Konstruktion transitiver Permutationsgruppen

Von der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinisch-Westfälischen Technischen Hochschule Aachen
zur Erlangung des akademischen Grades eines Doktors
der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Mathematiker
Alexander Hulpke
aus Mainz

Referent: Universitätsprofessor J. Neubüser
Korreferent: Universitätsprofessor H. Pahlings

Tag der mündlichen Prüfung: 11. 7. 1996

D 82 (Diss. RWTH Aachen)

AACHENER BEITRÄGE ZUR MATHEMATIK

Herausgeber:

Professor Dr. H. H. Bock, Institut für Statistik und Wirtschaftsmathematik
Professor Dr. H. Th. Jongen, Lehrstuhl C für Professor Dr. W. Plesken, Lehrstuhl B für Mathematik

Hulpke, Alexander:
Konstruktion transitiver Permutationsgruppen
1. Auflage Aachen:
Verlag der Augustinus Buchhandlung, 1996
(Aachener Beiträge zur Mathematik, Band 18)

ISBN 3-86073-427-X

Verlag der Augustinus Buchhandlung
Pontstraße 96
52062 Aachen
Tel. & Fax: 0241-23948

Druck: COPYTEAM, Aachen
Gedruckt auf chlorfrei gebleichtem Papier

"D 82 (Diss. RWTH Aachen)"

Meinen Eltern

Inhalt

Prolog

Versucht man einem Nichtmathematiker zu erklären, womit sich die Mathematik beschäftigt, so kann man zwei große Bereiche auseinanderhalten: Zum einen die Suche nach Methoden, um durch gewisse Eigenschaften (dies können zum Beispiel Gleichungen sein) gegebene Objekte konkret angeben (oder „ausrechnen“) zu können; zum anderen der Versuch, Klassen von Objekten, die durch eine Reihe von Eigenschaften definiert sind, zu charakterisieren, sei es durch Aufzählung, oder durch genauere Beschreibung.

Die vorliegende Arbeit gehört in beide Bereiche: Das Ziel ist zunächst die Beschreibung der Struktur transitiver Gruppen. Hierauf aufbauend soll ein Algorithmus entwickelt werden, der für einen gegebenen Grad $n \in \mathbb{N}$ Repräsentanten der Klassen transitiver Gruppen von Grad n ermittelt. Dabei soll es auch möglich sein, nur Gruppen mit vorgegebenen Eigenschaften zu konstruieren. Dieser Algorithmus soll dann schließlich benutzt werden, um konkret die Klassen transitiver Permutationsgruppen für einige Grade n zu bestimmen.

Die Beschreibung von Algorithmen für (Permutations)gruppen nimmt daher einen Gutteil der Arbeit ein. Bei der Beschreibung dieser Algorithmen wurde darauf verzichtet, formalen Pseudocode anzugeben, da dieser für gewöhnlich nicht zum Verständnis der Vorgehensweise beiträgt. Ich möchte mich diesbezüglich den Ausführungen in [Coh1993, Abschnitt 1.1.4] anschließen.

Die eigentliche Ausführung der Algorithmen wurde dann – mit Ausnahme einiger Beispiele, die lediglich der Illustration dienen – einem Computer überlassen, der solche Dinge erfahrungsgemäß geduldiger, schneller und korrekter ausführt, als es der Autor jemals könnte.

Die Erstellung dieser Arbeit ist von Oktober 1993 bis April 1996 durch ein Stipendium des DFG-Graduiertenkollegs „Analyse und Konstruktion in der Mathematik“ an der RWTH Aachen gefördert worden. Ich möchte mich an dieser Stelle beim Kolleg und insbesondere bei dessen Sprecher Volker Enß für die erhaltene Unterstützung bedanken.

John McKay und dem Centre Interuniversitaire de Calcul Mathématique Algebraique sei für die Ermöglichung eines Aufenthaltes an der Concordia-University in Montréal gedankt, der in den ersten Monaten 1995 stattfand.

John Conway brachte mir seine Notation für Permutationsgruppen bei und zeigte mir, wie man Listen transitiver Gruppen für kleine Grade von Hand erstellt.

Gene Cooperman und Larry Finkelstein möchte ich für Diskussionen während eines Aufenthaltes im Mai 1995 an der Northeastern University in Boston, sowie für die Möglichkeit, die dortigen Rechner auch danach noch benutzen zu können, danken.

Den Mitarbeitern und Besuchern des Lehrstuhl D sei für ungezählte Diskussionen und Hilfen, sowie Geduld mit meinen bisweilen ausufernden Berechnungen gedankt.

Meinem Betreuer, Joachim Neubüser, möchte ich schließlich für die Freiheiten bei der Bearbeitung des Themas danken. Ihm und Herbert Pahlings sei darüberhinaus für die Geduld mit einer vorläufigen Fassung dieser Arbeit und deren bisweilen nur schwer nachvollziehbaren Argumentationen gedankt.

Konventionen

Da in der Literatur verschiedene Notationen verwandt werden, seien hier einige in dieser Arbeit ohne weitere Anmerkungen verwendete Konventionen und Notationen zusammengestellt, die bis auf Widerruf gelten:

Die betrachteten Gruppen sind endlich.
Gruppen operieren – sofern es sich irgend einrichten läßt – von rechts. Dementsprechend betrachten wir für gewöhnlich Nebenklassen der Form Ug, die wir als *Rechtsnebenklassen* aus der Nebenklassenmenge $U\backslash G$ bezeichnen.
Abbildungen werden ebenfalls von rechts geschrieben. Dabei werden lediglich Konjugation und Permutationsoperationen als Exponentiation geschrieben.
Durch einen Repräsentanten R gegebene Klassen werden mit $[R]$ bezeichnet.
Um eine Verwechselung mit Indizes zu vermeiden werden direkte Potenzen in der Form $G^{\times m} = \underbrace{G \times \cdots \times G}_{m}$ geschrieben.

Die Welt der Permutationsgruppen

Ist Ω eine Menge, so bezeichnen wir die Menge aller Permutationen von Ω als S_Ω. Diese Menge bildet bezüglich Hintereinanderausführung von Permutationen eine Gruppe. Operiert eine Gruppe G auf einer Menge Ω so erhalten wir einen Homomorphismus α von G in S_Ω. Ein solcher Homomorphismus heißt *Permutationsdarstellung* von G. Er heißt *treu*, wenn das einzige Element von G, das alle Elemente aus Ω festlässt, die Identität ist. In diesem Fall bezeichnen wir (G, Ω) als *Permutationsgruppe*. So ist zum Beispiel (S_Ω, Ω) eine Permutationsgruppe. Wir schreiben die Operation in der Form ω^g. Ist $\omega \in \Omega$, so bezeichnen wir die Menge

$$\omega^G := \{\omega^g \mid g \in G\}$$

als *Bahn* von ω unter G und teilen Ω dementsprechend disjunkt in Bahnen von G auf. Besitzt G nur eine Bahn, so nennen wir die Operation *transitiv*, ansonsten *intransitiv*. Ist $\Delta \subset \Omega$ Vereinigung einer Menge von Bahnen von G, so liefert die Einschränkung der Operation auf Δ eine Permutationsdarstellung von G.

Dual zur der Bahn von ω bezeichen wir die Untergruppe

$$G_\omega := \mathrm{Stab}_G(\omega) = \{g \in G \mid \omega^g = \omega\}$$

als *Stabilisator* von ω in G. Dann gilt

(1) Lemma (Bahnensatz): $G_\omega g \mapsto \omega^g$ ist eine Bijektion zwischen den Nebenklassen $G_\omega\backslash G$ und der Bahn ω^G.

Ist Ω endlich (was hier stets der Fall ist), so heißt $n = |\Omega|$ der *Grad* der Permutationsgruppe. Ist der Operationsbereich aus dem Kontext ersichtlich, so bezeichnen wir oftmals auch eine Gruppe alleine als Permutationsgruppe. Eine Permutationsgruppe (G,Ω) heißt *semiregulär*, wenn für alle $\omega \in \Omega$ gilt, daß $G_\omega = \langle 1 \rangle$ ist. Eine transitive semireguläre Gruppe heißt *regulär* und erfüllt $|G| = |\Omega|$.

Zwei Permutationsgruppen (G,Ω) und (H,Δ) heißen *äquivalent*, wenn es eine Bijektion $\psi\colon \Omega \to \Delta$ und einen Isomorphismus $\varphi\colon G \to H$ gibt, so daß $(\omega^g)\psi = (\omega\psi)^{g\varphi}$ für alle $\omega \in \Omega$ und alle $g \in G$ gilt.

Die Aussage von Lemma (1) kann folglich dahingehend interpretiert werden, daß jede transitive Permutationsgruppe (G,Ω) bei Wahl eines festen $\omega \in \Omega$ äquivalent ist zur Permutationsgruppe $(G, G_\omega \backslash G)$, die auf den Nebenklassen per Rechtsmultiplikation operiert. Ist umgekehrt G eine Gruppe und $U \leq G$, so hat die Permutationsdarstellung auf den Nebenklassen von U den Kern $\bigcap_{g\in G} U^g$.

Sind (G,Ω) und (H,Ω) äquivalente Permutationsgruppen und ist die die Äquivalenz erzeugende Bijektion $\psi\colon \Omega \to \Omega$ durch die Permutation $s \in S_\Omega$ gegeben, so ist der Isomorphismus $\varphi\colon G \to H$ durch *Konjugation* mit s, das heißt die Abbildung $g \mapsto g^s = s^{-1}gs$, definiert[1].

Ist Ω endlich, so können wir es mit einem Anfangsstück der natürlichen Zahlen identifizieren. Wir bezeichnen die Gruppe $S_{\{1,\dots,n\}}$ aller Permutationen von $\{1,\dots,n\}$ kurz als S_n und nennen sie die *symmetrische Gruppe* von Grad n. Eine Permutationsgruppe (G,Ω) mit $|\Omega| \leq n$ ist somit äquivalent zu einer Untergruppe von S_n. Es genügt daher, die Untergruppen von S_n zu betrachten, um alle Permutationsgruppen von Grad n bis auf Äquivalenz zu bestimmen.

Permutationen aus der S_n werden für gewöhnlich in *Zykelform* geschrieben, das heißt

$$\begin{pmatrix} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \\ 4 \mapsto 5 \\ 5 \mapsto 6 \\ 6 \mapsto 4 \end{pmatrix} \qquad \text{wird als (1,2)(4,5,6) notiert.}$$

Konsistent mit der Rechtsoperation ergeben sich dann Produkte in der Form $(1,2,3)\cdot(1,2) = (2,3)$.

Ist G eine Permutationsgruppe die auf Ω operiert, so operiert G in natürlicher Weise (durch Operation auf den Einträgen) auch auf der Menge der Teilmengen oder Folgen aus Ω. Ist $\Phi \subset \Omega$ eine Teilmenge so bezeichnen wir den *Mengenstabilisator* von Φ als G_Φ. Ist Φ dagegen eine Folge, so sei der Stabilisator zur Unterscheidung mit

$$G_{[\Phi]} = \bigcap_{\omega\in\Phi} G_\omega$$

bezeichnet.

Operiert G transitiv auf Ω und ist $\mathcal{B}$ eine Partition von Ω, die unter der Operation von G invariant ist, so heißt $\mathcal{B}$ ein *Blocksystem* für G, eine Teilmenge aus $\mathcal{B}$ heißt *Block*. Die Partitionen $\mathcal{B}_0 = \{\{\omega\} \mid \omega \in \Omega\}$ und $\mathcal{B}_\infty = \{\Omega\}$ heißen *triviale Blocksysteme*. Ist $\mathrm{B} \in \mathcal{B}$, so heißt der mengenweise Stabilisator G_B *Blockstabilisator*. Die Blocksysteme einer

[1] Damit ist der Äquivalenzbegriff konsistent mit Definition (6)

Permutationsgruppe stehen bei Wahl eines $\omega \in \Omega$ vermöge $\mathcal{B} \mapsto G_{\mathrm{B}}$,wobei $\mathrm{B} \in \mathcal{B}$ der (eindeutige) Block sei, der ω enthält, in Bijektion zu den Untergruppen $G_\omega \leq U \leq G$. Besitzt eine Gruppe lediglich triviale Blocksysteme, so heißt sie *primitiv*, ansonsten *imprimitiv*. Da ein Blocksystem von G unter G invariant ist, erhält man zu jedem Blocksystem eine Permutationsdarstellung von G in die Gruppe $S_{\mathcal{B}}$. Für $\mathcal{B}_0$ ergibt sich eine zu G äquivalente Gruppe, für $\mathcal{B}_\infty$ die triviale Gruppe.

Bezüglich der in dieser Arbeit verwandten Nomenklatur transitiver Gruppen sei auf Anhang A verwiesen.

Symbolverzeichnis

Die Zahlen hinter den Begriffen geben die Seite an, auf der das entsprechende Objekt erstmals auftritt. Der Leser sei auch auf den Index verwiesen.

A	subdirekter Faktor, 21; Blockoperation, 37
A_i	alternierende Gruppe; Kopie von A in direktem Produkt
$A^{\times m}$	direkte Potenz $\overset{m}{\underset{i=1}{\times}} A$
$\mathfrak{A}_T$	Repräsentantensystem von Aufblasungen von T , 36
$\mathcal{A}$	Repräsentantensystem aller Aufblasungen, 36
B	subdirekter Faktor, 21
B_k	Lexikographisch kleinste unverkürzbare Base, 103
$\mathcal{B}$	Blocksystem, 31
C	$N_{S_{\Omega_A}}(A)$, 26
$\mathcal{C}$	weiteres Blocksystem, 40
D	$N_{S_{\Omega_B}}(B)$, 26
deg	Grad eines Elements aus $\mathcal{S}$, 47
E	Normalteiler in A, 21
$\mathcal{E}$	C-Klassen der E, 27
F	Normalteiler in B, 21
$\mathcal{F}$	D-Klassen der F, 27
G, H	Gruppe, 2
$\hat{G}_M$	Gruppen mit M als Basis, 40
$\mathfrak{G}_M$	Repräsentanten der $\triangleq$-Klassen, 40
$\mathcal{G}_M$	Repräsentantensystem der Gruppen mit M als Basis, 40
ggT	für Elemente aus $\mathcal{S}$, 47
$\mathcal{H}, \mathfrak{H}$	Klassen transitiver Untergruppen, 82
$\mathcal{I}$	Invariante Moduln, 75
I	Blockkernprojektionsklassenmatrix eines Anfangsstücks, 72
J	Nebenklassenvertretersystem, 25
K	Kern $\varphi\|_N$, 39; Kernklasse, 46; Komplement, 81
kgV	für Elemente aus $\mathcal{S}$, 47
L	Konjugiertes von M, 59; Blockkernprojektionsklassenmatrix, 72
l	Blockordnung, 35
len	Länge einer Subpotenz, 38

M	(iteriertes) subdirektes Produkt, 22; Basis Kern φ, 35
M_N	N-Anteil von M, 82
$\underleftarrow{M}_{i}$	Anfangsstück, 42
M_i	Blockkern Kern $\pi_i \cap M$, 42
M_i^j	Blockkernprojektion $M_i \pi_j$, 42
M^i	Schnitt der Blockkerne $M^i \bigcap_{i \neq j} M_j$, 42
$\mathcal{M}$	Repräsentantensystem der M, 27
m	Blockanzahl, 35
N	Normalisator von M, 39
No	Normalisator einer zu kanonisierenden Untergruppe, 79
$\mathcal{N}$	Klassen von Normalteilern von A, 47
NVS	Vertretersysteme von Nebenklassen, 95
n	Grad
o	Stufe einer Verschachtelung, 50
P	Kern π, 21
Q	Kern ϱ, 21
$\mathbb{Q}$	rationale Zahlen, 7
R	$\langle P, Q \rangle$, 21; $N\varphi$, 39
$\mathfrak{R}_n$	Repräsentantensystem von $\mathfrak{T}_n$, 33
r_i	Signaturkofaktor, 72
S	$S_{\Omega_B} \times S_{\Omega_A}$, 26; GK, 39
S_i	symmetrische Gruppe
$\mathcal{S}$	Freie abelsche Gruppe auf $\mathcal{N}$, 47
s, t	Elemente aus $\mathcal{S}$, 47
sign_i	i-te Signatur, 48
T	$G\varphi$, 35; Transversale, 56; transitive Gruppe, 92
$\mathfrak{T}_n$	Klassen transitiver Gruppen von Grad n, 33
U, V	Untergruppen, 2
Vkl	Vorkommende Kernklassen, 46
v	Teilprodukt, 58
W, Z	Kranzprodukt, 30
X	Basis, 30
Y	G/R, 21; Komponente einer Verschachtelung, 49
α	Einbettung $A \to B \times A$, 25; Automorphismus, 35
B	Block, 31
β	Einbettung $B \to B \times A$, 25
γ	Isomorphismus $B/F \to A/E$, fest gewählt, 25
$\gamma_{[F,E]}$	Satz der γ, 27
Γ, Δ, Ω	Operationsbereiche, 23
ζ	natürlicher Homomorphismus $B \to B/F$, 21
η	γ modifizierender Automorphismus von A/E, 25
θ_x	von x induzierter innerer Automorphismus
ϑ_x	von x induzierter innerer Automorphismus eines Faktors, 27

ι	Einbettung $G \to B \times A, 21$
μ_i	$(\pi_1, \ldots, \pi_i), 42$
ξ	natürlicher Homomorphismus $A \to A/E, 21$
Π_I	$(\pi_i)_{i \in I}, 49$
π	$G \to A, 21$
π_i	Projektion von Subpotenz auf Komponenten, 42
ϖ	Projektion auf zwei Komponenten, 43
ϱ	$G \to B, 21$
σ	Permutation, 20
φ	Operation auf $\mathcal{B}, 31$
χ	Isomorphismus $B/F \to A/E, 21$
ψ	Operation von $\mathrm{Stab}_G(B)$ auf $B, 31$
Ω_A	Operationsbereich von $A, 26$
Ω_B	Operationsbereich von $B, 26$
ω	Punkt
$\sim_K$	Äquivalenz über Indizes gleicher Kernklassen, 46
$\preceq$	Willkürlich gesetzte Ordnung, 54
$\triangleq$	Konjugationsäquivalenz auf $\hat{G}_M, 40$

KAPITEL I

Einleitung

Quels peuvent être les nombres de valeurs
des fonctions bien définies qui contiennent
un nombre donné de lettres,
et comment peut-on former les fonctions pour lesquelles
il existe un nombre donné de valeurs?
Grand Prix der Académie des Sciences von 1858.

I.1. Historie

Die Definition einer „Gruppe“ stammt aus dem 19. Jahrhundert. Gegenstand der Betrachtung waren zunächst nur Galoisgruppen. Diese waren nicht im heutigen Sinne abstrakt als Menge von Körperautomorphismen, sondern als von Galoisautomorphismen induzierte Permutationen der Wurzeln einer Polynomgleichung definiert. Im heutigen Sprachgebrauch würde man von der treuen Permutationsdarstellung der Galoisgruppe auf den Nullstellen eines irreduziblen Polynoms sprechen.

Ist f ein irreduzibles Polynom über $\mathbb{Q}$ vom Grad n mit Wurzeln $\{\alpha_1, \ldots, \alpha_n\}$, so operieren die Elemente der Galoisgruppe auf Ausdrücken in diesen Wurzeln per Permutation der Indizes. Von dieser Interpretation aus ist der Weg zur Invariantentheorie nicht mehr weit: Wir betrachten einen n-fachen Polynomring $R = \mathbb{Q}[x_1, \ldots, x_n]$ und lassen die symmetrische Gruppe S_n per Permutation der Unbestimmten operieren. Unter dem Einsetzungshomomorphismus $x_1 \mapsto \alpha_i$ erhalten wir also wiederum die Situation der Galoistheorie.

Möchte man die Elemente von R unter der Operation von S_n klassifizieren, so ergeben sich natürlicherweise Fragen nach Bahnen und Stabilisatoren. Dies ist in heutiger Sprache genau die oben zitierte Aufgabe der Académie des Sciences, die in [Aca1858] publiziert ist: Was ist die Anzahl („*nombre*“) der Bilder („*valeurs*“) – also die Bahnlänge – von Polynomen aus R („*fonctions bien definies qui contiennent un nombre donné de lettres*“)? In heutiger Sprache: Welche möglichen Bahnlängen gibt es?

Und schließlich: Wie klassifizieren sich die $r \in R$ mit vorgegebener Bahnlänge („*comment peut-on former les fonctions [...]* “)?

Elementare Gruppentheorie liefert partielle Antworten: Die Bahnlänge ist der Index des Stabilisators, also einer Untergruppe von S_n. Schließlich gilt:

(2) Lemma: Ist $U \leq S_n$ und $r_0 = \prod_{i=1,\ldots,n} x_i^i$, so ist $r_U = \sum_{u \in U} r_0^u$ unter U, aber unter keiner größeren Untergruppe invariant.

Beweis: Der Stabilisator von r_0 in S_n ist die triviale Untergruppe. Also stehen die Elemente der Bahn r_0^U und damit die Summanden von r_U in Bijektion zu den Elementen von U.

Damit ist r_U unter U aber keiner größeren Untergruppe invariant. □

Kenntnis der Untergruppen von S_n erlaubt also (modulo des Problems der Klassifikation von Invarianten einer Untergruppe, das nicht Gegenstand dieser Arbeit sein soll, [Hil1893, Stu1993]) die vollständige Beantwortung der gestellten Frage. Dabei genügt es offensichtlich, jeweils nur Repräsentanten der S_n-Konjugiertenklassen zu betrachten, wenn wir die Numerierung der Unbestimmten nicht vorgeben.

Einige einfache Überlegungen (siehe (25)) gestatten dabei im wesentlichen die Reduktion auf transitive Untergruppen, Klassifikationen insbesondere höherer Grade beschreiben meist nur die transitiven Gruppen.

I.1.1. Obgleich bereits einer der ersten Artikel zu diesem Thema [Kir1862] den quasi abschließenden Titel „*The complete theory of groups*“ trägt, erschienen bis zum Anfang dieses Jahrhunderts eine ganze Reihe an Arbeiten zur Klassifikation von Permutationsgruppen. Zeitgenössische Zusammenstellungen der Ergebnisse bieten die Einleitung der Werkausgabe [Mil1935], sowie der Enzyklopädieartikel [Bur1898] (beziehungsweise die erweiterte Übersetzung ins Französische [BV1909]), dessen lapidare Zusammenfassung „*fast jede der betr. Arbeiten stellt Versehen der vorhergehenden richtig*“ berechtigte Zweifel an der Vollständigkeit der Klassifikationen aufwirft.

Im Rahmen seiner Arbeit zur Klassifikation der auflösbaren primitiven Gruppen von Grad kleiner 256 [Sho1992] hat M. SHORT sich der enormen Mühe unterzogen, die alten Arbeiten zu sichten, zu vergleichen und im Lichte der heutigen Ergebnisse auf Korrektheit zu untersuchen. Da dies kaum verbessert werden kann, seien seine Resultate hier zitiert (aus [Sho1992, Appendix A, pp. 122–124], wobei lediglich die Literaturzitate dem Schema dieser Arbeit angepasst wurden). Zum Verständnis sei bemerkt, daß mit „den Gruppen eines Grades“ jeweils nur die fixpunktfreien Gruppen gemeint sind, da die übrigen Untergruppen der S_n bereits von kleinerem Grad realisiert werden können. Die Verweise auf C. SIMS beziehen sich auf die gegen Ende erwähnte Liste der primitiven Gruppen bis Grad 50.

> *The first work in this area is probably due to* RUFFINI [Ruf1799], *who gives the possible orders of groups of degree 5. This theme is taken up again by* CAUCHY [Cau1845], *who determines the possible orders of the groups of degree up to 6.* MATHIEU [Mat1858] *continues* CAUCHY*'s work, determining the possible orders of the groups of degree 7 and 8.* MILLER [Mil1896a] *suggests that* RUFFINI*'s work is incomplete, and cites an omission in* CAUCHY*'s list for degree 6.*
>
> SERRET [Ser1850] *determines all subgroups of S_4 and S_5.* MILLER [Mil1896a] *says that this work is correct.*
>
> KIRKMAN [Kir1862] *lists the transitive groups of degree 3 to 10.* MILLER [Mil1896a] *says that this list is correct up to degree 7, has missing six groups of degree 8, another six of degree 9, and is highly inaccurate for degree 10.*
>
> JORDAN [Jor1871b], *using the theory that was discussed in Chapter 2* [der zitierten Arbeit], *gives a table containing the numbers of conjugacy classes of primitive maximal soluble groups of degree less than 10^6. He*

claims that there are five such classes of degree 81, but there are only four, as is pointed out in Chapter 8 (see page 94). This error is likely to lead to errors for larger degrees. Also, the second and third entries in the last row of this table should be swapped. In the same paper, JORDAN *also gives a table containing the numbers of conjugacy classes of transitive maximal soluble groups of degree up to 10 000. (This is an astounding achievement if for no other reason than the amount of counting required to prepare it. For example if p is a prime greater than 3,* JORDAN *claims that the number of conjugacy classes of transitive maximal soluble groups of degree* $2^6 3^3 p$ *is 8306.) Again the error in the first table is likely to lead to errors in this one too.* JORDAN [Jor1872] *counts all the primitive groups of degrees 4 to 17. His count matches that of* SIMS *except that* JORDAN *has one less for degrees 9, 12 and 15, eight less for degree 16, and two less for degree 17. These errors are pointed out by* MILLER [Mil1894a, Mil1895a, Mil1897a, Mil1897b, Mil1900b]. JORDAN [Jor1874] *states that every transitive group of degree 19 is either alternating, symmetric or affine. this agrees with* SIMS*' list.*

VERONESE [Ver1883] *determines all groups of degree up to 6.* MILLER [Mil1935] *cites several errors for degree 6.*

ASKWITH [Ask1890b] *and* CAYLEY [Cay1891] *determine the groups of degree 6 and get the same answers. Their count of the intransitive ones is correct but they undercount the transitive groups by three, as* COLE [Col1893b] *points out. As* KIRKMAN [Kir1862] *had already (successfully, according to* MILLER*) determined the transitives, degree 6 was then complete.*

ASKWITH [Ask1890b] *and* CAYLEY [Cay1891] *also arrive at the same determination of the groups of degree 7. They undercount both the transitives and intransitives by one, as* COLE [Col1893b] *points out. With* KIRKMAN*'s transitives and* COLE*'s additional intransitives, degree 7 was then complete.*

ASKWITH [Ask1890a] *and* CAYLEY [Cay1891] *determine the groups of degree 8, but this time they differ;* CAYLEY *points out a number of errors in* ASKWITH*'s list.* COLE [Col1893b] *exhibits 40 groups missing from* CAYLEY*'s list, 20 transitive and 20 intransitive.* ASKWITH*'s list is similarly inaccurate. However,* MILLER [Mil1894b] *points out that two of the 'new' groups of degree 8 given by* COLE *are equal, and also produces an imprimitive group of degree 8 that he claims is neither on* CAYLEY*'s list nor* COLE*'s.* MILLER [Mil1894a] *produces a second group of degree 8 (a primitive one) that he claims both* CAYLEY *and* COLE *missed. He says that this group can be found in both* [Kir1862] *and* [Jor1871a]. *No further corrections have been made to the lists for degree 8; their number stands at 200, with 50 being transitive, and 7 primitive.*

ASKWITH [Ask1893] *determines the transitive groups of degree 9.* COLE [Col1893c, Col1893a] *determines the groups of degree 9, and finds 12 more transitive ones than* ASKWITH. COLE*'s numbers for the transitive groups agree with those of* BUTLER *and* MCKAY [BM1983] *and* SIMS [Sim1970]. MILLER [Mil1894a] *gives two intransitive groups that are not on* COLE*'s list. No further corrections have been made to the lists for degree 9; their number stands at 258, with 34 being transitive, and 11 primitive.*

COLE [Col1895] *lists the transitive groups of degree 10.* MILLER [Mil1895b] *shows that* COLE*'s list of imprimitive groups has six repetitions. With these corrections,* COLE*'s numbers for the transitive groups agree with those of* [BM1983] *and* [Sim1970]. MILLER [Mil1895c] *gives a list of the intransitive groups of degree 10; it contains 994 such groups* [was korrekt ist]. MILLER [Mil1900a] *gives what he considers a formal derivation of the primitive groups of degree 10.*

COLE [Col1895] *determines the transitive groups of degree 11. His list agrees with that of* SIMS [Sim1970]. MILLER *and* LING [ML1901] *determine the intransitive groups of degree 11; they find 1492 such groups.*

MILLER [Mil1895a, Mil1896b] *determines the transitive groups of degree 12. His count for the primitives matches that of* SIMS [Sim1970], *but for the imprimitives it differs from that of* ROYLE [Roy1987] *in several places.*

MILLER [Mil1897a, Mil1897b, Mil1898b, Mil1898a, Mil1900b] *determines the primitive groups of degrees 13 to 17. His enumerations agree with those of* SIMS [Sim1970]. *In* [Mil1898b] *he also determines the imprimitive groups of degree 14, obtaining 59.*

MILLER [Mil1898a] *correctly gives a table of the numbers of soluble primitive groups of degree up to 24.*

BURNSIDE [Bur1897] *determines all primitive groups of degrees 3 to 8. His work is correct, except that he obtains two non-existent primitive groups of degree 8, their construction having been left as an exercise. This error also occurs in the second edition* [Bur1911] *of his book, despite* MILLER [Mil1899] *having pointed it out.*

MARTIN [Mar1901] *and* KUHN [Kuh1904] *determine the imprimitive groups of degree 15; they both find 70.* [KUHN findet 98 imprimitive, was korrekt ist; MARTIN besagte 70, verweist aber bereits auf KUHNS Resultat]

MARTIN [Mar1901] *determines the primitive groups of degree 18; her list agrees with that of* SIMS.

BENNETT [Ben1912] *determines the primitive groups of degree 20; her list agrees with that of* SIMS.

