ_i, welches ähnlich ist zu einer monomialen Darstellung, *gleich* ist zu einer monomialen Darstellung. Woran liegt das? Nehmen wir an, ϕ ist eine irreduzible Komponente von $\lambda_H \uparrow N_i$. Dann gibt es nach dem Satz 1.71 von Clifford auf S. 56 zwei Möglichkeiten: entweder die Induktion $\phi \uparrow N_{i-1}$ ist irreduzibel, oder ϕ besitzt eine Erweiterung $\overline{\phi}$ auf N_{i-1}. Der erste Fall erzeugt aus einer monomialen Darstellung wieder eine monomiale Darstellung, im zweiten Fall muß nach Algorithmus 1.74 (Erweiterung ohne Charakter, S. 58) eine Matrix M aus dem eindimensionalen Raum $\mathsf{Int}(\phi, \phi^t)$, $t \in N_{i-1} \setminus N_i$ (Differenz) berechnet werden und $\overline{\phi}$ ist monomial genau dann, wenn M und damit jede Matrix $\neq \mathbf{0}$, $\in \mathsf{Int}(\phi, \phi^t)$ monomial ist.

2.2 Ein Beispiel

Zum Abschluß dieses Kapitels wollen wir ein ausführliches Beispiel zu Algorithmus 2.2 rechnen.

2.4 Beispiel Der Übersichtlichkeit wegen geben wir die folgenden Gruppen nicht durch Erzeugende und Relationen an, sondern als Permutationsgruppen. Sei

$$G = \langle (1,2,3,4),(1,2)\rangle \cong \mathsf{S}_4$$

die symmetrische Gruppe auf 4 Punkten mit Darstellung

$$\begin{aligned} \mu: \quad (1,2,3,4) &\mapsto [\,(1,10,17,19)(2,9,18,20)(3,12,14,21) \\ &\qquad (4,11,13,22)(5,7,16,23)(6,8,15,24),\ \ 24\,], \\ (1,2) &\mapsto [\,(1,7)(2,8)(3,9)(4,10)(5,11)(6,12)(13,15) \\ &\qquad (14,16)(17,18)(19,21)(20,22)(23,24),\ \ 24\,]. \end{aligned}$$

μ ist transitiv vom Grad 24, also eine reguläre Darstellung von G. Wir wollen die einzelnen Schritte von Algorithmus 2.2 Schritt für Schritt durchführen. Man sieht leicht ein, daß erst Fall 8 anwendbar ist.

1. Mit Algorithmus 1.26 (Zerlegung in eine Induktion, S. 29) zerlegen wir μ in

$$\mu^{D_1} = (1_H \uparrow_T G),$$

mit $D_1 = \mathbf{1}_{24}$, $H = \mathsf{E}$ und

$$\begin{aligned} T \quad = \quad &(\,(1),(3,4),(2,3),(2,3,4),(2,4,3),(2,4),(1,2),(1,2)(3,4), \\ &(1,2,3),(1,2,3,4),(1,2,4,3),(1,2,4),(1,3,2),(1,3,4,2), \\ &(1,3),(1,3,4),(1,3)(2,4),(1,3,2,4),(1,4,3,2),(1,4,2), \\ &(1,4,3),(1,4),(1,4,2,3),(1,4)(2,3)\,). \end{aligned}$$

2. Es gibt nur einen Normalteiler $N \trianglelefteq G$ von Primzahlindex, nämlich

$$N = \langle (1,3,2),(1,4)(2,3)\rangle \cong \mathsf{A}_4$$

und es ist $(G:N) = p = 2$.

3. Wir zerlegen $1_{\mathsf{E}} \uparrow_T G$ mit Algorithmus 1.2 (Transversalenwechsel, S. 15) in eine zweifache Induktion, das heißt

$$(1_{\mathsf{E}} \uparrow_T G)^M = (1_{\mathsf{E}} \uparrow_{T_1} N) \uparrow_{T_2} G$$

mit

$$\begin{aligned} M \quad &= \quad [\,(2,22,19,21,11,14,18,17,9,5,3,23,20,10,13,7,15,16,8,4) \\ &\qquad (6,24,12),\ \ 24\,], \\ T_1 \quad &= \quad (\,(1),(2,3,4),(2,4,3),(1,2)(3,4),(1,2,3),(1,2,4),(1,3,2), \\ &\qquad (1,3,4),(1,3)(2,4),(1,4,2),(1,4,3),(1,4)(2,3)\,), \\ T_2 \quad &= \quad (\,(1),(1,2,3,4)\,). \end{aligned}$$

Die Transversale $T_2 = (t^0, t^1)$ wird erzeugt von $t = (1,2,3,4)$.

4. Wir zerlegen rekursiv die reguläre Darstellung $1_{\mathsf{E}} \uparrow_{T_1} N$ von N. Die einzelnen Schritte hierzu wollen wir nicht ausführen, sondern lediglich das Ergebnis angeben. Es ist

$$(1_{\mathsf{E}} \uparrow_{T_1} N)^B = \rho_1 \oplus \rho_2 \oplus \rho_3 \oplus \rho_4 \oplus \rho_4 \oplus \rho_4,$$

wobei die ρ_i durch

$$\begin{array}{lll} \rho_1 = 1_N & & \\ \rho_2: & (1,3,2) \mapsto \omega_3^2, & (1,4)(2,3) \mapsto 1, \\ \rho_3: & (1,3,2) \mapsto \omega_3, & (1,4)(2,3) \mapsto 1, \\ \rho_4: & (1,3,2) \mapsto [\,(1,2,3),\ 3\,], & (1,4)(2,3) \mapsto \mathrm{diag}(1,-1,-1), \end{array}$$

und die Zerlegungsmatrix B durch

$$\begin{aligned} B \;=\; & [\,(2,6,7,5,9,3,11,8,10,12,4),\ 12\,]\cdot \\ & (\mathbf{1}_3 \otimes [\,(2,3),\ 4\,] \cdot (\mathrm{DFT}_2 \otimes \mathrm{DFT}_2) \cdot [\,(2,4),\ 4\,]) \cdot \\ & [\,(2,4,8,9,3,12,7,10,6,5),\ 12\,]\cdot \\ & (\mathrm{DFT}_3 \oplus \mathbf{1}_9) \cdot [\,(2,3),\ 12\,] \end{aligned}$$

gegeben sind.

5. Es sind die 4 paarweise nicht äquivalenten irreduziblen Darstellungen $\rho_1, \ldots, \rho_4$ zu betrachten.

6. Es ist $(\,(1),(2,3,4),(2,4,3),(1,2)(3,4)\,)$ ein Vertretersystem der Konjugiertenklassen von N. Die Charaktere der ρ_i sind gegeben durch ihre Werte auf den Konjugiertenklassen:

$$\chi_{\rho_1}:\ (1,1,1,1),\ \ \chi_{\rho_2}:\ (1,\omega_3^2,\omega_3,1),\ \ \chi_{\rho_3}:\ (1,\omega_3,\omega_3^2,1),\ \ \chi_{\rho_4}:\ (3,0,0,-1).$$

Der Transversalenerzeuger t permutiert die Konjugationsklassen wie $(2,3)$, also besitzt ρ_i eine Erweiterung auf G genau dann, wenn die Liste der Charakterwerte invariant unter $(2,3)$ ist. Damit besitzen ρ_1 und ρ_4 eine Erweiterung auf G und es ist

$$\eta_1 = \rho_1,\ \ \eta_2 = \eta_3 = \eta_4 = \rho_4,\ \ \eta = \bigoplus_{i=1}^{4} \eta_i.$$

7. ρ_2 und ρ_3 besitzen keine Erweiterung auf G. Die Charakterwerte zeigen $\rho_2^t \cong \rho_3$, und da beide den Grad 1 haben gilt sogar $\rho_2^t = \rho_3$.

8. Die Permutationsmatrix $P_1 = [\,(2,11,9,7,5,3,12,10,8,6,4),\ 12\,]$ konjugiert die Irreduziblen ρ_i in die Reihenfolge

$$\rho_1 \oplus \rho_4 \oplus \rho_4 \oplus \rho_4 \oplus \rho_2 \oplus \rho_2^t.$$

9. Da bereits $\rho_2^t = \rho_3$ gilt, kann $D_2 = \mathbf{1}_{12}$ gewählt werden. Es ist $\nu_1 = \rho_2 \oplus \rho_2^t$ und
$$(1_{\mathsf{E}} \uparrow_{T_1} N)^{B \cdot P_1 \cdot D_2} = \eta \oplus \nu_1,$$
bzw.
$$((1_{\mathsf{E}} \uparrow_{T_1} N) \uparrow_{T_2} G)^{\mathbf{1}_2 \otimes B \cdot P_1 \cdot D_2} = (\eta \oplus \nu_1) \uparrow_{T_2} G.$$

10. Mit Satz 1.5 auf S. 17 finden wir
$$P_2 = [\,(11,13,15,17,19,21)(12,14,16,18,20,22,23),\;\; 24\,]$$
und es gilt
$$((\eta \oplus \nu_1) \uparrow_{T_2} G)^{P_2} = (\eta \uparrow_{T_2} G) \oplus (\rho_2 \uparrow_{T_2} G) \oplus (\rho_2^t \uparrow_{T_2} G).$$

11. Wir erweitern η auf G. Die Darstellung $\eta_1 = \rho_1 = 1_N$ besitzt offenbar die Erweiterung $\overline{\eta}_1 = 1_G$, $\eta_2 = \rho_4$ wird erweitert mit Minkwitz oder Algorithmus 1.74 (Erweiterung ohne Charakter, S. 58) zu
$$\overline{\eta}_2 :\; (1,2,3,4) \mapsto [\,(1,2),\;(-1,1,1)\,],\;\; (1,2) \mapsto [\,(1,3),\;(-1,-1,-1)\,].$$
Es gilt $\overline{\eta}_2 = \overline{\eta}_3 = \overline{\eta}_4 = \overline{\rho}_4$ und
$$\overline{\eta} = \bigoplus_{i=1}^{4} \eta_i.$$

12. Es ist $\overline{\eta}(t) = [\,(2,3)(5,6)(8,9),\;(1,-1,1,1,-1,1,1,-1,1,1)\,]$ und damit
$$D_3 = \mathbf{1}_{10} \oplus \overline{\eta}(t).$$
D_3 zerlegt $\eta \uparrow_{T_2} G$ in ein Tensorprodukt
$$(\eta \uparrow_{T_2} G)^{D_3} = (1_N \uparrow_{T_2} G) \otimes \overline{\eta}.$$

13. Es ist
$$\lambda :\; (1,2,3,4) \mapsto -1,\;\; (1,2) \mapsto -1,$$
die erzeugende eindimensionale Darstellung von G/N und
$$((1_N \uparrow_{T_2} G) \otimes \overline{\eta})^{\mathrm{DFT}_2 \otimes \mathbf{1}_{10}} = \bigoplus_{i=1}^{2} \bigoplus_{j=1}^{4} \lambda^i \cdot \overline{\eta}_j$$
ist in Irreduzible zerlegt.

14. Es gilt $(\rho_2^t \uparrow_{T_2} G)^{[(1,2),2]} = (\rho_2 \uparrow_{T_2} G)$, also ist $D_4 = [\,(3,4),\;4\,]$.

15. Die Irreduziblen werden nach Grad sortiert durch

$$\begin{aligned} P_4 \;=\; & [\,(2,16,11)(3,17,12,7,21)(4,18,13,8,22) \\ & (5,19,14,9,23)(6,20,15,10,24),24),\;\; 24\,]. \end{aligned}$$

Nach Vereinfachungen ergibt sich

$$\mu^A = 1_G \oplus \lambda \oplus (\rho_2 \uparrow_{T_2} G) \oplus (\rho_2 \uparrow_{T_2} G) \oplus \lambda \cdot \overline{\rho}_4 \oplus \lambda \cdot \overline{\rho}_4 \oplus \lambda \cdot \overline{\rho}_4 \oplus \overline{\rho}_4 \oplus \overline{\rho}_4 \oplus \overline{\rho}_4,$$

mit

$$\begin{aligned} A \;=\; & [\,(2,22,19,21,11,14,18,17,9,5,3,23,20,10,13,7,15,16,8,4) \\ & (6,24,12),\;\; 24\,]\cdot \\ & (\mathbf{1}_2 \otimes B)\cdot \\ & [\,(2,21,17,12,10,8,6,4)(3,24,20,15,23,18,14,22,19,16,13,11,9,7,5), \\ & (1,1,1,1,1,1,1,1,1,1,1,1,-1,1,1,-1,1,1,-1,1,1,1,1,1,1)\,]\cdot \\ & ((\mathrm{DFT}_2 \otimes \mathbf{1}_{10}) \oplus \mathbf{1}_4)\cdot \\ & [\,(2,16,11)(3,17,12,7,21)(4,18,13,8,22)(5,19,14,9,23) \\ & (6,20,15,10,24),\;\; 24\,]. \end{aligned}$$

Die vollständige Zerlegung der Darstellung μ mit der implementierten Funktion `DecompositionMonRep` (siehe Anhang) benötigt 4.5 s CPU-Zeit auf einer SUN Ultra-Sparc 150 MHz. ∎

3

Symmetrie und Zerlegung von Matrizen

In diesem Kapitel wollen wir den Begriff *Symmetrie* für Matrizen einführen und erklären, wie aus der Symmetrie eine Zerlegung der Matrix gewonnen werden kann. Allgemein ist eine Symmetrie einer $(m \times n)$-Matrix gegeben durch ein Paar (ϕ_1, ϕ_2) von Darstellungen derselben Gruppe G, so daß M im Intertwiningraum $\mathsf{Int}(\phi_1, \phi_2)$ von ϕ_1 und ϕ_2 liegt, das heißt

$$\phi_1(g) \cdot M = M \cdot \phi_2(g) \text{ für alle } g \in G.$$

Wir nennen G eine *Symmetriegruppe* von M. Betrachtet man diese allgemeine Definition, dann besitzt jede Matrix beliebig viele Symmetrien. Ist beispielsweise M eine invertierbare $(n \times n)$-Matrix und ϕ irgendeine Darstellung vom Grad n einer beliebigen Gruppe G, dann gilt $M \in \mathsf{Int}(\phi, \phi^M)$, das heißt M besitzt die Symmetrie (ϕ, ϕ^M).
Die Bestimmung der Symmetrie eines bestimmten Typs einer Matrix ist der duale Operator zur Bestimmung des Intertwiningraums zu einem Paar von Darstellungen (vgl. 1.5): der Intertwiningraum eines Paars (ϕ_1, ϕ_2) von Darstellungen ist genau die Menge der Matrizen, welche die Symmetrie (ϕ_1, ϕ_2) besitzen.
Die speziellen Symmetrietypen, die in den drei Abschnitten dieses Kapitels behandelt werden, entstehen durch einschränkende Bedingungen an die Darstellungen ϕ_1 und ϕ_2. Beispielsweise fordert die Definition der *Perm-Perm-Symmetrie* (siehe Abschnitt 3.2), daß ϕ_1 und ϕ_2 Permutationsdarstellungen sind. Ist zum Beispiel

$$M = \begin{bmatrix} a & b \\ b & a \end{bmatrix}, \ a, b \in \mathbb{K},$$

und

$$\mathsf{Z}_2 = \langle x \mid x^2 = 1 \rangle, \ \phi : \ x \mapsto [(1,2), 2],$$

dann gilt $M \in \mathsf{Int}(\phi, \phi)$, das heißt M besitzt die Symmetrie (ϕ, ϕ). Offensichtlich bedeutet Perm-Perm-Symmetrie von M die Existenz von Paaren von Permutationen (σ_1, σ_2), so daß Permutieren der Zeilen von M mit σ_1 zum gleichen Ergebnis

führt, wie Permutieren der Spalten von M mit σ_2. Enthält also eine Matrix paarweise verschiedene Einträge, so besitzt sie nur die triviale Perm-Perm-Symmetrie.
Die Zerlegung einer Matrix anhand einer Symmetrie ist unabhängig vom Symmetrietyp und wird im folgenden beschrieben. Sei $M \in \mathbb{K}^{m \times n}$ eine Matrix mit Symmetrie (ϕ_1, ϕ_2), das heißt $M \in \mathsf{Int}(\phi_1, \phi_2)$. Zunächst bestimmt man zwei Zerlegungsmatrizen A_1, A_2 von ϕ_1 bzw. ϕ_2. Dann sind $\phi_1^{A_1} = \rho_1$ und $\phi_2^{A_2} = \rho_2$ jeweils eine direkte Summe vom Irreduziblen. Es folgt, daß die Matrix $D = A_1^{-1} \cdot M \cdot A_2 \in \mathsf{Int}(\rho_1, \rho_2)$ im Intertwiningraum zweier vollständig zerlegter Darstellungen liegt (siehe Abbildung 3.1).