There does not seem to be any more literature on this topic until SIMS [Sim1970] *lists all primitive groups of degrees up to 20. He says that he took the list from the literature and verified it partly by hand and partly by machine. He later extended this list to degree 50. Although the full list has never been published, it was made available in version 3.5 of* CAYLEY, *released in 1987, as the* CAYLEY *library* PRMGPS. [Diese Listen finden sich seit Version 3.1 ebenfalls in GAP]

In [HY1979], *there is an undated reference to a master's thesis by* MIZUTANI*; the title of the thesis is "The classification of primitive permutation groups of degree less than 49". No material from this thesis seems to have been published.*

POGORELOV [Pog1980, Pog1982] *lists, up to isomorphism, all primitive groups with insoluble socles for degree 21 to 64. This work was done by hand using* M. HALL*'s classification of simple groups of order less than* 10^6 *and various theorems on simple groups and primitive groups. Unfortunately he does not tabulate his results and so it is difficult to compare his list with that of* SIMS.

BUTLER *and* MCKAY [BM1983] *determine, with the help of* CAYLEY, *all imprimitive groups up to degree 11.* ROYLE [Roy1987] *makes considerable use of* CAYLEY *to determine all imprimitive groups of degree 12. In version 3.6 of* CAYLEY, *released in 1987,* ROYLE *provides a library,* TRNGPS, *containing all transitive groups of degree up to 12.* [GAP enthält seit Version 3.4 die transitiven Gruppen bis Grad 11. Mit Patchlevel 3 sind außerdem die Gruppen bis Grad 15 hinzugefügt worden.] *For the primitive groups he relies on* SIMS*' list, but for the imprimitive groups he uses the methods he developed for degree 12. He says that his list matches that of* BUTLER *and* MCKAY.

TANG *and* WANG [TW1988] *determine by hand the primitive groups of degrees 21 to 30. Their count agrees with that of* SIMS.

IL'IN *and* TAKAMAKOV [IT1986] *determine the simple primitive groups of degree up to 1000.* DIXON *and* MORTIMER [DM1988] *list the primitive groups of degree less than 1000 that have insoluble socles. Their calculations are done by hand, but depend on the classification of finite simple groups, and on detailed information in the* ATLAS [CCN$^+$1985]. *They point out some errors in the list of* IL'IN *and* TAKAMAKOV.

I.1.2. Zur Ergänzung seien die Resultate seit der Publikation dieser Zusammenfassung aufgeführt. G. BUTLER [But1993] bestimmte mit Rechnerhilfe die transitiven Gruppen von Grad 14 und 15 und erhält 63, beziehungsweise 104 Gruppen was mit [Mil1898b], beziehungsweise [Kuh1904] übereinstimmt. Diese Listen sind korrekt, jedoch ist die Schlussweise in einigen Fällen nicht nachvollziehbar[1].

Die Untergruppenverbände der symmetrischen Gruppen von Grad 8,9 und 10 wurden von G. PFEIFFER über Markentafeln bestimmt [Pfe1996]. Er erhält 296 (was mit [Mil1894a] übereinstimmt), 554, beziehungsweise 1593 Gruppen.

Mit Ausnahme einer Arbeit, die eine sehr spezielle Klasse von Gruppen von Grad 18 in elementarer Weise klassifiziert [AR1993], ist dies der Kenntnisstand des Jahres 1994.

[1] Hierzu siehe IV.6.5

Es ist bemerkenswert, daß er mit Ausnahme von Fehlerkorrekturen nicht wesentlich über denjenigen zu Anfang des Jahrhunderts hinausgeht.

Zum Vergleich sei eine Abschätzung der zur Zeit zur Verfügung stehenden Rechenleistung gegeben: Benutzt man lediglich Standardprogramme und übliche Arbeitsplatzrechner, so ist es zur Zeit möglich, in etwa den Untergruppenverband von S_9 automatisch zu erstellen, für höhere Grade steigt der Aufwand dabei mit der Gruppenordnung, so daß diese Strategie selbst bei leistungsfähigeren Rechnern kaum weiterführen würde.

I.1.3. In Tabelle 1 gebe ich zusammengefasst Klassenzahlen von Gruppen an, soweit ich sie als korrekt ansehe. Die Zeile „prim." gibt die Anzahl Klassen primitiver Gruppen, „trans." die Anzahl Klassen transitiver Gruppen an. In der Zeile „fpf." ist die Anzahl der Klassen von transitiven und intransitiven Gruppen von genau diesem Grad (das heißt fixpunktfreie Gruppen des Grades) angegeben. Diese Zahlen werden in der Zeile „Gesamt" aufsummiert, die damit die Anzahl an Klassen von Untergruppen der symmetrischen Gruppe angibt.

Die Zahlen entstammen, beziehungsweise sind in Übereinstimmung mit den folgenden Quellen:

- Die Anzahl Klassen von Untergruppen für die symmetrischen Gruppen bis Grad 10 wurden Markentafeln entnommen, die G. Pfeiffer berechnet hat [Pfe1996].
- Für die Grade $2-9$ wurden diese Angaben mit dem Untergruppenverbandsprogramm in GAP [S^+1995] nachgerechnet.
- Primitive Gruppen stammen aus der Liste von C. Sims wie sie sich in GAP findet.
- Transitive imprimitive Gruppen wurden nachgerechnet und sind bis Grad 15 in Übereinstimmung mit [BM1983, Roy1987, But1993].

Kursive Zahlen wurden – bei Vorgabe der primitiven Gruppen – im Rahmen dieser Arbeit nachgerechnet, fette Zahlen sind neue Resultate.

I.1.4. Die Tabelle zeigt auch, daß aufgrund der bei Grad 16 stark ansteigenden Anzahlen transitiver Gruppen eine Bestimmung von Klassenrepräsentanten über den Bereich von Grad 15 hinaus ohne Rechnerhilfe kaum machbar wäre. Dementsprechend hat sich die historische Entwicklung zunächst einmal auf primitive Gruppen konzentriert. Der Satz von Krasner und Kaloujnine (37) [KK1951], der zwar erst 1950 publiziert wurde, dessen Aussage aber wohl bereits früher im Prinzip bekannt war zeigt, daß jede transitive Gruppe Untergruppe eines Kranzproduktes „primitiverer" Gruppen ist. Dies machte – ähnlich der Einschränkung auf transitive Gruppen – eine Einschränkung auf primitive Gruppen plausibel.

Primitive Gruppen unterliegen weit mehr Einschränkungen in der Struktur und sind somit einfacher zu klassifizieren. So gab C. Jordan bereits 1872 eine Liste der primitiven Gruppen bis Grad 17 bekannt [Jor1872], eine Liste bis Grad 20 wurde von C. Sims in [Sim1970] publiziert und in der Zwischenzeit (verfügbar in der Form einer Bibliothek im System GAP[S^+1995]) bis zum Grad 50 erweitert.

Allgemeine Klassifikationssätze wurden insbesondere für mehrfach transitive Gruppen entwickelt. Als – besonders illustre aber in keinster Weise auch nur annähernd erschöpfende – Auswahl seien hier nur [Jor1870, Mat1873, Wie1960] sowie der Überblicksartikel [Cam1981]

Grad	2	3	4	5	6	7	8	9	10	11
prim.	1	2	2	5	4	7	7	11	9	8
trans.	1	2	*5*	5	*16*	7	*50*	*34*	*45*	8
fpf.	2	2	7	8	37	40	200	258	1039	
Gesamt	2	4	11	19	56	96	296	554	1593	

Grad	12	13	14	15	16	17	18	19	20	21
prim.	6	9	4	6	22	10	4	8	4	9
trans.	*301*	9	*63*	*104*	**1954**	10	**983**[2]	8	**1117**	**164**

Grad	22	23	24	25	26	27	28	29	30	31
prim.	4	7	5	28	7	15	14	8	4	12
trans	**59**	7	**26813**[2]	**211**	**96**	**2382**	**1852**	8	**5712**	12

Tabelle 1. Klassenanzahlen von Permutationsgruppen

genannt. Die Entwicklung gipfelte schließlich 1979 im Satz von O'Nan und Scott [Sco1980], der – unter Verwendung der Klassifikation endlicher einfacher Gruppen [Gor1982][3] – im wesentlichen eine Beschreibung aller primitiven Gruppen liefert. Darauf aufbauend gelang in den vergangenen Jahren schließlich die Klassifikation der auflösbaren primitiven Gruppen bis Grad 255 (unter Benutzung von Rechnern) [Sho1992] sowie eine – nicht ganz explizite – Beschreibung der nichtauflösbaren primitiven Gruppen bis Grad 1000 [DM1988] (welche aber im wesentlichen ohne Rechnerhilfe auskommt).

Die Beschreibung der primitiven Gruppen geschieht dabei über ihre Sockel, die aus einfachen Gruppen gemäß den Informationen im ATLAS [CCN$^+$1985] und ähnlichen Werken konstruiert werden. Die primitiven Gruppen liegen dann im Normalisator ihrer Sockel. Für nichtabelsche Sockel sind die Normalisatorfaktoren aufgrund der Schreierschen Vermutung [SvdW1928] meist sehr klein, so daß die aus einem solchen Sockel hervorgehenden primitiven Gruppen meist gut beschreibbar sind (genau dies ist in [DM1988] geschehen).

Kann man den Normalisator aber sogar explizit (das heißt: durch erzeugende Permutationen) angeben, so sollte es dadurch möglich sein, diese Listen primitiver Gruppen auch explizit anzufertigen. Jüngere Fortschritte bei der Normalisatorberechnung [Leo1991, The1996] lassen dies in der Tat in den Bereich des Möglichen geraten. Eine solche Explizierung der Listen aus [DM1988] wird zur Zeit von H. Theissen durchgeführt.

Die gewählten Beschränkungen der Gradbereiche beruhen im übrigen weniger auf prinzipiellen Schwierigkeiten oder Einschränkungen der Methoden sondern vor allem auf der Tatsache, daß die Anzahl der Gruppen rasch wächst und die Menge der Gruppen bis zur

[2] Siehe Kapitel VII.

[3] Im Hinblick auf mögliche Zweifel an der Korrektheit der Klassifikation sei erwähnt, daß in dieser Arbeit nur primitive Gruppen von kleinem Grad benutzt werden, deren Beschreibung auch ohne die Klassifikation der einfachen Gruppen möglich ist

nächsten runden Gradschranke nur noch schwer handhabbar gewesen wäre. Festzuhalten ist aber, daß die primitiven Gruppen gegebenen Grades im wesentlichen klassifizierbar sind.

I.1.5. Für die Klassifikation der transitiven Gruppen bedeutet dies, daß die primitiven Gruppen für die betreffenden Grade als gegeben angenommen werden können, und lediglich die imprimitiven Gruppen zu beschreiben sind. Dazu bietet es sich an, Blocksysteme dieser Gruppen zu benutzen. Mit Ausnahme der allerersten Arbeiten geschah dies auch bereits bei den oben erwähnten Klassifikationen des vergangenen Jahrhunderts.

Der erste Schritt hierzu ist die Beschreibung der möglichen Kerne von Blockdarstellungen (die meist „base“ oder „head“ der transitiven Gruppe genannt werden, wir verwenden den Begriff „Basis“). Diese Gruppen werden in sämtlichen erschienenen Arbeiten durch gradspezifische Argumentationen und Fallunterscheidungen beschrieben.

Der zweite Schritt besteht darin, zu einer gegebenen Basis die daraus hervorgehenden transitiven Gruppen zu beschreiben. Die Arbeiten des vergangenen Jahrhunderts suchten dazu – ohne genauer auf die Methode hierzu einzugehen – nach Permutationen, die die Basis normalisieren und die Blöcke (die nichts anderes als die Transitivitätsbereiche der Basis sind) dabei in vorgegebener Weise permutieren. Die neueren Arbeiten bestimmen dahingegen mit Rechnerhilfe den Teil des Untergruppenverbandes des Basisnormalisators oberhalb der Basis und suchen unter den Urbildern dieser Gruppen solche, die transitiv operieren.

Für kleinere Grade ist dies praktikabel, die Methoden sind aber im wesentlichen auf den – damit auch bestimmten – Gradbereich bis Grad 15 eingeschränkt. Bei Grad 16 sind zum Beispiel allein bei Blöcken von Ordnung vier 24 verschiedene Basen zu berücksichtigen, was eine Beschreibung schwierig macht. Darüberhinaus ergibt sich für die „diagonale“ Basis von Ordnung 2 eine Normalisatorfaktorgruppe vom Typ $2^7.S_8$, deren Ordnung demnach 5160960 beträgt. Hier wäre sowohl die Suche nach normalisierenden Elementen als auch die Bestimmung eines partiellen Untergruppenverbandes hoffnungslos. Auch für die meisten weiteren Grade stellen sich ähnliche Probleme.

Ziel dieser Arbeit soll es daher sein, eine genauere Beschreibung der Klassen transitiver Permutationsgruppen zu liefern. Aus dieser soll ein automatisierbares Konstruktionsverfahren für Klassenrepräsentanten gewonnen werden, mit dessen Hilfe man Listen für weitere Grade erstellen kann. Dafür stehen mit Computeralgebrasystemen wie GAP [S$^+$1995] oder Magma [CP1993] Hilfsmittel zu Verfügung, die zu Zeiten der ersten Klassifikationen kleiner Grade noch vollkommen undenkbar waren.

Da Abschätzungen und Plausibilitätsbetrachtungen für Grad 32 eine Größenordnung von 10^5 Klassen transitiver Gruppen vorhersagen, hatte ich mir zunächst das Ziel gesetzt, vollständige Listen bis zum Grad 31 zu erstellen. Mit der Ausnahme eines Falles bei Grad 24 (siehe VI.0.10) ist dies auch gelungen.

Das Verfahren soll sich aber darüber hinaus so verallgemeinern lassen, daß man auch gezielt nur Gruppen mit gewissen vorgegebenen Eigenschaften (die womöglich wieder eine überschaubare Klasse bilden) konstruieren und klassifizieren kann.

I.2. Anwendungen

Primäre Intention dieser Arbeit war, eine bessere Beschreibung transitiver Permutationsgruppen zu finden. Die Konstruktion expliziter Gruppenlisten dient hierbei zunächst nur als Nachweis der Tragfähigkeit der gefundenen Beschreibungsstrukturen. Unabhängig davon aber werden vollständige Listen der (transitiven) Gruppen von vorgegebenem Grad in der Mathematik bei der Untersuchung diverser Strukturen benutzt:

Zunächst einmal sind solche Listen in der Gruppentheorie von Interesse. Hier ist es oft wünschenswert, auch größere Klassen von Gruppen explizit klassifiziert zu haben, um nach Beispielen von Gruppen mit gewissen Eigenschaften zu suchen, oder Aussagen der Nichtexistenz gewisser Gegenbeispiele treffen zu können. Für auflösbare Gruppen oder spezieller p-Gruppen existieren bereits extensive Listen [Neu1967, Lau1982, O'B1991], die bisher bekannten Listen der Permutationsgruppen bis Grad 15 umfassen demgegenüber einen verhältnismäßig kleinen Bereich. Eine Erweiterung dieses Bereichs ist dabei umso wünschenswerter, da gewisse Phänomene erst bei höheren Graden auftreten (vergleiche zum Beispiel Bemerkung (51)), die Untersuchung dieser Gruppen daher womöglich zu allgemeinen Aussagen über Permutationsgruppen verhilft.

Der Konstruktionsprozeß teilt die Gruppen dabei automatisch in Klassen auf (die Feinheit der Unterteilung ist dabei in gewissen Grenzen noch wählbar). Diese Unterteilung wiederum hilft, die mit wachsendem Grad doch sehr großen Listen zu übersehen.

Schließlich kann man, wie in IV.9.3 gezeigt werden wird, die erhaltenen Repräsentantensysteme transitiver Untergruppen der symmetrischen Gruppe auch dazu benutzen, Repräsentanten der Klassen transitiver Untergruppen einiger großer Untergruppen der symmetrischen Gruppe zu bestimmen.

I.2.1. Die Automorphismengruppe diskreter kombinatorischer Objekte (zum Beispiel von Graphen oder Designs) besitzt eine treue Darstellung auf Konstituenten der Objekte. Intransitivität entspricht dabei oft auch kombinatorischen Reduktionen.

Die Einteilung der Objekte gemäß ihrer Automorphismengruppe separiert dann die oftmals sehr großen Mengen in handhabbarere Klassen. Diese Einteilung kann ebenfalls der Konstruktion dienen, die Klassifikation der Gruppen von Grad 12 [Roy1987] wurde zum Beispiel mit der eigentlichen Intention der Bestimmung aller vertex-transitiver Graphen von Ordnung 24 [RP1989] durchgeführt, bei der theoretische Überlegungen eine Reduktion auf den Fall eines Blocksystems mit 12 Blöcken von Ordnung 2 und eine Reihe weiterer Reduktionen gestatten.

I.2.2. In der Zahlentheorie finden Listen der transitiven Gruppen gegebenen Grades bei der Identifikation von Galoisgruppen Verwendung: Ist K ein vollkommener Körper, $f \in K[x]$ irreduzibel und $L > K$ der Zerfällungskörper von f, so operiert die Galoisgruppe $\mathrm{Gal}(f) = \mathrm{Aut}(L/K)$ transitiv und treu auf der Menge der Nullstellen von f. Die Bestimmung der Galoisgruppe als Gruppe von Körperautomorphismen ist jedoch im wesentlichen äquivalent zur Faktorisierung über L eines Minimalpolynoms $\in K[x]$ für L als Erweiterung von K, was praktisch nur für sehr kleine Grade des Zerfällungskörpers (in etwa für $[L:K] \leq 15$) möglich ist. Statt dessen begnügt man sich damit, den Permutationstyp der

Operation von G auf den Wurzeln von f zu bestimmen, was zum Beispiel für Rechnungen im Rahmen des Umkehrproblems der Galoistheorie [Mat1987] oft ausreicht.

Dies kann dadurch geschehen, daß hinreichend viele Eigenschaften der Galoisgruppe bestimmt werden (im wesentlichen Bahnlängen) um die Gruppe eindeutig in einer Liste identifizieren zu können [SM1985]. Alternativ wird eine Invariante der Gruppe numerisch mit hinreichender Genauigkeit auf den Wurzeln ausgewertet und gezeigt, daß diese Zahl im Grundkörper liegt [Sta1973, Coh1993]. Um zeigen zu können, daß ein Ausdruck Invariante einer vorgegebenen Untergruppe $U \leq S_n$ ist benötigt man – so die Invariante nicht genau die Elemente von U beschreibt[4], was aber eine für praktische Zwecke unbrauchbar hohe Rechengenauigkeit erzwingt – aber den Teilverband aller Untergruppen von S_n oberhalb von U. Für kleine U bedingt dies zumindestens eine partielle Bestimmung der Liste aller Gruppen.

Zusätzlich wird dieser Teilverband dazu benötigt, die Zuordnung von Punkten zu Wurzeln schrittweise durchzuführen, da ansonsten $[S_n : U]$ viele Möglichkeiten betrachtet werden müssen. Einfügen von Untergruppen $U < V < S_n$ kann den Aufwand logarithmieren (beziehungsweise wäre der Aufwand ansonsten noch exponentieller).

Implementationen existieren für kleinere Grade [Gey1993, Mat1992, Oli1993, Val1995, Hul].

I.2.3. Variation dieses Themas ist eine Anwendung bei der Polynomfaktorisierung. Da die Grade der Faktoren modulo einer Primzahl p eines irreduziblen Polynoms $f \in \mathbb{Z}[x]$ der Zykelstruktur eines Elementes aus der Galoisgruppe von f entsprechen [vdW1971, §66]; beziehungsweise – allgemeiner – die Grade der Faktoren eines homomorphen Bildes eines irreduziblen Polynoms stets Bahnlängen einer Untergruppe der Galoisgruppe sind, erhält man aus einer Liste der transitiven Permutationsgruppen bei Untersuchung der Bahnlängen von (zyklischen) Untergruppen Aussagen über das mögliche Aufspaltungsverhalten irreduzibler Polynome. Solche Aussagen finden Anwendung bei der Analyse des Laufzeitverhaltens von Faktorisierungsalgorithmen [Dav1996].

I.2.4. Ist G eine Gruppe und $H \leq G$ eine Untergruppe von Index n, so operiert G transitiv auf den Nebenklassen von H, hat also eine Faktorgruppe, die eine treue transitive Permutationsdarstellung vom Grad n besitzt. Kenntnis der transitiven Gruppen von Grad n impliziert folglich Kenntnis über kleine Quotienten von Gruppen mit Untergruppen von Index n. Operiert G auch auf anderen Objekten, so kann man bisweilen diesen Objekten transitive Permutationsgruppen zuordnen. Als Musterbeispiel mag der folgende Satz aus [Bir1994] dienen:

(3) SATZ: Ist $n \in \mathbb{N}$, so stehen die folgenden Familien von Objekten in Bijektion:

i) Tripel $(\mathcal{R}, \phi, O)$ mit $\mathcal{R}$ eine n-blättrige RIEMANNsche Fläche, $\phi\colon \mathcal{R} \to \hat{\mathbb{C}}$ eine höchstens an $\{\infty, 0, k\}$ verzweigte Überlagerungsabbildung und O ein Punkt von $\mathcal{R}$ über 0.

ii) Quadrupel $(\sigma_\infty, \sigma_0, \sigma_1; \nu)$ bis auf Konjugation mit S_n. Dabei ist $\sigma_\infty, \sigma_0, \sigma_1 \in S_n$, $\sigma_\infty\sigma_0\sigma_1 = id$, $\langle\sigma_0, \sigma_1\rangle$ transitiv von Grad n und ν ein markierter Zykel aus σ_∞.

[4] Dies gilt zum Beispiel für die Invariante aus Lemma (2)

iii) Untergruppen $\Gamma \leq \Gamma(2) = \left\{ z \mapsto \frac{az+b}{cz+d} \;\middle|\; a,b,c,d \in \mathbb{Z}; ad-bc=1; b,c \equiv 0 \pmod 2 \right\}$ und

iv) Zeichnungen mit n Kanten.

Paare von Permutationen mit transitiven Erzeugnis parametrisieren daher unter anderem gewisse Überlagerungen RIEMANNscher Flächen. Die Arbeit [AR1993] zum Beispiel klassifiziert zu diesem Zweck Paare von Permutationen von gewissem Zykeltyp bis auf Konjugation in S_{18}.

Die Klassen transitiver Permutationsgruppen liefern natürlich eine erste gröbere Einteilung der Paare von Permutationen, deren Erzeugnis transitiv ist.

I.2.5. Schließlich hat sich bei der praktischen Durchführung herausgestellt, daß das Klassifikationsprogramm auch als Test für das benutzte Computeralgebrasystem dienen kann: Die benutzten Methoden umfassen mit Ausnahme der Charaktertheorie sowie der Erkennung von Matrixgruppen nahezu alle Bereiche der Gruppentheorie, für die bislang Algorithmen existieren und in Systemen wie GAP oder Magma implementiert sind. Während des Konstruktionsprozesses werden diese Algorithmen auf eine Vielzahl von Gruppen angewandt wodurch sich zunächst Fehler zeigen, die in einen Abbruch eines Algorithmus münden. Durch Zufallsauswahl und Modifikation von Anordnungen läßt es sich aber darüberhinaus erreichen, daß bei erneuter Konstruktion der Gruppen eines vorgegebenen Grades andere Repräsentanten gewählt und damit die Algorithmen auf andere Gruppen angewandt werden. Rechenfehler zeigen sich dabei dann oft in einer – theoretisch verbotenen – Diskrepanz der Ergebnisse verschiedener Läufe.

In diesem Zusammenhang stellt sich natürlich auch die Frage nach der Korrektheit der erhaltenen Ergebnisse. Dieses Problem wird in Abschnitt VI.1 angesprochen.

KAPITEL II

Grundlagen aus der Gruppentheorie

In diesem Kapitel sollen – nicht zuletzt, um die hier benutzte Sprache und Notation einzuführen – einige gruppentheoretische Definitionen und grundlegende Aussagen zusammengefasst werden. Viele der hier bewiesenen Sätze und Lemmata dürften zum „common lore“ der Gruppentheorie zählen. Da sie aber zum Teil in der Literatur versteckt sind oder einen anderen Begriffsapparat benutzen seien hier eigene Beweise gegeben.

II.0.6. Dieser Abschnitt enthält einige triviale Folgerungen aus dem Bahnensatz, die die Bahnen einer Untergruppe in Bijektion zu Doppelnebenklassen setzen.

(4) LEMMA: Ist G eine Gruppe, die transitiv auf Ω operiert und $U \leq G$, so entsprechen die U-Bahnen auf Ω den Doppelnebenklassen $\mathrm{Stab}_G(\omega)\backslash G/U$ für ein fest gewähltes $\omega \in \Omega$ vermöge $\mathrm{Stab}_G(\omega)rU \mapsto (\omega^r)^U$ für Repräsentanten $r \in G$.

Beweis: Liegen ω^r und ω^s in derselben U-Bahn, so existiert ein $u \in U$ mit $\omega^{ru} = \omega^s$, das heißt es ist $\mathrm{Stab}_G(\omega)rU = \mathrm{Stab}_G(\omega)sU$. Die Umkehrung folgt analog. $\square$

Es sei G eine Gruppe und $U, V \leq G$. Ist $g \in G$, welches U auf V konjugiert, so liegen die Elemente von G, die U per Konjugation auf V abbilden, somit in der Doppelnebenklasse $N_G(U)gN_G(V)$. Weiterhin gilt bei gleichen Voraussetzungen:

(5) LEMMA: Ist $U^g = V$, so ist $N_G(U)^g = N_G(V)$, und es gilt $N_G(U)g = N_G(U)gN_G(V) = gN_G(V)$.

Beweis: Es ist

$$N_G(U)^g = \{x^g \mid U^x = U\} = \{x \mid U^{gxg^{-1}} = U^{x^{g^{-1}}} = U\} = \{x \mid (U^g)^x = U^g\} = N_G(V).$$

Ist nun $gy \in gN_G(V)$, so existiert ein $x \in N_G(U)$ mit $y = x^g$, also $gy = gg^{-1}xg = xg$, woraus die zweite Behauptung folgt. $\square$

Sind Untergruppen U und V gegeben, so findet sich ein Element g, das U auf V konjugiert somit — so ein solches g existiert — in einem Vertretersystem der Rechtnebenklassen $N_G(U)\backslash G$, die Menge aller dieser Elemente ist die Nebenklasse $gN_G(V)$.

II.1. Isomorphismen von Permutationsgruppen

II.1.1.

(6) DEFINITION: Zwei Permutationsgruppen $G, H \leq S_n$ heißen *permutationsisomorph* oder *äquivalent*, wenn sie in S_n konjugiert sind.

(7) Lemma: Es seien $G, H \leq S_n$ transitive Gruppen, G_1 und H_1 die entsprechenden Punktstabilisatoren sowie $\varphi\colon G \to H$ ein Isomorphismus. Dann ist φ durch Konjugation in S_n realisiert (das heißt, es existiert ein $\sigma \in S_n$ mit $g\varphi = g^\sigma$ für alle $g \in G$) genau dann, wenn $G_1\varphi$ in H zu H_1 konjugiert ist.

Beweis: Angenommen, $G_1\varphi = H_1^h$ für ein geeignetes $h \in H$. Wir können ohne Einschränkung annehmen, daß $G_1\varphi = H_1$ gilt, da wir φ ansonsten nur um einen inneren Automorphismus von H abändern müssen (der durch Konjugation in $H \leq S_n$ realisiert ist). Dann muß φ aber die Nebenklassen $G_1 \backslash G$ auf Nebenklassen $H_1 \backslash H$ abbilden. Diese stehen jeweils in Bijektion zu $\Omega = \{1, \dots, n\}$; es seien $\{g_i\}$ und $\{h_i\}$ Repräsentantensysteme der Nebenklassen nach G_1, beziehungsweise H_1 mit $1^{g_i} = i = 1^{h_i}$. Damit sei $\sigma \in S_n$ vermöge $i^\sigma = j$ definiert, wenn $(G_1 g_i)\varphi = H_1 h_j$ ist. Folglich gilt:

$$(G_1 g_i)\varphi = H_1 h_{(i^\sigma)}. \tag{8}$$

Nun seien $g \in G$ und $i \in \Omega$ beliebig und $k = i^g$. Also ist

$$G_1 g_i g = G_1 g_k \tag{9}$$

und damit

$$H_1 h_{(i^\sigma)}(g\varphi) \overset{(8)}{=} (G_1 g_i)\varphi(g\varphi) = (G_1 g_i g)\varphi \overset{(9)}{=} (G_1 g_k)\varphi \overset{(8)}{=} H_1 h_{(k^\sigma)}.$$

Es ist also $(i^\sigma)^{(g\varphi)} = k^\sigma = (i^g)^\sigma$. Ersetzen wir i durch $i^{\sigma^{-1}}$ so erhalten wir $i^{(g\varphi)} = i^{\sigma^{-1} g \sigma}$. Für alle $i \in \Omega$ ist damit $i^{(g\varphi)} = i^{(g^\sigma)}$. Da die Darstellung von G und H auf Ω treu ist, gilt somit $g\varphi = g^\sigma$.
Existiert andererseits ein solches σ, so bildet dieses Punktstabilisatoren auf Punktstabilisatoren ab, woraus die Behauptung folgt. □

II.1.2. Dieses Lemma gestattet uns eine Reihe von Folgerungen:

(10) Folgerung: Zwei reguläre Untergruppen von S_n sind genau dann konjugiert, wenn sie isomorph sind.

(11) Folgerung: Ist $G \leq S_n$ transitiv und φ ein Automorphismus von G, so läßt sich φ genau dann durch Konjugation mit $\sigma \in N_{S_n}(G)$ realisieren, wenn φ die G-Konjugiertenklasse von G_1 fest läßt.

und daher

(12) Folgerung: Ist $G \leq S_n$ transitiv und die Konjugiertenklasse von G_1 in G charakteristisch, so ist jeder Automorphismus von G durch Konjugation in $N_{S_n}(G)$ realisierbar.

sowie schließlich:

(13) Satz: Sei G eine endliche Gruppe, $|G| = n$ und ρ die reguläre Permutationsdarstellung von G. Es sei $N = N_{S_n}(G\rho)$. Dann besteht $\mathrm{Aut}(G)$ aus den von N per Konjugation auf $G\rho$ induzierten Abbildungen.