$$\begin{tikzcd}
\phi_1 \arrow[r, "M"] \arrow[d, "A_1"] & \phi_2 \arrow[d, "A_2"] \\
\rho_1 \arrow[r, "D"] & \rho_2
\end{tikzcd}$$

Abbildung 3.1: Zerlegung einer Matrix mit Symmetrie (ϕ_1, ϕ_2)

Nach Satz 1.48 ist D eine blockpermutierte Matrix. Auflösen nach M ergibt die Zerlegung
$$M = A_1 \cdot D \cdot A_2^{-1}.$$
Zerlegt man verschiedene Matrizen mit gleicher Symmetrie, so variiert lediglich die blockpermutierte Matrix D.
Die Matrizen A_1, A_2^{-1} in dieser Zerlegung sind im allgemeinen Fall jedoch keineswegs dünn besetzt oder überhaupt strukturiert. Außerdem sind Zerlegungsmatrizen für beliebige Darstellungen nur schwer zu finden. Die Motivation für die Betrachtung von Symmetrien, bei denen ϕ_1 und ϕ_2 Permutations- bzw. monomiale Darstellungen sind, liegt in der Tatsache, daß in diesen Fällen die Matrizen A_1 und A_2 mit Algorithmus 2.2 als Produkt dünn besetzter Matrizen gewonnen werden können und darüber hinaus noch erheblich mehr Struktur besitzen. Genauer gesagt sind sie im wesentlichen zusammengesetzt aus monomialen Matrizen und DFTs kleinen Grades mit Hilfe der Operatoren $\cdot$ (Produkt), $\oplus$ und $\otimes$. Die Zerlegung $M = A_1 \cdot D \cdot A_2^{-1}$ ist damit als schneller Algorithmus für die Multiplikation mit M nutzbar. Die Anwendungen gehen darüber aber weit hinaus. Verwendet man bekannte Sätze über das Verhalten von Funktionen wie Determinante, Eigenwerte und Inverse einer Matrix unter den genannten Operatoren, so ist eine (in unserem Sinne) zerlegte Matrix in vielerlei Hinsicht gut zu handhaben.
Anschaulich gesprochen erfaßt eine Symmetrie der in diesem Kapitel betrachteten Typen einen Teil der Redundanz in der Matrix. Die Zerlegung der Symmetrie macht es dann möglich, diese Redundanz in eine Zerlegung der Matrix umzusetzen.

Um eine Matrix M automatisch zu zerlegen, müssen also die folgenden beiden Schritte ausgeführt werden:

1. Bestimme die Symmetrie eines bestimmten Typs von M.

2. Zerlege M anhand dieser Symmetrie.

Der erste Punkt war Gegenstand der Dissertation von Egner (1997), [26], in deren Rahmen auch Algorithmen zur Symmetriefindung implementiert wurden. Zusammen mit den implementierten Algorithmen der vorliegenden Arbeit entstand ein Programm in der Programmiersprache GAP [57], das Matrixzerlegungen automatisch generiert.
Die drei Abschnitte dieses Kapitels entsprechen den drei betrachteten Symmetrietypen: Perm-Irred-Symmetrie in Abschnitt 3.1, Perm-Perm-Symmetrie in Abschnitt 3.2 und schließlich Mon-Mon-Symmetrie in Abschnitt 3.3. Es wird jeweils der Symmetrietyp definiert und ein Algorithmus zur Matrixzerlegung anhand dieser Symmetrie beschrieben. Die vorhandenen Algorithmen zum Finden von Perm-Irred-Symmetrie und Perm-Perm-Symmetrie werden kurz vorgestellt. In Abschnitt 3.3 wird ein Algorithmus hergeleitet, der in der Lage ist, eine große Klasse von Mon-Mon-Symmetrie zu berechnen.
Für eine genaue strukturelle Beschreibung der Symmetrien und der Algorithmen zum Finden von Perm-Irred-Symmetrie und Perm-Perm-Symmetrie verweisen wir auf die Dissertation von Egner (1997), [26]. Die Idee zur Zerlegung einer Matrix anhand von Symmetrie stammt aus Minkwitz (1993), [45], wo bereits Perm-Irred-Symmetrie und Perm-Perm-Symmetrie zur Algorithmengenerierung verwendet werden. Zerlegungsbeispiele finden sich in Kapitel 4. Zur Notation siehe Abschnitt 1.2. Die Maschke-Bedingung soll, wie auch in den übrigen Kapiteln, stets erfüllt sein.

3.1 Perm-Irred-Symmetrie

3.1 Definition *Sei $M \in \mathsf{GL}_n(\mathbb{K})$. Ein Paar von Darstellungen (ϕ, ρ) derselben Gruppe G heißt „Perm-Irred-Symmetrie“ von M, wenn $M \in \mathsf{Int}(\phi, \rho)$, ϕ eine Permutationsdarstellung ist, und*

$$\rho = (\rho_1 \oplus \ldots \oplus \rho_k)^{[\sigma,n]} \text{ für ein } \sigma \in \mathsf{S}_n,\ \rho_i \text{ irreduzibel },\ i = 1 \ldots n,$$

eine permutierte direkte Summe irreduzibler Darstellungen von G ist.

Die Bedingung, die an ρ gestellt wird, läßt sich auch so formulieren: es gibt eine Permutation $\sigma \in \mathsf{S}_n$, so daß $M \cdot [\sigma^{-1}, n]$ eine Zerlegungsmatrix für ϕ ist. Man beachte, daß es für die Existenz einer Perm-Irred-Symmetrie notwendig ist, daß die Matrix quadratisch und invertierbar ist. Zunächst einige Beispiele.

3.2 Beispiel Ist $\mathsf{Z}_3 = \langle x \mid x^3 = 1 \rangle$, $\phi: \ x \mapsto [(1,2,3),3]$ die reguläre Darstellung von Z_3 sowie $\rho: \ x \mapsto \mathrm{diag}(1, \omega_3, \omega_3^2)$ deren Zerlegung, dann besitzt DFT_3 die Perm-Irred-Symmetrie (ϕ, ρ).
Ist $\mathsf{S}_3 = \langle x, y \mid x^3 = y^2 = 1, x^y = x^{-1} \rangle$, mit Darstellung auf drei Punkten

$$\psi: \ x \mapsto [(1,2,3),3], \ y \mapsto [(2,3),3],$$

und den beiden in Irreduzible zerlegten Darstellungen

$$\rho_1: \ x \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega_3 & 0 \\ 0 & 0 & \omega_3^2 \end{bmatrix}, \ y \mapsto [(2,3),3],$$

und

$$\rho_2: \ x \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix}, \ y \mapsto [(2,3),3],$$

dann besitzt DFT_3 auch die Perm-Irred-Symmetrie (ψ, ρ_1). Die Matrix

$$\mathrm{SOR}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix}$$

besitzt die Perm-Irred-Symmetrie (ψ, ρ_2). Die Einschränkung $\phi = \psi \downarrow \mathsf{Z}_3$ wird von SOR_3 aber nicht in Irreduzible zerlegt! Allgemeiner besitzt die Matrix DFT_n die Perm-Irred-Symmetrie (ϕ, ρ) der Gruppe $\mathsf{Z}_n = \langle x \mid x^n = 1 \rangle$ mit Darstellungen

$$\phi: \ x \mapsto [(1,\ldots,n),n], \ \rho: \ x \mapsto \mathrm{diag}(\omega_n^0, \ldots, \omega^{(n-1)}).$$

Es gilt $\phi^{\mathrm{DFT}_n} = \rho$. ∎

Jetzt wenden wir uns der Zerlegung einer Matrix anhand ihrer Perm-Irred-Symmetrie zu. Sei dazu $M \in \mathsf{GL}_n(\mathbb{K})$ mit Perm-Irred-Symmetrie (ϕ, ρ), wobei ϕ und ρ Darstellungen von G sind und

$$\rho = (\rho_1 \oplus \ldots \oplus \rho_k)^{[\sigma,n]}, \ \rho_i \text{ irreduzibel}, \ i = 1 \ldots k, \ \sigma \in \mathsf{S}_n.$$

Sei A_ϕ eine Zerlegungsmatrix von ϕ im Sinne von Kapitel 2, das heißt

$$\phi^{A_\phi} = \psi = \bigoplus_{i=1}^{\ell} \underbrace{(\psi_i \oplus \ldots \oplus \psi_i)}_{r_i}, \ \psi_i \text{ irreduzibel}, \ \psi_i \not\cong \psi_j \text{ für } i \neq j.$$

Auf diese Weise haben wir jetzt zwei Zerlegungsmatrizen für dieselbe Darstellung ϕ, nämlich $M \cdot [\sigma^{-1}, n]$ und A_ϕ. Sei B nun die blockpermutierte Matrix mit

$$(\rho_1 \oplus \ldots \oplus \rho_k)^B = \bigoplus_{i=1}^{\ell} \underbrace{(\psi_i \oplus \ldots \oplus \psi_i)}_{r_i},$$

das heißt B permutiert die Irreduziblen der ersten Zerlegung in die gleiche Reihenfolge wie sie in der zweiten Zerlegung vorliegen. Außerdem werden ähnliche Irreduzible auf Gleichheit konjugiert. Die Blöcke in B haben maximal die Größe d_i^2, wenn $d_i = \deg(\rho_i)$ ist. Insgesamt enthält B also höchstens $\sum_{i=1}^k r_i d_i^2$ Einträge $\neq 0$. Die Darstellung ϕ wird nun von den Matrizen $M \cdot [\sigma^{-1}, n] \cdot B$ und A_ϕ identisch zerlegt (siehe Abbildung 3.2), woraus folgt, daß

$$A_\phi^{-1} \cdot M \cdot [\sigma^{-1}, n] \cdot B = D \in \mathsf{Int}(\psi, \psi).$$

$$\begin{tikzcd}
 & \psi \arrow[dd, "D"] \\
\phi \arrow[ur, "A_\phi"] \arrow[dr, "M\cdot[\sigma^{-1},n]\cdot B"'] & \\
 & \psi
\end{tikzcd}$$

Abbildung 3.2: Zerlegung via Perm-Irred-Symmetrie

Nach Satz 1.48, iv) gilt

$$\mathsf{Int}(\psi, \psi) = \bigoplus_{i=1}^{\ell} (\mathbb{K}^{r_i \times r_i} \otimes \mathbf{1}_{d_i}),$$

das heißt die Matrix D enthält höchstens $\sum_{i=1}^{\ell} r_i^2 d_i$ Einträge $\neq 0$. Auflösen nach M liefert die Zerlegung von M:

$$M = A_\phi \cdot D \cdot B^{-1} \cdot [\sigma, n].$$

Wir erhalten somit folgenden Algorithmus für die Zerlegung einer Matrix anhand ihrer Perm-Irred-Symmetrie:

3.3 Algorithmus (Zerlegung einer Matrix mit Perm-Irred-Symmetrie)
Gegeben sei eine Matrix $M \in \mathsf{GL}_n(\mathbb{K})$ mit Perm-Irred-Symmetrie (ϕ, ρ), $\phi^M = \rho^{[\sigma,n]} = (\bigoplus_{i=1}^k \rho_i)^{[\sigma,n]}$. M soll anhand der Symmetrie in ein Produkt zerlegt werden.

1. Bestimme eine Zerlegungsmatrix A_ϕ mit Algorithmus 2.2. Es gilt

$$\phi^{A_\phi} = \psi = \bigoplus_{i=1}^{\ell} \underbrace{(\psi_i \oplus \ldots \oplus \psi_i)}_{r_i}, \;\; \psi_i \text{ irreduzibel}, \;\; \psi_i \not\cong \psi_j \text{ für } i \neq j.$$

2. Bestimme eine blockpermutierte Matrix B mit

$$(\rho_1 \oplus \ldots \oplus \rho_k)^B = \bigoplus_{i=1}^{\ell} \underbrace{(\psi_i \oplus \ldots \oplus \psi_i)}_{r_i},$$

Hierzu müssen k Matrizen aus Intertwiningräumen $\mathsf{Int}(\rho_i, \psi_j)$ berechnet werden. Dazu werden lineare Gleichungssysteme gelöst nach Satz 1.56.

3. Bestimme eine Matrix D durch

$$D = A_\phi^{-1} \cdot M \cdot [\sigma^{-1}, n] \cdot B.$$

Man beachte, daß A_ϕ als Ergebnis von Algorithmus 2.2 zerlegt ist, so daß das Invertieren leicht fällt. Die Multiplikation der Matrizen in obiger Gleichung ist jedoch teuer.

Es ist

$$M = A_\phi \cdot D \cdot B^{-1} \cdot [\sigma, n].$$

■

Man beachte, daß die Matrix A_ϕ in Algorithmus 3.3 ebenfalls zerlegt ist.
Das Finden von Perm-Irred-Symmetrie wird in Egner (1997), [26] behandelt. Der dort präsentierte Algorithmus ist exponentiell in n, wenn alle Perm-Irred-Symmetrien gefunden werden sollen. Beschränkt man die Größen der irreduziblen Blöcke einer möglichen Symmetrie durch k, dann ist der Aufwand polynomial in n, genauer gegeben durch $O(n^{2k+1})$ arithmetische Operationen im Grundkörper $\mathbb{K}$. Für $k = 3$ ist damit die Bestimmung dieser Symmetrie praktikabel bis zu einer Matrixgröße von ca. 20, für $k = 2$ bis ca. 50. Unter den in diesem Kapitel vorgestellten Symmetrietypen ist damit die Perm-Irred-Symmetrie mit Abstand am schwersten zu finden.
Selbstverständlich könnte man auch eine „Mon-Irred-Symmetrie" definieren und eine Zerlegung anhand dieser Symmetrie würde vollkommen analog zur Zerlegung anhand der Perm-Irred-Symmetrie laufen. Da es zur Zeit jedoch noch nicht möglich ist, diese zu finden, wurde davon Abstand genommen.

3.2 Perm-Perm-Symmetrie

3.4 Definition *Sei $M \in \mathbb{K}^{m \times n}$. Ein Paar von Permutationsdarstellungen (ϕ, ψ) derselben Gruppe G heißt „Perm-Perm-Symmetrie" von M, wenn $M \in \mathsf{Int}(\phi, \psi)$.*

Im Unterschied zur Perm-Irred-Symmetrie muß hier M weder invertierbar noch quadratisch sein. Außerdem ist mit (ϕ, ψ) auch $(\phi \downarrow H, \psi \downarrow H)$ eine Perm-Perm-Symmetrie von M und es gibt offensichtlich eine *maximale* Perm-Perm-Symmetrie zu einer Matrix M, die jede andere enthält.

Eine Matrix M hat offensichtlich eine Perm-Perm-Symmetrie genau dann, wenn es Paare (σ_1, σ_2) von Permutationen gibt, so daß Permutieren der Zeilen von M mit σ_1 das gleiche bewirkt wie Permutieren der Spalten von M mit σ_2. Es kommt bei der Perm-Perm-Symmetrie also nur darauf an, ob gewisse Einträge der Matrix gleich sind oder nicht.

3.5 Beispiel Sei $\mathsf{Z}_3 = \langle x \mid x^3 = 1\rangle$ mit Darstellung $\phi: \ x \mapsto [(1,2,3),3]$. Dann besitzt die Matrix

$$M = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}, \ a,b,c \in \mathbb{K},$$

die Perm-Perm-Symmetrie (ϕ, ϕ). Allgemeiner besitzt jede zirkulante Matrix

$$M_n = [x_{(j-i) \bmod n} \mid i,j \in \{0,\ldots,n-1\}], \ x_k \in \mathbb{K}, \ k = 1\ldots n,$$

die Perm-Perm-Symmetrie (ψ, ψ), wo $\psi: \ x \mapsto [(1,\ldots,n),n]$ die reguläre Darstellung von $\mathsf{Z}_n = \langle x \mid x^n = 1\rangle$ bezeichnet.
Für ein anderes Beispiel betrachten wir die Diedergruppe mit 8 Elementen, $\mathsf{D}_8 = \langle x, y \mid x^4 = y^2 = 1, \ x^y = x^{-1}\rangle$, mit der natürlichen Darstellung auf 4 Punkten

$$\phi: \ x \mapsto [(1,2,3,4),4], \ y \mapsto [(2,4),4],$$

und der regulären Darstellung auf 8 Punkten

$$\psi: \ x \mapsto [(1,4,6,7)(2,3,5,8),8], \ y \mapsto [(1,2)(3,7)(4,8)(5,6),8].$$

Die Matrix

$$M = \begin{bmatrix} a & a & b & c & d & d & b & c \\ b & c & a & a & b & c & d & d \\ d & d & c & b & a & a & c & b \\ c & b & d & d & c & b & a & a \end{bmatrix}, \ a,b,c,d \in \mathbb{K},$$

besitzt die Perm-Perm-Symmetrie (ϕ, ψ).
Die DFT_n besitzt ebenfalls eine Perm-Perm-Symmetrie. Betrachten wir den Fall $n = 5$. Sei $\mathsf{Z}_4 = \langle x \mid x^4 = 1\rangle$ mit Darstellungen

$$\phi: \ x \mapsto [(2,3,5,4),5], \ \psi: \ x \mapsto [(2,4,5,3),5].$$

Man beachte, daß ϕ und ψ beide nicht transitiv sind. DFT_5 hat die Perm-Perm-Symmetrie (ϕ, ψ). ∎

Wir erklären nun, wie eine Matrix M mit Perm-Perm-Symmetrie (ϕ, ψ) zerlegt werden kann. Seien A_ϕ und A_ψ Zerlegungsmatrizen von ϕ bzw. ψ im Sinne von Kapitel 2, das heißt es gilt

$$\phi^{A_\phi} = \rho = \bigoplus_{i=1}^{k} \underbrace{(\rho_i \oplus \ldots \oplus \rho_i)}_{r_i}, \ \rho_i \text{ irreduzibel}, \ \rho_i \not\cong \rho_j \text{ für } i \neq j.$$

und

$$\psi^{A_\psi} = \theta = \bigoplus_{i=1}^{\ell} \underbrace{(\theta_i \oplus \ldots \oplus \theta_i)}_{s_i}, \ \theta_i \text{ irreduzibel}, \ \theta_i \not\cong \theta_j \text{ für } i \neq j.$$

Manche Irreduziblen ρ_i bzw. θ_j treten jetzt (bis auf Äquivalenz) in beiden Zerlegungen auf, manche nicht. Indem wir für r_i bzw. s_i den Wert 0 zulassen, können wir erreichen, daß jedes ρ_i äquivalent ist zu einem θ_j und umgekehrt. Die Darstellungen ρ und θ schreiben sich dann wie folgt:

$$\rho = \bigoplus_{i=1}^{m} \underbrace{(\rho_i \oplus \ldots \oplus \rho_i)}_{r_i}, \ \theta = \bigoplus_{i=1}^{m} \underbrace{(\theta_i \oplus \ldots \oplus \theta_i)}_{s_i}.$$

Die Summation erstreckt sich nun in beiden Fällen bis zu einer Zahl $m \leq k + \ell$. Sei B die blockpermutierte Matrix mit

$$\theta^B = \bigoplus_{i=1}^{m} \underbrace{(\rho_i \oplus \ldots \oplus \rho_i)}_{s_i},$$

das heißt B permutiert die Irreduziblen θ_i in die gleiche Reihenfolge wie die ρ_j und stellt Gleichheit her. Die Blöcke in B entsprechen den Graden d_i der Irreduziblen ρ_i, das heißt B enthält höchstens $\sum_{i=1}^{m} s_i d_i^2$ Einträge $\neq 0$. Es folgt, daß (siehe Abbildung 3.3)

$$A_\phi^{-1} \cdot M \cdot A_\psi \cdot B = D \in \mathsf{Int}(\rho, \theta^B).$$

$$\begin{tikzcd}
\phi \arrow[r, "M"] \arrow[d, "A_\phi"] & \psi \arrow[d, "A_\psi \cdot B"] \\
\rho \arrow[r, "D"] & \theta^B
\end{tikzcd}$$

Abbildung 3.3: Zerlegung via Perm-Perm-Symmetrie

Nach Satz 1.48, iv) gilt

$$\mathsf{Int}(\rho, \theta^B) = \bigoplus_{i=1}^{m} (\mathbb{K}^{r_i \times s_i} \otimes \mathbf{1}_{d_i}),$$

das heißt die Matrix D enthält höchstens $\sum_{i=1}^{m} r_i s_i d_i$ Einträge. Auflösen nach M ergibt die Zerlegung

$$M = A_\phi \cdot D \cdot B^{-1} \cdot A_\psi^{-1}.$$

Wir erhalten somit den folgenden Algorithmus für die Zerlegung einer Matrix anhand ihrer Perm-Perm-Symmetrie:

3.6 Algorithmus (Zerlegung einer Matrix mit Perm-Perm-Symmetrie) Gegeben sei eine Matrix $M \in \mathbb{K}^{m \times n}$ mit Perm-Perm-Symmetrie (ϕ, ψ). M soll anhand der Symmetrie in ein Produkt zerlegt werden.

1. Bestimme Zerlegungsmatrizen A_ϕ, A_ψ von ϕ bzw. ψ. Es gilt

$$\phi^{A_\phi} = \rho = \bigoplus_{i=1}^{m} \underbrace{(\rho_i \oplus \ldots \oplus \rho_i)}_{r_i},\ \rho_i \text{ irreduzibel},\ \rho_i \not\cong \rho_j,\ i \neq j,\ r_i \geq 0,$$

$$\psi^{A_\psi} = \theta = \bigoplus_{i=1}^{m} \underbrace{(\theta_i \oplus \ldots \oplus \theta_i)}_{s_i},\ \theta_i \text{ irreduzibel},\ \theta_i \not\cong \theta_j,\ i \neq j,\ s_i \geq 0.$$

   Jedes ρ_i ist äquivalent zu einem θ_j und umgekehrt.

2. Bestimme die blockpermutierte Matrix B mit

$$\theta^B = \bigoplus_{i=1}^{m} \underbrace{(\rho_i \oplus \ldots \oplus \rho_i)}_{s_i}.$$

   Dazu muß zu den θ_i, welche (bis auf Äquivalenz) als ρ_j vorkommen, eine Matrix $\in \mathsf{Int}(\theta_i, \rho_j)$ berechnet werden. Löse hierzu ein lineares Gleichungssystem nach Satz 1.56. Es müssen maximal m solche Gleichungssysteme gelöst werden.

3. Bestimme eine Matrix D durch

$$D = A_\phi^{-1} \cdot M \cdot A_\psi \cdot B.$$

Es ist

$$M = A_\phi \cdot D \cdot B^{-1} \cdot A_\psi^{-1}.$$

■

Man beachte, daß in Algorithmus 3.6 die Matrizen A_ϕ und A_ψ^{-1} ebenfalls zerlegt sind.
Das Finden von Perm-Perm-Symmetrie wird in Leon (1991), [39] behandelt. Der dort präsentierte Lösungsvorschlag ist eine spezielle Anwendung der von Leon entwickelten partitionsbasierten Backtracksuche in Permutationsgruppen. Basierend darauf existiert ebenfalls von Leon eine hocheffiziente Implementierung in der Programmiersprache C. Das Programm ist in der Lage die Perm-Perm-Symmetrie von (100×100)-Matrizen in wenigen Sekunden zu bestimmen. Die Matrix darf jedoch höchstens 256 verschiedene Einträge enthalten. Es existiert ebenfalls eine Implementierung in der Programmiersprache GAP von Egner ohne diese Beschränkung. In [26] wird gezeigt, daß das Problem des Findens der Perm-Perm-Symmetrie nicht einfacher ist als das Problem des Findens eines Graph-Isomorphismus.

3.3 Mon-Mon-Symmetrie

3.7 Definition *Sei $M \in \mathbb{K}^{m \times n}$. Ein Paar von monomialen Darstellungen (ϕ, ψ) derselben (nicht notwendig endlichen) Gruppe G heißt „Mon-Mon-Symmetrie" von M, wenn $M \in \mathsf{Int}(\phi, \psi)$.*

Die Mon-Mon-Symmetrie ist somit eine Verallgemeinerung der Perm-Perm-Symmetrie. Mit (ϕ, ψ) ist auch $(\phi \downarrow H, \psi \downarrow H)$ eine Mon-Mon-Symmetrie von M für jede Untergruppe $H \leq G$ und es gibt offensichtlich eine *maximale* Mon-Mon-Symmetrie zu M, welche jede andere enthält. Ist $M \in \mathbb{K}^{m \times n}$, und $\alpha \in \mathbb{K}$, dann gilt

$$\alpha \cdot \mathbf{1}_m \cdot M = M \cdot \alpha \cdot \mathbf{1}_n,$$

das heißt die maximale Mon-Mon-Symmetrie enthält $|\mathbb{K}|$ viele Paare von Skalarmatrizen aus dem Zentrum $Z(\mathsf{GL}_m(\mathbb{K}))$ bzw. $Z(\mathsf{GL}_n(\mathbb{K}))$. Diese stellen keine einschränkende Bedingung an M und sind für Zerlegungszwecke uninteressant. Die Mon-Mon-Symmetrie, welche aus den Skalarmatrizen besteht, wird im folgenden als triviale Symmetrie bezeichnet. Im Unterschied zur Perm-Perm-Symmetrie kann die Mon-Mon-Symmetrie einer Matrix durchaus irreduzibel sein (siehe Beispiel 3.8). Erst das Einschränken der Symmetrie auf eine Untergruppe liefert dann eine für die Zerlegung der Matrix brauchbare Symmetrie. Wie diese Untergruppe zu wählen ist, ist ein offenes Problem.

3.8 Beispiel Die Mon-Mon-Symmetrie der DFT_n entsteht durch Zusammenfassen der Perm-Perm-Symmetrie und der Perm-Irred-Symmetrie. Da DFT_n symmetrisch ist, erhält man aus jeder Mon-Mon-Symmetrie (ϕ, ψ) durch Transposition eine Mon-Mon-Symmetrie (ψ^T, ϕ^T). Betrachten wir den Fall $n = 3$. Die DFT(3) besitzt die Perm-Perm-Symmetrie

$$[(2,3),3] \cdot \mathrm{DFT}_3 = \mathrm{DFT}_3 \cdot [(2,3),3]$$

und die Perm-Irred-Symmetrie

$$[(1,2,3),3] \cdot \mathrm{DFT}_3 = \mathrm{DFT}_3 \cdot \mathrm{diag}(1, \omega_3, \omega_3^2)$$

bzw.

$$\mathrm{diag}(1, \omega_3, \omega_3^2) \cdot \mathrm{DFT}_3 = \mathrm{DFT}_3 \cdot [(1,3,2),3].$$

Insgesamt ergibt sich eine Gruppe

$$\begin{aligned} G &= (\langle w \rangle \ltimes \langle x \rangle) \ltimes (\langle y \rangle \times \langle z \rangle) \\ &\cong (\mathsf{Z}_2 \ltimes \mathsf{Z}_3) \ltimes (\mathsf{Z}_3 \times \mathsf{Z}_3) \end{aligned}$$

der Größe 54 mit Darstellungen

$$\phi: \; w \mapsto [(2,3),3], \; x \mapsto [(1,2,3),3], \; y \mapsto \mathrm{diag}(1, \omega_3, \omega_3^2), \; z \mapsto \mathrm{diag}(\omega_3, \omega_3, \omega_3)$$

und

$$\psi: \; w \mapsto [(2,3),3], \; x \mapsto \mathrm{diag}(1,\omega_3,\omega_3^2), \; y \mapsto [(1,3,2),3], \; z \mapsto \mathrm{diag}(\omega_3,\omega_3,\omega_3).$$

DFT_3 besitzt die Mon-Mon-Symmetrie (ϕ,ψ). Beide Darstellungen sind irreduzibel.
Für ein anderes Beispiel betrachten wir $\mathsf{S}_4 = \langle x, y \mid x^4 = y^2 = (xy)^3 = 1\rangle$ mit den beiden treuen Darstellungen

$$\begin{aligned}
\phi: x &\mapsto [(1,6,7,3)(2,5,8,4),\; (\omega_3,\omega_3^2,\omega_3,\omega_3^2,\omega_3,\omega_3^2,\omega_3^2,\omega_3)],\\
y &\mapsto [(1,6)(2,5)(3,4)(7,8),\; (\omega_3^2,\omega_3,\omega_3^2,\omega_3,\omega_3^2,\omega_3,\omega_3^2,\omega_3)],\\
\psi: x &\mapsto [(2,5,4,3),\; (\omega_4,\omega_4,-1,-\omega_4,-1,-\omega_4)],\\
y &\mapsto [(1,4)(2,6)(3,5),\; (\omega_4,\omega_4,-1,-\omega_4,-1,-\omega_4)].
\end{aligned}$$

Die Matrix

$$M = \begin{bmatrix}
a & b & \omega_3^2 b & \omega_3^2 a & \omega_3 a & \omega_3 b\\
b & a & \omega_3 a & \omega_3 b & \omega_3^2 b & \omega_3^2 a\\
-\omega_{12}^7 a & -\omega_3^2 a & -\omega_{12}^7 b & -b & \omega_4 a & \omega_{12}^{11} b\\
-\omega_{12}^{11} b & -\omega_3 b & -\omega_{12}^{11} a & -a & \omega_4 b & \omega_{12}^7 a\\
\omega_{12}^{11} b & \omega_4 a & -b & -\omega_{12}^7 b & -\omega_3^2 a & -\omega_{12}^7 a\\
\omega_{12}^7 a & \omega_4 b & -a & -\omega_{12}^{11} a & -\omega_3 b & -\omega_{12}^{11} b\\
-\omega_3^2 a & -\omega_{12}^7 a & \omega_4 a & \omega_{12}^{11} b & -\omega_{12}^7 b & -b\\
-\omega_3 b & -\omega_{12}^{11} b & \omega_4 b & \omega_{12}^7 a & -\omega_{12}^{11} a & -a
\end{bmatrix}, \quad a,b \in \mathbb{C},$$

hat die Mon-Mon-Symmetrie (ϕ,ψ). ■

Die Zerlegung einer Matrix anhand einer Mon-Mon-Symmetrie geschieht vollkommen analog zur Zerlegung anhand einer Perm-Perm-Symmetrie. Der zugehörige Algorithmus ergibt sich durch Ersetzen des Wortes „Perm-Perm-Symmetrie“ durch „Mon-Mon-Symmetrie“ in Algorithmus 3.6.
Da es unendlich viele monomiale Matrizen jeder Größe gibt, ist das Finden der Mon-Mon-Symmetrie erheblich schwieriger als das Finden der Perm-Perm-Symmetrie zu einer Matrix. Der Algorithmus, den wir im folgenden entwickeln werden, findet Mon-Mon-Symmetrie eines bestimmten Typs, das heißt die Menge aller möglichen monomialen Matrizen einer Symmetrie wird eingeschränkt. Die Bestimmung der Mon-Mon-Symmetrie wird dann zurückgeführt auf die Bestimmung der Perm-Perm-Symmetrie einer größeren Matrix.