II.1.3. Konjugation in der S_n läßt die Zykelstruktur von Elementen invariant. Damit erhält man das folgende offensichtliche notwendige Kriterium für die Konjugation von Untergruppen:

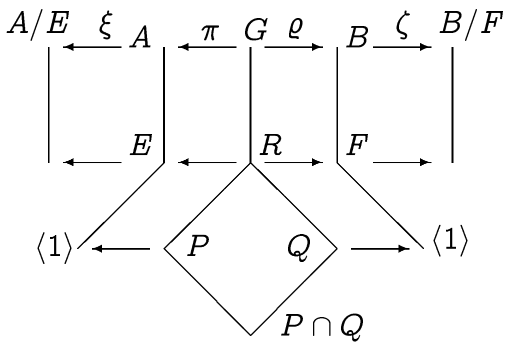
(14) BEMERKUNG: Zwei Permutationsgruppen können nur dann konjugiert sein, wenn sie die gleiche Größe haben, die Mengen der Paare von Konjugiertenklassenordnung und -repräsentantenzykelstruktur gleich sind sowie die Normalisatoren in einer Obergruppe, die das konjugierende Element enthält, ebenfalls konjugiert sind.

Als weitere notwendige Bedingungen können natürlich zusätzlich jedwede Isomorphieinvarianten, wie zum Beispiel Ordnungen oder Isomorphietypen der Kommutatorgruppe oder der Sylowgruppen dienen.

II.2. Subdirekte Produkte

In diesem Abschnitt sollen subdirekte Produkte als Gruppen, die durch eine Reihe von Projektionen eindeutig bestimmt sind, beschrieben werden. Auch betrachten wir eine Reihe von Automorphismen derselben. Die Definition eines subdirekten Produktes stammt von R. REMAK [Rem1930], die grundlegenden Aussagen finden sich aber schon in [Gou1889, §11,12]. Aufgrund der verschiedenen Schreib- und Sprechweisen seien die benötigten Aussagen hier nochmals zusammengefasst.

II.2.1. Es sei G eine Gruppe mit Normalteilern $P, Q \lhd G$. Die Projektionen auf die Faktorgruppen $A = G/P$ und $B = G/Q$ seien mit $\pi\colon G \twoheadrightarrow A$ und $\varrho\colon G \twoheadrightarrow B$ bezeichnet. Es sei $R = \langle P, Q \rangle$. Die Bilder $E = R\pi \lhd A$ und $F = R\varrho \lhd B$ sind Normalteiler, die dazugehörigen natürlichen Epimorphismen seien mit $\xi\colon A \twoheadrightarrow A/E$ und $\zeta\colon B \twoheadrightarrow B/F$ bezeichnet. Aufgrund des Homomorphiesatzes ist $A/E \cong G/R \cong B/F$. Dieser gemeinsame Quotient G/R sei mit Y bezeichnet.



(15) LEMMA: Definieren wir somit eine Abbildung $\chi\colon B/F \to A/E$ der Faktorgruppen[1] durch:

$$g\varrho\zeta\chi = g\pi\xi \tag{16}$$

für $g \in G$, so ist χ Isomorphismus.

<u>Beweis:</u> Ist $g\varrho\zeta = h\varrho\zeta$, so ist $(g/h)\varrho \in \operatorname{Kern}\zeta$ und somit $g/h \in R$. Also ist $(g/h)\pi \in \operatorname{Kern}\xi$ und daher $g\pi\xi = h\pi\xi$. Die Abbildung ist also wohldefiniert. Mit analogen Rechnungen folgen die Homomorphismuseigenschaft und die Injektivität. Die Surjektivität ist trivial.

[1] Die Benennung scheint hier und in Folge jeweils in unnatürlicher Reihenfolge zu sein. Sie erweist sich aber als günstiger in Hinblick auf eine später getroffene Wahl von A

□

Gilt nun zusätzlich $P \cap Q = \langle 1 \rangle$, so ist jedes Element $g \in G$ durch seine Projektionen $g\varrho$ und $g\pi$ eindeutig bestimmt, die Einbettung $\iota\colon g \mapsto (g\varrho, g\pi)$ von G in das direkte Produkt $B \times A$ ist injektiv. Nachrechnen verifiziert unmittelbar, daß ι auch Gruppenhomomorphismus ist. Wir können G somit als Untergruppe des direkten Produktes auffassen und bezeichnen es auch als (inneres) *subdirektes Produkt* von $B = G/Q$ und $A = G/P$ zu den Normalteilern $F \lhd B$, $E \lhd A$ sowie dem Isomorphismus χ der Faktorgruppen. Aus dem Isomorphiesatz folgt unmittelbar, daß $P \cong F$ vermöge ϱ und $Q \cong E$ vermöge π gilt.

(17) Definition: Zu Gruppen B und A mit Normalteilern $F \lhd B$, $E \lhd A$, den natürlichen Homomorphismen $\zeta\colon B \twoheadrightarrow B/F$ und $\xi\colon A \twoheadrightarrow A/E$ sowie einem Isomorphismus χ der Faktorgruppen betrachten wir nun die Menge

$$M = \{(b, a) \in B \times A \mid b\zeta\chi = a\xi\} \subseteq B \times A.$$

Diese heißt das (äußere) subdirekte Produkt von B und A zu F, E, ζ, ξ und χ.

(18) Lemma: M ist eine Untergruppe des direkten Produktes.

Beweis: Es genügt, die Abgeschlossenheit zu zeigen, die unmittelbar durch Nachrechnen folgt: $(b, a)(d, c) = (bd, ac)$ und $(bd)\zeta\chi = (b\zeta\chi)(d\zeta\chi) = (a\xi)(c\xi) = (ac)\xi$; inverse analog.
□

(19) Lemma: Mit oben gewähltem ι und χ ist $G\iota = M$.

Beweis: Aus (16) folgt, daß $G\iota \subseteq M$ gilt. Sei also andererseits $(b, a) \in M$. Wähle $g \in G$ mit $g\varrho = b$. Dann ist wegen (16) $g\varrho\zeta\chi = g\pi\xi = a\xi$, also $g\pi = ac$ mit $c \in \operatorname{Kern}\xi = E$. Wähle $h \in Q$ mit $h\pi = c^{-1}$ und setze $\hat{g} = gh$. Dann ist $\hat{g}\varrho = (g\varrho)(h\varrho) = g\varrho = b$ und $\hat{g}\pi = a$. □

Das (isomorphe) Bild $G\iota$ ist also bei fest gewählten Projektionen nur durch die Faktorgruppen B, A, F, E und die Homomorphismen ζ, ξ und χ bestimmt. Es ist also gerechtfertigt, von dem inneren subdirekten Produkt zu sprechen.

(20) Bemerkung: Da das äußere subdirekte Produkt in sich selber inneres subdirektes Produkt zu den Projektionskernen ist, seien äußere und innere Produkte nicht mehr formal unterschieden; wir sprechen im folgenden nur noch von *dem* subdirekten Produkt.

Der Übersichtlichkeit halber werden wir später ein subdirektes Produkt als durch B, A, F, E und χ gegeben annehmen ohne die natürlichen Homomorphismen ζ und ξ (die als durch F und E impliziert angesehen werden sollten) explizit zu erwähnen.

(21) Lemma: Mit gleichen Bezeichnungen wie oben ist $F = \operatorname{Kern}(\pi)\varrho$ und $E = \operatorname{Kern}(\varrho)\pi$.

Beweis: Nachrechnen verifiziert unmittelbar

$$F = (\langle P, Q \rangle)\varrho \overset{Q\varrho = 1}{=} P\varrho = (\operatorname{Kern}\pi)\varrho$$

und analog für E. □

(22) BEMERKUNG: Da das subdirekte Produkt Untergruppe des direkten Produktes ist, übertragen sich Eigenschaften wie „abelsch", „elementar", „auflösbar" oder „nilpotent", die für beide Faktoren gelten, auch auf das subdirekte Produkt derselben.

II.2.2. Der Vollständigkeit halber sei noch eine weitere, kategorielle, Beschreibung des subdirekten Produktes gegeben, die zeigt, daß dieses auch über universelle Eigenschaften definiert werden kann.

Zu Gruppen A, B und Y und Epimorphismen $\xi\colon A \twoheadrightarrow Y$ sowie $\zeta\colon B \twoheadrightarrow Y$ betrachten wir das folgende Diagramm:

$$\begin{tikzcd} & A \arrow[d, "\xi"'] \\ B \arrow[r, "\zeta"] & Y \end{tikzcd}$$

(23) LEMMA: Das subdirekte Produkt M zu B, A, Kern ζ, Kern ξ und dem impliziten Isomorphismus $\bar{\zeta}\mathrm{id}_Y\bar{\xi}^{-1}$ der Faktorgruppen ist der *pull-back* dieses Diagramms, d.h. es gibt Morphismen $\varrho\colon M \to A$, $\pi\colon M \to B$, die das Diagramm M-A-B-Y kommutativ machen und zu jedem L mit diesen Eigenschaften gibt es ein $\varphi\colon L \to M$, so daß das folgende Diagramm kommutativ wird:

$$\begin{tikzcd} L \arrow[dr, "\varphi"] \arrow[drr, "\alpha"] \arrow[ddr, "\beta"'] & & \\ & M \arrow[r, "\varrho"] \arrow[d, "\pi"] & A \arrow[d, "\xi"'] \\ & B \arrow[r, "\zeta"] & Y \end{tikzcd}$$

<u>Beweis:</u> Ohne Beschränkung der Allgemeinheit sei angenommen, daß α und β surjektiv sind (ansonsten ersetzen wir A und B durch die jeweiligen Bilder). Betrachte $K :=$ Kern $\alpha \cap$ Kern β. Nach obiger Definition ist dann L/K subdirektes Produkt von A und B. Dies liefert den Morphismus φ. □

II.2.3. Für uns sind subdirekte Produkte insbesondere deshalb von Bedeutung, weil intransitive Permutationsgruppen iterierte subdirekte Produkte transitiver Gruppen sind.

(24) BEISPIEL: Es sei G intransitive Permutationsgruppe, die auf $\Omega = \Delta \cup \Gamma$ mit $\Delta \cap \Gamma = \emptyset$ treu operiert, so daß Δ und Γ unter G invariant sind. Dann ist G subdirektes Produkt zu den Operationshomomorphismen ϱ und π auf $G|_\Delta$ und $G|_\Gamma$ (mit geeigneten Normalteilern und Isomorphismen der Faktorgruppen). Es sei wieder $B = G\varrho$ und $A = G\pi$. Das direkte Produkt $B \times A$ operiert ebenfalls intransitiv auf $\Delta \cup \Gamma$ vermöge

$$\omega^{(b,a)} = \begin{cases} \omega^b & \omega \in \Delta \\ \omega^a & \omega \in \Gamma \end{cases}$$

und läßt Δ und Γ dabei fest[2]. Mit dieser Operation des direkten Produktes ist $G = G\iota$ als Permutationsgruppen.

<u>Beweis:</u> Für $g \in G$ und $\omega \in \Delta$ ist

$$\omega^{g\iota} = \omega^{(g\varrho, g\pi)} = \omega^{g\varrho} \overset{\omega \in \Delta}{=} \omega^{g}$$

und analog für $\omega \in \Gamma$. □

Eine Permutationsgruppe, die mehr als zwei Bahnen besitzt, ist demnach zunächst als subdirektes Produkt der Projektion auf eine Bahn sowie der Projektion auf die Vereinigung der übrigen Bahnen darstellbar. Letztere Projektion kann aber iteriert wiederum als subdirektes Produkt dargestellt werden. Die Gruppe selber ist damit iteriertes subdirektes Produkt der Projektionen auf die einzelnen Bahnen.

Die Reihenfolge, in der wir die Bahnen dem Produkt hinzufügen, ist dabei jedoch für das endgültige Produkt unerheblich, lediglich die in den Zwischenschritten zu betrachtenden Normalteiler und Isomorphismen ändern sich dabei. Die – im Permutationskontext natürliche – Projektion auf eine beliebige Bahn ist dabei dann für das subdirekte Produkt formal als Verkettung von Projektionen aufzufassen, die auf immer kleinere Teilmengen von Bahnen abbilden. Da dies aber das gleiche Ergebnis wie die offensichtliche Bahnenprojektion liefert, werden wir diese beiden Abbildungen meist miteinander identifizieren und von einem solchen iterierten subdirekten Produkt auf jede Teilmenge der Bahnen projizieren.

(25) Bemerkung: Kennt man alle transitiven Gruppen von Grad $\leq n$, so kennt man somit im wesentlichen alle Permutationsgruppen von Grad n (zur eigentlichen Konstruktion siehe IV.3.8). Dies motiviert letztendlich auch die Einschränkung dieser Arbeit auf transitive Gruppen.

II.2.4. Im letzten Abschnitt war bereits von iterierten subdirekten Produkten die Rede. Natürlich läßt sich die Definition aus (II.2.1) auch auf beliebig (endlich) viele Gruppen mit gemeinsamer isomorpher Faktorgruppe erweitern. In der Sprache von R. Remak [Rem1930] heißt eine solche Gruppe ein „meromorphes Produkt". Nicht jedes iterierte subdirekte Produkt ist jedoch ein meromorphes Produkt(de facto sogar nur die allerwenigsten), wie das folgende Beispiel zeigt:

(26) Beispiel: Es sei $G = \langle (1,2)(3,4), (1,2)(5,6) \rangle$. Dann ist $G \cong C_2 \times C_2$ eine intransitive Gruppe mit 3 Bahnen, auf denen sie jeweils wie C_2 operiert. G ist somit als zweifach iteriertes subdirektes Produkt von C_2 darstellbar. Ein meromorphes Produkt von drei Gruppen isomorph C_2 hätte nun aber entweder C_2 oder $\langle 1 \rangle$ als gemeinsame Faktorgruppe und wäre damit von Ordnung 2 oder 8 (d.h. Diagonale oder direktes Produkt). G kann also kein meromorphes Produkt sein. Nichtsdestotrotz ist G Kern der Blockdarstellung der Gruppe $A_4(6) = \langle (1,2)(3,4), (1,3,5)(2,4,6) \rangle$ (Zur Nomenklatur der Gruppe siehe A). Im Vorgriff auf Kapitel III sei daher an dieser Stelle bereits bemerkt, daß meromorphe Produkte zur Beschreibung von Blockkernen nicht ausreichen.

[2] Diese Operation ist zu unterscheiden von der transitiven Operation auf $\Delta \times \Gamma$

II.2.5. Wir wollen nun intransitive Permutationsgruppen bis auf Äquivalenz klassifizieren. Dazu betrachten wir wie oben eine intransitive Gruppe G, die auf $\Omega = \Delta \cup \Gamma$ mit $\Delta \cap \Gamma = \emptyset$ operiert und Δ und Ω dabei festlässt. Bei Identifikation von Ω mit $\{1, \dots, |\Omega|\}$ setzen wir $\Omega_B := \{1, \dots, |\Delta|\}$ und $\Omega_A := \{|\Delta| + 1, \dots, |\Omega|\}$. In S_Ω können wir Δ auf Ω_B und simultan Γ auf Ω_A abbilden. G ist also äquivalent zu einer Gruppe, die Ω_A und Ω_B als Vereinigungen von Bahnen besitzt. Wollen wir nur Repräsentanten der Äquivalenzklassen betrachten, so genügt es folglich, Gruppen zu betrachten, die Ω_B und Ω_A invariant lassen. Die Konjugation wird damit auf den Stabilisator dieser Partition von Ω eingeschränkt. Ist $|\Omega_B| \neq |\Omega_A|$, so ist dies $S := S_{\Omega_B} \times S_{\Omega_A}$, andernfalls $S \rtimes S_{\{\Omega_B, \Omega_A\}} \cong S_{\Omega_B} \wr C_2$. Die dazugehörigen Einbettungen seien $\beta\colon S_{\Omega_B} \to S$ und $\alpha\colon S_{\Omega_A} \to S$. Da der zweite Fall komplizierter ist, betrachten wir hier nur Konjugation mit S, der allgemeine Fall wird später in Kapitel IV betrachtet werden.

Als nächstes betrachten wir die Bilder einer intransitiven Gruppe unter den Projektionen ϱ auf S_{Ω_B} und π auf S_{Ω_A}. Durch Konjugation in S_{Ω_B}, beziehungsweise S_{Ω_A} (und damit Konjugation in S) können wir die Projektionsbilder auf beliebige zu ihnen äquivalente Gruppen abbilden. Da uns nur ein Repräsentantensystem der Äquivalenzklassen intransitiver Gruppen auf Ω interessiert, seien ab jetzt nur noch solche Gruppen betrachtet, deren Projektionen jeweils Repräsentanten der lokalen (unter der symmetrischen Gruppe auf der jeweiligen Menge) Äquivalenzklassen sind. Da $|\Omega_A|, |\Omega_B| \lneqq |\Omega|$ ist können wir annehmen, daß hierfür bereits Repräsentantensysteme bestimmt worden sind.

Nun seien zwei spezielle Bilder $G\varrho = B \leq S_{\Omega_B}$ und $G\pi = A \leq S_{\Omega_A}$ vorgegeben. Die betrachteten Gruppen sind also subdirekte Produkte von B und A. Da wir keine Gruppen mit zu B, beziehungsweise A äquivalenten (aber ungleichen) Projektionen betrachten, brauchen wir damit bei der Suche nach äquivalenten Gruppen nur noch mit solchen Elementen zu konjugieren, die diese Projektionen festlassen. Dies ist offenbar die Gruppe $(D\beta) \times (C\alpha) \leq S$ mit $D = N_{S_{\Omega_B}}(B)$ und $C = N_{S_{\Omega_A}}(A)$.

II.2.6. Um die Konjugationsoperation auf solchen subdirekten Produkten besser beschreiben zu können, wollen wir sie genauer parametrisieren. Die Menge der (in $(B\beta) \times (A\alpha) \leq S$ eingebetteten) verschiedenen subdirekten Produkte von B und A wird nach der Definition aus II.2.1 bestimmt durch:

i) Die Normalteiler $F \trianglelefteq B$,
ii) die Normalteiler $E \trianglelefteq A$, so daß $B/F \cong A/E$ sowie
iii) die Isomorphismen χ zwischen B/F und A/E.

Ein so parametrisiertes subdirektes Produkt sei im weiteren als

$$M(F, E, \chi) = \{(b, a) \in S \mid (Fb)\chi = Ea\}$$

bezeichnet. Ist umgekehrt ein solches M gegeben, so sind die dazugehörigen Normalteiler $F = \mathrm{Kern}(\pi|_M)\varrho \lhd B$ und $E = \mathrm{Kern}(\varrho|_M)\pi \lhd A$ Kernbilder.

Die Isomorphismen χ in iii) werden bei Wahl eines zu B und A fest gewählten Isomorphismus $\gamma\colon B/F \to A/E$ per Rechtsmultiplikation $\chi = \gamma\eta$ mit $\eta \in \mathrm{Aut}(A/E)$ erhalten.

(27) Lemma: Sind $E \lhd A$ und $F \lhd B$ Normalteiler und $\gamma\colon B/F \to A/E$ der fest gewählte Isomorphismus von B/F auf A/E, so erhält man für jedes $\eta \in \mathrm{Aut}(A/E)$ ein subdirektes

Produkt $M \leq B \times A$, welches von $F\beta$ sowie der Menge der Paare

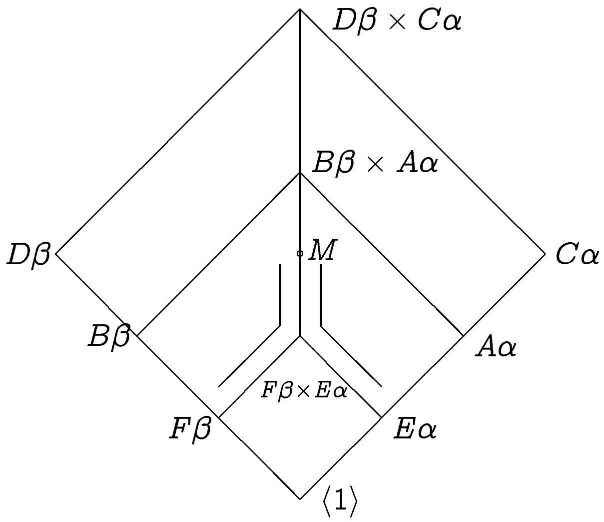
$$J = \{(b,a) | (Fb)\gamma\eta = Ea\}$$

erzeugt wird, wobei a ein Erzeugendensystem von A durchlaufe und es keine (b, a) und $(b', a) \in J$ mit gleichem a und verschiedenem b und b' gebe. Jedes subdirekte Produkt zu B, A, F und E wird auf diese Weise erhalten.

Beweis: Als Verkettung von Isomorphismen ist auch $\gamma\eta$ ein Isomorphismus der Faktorgruppen. Sind umgekehrt χ und χ' Isomorphismen, so ist χ^{-1}/χ' Automorphismus.

Gemäß Definition liegen $F\beta$ und J im subdirekten Produkt zu $\gamma\eta$. J erzeugt $E\alpha$ als $(1, E)$ sowie ein Nebenklassenvertretersystem von $M/((F\beta) \times (E\alpha))$, womit ganz M erzeugt wird. $\square$

II.2.7. Als nächstes wollen wir die Konjugation unter $(D\beta) \times (C\alpha)$ betrachten.



(28) Lemma: Sind F und F' unter D konjugiert, so führen sie zu Klassen von subdirekten Produkten, die unter $D\beta \leq S$ konjugiert sind

Beweis: Es seien χ ein Isomorphismus $B/F \to A/E$ und $d \in D$ mit $F = F'^d$. Wir setzen $\tilde{\chi}\colon F'b \mapsto ((F'b)^d)\chi = (Fb^d)\chi$ als Isomorphismus $B/F' \to A/E$. Dann ist

$$\begin{aligned} M(F,E,\chi)^{(d,1)^{-1}} &= \{(b^{d^{-1}}, a) \mid (Fb)\chi = Ea\} \\ &= \{(b,a) \mid ((F'^d)b^d)\chi = ((F'b)^d)\chi = (F'b)\tilde{\chi} = Ea\} \\ &= M(F', E, \tilde{\chi}) \end{aligned}$$

subdirektes Produkt zu F', E und $\tilde{\chi}$. Modifikationen von χ zu $\chi\eta$ impliziert Modifikation von $\tilde{\chi}$ zu $\tilde{\chi}\tilde{\eta}$ und umgekehrt. $\square$

(29) Corollar: Ebenso folgt hier, daß unter C konjugierte E und E' zu konjugierten subdirekten Produkten führen.

Sind F und F' unter D konjugierte Normalteiler von B, so gibt es also zu jedem subdirekten Produkt zu F ein S-konjugiertes subdirektes Produkt zu F' und umgekehrt. Da wir uns jedoch nur für ein Repräsentantensystem der Klassen interessieren, genügt es somit, nur noch subdirekte Produkte zu F (und zu keinem seiner Konjugierten) zu betrachten. Damit schränken wir die Konjugation natürlich auf F normalisierende Elemente ein. Gleiches gilt für E. Es zeigt sich, daß wir die danach verbliebenen Konjugationen alternativ auch durch Änderung des Isomorphismus beschreiben können:

(30) LEMMA: Es sei $\chi\colon B/F \to A/E$. Ist $d \in N_D(F)$ und ϑ_d der innere Automorphismus von $N_D(F)/F$ zu Fd, so führen χ und $\vartheta_d\chi$ zu unter $D\beta$ konjugierten subdirekten Produkten.

<u>Beweis:</u> Es ist

$$\begin{aligned} M(F,E,\chi)^{(d^{-1},1)} &= \{(b^{d^{-1}},a) \mid (Fb)\chi = Ea\} \\ &= \{(b,a) \mid Ea = (Fb^d)\chi = ((F^d)b^d)\chi = (Fb)^{Fd}\chi = Fb\vartheta_d\chi \\ &= \{(b,a) \mid (Fb)\vartheta_d\chi = Ea\} = M(F,E,\vartheta_d\chi) \end{aligned}$$

das Produkt zu $\vartheta_d\chi$. □

Setzt man $F' := F$, so kann man diesen Beweis natürlich als Spezialfall des Beweises von Lemma (28) ansehen. Die Aussagen wurden lediglich getrennt, um eine gewisse Hierarchie bei der Auswahl von Konjugationsrepräsentanten zu erreichen.

(31) COROLLAR: Auch hier folgt, daß für $c \in N_C(E)$ mit zugehörigem inneren Automorphismus ϑ_c die beiden Isomorphismen $\chi\vartheta_c$ und χ zu unter C konjugierten subdirekten Produkten führen.

Ist $\gamma\colon B/F \to A/E$ ein fest gewählter Isomorphismus und ϑ_d ein durch Konjugation induzierter Automorphismus von B/F, so ist $\gamma^{-1}\vartheta_d\gamma$ ein Automorphismus von A/E. Durch diese Übertragung ist es möglich, nur noch in einer Automorphismengruppe rechnen zu müssen.

Die Aussagen der vergangenen Lemmata zusammen gestatten nun eine Parametrisierung der S-Klassen subdirekter Produkte von B und A mittels Repräsentanten der Normalteiler F und E sowie eines Repräsentantensystems von Automorphismen.

(32) SATZ: Es sei $\mathcal{E}$ ein Repräsentantensystem der C-Klassen von Normalteilern $E \lhd A$. Zu $E \in \mathcal{E}$ sei

$$V_E = \{\vartheta_c \in \mathrm{Aut}(A/E) \mid c \in N_C(E)\}$$

die Menge der durch Konjugation induzierten Automorphismen der Faktorgruppe A/E. Zu $E \in \mathcal{E}$ sei die Menge $\mathcal{F}_E$ ein Repräsentantensystem der D-Klassen von Normalteilern $F \lhd B$, für die ein Isomorphismus $\gamma_{(F,E)}\colon B/F \to A/E$ existiert (andere F brauchen wir zu diesem E nicht zu betrachten). Diese Isomorphismen seien einmal fest gewählt. Zu $F \in \mathcal{F}_E$ sei zusätzlich

$$U_{(F,E)} = \{\gamma_{(F,E)}^{-1}\vartheta_d\gamma_{(F,E)} \in \mathrm{Aut}(A/E) \mid d \in N_D(F)\}$$

die Menge der mittels $\gamma_{(F,E)}$ von Konjugation in $N_D(F)$ induzierten Automorphismen der Faktorgruppe A/E. Schließlich sei die Menge $X_{(F,E)}$ ein Repräsentantensystem der

Doppelnebenklassen $U_{(F,E)}\backslash\mathrm{Aut}(A/E)/V_E$. Dann ist

$$\mathcal{M} = \bigcup_{E\in\mathcal{E}} \bigcup_{F\in\mathcal{F}_E} \bigcup_{\eta\in X_{(F,E)}} M(F,E,\gamma_{(F,E)}\eta)$$

ein Repräsentantensystem der S-Klassen in S eingebetteter subdirekter Produkte von B und A.

Beweis: Es sei M ein mittels $\iota = (\beta,\alpha)$ in S eingebettetes subdirektes Produkt von B und A. Nach Lemma (28) und (29) können wir (indem wir M durch ein geeignetes S-Konjugiertes ersetzen) ohne Beschränkung der Allgemeinheit annehmen, daß $M = M(F,E,\chi)$ für $E \in \mathcal{E}$ $F \in \mathcal{F}_E$, sowie einen Isomorphismus χ der Faktorgruppen ist. Durch Konjugation in $N_D(F)\beta$ und $N_C(E)\alpha$ können wir χ gemäß (30) und (31) durch ϑ_c, beziehungsweise ϑ_d abändern. Damit läßt sich schließlich M auf ein $M(F,E,\gamma_{(F,E)}\eta)$ mit $\eta \in X_{(F,E)}$ konjugieren. M ist also zu einem Vertreter aus $\mathcal{M}$ konjugiert.

Nun seien $M = M(F,E,\gamma_{(F,E)}\eta)$ und $M' = M(F',E',\gamma_{(F',E')}\eta')$ aus $\mathcal{M}$ unter S konjugiert: $M^s = M'$. Da $M\varrho = M'\varrho = B$ und $M\pi = M'\pi = A$ ist, muß die Konjugation bereits in $D\beta \times C\alpha$ stattfinden, es ist also $s = (d,c)$. Die Kerne $F^{(\prime)}$ und $E^{(\prime)}$ sind durch Kerne und Bilder von ϱ und π definiert, es muß also $F^d = F'$ und $E^c = E'$ gelten. Da $\mathcal{E}$ und $\mathcal{F}_E$ Repräsentantensysteme sind muß somit $E = E'$ und $F = F'$ gelten. Folglich ist $\gamma_{(F,E)} = \gamma_{(F',E')} =: \gamma$. Dann ist aber $\gamma\gamma^{-1}\vartheta_d\gamma\eta\vartheta_c = \gamma\eta'$, also $U_{(F,E)}\eta V_E = U_{(F,E)}\eta' V_E$ und daher $\eta = \eta'$. Also ist $M = M'$, was zu zeigen war. □

Für praktische Zwecke ist die Charakterisierung der Klassen aus diesem Satz jedoch nur mit Einschränkungen brauchbar, da die Doppelnebenklassenberechnung in der Automorphismengruppe sehr aufwendig werden kann.

II.2.8. Der vorangegangene Satz beschrieb die S-Klassen. Möchte man hingegen vorgegebene subdirekte Produkte auf S-Konjugiertheit testen, so ist man bisweilen in der folgenden Situation: Zu einem gegebenen M soll die $C\alpha \times D\beta$-Bahn (beziehungsweise deren kleinstes Element) bestimmt werden. Dies geschieht dadurch, daß zunächst alle $C\alpha$-Bilder berechnet werden und diese danach mit $D\beta$ konjugiert werden. Existiert zu $c \in C$ jedoch ein $d \in D$, so daß die Konjugation mit (d,c) die Gruppe M normalisiert, so kann das Bild von M unter $c\alpha$ auch als Bild unter $D\beta$ erreicht werden, was die notwendigen Konjugationen einschränkt. Wir wollen ein Kriterium angeben, wann solches geschehen kann. Im Geiste des vorangegangenen Satzes könnte dies durch Gleichheit gewisser Doppelnebenklassen beschrieben werden. Statt dessen soll hier aber ein in der Praxis besser testbares Kriterium angegeben werden.