3.9 Definition *Sei $M \in \mathbb{K}^{m\times n}$ und $k \geq 1$. Ein Paar (ϕ,ψ) von Darstellungen einer Gruppe G heißt „Mon-Mon-Symmetrie der Ordnung k“, wenn (ϕ,ψ) eine Mon-Mon-Symmetrie von M ist und die Einträge $\neq 0$ in allen Matrizen $\phi(g),\psi(g)$ k-te Einheitswurzeln sind.*

In dieser Definition ist also die Perm-Perm-Symmetrie gerade die Mon-Mon-Symmetrie der Ordnung 1. Durch diese Einschränkung bewegen wir uns jetzt in der endlichen Menge aller monomialer Matrizen mit k-ten Einheitswurzeln als Einträge $\neq 0$. Ist beispielsweise $\mathbb{K} = \mathbb{F}_q$ ein endlicher Körper, dann hat jede Mon-Mon-Symmetrie die Ordnung $q-1$. Wir werden im folgenden einen Algorithmus entwickeln, der die maximale Mon-Mon-Symmetrie der Ordnung k einer Matrix findet. Die Idee hierzu stammt aus Leon (1991), [39]. Die Matrix M wird zu einer Matrix $\mathcal{C}_k(M)$ so codiert, daß jedes Paar monomialer Matrizen der Symmetrie von M einem Paar von Permutationen der Perm-Perm-Symmetrie von $\mathcal{C}_k(M)$ entspricht. Diese Permutationen haben eine Blockstruktur, die der monomialen Matrix entspricht. Der Parameter zu der Codierung ist die Zahl k.

3.10 Definition *Sei $a \in \mathbb{K}$ und ω_k eine k-te Einheitswurzel in $\mathbb{K}$. Wir nennen*

$$\begin{aligned}
\mathcal{C}_k(a) &= \begin{bmatrix} a \cdot \omega_k^0 & a \cdot \omega_k^1 & \cdots & a \cdot \omega_k^{(k-1)} \\ a \cdot \omega_k^1 & a \cdot \omega_k^2 & \cdots & a \cdot \omega_k^0 \\ \vdots & \vdots & \ddots & \vdots \\ a \cdot \omega_k^{(k-1)} & a \cdot \omega_k^0 & \cdots & a \cdot \omega_k^{(k-2)} \end{bmatrix} \\
&= [a \cdot \omega_k^{(i-1)+(j-1)} \mid i, j \in \{1, \ldots, k\}]
\end{aligned}$$

die Codierung von a mit Parameter k. Ist $A \in \mathbb{K}^{m \times n}$, dann nennen wir entsprechend

$$\begin{aligned}
\mathcal{C}_k(A) &= \begin{bmatrix} \mathcal{C}_k(a_{1,1}) & \cdots & \mathcal{C}_k(a_{1,n}) \\ \vdots & \ddots & \vdots \\ \mathcal{C}_k(a_{m,1}) & \cdots & \mathcal{C}_k(a_{m,n}) \end{bmatrix} \\
&= [\mathcal{C}_k(a_{i,j}) \mid i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}]
\end{aligned}$$

die Codierung von A mit Parameter k.

Die beschriebene Codierung ist offensichtlich eine bijektive Abbildung. Der Parameter k entspricht, wie wir später sehen werden, der Ordnung der monomialen Symmetrie, die über die Codierung gefunden werden kann. Ist $a \in \mathbb{K}$, dann geht die $(i+1)$-te Zeile von $\mathcal{C}_k(a)$ aus der i-ten durch Multiplikation mit ω_k hervor. Entsprechendes gilt für die Spalten. Damit gilt das folgende Lemma:

3.11 Lemma Es gilt

$$\mathcal{C}_n(a \cdot \omega_k^\ell) = \mathcal{C}_n(a) \cdot [(1, \ldots, k)^{-\ell}, k] = [(1, \ldots, k)^\ell, k] \cdot \mathcal{C}_n(a).$$

Beweis Trivial. ∎

Wie oben bereits angedeutet sollen monomiale Matrizen, die als Symmetrie von $M \in \mathbb{K}^{m\times n}$ auftreten, Blockpermutationen der Perm-Perm-Symmetrie von $\mathcal{C}_k(M) \in \mathbb{K}^{km\times kn}$ entsprechen. Eine solche Blockpermutation $\sigma \in \mathsf{S}_{km}$ bzw. $\in \mathsf{S}_{kn}$ permutiert Blöcke der Größe k und die Einschränkung von σ auf jeden Block hat die Form $(1,\ldots,k)^i$. Hier ein Beispiel mit $k = 2$, die Blockstruktur ist hervorgehoben:

$$\begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix} \longleftrightarrow \left[\begin{array}{cc|cc|cc} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right] = [\sigma, 6],\ \ \sigma = (1,4,6)(2,3,5).$$

Die Permutationsmatrix $[\sigma, 6]$ läßt sich anhand ihrer Blockstruktur dekomponieren durch

$$\begin{aligned} [\sigma, 6] &= ([(1,2),2] \oplus [(1),2] \oplus [(1,2),2]) \cdot ([(1,2,3),3] \otimes [(1),2]) \\ &= ([(1,2,3),3] \otimes [(1),2]) \cdot ([(1,2),2] \oplus [(1,2),2]) \oplus [(1),2]) . \end{aligned}$$

Allgemein haben die betrachteten Blockpermutationen $\sigma \in \mathsf{S}_{kn}$ folgende Struktur:

$$[\sigma, kn] = ([\tau, n] \otimes \mathbf{1}_k) \cdot \left(\bigoplus_{i=1}^{n} [\sigma_i, k] \right),$$

wobei $\tau \in \mathsf{S}_n$ die Makropermutation darstellt und $\sigma_i \in \mathsf{Z}_k = \langle (1,\ldots,k) \rangle$ ein k-Zyklus ist. Algebraisch entspricht die Gruppe der Blockpermutationen $\sigma \in \mathsf{S}_{kn}$ dem Kranzprodukt $\mathsf{Z}_k \wr \mathsf{S}_n$. Zum Kranzprodukt siehe zum Beispiel das Buch von James/Kerber (1981), [37].

3.12 Lemma Es sei $\tau \in \mathsf{S}_n$ und $\sigma_i \in \mathsf{S}_k,\ i = 1\ldots n$. Dann gilt

$$([\tau, n] \otimes \mathbf{1}_k) \cdot \left(\bigoplus_{i=1}^{n} [\sigma_i, k] \right) = \left(\bigoplus_{i=1}^{n} [\sigma_{i^\tau}, k] \right) \cdot ([\tau, n] \otimes \mathbf{1}_k).$$

Beweis Einfaches Nachrechnen. ∎

Wir werden nun beweisen, daß sich durch Codieren einer Matrix M mit Parameter k die maximale Mon-Mon-Symmetrie der Ordnung k finden läßt.
Vorher noch ein paar Worte zur Notation. Wir erinnern daran, daß eine monomiale $(m \times m)$-Matrix dargestellt wird als $[\sigma, (s_1,\ldots,s_m)] = [\sigma, m] \cdot \mathrm{diag}(s_1,\ldots,s_m)$, $\sigma \in \mathsf{S}_m,\ s_i \in \mathbb{K},\ i = 1\ldots n$. Ist $A = [a_{i,j}] \in \mathbb{K}^{m\times n}$, $\sigma \in \mathsf{S}_m,\ \tau \in \mathsf{S}_n$, dann gelten die folgenden Rechenregeln:

1. $[\sigma, m] \cdot [a_{i,j}] = [a_{i^\sigma,j}]$.

2. $[a_{i,j}] \cdot [\tau, n] = [a_{i,j^{\tau^{-1}}}]$.

3. $[a_{i,j}] \cdot \mathrm{diag}(s_1, \ldots, s_n) = [s_j \cdot a_{i,j}]$.

4. $\mathrm{diag}(s_1, \ldots, s_n) \cdot [a_{i,j}] = [s_i \cdot a_{i,j}]$.

5. $[\sigma, m] \cdot \mathrm{diag}(s_1, \ldots, s_m) = \mathrm{diag}(s_{1^\sigma}, \ldots, s_{m^\sigma}) \cdot [\sigma, m]$.

3.13 Satz *Sei $A \in \mathbb{K}^{m\times n}$. Die Mon-Mon-Symmetrie der Ordnung k von A läßt sich finden durch Bestimmung der Perm-Perm-Symmetrie der Matrix $\mathcal{C}_k(A)$. Genauer gilt: Sind $s_i = \omega_k^{u_i}$, $i = 1 \ldots m$, $t_j = \omega_k^{v_j}$, $j = 1 \ldots n$, dann gilt*

$$\begin{aligned}
& [\sigma, (s_1, \ldots, s_m)] \cdot A = A \cdot [\tau, (t_1, \ldots, t_n)] \\
\Leftrightarrow\quad & ([\sigma, m] \otimes \mathbf{1}_k) \cdot \bigoplus_{i=1}^{m} [(1, \ldots, k)^{u_i}, k] \cdot \mathcal{C}_k(A) = \\
& \mathcal{C}_k(A) \cdot \bigoplus_{j=1}^{n} [(1, \ldots, k)^{-v_j}, k] \cdot ([\tau, n] \otimes \mathbf{1}_k)\,.
\end{aligned}$$

Beweis Wir betrachten ein Paar $[\sigma, (s_1, \ldots, s_m)]$, $[\tau, (t_1, \ldots, t_n)]$ monomialer Matrizen der Symmetrie von $A = [a_{i,j}]$, mit $s_i = \omega_k^{u_i}$, $t_j = \omega_k^{v_j}$, wie im Satz definiert. Dann gilt

$$\begin{aligned}
& [\sigma, (s_1, \ldots, s_m)] \cdot A = A \cdot [\tau, (t_1, \ldots, t_n)] \\
\Leftrightarrow\quad & [s_{i^\sigma} \cdot a_{i^\sigma, j}] = [t_{j^{\tau^{-1}}} \cdot a_{i,j^{\tau^{-1}}}] \\
\Leftrightarrow\quad & [\omega_k^{u_{i^\sigma}} \cdot a_{i^\sigma, j}] = [\omega_k^{v_{j^{\tau^{-1}}}} \cdot a_{i,j^{\tau^{-1}}}] \\
\Leftrightarrow\quad & \forall i, j:\ \mathcal{C}_k(\omega_k^{u_{i^\sigma}} \cdot a_{i^\sigma, j}) = \mathcal{C}_k(\omega_k^{v_{j^{\tau^{-1}}}} \cdot a_{i,j^{\tau^{-1}}}) \\
& \text{(Lemma 3.11)} \\
\Leftrightarrow\quad & \forall i, j: [(1, \ldots, k)^{u_{i^\sigma}}, k] \cdot \mathcal{C}(a_{i^\sigma, j}) = \mathcal{C}_k(a_{i,j^{\tau^{-1}}}) \cdot [(1, \ldots, k)^{-v_{j^{\tau^{-1}}}}, k] \\
\Leftrightarrow\quad & \bigoplus_{i=1}^{m} [(1, \ldots, k)^{u_{i^\sigma}}, k] \cdot ([\sigma, m] \otimes \mathbf{1}_k) \cdot \mathcal{C}_k(A) = \\
& \mathcal{C}_k(A) \cdot ([\tau, n] \otimes \mathbf{1}_k) \cdot \bigoplus_{j=1}^{n} [(1, \ldots, k)^{-v_{j^{\tau^{-1}}}}, k] \\
& \text{(Lemma 3.12)} \\
\Leftrightarrow\quad & ([\sigma, m] \otimes \mathbf{1}_k) \cdot \bigoplus_{i=1}^{m} [(1, \ldots, k)^{u_i}, k] \cdot \mathcal{C}_k(A) = \\
& \mathcal{C}_k(A) \cdot \bigoplus_{j=1}^{n} [(1, \ldots, k)^{-v_j}, k] \cdot ([\tau, n] \otimes \mathbf{1}_k)\,,
\end{aligned}$$

was zu zeigen war. ∎

Das verbleibende Problem ist die geeignete Wahl des Parameters k. Ist $\mathbb{K} = \mathbb{F}_q$ ein endlicher Körper, dann kann $k = q - 1$ gewählt werden, um sogar die maximale Mon-Mon-Symmetrie zu bestimmen. Im Fall $\mathbb{K} \leq \mathbb{C}$ kann eine Matrix durchaus nichttriviale Mon-Mon-Symmetrie beliebiger Ordnung besitzen. Ist beispielsweise

$$M = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \; a, b \in \mathbb{K},$$

dann gilt

$$\begin{bmatrix} \omega_n & 0 \\ 0 & \omega_n^{-1} \end{bmatrix} \cdot M = M \cdot \begin{bmatrix} \omega_n & 0 \\ 0 & \omega_n^{-1} \end{bmatrix} \quad \text{für alle } n = 1, 2, \ldots .$$

Besitzt eine Matrix mit komplexen Einträgen monomiale Symmetrie beliebiger Ordnung, dann werden durch diese Symmetrie Einträge gleichen Betrages permutiert. Zur Bestimmung der Ordnung einer möglichen Symmetrie ist es daher naheliegend, die Quotienten von Matrixeinträgen gleichen Betrages zu betrachten. Diese Beobachtung führt zu dem im folgenden beschriebenen Verfahren zur Bestimmung des Parameters k zur Codierung der Matrix. Sei $A \in \mathbb{K}^{m \times n}$, $\mathbb{K} \leq \mathbb{C}$ und $M = \{a_1, \ldots, a_r\}$ die Menge aller Einträge von A. Wir definieren folgende Äquivalenzrelation auf M:

$$a_i \sim a_j \Leftrightarrow |a_i| = |a_j|.$$

Sei $P = \{P_1, \ldots, P_\ell\}$ die Partition von M nach „$\sim$" und $P_i = \{p_{i,1}, \ldots, p_{i,r_i}\}$. Für $i = 1 \ldots \ell$ setzen wir k_i gleich dem kgV der Ordnungen der $r_i - 1$ Einheitswurzeln $p_{i,2}/p_{i,1}, \ldots, p_{i,r_i}/p_{i,1}$, sofern $0 \notin P_i$ und die Ordnungen dieser Einheitswurzeln endlich sind. Ansonsten setzen wir $k_i = 1$. Der Parameter zur Codierung ist dann $k = \mathrm{kgV}(k_i \mid i = 1 \ldots \ell)$.
Es ergibt sich der folgende Algorithmus zum Finden von Mon-Mon-Symmetrie.

3.14 Algorithmus (Finden von Mon-Mon-Symmetrie) Gegeben sei eine Matrix $M \in \mathbb{K}^{m \times n}$, $\mathbb{K} \leq \mathbb{C}$. Es soll eine Mon-Mon-Symmetrie (ϕ, ψ) von M bestimmt werden, bei der die Einträge $\neq 0$ in den Bildmatrizen $\phi(g), \psi(g)$ nur Einheitswurzeln sind.

1. Bestimme den Parameter k mit dem oben beschriebenen Verfahren.
2. Codiere M mit Parameter k zu $\mathcal{C}_k(M)$.
3. Bestimme die Perm-Perm-Symmetrie (ϕ_1, ψ_1) von $\mathcal{C}_k(M)$.
4. Schränke ϕ_1, ψ_1 ggf. auf eine Untergruppe H ein, so daß $\phi_1(h), \psi_1(h)$ Blockpermutationen der Gestalt wie in Satz 3.13 sind.
5. Decodiere $\phi_1 \downarrow H, \psi_1 \downarrow H$ nach Satz 3.13 zu ϕ, ψ.

M hat die monomiale Symmetrie (ϕ, ψ). ∎

Zu Punkt 4. in Algorithmus 3.14 bemerken wir, daß in fast allen betrachteten Anwendungen $H = G$ ist. Es ist jedoch nicht gelungen, ein Kriterium zu finden, welches die Fälle charakterisiert, in denen dies nicht der Fall ist.