Es sei wiederum $M = M(F,E,\chi)$, die zugehörigen Epimorphismen seien mit $\xi\colon A \to A/E$ und $\zeta\colon B \to B/F$ bezeichnet. Dann gilt:

(33) Lemma: Zu $c \in C$ gibt es ein $d \in D$ mit $M^{(d,c)} = M$ (das heißt $(d,c) \in N_{D\beta\times C\alpha}(M)$) genau dann, wenn $E^c = E$, $F^d = F$ und

$$(b^d)\zeta\chi = (a^c)\xi \tag{34}$$

für alle $a \in A$ und $b \in B$ mit $b\zeta\chi = a\xi$ gilt. Mit anderen Worten: Wenn das Diagramm

$$\begin{array}{rccc}
c\colon & A & \to & A \\
& \xi\downarrow & & \downarrow\xi \\
\bar{c}\colon & A/E & \to & A/E \\
& \chi\updownarrow & & \updownarrow\chi \\
\bar{d}\colon & B/F & \to & B/F \\
& \zeta\uparrow & & \uparrow\zeta \\
d\colon & B & \to & B
\end{array}$$

kommutativ ist.

Beweis: Angenommen es gebe ein solches d. Es ist $E = \mathrm{Stab}_M(\Omega_B)\pi$ (Stabilisatoren seien in diesem Beweis immer punktweise verstanden). Dann ist

$$\begin{aligned}
E^c &= (\mathrm{Stab}_M(\Omega_B)^{(1,c)})\pi = (\mathrm{Stab}_M(\Omega_B)^{(d,c)})\pi \\
&= \{m^{(d,c)} \mid m \in M, \omega^m = \omega \forall \omega \in \Omega_B\}\pi \\
&= \{m \in M^{(d,c)} = M \mid \omega^{((d,c)m(d^{-1},c^{-1}))} = \omega \forall \omega \in \Omega_B\}\pi \\
&= \{m \in M \mid (\omega^{(d,c)})^m = \omega^{(d,c)} \forall \omega \in \Omega_B\}\pi = \{m \in M \mid \omega^m = \omega \forall \omega \in \Omega_B^{(d,c)} = \Omega_B\}\pi \\
&= \mathrm{Stab}_M(\Omega_B)^\pi = E.
\end{aligned}$$

Ebenso folgt $F^d = F$. Ist schließlich $b \in B$ und $a \in A$ mit $b\zeta\chi = a\xi$, also $(b,a) \in M$, so ist $(b^d, a^c) = (b,a)^{(d,c)} \in M^{(d,c)} = M$, womit (34) gezeigt ist.

Die Umkehrung folgt unmittelbar durch Nachrechnen: Ist $(b,a) \in M$, also $b^{\zeta\chi} = a^\xi$, so ist $(b,a)^{(d,c)} = (b^d, a^c)$ aufgrund der Voraussetzung (34) wieder in M, also $M^{(d,c)} = M$. □

II.2.9. Wir betrachten nun nur noch solche $c \in C$, die E normalisieren. Es sei $\bar{\ }$ der natürliche Homomorphismus zur Faktorgruppe $N_C(E)/E$ und

$$\vartheta\colon N_C(E) \to \mathrm{Aut}(A/E), \quad c \mapsto (Ea \mapsto Ea^c)$$

der Homomorphismus, der Elementen die Automorphismen der Faktorgruppe zuordnet.

(35) Bemerkung: Einfache Kriterien für die Fortsetzungsbedingung (34) sind offensichtlich:

1) c ist vom Normalisator $N_{D\beta\times C\alpha}(M)$ induziert (d.h. es gibt ein normalisierendes Element (d,c)).
2) $c\vartheta$ ist innerer Automorphismus.
3) Alle Automorphismen von B/F werden durch Elemente aus D induziert.

Die zweite Bedingung besagt, daß $c\vartheta \in \mathrm{Inn}(A/E)$ liegt. Dies ist äquivalent zu $c \in \mathrm{Kern}\,\vartheta \cdot A$. Dabei ist

$$\begin{aligned}
\mathrm{Kern}\,\vartheta &= \{c \in N_C(E) \mid Ea^c = Ea \text{ für alle } a \in A\} \\
&= \{c \in N_C(E) \mid \bar{c} \in C_{C/E}(A/E)\}
\end{aligned}$$

das volle Urbild des Zentralisators.

II.3. Kranzprodukte

II.3.1. Es sei H eine Gruppe und G eine Gruppe, die transitiv auf Ω operiert. Des weiteren sei $X = H^{\Omega}$ die Menge aller Funktionen von Ω nach H, die mit punktweiser Operation $\omega.(ef) := (\omega.e)(\omega.f)$ zu einer Gruppe wird. Eine Permutationsabbildung $\alpha\colon G \to \mathrm{Aut}(X)$ sei wie folgt definiert: Ist $g \in G$ und $f \in X$, so sei $f^{g\alpha}$ vermöge

$$\omega.f^{g\alpha} = \omega^{g^{-1}}.f$$

definiert. Nachrechnen verifiziert sofort, daß $g\alpha$ Automorphismus und α Homomorphismus ist: Für $\omega \in \Omega$, $g, h \in G$ und $e, f \in X$ ist

$$\begin{aligned}\omega.(ef)^{g\alpha} &= \omega^{g^{-1}}.(ef) = (\omega^{g^{-1}}.e)(\omega^{g^{-1}}.f)\\ &= (\omega.e^{g\alpha})(\omega.f^{g\alpha}) = \omega.(e^{g\alpha}f^{g\alpha}),\end{aligned}$$

sowie

$$\omega.f^{(gh)\alpha} = \omega^{(gh)^{-1}}.f = (\omega^{h^{-1}})^{g^{-1}}.f = \omega^{h^{-1}}.f^{g\alpha} = \omega.f^{(g\alpha h\alpha)}.$$

Das zu α gehörende semidirekte Produkt $W = X \rtimes G$ heißt das *Kranzprodukt* von H mit G und wird mit $H \wr G$ bezeichnet[3]. Die Untergruppe X heißt der *Basisnormalteiler* oder die *Basis* von W, G das *Basiskomplement* (wobei G und X mit ihren Einbettungen in W identifiziert seien).

II.3.2. Operiert G treu auf Ω und H treu auf Δ, so operiert W treu auf $\Delta \times \Omega$: Für $(f,g) \in W$ und $(\delta,\omega) \in \Omega \times \Delta$ setzen wir $(\delta,\omega)^{(f,g)} = (\delta^{\omega.f}, \omega^g)$ (da $\omega.f \in H$ ist dies definiert). Dies ist eine Operation, da

$$\begin{aligned}(\delta,\omega)^{(f,g)(f',g')} &= (\delta,\omega)^{(f(f'^{(g^{-1})\alpha}),gg')} = (\delta^{\omega.f(f'^{(g^{-1})\alpha})}, \omega^{gg'})\\ &= (\delta^{(\omega.f)(\omega.(f'^{(g^{-1})\alpha}))}, \omega^{gg'}) = ((\delta^{\omega.f})^{\omega^g.f'}, (\omega^g)^{g'})\\ &= (\delta^{\omega.f}, \omega^g)^{(f',g')} = \left((\delta,\omega)^{(f,g)}\right)^{(f',g')}\end{aligned}$$

gilt. Treue folgt unmittebar aus der Treue von H und G.

Operieren G und H transitiv, so operiert auch W transitiv aber imprimitiv auf $\Delta \times \Omega$, die Mengen $\mathrm{B}_\omega = \{(\delta,\omega) \mid \delta \in \Delta\}$ bilden als Bahnen des Basisnormalteilers ein Blocksystem.

(36) Bemerkung: Ist $\Delta = \{1,\dots,m\}$ und $\Omega = \{1,\dots,n\}$, so identifizieren wir $\Delta \times \Omega$ mit $\{1,\dots,m\cdot n\}$, indem wir (δ,ω) auf $m(\omega-1)+\delta$ abbilden. Damit ist

$$\{\{1,\dots,m\},\{m+1,\dots,2m\},\dots,\{(n-1)m+1,\dots,nm\}\}$$

das Blocksystem zum Kranzprodukt $H \wr G$.

Im Rahmen der Theorie *primitiver* Gruppen wird manchmal eine weitere Operation des Kranzproduktes, die sogenannte *Produktoperation* (*product action*) benötigt. Diese geschieht auf der Menge Δ^{Ω}, dabei operiert X vermöge $(\delta_1,\dots,\delta_{|\Omega|})^{(h_1,\dots,h_{|\Omega|})} = (\delta_1^{h_1},\dots,\delta_{|\Omega|}^{h_{|\Omega|}})$ (transitiv) auf $\Delta \times \cdots \times \Delta = \Delta^{\Omega}$ und G durch Permutation der direkten

[3] in der russischen Literatur ist die Schreibweise $G \wr H$ üblich

Faktoren. Diese Operation ist folglich transitiv von Grad m^n, verglichen mit Grad $m \cdot n$ der imprimitiven Operation.

II.3.3. Kranzprodukte operieren nicht nur imprimitiv, sondern sind gewissermaßen die „universellen" transitiven imprimitiven Gruppen: Jede imprimitive Permutationsgruppe läßt sich in ein geeignetes Kranzprodukt von gleichem Grad einbetten.

(37) SATZ (M. KRASNER, L. A. KALOUJNINE, [KK1951]): Es sei G eine transitive, imprimitive Permutationsgruppe auf Ω mit Blocksystem $\mathcal{B}$. Außerdem sei $1 \in \mathrm{B} \in \mathcal{B}$ und $U = \mathrm{Stab}_G(\mathrm{B})$ der Blockstabilisator. Die Operation auf den Blöcken sei $\varphi\colon G \to S_{\mathcal{B}}$, die Operation von U auf B sei $\psi\colon U \to S_{\mathrm{B}}$. Dann ist G bei geeigneter Identifikation von $\mathrm{B} \times \mathcal{B}$ mit Ω als Permutationsgruppe Untergruppe des Kranzproduktes $(U\psi) \wr (G\varphi)$. Bei dieser Identifikation bilden $\{\{(b, \mathrm{B}_i) | b \in \mathrm{B}\} \mid \mathrm{B}_i \in \mathcal{B}\}$ die Bahnen des Basisnormalteilers.

Beweis: Ohne Beschränkung der Allgemeinheit identifizieren wir B und $\mathcal{B}$ jeweils mit einem Anfangsstück der natürlichen Zahlen. Es sei $V = \mathrm{Stab}_G(1)$ der Punktstabilisator. Dann gilt $G > U > V$. Es sei $\{s_j \mid 1 \le j \le |\mathcal{B}|\}$ Repräsentantensystem der Nebenklassen $U \backslash G$ und $\{r_i \mid 1 \le i \le |\mathrm{B}|\}$ eines von $V \backslash U$. Dann ist $\{r_i s_j\}$ Repräsentantensystem der Nebenklassen $V \backslash G$. Die Operation auf den Nebenklassen per Rechtsmultiplikation ist äquivalent zu der Operation auf den Punkten. Wir setzen die Punkte (dies entspricht der Umnumerierung) über die Doppelindizes der Nebenklassenvertreter in Bijektion zu der Paarmenge $\{(i, j)\}$ (die $\mathrm{B} \times \mathcal{B}$ entspricht).

Es sei $g \in G$ beliebig dargestellt als $g = kh$ mit $k \in \operatorname{Kern}\varphi$ und Nebenklassenvertreter h. Dann operiert k trivial auf den Nebenklassen $U \backslash G$, es ist $s_j k =: \tilde{k}_j s_j$ mit $\tilde{k}_j \in U$. Außerdem ist $s_j h =: u_j s_{(j^h)}$ mit $u_j \in U$ (wobei $j^h := j^{(h\varphi)}$ die induzierte Operation der Faktorgruppe auf den Blöcken ist). Wir definieren eine Funktion $f_g\colon \{1, \ldots, [G : U]\} \to U$ vermöge $j.f_g := \tilde{k}_j u_j$. Dann ist

$$V r_i s_j k h = V r_i \tilde{k}_j s_j h = V r_i \tilde{k}_j u_j s_{j^h} = V r_i (j.f_g) s_{j^h} = V r_{(i^{j.f_g})} s_{j^h}$$

und es gilt somit

$$(i, j)^g = (i^{j.f_g}, j^h).$$

Dies ist genau die oben definierte Operation des Kranzproduktes. Wir können G also vermöge $g = kh \mapsto f_g h$ operationserhaltend in das Kranzprodukt einbetten. Da es sich in beiden Fällen um Gruppenoperationen handelt ist diese Einbettung ein Gruppenhomomorphismus, der wegen der Treue der Operation injektiv ist. □

Aus diesem Satz erhalten wir nun ohne weitere Mühe den Einbettungssatz für Erweiterungen [Hup1967, Satz I.15.9]:

(38) FOLGERUNG: Ist G eine Gruppe und $N \lhd G$, so gibt es eine Einbettung $G \to N \wr_r (G/N)$ in das reguläre Kranzprodukt.

Beweis: Betrachte die reguläre Permutationsdarstellung von G. Die Bahnen $\{gN = Ng\}$ von N bilden als Bahnen eines Normalteilers ein Blocksystem von G, wobei N der Stabilisator des Blockes $N1$ ist. Die Operation auf den Blöcken ist die reguläre Darstellung von G/N. Also bettet G nach (37) in $N \wr_r (G/N)$ ein. □

Während intransitive Gruppen direkt als subdirekte Produkte beschrieben werden konnten, liefert dieser Satz jedoch nur die Aussage, daß imprimitive Gruppen Untergruppen eines geeigneten Kranzproduktes sind. Die Konstruktion der imprimitiven Gruppen aus primitiveren, die in dieser Arbeit vorgenommen werden soll, wird sich als aufwendiger erweisen und kann sich nicht alleine auf die Konstruktion von Kranzprodukten beschränken.

II.3.4.

(39) SATZ: Es sei $M \leq S_n$ eine intransitive Permutationsgruppe mit Bahnenmenge $\mathcal{B} = \{\mathrm{B}_1, \ldots, \mathrm{B}_m\}$. Es gelte $|\mathrm{B}_1| = |\mathrm{B}_2| = \cdots = |\mathrm{B}_m| = l$. Es sei $\pi_i\colon M \to S_l$ der Konstituentenhomomorphismus in S_{B_i}. Weiterhin gelte für alle i, daß $M\pi_i = A \leq S_l$ eine feste transitive Permutationsgruppe sei. Dann ist $N = N_{S_n}(M) \leq N_{S_l}(A) \wr S_m$, wobei die Punkte des Kranzproduktes so gewählt seien, daß $\mathcal{B}$ ein Blocksystem wird und die Basiskonstituenten jeweils entsprechend der Operation von A operieren.

<u>Beweis:</u> Wir betrachten zunächst den Fall, daß N transitiv auf $\Omega = \{1, \ldots, n\}$ operiert. Die Partition $\mathcal{B}$ bildet als Menge von Bahnen eines Normalteilers ein Blocksystem von N. Es sei $U = \mathrm{Stab}_N(\mathrm{B}_1)$ Blockstabilisator in N und $C = U\pi_1$. Dann ist $M \lhd U$, also $M\pi_1 = A \lhd C$ und damit $C \leq N_{S_l}(A)$.

Die Operation von N auf $\mathcal{B}$ ist andererseits eine Untergruppe von S_m. Nach Satz (37) ist damit N Untergruppe von $C \wr S_m \leq N_{S_l}(A) \wr S_m$.

Operiert N nicht transitiv, so betrachten wir die transitiven Konstituenten, für die nach obigem jeweils eine entsprechende Aussage gilt. Wir können somit N in das direkte Produkt geeigneter Kranzprodukte einbetten, das aber offensichtlich wiederum Untergruppe des vollen Kranzproduktes $N_{S_l}(A) \wr S_m$ ist. □

Eine in vielen Fällen bessere Abschätzung der Obergruppe des Normalisators werden wir in Abschnitt III.4.7 geben.

(40) BEMERKUNG: Satz (39) besitzt eine offensichtliche Verallgemeinerung auf transitive, aber imprimitive Gruppen. Ist $G \leq S_n$ transitiv und $\mathcal{B}$ ein Blocksystem für G, das vom Normalisator auf kein weiteres Blocksystem von G abgebildet werden kann (zum Beispiel weil es bezüglich der Ordnung der Blöcke oder des Isomorphietyps der Operation auf den Blöcken unter allen Blocksystemen von G eindeutig bestimmt ist), so muß der Normalisator von G ebenfalls $\mathcal{B}$ festlassen. Gleichzeitig normalisiert ein Blockstabilisator des Normalisators den entsprechenden Blockstabilisator von G.

Ist also A das Bild der Operation eines Blockstabilisators von G auf seinem Block und C der Normalisator in der entsprechenden symmetrischen Gruppe, so ist (bei passender Einbettung) $N_{S_n}(G) \leq C \wr S_{|\mathcal{B}|}$.

KAPITEL III

Analyse

III.1. Transitive Permutationsgruppen

Wir bezeichnen die Menge der S_n-Klassen von transitiven Gruppen von Grad n mit $\mathfrak{T}_n$, $\mathfrak{R}_n$ sei ein Repräsentantensystem derselben. Weiterhin sei auf den Untergruppen von S_n eine totale Ordnung definiert. Diese induziert bei Auswahl fester Klassenrepräsentanten auch eine Ordnung auf $\mathfrak{T}_n$. Wir wollen $\mathfrak{T}_n$ – die Klassen transitiver Gruppen von Grad n – beschreiben.

III.1.1. Als Grundlage gehen wir davon aus, daß die primitiven Gruppen sowie die transitiven Gruppen von kleinerem Grad bereits klassifiziert sind. Es genügt daher, die imprimitiven Gruppen zu beschreiben. Jede imprimitive Gruppe besitzt ein nichttriviales Blocksystem (im Folgenden werden wir den Zusatz „nichttriviales" nicht mit notieren, Blocksysteme seien – sofern nicht das Gegenteil erlaubt ist – grundsätzlich als nichttrivial angenommen). Wir wollen die Gruppen entsprechend dieser Blocksystem klassifizieren.

Da eine Gruppe mehrere nichttriviale Blocksysteme besitzen kann, ist das erste Ziel, jeder transitiven Permutationsgruppe wenn möglich ein „schönes" Blocksystem zuzuordnen.

Danach werden wir die Struktur einer einzelnen transitiven imprimitiven Gruppe näher untersuchen, und angeben, wie man diese Gruppe aus „kleineren" Bausteinen erhalten kann. In Abschnitt III.3 werden wir dann untersuchen, wie sich Konjugation in der symmetrischen Gruppe auf diese Bausteine auswirkt. Das Ziel wird es dabei sein, die Konjugation in der großen symmetrischen Gruppe auf Konjugation der Bausteine in kleineren Gruppen zurückzuspielen, um aufwendige Konjugationstests zu sparen.

Darauf folgend wollen wir in Abschnitt III.4 eine bessere Beschreibung für eine Sorte von Bausteinen (die Basen der Gruppen) herleiten. Da wir für diese Sorte von Bausteinen bis dahin nur wissen, daß sie in einer sehr großen Klasse liegen (derjenigen der Subpotenzen), wird uns diese Beschreibung helfen, gewisse Kandidaten für Bausteine a priori zu eliminieren, anstatt erst beim Fehlschlag eines Konstruktionsversuchs festzustellen, daß diese Kandidaten de facto doch keine Bausteine sein können.

Der abschließende Abschnitt III.5 dieses Kapitels untersucht schließlich das Zusammenspiel der betrachteten Zerlegung mit weiteren Blocksystemen einer transitiven Gruppe.

III.1.2. Wir betrachten im folgenden eine transitive, imprimitive Gruppe $G \leq S_n$. Weil G transitiv auf $\Omega = \{1, \ldots, n\}$ operiert, ist jedes Blocksystem bereits eindeutig durch denjenigen Block, der 1 enthält, identifiziert. Die 1 enthaltenden Blöcke aller Blocksysteme von G sind bezüglich Inklusion halbgeordnet, wir übertragen diese Halbordnung auf die

Blocksysteme und definieren so *minimale* oder *feinste* Blocksysteme.

(41) DEFINITION: Eine Partition $\mathcal{B}$ von Ω, die ein Blocksystem von G bildet, heißt *zugehörig* zu G, wenn gilt:

Z1 G besitzt kein (nichttriviales) Blocksystem mit Blöcken kleinerer Ordnung.
Z2 Unter allen Blocksystemen von G minimaler Ordnung ist die Ordnung des Stabilisators aller Blöcke (d.h. des Kerns der Darstellung auf den Blöcken) minimal
Z3 Unter allen verbleibenden Blocksystemen ist die Klasse $[(G_B)^B]$ der Operation eines Blockstabilisators auf seinem Block bezüglich der Ordnung auf $\mathfrak{T}_{|\mathcal{B}|}$ minimal.
Z4 Unter allen verbleibenden Blocksystemen ist die Klasse $[T]$ der Operation auf den Blöcken bezüglich der Ordnung auf $\mathfrak{T}_{|\mathcal{B}|}$ minimal.

Ein zugehöriges Blocksystem ist aufgrund der ersten Bedingung stets minimal. Jede imprimitive Gruppe besitzt mindestens ein zugehöriges Blocksystem. Sie kann aber mehrere besitzen:

(42) BEISPIEL: Die KLEINsche Vierergruppe $V_4 = \langle(1,2)(3,4),(1,3)(2,4)\rangle$ besitzt drei Blocksysteme:

$$\{\{1,2\},\{3,4\}\}, \quad \{\{1,3\},\{2,4\}\} \quad \text{und} \quad \{\{1,4\},\{2,3\}\}.$$

Die Kerne der Blockdarstellungen sind jeweils von Ordnung 2, die Blockdarstellungen vom Typ S_2. Alle drei Systeme sind also zugehörig.

Das zugehörige Blocksystem muß nicht notwendigerweise ein „natürliches“ Blocksystem sein:

(43) BEISPIEL: Es sei

$$\begin{aligned} G = V_4 \wr S_4 = \langle &(1,2)(3,4),(1,3)(2,4),(1,13)(2,14)(3,15)(4,16),\\ &(5,9,13)(6,10,14)(7,11,15)(8,12,16)\rangle . \end{aligned}$$

Offenbar besitzt G als Kranzprodukt ein Blocksystem mit Blöcken von Ordnung 4. Zugehörig zu G sind jedoch drei Blocksysteme mit Blöcken von Ordnung 2. Diese stammen von der V_4 wie im vorangegangenen Beispiel (die Blöcke die 1 enthalten sind $\{1,2\}$, $\{1,3\}$ und $\{1,4\}$).

III.1.3. Da wir die imprimitiven Gruppen über ihre Blocksysteme konstruieren wollen, werden wir alle diejenigen Gruppen, die mehrere Blocksysteme besitzen, mehrfach erhalten. Indem wir solche Gruppen nur dann registrieren, wenn das Blocksystem der Gruppe auch zugehörig ist, können wir auf eine Reihe von Konjugationstests verzichten.

Die Bedingungen aus Definition (41) sind dazu so gewählt, daß sie mit möglichst wenig Aufwand überprüft werden können, beziehungsweise schnell eine möglichst große Zahl an Blocksystemen herausfiltern.

Sind einer Gruppe mehrere Blocksysteme zugehörig, so werden wir versuchen, diese anhand weiterer Eigenschaften, wie zum Beispiel des Isomorphietyps der Operation des Blockstabilisators auf seinem Block zu unterscheiden. Indem wir auf diesen Eigenschaften künstlich Ordnungen einführen, können wir die Registrierung auf diejenigen Gruppen beschränken, bei denen diese Eigenschaften minimal sind.

Ein Konjugationstest ist damit nur dann vonnöten, wenn einer Gruppe mehrere „gleichwertige" (die genaue Bedeutung diese Begriffs wird in einzelnen Fällen unterschiedlich sein) Blocksysteme zugehörig sind. In einigen Fällen wird sich von der „Gleichwertigkeit" dann auf Automorphismen der Konstituenten schließen lassen, die letztendlich für die Konjugiertheit verantwortlich sind.

III.2. Struktur einer imprimitiven Gruppe

Nun soll die Struktur einer imprimitiven Gruppe, die mit einem zugehörigen Blocksystem zusammenhängt, näher untersucht werden. G sei weiterhin eine imprimitive Gruppe. Dieser sei das Blocksystem $\mathcal{B} = \{\mathrm{B}_1, \dots, \mathrm{B}_m\}$ zugehörig.

III.2.1. Ohne Beschränkung der Allgemeinheit können wir $1 \in \mathrm{B}_1$ annehmen, des weiteren sei $|\mathrm{B}_1| = l$ und damit $n = lm$.

Wir bezeichnen Punkt- und Blockstabilisator mit $V = \mathrm{Stab}_G(1)$ und $U = \mathrm{Stab}_G(\mathrm{B}_1)$, daher ist $U \geq V$. Außerdem ist $[G : U] = |\mathcal{B}| = m$ und $[U : V] = |\mathrm{B}_1| = l$. Die Operation φ von G auf $\mathcal{B}$ liefert eine Permutationsdarstellung $T := G\varphi$ von G von Grad m, deren Kern M gleich $\bigcap_{g \in G} U^g$ ist. M heißt die *Basis* von G (bezüglich $\mathcal{B}$). Die Darstellung von G auf den Nebenklassen von V ist treu, das heißt, es gilt

$$\bigcap_{g \in G} V^g = \langle 1 \rangle. \tag{44}$$

Da $\mathcal{B}$ minimal bezüglich Inklusion gewählt war, ist V eine maximale Untergruppe von U. Daher ist $\langle M, V \rangle = U$ oder $M \leq V$. Ist letzteres der Fall, so folgt aus (44) sofort, daß $M = \langle 1 \rangle$ gilt.

Fall 1: Aufblasungen

III.2.2. Im letzten Fall ist die Darstellung φ von G treu. Dann ist $T = G\varphi$ eine transitive Permutationsgruppe von Grad $m < n$. Da $T \cong G$ ist, erhält man G (bis auf Konjugation in S_n) durch Operation von T auf den Nebenklassen von $V\varphi =: \tilde{V} \leq T$, welches eine maximale Untergruppe des Punktstabilisators $U\varphi =: \tilde{U} \leq T$ in T von Index l ist. Ein solches G bezeichnen wir als *Aufblasung* von T. Jede maximale Untergruppe von Index l des Punktstabilisators von T definiert eine Aufblasung, die Untergruppe von S_n ist.

Es seien G_1 und G_2 Aufblasungen von T zu den maximalen Untergruppen $\tilde{V}_1$ und $\tilde{V}_2$ des Punktstabilisators von T. Die dazugehörigen (treuen) Permutationsdarstellungen seien mit $\varphi_1 \colon T \to G_1$ und $\varphi_2 \colon T \to G_2$ bezeichnet. Sind G_1 und G_2 in S_n konjugiert, und ist σ ein innerer Automorphismus von S_n, der einem konjugierenden Element entspricht, so ist $\alpha = \varphi_1 \sigma \varphi_2^{-1} \colon T \to T$ ein Automorphismus von T. Da σ nach Lemma (7) den Punktstabilisator von 1 in G_1 auf ein Konjugiertes des Punktstabilisators von 1 in G_2 abbildet, ist $\tilde{V}_1 \alpha = \tilde{V}_2^t$ mit geeignetem $t \in T$. Die Untergruppen $\tilde{V}_1$ und $\tilde{V}_2$ sind also unter der Automorphismengruppe konjugiert.

Umgekehrt induziert ein Automorphismus von T, der zwei Untergruppen des Punktstabilisators aufeinander abbildet, eine Bijektion der Nebenklassen, die dazugehörigen Darstellungen sind damit permutationsisomorph. Insgesamt haben wir also die folgende Aussage:

(45) LEMMA: Die $\mathrm{Aut}(T)$-Konjugiertenklassen maximaler Untergruppen des Punktstabilisators von T stehen in Bijektion zu den S_n-Klassen von Aufblasungen von T.

Damit können wir die Menge aller transitiven Gruppen beschreiben, die als Aufblasung bezüglich zugehöriger Blocksystem erhalten werden: Zu einer Gruppe T sei $\mathfrak{A}_T$ ein Repräsentantensystem der S_n-Klassen von Aufblasungen von T über zugehörige Blocksysteme. Dann gilt:

(46) SATZ:

(47)
$$\mathcal{A} := \bigcup_{1,n\neq m \mid n} \bigcup_{T\in\mathfrak{R}_m} \mathfrak{A}_T$$

ist ein Repräsentantensystem der S_n-Klassen von Gruppen, die als Aufblasung zu Blocksystemen erhalten werden können, die der Gruppe zugehörig sind.

Beweis: Es sei G eine solche Aufblasung. Dann ist $[T]$ wegen Bedingung Z4 minimal, G also zu genau einem Repräsentanten aus $\mathfrak{A}_T$ konjugiert. Konjugiertheit zu mehreren Repräsentanten aus $\mathcal{A}$ widerspräche der Minimalität von $[T]$. □

Wir werden den Prozeß der Konstruktion von Aufblasungen genauer in Abschnitt IV.10 beschreiben.

(48) BEMERKUNG: In der Praxis wird nur eine Minorität der transitiven Gruppen als Aufblasung erhalten, siehe VI.2.

III.2.3. Die Berechnung der vollen Automorphismengruppe von T kann recht aufwendig werden. Dagegen läßt sich der Normalisator $N_{S_m}(T)$, der mit seiner Operation auf T eine Untergruppe von $\mathrm{Aut}(T)$ induziert, meist einfacher bestimmen. Daher soll ein notwendiges Kriterium gegeben werden, wann Automorphismen, die nicht von Normalisator induziert sind, maximale Untergruppen des Punktstabilisators aufeinander abbilden können.