4

Anwendung auf Signaltransformationen

Die automatische Generierung schneller Algorithmen für diskrete Signaltransformationen liefert einen Anwendungsbereich für die in Kapitel 3 entwickelten Algorithmen. Die dort beschriebene Zerlegung einer Matrix läßt sich als schneller Algorithmus für die Matrix-Vektor- bzw. Matrix-Matrix-Multiplikation verwenden.
In diesem Kapitel werden wir einige klassische Signaltransformationen auf Symmetrie untersuchen. Es stellt sich heraus, daß alle betrachteten Transformationen eine Symmetrie aufweisen, die eine substantielle Zerlegung ermöglicht. Exemplarisch wird diese Zerlegung mit den implementierten Algorithmen aus Kapitel 3 durchgeführt. Alle Zerlegungen sind in der präsentierten Form erzeugt worden. Die dazu benötigten Rechenzeiten sind angegeben in CPU-Zeit auf einer SUN Ultra-Sparc 150 MHz.
Sicherlich liefern die automatisch generierten Zerlegungen keine optimalen Algorithmen für die jeweilige Signaltransformation, was zum einen daran liegt, daß sich nicht jeder schnelle Algorithmus zur Matrix-Vektor-Multiplikation als Produkt dünnbesetzter Algorithmen schreiben läßt, zum anderen liegen Feinheiten, die hier und da eine Multiplikation sparen, außerhalb der Mächtigkeit der verwendeten Methoden. Darüber hinaus ist die Schnelligkeit dieser Algorithmen stark abhängig vom gegebenen Maschinenmodell. Zählt man jedoch die arithmetischen Operationen im Grundkörper, dann stimmt die asymptotische Komplexität der generierten Zerlegungen mit der asymptotischen Komplexität der bekannten, schnellsten Algorithmen überein. Damit liefert die Darstellungstheorie nicht nur einen vom theoretischen Standpunkt zufriedenstellenden Grund für die Existenz eines schnellen Algorithmus für eine Signaltransformation, sondern auch die Möglichkeit, diesen zu generieren!
Jeder der folgenden Abschnitte beschäftigt sich mit einer Serie von Signaltransformationen, die untersucht wird auf Symmetrie der betrachteten Typen. Es wird jeweils die Größe und der Isomorphietyp der Symmetriegruppe angegeben sowie ei-

nige Eigenschaften der zugehörigen Darstellungen. Bei der Mon-Mon-Symmetrie wird zusätzlich noch die Ordnung angegeben, das heißt die Ordnung der Einheitswurzeln in den Bildmatrizen. Zum Finden der Perm-Irred-Symmetrie und der Perm-Perm-Symmetrie wurden die implementierten Algorithmen von Egner verwendet, bei der Zerlegung der Matrizen arbeiten diese mit dem Programm zur Zerlegung monomialer Darstellungen Hand in Hand.
Die Ergebnisse zu den Symmetriegruppen sind entstanden durch Untersuchung der jeweiligen Transformation für kleine Größen und Extrapolation der Ergebnisse. Für die DFT sind die Symmetrien jedoch bewiesen (siehe z. B. Egner, [26]).
Zur Notation verweisen wir auf Abschnitt 1.1. Die Definitionen der Cosinustransformationen folgt Mertins (1996), [44], die anderen Transformationen Elliott/Rao (1982), [28].

4.1 Diskrete Fouriertransformation

Die Diskrete Fouriertransformation DFT_n der Größe n ist definiert als

$$\mathrm{DFT}_n = [\omega_n^{ij} \mid i, j \in \{0, \ldots, n-1\}].$$

Die DFT_n ist *die* Transformation in der Signalverarbeitung und wird in jedem Standardwerk ausführlich behandelt. Die meisten der zahlreichen Eigenschaften dieser Matrix spiegeln sich in den unten aufgeführten Symmetrien wider.
Das Buch von Beth (1984), [6] befaßt sich mit der algebraischen Interpretation der Fouriertransformation und ist das erste wesentliche Werk zur Verknüpfung von Signaltransformationen und Darstellungstheorie endlicher Gruppen.
Die Perm-Irred-Symmetrie und die Perm-Perm-Symmetrie sind hinlänglich bekannt (siehe z. B. [26]). Ist $\mathsf{Z}_n = \langle x \mid x^n = 1 \rangle$ die zyklische Gruppe der Ordnung n mit regulärer Darstellung

$$\phi: \ x \mapsto [(1, \ldots, n), n]$$

und zugehöriger zerlegter Darstellung

$$\rho: \ x \mapsto \mathrm{diag}(\omega_n^0, \omega_n^1, \ldots, \omega_n^{(n-1)}),$$

dann besitzt DFT_n die Perm-Irred-Symmetrie (ϕ, ρ). Ist $\mathsf{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$, dann werden durch

$$\phi_1: \ k \mapsto [i \mapsto ki \bmod n]$$

und

$$\phi_2 = \phi_1^{-1}: \ k \mapsto [i \mapsto k^{-1}i \bmod n]$$

zwei Permutationsdarstellungen von $\mathsf{Z}_n^\times$ auf n Punkten definiert und die Perm-Perm-Symmetrie von DFT_n ist gegeben durch (ϕ_1, ϕ_2).

Die Mon-Mon-Symmetrie vom Grad n entsteht durch Zusammenfassen der beiden anderen Symmetrien und Ergänzen der trivialen Symmetrie. Wir halten die Ergebnisse in Tabelle 4.1 fest. Es bezeichnet φ die Eulersche Phifunktion ($\varphi(n) =$ Anzahl der primen Reste modulo n).

Symmetrietyp	Gruppe	Größe	Eigenschaften
Perm-Irred (ϕ, ρ)	Z_n	n	ϕ ist regulär
Perm-Perm (ϕ_1, ϕ_2)	$\mathsf{Z}_n^\times$	$\varphi(n)$	ϕ_1, ϕ_2 nicht transitiv
Mon-Mon (ϕ_1, ϕ_2) (Ordnung n)	$(\mathsf{Z}_n^\times \ltimes \mathsf{Z}_n) \ltimes (\mathsf{Z}_n \times \mathsf{Z}_n)$	$\varphi(n)n^3$	ϕ_1, ϕ_2 irreduzibel

Tabelle 4.1: Symmetrie der DFT_n

Wie bereits mehrfach erwähnt entsprechen die Cooley-Tukey-Zerlegung und die Good-Thomas-Zerlegung einer DFT_n der Zerlegung anhand der Perm-Irred-Symmetrie dieser Matrix. Der Algorithmus von Rader (1968), [53] verwendet die Perm-Perm-Symmetrie im Falle $n = p$, prim. Die zugehörige Gruppe ist in diesem Fall (siehe Tabelle 4.1) $\mathsf{Z}_p^\times \cong \mathsf{Z}_{p-1}$ isomorph zu einer zyklischen Gruppe der Ordnung $p-1$. Anhand dieser Symmetrie wird die DFT_p im wesentlichen in zwei $\mathrm{DFT}_{(p-1)}$ zerlegt.
Es folgt die mit Algorithmus 3.6 generierte Zerlegung der DFT_5, benötigte Laufzeit: 0.2 s. Man beachte, daß sich die asymptotisch ($p \to \infty$) bessere Komplexität dieser Zerlegung für $p = 5$ noch nicht niederschlägt.

$$
\begin{aligned}
&\mathrm{DFT}_5 = \\
&\quad [(4,5),\ 5]\cdot \\
&\quad \Big(\mathbf{1}_1 \oplus (\mathrm{DFT}_2 \otimes \mathbf{1}_2) \cdot \mathrm{diag}(1,1,1,\omega_4) \cdot (\mathbf{1}_1 \otimes \mathrm{DFT}_2) \cdot [(2,3),\ 4]\Big)\cdot \\
&\quad \left(\begin{bmatrix} 1 & 4 \\ 1 & -1 \end{bmatrix} \oplus \mathrm{diag}(a,b,c)\right) \cdot \\
&\quad \Big(\mathbf{1}_1 \oplus \tfrac{1}{4} \cdot [(2,3),\ 4] \cdot (\mathbf{1}_2 \otimes \mathrm{DFT}_2) \cdot \mathrm{diag}(1,1,1,-\omega_4) \cdot (\mathrm{DFT}_2 \otimes \mathbf{1}_2)\Big) \cdot \\
&\quad [(3,4,5),\ 5],
\end{aligned}
$$

wobei

$$a = \omega_{20}^4 - \omega_{20}^{13} - \omega_{20}^{16} + \omega_{20}^{17},\ b = \omega_5 - \omega_5^2 - \omega_5^3 + \omega_5^4,\ c = \omega_{20}^4 + \omega_{20}^{13} - \omega_{20}^{16} - \omega_{20}^{17}$$

bezeichnet. Die ersten und letzten beiden Zeilen in der Zerlegung entsprechen jeweils der DFT_4, die mittlere Matrix ist aus dem Intertwiningraum der zerlegten Darstellungen.

4.2 Walsh-Hadamard-Transformation

Die Walsh-Hadamard-Transformation WHT_{2^k} ist das k-fache Tensorprodukt einer DFT_2 mit sich selbst:

$$\mathrm{WHT}_{2^k} = \underbrace{\mathrm{DFT}_2 \otimes \ldots \otimes \mathrm{DFT}_2}_{k\text{-fach}}.$$

Eine ausführliche Beschreibung der WHT in der Signalverarbeitung liefert das Buch von Beauchamp (1984), [4]. Die Bedeutung der WHT für Reed-Muller-Codes und andere fehlerkorrigierende Codes ist beschrieben in MacWilliams/Sloane (1992), [41]. Zur Codierung auf Quantenrechnern siehe zum Beispiel Beth/Grassl (1996), [8].
Der schnelle Algorithmus zur WHT steckt selbstverständlich bereits in der obigen Definition. Wäre die Struktur der WHT jedoch nicht bekannt, dann würde sie sich über die Perm-Irred-Symmetrie finden lassen.
Wie bei der DFT entsteht auch bei der WHT die Mon-Mon-Symmetrie durch Zusammenfassen der Perm-Irred-Symmetrie und der Perm-Perm-Symmetrie.

Symmetrietyp	Gruppe	Größe	Eigenschaften
Perm-Irred (ϕ, ρ)	Z_2^k	2^k	ϕ ist regulär
Perm-Perm (ϕ_1, ϕ_2)	$\mathsf{GL}(k, 2)$	$(2^k - 2^{k-1}) \cdots (2^k - 1)$	ϕ_1, ϕ_2 nicht transitiv
Mon-Mon (ϕ_1, ϕ_2)	G_k	$\lvert \mathsf{GL}(k, 2) \rvert \cdot 2^{2k+1}$	ϕ_1, ϕ_2 irreduzibel
(Ordnung 2)	$G_k \cong (\mathsf{GL}(k, 2) \ltimes \mathsf{Z}_2^k) \ltimes (\mathsf{Z}_2 \times \mathsf{Z}_2^k)$		

Tabelle 4.2: Symmetrie der WHT_{2^k}

4.3 Diskrete Cosinustransformation I

Die Cosinustransformation $\mathrm{DCT\text{-}I}_n$ ist eine $((n + 1) \times (n + 1))$-Matrix definiert durch

$$\mathrm{DCT\text{-}I}_n = \left[\sqrt{2/n} \cdot c_i c_j \cdot \cos\left(\frac{ij\pi}{n}\right) \mid i, j \in \{0, \ldots, n\}\right],$$

wobei

$$c_k = \begin{cases} 1/\sqrt{2} & \text{für } k = 0, n \\ 1 & \text{sonst} \end{cases}.$$

Die DCT-I spielt kaum eine Rolle in der Signalverarbeitung. Zur Symmetrie siehe Tabelle 4.3.

Symmetrietyp	Gruppe	Größe	Eigenschaften
Perm-Perm (ϕ_1, ϕ_2)	n gerade: $\mathsf{Z}_{2^{k-1}} \times \mathsf{Z}_m^\times$	$\varphi(n)$	ϕ_1, ϕ_2 intransitiv
	$n = 2^k m, 2 \not| m$		
	n ungerade: G_n	$\varphi(n)/2$	
	mit $(\mathsf{Z}_n^\times : G_n) = 2$		
Mon-Mon (ϕ_1, ϕ_2)	n gerade: $\mathsf{Z}_2^3 \times \mathsf{Z}_n^\times$	$8 \cdot \varphi(n)$	ϕ_1, ϕ_2 transitiv
(Ordnung 2)	n ungerade: $\mathsf{D}_8 \times H_n$	$4 \cdot \varphi(n)$	$\Leftrightarrow n = 1, 3$
	mit $(\mathsf{Z}_n^\times : H_n) = 2$		

Tabelle 4.3: Symmetrie der DCT-I_n

4.4 Diskrete Cosinustransformation II und III

Die Cosinustransformation DCT-III_n ist definiert durch

$$\text{DCT-III}_n = \left[\sqrt{2/n} \cdot c_j \cdot \cos\left(\frac{(i+1/2)j\pi}{n}\right) \mid i, j \in \{0, \ldots, n-1\}\right],$$

wobei

$$c_j = \begin{cases} 1/\sqrt{2} & \text{für } j = 0 \\ 1 & \text{sonst} \end{cases} .$$

Die DCT-II ist die Transponierte der DCT-III. Damit entsprechen sich die Perm-Perm-Symmetrie und die Mon-Mon-Symmetrie der beiden Matrizen. Lediglich die DCT-III besitzt jedoch eine Perm-Irred-Symmetrie, die von Minkwitz im Rahmen seiner Dissertation [45] entdeckt wurde.
Die DCT-II hat große Bedeutung bei der Kompression von Bilddaten. Sie wird im JPEG-Standard (siehe Pennebaker/Mitchell (1993), [51]) verwendet. Dort wird sie in der Größe 8×8 eingesetzt, im MPEG-Standard in der Größe 16×16. Siehe dazu das Buch von Rao/Hwang (1996), [54].

Symmetrietyp	Gruppe	Größe	Eigenschaften
Perm-Irred (ϕ, ρ)	D_{2n}	$2n$	ϕ ist transitiv
Mon-Mon (ϕ_1, ϕ_2)	$n = 2$: D_8	8	ϕ_1 ist transitiv
(Ordnung 2)	$n = 4$: $\mathsf{Z}_2 \ltimes (\mathsf{Z}_2 \times \mathsf{Z}_4)$	16	$\Leftrightarrow n \leq 2$,
	sonst: $\mathsf{Z}_2 \times \mathsf{Z}_{2^k} \times \mathsf{Z}_m^\times$,	$2^{(k+1)}\varphi(m)$	ϕ_2 ist transitiv
	mit $n = 2^k m,\ 2 \not| m$		$\Leftrightarrow n = 2^k$

Tabelle 4.4: Symmetrie der DCT-III_n

Hier eine anhand der Perm-Irred-Symmetrie (Algorithmus 3.3) generierte Zerlegung der DCT-III_8, benötigte Laufzeit: 10.5 s.

$$
\begin{aligned}
&\text{DCT-III}_8 = \\
&\quad [(1,2,6,8)(3,7,5,4),\ 8] \cdot (\mathbf{1}_2 \otimes (\mathbf{1}_2 \otimes \mathrm{DFT}_2) \cdot [(2,3),\ 4] \cdot (\mathrm{DFT}_2 \oplus \mathbf{1}_2)) \cdot \\
&\quad [(2,7,6,8,5,4,3),\ 8] \cdot \left(\mathbf{1}_4 \oplus \tfrac{1}{\sqrt{2}} \cdot \mathrm{DFT}_2 \oplus \mathbf{1}_2\right) \cdot [(5,6),\ 8] \cdot \\
&\quad ((\mathrm{DFT}_2 \otimes \mathbf{1}_3) \oplus \mathbf{1}_2) \cdot [(2,7,3,8,4),\ 8] \cdot \\
&\quad \tfrac{1}{4} \cdot \left(\mathrm{diag}(\sqrt{2},\sqrt{2}) \oplus \begin{bmatrix} a & b \\ b & -a \end{bmatrix} \oplus \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \oplus \begin{bmatrix} e & f \\ f & -e \end{bmatrix}\right),
\end{aligned}
$$

wobei

$$
\begin{array}{lll}
a = \omega_{16} - \omega_{16}^7, & b = \omega_{16}^3 - \omega_{16}^5, & c = -\omega_{32} + \omega_{32}^{15}, \\
d = \omega_{32}^7 - \omega_{32}^9, & e = -\omega_{32}^3 + \omega_{32}^{13}, & f = -\omega_{32}^5 + \omega_{32}^{11}.
\end{array}
$$

Die ersten 3 Zeilen entsprechen der Zerlegungsmatrix der Permutationsdarstellung der D_{16}, die letzte Zeile ist die Blockdiagonalmatrix aus dem Intertwiningraum der zerlegten Darstellungen. Eine Zerlegung der DCT-II$_8$ enthält man durch Transposition obiger Zerlegung.