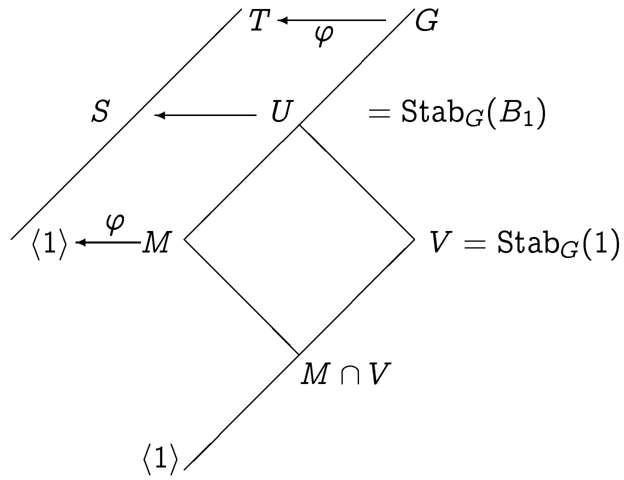
Dazu sei ein $\alpha \in \mathrm{Aut}(T)$ gegeben, das $\tilde{V}_1$ auf $\tilde{V}_2$ abbildet. Ist $\tilde{U}\alpha = \tilde{U}^t$ für ein geeignetes $t \in T$, so wird α nach Lemma (7) durch den Normalisator $N_{S_m}(T)$ induziert.

Ist α nicht vom Normalisator induziert, so ist $\tilde{U}$ nicht in T zu $\tilde{U}\alpha \geq \tilde{V}_1\alpha = \tilde{V}_2$ konjugiert. Die Operation von T auf den Nebenklassen von V_2 besitzt also zwei minimale Blocksysteme mit nicht konjugierten Blockstabilisatoren, so daß die Operation auf den Blöcken jeweils permutationsisomorph zu T ist.

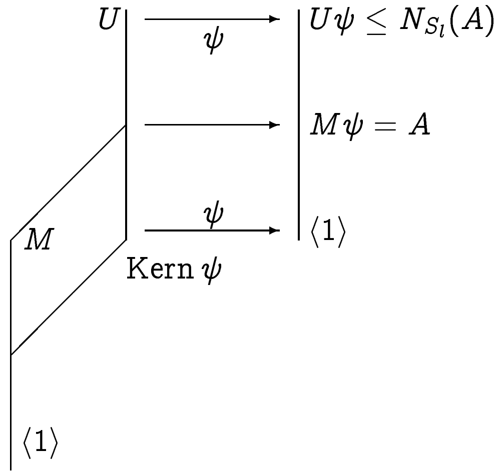
Anstelle die $\mathrm{Aut}(T)$-Klassen maximaler Untergruppen zu bestimmen, genügt es also zunächst, die $N_{S_m}(T)$-Klassen zu ermitteln. Eine weitere Fusion kann nur dann stattfinden, wenn die Aufblasung zwei Blocksysteme mit zu T isomorpher Blockdarstellung und nicht konjugierten Blockstabilisatoren besitzt.

Fall 2: Echte Erweiterung der Blockpermutationsgruppe

III.2.4. Nun wollen wir den Fall eines nichttrivialen M untersuchen. Im folgenden gehen wir daher davon aus, daß $M \neq \langle 1 \rangle$ und damit $\langle M, V \rangle = U$ gilt. Es ergibt sich damit die Situation aus Bild 1.



φ Blockhomomorphismus,



ψ Restriktionshomomorphismus auf B_1.

BILD 1. Struktur von echten Erweiterungen der Blockpermutationsgruppe

Wir bezeichnen den Restriktionshomomorphismus auf B_1 mit $\psi\colon U \to S_l$. Da V maximal in U und U transitiv auf B_1 ist, ist $U\psi$ eine primitive Gruppe. Des weiteren enthält M Repräsentanten für alle Nebenklassen von V in U und operiert somit ebenfalls transitiv auf $\mathrm{B}_1 = 1^U$. Damit ist $A := M\psi$ ein transitiver Normalteiler der primitiven Gruppe $U\psi$, und es gilt:

$$[U\psi : A] = [U\psi : M\psi] \;\Bigg|\; [U : M] = \left|\mathrm{Stab}_{G\varphi}(1)\right|, \tag{49}$$

wobei φ die Darstellung von G auf $\mathcal{B}$ war. Als Kern φ läßt M alle Blöcke aus $\mathcal{B}$ fest. Ist $B' \in \mathcal{B}$ ein weiterer Block, so existiert ein $g \in G$, das B' auf B abbildet, denn G ist transitiv. Damit ist die Operation von M auf B' äquivalent der Operation von M^g auf B. Nun ist aber M normal in G, folglich sind die Operationen von M auf allen Blöcken jeweils permutationsisomorph zu A. M ist somit iteriertes subdirektes Produkt von m Kopien von A, also Untergruppe der direkten Potenz $A^{\times m}$.

(50) Definition: Zur Abkürzung bezeichnen wir ein iteriertes subdirektes Produkt von m Kopien von A als eine *Subpotenz* von A von Länge $m = \operatorname{len} M$.

(51) Bemerkung: Der Fall eines nicht primitiven A kann erstmals bei Grad 16 auftreten: Ist die Blockgröße l kleiner als 4, so sind alle transitiven Untergruppen von S_l primitiv. Der Fall einer imprimitiven transitiven Gruppe tritt erstmals bei $l = 4$ mit $A = V_4$ auf. Die primitive Obergruppe $U\psi$ müsste dann gleich A_4 oder gleich S_4 sein, also wäre $[U\psi : A] \geq 3$. Wäre $A = V_4$ aber gleichzeitig die Blockanzahl m kleiner als 4, so wäre die Ordnung eines Punktstabilisators der transitiven Operation $T = G\varphi$ maximal gleich 2, ein Widerspruch zu (49).

Für $m = 4$ ist für $A = V_4$ die Bedingung (49) allerdings erfüllbar, wenn das Bild $G\varphi$ der Operation gleich A_4 oder S_4 ist. In der Tat gibt es solche Gruppen, zum Beispiel

$$\begin{aligned} G = \ & \langle (1,9,4,10)(2,11,3,12)(5,14,7,15)(6,16,8,13), \\ & (1,9,15,4,11,13)(2,12,16,3,10,14)(5,8,6) \rangle \end{aligned}$$

von Ordnung 384, für die $|G\varphi| = 12$ gilt.

III.2.5. Betrachten wir eine Untergruppe $H \leq G$, die volles Urbild einer minimal transitiven Untergruppe $\hat{T} \leq T$ ist, so ist auch H eine transitive Permutationsgruppe. Die Basis M_H in H zum Blocksystem $\mathcal{B}$ ist

$$M_H = \{h \in H \mid \mathrm{B}^h = \mathrm{B} \text{ für alle } \mathrm{B} \in \mathcal{B}\} = \{h \in H \mid h \in M\}.$$

Als volles Urbild enthält H aber auch die Untergruppe M, folglich ist $M_H = M$.

Wir haben also gesehen, daß H ebenfalls M als Basis zum Blocksystem $\mathcal{B}$ besitzt. Dieses ist nicht notwendigerweise H zugehörig. Geht es jedoch nur um die Analyse von M, so können wir, soweit Zugehörigkeit des Blocksystems nicht eingeht, daher annehmen, daß T minimal transitiv ist.

Zur Warnung sei angemerkt, daß die Tatsache, daß $\mathcal{B}$ der Gruppe H nicht zugehörig sein braucht, zum Beispiel bedeuten kann, daß der Blockstabilisator H_B von H nicht mehr primitiv auf dem Block B operiert. Möchte man daher die Menge der zu betrachtenden Gruppen A mittels (49) einschränken, so sind hierbei *alle* transitiven Gruppen von Grad m als mögliche $G\varphi$ in Erwägung zu ziehen. Es genügt dabei nicht, sich auf die minimal transitiven Gruppen zu beschränken.

Ist A nicht primitiv, so können wir dafür Bedingung (49) dazu benutzen, die Menge der zu betrachtenden $G\varphi$ einzuschränken. Dies bedeutet, daß jedes vorkommende T nicht nur ein minimal transitives $\hat{T}$, sondern sogar eine Untergruppe $\tilde{T} \leq T$ enthalten muß, die minimal mit einem Punktstabilisator ist, dessen Ordnung von $[P : A]$ (mit $P \rhd A$ minimale primitive Obergruppe) geteilt wird. Natürlich enthält $\tilde{T}$ ein minimal transitives $\hat{T}$; die im allgemeinen größere Gruppe $\tilde{T}$ liefert aber bisweilen stärkere Einschränkungen.

III.2.6. Nun betrachten wir den Normalisator N von M in S_n. Dieser enthält G. Nach Satz (39) muß N im Kranzprodukt $W = C \wr S_m$ mit $C = N_{S_l}(A)$ liegen. Da das zur Konstruktion von W gehörige Blocksystem mit $\mathcal{B}$ identisch ist, bezeichnen wir die (fortgesetzte) Operation von ganz W auf $\mathcal{B}$ weiterhin mit φ (genau genommen gilt $\varphi_{\text{alt}} = \varphi_{\text{neu}}|_G$). Wir setzen nun $K := \text{Kern}(\varphi_{(\text{neu})})$ und $R := N\varphi$. Da G transitiv operiert, ist R eine transitive Untergruppe von S_m. Die Basis von G ist M, daher ist $G \cap K = M$. Andererseits ist $S := GK$ eine transitiv operierende Untergruppe. $S\varphi \leq R$ ist also eine auf $\mathcal{B}$ transitive Untergruppe von R und G/M somit Komplement zu K/M in S/M. Bild 2 stellt die Verhältnisse dar.

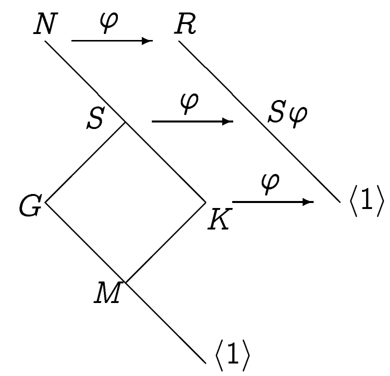


Bild 2. Obergruppen der Subpotenz

Geben wir jetzt umgekehrt eine Subpotenz M von A vor, setzen wiederum $N = N_{S_n}(M)$ und $K := \text{Kern}\,\varphi$ und betrachten eine Zwischengruppe $M \leq G \leq N$ mit $G \cap K = M$ und $G\varphi$ transitiv, so operiert G transitiv auf den Blöcken in $\mathcal{B}$. Damit operiert G auch transitiv auf Ω und besitzt M als Basis zum Blocksystem $\mathcal{B}$. Die transitiven Gruppen, die ein vorgegebenes M als Basis besitzen sind also genau die Urbilder (bezüglich des natürlichen Homomorphismus $N \to N/M$) von Komplementen zu K/M in S/M, wobei S Urbild einer transitiv operierenden Untergruppe von $N\varphi = R$ ist.

III.3. Auswirkung der Konjugation

III.3.1. Wir wollen nun den Einfluß der Konjugation in S_n auf obige Strukturen untersuchen. Dazu seien G und G' zwei in S_n konjugierte transitive Gruppen. Ein konjugierendes Element sei g, es gelte $G'^g = G$. Ist M Kern einer Blockdarstellung von G, so existiert damit eine – konjugierte – Blockdarstellung von G', so daß deren Kern M' in S_n zu M konjugiert ist (man setze $M' := M^{g^{-1}}$ und betrachte die Operation von G' auf den Bahnen von M').

Sind andererseits M und M' konjugiert, so gibt es zu jedem $G' \geq M'$ ein konjugiertes $G \geq M$. Um Repräsentanten der Gruppen zu erhalten, genügt es somit, ein Repräsentantensystem der M zu betrachten.

Wir können uns daher auf den Fall $M = M'$ beschränken. G und G' seien also in S_n konjugierte Untergruppen des Normalisators N, die beide M als Kern eines zugehörigen Blocksystems besitzen.

III.3.2. Zunächst sei angenommen, daß das konjugierende Element g bereits M invariant läßt, das heißt im Normalisator N liegt. (Diesen Fall werden wir später als den häufigsten identifizieren, siehe (177)) In diesem Falle folgt aus der Konjugation von G und G' eine Konjugation der Faktoren G/M und G'/M im Faktor N/M. Da K Normalteiler ist, impliziert dies wiederum, daß die zugehörigen Untergruppen $S/K = GK/K$ und $S'/K = G'K/K$ in N/K konjugiert sind.

Sind umgekehrt S/K und S'/K in $N/K = R$ konjugiert, so sind deren Urbilder S/M und S'/M in N/M konjugiert. Dies impliziert aber wiederum, daß die Menge der Komplementklassen zu K/M in S/M unter N/M zu der Menge der Komplementklassen zu K/M in S'/M konjugiert ist.

Will man nur Repräsentanten modulo Konjugation erhalten, so genügt es folglich, die möglichen S/K nur bis auf R-Konjugation zu bestimmen, dann Repräsentanten der S/M-Klassen von Komplementen in S/M zu K/M zu berechnen und aus diesen (S/M-)Repräsentanten dann Repräsentanten bezüglich der Konjugationsoperation von N/M auszuwählen.

III.3.3. Es verbleibt der Fall, daß das konjugierende Element g nicht im Normalisator N von M in S_n liegt. Da $M \lhd G$, $M \lhd G'$ und $G'^g = G$, ist $\tilde{M} = M^g$ ein weiterer intransitiver Normalteiler von G, dessen Bahnen ein Blocksystem $\mathcal{C}$ von G bilden müssen. Aus der Definition von $\tilde{M}$ folgt unmittelbar $\mathcal{C} = \mathcal{B}^g$.

$$\begin{array}{ccccc} G' & \supset & M & \mathcal{B} & \\ g\downarrow & & \downarrow g & \downarrow & \qquad g \notin N_{S_n}(M) \\ M \subset G & \supset & \tilde{M} & \mathcal{C} & \end{array}$$

Da M Basis von G' bezüglich $\mathcal{B}$ ist, ist $\tilde{M}$ Basis von G bezüglich $\mathcal{C}$. Da $M \neq \tilde{M}$ muß daher auch $\mathcal{B} \neq \mathcal{C}$ gelten. G besitzt also zwei minimale Blocksysteme gleicher Ordnung. Da G und G' permutationsisomorph sind, sind auch die Operationen von G auf $\mathcal{B}$ und $\mathcal{C}$ permutationsisomorph.

In dieser Situation müssen wir also $\tilde{M}$ und M durch Konjugation aufeinander abbilden. Wir wählen daher ein $x \in S_n$, welches $\tilde{M}$ auf M konjugiert. Wir könnten zum Beispiel $x = g^{-1}$ wählen, jedoch ist es im Konstruktionsprozeß später einfacher, lediglich das passende Abbilden von $\tilde{M}$ zu verlangen. Bedingung ist daher lediglich, daß die Nebenklassen $N_{S_n}(\tilde{M})x$ und $N_{S_n}(\tilde{M})g^{-1}$ gleich sind.

Ersetzen wir G durch das Konjugierte G^x, so ist $\tilde{M}^x = M$ Kern eines Blocksystems von G. Ein Element, das G^x auf G' konjugiert, läßt dann M invariant und die Argumentation aus III.3.1 ist anwendbar.

Dieser Fall kann nur eintreten, wenn ein G erhalten wird, dem zwei Blocksysteme zugehörig sind, so daß die entsprechenden Operationen auf den Blöcken permutationsisomorph sind.

III.3.4. Wir fassen die obigen Resultate nun zusammen:

Es sei M eine Subpotenz von A. Auf der Menge der M als Blockstabilisator besitzenden transitiven Gruppen, denen $\mathcal{B}$ zugehörig ist

(52) $$\hat{G}_M = \left\{ G \;\middle|\; M \leq G \leq N, G \cap K = M, G\varphi \text{ transitiv}, \mathcal{B} \text{ zugehörig zu } G \right\}$$

führen wir die folgende Äquivalenzrelation $\triangleq$ ein:

$$
\begin{array}{lll}
G \triangleq G' & \text{wenn} & \\
& & G/M \sim_{N/M} G'/M \\
& \text{oder} & G^x/M \sim_{N/M} G'/M, \text{ mit } x \in S_n, \text{ wobei } M \neq M^{x^{-1}} \lhd G \\
& & \text{Basis eines weiteren zugehörigen Blocksystems von } G \text{ ist.}
\end{array}
$$

Es sei $\mathfrak{G}_M$ ein Repräsentantensystem der $\triangleq$-Klassen aus $\hat{G}_M$. Dann ist wegen III.3.3 $\mathfrak{G}_M$ ebenfalls ein Repräsentantensystem der S_n-Klassen von transitiven Gruppen, die M als Basis eines Blocksystems besitzen.

III.3.5. Mit diesen $\mathfrak{G}_M$ sollen nun die Klassen transitiver Gruppen parametrisiert werden, wobei M ein Repräsentantensystem von $\mathcal{M}$, der Menge von S_n-Klassen von Subpotenzen von A durchläuft. Eine Gruppe G, die mehrere Blocksysteme besitzt, kann aber in mehreren $\mathfrak{G}_M$ liegen. Um dadurch entstehende Duplikate auszuschließen, führen wir eine (willkürliche) totale Anordnung auf $\mathcal{M}$ ein. Schließlich sei

(53) $$\mathcal{M}_G := \left\{ [L] \in \mathcal{M} \;\middle|\; L \text{ ist Basis eines Blocksystems, das } G \text{ zugehörig ist} \right\}.$$

Damit gilt

(54) Satz: Ist

(55) $$\mathcal{G}_M := \left\{ G \in \mathfrak{G}_M \;\middle|\; [M] \text{ ist minimal in } \mathcal{M}_G \right\},$$

so parametrisiert

(56) $$\bigcup_{[M]\in\mathcal{M}} \mathcal{G}_M$$

die S_n-Klassen imprimitiver transitiver Gruppen mit minimalem Blocksystem von Ordnung m, welche nicht wie in III.2.2 durch „Aufblasen" von Gruppen kleineren Grades herrühren.

Beweis: Es sei G transitiv, imprimitiv und nicht als Aufblasung zu erhalten. Wähle unter den Blocksystemen, denen G zugehörig ist, ein solches aus, welches ein minimales $[M]$ liefert. Dann ist G zu genau einem Vertreter aus $\mathfrak{G}_M$ konjugiert (der in $\mathcal{G}_M$ liegt). Zu allen übrigen zugehörigen Blocksystemen von G ist G nicht im entsprechenden $\mathcal{G}_M$ enthalten, da $[M]$ für diese nicht minimal ist.

Umgekehrt sind alle Gruppen aus $\mathcal{G}_M$ nicht als Aufblasung zu einem zugehörigen Blocksystem zu erhalten, da die Zugehörigkeitsbedingung Z2 impliziert, daß es kein Blocksystem gleicher Ordnung mit trivialem (und damit kleinerem als $|M|$) Kern geben kann. □

III.3.6. Als Folgerung erhalten wir nun eine Klassifikation der S_n-Klassen von transitiven Permutationsgruppen:

(57) Satz: Sei G eine transitive Permutationsgruppe von Grad n. Dann erfüllt G genau eine der folgenden Bedingungen:

1. G ist primitiv;
2. G ist zu genau einem $A \in \mathcal{A}$ gemäß Satz 46 konjugiert;
3. G ist zu genau einem $H \in \mathcal{G}_M$ gemäß Satz 54 konjugiert.

Bei Punkt 2. und 3. geht die Zugehörigkeit eines Blocksystems implizit bei den Sätzen 46 und 54 ein.

III.4. Mögliche Basen

Die Analyse der vorangegangenen Abschnitte hat die Klassifikation intransitiver Permutationsgruppen auf eine Klassifikation von deren Basen M zurückgeführt. Von diesen Basen ist bisher nur bekannt, daß sie Subpotenzen einer Gruppe A sind, deren Normalisator $N = N_{S_n}(M)$ transitiv operiert. Letzteres ist eine Einschränkung an die Struktur von M, nicht jede Subpotenz gestattet eine transitive Normalisatoroperation.

Ist nun aber mit M eine (beliebige) Subpotenz von A gegeben, so können wir dieser zunächst nicht einfach (das heißt ohne Berechnung des Normalisators) ansehen, ob deren Normalisator in S_n transitiv operiert. Wir wollen im Folgenden durch Untersuchung der subdirekten Struktur von M ein notwendiges Kriterium für eine transitive Operation von $N = N_{S_n}(M)$ herleiten. Hierfür betrachten wir zunächst beliebige Subpotenzen einer (beliebigen) Gruppe A.

III.4.1. Im Folgenden sei $A \leq S_l$ eine (nicht notwendigerweise transitive) Permutationsgruppe und $C = N_{S_l}(A)$. Die Gruppe M sei eine Subpotenz von A von Länge m, die wir als Untergruppe von $A^{\times m} \lhd C^{\times m}$ ansehen. $C^{\times m}$ sei in natürlicher Weise als intransitive Permutationsgruppe auf Ω gegeben, $\mathcal{B}$ sei eine Partition von Ω in Mengen gleicher Kardinalität, so daß die Projektionen auf die Konstituenten

$$\pi_i\colon \begin{array}{ccc} C^{\times m} & \to & C \\ (c_1, \dots, c_m) & \mapsto & c_i \end{array}$$

auch als Restriktionen auf die i-ten Teilmengen $B_i \in \mathcal{B}$ angesehen werden können.

(58) Definition: Wir nennen die Teilmengen von $\mathcal{B}$ (die Vereinigungen von Bahnen sind) *Komponenten*.

Außerdem sei

$$\mu_i\colon \begin{array}{ccc} C^{\times m} & \to & C^{\times i} \\ (c_1, \dots, c_m) & \mapsto & (c_1, \dots, c_i) \end{array}$$

die Restriktion auf die Vereinigung der ersten i Komponenten.

Im allgemeinen werden wir bei Identifikation von A oder C mit einem der Bilder die dazugehörigen Indexverschiebungen nicht explizit notieren, sofern dies keine Probleme aufwirft.

III.4.2.

(59) Definition: Das Bild $\underset{\overleftarrow{i}}{M} = M\mu_i$ heißt das i-te *Anfangsstück* von M, umgekehrt heißt M *Ergänzung* seiner Anfangsstücke.

(60) Definition: Der Normalteiler

$$M_i := \mathrm{Kern}(\pi_i) \cap M = \{(a_1, \ldots, a_m) \in M \mid a_i = id\}$$

heißt der i-te *Blockkern* von M. Weiterhin sei

$$M_i^j := M_i \pi_j$$

und

$$M^i := \bigcap_{i \neq j} M_j = \{(a_1, \ldots, a_m) \in M \mid a_j = id \text{ für } j \neq i\}.$$

(61) Bemerkung: Der Schnitt M^i operiert nach Definition auf allen Komponenten außer der i-ten trivial. Somit ist $\pi_i|_{M^i}$ injektiv. Außerdem ist

$$M^i \pi_i = \left(\bigcap_{j \neq i} M_j \right) \pi_i \subseteq \bigcap_{j \neq i} M_j \pi_i = \bigcap_{j \neq i} M_j^i \tag{62}$$

(63) Bemerkung: Es seien $1 \leq i < j \leq m$. Das Bild von M unter der Restriktion

$$\varpi := (\pi_i, \pi_j) \colon \begin{array}{ccc} C^{\times m} & \to & C \times C \\ (c_1, \ldots, c_m) & \mapsto & (c_i, c_j) \end{array}$$

auf die Vereinigung der i-ten und j-ten Komponente ist subdirektes Produkt von A mit A zu den Normalteilern M_i^j und M_j^i.

<u>Beweis:</u> Es seien $\tilde{\pi}_1 \colon C \times C \to C$ die Restriktion auf die erste und $\tilde{\pi}_2 \colon C \times C \to C$ die Restriktion auf die zweite Komponente von $C \times C$. Dann ist $\varpi\tilde{\pi}_1 = \pi_i$ und $\varpi\tilde{\pi}_2 = \pi_j$. Nach II.2.1 ist $M\varpi$ subdirektes Produkt von $M\varpi\tilde{\pi}_1 = A$ und $M\varpi\tilde{\pi}_2 = A$ zu den Normalteilern $\{m\varpi\tilde{\pi}_1 = m\pi_i \mid 1 = m\varpi\tilde{\pi}_2 = m\pi_j\} = M_j^i$ und M_i^j. □

Aus Lemma (15) folgt dann:

(64) Folgerung: $A/M_i^j \cong A/M_j^i$

III.4.3. Für $i \leq j$ ist (bei Identifikation von $C^{\times j}$ als Teilmenge von $C^{\times m}$) $\mu_j \pi_i = \pi_i$. Dies gestattet, die Blockkernprojektionen von M mit denen eines Anfangsstücks zu vergleichen:

(65) Lemma: Für $i, j \leq k \leq m$ ist $M_i^j = {\underleftarrow{M}_k}_i^j$.

<u>Beweis:</u>

$$\begin{aligned} M_i^j &= \{m\pi_j \mid m \in M, m\pi_i = 1\} \\ &= \{m\mu_k\pi_j \mid m\mu_k \in M\mu_k = \underleftarrow{M}_k, m\mu_k\pi_i = 1\} \\ &= \{m\pi_j \mid m \in \underleftarrow{M}_k, m\pi_i = 1\} = {\underleftarrow{M}_k}_i^j \end{aligned}$$

□

(66) Lemma: Betrachten wir M als subdirektes Produkt von $\underleftarrow{M}_{m-1}$ mit A zu Normalteilern $F \lhd \underleftarrow{M}_{m-1}$ und $E \lhd A$, so ist $F = M_m \mu_{m-1}$ und $E = \left(\bigcap_{i<m} M_i\right) \pi_m = M^m \pi_m$.

Beweis: Folgt unmittelbar aus (21). □

III.4.4. Nun sei $SB := C \wr S_m = C^{\times m} \rtimes S_m$ und $N := N_{SB}(M)$ der Normalisator von M in SB. (Ist A transitiv, so ist nach Satz (39) $N = N_{S_n}(M)$.) Dieser muß die Komponenten aus $\mathcal{B}$ permutieren, es sei $\varphi\colon N \to R \leq S_{\mathcal{B}}$ der entsprechende Homomorphismus. Indem wir die Teilmengen aus $\mathcal{B}$ durchnumerieren sei $S_{\mathcal{B}}$ mit $S_{|\mathcal{B}|}$ identifiziert.

Wir wollen eine Operation von R auf den M_i definieren:

(67) Lemma: Es sei $g \in N$ gegeben[1] mit $j^{g\varphi} = i$. Der von g induzierte Automorphismus von M sei mit θ bezeichnet. Dann gilt: Es gibt ein $\alpha \in \mathrm{Aut}(A)$, so daß

$$\theta\pi_i = \pi_j\alpha = \pi_{\left(i^{(g^{-1}\varphi)}\right)}\alpha, \tag{68}$$

wobei α von einem Element aus $C = N_{S_l}(A)$ per Konjugation induziert ist.

Beweis: Da $N \leq SB$ ist, können wir g als Produkt $g = rc$ darstellen mit $c = (c_1, \dots, c_m)$, $c_i \in C$ und r die Komponenten wie $g\varphi$ permutierend. Für $m \in M$ gilt dann:

$$m\theta\pi_i = (c^{-1}r^{-1}mrc)\pi_i = ((m^r)^c)\,\pi_i = ((m^r)\pi_i)^{(c\pi_i)} = (m\pi_j)^{c_i} = m\pi_j\alpha,$$

wobei α der innere Automorphismus von C zu c_i sei. □

(69) Folgerung: Für $g \in N$ ist $(M_k)^g\,\pi_i = M_k^{\left(i^{(g^{-1}\varphi)}\right)}\alpha$, mit α induziert durch Konjugation mit $c \in C$.

(70) Lemma: Für $g \in N$ ist

$$(M_i)^g = M_{\left(i^{(g\varphi)}\right)}$$

und

$$(M^i)^g = M^{\left(i^{(g\varphi)}\right)}$$

Beweis: Es ist

$$M_i{}^g = \{m^g \mid m \in M, m\pi_i = 1\} = \{m \in M \mid (m^{g^{-1}})\pi_i = 1\}.$$

Aus (68) folgt nun aber durch Inversion, daß $m^{g^{-1}}\pi_i = m\pi_{\left(i^{(g\varphi)}\right)}\alpha^{-1}$ gilt, wobei α wiederum durch C induziert ist. Also ist

$$M_i{}^g = \{m \in M \mid m(\pi_{\left(i^{(g\varphi)}\right)}) = 1\alpha = 1\} = M_{\left(i^{(g\varphi)}\right)}.$$

Da $g\varphi$ die Komponenten permutiert, folgt die zweite Aussage unmittelbar durch Schnittbildung. □

---

[1] Da n bereits den Grad angibt, kann das Normalisatorelement nicht auch so heißen.

Für $r \in R$ sind daher die Operationen

(71) $$(M_i)^r := (M_i)^g = M_{(i^r)}, \qquad (M^i)^r := (M^i)^g = M^{(i^r)}$$

mit $g\varphi = r$ wohldefiniert und Gruppenisomorphismen.

(72) FOLGERUNG: Operiert $N = N_{SB}(M)$ *transitiv* auf $\mathcal{B}$, so operiert R *transitiv* mittels Permutationsisomorphismen auf der Menge der M_i sowie der Menge der M^i.

III.4.5. Wir wollen nun den Einfluß dieser Operation auf die M_i^j untersuchen. Nach (69) liefert die Operation mit $g \in N$ möglicherweise von Elementen von C induzierte Automorphismen α. Wir betrachten daher Klassen $[E]$ von Normalteilern von A die durch

$$[E] = [F] :\Leftrightarrow A/E \cong A/F$$

definiert seien. Diese Klassen umfassen offenbar die C-Klassen.

(73) BEMERKUNG: Eine (schwächere) Äquivalenz ist durch

$$[[E]] = [[F]] :\Leftrightarrow |E| = |F|$$

gegeben. Offenbar impliziert $[E] = [F]$, daß $[[E]] = [[F]]$ gilt. Sämtliche folgende Aussagen bleiben gültig, wenn man $[\cdot]$ durch $[[\cdot]]$ ersetzt, was in der Praxis einfacher zu testen ist, da es keinen Isomorphietest benötigt.

Nach (64) ist dann

(74) $$[M_i^j] = [M_j^i]$$

Aus (69) und (70) folgt außerdem für $r \in R$ mit $g\varphi = r$:

$$M_{i^r}^j = M_{i^r}\pi_j = (M_i)^g\pi_j = M_i^{j^{r^{-1}}}\alpha$$

und damit, da $\alpha \in \mathrm{Aut}(A)$ und somit $A/M_i^j \cong A/M_i^{j r^{-1}}$

(75) $$[M_i^j] = [M_{i^r}^{j^r}].$$

Bildet r die i-te Komponente auf i'-te Komponente ab, so bildet es dabei die jeweils verbleibenden Komponenten aufeinander ab. Damit erhalten wir unmittelbar:

(76) SATZ (Transitivitätskriterium 1): Ist R *transitiv* auf $\{1, \ldots, m\}$, dann gilt für $1 \leq i, j \leq m$:

$$\{[M_i^k] \mid k \neq i\} = \{[M_j^k] \mid k \neq j\}.$$

Mit anderen Worten: eine Subpotenz M kann nur dann einen transitiv operierenden Normalisator besitzen, wenn in der symmetrischen Matrix $\left([M_i^j]\right)_{i,j}$ jeder Eintrag $[E]$ in jeder Zeile mit gleicher Vielfachheit auftritt:

$$\forall E \lhd A \quad \exists e \in \mathbb{N}_0 : \quad \forall 1 \leq i \leq m : \quad \left|\{j \mid M_i^j = [E]\}\right| = e$$

III.4.6. Es sei $Vkl(M) := \{[M_i^j] \mid 1 \leq i, j \leq m\}$ die Menge der in M vorkommenden Kernklassen. Zu $K \in Vkl(M)$ sei eine Relation $\sim_K$ auf $\{1, \ldots, m\}$ durch

$$i \sim_K j :\Leftrightarrow [M_i^j] = K$$

definiert. Diese Relation ist nach (64) symmetrisch und trivialerweise reflexiv. Der transitive Abschluß, den wir im folgenden ebenfalls mit $\sim_K$ bezeichnen werden, ist daher eine Äquivalenzrelation. Wegen (75) ist diese Relation unter der Operation von R invariant und es gilt somit:

(77) Lemma: Die $\sim_K$-Klassen bilden ein Blocksystem für die Operation von R auf der Punktmenge $\{1, \ldots, m\}$.

(78) Folgerung (Transitivitätskriterium 2): Operiert R transitiv, so müssen alle $\sim_K$-Klassen von gleicher Ordnung sein.

III.4.7. Unter Verwendung dieser Sätze und Lemmata können wir nun die Abschätzung der Obergruppe des Normalisators in Satz (39) verbessern. Die entsprechenden Überlegungen werden später bei der Normalisatorberechnung benutzt; sind aber für die Analyse transitiver Gruppen entbehrlich. Beim ersten Lesen mag man daher zunächst den folgenden Einschub (der argumentationshalber an diese Stelle gehört) überspringen, und mit III.4.9 fortfahren.

Die Voraussetzungen seien wie in Satz (39) gegeben; das heißt, es sei $M \leq S_n$ eine intransitive Permutationsgruppe mit Bahnen $\mathcal{B} = \{B_1, \ldots, B_m\}$. Es gelte $|B_1| = |B_2| = \cdots = |B_m| = l$. Die Konstituentenhomomorphismen in die symmetrische Gruppe auf B_i seien $\pi_i \colon M \to S_l$, und es gelte für alle i, daß $M\pi_i = A \leq S_l$ eine feste transitive Permutationsgruppe sei. Bestimmt werden soll der Normalisator $N = N_{S_n}(M)$.

Wir fassen M und N bereits (bei geeigneter Umnumerierung der Punkte) als Untergruppe von $W = N_{S_l}(A) \wr S_m$ auf. Unter Verwendung des Transitivitätskriteriums (76) können wir nun Transitivitätsbereiche für die Operation des Normalisators $N = N_{S_n}(M)$ auf $\mathcal{B}$ bestimmen:

Zunächst einmal gestattet das Kriterium, zu untersuchen, ob N auf ganz $\mathcal{B}$ transitiv operiert; beziehungsweise äquivalent: ob $N\varphi$ auf $\{1, \ldots, m\}$ transitiv operiert. Ist dies nicht der Fall, so wählen wir eine Teilmenge $\mathcal{C} \subset \mathcal{B}$ aus. Wäre N auf $\mathcal{C}$ transitiv, so gäbe es eine Restriktion ψ von N auf die Vereinigung von $\mathcal{C}$. Das Bild $N\psi$ dieser Restriktion besäße die Restriktion $M\psi$ von M als Kern einer Blockdarstellung. Da auch $M\psi$ Subpotenz ist müßte Satz (76) hierfür ein positives Ergebnis liefern. Die Matrix für $M\psi$ erhält man aber (der Beweis ist analog dem von Lemma (65)) als Minor der Matrix für M, wenn man nur die Einträge auswählt, deren Indizes Mengen aus $\mathcal{C}$ (als Teilmenge von $\mathcal{B}$) entsprechen. Anhand der Matrix für M ist daher testbar, ob N transitiv auf $\mathcal{C}$ operieren könnte.

Um nun letztendlich Transitivitätsbereiche für die Operation von N auf $\mathcal{B}$ zu bestimmen, testet man alle $\mathcal{C}$ in Reihenfolge absteigender Kardinalität, bis jeweils eine transitive Operation nicht mehr ausgeschlossen werden kann.

Mit solchen Überlegungen können wir die Faktorgruppe S_m oft bereits durch ein direktes Produkt $S_{m_1} \times \cdots \times S_{m_z}$ ersetzen, was gleichbedeutend mit der Ersetzung von W

durch das direkte Produkt

$$W_1 \times \cdots \times W_z = N_{S_l}(A) \wr S_{m_1} \times \cdots \times N_{S_l}(A) \wr S_{m_z} \tag{79}$$

ist.

III.4.8. Nun betrachten wir die Restriktionen auf die von einem W_i bewegten Komponenten. N_i sei das Bild des Normalisators N unter dieser Restriktion. Für die Restriktion von M auf diese Komponenten bestimmen wir dann die Äquivalenzklassen $\sim_K$ aus III.4.6. Sind zu einem K die $\sim_K$-Klassen nicht von gleicher Ordnung, so folgt aus (78), daß N_i nicht transitiv auf diesen Komponenten operieren kann, was dieses W_i erneut wie oben in ein direktes Produkt aufspaltet.

Ist dies nicht der Fall, und existieren nichttriviale $\sim_K$-Klassen, so operiert N_i imprimitiv auf den Blöcken und ist daher nicht nur Untergruppe von W_i, sondern bereits von einem geeigneten – erheblich kleineren – iterierten Kranzprodukt $\tilde{W}_i = N_{S_l}(A) \wr (S_a \wr S_b)$ mit $m_i = ab$. Damit kann W_i in (79) durch $\tilde{W}_i$ ersetzt werden. Dies liefert eine kleinere Obergruppe des Normalisators, was wiederum die übliche Backtrack-Suche nach dem Normalisator beschleunigt.

Operiert N_i primitiv, so können wir W_i nicht verkleinern, doch besteht dann die Hoffnung, daß die Operation von N_i auf den Blöcken als primitive Gruppe verhältnismäßig groß ist (was zumindestens für nicht prime m_i zutrifft). Die Backtracksuche sollte daher recht schnell Normalisatorelemente finden, und damit automatisch selbst den Suchbaum beschränken.

III.4.9. Wir kehren zur Analyse von Subpotenzen zurück und vergessen die zusätzlichen Voraussetzungen aus III.4.7 wieder. Um die Zählargumente, die zur Anwendung von Satz (76) benötigt werden, vereinfachen zu können, sollen nun Objekte definiert werden, die im wesentlichen nur Häufigkeiten zählen. Als Vorbild dienen dabei Divisoren, die in der Zahlentheorie Bewertungen zusammenfassen.

(80) Definition: Es sei $\mathcal{N}$ die Menge der Klassen von Normalteilern von A mit isomorpher Faktorgruppe:

$$\mathcal{N} = \left\{ [E] \mid A/E \cong A/E' \text{ für alle } E' \in [E] \right\}$$

und $\mathcal{S}$ die freie abelsche Gruppe auf $\mathcal{N}$, die wir multiplikativ schreiben. Für das Element $s = \prod_{[E]\in\mathcal{N}} [E]^{a_E} \in \mathcal{S}$ sei $\deg(s) = \sum a_E$ der *Grad* von s. Ist $a_E \geq 0$ für alle $[E] \in \mathcal{N}$, so heißt s eine *Signatur*. Signaturen von Grad 1 (also im Prinzip Klassen aus $\mathcal{N}$) heißen *Primsignaturen*.

Sind $s, t \in \mathcal{S}$, so daß s/t eine Signatur ist, so sagen wir, daß s von t geteilt wird: $t \mid s$. Des weiteren seien für $s = \prod [E]^{s_E}$ und $t = \prod [E]^{t_E}$ der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache als

$$\operatorname{ggT}(s,t) = \prod_{[E]\in\mathcal{N}} [E]^{\min(s_E,t_E)}, \qquad \operatorname{kgV}(s,t) = \prod_{[E]\in\mathcal{N}} [E]^{\max(s_E,t_E)}$$

definiert. Diese erfüllen die von ggT und kgV aus der Zahlentheorie bekannten Eigenschaften, wie man leicht mittels der Abbildung $\prod [E]^{s_E} \mapsto \prod p_E^{s_E}$ sieht, wobei jedem $[E]$ eindeutig eine Primzahl p_E zugeordnet sei.

(81) Definition: Für $1 \leq i \leq m$, eine Subpotenz M von A von Länge m und $[E] \in \mathcal{N}$ sei a_E die Anzahl der $1 \leq j \leq m$, für die $[M_i^j] = [E]$ gilt. Dann heißt $\operatorname{sign}_i(M) = \prod_{[E]\in\mathcal{N}}[E]^{a_E}$ die i-te Signatur von M.

Offenbar ist $\deg(\operatorname{sign}_i(M)) = \operatorname{len}(M)$, da jede Komponente genau 1 zum Grad der Signatur beiträgt. Die Aussage aus (65) übersetzt sich damit zu:

(82) Lemma: Ist $i \leq M$ und $\underset{i}{\underleftarrow{M}}$ das i-te Anfangsstück von M, so gilt für alle $j \leq i$:

$$\operatorname{sign}_j(\underset{i}{\underleftarrow{M}}) \,\Big|\, \operatorname{sign}_j(M)$$

(83) Definition: Ist $\operatorname{sign}_i(M) = s \in \mathcal{S}$ für alle $1 \leq i \leq m$, so heißt M in *Parität* und $\operatorname{sign}(M) := s$ die Signatur von M.

Aus (76) folgt dann:

(84) Lemma: Operiert N transitiv auf $\mathcal{B}$, so ist M in Parität.

Da der Normalisator der Basis einer transitiven Gruppe offenbar transitiv auf den durch die Bahnen der Basis gegebenen Komponenten operiert, ist dies insbesondere auch eine notwendige Bedingung dafür, daß eine Subpotenz Basis einer transitiven Gruppe sein kann.

Zusätzlich erhalten wir ein Kriterium, ob eine Subpotenz M Anfangsstück einer Basis einer transitiven Gruppe sein kann:

(85) Satz (Anfangsstückkriterium 1): Es sei M eine Subpotenz von Länge i. Es sei

$$d = \deg(\operatorname{kgV}_{1\leq j\leq i}(\operatorname{sign}_j(M)).$$

Wenn ein transitives imprimitives G mit Basis $\tilde{M}$ existiert, so daß M gleich dem i-ten Anfangsstück $\underset{i}{\underleftarrow{\tilde{M}}}$ ist, so gilt:

$$\operatorname{kgV}_{1\leq j\leq i}(\operatorname{sign}_j(M)) \,\Big|\, \operatorname{sign}(\tilde{M})$$

und somit auch $d \leq \operatorname{len}(\tilde{M})$.

Beweis: Nach Lemma (84) ist $\tilde{M}$ in Parität. Wegen (82) teilt jedes der $\operatorname{sign}_j(M)$ die Signatur $\operatorname{sign}(\tilde{M})$, also teilt auch deren kgV die Signatur. Da $\operatorname{len}(\tilde{M}) = \deg(\operatorname{sign}(\tilde{M}))$ gilt, folgt die Behauptung. □

III.5. Operation der Faktorgruppe auf den Projektionen

Wir kehren nun zurück zur Situation aus III.2.1: G ist eine transitive Permutationsgruppe mit zugehörigem Blocksystem $\mathcal{B}$. Der Blockhomomorphismus ist $\varphi\colon G \to S_m$, sei Bild sei $T := G\varphi$. Der Kern von φ sei M, M ist also Basis von G zu $\mathcal{B}$. Da $G \leq N_{S_n}(M)$ können wir die Aussagen aus (67) übertragen.

Nachdem wir im vorangegangenen Abschnitt mit Lemma (77) ein Kriterium hergeleitet haben, das bei vorgegebenem M eine imprimitive Operation des Normalisators von M auf $\mathcal{B}$ impliziert, wollen wir jetzt den Spieß umdrehen und untersuchen, inwieweit die Imprimitivität der Faktorgruppe T die Struktur des Kerns M beeinflußt. Dabei sei darauf hingewiesen, daß für Zwecke der Analyse von M der Faktor T nach III.2.5 als minimal transitiv angenommen werden kann. Dementsprechend wird der Fall eines imprimitiven T recht häufig eintreten.

III.5.1. Zunächst soll die Aussage von Lemma (67) auf mehrfache Projektionen erweitert werden. Dazu sei $I = \{i_1, \ldots, i_k\} \subset \{1, \ldots, m\}$ eine Indexmenge und

$$\Pi_I = (\pi_{i_1}, \ldots, \pi_{i_k}) = (\pi_i)_{i \in I} \colon M \to C^{\times |I|}$$

die Restriktion auf die durch I indizierten Komponenten. Nun sei $g \in N_{S_n}(M)$ gegeben, der innere Automorphismus zu g sei mit θ bezeichnet. Gemäß (68) sei $\alpha_i \in \mathrm{Inn}(C)$ durch

$$\theta \pi_i = \pi_{\left(i^{(g^{-1}\varphi)}\right)} \alpha_i$$

definiert. Schließlich setzen wir für $i \in I$:

$$\hat{\alpha}_i := \alpha_{\left(i^{(g\varphi)}\right)}$$

und wenn i das j-te Element aus I ist:

$$\tilde{\alpha}_j := \hat{\alpha}_i.$$

Dann ist nach (68) für $m \in M$:

$$\begin{aligned}
(m^g)\Pi_{(I^{g\varphi})} &= (m\theta)\Pi_{(I^{g\varphi})} = (m\theta\pi_i)_{i \in I^{g\varphi}} = m(\pi_{i^{(g^{-1}\varphi)}}\alpha_i)_{i \in I^{g\varphi}} \\
&= m(\pi_i \alpha_{\left(i^{(g\varphi)}\right)})_{i \in I^{g\varphi}} \\
&= m(\pi_i \hat{\alpha}_i)_{i \in I} = m\Pi_I(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k),
\end{aligned}$$

Also ist $M\Pi_I\bar{\alpha} = (M^g)\Pi_{(I^{g\varphi})} = M\Pi_{(I^{g\varphi})}$, wobei $\bar{\alpha} = (\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k)$ Permutationsautomorphismus von $C^{\times |I|}$ ist. Mit anderen Worten:

(86) Lemma: Ist $g \in N_{S_n}(M)$, so ist die Restriktion von M auf die durch I indizierten Komponenten permutationsisomorph zur Restriktion von M auf die durch $I^{g\varphi}$ indizierten Komponenten.

III.5.2. Besitzt $T = G\varphi$ ein nichttriviales Blocksystem $\mathcal{C}$, so werden die Blöcke von $\mathcal{C}$ durch T untereinander permutiert. Für jeden Block $\Gamma \in \mathcal{C}$ ist die Restriktion von M auf die durch Γ indizierten Komponenten demnach vom gleichen Permutationsisomorphietyp. Folglich gilt:

(87) Satz: Besitzt $G\varphi$ ein nichttriviales Blocksystem mit $\frac{m}{k}$ Blöcken von Ordnung k, so ist M Subpotenz von $\frac{m}{k}$ Kopien einer Gruppe Y, die ihrerseits Subpotenz von k Kopien von A ist.

Beweis: Ist Γ Block, so setze $Y := M\Pi_\Gamma$. Die Bilder von Γ schöpfen $\{1, \ldots, m\}$ disjunkt aus. $\square$

(88) Definition: Ist M Subpotenz von Y, wobei Y wiederum Subpotenz von A von Länge k ist, so bezeichnen wir M als *verschachtelte Subpotenz* oder *Verschachtelung* von A von der Stufe k.

In (41) hatten wir die Betrachtungen auf Blocksysteme mit minimalen Blöcken eingeschränkt. Ist M verschachtelte Subpotenz, so entspricht dies gröberen Blocksystemen von G. Aus obigem Satz folgt unmittelbar:

(89) COROLLAR: Besitzen alle minimal transitiven Gruppen von Grad m ein nichttriviales Blocksystem (dessen Blöcke eine Ordnung aus $O \subset \{2, \ldots, \lfloor m/2 \rfloor\}$ haben), so sind alle möglichen Blockkerne aus m Komponenten als verschachtelte Subpotenzen von Stufen $o \in O$ darstellbar.

III.5.3. Leider gilt keine Umkehrung von Satz (87) wie das folgende Beispiel zeigt. Man kann im allgemeinen daraus, daß M verschachtelte Subpotenz ist, nicht schließen, daß eine M normalisierende Gruppe imprimitiv auf den Blöcken operieren muß.

(90) BEISPIEL: Es sei $M = \langle (1,2)(3,4)(5,6)(7,8) \rangle$. Dann ist M Subpotenz von $\langle (1,2)(3,4) \rangle$ welches selbst Subpotenz von $\langle (1,2) \rangle$ ist. M ist also verschachtelte Subpotenz. Andererseits operiert (da M auch bezüglich anderer Partitionierung der Komponenten als verschachtelte Subpotenz erhältlich ist) der Normalisator von M als symmetrische Gruppe auf den Komponenten und ist somit primitiv.

Einem gegebenen M kann daher nicht anhand normalisierender Obergruppen angesehen werden, ob es verschachtelte Subpotenz ist. Es gilt lediglich die offensichtliche Beobachtung:

(91) BEMERKUNG: Ist $\{I_1, \ldots, I_{\frac{m}{k}}\}$ eine Partitionierung von $\{1, \ldots, m\}$ mit $|I_j| = k$ und sind für alle i und j die Restriktionen $M\Pi_{I_i}$ und $M\Pi_{I_j}$ permutationsisomorph, so ist M verschachtelte Subpotenz.

III.5.4. Blocksysteme der Faktorgruppe $T = G\varphi$ entsprechen Untergruppen von T, die oberhalb des Punktstabilisators $T_1 \leq T$ liegen. Dieser ist jedoch das Bild des Blockstabilisators G_B in G unter der Blockoperation φ. Untergruppen von G, die oberhalb G_B liegen, entsprechen aber wiederum Blocksystemen von G, die gröber als $\mathcal{B}$ sind. Mit anderen Worten: Blocksysteme von T entsprechen Blocksystemen von G, die gröber als $\mathcal{B}$ sind.

Anstelle Verschachtelungen zu betrachten, könnten wir daher auch einfach größere Blocksysteme als $\mathcal{B}$ wählen. In diesem Fall ist die Operation eines Blockstabilisators auf seinem Block aber nicht mehr primitiv, der Kern der Blockoperation operiert nicht notwendigerweise transitiv auf den Blöcken:

(92) BEISPIEL: Es sei

$$\begin{aligned} G = \; & \langle (1,11,16,6)(2,12,15,5)(3,10,14,7)(4,9,13,8), \\ & (1,3,2,4)(5,16,6,15)(7,13,8,14)(9,11,10,12) \rangle \end{aligned}$$

eine transitive Gruppe von Grad 16 und Ordnung 48. Die Partitionen

$$\{\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{9,10\},\{11,12\},\{13,14\},\{15,16\}\}$$

und

$$\{\{1,2,3,4\},\{5,6,7,8\},\{9,10,11,12\},\{13,14,15,16\}\}$$

bilden (neben anderen) Blocksysteme von G. Die zweite angegebene Partition ist also kein minimales Blocksystem für G. Die Gruppe G operiert auf den Blöcken dieser Partition jedoch als volle symmetrische Gruppe, die Faktorgruppe $G\varphi$ hat also Ordnung 24. Der Kern M hat also Ordnung 2 und kann daher nicht transitiv auf den Blöcken von Ordnung 4 operieren.

Dies würde die Konstruktion der möglichen M erschweren, da auch Subpotenzen intransitiver Gruppen berücksichtigt werden müssten. (Wie wir hier sehen, sind diese intransitiven Gruppen aber wiederum Subpotenzen.)

Statt dessen werden wir mögliche gröbere Blocksysteme dadurch berücksichtigen, daß wir den Kern zu einem feineren Blocksystem als Verschachtelung auffassen und entsprechend konstruieren werden. Dies schränkt die Anzahl der zu konstruierenden Subpotenzen merklich ein.

Schließlich beachten wir, daß in einer transitiven Gruppe ein Blockstabilisator transitiv auf seinem Block operiert:

(93) BEMERKUNG: Es sei m derart gegeben, daß nach (89) jede Subpotenz, die Kern einer transitiven Gruppe ist, als Verschachtelung erhalten werden kann. Die Gruppe M sei eine solche Verschachtelung, sei also Subpotenz von Y, welches seinerseits wieder Subpotenz von A ist. Dann ist auch Y Basis einer transitiven Gruppe (von entsprechend kleinerem Grad).

Beweis: Nach (89) ist Y Bild der Restriktion von M auf die durch ein Blocksystem der Faktorgruppe angegebenen Komponenten. Betrachte einen entsprechenden Blockstabilisator in der Faktorgruppe und betrachte dessen vollständiges Urbild $Q > M$. Dann ist M weiterhin Kern der (nicht mehr transitiven) Darstellung von Q auf $\mathcal{B}$. Projizieren wir nun auf den Block, so erhalten wir aus Q eine transitive Gruppe, aus M das Bild Y. $\square$

KAPITEL IV

Konstruktion

IV.1. Kanonische Repräsentanten

Im vorangegangenen Kapitel wurde die Struktur transitiver Permutationsgruppen beschrieben. Wir wollen die dabei gewonnenen Erkenntnisse jetzt dazu verwenden, ein Repräsentantensystem der transitiven Gruppen eines gegebenen Grades n zu erhalten. Während wir die primitiven Gruppen dabei als gegeben ansehen dürfen, werden wir die imprimitiven Gruppen gemäß Satz (57) entsprechend der Größen zugehöriger Blocksysteme konstruieren. Die Konstruktion von Aufblasungen stellt dabei kaum Probleme dar, siehe IV.10. Um die übrigen Gruppen zu erhalten, werden gemäß Satz (54) zunächst Repräsentanten ihrer Kerne M konstruiert. Diese sind nach III.2.4 Subpotenzen einer Gruppe A, die transitiver Normalteiler einer primitiven Gruppe von Grad l ist. Entsprechend dieser Definition werden sie als iterierte subdirekte Produkte konstruiert, siehe IV.3.

Die Hauptschwierigkeit dabei besteht darin, die Elimination von konjugierten Gruppen bereits in den Konstruktionsprozeß aufzunehmen und wenn möglich lediglich ein Repräsentantensystem von Konjugiertenklassen zu konstruieren. Dies geschieht, indem wir eine Normalform definieren (siehe IV.2) und dann versuchen, möglichst nur Gruppen in Normalform zu konstruieren. Dieser Konstruktionsprozeß benutzt zunächst einmal keine weiteren Restriktionen und liesse sich mit geringem Aufwand auch auf beliebige subdirekte Produkte anpassen. In der Tat kann er zum Beispiel auch zur Gewinnung aller Permutationsgruppen aus den transitiven genutzt werden, siehe IV.3.8.

Da uns primär aber nur solche Subpotenzen interessieren, die Basis einer transitiven Gruppe sind, werden wir im darauf folgenden Abschnitt IV.4 Möglichkeiten beschreiben, dahingehend auf den Konstruktionsprozeß einzuwirken und Zweige des Konstruktionsbaumes, die nur zu Subpotenzen führen, welche nicht Basis sein können, möglichst früh zu beschneiden. Schließlich soll die Struktur der Basisfaktorgruppen, die ja transitive Permutationsgruppen auf den Blöcken sind, genutzt werden, die Menge an Basiskandidaten weiter einzuschränken. In einigen Fällen gelingt dies dadurch, daß man Invarianz der Basis unter (einer geeigneten Operation) der Faktorgruppe zeigen kann, und dementsprechend die Basiskandidaten als invariante Untergruppen gewinnt, siehe IV.5 und IV.6. Da dieser Konstruktionsprozeß nicht iteriert arbeitet, muß hierfür eine andere Normalform benutzt werden (siehe IV.5.4), damit lediglich Konjugationsrepräsentanten verbleiben.

Im allgemeinen Fall schließlich können wir die Imprimitivitätsstrukturen der Faktorgruppe auf die Subpotenzen übertragen, was in IV.7 geschieht.

Ist damit die Konstruktion der Basen abgehandelt, so verbleibt nach Satz (54), die aus einer Basis hervorgehenden transitiven Gruppen zu klassifizieren. Dies benutzt im wesentlichen Informationen über die transitiven Gruppen kleineren Grades, siehe IV.9.

Abschließend werden in IV.12 Modifikationen der Vorgehensweise angesprochen, die dazu dienen können, nur eine Teilklasse der Gruppen zu konstruieren.

Während dieses gesamten Kapitels werden wir uns kaum mit konkretem Rechnen in den betrachteten Gruppen beschäftigen, das letztendlich die Realisierung im Computer benutzt. Wir werden dies in Kapitel V nachholen.

IV.2. Kanonische Form subdirekter Produkte

IV.2.1. Um die Subpotenzen M zu erhalten, aus denen wir dann die Basen transitiver Gruppen auswählen, wollen wir Repräsentanten der S_n-Klassen von Subpotenzen von Länge m eines gegebenen A erzeugen. Wir beschreiben zunächst die Konstruktion sämtlicher Subpotenzen, wobei noch keinerlei Einschränkungen bezüglich einer (für die Konstruktion transitiver Gruppen letzendlich erwünschten) transitiven Operation des Normalisators auf den Bahnen gemacht werden sollen. Diese sollen dann in den Abschnitten IV.3.5 und IV.4 betrachtet werden.

Da wir die verschiedenen Bahnlängen (die jeweils Grad der transitiven Permutationsgruppe A sind) nacheinander abhandeln, genügt es, sich im folgenden auf eine Bahnlänge zu beschränken. Wie zuvor sei $\mathcal{B}$ eine Partition von Ω in m Teilmengen der Ordnung l, es ist also $n = lm$.

Als erste Einschränkung seien die Bahnen einer Subpotenz M von A (diese bilden die Partition $\mathcal{B}$, weshabl wir die Teilmengen aus $\mathcal{B}$ auch als Bahnen bezeichnen), stets von der Form

$$\mathcal{B} = \{\{1, \ldots, l\}, \{l+1, \ldots, 2l\}, \ldots, \{n-l+1, \ldots, n\}\}$$

gewählt. Außerdem sei die Operation von M auf B_i unter der Abbildung

$$\mathrm{B}_i \to \{1, \ldots, l\}, \quad j \mapsto j - l(i-1)$$

stets identisch mit der Operation von A auf $\{1, \ldots, l\}$ gewählt.

(94) Lemma: Sind solche M und M' in S_n konjugiert, so sind sie bereits in $W = C \wr S_m$ mit $C = N_{S_l}(A)$ konjugiert.

Beweis: Da das konjugierende Element $\mathcal{B}$ festläßt, muß es in $S_l \wr S_m$ liegen. Der Anteil im Basisnormalteiler $S_l^{\times m}$ normalisiert dann jedoch alle Projektionen, liegt also bereits in $C^{\times m}$. □

Um nun eine große Anzahl an Konjugationstests zu vermeiden, sollen wenn irgend möglich direkt nur Repräsentanten konstruiert werden. Zu diesem Zweck definieren wir einen „kanonischen“ Klassenrepräsentanten, wobei sich Kanonizität lediglich auf das hier gewählte Verfahren bezieht. Bedingung dazu ist, daß effizient (das heißt, ohne jedesmal die ganze Klasse berechnen und im Speicher halten zu müssen, oder viele Konjugationstests durchzuführen) bestimmt werden kann, ob ein Klassenrepräsentant kanonisch ist; beziehungsweise, daß der dazugehörige kanonische Repräsentant ermittelt werden kann.

Da wir auch hier letztendlich wiederum eine Auswahl treffen müssen, sei eine (willkürliche) totale Ordnung $\preceq$ auf der Menge aller (Permutations)gruppen gegeben, mittels derer wir solche Entscheidungen dann aufgrund der Minimalität treffen können. Vergleiche oder Minimalitätsaussagen für Gruppen seien im folgenden stets auf diese Anordnung bezogen.

Um bei Operation auf verschiedenen Blöcken nicht in Probleme zu geraten, sei diese Anordnung translationsinvariant gewählt, daß heißt, die Anordnung von Gruppen soll sich nicht ändern, wenn für ein festes $j \in Z$ die Punkte i durch $i+j$ ersetzt werden (die in V.1 konstruierte Anordnung hat diese Eigenschaft). Mit dieser zusätzlichen Bedingung erreicht man, daß bei Einbettung $\iota\colon C \to C_i$ und $U, V \leq C$ gilt, daß $U \preceq V$ dann und nur dann, wenn $U\iota \preceq V\iota$.

Wir wollen diese Einbettungsabbildungen im folgenden nicht mehr explizit angeben, da die Gleichungen ansonsten sehr unübersichtlich werden, sie seien implizit dazugedacht.