4.5 Diskrete Cosinustransformation IV

Die Cosinustransformation DCT-IV$_n$ ist definiert durch

$$\text{DCT-IV}_n = \left[\sqrt{2/n} \cdot \cos\left(\frac{(i+1/2)(j+1/2)\pi}{n}\right) \mid i,j \in \{0,\ldots,n-1\}\right].$$

Die DCT-IV spielt eine Rolle bei schnellen Algorithmen zur DCT-II und bei der Berechnung von sogenannten Lapped Orthogonal Transforms. Siehe dazu das Buch von Malvar (1992), [42].
Die DCT-IV besitzt lediglich eine Mon-Mon-Symmetrie, die aber zu einer effektiven Zerlegung der Matrix führt.

Symmetrietyp	Gruppe	Größe	Eigenschaften
Mon-Mon (ϕ_1,ϕ_2) (Ordnung 2)	$\mathsf{Z}_{2^{(k+1)}} \times \mathsf{Z}_m^\times$ mit $n = 2^k m,\ 2 \nmid m$	$2^{(k+1)}m$	ϕ_1,ϕ_2 transitiv $\Leftrightarrow n = 2^k$

Tabelle 4.5: Symmetrie der DCT-IV$_n$

Hier eine anhand der Mon-Mon-Symmetrie generierte Zerlegung der DCT-IV$_8$, benötigte Laufzeit: 1.4 s.

$$
\begin{aligned}
&\text{DCT-IV}_8 = \\
&\quad [(3,4,7,6,8,5),\ (\omega_4, \omega_{16}^5, \omega_8^3, -\omega_{16}^7, 1, -\omega_{16}, \omega_8, -\omega_{16}^3)] \cdot (\mathrm{DFT}_2 \otimes \mathbf{1}_4) \cdot \\
&\quad \mathrm{diag}(1,1,1,1,1,\omega_8,\omega_4,\omega_8^3) \cdot (\mathbf{1}_2 \otimes \mathrm{DFT}_2 \otimes \mathbf{1}_2) \cdot \\
&\quad \mathrm{diag}(1,1,1,\omega_4,1,1,1,\omega_4) \cdot (\mathbf{1}_4 \otimes \mathrm{DFT}_2) \cdot \\
&\quad \mathrm{diag}(-\omega_{64}, -\omega_{64}, \omega_{64}^9, -\omega_{64}^9, \omega_{64}^{23}, -\omega_{64}^{23}, \omega_{64}^{31}, \omega_{64}^{31}) \cdot \\
&\quad \left(\mathbf{1}_4 \otimes \tfrac{1}{2} \cdot \mathrm{DFT}_2\right) \cdot \mathrm{diag}(1,1,1,-\omega_4,1,1,1,-\omega_4) \cdot \\
&\quad \left(\mathbf{1}_2 \otimes \tfrac{1}{2} \cdot \mathrm{DFT}_2 \otimes \mathbf{1}_2\right) \cdot \mathrm{diag}(1,1,1,1,1,-\omega_8^3,-\omega_4,-\omega_8) \cdot \\
&\quad \left(\tfrac{1}{2} \cdot \mathrm{DFT}_2 \otimes \mathbf{1}_4\right) \cdot [(2,6,3,4,7,5,8),\ (\omega_4, \omega_{16}^5, -\omega_{16}^7, \omega_8, \omega_8^3, -\omega_{16}^3, -\omega_{16}, 1)].
\end{aligned}
$$

Die ersten und die letzten drei Zeilen entsprechen den Zerlegungsmatrizen der monomialen Darstellungen der Symmetrie. Die mittlere Diagonalmatrix ist aus dem Intertwiningraum der zerlegten Darstellungen.

4.6 Haartransformation

Die Haartransformation HT_{2^k} wird rekursiv definiert:

$$
\mathrm{HT}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \ \mathrm{HT}_{2^{k+1}} = \begin{bmatrix} \mathrm{HT}_{2^k} & \otimes [1 \quad 1] \\ 2^{k/2} \cdot \mathbf{1}_{2^k} & \otimes [1 \ -1] \end{bmatrix}, \ k > 1.
$$

Die Haartransformation kann als die erste Wavelettransformation betrachtet werden, siehe Haar (1910), [32]. Wie fast alle Wavelettransformationen kann sie anhand ihrer rekursiven Konstruktion mit $O(2^k)$ Additionen und Multiplikationen berechnet werden.

Symmetrietyp	Gruppe	Größe	Eigenschaften
Mon-Mon (ϕ_1, ϕ_2) (Ordnung 2)	?	2^{2^k+1}	ϕ_1 ist transitiv $\Leftrightarrow k = 1$ ϕ_2 ist transitiv

Tabelle 4.6: Symmetrie der HT_{2^k}

Wie wir in der Tabelle sehen, besitzt die Haartransformation eine exponentiell große Symmetriegruppe, was es sehr schwer macht, den Isomorphietyp zu bestimmen. Für $k = 1 \ldots 4$ ergab sich, daß der linke Teil ϕ_1 der Symmetrie eine permutierte direkte Summe irreduzibler Darstellungen ist, so daß wir es sogar mit einer Mon-Irred-Symmetrie (eigentlich Irred-Mon-Symmetrie) zu tun haben. Die Zerlegung der Haartransformation ergibt sich aus ihrer rekursiven Definition. So ist zum Beispiel für $k = 3$:

$$
\mathrm{HT}_8 = \left(\mathrm{DFT}_2 \oplus \sqrt{2} \cdot \mathbf{1}_2 \oplus \mathbf{1}_4\right) \cdot \left(\begin{bmatrix} \mathbf{1}_2 \otimes [1 \quad 1] \\ \mathbf{1}_2 \otimes [1 \ -1] \end{bmatrix} \oplus 2 \cdot \mathbf{1}_4 \right) \cdot \begin{bmatrix} \mathbf{1}_4 \otimes [1 \quad 1] \\ \mathbf{1}_4 \otimes [1 \ -1] \end{bmatrix}.
$$

Hierbei wird mehrfach eine Einheitsmatrix mit einer (1×2)-Matrix tensoriert, was bei einer automatisch erzeugten Zerlegung nicht auftreten kann (bei der Zerlegung einer Darstellung treten nur quadratische Matrizen auf). Der dritte Faktor läßt sich aber beispielsweise durch Multiplikation mit Permutationsmatrizen in ein Tensorprodukt $\mathbf{1}_4 \otimes \mathrm{DFT}_2$ verwandeln. Transformiert man die obige Zerlegung in dieser Weise, erhält man im wesentlichen die Zerlegung, die unser Algorithmus liefert. Bei einer Gruppengröße von 512 wurden insgesamt 20 s benötigt.

$$
\begin{aligned}
\mathrm{HT}_8 = &\\
&[(1,8,6,4,2,7,5,3),\ 8]\cdot\\
&\left(\mathrm{diag}\left(-\sqrt{2},\sqrt{2}\right) \oplus \mathbf{1}_4 \oplus \mathrm{DFT}_2\right)\cdot\\
&[(1,5,4,8,6,3,7,2),\ 8]\cdot\\
&(\mathbf{1}_2 \otimes ([(1,2),\ 4]\cdot(\mathrm{DFT}_2 \oplus 2\cdot \mathbf{1}_2)\cdot[(2,3),\ 4]\cdot(\mathbf{1}_2 \otimes \mathrm{DFT}_2)))\cdot\\
&[(1,8,4,7)(3,6,2,5),\ (1,1,1,1,-1,-1,-1,-1)].
\end{aligned}
$$

Anhang A

AREP – ein Softwarepaket zur konstruktiven Darstellungstheorie

Im Rahmen dieser Dissertation entstand in Zusammenarbeit mit Sebastian Egner das Softwarepaket AREP zum Rechnen mit Matrixdarstellungen von Gruppen. Die benutzte Programmiersprache ist GAP, [57], Version 3.4.4. AREP wird ab Mitte 98 als GAP Share Package zur Verfügung stehen.
Das Paket gliedert sich in drei Teile:

1. Die Kategorie `AMat` (**A**bstract **Mat**rices) stellt die Datentypen und Funktionen zum Rechnen mit strukturierten Matrizen bereit.

2. Entsprechend sind in `ARep` (**A**bstract **Rep**resentations) die Datentypen und Funktionen zum Rechnen mit Matrixdarstellungen endlicher Gruppen implementiert.

3. Im dritten Teil werden höhere Funktionen zum Rechnen mit Darstellungen bereitgestellt. Diese basieren auf Ergebnissen der Kapitel 1 und 2.

Es folgt die entsprechend gegliederte Dokumentation in Englisch.

```
The category AMat of structured matrices
========================================

The category AMat contains elements representing matrices
(rectangular matrices over GAP-fields) in a structured way.
In fact AMat is a term-algebra representing matrices. Basic
building blocks are literal matrices (Lists of Lists), monomial
matrices and permutation matrices (Permutations). Important
compositions are sums, products, direct sums (diag) and
tensor products.
```

```
We define the representation of AMat recursively in BNF as
the disjoint union of the following cases

<AMat> ::=
; atomic cases
    <perm>                                  ; "perm" (invertible)
  | <mon>                                   ; "mon"  (invertible)
  | <mat>                                   ; "mat"

; composed cases
  | <scalar> * <AMat>                       ; "scalarMultiple"
  | <AMat> * .. * <AMat>                    ; "product"
  | <AMat> ^ <int>                          ; "power"
  | <AMat> ^ <AMat>                         ; "conjugate"
  | DirectSum(<AMat>, .., <AMat>)           ; "directSum"
  | TensorProduct(<AMat>, .., <AMat>)       ; "tensorProduct"
  | GaloisConjugate(<AMat>, <aut>)          ; "galoisConjugate".

An AMat is a GAP-Rec A with the following mandatory
fields common to all types of AMat

  isAMat       := true, identifies AMats
  operations   := AMatOps, GAP operations record for A
  type         : a string identifying the type of A
  dimensions   : size of the matrix represented
                 (= [rows, columns])
  char         : the characteristic of the field

The following fields are mandatory to special types

A.type = "perm"
  A.element      : defining permutation

A.type = "mon"
  A.element      : defining mon-object

A.type = "mat"
  A.element      : defining matrix
  A.isDFT        : optional field indicating that A is a DFT
  A.isSOR        : optional field indicating that A is a SOR

A.type = "scalarMultiple"
  A.element      : the AMat multiplied
  A.scalar       : the scalar

A.type = "product"
  A.factors      : List of AMats of suitable dimensions
                   and characteristic
A.type = "power"
  A.element      : the square AMat to be raised to A.exponent
```

```
  A.exponent     : the exponent (an integer)

A.type = "conjugate"
  A.element      : the square AMat to be conjugated
  A.conjugation  : the conjugating invertible AMat

A.type = "directSum"
  A.summands     : List of AMats of the same characteristic

A.type = "tensorProduct"
  A.factors      : List of AMats of the same characteristic

A.type = "galoisConjugate"
  A.element      : the AMat to be Galois conjugated
  A.galoisAut    : the Galois automorphism

Optional fields for all types of AMats

  A.name         : a string for the name
  A.isInvertible : flag to indicate, that A is invertible
  A.inverse      : an AMat representing A^-1
  A.determinant  : the determinant of A
  A.trace        : the trace of A
  A.rank         : the rank of A
  A.isPermMat    : a flag indicating that A is a
                   permutation matrix
  A.perm         : the perm represented by A
  A.isMonMat     : a flag indicating that A is a
                   monomial matrix
  A.mon          : the mon represented by A
  A.mat          : the mat represented by A
  A.isSimplified : a flag indicating, that A is simplified
                   by the function SimplifyAMat

Fundamental Constructors and Tests for AMats
--------------------------------------------

IsAMat( <obj> )
  tests whether <obj> is an AMat. The particular case of AMat
  is provided by A.type and the additional fields are available
  directly from the record.

IsInvertibleMat( <amat> )
  tests if <amat> is invertible and sets the field
  <amat>.isInvertible.

IsIdentityMat( <amat> )
  checks whether <amat> is a square IdentityMat.

IdentityPermAMat( <size> [, <char/field> ] )
```

```
IdentityMonAMat( <size> [, <char/field> ] )
IdentityMatAMat( <size> [, <char/field> ] )
IdentityMatAMat( <dimensions> [, <char/field> ] )
  construct an "perm"/"mon"/"mat"-amat representing
  the identity matrix of size <size>. In the case "mat"
  the matrix may be rectangle containing at the position
  (i, j) one, if i = j and zero else.

AllOneAMat( <size> [, <char/field> ] )
AllOneAMat( <dimensions> [, <char/field> ] )
  constructs the all-one matrix of type "mat" of given
  size and characteristic. The default characteristic is 0.

NullAMat( <size> [, <char/field> ] )
NullAMat( <dimensions> [, <char/field> ] )
  construct the all-zero matrix of type "mat" of given
  size and characteristic. The default characteristic is 0.

DiagonalAMat( <list> )
  construct the amat having <list> as diagonal. If all
  elements of <list> are <> 0, then the resulting amat
  is of type "mon", else of type "directSum".
  Note that the elements of list must lie in a common
  field.

DFTAMat( <size> [, <char/field>] )
  constructs a "mat"-amat representing a DFT of
  size <size>. The default characteristic is 0.
  If <char> is given, then a DFT is constructed
  iff <size> and <char> are coprime, if <field> is
  given, then a DFT is constructed iff <size>
  divides Size(<field>) - 1.
  The field <amat>.isDFT is set.

SORAMat( <size> [, <char/field>] )
  constructs a "mat"-amat representing an SOR of
  size <size>. SOR(n) (Split One Rep) is defined
  as the following (n x n) - matrix

             _                  _
            |1  1  1  1  .  .    |
            |1 -1  0  0          |
            |1  0 -1  0          |
   SOR(n) = |1  0  0 -1          |
            |.           .       |
            |.              .    |
            |                    |

  The SOR(n) is the sparsest matrix that splits off
  the onerep contained in a permrep. The number of
```

```
  entries is 3n - 2.
  The default characteristic is 0. The field
  <amat>.isSOR is set.

AMatPerm( <perm>, <degree> [, <char/field> ] )
  constructs a "perm"-amat from <perm> of given degree
  <degree> and characteristic <char/field>.

AMatMon( <mon> )
  constructs a "mon"-amat from <mon>.

AMatMat( <mat> [, <hint>] )
  constructs a "mat"-amat from <mat>. The <hint>
  "invertible" may be given.

Structural Symbolic Constructors for AMats
------------------------------------------

ScalarMultipleAMat( <scalar>, <amat> )
  forms the amat of type "scalarMultiple" representing
  the scalar multiple of <scalar> and <amat>, which must
  have the same characteristic. In addition, the integers
  operate on the finite fields. Hence, -<amat> is possible.

<amat> * <amat>
<scalar> * <amat>
  forms the product resp. the scalarMultiple. In the first
  case the sizes must be compatible, in both cases the
  characteristic must be compatible. In addition, the integers
  operate on the finite fields. Hence, -<AMat> is admissible.
<amat> / <amat>
  forms the quotient of the amats. Characteristic and
  size have to be compatible, the second amat must be
  square and invertible.

PowerAMat( <amat>, <int> [, <hint> ] )
  forms the amat <amat> ^ <int> of type "power". If <int>
  is negative then <amat> is checked for invertibility if
  not the hint "invertible" is supplied.

ConjugateAMat( <amat1>, <amat2> [, <hint> ] )
  forms the conjugate <amat1> ^ <amat2> of type "conjugate" .
  The amat <amat2> is checked if it is invertible if not the
  hint "invertible" is supplied

<amat> ^ <int>
<amat> ^ <amat>
  forms the power of an amat resp. the conjugate of
  an amat by another amat. The amats have to be square.
```

```
DirectSumAMat( <amat1>, .., <amatN> ) ; N >= 1
DirectSumAMat( <list-of-amat> )
  forms the direct sum of the amats given. Note that the
  amats does not have to be square, but must be of common
  characteristic.

TensorProductAMat( <amat1>, .., <amatN> ) ; N >= 1
TensorProductAMat( <list-of-amat> )
  forms the tensor (or kronecker) product of the
  amats given. Note that the amats does not have to be
  square, but must be of common characteristic.

GaloisConjugateAMat( <amat>, <gal-aut/int> )
  forms the Galois-conjugate of A under the field automorphism
  aut. The automorphism may be specified by an integer k.
  In case of a finite field
    aut = FrobeniusAutomorphism(A.baseField)^k.
  In case of a number field (in GAP a subfield of a cyclotomic
  field) it is
    aut = NFAutomorphism(A.baseField, k) = x -> GaloisCyc(x, k).

Pretty Printing of AMats
------------------------

AMatOps.Print( <amat> [, <indent> , <indentStep> , <bp> ] )

Fundamental Operations with AMats
---------------------------------

InverseAMat( <amat> )
  returns an amat representing the inverse of
  <amat> if possible. The calculation uses the fact,
  that inversion is compatible with most of the
  structures represented by an mat.

DeterminantAMat( <amat> )
  calculates the determinant of <amat> if it is square
  and stores the result in <amat>.determinant

TraceAMat( <amat> )
  calculates the trace of <amat> if it is square
  and stores the result in <amat>.trace

RankAMat( <amat> )
  calculates the rank of <amat>. The result is stored
  in A.rank.

Flattening out AMats
--------------------
```

```
IsPermMat( <amat> )
IsMonMat( <amat> )
  test if <amat> can be flattened into a "perm" or "mon" amat.
  The result is memorized in <amat>.isPermMat/.isMonMat.
  A "mon" amat is always invertible!
  Note that the names of the operations are not IsPermAMat,
  IsMonAMat since <amat> can be of any type but represents
  a permutation/monomial matrix in a mathematical sense.

PermAMat( <amat> )
MonAMat( <amat> )
MatAMat( <amat> )
  converts <amat> into a Perm/Mon/Mat-object and memorizes
  the result in <amat>.perm/mon/mat. If <amat> cannot be
  converted then false is returned.

PermAMatAMat( <amat> )
MonAMatAMat( <amat> )
MatAMatAMat( <amat> )
  construct a "perm"/"mon"/"mat"-amat equal to <amat> if
  possible or returns false otherwise.

Simplifying AMats
-----------------

SimplifyAMat( <amat> )
  simplifies <amat>, e.g. by removing identity matrices
  in products.

Functions for AMats
-------------------

kbsAMat( <amat1>, .., <amatN> ) ; N >= 1
kbsAMat( <list-of-amat> )
  calculates the joined kbs of the amats given
  (cf. kbs() in permblk.g).

SubmatrixAMat( <amat>, <list-of-indices> )
  calculates the submatrix of amat obtained by
  extracting all components with indices in <inds>.
  A "mat"-amat is returned.

kbsDecompositionAMat( <amat> )
  decomposes <amat> into a conjugated (by a "perm"-amat)
  direct sum of "mat"-amats as far as possible.

LinearComplexityAMat( <amat> )
  computes an upper bound for the linear complexitiy
  according to the model of Clausen.
```

```
Abstract Representations of Finite Groups (ARep)
================================================

The class ARep provides a term algebra for matrix
representations of finite groups. This means there
are a number of symbolic constructions for AReps
like direct sum or Galois conjugation which return
expressions (terms) in the original representations.
  The strategy for simplification of the expressions
is to construct even trivial expressions and provide
functions to apply simplifications. Hence, a term
can be R^id unless you explicitly request simplification.

<ARep> ::=
; atomic cases
    <perm>                                 ; "perm"
  | <mon>                                  ; "mon"
  | <mat>                                  ; "mat"

; composed cases
  | <ARep> ^ <AMat>                        ; "conjugate"
  | DirectSum(<ARep>, .., <ARep>)          ; "directSum"
  | InnerTensorProduct(<ARep>, .., <ARep>) ; "innerTensorProduct"
  | OuterTensorProduct(<ARep>, .., <ARep>) ; "outerTensorProduct"
  | GaloisConjugate(<ARep>, <aut>)         ; "galoisConjugate".
  | Restriction(<ARep>, <subgrp>)          ; "restriction"
  | Induction(<ARep>, <supergrp>)          ; "induction"
  | Extension(<ARep>, <ext-char>)          ; "extension"

An ARep is a GAP-Rec R with the following
mandatory fields common to all types of ARep

  R.isARep       := true, identifies AReps
  R.operations   := ARepOps, GAP-operations record of R
  R.char         : characteristic of the base field
  R.degree       : degree of the representation
  R.source       : group being represented; the group must
                  contain a list R.source.theGenerators
                  of generators which are never changed;
                  representations are specified by giving
                  images for R.source.theGenerators
  R.type         : string identifying the type of ARep

The following fields are mandatory to special types

R.type = "perm"
  R.theImages    : list of Perms for the images of
                   R.source.theGenerators
  R.isTransitive : optional field to indicate, that
                   R is transitive
```

```
  R.transitivity : optional field containing the degree of
                   transitivity of R, at the moment
                   this is an integer
  R.induction    : optional field containing a conjugated
                   (by a "mon"-AMat) "induction"-ARep of a
                   one dimensional "mon"-ARep equal to R

R.type = "mon"
  R.theImages    : list of Mons (cf. mon.g)
  R.isTransitive : optional field to indicate, that
                   R is transitive
  R.transitivity : optional field containing the degree of
                   transitivity of R, at the moment
                   this is an integer
  R.induction    : optional field containing a conjugated
                   (by a "mon"-AMat) "induction"-ARep of a
                   one dimensional "mon"-ARep equal to R

R.type = "mat"
  R.theImages    : list of Mats

R.type = "conjugate"
  R.rep          : an ARep to be conjugated
  R.conjugation  : an AMat conjugating R.rep

R.type = "directSum"
  R.summands     : list of AReps of the same R.source, R.char
                  The sources of the areps is the same GAP-Rec.

R.type = "innerTensorProduct"
  R.factors      : list of AReps of the same R.source, R.char
                  The sources of the areps is the same GAP-Rec.

R.type = "outerTensorProduct"
  R.isOuter      : flag to indicate that R.source is the
                  outer direct product of the sources of
                  the factors; otherwise R.source is the
                  inner direct product of the sources of
                  the factors (which are normal subgroups)
  R.factors      : list of AReps of the same R.char; note that
                  the R.source is the direct product of all
                  Rk.source for Rk in R.factors
  R.projections  : list of group homomorphisms from R.source
                  into R.factors[i].source; the individual
                  entries of this list may be empty if
                  the projection has not been used before
  R.embeddings   : list of group homomorphisms from the
                  sources of the factors into R.source; the
                  entries may be empty if the embeddings
                  have not been used before
```

```
R.type = "galoisConjugate"
  R.rep          : an ARep to be conjugated
  R.galoisAut    : a Galois automorphism or an integer for
                   the Galois conjugation in CF(n) or GF(p^n)

R.type = "restriction"
  R.rep          : an ARep of a supergroup of R.source;
                   the group R.source and R.rep.source
                   have a common parent group

R.type = "induction"
  R.rep          : an ARep of a subgroup of R.source;
                   the group R.rep.source has the same
                   parent group as R.source
  R.transversal  : a transversal of Cosets(R.source, R.rep.source)

R.type = "extension"
  R.rep          : an irreducible ARep of a subgroup of
                   R.source with R.rep.character being bound;
                   the groups R.source and R.rep.source share
                   a common parent group
  R.character    : the irreducible character of the extended
                   representation of R.source such that the
                   restriction to R.rep.source is R.rep.character

Optional fields common to all types of ARep

  R.character     : the GAP-character belonging to R
  R.isIrreducible : set if R is known to be irreducible or not
  R.kernel        : the kernel of R if known
  R.hom           : the GAP-group homomorphism corresponding
                    to R constructed as
                      GroupHomomorphismByImages(
                        R.source,              Group(R.theImages),
                        R.source.theGenerators, R.theImages )
  R.name          : field to give a name to R
  R.isPermRep     : flag to indicate if R can be replaced by
                    a "perm"-ARep equal to R
  R.permARep      : the "perm"-ARep equal to R
  R.isMonRep      : flag to indicate if R can be replaced by
                    a "mon"-ARep equal to R
  R.monARep       : the "mon"-ARep equal to R
  R.matARep       : a "mat"-ARep equal to R

Fundamental Constructors for AReps
----------------------------------

IsARep( <obj> )
  tests of <obj> is an ARep.
```

```
TrivialPermARep( <grp>, [, <degree> [,<char/field> ] )
TrivialMonARep(  <grp>, [, <degree> [,<char/field> ] )
TrivialMatARep(  <grp>, [, <degree> [,<char/field> ] )
  the "perm"/"mon"/"mat"-ARep of mapping every group element
  onto a one of degree <degree>. The default for the degree is 1,
  the  default for the characteristic is 0.

RegularARep( <grp> [, <char/field> ] )
  returns an "induction"-arep of the onerep on
  the trivial subgroup of <grp>.

NaturalARep( <matgrp> )
NaturalARep( <mongrp> )
NaturalARep( <permgrp>, <degree> [, <char/field> ] )
  a group taken as a representation of itself.

ARepByImages( <grp>, <list-of-perm>, <degree>
              [, <char/field> ] [, <hint> ] )
ARepByImages( <grp>, <list-of-mon> [, <hint> ] )
ARepByImages( <grp>, <list-of-mat> [, <hint> ] )
  the representation defined by mapping the list of generators
  grp.theGenerators pointwise onto the elements of the list
  given as the second argument. The optional argument <hint>
  is a string which gives a hint to avoid the check if the
  list of images actually defines a group homomorphism. The
  possible hints are "hom" (image do define a homomorphism)
  and "faithful" (image define an injective homomorphism).

ARepByHom( <grphom-to-matgrp> )
ARepByHom( <grphom-to-mongrp> )
ARepByHom( <grphom-to-permgrp>, <degree> [, <char/field> ] )
  the representation defined by a group homomorphism.

ARepByCharacter( <1dim-character> )
  the monomial representation defined by a
  1-dimensional character.

Structural Symbolic Constructors for AReps
------------------------------------------

ConjugateARep( <arep>, <amat> [, <hint> ] )
<arep> ^ <amat> ; shorthand
  the representation <arep> conjugated with an invertible matrix
  represented by <amat>, an object of type AMat. Note that the
  <hint> can be the string "invertible" to avoid the check for
  <amat> to be invertible.

DirectSumARep( <arep1>, .., <arepN> ) ; N >= 1
DirectSumARep( <list-of-areps> )
```

```
  direct sum of AReps. Note that the areps have to represent a
  common group in a common characteristic.

InnerTensorProductARep( <arep1>, .., <arepN> ) ; N >= 1
InnerTensorProductARep( <list-of-areps> )
  inner tensor product of AReps. Note that the areps have to
  represent a common group in a common characteristic.

OuterTensorProductARep( [ <grp> ,] <arep1>, .., <arepN> ) ; N >= 1
OuterTensorProductARep( [ <grp> ,] <list-of-arep> )
  outer tensor product of AReps. Note that the areps have to
  have a common characteristic. If the first argument is the
  optional <grp>, then this group is the source of the result.
  Note that <grp> has to be the inner direct product of the
  sources of all factors and that this is not tested! If no
  <grp> is given, then the GAP-function DirectProduct() is
  used to construct the outer direct product of the sources
  of the factors.

GaloisConjugateARep( <arep>, <gal-aut/int> )
  the Galois conjugate of <arep> with the galois conjugation
  defined by <gal-aut/int>. This can be a field automorphism
  or an integer k, in which case x -> x^(FrobeniusAut^k) or
  x -> GaloisCyc(x, k) is meant.

RestrictionARep( <arep>, <subgrp> )
  the representation <arep> restricted to a subgroup.
  It is allowed that <subgrp> does not have the same
  parent group as <arep>.source.

InductionARep( <arep>, <supergroup> [, <transversal> ] )
  the induced representation <arep> on the <supergroup>.
  If no transversal is provided then the function will
  choose one as [t_1, .., t_r]. The convention for the
  induction is RG = g -> [ RHDot(t_i g t_j^-1) | i, j ],
  what implies, that [t_1, .., t_r] is a right transversal.
  It is allowed that <supergroup> does not have the same
  parent group as <arep>.source. The given <transversal>
  is not checked to be one.

ExtensionARep( <arep>, <extending-character> )
  the representation <arep> extended to a representation
  of a supergroup affording the extending character.
  Note that the extending character and the character of
  <arep> must both be irreducible. (The extension is
  evaluated using Minkwitz's extension formula.)
  It is allowed that <supergroup> does not have the same
  parent group as <arep>.source.
```

```
Pretty Printing of AReps
------------------------

GroupWithGenerators( <group> )
GroupWithGenerators( <list-of-grpelts> )
  construct a group with the field .theGenerators being
  set to a fixed non-empty generating list. If <group>
  is given then this group record is modified by adding
  the field .theGenerators if this does not exist already.
  If <list-of-grpelts> is given then this must be a non-
  empty list of group elements acting as the fixed generating
  list of the resulting group.

ARepOps.Print( <arep> [, <indent> ] )
  prints the <arep> beginning at the current cursor
  position which is assumed to be at the beginning
  of a line, indented at <indent> spaces.

Fundamental Operations with AReps
---------------------------------

ImageARep( <grpelt/list-of-grpelts>, <arep> )
<grpelt> ^ <arep> ; shorthand
  evaluates the ARep at the group element;
  the result is an AMat.

IsEquivalentARep( <arep1>, <arep2> )
  determines, whether <arep1> and <arep2> are equivalent
  representations of the same source and char.

CharacterARep( <arep> )
  the character of the representation. The result
  is stored in <arep>.character.

IsIrreducibleARep( <arep> )
  determines if <arep> is an irreducible representation.

KernelARep( <arep> )
  the kernel of the representation.

IsFaithfulARep( <arep> )
  determines if <arep> is an injective homomorphism.

Flattening Out AReps
--------------------

IsPermRep( <arep> )
IsMonRep(  <arep> )
  test if <arep> can be turned into a "perm" or "mon" ARep.
  The result is memorized in .isPermRep/.isMonRep. Note that
```

```
  the names of the operations are *not* 'IsPermARep' etc.
  since <arep> can be any type but it *represents* a
  permutation representation in the mathematical sense.

PermARepARep( <arep> )
MonARepARep(  <arep> )
MatARepARep(  <arep> )
  constructs a "perm"/"mon"/"mat"-ARep equal to the
  given <arep> or returns false if this is not possible.
  The result is memorized in .permARep/.monARep/.matARep.
```

```
Constructive Representation Theory
==================================

Based on the class ARep a number of functions is
provided to calculate with representations. The
most functions deal with permutation and monomial
representations and are decompositions in a sense.

Functions for Characters
------------------------

IsRestrictedCharacter( <chi>, <chisub> )
  tests if <chisub> is a restriction of <chi>.

AllExtendingCharacters( <chi>, <supergrp> )
  calculates the list of all irreducible characters
  of <supergrp> whose restriction is the irreducible
  character <chi>.

OneExtendingCharacter( <character>, <supergroup> )
  calculates a character of <supergroup> extending
  <character> or returns false.

Intertwining Space of Representations
-------------------------------------

IntertwiningSpaceARep( <arep1>, <arep2> )
  computes a base of the intertwining space
    Int( <arep1>, <arep2> ) = { M | <arep1> M = M <arep2> }
  represented by a list of amats.
  The convention for the intertwining space follows
  Clausen, Baum. It is consistent with Minkwitz.
  Note that Int( <arep1>, <arep2> ) consists of
  deg(rep2) x deg(rep1)-matrices.

IntertwiningNumberARep( <arep1>, <arep2> )
  calculates the intertwining number of <arep1>, <arep2>
  which is the dimension of the intertwining space
  or the scalar product of the characters resp.

Functions for Permutation and Monomial Representations
------------------------------------------------------

UnderlyingPermARep( <arep> )
  constructs the underlying permrep of the monrep <arep>
  as a "perm"-ARep, which can be obtained by replacing
  all entries in the monomial matrices by 1 (in the
  suitable field).

IsTransitiveMonRep( <arep> )
```

```
  decides whether <arep> is a transitive monrep or not.
  The result is stored in the field <arep>.isTransitive.

IsPrimitiveMonRep( <arep> )
  decides whether <arep> is a primitive monrep or not.

TransitivityDegreeMonRep( <arep> )
  returns the transitivity degree of the monrep <arep>

OrbitDecompositionMonRep( <arep> )
  decomposes the monrep <arep> with respect to the
  orbits as
    <arep> = DirectSum(R1, .., Rn) ^ P
  where R1 .. Rn are "mon"-AReps and P denotes a
  "perm"-AMat.

TransitiveToInductionMonRep( <arep> [, <point> ] )
  decomposes a transitive monrep <arep> as
    <arep> =
      ConjugateARep(
        InductionARep(L, <arep>.source, T),
        D
      )
  where Stab is the stabilizer of <point>, L a onedimensional
  "mon"-arep of Stab and D a diagonal "mon"-AMat. The list
  T is a transversal of Stab in <arep>.source.
  The default for <point> is the largest point (<arep>.degree).
  If <arep> is a permrep then D is the IdentityMonAMat of
  suitable size and char. If <point> = <arep>.degree, then
  the result is stored in <arep>.induction.

DirectSumOfInducedMonRep( <arep> )
  decomposes a monrep <arep> with respect to the
  orbits into a conjugated (by a "mon"-AMat) direct
  sum of induced onedimensional "mon"-AReps.

General Functions
-----------------

kbsARep( <arep> )
  determines the conjugated block structure of <arep>
  (cf. kbs in permblk.g). Note that if <arep> is
  monomial, the kbs is exactly the list of orbits
  of <arep> on [1..R.degree].

Decomposing Representations
---------------------------

InsertedInductionARep( <"induction"-arep>, <group> )
  given an "induction"-ARep RUG = InductionARep(RU, G)
```

```
  and the <group> H such that U <= H <= G, this function
  decomposes RUG into
    RUG = InductionARep(InductionARep(RU, H), G) ^ M
  where M is an AMat with structure similar to the
  induced representation RUG.

ConjugationPermLists (
  [ <permgrp>,] <list-of-perm1>, <list-of-perm2>
)
  calculates a permutation p in <permgrp> which conjugates
  <list-of-perm1> elementwise onto <list-of-perm2>.
  The default for <permgrp> is the symmetric group on degree
  many points.

ConjugationTransitivePermReps( <arep1>, <arep2> )
  returns a "perm"-amat p on <arep1>.degree many points
  such that <arep1> ^ p = <arep2> and false if this is
  not possible. The areps must have common source and
  characteristic.

ConjugationTransitiveMonReps( <arep1>, <arep2> )
  returns a "mon"-amat m on <arep1>.degree many points
  such that <arep1> ^ m = <arep2> and false if this is
  not possible. The areps must have common source and
  characteristic.

ConjugationPermReps( <arep1>, <arep2> )
  returns for permutation areps <arep1>, <arep2> a
  "perm"-amat p on <arep1>.degree many points such
  that <arep1> ^ p = <arep2> and false if this is
  not possible. The areps must have common source
  and characteristic.

TransversalChangeInductionARep(
  <"induction"-arep>, <transversal> [, <hint> ]
)
  Given an "induction"-ARep R,
    R = InductionARep(L, G, T)
  and a <transversal> of L.source\G, R is decomposed as
    R = InductionARep(L, G, <transversal>) ^ M.
  If L is a monrep (e.g. L.degree = 1), then M is a
  "mon"-AMat, else an AMat with a structure similar to R.
  The <hint> "isTransversal" can be supplied to avoid
  testing it.

OuterTensorProductDecompositionMonRep( <arep> )
  decomposes the transitive monrep <arep> into a
  conjugated (by a "mon"-AMat) outer tensorproduct
  of "mon"-AReps as far as possible, namely
    <arep> =
```

```
      ConjugateARep(
        OuterTensorProductARep(
          <arep>.source,
          "mon"-ARep1, .., "mon"-ARepN
        ),
        M
      )
  with a monomial matrix M.

InnerConjugationARep( <arep>, <supergroup>, <element> )
  calculates <arep> ^ <element> as representation of
  <arep>.source ^ <element>, <element> must lie in <supergroup>.
  For a representation R of H <= G, and an
  element t in G the representation R ^ t is defined as
    (R ^ t)(x) = R(t x t^-1) for all x in H ^ t.
  The returned arep is of type "perm", "mon" or "mat",
  whatever poosible.
  If H is normal in G, then R ^ t is returned as rep of H,
  else  H ^ t is constructed as a group with
    (H ^ t).theGenerators = H.theGenerators ^ t.

RestrictionInductionARep( <"induction"-arep>, <subgroup> )
  Given an <"induction"-arep> R of G, induced from a
  onedimensional representation L of a subgroup H <= G
  and a <subgroup> K of G, the function calculates
  an arep equal to R decomposing (R restriction K)
  according to Mackey's subgroup theorem.
  If s_1, .., s_k represent the double cosets H\G/K,
  the the decomposition is given by
    (R restriction K) =
      ConjugateARep(
        DirectSumARep(
          InductionARep(R_i, K),
          i = 1..k
        ),
        M
      ),
   where M is a monomial matrix and R_i are onedimensional
   "mon"-areps obtained by restricting L^(s_i) to
   (H^(s_i) intersect K).

AllMaximalNormalSubgroupsBetween( <group>, <subgroup> )
  calculates all normal subgroups N of <group> with
    <subgroup> <= N < <group> and (<group> : N) = prime,
  if no such N exists, then false is returned.

OneMaximalNormalSubgroupBetween( <group>, <subgroup> )
  calculates one normal subgroup N of <group> with
    <subgroup> <= N < <group> and (<group> : N) = prime,
  if no such N exists, then false is returned.
```

```
RestrictionToSubmoduleARep( <arep>, <list> [, <hint> ] )
  calculates the restriction of <arep> to
  the submodule generated by the basevectors
  with the indices in <list>.
  The optional hint "hom" indicates, that the restriction
  yields a representation, i.e. that <list-of-posints>
  is contained in the kbs of <arep>.
  The restriction is of type "perm", "mon", "mat", if
  <arep> is a perm-, mon-, matrep.

kbsDecompositionARep( <arep> )
  decomposes <arep> into a conjugated direct sum
  according to the kbs (cf. permblk.g) as far as
  possible
    <arep> =
      ConjugateArep(
        DirectSumARep( <arep1>, .., <arepN> ),
        P
      )
  with a permutation matrix P. For monreps this
  function does exactly the same as the function
  OrbitDecompositionMonRep.
  The <arepi> are of type "perm", "mon", "mat", if
  <arep> is  a perm-, mon-, matrep resp.

ExtensionOnedimensionalAbelianRep( <arep>, <group> )
  calculates an extension of an <arep> of degree 1 of
  a subgroup H of <group>, if <group>/kernel(R) is abelian.
  The extension is a "mon"-arep and chosen to be over the
  smallest possible extension field. No character theory is used.

ARepWithCharacter( <chi> )
  calculates an arep with character <chi>.
  The group must be solvable.

DecompositionMonRep( <arep> [, <hint> ] )
  decomposes <arep> into irreducibles and determines
  a factorized decomposition matrix A. More precisely
  <arep> is decomposed as
    <arep> =
      ConjugateARep(
        DirectSumARep(R_i, i = 1..k),
        A ^ -1
      )
  where all R_i are irreducible. The R_i are ordered
  according to their character with the exception, that
  the trivial onerep is the smallest rep. Equivalent
  R_i are equal.
  If the <hint> "noOuter" is supplied, <arep> is not
```

```
checked to be an outer tensor product.
Note, that the decomposition matrix A is accessible by
A = R.conjugation.element. A is simplified by the
function SimplifyAMat.
The structure of A represents a fast algorithm for
multiplication with A.
```