(95) Definition: Ist X eine Gruppe, die auf der Gruppe Y als Gruppe von Automorphismen operiert, und $Z \leq Y$, so heißt Z *klein unter* X, wenn Z bezüglich $\preceq$ minimales Element der Bahn $Z^X = \{Z^x \mid x \in X\}$ ist.

(96) Bemerkung: Ist $V \leq X$ und $Z \leq Y$ klein unter X, so ist Z auch klein unter V.

IV.2.2. Die Untergruppe C_i sei diejenige Kopie von C im Basisnormalteiler von W, die auf der i-ten Bahn operiert. M sei subdirektes Produkt des Anfangsstückes $\underset{\overleftarrow{m-1}}{M}$ und A mit nach II.2.1 dazugehörigen Normalteilern $F \lhd \underset{\overleftarrow{m-1}}{M}$ und $E \lhd A$. Dabei operiert A auf der m-ten Bahn und kann daher als Untergruppe von C_m angesehen werden. M heißt *kanonischer Repräsentant*, wenn es die folgenden Bedingungen erfüllt:

- K1 Das Anfangsstück $\underset{\overleftarrow{m-1}}{M}$ ist kanonisch (implizit folgt dies dann auch für die übrigen Anfangsstücke).
- K2 F ist klein unter $N_{C \wr S_{m-1}}(\underset{\overleftarrow{m-1}}{M})$ (dabei sei $C \wr S_{m-1}$ gemäß Bemerkung (36) als Gruppe aufgefaßt, die auf den ersten $m-1$ Bahnen operiert).
- K3 E ist klein unter C_m.
- K4 Unter den nach K1 bis K3 verbleibenden W-Konjugierten von M ist M minimal.

Diese Definition mag zunächst recht komplex scheinen, ist jedoch an den Konstruktionsprozeß angepasst: Bedingung K1 wird es gestatten, die Konstruktion rekursiv durchzuführen. Bedingungen K2 und K3 schränken die „lokalen" (d.h. nur auf einigen Bahnen stattfindenden) Konjugationen ein (vergleiche Lemma (28) und Corollar (29)). Dadurch läßt sich die Anzahl der zu konstruierenden Produkte reduzieren.

(97) Lemma: Es sei M Subpotenz. Dann existiert genau ein kanonischer Repräsentant in der W-Konjugiertenklasse $[M]$ von M.

Beweis: Bedingung K4 erzwingt, daß es höchstens einen kanonischen Repräsentanten gibt.

Durch Konjugation in $C \wr S_{m-1}$ läßt sich rekursiv stets Bedingung K1 erzwingen. Bedingungen K2 und K3 schränken die Konjugation weiter ein, wobei jedoch stets nur mit solchen Gruppen konjugiert wird, die die vorangegangenen Bedingungen respektieren. Folglich gibt es Konjugierte von M, die die Bedingungen K1 bis K3 erfüllen. $\square$

Es wird sich später herausstellen, daß in manchen Fällen für die Diagonale des direkten Produktes eine andere Definition des kanonischen Repräsentanten sinnvoller ist, siehe

IV.2.15. Ähnliches gilt in einigen Fällen, in denen M durch Invarianzeigenschaften erhalten werden kann, siehe IV.5.4

IV.2.3. Um die Konjugation ebenfalls in Schritte zu den einzelnen Bahnen unterteilen zu können, faktorisieren wir W in geeigneter Form: Es sei $W_1 = \mathrm{Stab}_W(B_1)$ der punktweise Stabilisator der ersten Bahn. Dann ist W_1 von der Form $C \wr R = C^{\times(m-1)} \rtimes R$, wobei $R = \mathrm{Stab}_{S_m}(1) \leq W$ der Stabilisator der 1 im – die Bahnen permutierenden – Basiskomplement des Kranzproduktes ist. C_1 und W_1 kommutieren, da sie disjunkt operieren. T sei ein Vertretersystem der Linksnebenklassen von R in S_m. Damit läßt sich W als Produkt $W = T \cdot C_1 \cdot W_1 = T \cdot W_1 \cdot C_1$ schreiben.

In analoger Weise können wir $W_1 = T_2 C_2 W_3$ zerlegen und erhalten so die Faktorisierung

$$W = T_1 \cdot C_1 \cdot T_2 \cdot C_2 \cdot \cdots \cdot T_m \cdot C_m. \tag{98}$$

Ist eine Untergruppe $M \leq W$ gegeben, so können wir also jedes Bild von M unter Konjugation mit W erhalten, indem wir zunächst mit allen Elementen aus T_1 konjugieren, dann mit allen Elementen aus C_1 konjugieren und so weiter. Wir können dies durch einen Baum wie in Bild 1 beschreiben.

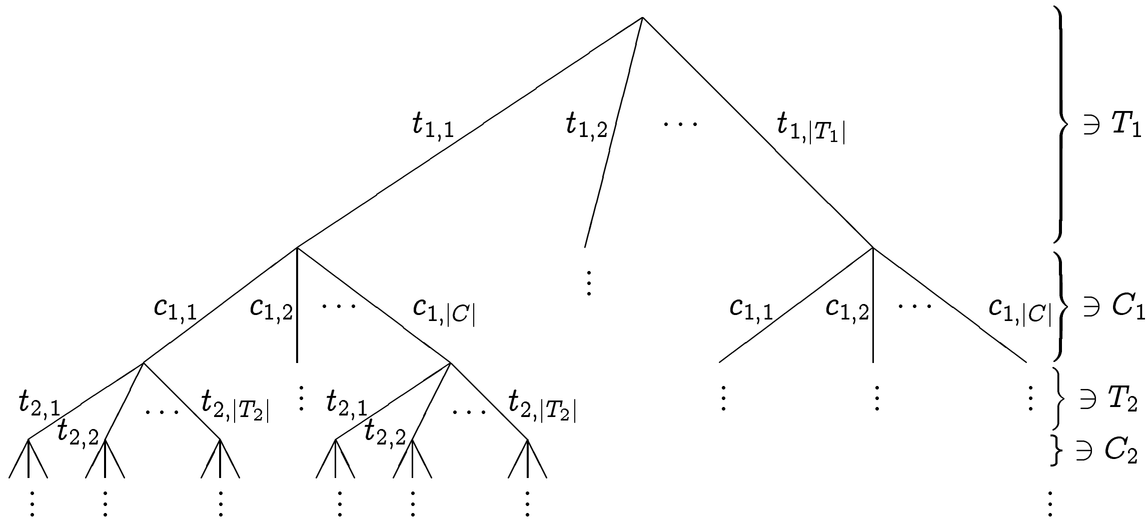


BILD 1. Baumstruktur von W

Um jedoch zu vermeiden, ganz W zu durchlaufen, wird unser Ziel in den nächsten Abschnitten sein, diesen Baum im Einzelfall zu beschneiden.

Wollen wir durch Konjugation mit W einen kanonischen Vertreter erhalten, so werden wir zur Baumbeschneidung benutzen, daß Teilprodukte $t_1 c_1 t_2 c_2 \cdots t_i c_i$ bereits das i-te Anfangsstück des Konjugationsbildes vorgeben. Soll das Bild kanonisch sein, so muß dieses Anfangsstück nach Kanonizitätsbedingung K1 ebenfalls kanonisch sein. Ist es dies nicht (was durch einfache Suche in der bereits bekannten Liste der kanonischen Vertreter geringerer Länge getestet werden kann), so ist es zwecklos, den entsprechenden Ast des Baumes weiter zu durchlaufen. In ähnlicher Weise können wir mit den Bedingungen K2 und K3 die lokale Konjugation auf einzelnen Bahnen weiter einschränken.

Bei diesem Prozeß müssen wir letzendlich Konjugationsbahnen bestimmen, und aus diesen minimale Elemente auswählen. Hiermit wäre ein naïver Bahnenalgorithmus jedoch schnell überfordert, da er oft Bilder erzeugt, die nach einem Vergleich als bereits bekannt erkannt und damit sofort verworfen werden. Der hierfür notwendige Vergleich von Permutationsgruppen (siehe V.1) benötigt jedoch stets eine Stabilisatorkette in allen verglichenen Gruppen. Eine Berechnung dieser Stabilisatorketten (selbst bei Benutzung der bereits bekannten Stabilisatorkette der konjugierten Gruppe) würde zu aufwendig.

Statt dessen lohnt es sich, den Bahnensatz (1) zu benutzen, und die Konjugationsbahn durch Konjugation der Gruppe mit Nebenklassenvertretern des Stabilisators bezüglich der Konjugationsoperation (also des Normalisators) zu erhalten. Wir benutzen dabei natürlich implizit, daß die Berechnung des Normalisators in Permutationsgruppen nicht etwa die Konjugationsbahn ausrechnet und den SCHREIERschen Untergruppensatz benutzt, sondern erheblich intelligenter vorgeht (siehe V.6).

Ein einzelner Schritt des Vorgehens soll jetzt genauer beschrieben werden. Zur Illustration des Vorgehens findet sich ein Beispiel in Abschnitt IV.2.13, das der Leser parallel zur Algorithmusbeschreibung konsultieren sollte.

IV.2.4. Es sei eine Subpotenz M von A gegeben. Der dazugehörige kanonische Repräsentant sei mit $\tilde{M}$, ein konjugierendes Element mit $w \in W$ bezeichnet: $M^w = \tilde{M}$. Im Kanonisierungsprozeß ist M gegeben und $\tilde{M}$, beziehungsweise w, gesucht. Nach (98) läßt sich $w \in W$ als Produkt $w = t_1c_1t_2c_2 \cdots t_mc_m$ mit $t_i \in T_i$ und $c_i \in C_i$ schreiben. Das gesuchte Element w soll gemäß dieser Zerlegung konstruiert werden. Hierzu durchlaufen wir den in Bild 1 dargestellten Suchbaum, der im Verlaufe dieses Prozesses gleichzeitig beschnitten wird.

Wir durchlaufen diesen Baum ebenenweise (eine Ebene besteht aus einem T_i- und einem C_i-Teil) und sammeln dabei auf jeder Ebene die „erlaubten" Äste des Baumes auf. Ein Ast ist „erlaubt", wenn nicht ausgeschlossen werden kann, daß die Darstellung des minimalkonjugierenden Elementes w über diesen Ast führt. (Offenbar ist diese Eigenschaft nicht sinnvoll a priori für den ganzen Baum definiert, sondern besagt lediglich, daß im Konstruktionsalgorithmus lokal einige Tests erfüllt wurden.) Stellt sich heraus, daß ein Ast nicht erlaubt ist, so sind alle von ihm wegführenden Zweige ebenfalls nicht erlaubt. Sind alle von einem Ast ausgehenden Zweige nicht erlaubt, so kann der Ast selber auch nicht erlaubt sein.

Die (Teilprodukte) für die möglichen konjugierenden Elemente multiplizieren sich von der Wurzel ausgehend entlang der erlaubten Äste auf.

Theoretisch wäre es anstelle des ebenenweisen Durchlaufes (bei dem zwischendurch eine Reihe von Elementen gespeichert werden müssen) auch möglich, den Baum rekursiv durch seine Äste zu durchlaufen. Dies bedingte jedoch einen rekursiven Algorithmus, in dem ein früher Abbruch (siehe Bemerkung (102)) schwieriger zu implementieren ist. Schließlich kann es sein, daß verschiedene Teilastverläufe des Baumes auf den zu konjugierenden Gruppen gleich operieren (d.h. Quotienten der konjugierenden Elemente normalisieren M). In diesem Fall genügt es offenbar, nur einen dieser Wege (und die davon ausgehenden Verzweigungen) weiter zu betrachten. Durchlaufen wir den Baum ebenenweise, so kann dies durch einfachen Vergleich der erhaltenen Konjugationsbilder auf einer Ebene geschehen. Beim rekursiven Verfahren müssten wir hierfür jeweils die Bilder aller Ebenen speichern, was zum einen aufwendiger ist, zum anderen den anfänglichen Speicherplatzgewinn des rekursiven Vorgehens mehr als wettmacht.

Grundbaustein des Algorithmus ist das Verhalten an einer einzelnen Astgabel, das wir jetzt genauer beschreiben.

IV.2.5. Nun sei angenommen, daß wir uns beim Durchlaufen des Baumes an einer Astgabelung in Tiefe i befinden. Das dorthin führende Teilprodukt sei $v := t_1c_1 \cdots t_{i-1}c_{i-1}$. Jedes $w \in W$, dessen Darstellung diese Astgabel durchläuft, beginnt also in der Darstellung gemäß (98) mit v. Dadurch ist aber bereits das $(i-1)$-te Anfangsstück von M^w bestimmt, es ist $\underleftarrow{M^w}_{i-1} = \underleftarrow{M^v}_{i-1}$. Wollen wir ein kanonisches Bild erhalten, so muß also aufgrund Bedingung K1 das Anfangsstück $\underleftarrow{M^v}_{i-1}$ bereits kanonisch sein, ansonsten wären die Äste, die zum betrachteten Knoten führen, nicht erlaubt. Dies sei angenommen, da die Filterung der vorangegangenen Schritte bereits diejenigen Äste eliminiert, für die dies nicht gilt.

Ist $w = vt_ic_i\cdots$, so bestimmt entsprechend vt_ic_i bereits das i-te Anfangsstück von M^w. Aufgrund Bedingung K1 sind nur diejenigen t_i und c_i erlaubte Äste, für die $\underleftarrow{M^{vt_ic_i}}_{i}$ kanonisch ist. Dies führt zur oben erwähnten Baumbeschneidung. Ebendiese t_ic_i definieren dann die v fortsetzenden erlaubten Teilprodukte für die nächste Ebene $i+1$.

Ist für alle t_ic_i das Anfangsstück $\underleftarrow{M^{vt_ic_i}}_{i}$ nicht kanonisch, so stellt sich damit heraus, daß bereits die allein zum betrachteten Knoten führenden Äste nicht erlaubt sind.

IV.2.6. Um nun die einzelnen Kanonizitätsbedingungen für das Anfangsstück $\underleftarrow{M^{vt_ic_i}}_{i}$ zu testen, betrachten wir es als subdirektes Produkt des (durch v bereits bestimmten) Anfangsstückes $\underleftarrow{M^v}_{i-1}$ mit A_i zu den Normalteilern $F \lhd \underleftarrow{M^v}_{i-1}$ und $E \lhd A_i$. (Wohlgemerkt: Auch wenn $\underleftarrow{M^v}_{i-1}$ bereits durch v festgelegt ist, so gilt dies nicht für F und E !)

Der Normalteiler F wird dabei durch Konjugation mit c_i (die ja auf disjunkter Bahn stattfindet) nicht verändert. Die Bedingung K2 ist also eine Bedingung, die nur t_i einschränkt. Nur diejenigen $t_i \in T_i$ sind geeignet, für die das entsprechende $F(t_i)$ (also der punktweise Stabilisator der i-ten Bahn in $\underleftarrow{M^{vt_i}}_{i}$) klein unter $N_{C\wr S_{i-1}}(\underleftarrow{M^v}_{i-1})$ ist. Da angenommen war, daß $\underleftarrow{M^v}_{i-1}$ kanonisch ist, können wir davon ausgehen, daß dieser Normalisator $N_{C\wr S_{i-1}}(\underleftarrow{M^v}_{i-1})$ bereits bekannt ist.

Für jedes $t_i \in T_i$, einem für die Ebene fest gewählten Vertretersystem von Linksnebenklassen, bestimmen wir also

$$\mathrm{Stab}_{[i\text{-te Bahn}]}\left(\underleftarrow{M^{vt_i}}_{i}\right) \lhd \underleftarrow{M^v}_{i-1}$$

(formal gesehen ist es das äquivalente Bild bei Einschränkung der Operation des Stabilisators auf die ersten $i-1$ Bahnen. Da die Operation auf der i-ten Bahn aber definitionsgemäß trivial ist, soll dieser Monomorphismus der Schreiberleichterung wegen nicht mit notiert werden.) und testen, ob dieser minimal unter $N_{C\wr S_{i-1}}(\underleftarrow{M^v}_{i-1})$ ist. Diejenigen t_i, für die dies gilt, sind an dieser Astgabelung erlaubt.

IV.2.7. Zu jedem der erlaubten t_i werden jetzt die möglichen c_i bestimmt. Wir betrachten ab jetzt nur noch ein festes t_i, rücken in der Beschreibung also eine Astgabelung, eine halbe Ebene, nach unten. Für die anderen t_i wird der gleiche Prozeß durchgeführt.

Konkret sollen nun diejenigen $c_i \in C_i$ gesucht werden, die $\underset{i}{\underleftarrow{M^{vt_i}}}$ auf den kanonischen Vertreter dieses Anfangsstücks abbilden, da ansonsten Bedingung K1 nicht erfüllt werden kann. Gibt es keine solchen c_i, so ist bereits t_i nicht erlaubt.

Wir betrachten wiederum $\underset{i}{\underleftarrow{M^{vt_i}}}$ als subdirektes Produkt von $\underset{i-1}{\underleftarrow{M^{v}}}$ und A_i mit den Normalteilern $F \lhd \underset{i-1}{\underleftarrow{M^{v}}}$ und $E \lhd A_i$. Hierfür ist Bedingung K3 noch zu erfüllen. Dazu sei $\tilde{E}$ der zu E unter C_i konjugierte Vertreter klein unter C_i. Alle erlaubten c_i müssen E auf $\tilde{E}$ konjugieren und liegen daher nach II.0.6 in einer Nebenklasse s_iX des Normalisators $X = N_{C_i}(\tilde{E})$. Für deren Repräsentanten s_i gilt, daß $E^{s_i} = \tilde{E}$ ist. Der Vertreter s_i kann dementsprechend aus einem Vertretersystem von $N_{C_i}(E)\backslash C_i$ gewählt werden. (Da $N_{C_i}(E)^{s_i} = N_{C_i}(\tilde{E}) = X$ braucht man natürlich nur einen Normalisator zu berechnen.)

Ab jetzt sei s_i der Nebenklassenvertreter mit minimalem Konjugationsbild. Als nächstes ist Bedingung K4 für das i-te Anfangsstück zu erfüllen. Dazu ist c_i (von dem wir bisher wissen, daß es in der Nebenklasse s_iX liegen muß) weiter so einzuschränken, daß das Anfangsstück $\underset{i}{\underleftarrow{M^{vt_ic_i}}}$ minimal ist. Wir müssen also nach einem $r_i \in X$ suchen, für welches das i-te Anfangsstück $\underset{i}{\underleftarrow{M^{vt_is_ir_i}}}$ minimal wird. Dabei genügt es nach II.0.6 wiederum, die r_i aus einem Vertretersystem von $N_X(\underset{i}{\underleftarrow{M^{vt_is_i}}})\backslash X$ zu wählen.

Ab jetzt sei r_i der Vertreter mit minimalem Konjugationsbild $\underset{i}{\underleftarrow{M^{vt_is_ir_i}}}$.

Ist $i < \mathrm{len}(M)$, so ist außerdem Bedingung K1 zu erfüllen, daß heißt, es ist sicherzustellen, daß $\underset{i}{\underleftarrow{M^{vt_is_ir_i}}}$ kanonisch ist. Dabei gehen wir davon aus, daß für alle Längen kleiner als $\mathrm{len}(M)$ die kanonischen Vertreter bereits bekannt sind, der Kanonizitätstest daher einfach durch Vergleich mit diesen Vertretern vonstatten gehen kann.

Stellt sich dabei heraus, daß $\underset{i}{\underleftarrow{M^{vt_is_ir_i}}}$ nicht in der Liste der kanonischen Vertreter von Länge i vorkommt, so gibt es zum gewählten t_i keine c_i, die zu kanonischen Konjugationsbildern führen. Alle Wege, die vom betrachteten Knoten aus über t_i laufen, sind also nicht erlaubt. Andernfalls gilt mit $D = N_X\left(\underset{i}{\underleftarrow{M^{vt_is_ir_i}}}\right)$ für alle

$$c_i \in s_ir_iD, \tag{99}$$

daß $\underset{i}{\underleftarrow{M^{vt_ic_i}}}$ kanonisch ist, und dementsprechend alle Äste zu diesen c_i zunächst erlaubt sind.

IV.2.8. Ist $i = \mathrm{len}(M)$ so liefern alle c_i das gleiche Konjugationsbild, da D die Gruppe $M^{vt_is_ir_i}$ normalisiert. In diesem Fall ist die Behandlung abgeschlossen. Die weiteren Betrachtungen betreffen nur den Fall $i < \mathrm{len}(M)$.

Wir nehmen nun an, daß es erlaubte c_i gibt, und setzen der Schreibersparnis halber $L := M^{vt_is_ir_i}$. Anstelle M^{vt_i} mit $c_i \in s_ir_iD$ zu konjugieren, können wir offenbar genausogut L mit $d \in D$ konjugieren. Von Interesse sind im allgemeinen aber nicht die konjugierenden Elemente, das heißt die Gruppe D, sondern die verschiedenen Konjugationsbilder, das heißt die Bahnen von D. Auch hier soll aber wieder, wenn möglich, ein Bahnenalgorithmus vermieden werden. Wir möchten daher D durch eine kleinere Menge ersetzen, die ausreicht, letztendlich alle erlaubten Konjugationsbilder zu erreichen. Dazu fassen wir L als subdirektes Produkt des Anfangsstückes $B = \underleftarrow{L}_i = \underleftarrow{M^{vt_is_ir_i}}_i$ mit dem entsprechenden Endstück $\bar{A}$ auf, das als Bild der Operation von M auf der $i+1$-ten bis m-ten Bahn erhalten wird. Dieser Zerlegung als subdirektes Produkt entsprechen Normalteiler $\bar{F} \lhd B$ und $\bar{E} \lhd \bar{A}$ (dies sind andere Normalteiler, als beim Anfügen eines *einzelnen* A an ein Anfangsstück! Wir benennen die Gruppen aber in Anlehnung an die Bezeichnungen für subdirekte Produkte in dieser Weise), sowie Epimorphismen $\zeta\colon B \to B/\bar{E}$, $\xi\colon \bar{A} \to \bar{A}/\bar{F}$ und ein Isomorphismus $\chi\colon B/\bar{F} \to \bar{A}/\bar{E}$. Die Gruppe D ist weiterhin die B normalisierende Untergruppe aus (99), $\bar{C}$ sei der Normalisator von $\bar{A}$ in der symmetrischen Gruppe auf den letzten Bahnen.

Wir wollen die Anzahl der zu betrachtenden Elemente aus D reduzieren und müssen also zu einzelnen Konjugenden $d \in D$ testen, ob deren Konjugation nicht auch durch Konjugation mit Elementen aus $\bar{C}$ (die ja später im Algorithmus auf höheren Ebenen noch durchgeführt werden wird) erreichbar ist. Die Bedingung aus (34) lautet dann:

> Es ist $\bar{F}^d = \bar{F}$ und es existiert ein $c \in N_{\bar{C}}(\bar{E})$, so daß für alle $b \cdot a \in L$ folgt, daß $(b^d)\zeta\chi = (a^c)\xi$ gilt.

Dabei beachten wir, daß die Darstellung von L als subdirektes Produkt von B mit $\bar{A}$ für alle $l \in L$ unmittelbar die Zerlegung $l = b \cdot a$ liefert.

IV.2.9. Um $\bar{F}^d = \bar{F}$ zu erzwingen, zerlegen wir D in Nebenklassen $N_D(\bar{F})\backslash D$. Ist $N_D(\bar{F})d = dN_D(\bar{F}^d)$ eine Nebenklasse, so bilden alle Elemente der Form dh aus dieser Nebenklasse bei Konjugation $\bar{F}$ auf $\bar{F}^d$ ab. Wir durchlaufen diese Nebenklassen $N_D(\bar{F})\backslash D$ in einer Schleife über den Repräsentanten d.

Nach der Konjugation mit d braucht also das Bild L^d nur noch mit Elementen $h \in H := N_D(\bar{F}^d)$ konjugiert werden, wobei der Kern $\bar{F}^d$ fest bleibt. Da wir nur an den verschiedenen Bildern interessiert sind, braucht des weiteren nur mit Nebenklassenvertretern von $N_H(L^d) = N_D(L)^d$ (um die Gleichheit zu sehen beachte, daß aus $H \leq D$ „$\leq$“ folgt, während L normalisierende D-Konjugation nach (33) automatisch $\bar{F}$ festlassen muß, was „$\geq$“ impliziert) konjugiert zu werden. Weiterhin können wir nun die Kriterien aus II.2.9 anwenden, um zu testen, wann Konjugation vom Normalisator induziert ist; beziehungsweise, welche $1 \neq dh$ ignoriert werden können:

Das dort gegebene dritte Kriterium ist nicht so einfach zu testen, da es den Normalisator von $B = B^d$ und von $\bar{F}^d$ benötigt; dieser muß erst neu berechnet werden, was nur bei einer großen äusseren Automorphismengruppe des Faktors die Einsparungen lohnte.

Das zweite Kriterium dagegen übersetzt sich offensichtlich: Wir bezeichnen den Homomorphismus von H in $\mathrm{Aut}(B/\bar{F}^d)$ mit ϑ. Aufgrund der zweiten Bedingung können wir diejenigen Elemente h, die in $\mathrm{Kern}\,\vartheta \cdot B$ liegen ignorieren. Setzen wir somit $Y := H \cap (\mathrm{Kern}\,\vartheta \cdot B)$, so ist $Y \lhd H$ ein Normalteiler, mit dessen Elementen nicht zu konjugiert werden braucht. Folglich genügt es sogar, die Konjugenden h aus einem Vertretersystem der Nebenklassen $N_H(L^d)Y\backslash H$ zu wählen.

IV.2.10. Das (offensichtliche) erste Kriterium benötigt sogar den Normalisator von L in S_n, der noch aufwendiger zu bestimmen ist. Im Sonderfall $i = 1$ läßt es sich jedoch manchmal einfach anwenden: Es sei M eine Subpotenz, die kanonisiert, beziehungsweise auf Kanonizität getestet werden soll. N sei der Normalisator von M (den wir zur Konstruktion der transitiven Gruppen, unabhängig von Kanonisierungsprozeß, immer berechnen müssen). Operiert N transitiv auf den Bahnen und ist die Operation von $\mathrm{Stab}_N(\mathrm{B}_1)$ auf B_1 gleich ganz C_1 (aufgrund der Transitivität folgt dies dann auch für die übrigen Bahnen), so induziert für beliebiges $w \in W$ der Normalisator $N_W(M^w) = N_W(M)^w$ stets die gesamte C_1-Konjugation auf der ersten Bahn. (Wollten wir das Kriterium auch auf die übrigen C_i anwenden, so benötigten wir, daß das Normalisatorelement auf den jeweils vorangegangenen Bahnen trivial operiert, was im allgemeinen nicht gilt. Daher ist dieses Kriterium nur für die erste Bahn praktikabel.)

IV.2.11. Setzen wir nun $\bar{D} \subset D$ gleich der Menge derjenigen d, die nach diesem Test verbleiben, so müssen wir damit für c_i alle Elements aus

$$s_i r_i \bar{D} = \{s_i r_i d \mid d \in \bar{D}\}$$

berücksichtigen. Wir bilden nun für jedes $c_i \in s_i r_i \bar{D}$ das Produkt $v t_i c_i$ und speichern es in einer Liste der Produkte über erlaubte Äste. Auf der nächsten Ebene entnehmen wir dann dieser Liste die Produkte v, die zu möglichen Knoten führen.

Ist die behandelte Ebene die letzte, so ist der kanonische Vertreter $\tilde{M}$ von M das minimale Konjugationsbild bei Konjugation von M mit Elementen aus dieser Liste.

In der Praxis benutzten wir, wenn nicht nach konjugierenden Elementen gesucht wird, nicht eine Liste der konjugierenden Elemente v, sondern speichern immer bereits die Konjugationsbilder. (Dementsprechend betrachten wir dann nicht $M^{v t_i c_i}$ sondern $\hat{M}^{t_i c_i}$, wobei $\hat{M}$ eines der gespeicherten Konjugierten ist.) Dies erspart mehrfache gleichartige Konjugationen, benötigt dafür aber mehr Speicher. Dies hat sich bisher aber nicht als Problem erwiesen.

IV.2.12. Auf diesen Überlegungen aufbauend ergibt sich nun der folgende Algorithmus zur Bestimmung des kanonischen Repräsentanten von M.

(100) ALGORITHMUS: Zu einer Subpotenz M in Normalform gemäß IV.2.1 bestimme den kanonischen Repräsentanten von M, beziehungsweise ein konjugierendes Element. Die kanonischen Repräsentanten von kleinerer Länge i seien in $Kanonisch_i$ gespeichert.

1. [Initialisierung] Setze $i := 1$, $Anfänge := \{M\}$. S sei das bahnpermutierende Basiskomplement in W, das als auf $\{1, \dots, m\}$ operierend angesehen wird.
2. [Bahnen] Setze $S' := \mathrm{Stab}_S(i)$ und T gleich einem Vertretersystem von S/S'.
   Setze $neue\_Anfänge := \{\}$. Mit μ_i sei die Projektion auf die ersten i Bahnen bezeichnet.
3. [Behandele alle bisherigen Anfänge] Wenn $|Anfänge| = 0$, dann gehe zu Schritt 8. Sonst sei $\hat{M} \in Anfänge$. Setze $Anfänge := Anfänge \setminus \{\hat{M}\}$.
4. [Durchlaufe Nebenklassen] Für alle $t_i \in T$ durchlaufe 5-7
5. [Teste, ob t_i geeignet] Wenn $\hat{M}^{t_i}\mu_i \notin Kanonisch_i$, dann gehe zu Schritt 7 (IV.2.5).

6. [Neue Konjugationsbilder] Bestimme nach IV.2.7-IV.2.11 die möglichen c_i zu t_i. (Dabei können die Normalisatoren der kanonischen Anfangsstücke per Induktion ebenfalls als bekannt angesehen werden, und brauchen nicht neu berechnet zu werden.) Für jedes mögliche c_i füge $\hat{M}^{t_i c_i}$ der Menge *neue_Anfänge* hinzu.
7. [Schleifenende] Sind noch nicht alle t_i durchlaufen, so gehe zu 4. Ansonsten gehe zu 3.
8. [Bahnwechsel] Setze *Anfänge* := *neue_Anfänge*, $i := i + 1$. Wenn $i <= \operatorname{len} M$ ist, gehe zu 2.
9. [Kanonischer Vertreter] Gib das minimale Element aus *Anfänge* als kanonischen Vertreter zurück.