Literaturverzeichnis

[1] Agarwal, R. C., und Cooley, J. W. New algorithms for digital convolution. *IEEE Trans. Acoustics, Speech, and Signal Processing ASSP-25* (1977), 392–410.

[2] Apple, G., und Wintz, P. Calculation of Fouriertransforms on Finite Abelian Groups. *IEEE Trans. Inform. Theory IT-16* (1970), 233–236.

[3] Atkinson, M. *Computational Group Theory.* Academic Press, 1984.

[4] Beauchamp, K. *Applications of Walsh and related functions.* Academic Press, 1984.

[5] Besche, H. U., und Eick, B. The Groups of Order up to 1000, except 512 and 768. *http://www-gap.dcs.st-and.ac.uk/~gap/Info/datalib.html* (1996).

[6] Beth, T. *Methoden der Schnellen Fouriertransformation.* Teubner Verlag, 1984.

[7] Beth, T. On the computational complexity of the general discrete Fourier transform. *Theoretical Computer Science 51* (1987), 331–339.

[8] Beth, T., und Grassl, M. Improved decoding of quantum error correcting codes from classical codes. In *PhysComp96* (1996), T. Toffoli, M. Biafore, und J. Leao, Hrsg.

[9] Beth, T., Jungnickel, D., und Lenz, H. *Design Theory.* BI-Wiss.-Verl., 1985.

[10] Bluestein, L. I. A linear filtering approach to the computation of the discrete fourier transform. *IEEE Trans. AU-18 18* (1970), 451–455.

[11] Buekenhout, F. *Handbook of Incidence Geometry.* Elsevier, North Holland, 1995.

[12] Butler, G. *Fundamental Algorithms for Permutation Groups.* Lecture Notes in Computer Science, 559. Springer, 1991.

[13] Clausen, M. *Beiträge zum Entwurf schneller Spektraltransformationen (Habilitationsschrift).* Univ. Karlsruhe, 1988.

[14] Clausen, M. Fast generalized Fourier transforms. *Theoretical Computer Science 67* (1989), 55–63.

[15] Clausen, M. A Direct Proof of Minkwitz's Extension Theorem. *Applicable Algebra in Engineering, Communication and Computing 8* (1997), 305–306.

[16] Clausen, M., und Baum, U. *Fast Fourier Transforms.* BI-Wiss.-Verl., 1993.

[17] Colbourn, C., und Dinitz, J. *The CRC Handbook of Combinatorial Designs.* CRC Press, 1996.

[18] Conway, J. H., Curtis, R. T., Norton, S. P., und Wilson, R. A. *Atlas of Finite Groups.* Clarendon Press, Oxford, 1985.

[19] Cooley, J. W., und Tukey, J. W. An algorithm for the machine computation of complex fourier series. *Mathematics of Computation 19* (1965), 297–301.

[20] Crouch, R. B. Monomial groups. *Trans. Am. Math. Soc. 80* (1955), 187–215.

[21] Curtis, W., und Reiner, I. *Representation Theory of Finite Groups.* Interscience, 1962.

[22] Curtis, W., und Reiner, I. *Methods of Representation Theory,* Vol. 1. Interscience, 1981.

[23] Diaconis, P., und Rockmore, D. Efficient computation of the Fourier transform on finite groups . *Amer. Math. Soc. 3(2)* (1990), 297–332.

[24] Dixon, J., und Mortimer, B. *Permutation Groups.* Springer, 1996.

[25] Dornhoff, L. *Group Representation Theory.* Pure and Applied Mathematics. Dekker New York, 1971.

[26] Egner, S. *Zur Algorithmischen Zerlegungstheorie Linearer Transformationen mit Symmetrie.* Diss., Univ. Karlsruhe, Informatik, 1997.

[27] Egner, S., Püschel, M., und Beth, T. Decomposing a Permutation into a Conjugated Tensor Product. *Proceedings of the ISSAC* (1997), 101–108.

[28] Elliott, D. F., und Rao, K. R. *Fast Transforms — Algorithms, Analyses, Applications.* Academic Press, 1982.

[29] FEIT, W. *The Representation Theory of Finite Groups.* North-Holland, 1982.

[30] FULTON, W., UND HARRIS, J. *Representation Theory.* Springer, 1991.

[31] GAUSS, C. F. *Carl Friedrich Gauss Werke*, Vol. 3. Königliche Gesellschaft der Wissenschaften: Göttingen, 1866.

[32] HAAR, A. Zur Theorie der orthogonalen Funktionen-Systeme. *Math. Ann. 69* (1910), 331–371.

[33] HALL JR., M. *The Theory of Groups.* Chelsea Publ., 1976.

[34] HEIDEMANN, M., JOHNSON, D., UND BURRUS, C. Gauss and the History of the Fast Fourier Transform. *Archive for History of Exact Sciences 34* (1985), 265–277.

[35] HUANG, T. How the Fast Fourier Transform Got its Name . *Computer 3* (1971), 15.

[36] HUPPERT. *Endliche Gruppen I.* Springer, 1967.

[37] JAMES, G., UND KERBER, A. *The representation theory of the symmetric group.* Addison-Wesley, 1981.

[38] JAMES, G., UND LIEBECK, M. *Representations and Characters of Groups.* Cambridge Univ. Press, 1993.

[39] LEON, S. J. Permutation Group Algorithms Based on Partitions, I: Theory and Algorithms . *Journal of Symbolic Computation 12* (1991), 533–583.

[40] LEOPOLDT, H.-W. Darstellungstheorie endlicher Gruppen. Vorlesungsskript (1979) an der Universität Karlsruhe, Fakultät für Mathematik.

[41] MACWILLIAMS, F., UND SLOANE, N. *The theory of error-correcting codes.* North-Holland Publ.Comp., 1992.

[42] MALVAR, H. S. *Signal Processing with Lapped Transforms.* Artech House, 1992.

[43] MASLEN, D., UND ROCKMORE, D. Generalized FFTs – a survey of some recent results. *Proceedings of IMACS Workshop in Groups and Computation 28* (1995), 182–238.

[44] MERTINS, A. *Signaltheorie.* Teubner Verlag, 1996.

[45] MINKWITZ, T. *Algorithmensynthese für lineare Systeme mit Symmetrie.* Diss., Universität Karlsruhe, 1993.

[46] Minkwitz, T. Algorithms Explained by Symmetry. *Lecture Notes on Computer Science 900* (1995), 157–167.

[47] Minkwitz, T. Extension of Irreducible Representations. *Applicable Algebra in Engineering, Communication and Computing 7* (1996), 391–399.

[48] Minkwitz, T. On the generation of algorithms for linear transforms and systems with symmetry. Tech. Rep., EISS, 1997.

[49] Ore, O. Theory of monomial groups. *Trans. Am. Math. Soc. 51* (1942), 15–64.

[50] Passman, D. *Permutation Groups.* Benjamin/Cummings, 1968.

[51] Pennebaker, W., und Mitchell, J. *JPEG: still image data compression standard.* Van Nostrand Reinhold, 1993.

[52] Pichler, F. *Mathematische Systemtheorie; Dynamische Konstruktionen.* de Gruyter, Berlin, 1975.

[53] Rader, C. M. Discrete fourier transforms when the number of data samples is prime. *Proceedings of the IEEE 56* (1968), 1107–1108.

[54] Rao, K., und Hwang, J. *Techniques & Standards for Image, Video and Audio Coding.* Prentice Hall PTR, 1996.

[55] Rockmore, D. Efficient computation of Fourier inversion for finite groups. *Assoc. Comp. Mach. 41(1)* (1994), 31–66.

[56] Rockmore, D. Some applications of generalized FFT's. *Proceedings of DIMACS Workshop in Groups and Computation 28* (1995), 329–370.

[57] Schönert, M. et al. GAP — Groups, Algorithms and Programming. Tech. Rep., Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany., fifth ed., 1995.

[58] Serre, J. *Linear Representations of Finite Groups.* Springer, 1977.

[59] Sturmfels, B. *Algorithms in Invariant Theory.* Springer, 1993.

[60] Wielandt, H. *Finite Permutation Groups.* Academic Press, 1964.

Index

Lebenslauf

29. Juli 1964	geboren in Augsburg
	Eltern: Claudia Bauer, geb. Petermann und Roland Püschel
1970 bis 1974	Besuch der Grundschule in Worms und Brühl
1974 bis 1983	Bach-Gymnasium, Mannheim Reifeprüfung: Juni 1983
1983 bis 1995	Mathematikstudium an der Universität Fridericiana zu Karlsruhe Diplomprüfung: Oktober 1995
1986 bis 1993	Professioneller Billardspieler (Carambolage Dreiband)
seit November 1995	Wissenschaftlicher Mitarbeiter am Institut für Algorithmen und kognitive Systeme (IAKS) der Universität Fridericiana zu Karlsruhe