Führt man parallel zu der Liste der Bilder in *Anfänge* auch Listen mit konjugierenden Elementen und bildet aus diesen ebenso in jedem Schritt eine neue Liste der Produkte mit den Elementen $t_i c_i$, so bekommt man in 9. auch ein konjugierendes Element.

(101) LEMMA: In Schritt 9 ist das minimale Element der Liste *Anfänge* der kanonische Repräsentant von M.

Beweis: Da Bedingung K4 gerade die Minimalität fordert, genügt es zu zeigen, daß jedes w, das M auf einen Vertreter konjugiert, der K1 bis K3 erfüllt, in der Schleife betrachtet wird. Nach (98) zerlegt sich dieses w als Produkt $w = \prod t_i c_i$. In jedem Schritt der Schleife werden nun die möglichen t_i gemäß IV.2.5 und die dazu möglichen c_i nach IV.2.7 betrachtet, und die entsprechenden Bilder gesammelt. Nach Beendigung der Schleife enthält die Liste daher alle diejenigen Konjugierten, die Bedingungen K1 bis K3 erfüllen. □

(102) BEMERKUNG: Soll nur getestet werden, ob ein Repräsentant kanonisch ist, so kann offensichtlich abgebrochen werden, sobald in der Liste eine Gruppe existiert, so daß deren Projektion auf die ersten $m-1$ Bahnen kanonisch ist, die Projektionskerne Bedingungen K1 bis K3 erfüllen, und sie kleiner als M ist.

IV.2.13. Wir illustrieren unser Vorgehen am Beispiel einer Subpotenz von S_3 von Länge 3. Um die Notation kompakt zu halten, seien für Subpotenzen von S_3 die folgenden Schreibweisen vereinbart: Es sei

$$a = (1,2,3), \quad b = (1,2), \quad a' = (1,3,2), \quad b' = (2,3), \quad \hat{b} = (1,3).$$

Permutationen der Bahnen werden durch einen darüberstehenden Balken bezeichnet: $\overline{(1,2)}$. Subpotenzen sind jeweils in die direkte Potenz eingebettet, Elemente werden entsprechend als Tupel notiert. So sind die kanonischen (bezüglich der in V.1 definierten Anordnung, wenn man die direkten Potenzen mit intransitiven Permutationsgruppen identifiziert) Vertreter der Subpotenzen von Länge 2:

$$\begin{aligned}
\mathrm{Diag}(S_3, S_3) &:= \langle (a,a), (b,b) \rangle \\
&\triangleq \langle (1,2,3)(4,5,6), (1,2)(4,5) \rangle \\
S_3 \times S_3 &:= \langle (a,1), (b,1), (1,a), (1,b) \rangle \\
&\triangleq \langle (1,2,3), (1,2), (4,5,6), (4,5) \rangle \\
S_3 \perp S_3 &:= \langle (a,1), (b,b), (1,a) \rangle \\
&\triangleq \langle (1,2,3), (1,2)(4,5), (4,5,6) \rangle .
\end{aligned}$$

Wir wollen nun die Subpotenz von Länge 3

$$M := \langle (a,a,1), (1,1,a), (b,b,b) \rangle$$

kanonisieren. Der Normalisator von M in $C \wr S_m$ ist nicht transitiv (M ist also nicht Basis einer transitiven Gruppe), die Methoden aus IV.2.10 sind daher nicht anwendbar. (Da es sich um die Vorführung eines Algorithmus handelt, sind Variablen stets nur lokal definiert.) Da das Beispiel recht klein ist, sind viele der Nebenklassenvertreter s_i und r_i gleich dem trivialen Element. In größeren Beispielen tritt dies nicht mehr so häufig auf.

Es ist

$$T_1 := \{ t_{1,1} = \overline{()}, t_{1,2} = \overline{(1,3)}, t_{1,3} = \overline{(1,2)} \}.$$

Dann ist $M^{t_{1,1}} = M$. Vorangegangene Bahnen gibt es nicht, das Anfangsstück $\underleftarrow{M^{t_{1,1}}}_{0}$ ist trivial. Wir können also $t_{1,1}$ als geeignet ansehen und direkt zu IV.2.7 gehen. Ebenso folgt, daß hier $E = A$ ist, und wir $s_{1,1} = 1$ und $X = C_1$ setzen können. (Für die anderen Vertreter aus T_1 gilt das gleiche.)

Die Projektion von $M^{t_{1,1}}$ auf die erste Bahn hat Bild $\langle (a), (b) \rangle$, dies ist auch der kanonische Vertreter dieser Gruppe. Wir setzen also $r_{1,1} := 1$ und erhalten $D = N_X(\underleftarrow{M^{t_{1,1}}}_{i}) = C_1$. Es ist also $L := M^{t_{1,1} s_{1,1} r_{1,1}} = M$. Wir fassen L als subdirektes Produkt des Anfangsstückes $B = \underleftarrow{L}_1 = \langle (a), (b) \rangle$ mit dem Endstück $\bar{A} = \langle (a,1), (1,a), (b,b) \rangle$ und den Normalteilern $\bar{F} = \langle \rangle \lhd B$ und $\bar{E} = \langle (1,a) \rangle \lhd \bar{A}$ auf. Nun wird $\bar{F}$ von D normalisiert, wir haben also $d = 1$ und $H := D$. Es ist $N_H(L^d) = \langle \rangle$. Weiterhin ist (da wir $B/\bar{F}$ als S_3 auffassen können) $\mathrm{Kern}\,\vartheta = \langle \rangle$ und $Y := H \cap (\mathrm{Kern}\,\vartheta \cdot B) = H$. Wir müssen also nur mit der Identität konjugieren, und merken uns als Ergebnis die Gruppe $M_{1,1} = M$.

Für $t_{1,2}$ erhalten wir ebenso $s_{1,2} = 1$, $r_{1,2} = 1$ und $D = C_1$. Setzen wir entsprechend der Beschreibung also

$$L := M^{t_{1,2} s_{1,2} r_{1,2}} = \langle (a,1,1), (1,a,a), (b,b,b) \rangle,$$

so ist L subdirektes Produkt von $B = \langle (a), (b) \rangle$ mit $\bar{A} = \langle (a,a)(b,b) \rangle$ zu den Normalteilern $\bar{F} = \langle (a) \rangle$ und $\bar{E} = \langle (a,a) \rangle$. Wiederum wird $\bar{F}$ von ganz D normalisiert, mit $d = 1$ und $H := D$ ist dann $N_H(L^d) = H$. Wiederum müssen wir nur mit der Identität konjugieren, und erhalten $M_{1,2} := L$.

Für $t_{1,3}$ schließlich ist das Vorgehen analog. Da $M^{t_{1,1}} = M^{t_{1,3}}$ gilt, sei dies nicht nochmals aufgeführt. Der Algorithmus stellt dann jedoch fest, daß $M_{1,3} = M_{1,1}$ gilt, die Liste *Anfänge* besteht daher zum Ende der Behandlung der ersten Bahn aus M und $M_{1,2}$.

Wir gehen zur nächsten Bahn über, und bestimmen das Vertretersystem

$$T_2 := \{t_{2,1} = \overline{()}, t_{2,2} = \overline{(2,3)}\}.$$

Zunächst behandeln wir $M = M_{1,1}$. Konjugation mit $t_{2,1}$ liefert wieder M. Nun betrachten wir $\underset{2}{\underleftarrow{M}} = \langle (a,a),(b,b)\rangle$ und dort als Untergruppe den Kern $F = \langle\rangle$ auf der ersten Bahn. Dieser ist klein unter $N_{C_1}(A_1) = C_1$, $t_{2,1}$ ist also zunächst erlaubt. Nun betrachten wir den Normalteiler $E = \langle\rangle$ zur zweiten Bahn. Dieser ist klein unter C_2, es ist also $s_{2,1} = 1$ und $X = S_3$. Nun ist $N_X(\underset{2}{\underleftarrow{M^{t_{2,1}s_{2,1}}}}) = \langle\rangle$. Zu jedem der sechs Nebenklassenvertreter betrachten wir das Konjugierte, und stellen fest, daß es für den Nebenklassenvertreter $r_{2,1} = 1$ minimal ist. Durch Nachsehen in der Liste der Subpotenzen von Länge 2 stellen wir fest, daß $\underset{2}{\underleftarrow{M^{t_{2,1}s_{2,1}r_{2,1}}}}$ kanonisch ist. Damit verbleibt $D = \langle\rangle$, wir brauchen also nicht weiter zu konjugieren, und merken uns $M_{2,1} = M_{1,1}^{t_{2,1}s_{2,1}r_{2,1}} = M$.

Nun konjugieren wir $M_{1,1}$ mit $t_{2,2}$, und betrachten $\underset{2}{\underleftarrow{M^{t_{2,2}}}} = \langle (a,1),(1,a),(b,b)\rangle$. Der Normalteiler zur ersten Bahn ist $F = \langle (a)\rangle$, dieser ist klein unter C_1. Auch $t_{2,2}$ ist hier also erlaubt. Der Normalteiler zur zweiten Bahn, $E = \langle (a)\rangle$, ist klein unter C_2, es ist also $s_{2,2} = 1$ und $X = C_2$. Nun ist $N_X(\underset{2}{\underleftarrow{M^{t_{2,2}s_{2,2}}}}) = X$, es ist also $r_{2,2} = 1$. Nachsehen in der Liste liefert, daß $\underset{2}{\underleftarrow{M^{t_{2,2}s_{2,2}r_{2,2}}}}$ kanonisch ist. Wir haben also $D = C_2$ und setzen $L := M^{t_{2,1}s_{2,1}r_{2,1}}$. Der Normalteiler in $B = \underset{2}{\underleftarrow{L}} = \langle (a,1),(1,a),(b,b)\rangle$ ist $\bar F = \langle (1,a)\rangle$. Es ist $D = N_D(\bar F)$, also ist $H = D$. Nun ist $N_H(L) = H$, es braucht also nur mit der Identität konjugiert zu werden, und wir merken uns $M_{2,2} = M_{1,1}^{t_{2,2}s_{2,2}r_{2,2}}$.

Als nächstes müssen wir $M_{1,2}$ ebenso behandeln. Konjugation mit $t_{2,1}$ liefert wieder $M_{1,2}$. Nun betrachten wir $\underset{2}{\underleftarrow{M_{1,2}}} = \langle (a,1),(1,a),(b,b)\rangle$ und dort als Untergruppe den Kern $F = \langle (a)\rangle$ auf der ersten Bahn. Dieser ist klein unter C_1, $t_{2,1}$ ist also zunächst erlaubt. Dann betrachten wir den Normalteiler $E = \langle (a)\rangle$ zur zweiten Bahn. Dieser ist klein unter C_2, es ist also $s_{2,1} = 1$ und $X = C_2$. Schließlich ist $N_X(\underset{2}{\underleftarrow{M_{1,2}^{t_{2,1}s_{2,1}}}}) = X$, also ist $r_{2,2} = 1$ und $D = C_2$. Das Anfangsstück $\underset{2}{\underleftarrow{M_{1,2}^{t_{2,1}s_{2,1}r_{2,1}}}}$ wird in der Liste der kanonischen Gruppen gefunden. Wir setzen also $L = M_{1,2}^{t_{2,1}s_{2,1}r_{2,1}}$ und erhalten dort den Normalteiler $\bar F = \langle (a,1)\rangle \lhd B = \underset{2}{\underleftarrow{L}}$. Es ist $N_D(\bar F) = D$, also ist $H = D$. Der Normalteiler $\operatorname{Kern}\vartheta$ ist trivial, es ist $Y = H \cap (\operatorname{Kern}\vartheta \cdot B) = \langle (a)\rangle$. Wir müssen L also mit der Identität und mit $b \in C_2$ (als einem Nebenklassenvertreter) konjugieren, und erhalten so $M_{2,3} = M_{1,2}$ und $M_{2,4} = \langle (b,b,b),(a,1,1),(1,a',a)\rangle$, die wir uns merken.

Da $M_{1,2}^{t_{2,1}} = M_{1,2}^{t_{2,2}}$ gilt, sei die Rechnung für $t_{2,2}$, die genauso verläuft, nicht extra angegeben.

Auf der dritten Ebene schließlich wird die Transversale trivial. Für $M_{2,1}$ ergibt sich der Kern $F = \langle (a,a)\rangle$, der klein unter $N_{C\wr 2}(\underset{2}{\underleftarrow{M_{2,1}}})$ ist. Der andere Kern, $E = \langle (a)\rangle$, ist normal in C_3, es ist also $X = C_3$ und $s_{3,1} = 1$. Nun ist nur noch $r_{3,1}$ so zu bestimmen, daß das

Konjugationsbild minimal ist. Da $M_{2,1}^{s_{3,1}}$ unter X normal ist, ist $r_{3,1} = 1$, und wir merken uns $M_{3,1} = M_{2,1} = M$.

Für $M_{2,2}$ ergibt sich der Kern $F = \langle(1, a)\rangle$, der klein unter $N_{C\wr 2}(\underset{\leftarrow 2}{M_{2,2}})$ ist. In diesem Fall ist $E = \langle\rangle$, also ist $s_{3,1} = 1$ und $X = C_3$. Nun ist $N_X(M_{2,2}) = \langle\rangle$, als minimalkonjugierendes Element ergibt sich $r_{3,1} = 1$, wir merken uns $M_{3,2} = M_{2,2}$.

Für $M_{2,3}$ ist $F = \langle(a, 1)\rangle$ nicht klein unter $N_{C\wr 2}(\underset{\leftarrow 2}{M_{2,3}})$, dieser Zweig des Kontruktionsbaumes wird verworfen. Gleiches gilt für $M_{2,4}$ mit $F = \langle(a, 1)\rangle$.

Am Ende verbleiben daher $M_{3,1}$ und $M_{3,2}$, wobei $M_{3,1} = M$ als kleinere (bezüglich der in V.1 definierten Ordnung) Gruppe kanonisch ist.

IV.2.14. Ist eine (beliebige) Subpotenz M von A gegeben die kanonisiert werden soll, so wird das System der Bahnen von M zunächst durch eine offensichtliche Konjugation von M in die in IV.2.1 definierte Gestalt gebracht. Die Operationen auf den Bahnen werden durch nachfolgende Konjugation von M auf den kanonischen Vertreter ihres Typs abgebildet, um die gesamten Bedingungen aus IV.2.1 zu erfüllen. Diese Konjugation muß im allgemeinen durch eine Backtracksuche [Leo1991, The1996] geschehen. Dabei kann der Typ des Bildes (und damit die kanonische Form, auf die die Projektion konjugiert werden muß) durch Invariantensuche gemäß (14) geschehen.

Auf das so normalisierte Konjugierte von M kann dann der beschriebene Kanonisierungsalgorithmus angewandt werden.

IV.2.15. Schließlich betrachten wir noch als Sonderfall die Diagonale

$$D = \langle(a, a, \dots, a), (b, b, \dots, b), \dots\rangle.$$

Da nicht zentralisierende Konjugation auf einer Bahn bereits die Diagonalstruktur zerstört ist die W-Klasse hier sehr groß und der Kanonisierungsvorgang wird sehr aufwendig. In vielen Fällen können wir hier aber bereits anhand der Ordnung des subdirekten Produktes entscheiden, ob es zu D konjugiert ist:

(103) Lemma: A besitze lediglich Automorphismen, die nach Lemma (7) von der S_l herrühren. Dann sind alle subdirekten Produkte M mit $|M| = |A|$ zu D konjugiert.

Beweis: Ist $|M| = |A|$, so ist muß M von der Form $\{(a, a\alpha_1, \dots, a\alpha_m)\}$ sein, wobei α_i Automorphismen von A sind. Nach Voraussetzung rühren diese jedoch von der Konjugation mit dem Normalisator $C = N_{S_l}(A)$ her. M kann also mittels Konjugation in $C^{\times m} \leq W = C \wr S_m$ auf D abgebildet werden. □

In diesem Fall wird D als kanonischer Repräsentant gewählt und die Klasse läßt sich einfach aufgrund der Ordnung des Repräsentanten identifizieren.

Bei der dualen Situation des direkten Produktes tritt ein solches Problem nicht auf, da selbiges in W normal ist.

IV.3. Konstruktion von Subpotenzen

Die eigentliche Konstruktion der Subpotenzen geschieht nun rekursiv. Aufgrund Bedingung K1 an kanonische Vertreter erhält man die kanonischen Vertreter der Subpotenzen von Länge i als Teilmenge aller möglichen subdirekten Produkte der kanonischen Vertreter der Subpotenzen von A von Länge $i-1$ mit A. Aus diesen Produkten werden dann diejenigen ausgewählt, welche kanonisch sind. Bedingungen K1 bis K3 schränken dabei die Menge der zu konstruierenden Produkte weiter ein. Der Kanonizitätstest kann in denjenigen Fällen entfallen, in denen offensichtlicherweise das Produkt nur einmal konstruiert wird. Dies tritt zum Beispiel beim direkten Produkt sowie im Falle von Lemma 103 bei der Diagonale ein. Die Gruppe B sei im folgenden eine kanonische Subpotenz von Länge $i-1$.

IV.3.1. Wie in II.2.6 parametrisieren wir die subdirekten Produkte von A und B mittels der Normalteiler $E \trianglelefteq A$, der Normalteiler $F \trianglelefteq B$ mit $B/F \cong A/E$ sowie der Isomorphismen zwischen B/F und A/E. Die Konstruktion geschieht dann aus genau diesen Bestandteilen: Es werden alle Normalteiler von B bestimmt, deren Faktorgruppe zu einem Faktor von A isomorph ist. Ausserdem wird ein geeigneter Isomorphismus der Faktorgruppen ermittelt. Die Einbettung in das direkte Produkt geschieht automatisch dadurch, daß A und B als Permutationsgruppen auf disjunkten Mengen Ω_A und Ω_B gegeben sind.

Da Subpotenzen von A gebildet werden sollen, werden zu Beginn des Konstruktionsprozesses alle Normalteiler von A bestimmt. Aufgrund Bedingung K3 (und der Translationsinvarianz der Anordnung) braucht aus jeder Bahn des Normalisators C auf den Normalteilern $E \triangleleft A$ nur jeweils der kleinste Repräsentant betrachtet zu werden. Zu den so erhaltenen Normalteilern werden die Automorphismengruppen der Faktorgruppen bestimmt.

Sollen dann alle subdirekten Produkte aus B und A erzeugt werden, so sind lediglich diejenigen Normalteiler in B zu bestimmen, deren Faktorgruppe zu einer Faktorgruppe eines (ausgewählten) Normalteilers von A isomorph ist. Aufgrund Bedingung K2 brauchen wiederum nur solche Normalteiler von B berücksichtigt zu werden, die klein unter dem Normalisator von B sind. Da die Faktorgruppen meist von geringer Ordnung sind, bietet es sich zudem an, nicht direkt nach Isomorphismen zu suchen, sondern zunächst mittels Gruppeninvarianten (welche kleine Gruppen meist eindeutig identifizieren, siehe [Neu1967]) diejenigen Normalteiler zu bestimmen, für deren Faktorgruppen sich ein Isomorphismus ergeben kann.

IV.3.2. Insbesondere bei kleinem A und großem m können die Anfangsstücke B recht groß werden und dementsprechend viele Normalteiler enthalten. Von diesen sind jedoch die allermeisten nicht von Interesse, da ihre Faktorgruppen zu groß sind. Besitzt nun jede der Faktorgruppen von A eine treue primitive Permutationsdarstellung, so erhält man alle möglichen Normalteiler als Kern einer maximalen Untergruppe. Letztere können in auflösbaren Gruppen (wie z.B. in [Eic1993] beschrieben) effizient bestimmt werden. Es genügt natürlich, die maximalen Untergruppen von A und ihre Kerne auszurechnen, um die Existenz primitiver Darstellungen der Faktorgruppen von A zu untersuchen.

Dies läßt sich ebenso auf maximale Untergruppen maximaler Untergruppen ausweiten, das folgende Lemma zeigt, daß sich damit für viele der zu betrachtenden Gruppen A die Normalteilerbestimmung vereinfacht:

(104) LEMMA: Ist $l \leq 7$, so sind alle Normalteiler aller möglichen A als Kerne maximaler Untergruppen maximaler Untergruppen von A zu erhalten. Dabei werden die iterierten maximalen Untergruppen nur für V_4, $F_{20}(5)$ und $F_{42}(7)$ benötigt.

Beweis: Nachrechnen. Die benötigten Tabellen der transitiven Gruppen finden sich in [BM1983], beziehungsweise [CHM]. □

Ist A dagegen nicht auflösbar, so müsste der Normalteilerverband von B berechnet werden, was die Bestimmung der Konjugiertenklassen von B bedingte. Für große A kann dies recht aufwendig werden. Wenn A nur wenige Normalteiler besitzt, ist es daher diesen Fällen günstiger, für alle möglichen Faktorgruppen A/N nach A/N-Quotienten von B zu suchen. Ein Algorithmus hierzu ist in V.5.6 beschieben. Der Aufwand dieses Algorithmus ist in etwa von der Klassenanzahl von A abhängig, die im Gegensatz zur Klassenanzahl der Anfangsstücke B konstant bleibt.

IV.3.3. Wir setzen wiederum wie in II.2.7: $C = N_{S_l}(A)$ und $D = N_{S_{\Omega_B}}(B)$. Dann können wir C und D nach Satz 39 als Untergruppen von $W = N_{S_l}(A) \wr S_m$ ansehen. Die Einschränkungen aus Lemma 28 und Corollar 29 sind bereits durch Berücksichtigung der Bedingungen K2 und K3 eingegangen.

Lemma 32 liefert weitere Konjugationsaussagen, die die Anzahl der zu betrachtenden Isomorphismen einschränken. Wählt man dabei aber ein beliebiges Repräsentantensystem der Doppelnebenklassen, so bleiben zwar Bedingungen K2 und K3 erfüllt, aber das Produkt ist nicht notwendigerweise minimal in seiner Klasse.

Um auch dies zu erreichen, müssen die erhaltenen subdirekten Produkte nachfolgend durch das minimale Element unter simultaner Konjugation mit den hierbei betrachteten „lokalen" Kernnormalisatoren $N_D(F)$ und $N_C(E)$ ersetzt werden. Da wir damit stets eine minimierende Konjugation nachschalten müssen, lohnt eine womöglich aufwendige Berechnung der Doppelnebenklassen in der Automorphismengruppe nicht. Wir betrachten daher lediglich ein Repräsentantensystem der Nebenklassen der von $N_C(E)$ induzierten Automorphismen. Dieses kann einmal zu Beginn für jeden Normalteiler $E \lhd A$ bestimmt werden. Wir konstruieren dann zu jedem der Repräsentanten eine Subpotenz und ermitteln nachfolgend den minimalen Repräsentanten unter Konjugation mit $N_D(F) \times N_C(E)$. Dabei kann es passieren, daß die gleiche Gruppe mehrfach konstruiert wird, das heißt, daß dieser minimale Vertreter bereits im bisher konstruierten Anteil der Liste der Subpotenzen enthalten ist. Er wird in diesem Fall natürlich nicht erneut aufgenommen.

IV.3.4. Abschließend muß noch Bedingung K4 überprüft werden. Dies geschieht durch Algorithmus (100). Produkte, die sich dabei als nicht kanonisch herausstellen, werden im folgenden ignoriert. Um in Fällen, in denen aus einer Klasse nur der kanonische Vertreter konstruiert wird, nicht unnütz den Kanonizitätstest durchzuführen, werden gemäß (14) zuvor eine Reihe von Konjugationsinvarianten von M bestimmt. Wurde bisher keine Gruppe konstruiert, die in diesen Invarianten übereinstimmt, so kann M probeweise als kanonisch angesehen werden. Wird später dann eine weitere Gruppe mit diesen Invarianten konstruiert, so muß M erst dann auf Kanonizität untersucht werden. Stellt sich dabei heraus, daß M nicht kanonisch war, so kann das neue M' in die Liste der probeweise als kanonisch angesehenen Gruppen aufgenommen werden, ansonsten muß es ebenfalls auf Kanonizität untersucht werden.

IV.3.5. Sind wir an den subdirekten Produkten nur zum Zwecke der Konstruktion transitiver Gruppen interessiert, so können wir außerdem alle diejenigen Subpotenzen M, die einen nicht transitiv operierenden Normalisator $N_{S_n}(M)$ besitzen und nicht mehr induktiv für die weitere Konstruktion benötigt werden (das heißt Gruppen, die auf allen Bahnen operieren) ignorieren, und brauchen sie nicht auf Kanonizität zu testen.

Gleiches gilt (wenn M nicht noch induktiv benötigt wird), wenn der Normalisator $N_{S_n}(M)$ ein Blocksystem mit Blöcken kleinerer Ordnung als die Länge der Bahnen aus $\mathcal{B}$ besitzt: Dieses ist auch Blocksystem für jede Untergruppe. Das der Konstruktion von M entsprechende Blocksystem $\mathcal{B}$ kann folglich allen aus M hervorgehenden Gruppen nicht zugehörig sein.

Diese beiden Schritte können den Rechenaufwand merklich reduzieren:

(105) Beispiel: Wir betrachten Subpotenzen von S_3. Anwendung des beschriebenen Algorithmus liefert 23 Klassen von Subpotenzen von Länge 4. Fordert man Transitivität des Normalisators, so verbleiben 9 Subpotenzen. Die Bedingung der Nichtexistenz von Blocksystemen mit kleineren Blöcken beläßt davon noch 7 Subpotenzen, der Kanonisierungsaufwand hat sich dabei in etwa gedrittelt.

IV.3.6. Wir fassen die Beschreibung der Konstruktion nochmals zusammen. Dabei sei die Y-Klasse von Untergruppen von Y mit dem Repräsentanten X mit $[X]_Y$ bezeichnet.

(106) Algorithmus: Gegeben sei eine transitive Permutationsgruppe $A \leq S_l$ und eine natürliche Zahl m. Dieser Algorithmus bestimmt kanonische Vertreter der Subpotenzen von A von Länge m.

1. [Faktorstruktur von A] Berechne $C := N_{S_l}(A)$ und
$$\mathcal{E} := \{E \lhd A \mid E \text{ klein unter } C\}.$$
Für $E \in \mathcal{E}$ sei $Au_E := \mathrm{Aut}(A/E)$ und
$$AuNo_E := \{\alpha \in Au_E \mid \alpha \text{ von } N_C(E) \text{ induziert}\}.$$
Schließlich setze ANK_E gleich einem Vertretersystem der Linksnebenklassen $Au_E/AuNo_E$.
2. [Test auf primitive Darstellungen der Faktorgruppen] Setze $PrimFaktDst := 0$. Ist A nicht auflösbar, so gehe zu Schritt 3. Ansonsten bestimme $\mathcal{U} := \{[U]_A \leq A \mid U \text{ maximal in } A\}$. Setze $\mathcal{K} := \{\bigcap_{a\in A} U^a \mid [U]_A \in \mathcal{U}\}$. Ist $\mathcal{E} \subseteq \mathcal{K}$, so setze $PrimFaktDst := 1$ und gehe zu Schritt 3. Andernfalls bestimme $\mathcal{V} := \{[V]_A \leq A \mid V \text{ maximal in } U \text{ für ein } [U]_A \in \mathcal{U}\}$. Setze $\mathcal{K} := \mathcal{K} \cup \{\bigcap_{a\in A} V^a \mid [V]_A \in \mathcal{V}\}$. Ist $\mathcal{E} \subseteq \mathcal{K}$, so setze $PrimFaktDst := 2$.
3. [Initialisierung der Subpotenzen] Setze $Länge := 1$ und $Subpotenzen(Länge) := \{A\}$.
4. [Schleife über die Länge] Wenn $Länge = m$, dann beende den Algorithmus. Ansonsten setze $Länge := Länge + 1$, $Subpotenzen(Länge) := \emptyset$ und $Vorläufig := \emptyset$.
5. [Schleife über Subpotenzen vorangegangener Länge] Für jedes $B \in Subpotenzen(Länge-1)$ durchlaufe Schritte 6-14:

6. [A/E-Quotienten] Ist A nicht auflösbar, so setze $\mathcal{F}$:=Kerne von A/E-Quotienten von B für ein $E \in \mathcal{E}$. Gehe zu Schritt 8.
7. [Normalteiler als Kerne maximaler Untergruppen] Ist $primFaktDst > 0$ so setze
$$\mathcal{U} := \{[U]_B \leq B \mid U \text{ maximal in } B\}.$$
Ist $primFaktDst > 1$, so setze
$$\mathcal{U} := \mathcal{U} \cup \{[V]_B \leq B \mid V \text{ maximal in } U \text{ für ein } [U]_B \in \mathcal{U}\}.$$
In jedem Fall setze
$$\mathcal{F} := \{\bigcap_{b \in B} U^b \mid [U]_B \in \mathcal{U}\} \cup \{B\}.$$
8. [Suche kleine Normalteiler] Setze $D := N_{C \wr S_{Laenge-1}}(B)$.
Setze $\mathcal{F} := \{F \in \mathcal{F} \mid F \text{ klein unter } D\}$. Für jedes $F \in \mathcal{F}$ durchlaufe 9-14.
9. [Schleife über Normalteiler mit isomorpher Faktorgruppe] Setze $\bar{\mathcal{E}} := \{E \in \mathcal{E} \mid B/F \cong A/E\}$. Für jedes $E \in \bar{\mathcal{E}}$ durchlaufe Schritte 10-14.
10. [Schleife über Automorphismen, die nicht von S_l stammen] Es sei $\chi_E \colon B/F \to A/E$ fest gewählter Isomorphismus. Für jedes $\alpha \in ANK_E$ durchlaufe Schritte 11-14.
11. [Subdirektes Produkt] Es sei M das subdirekte Produkt (als Permutationsgruppe vom Grad $Laenge \cdot l$) von B und A zu den Normalteilern $F \lhd B$ und $E \lhd A$, den natürlichen Homomorphismen zu diesen Normalteilern und dem Isomorphismus $\chi_E \cdot \alpha \colon B/F \to A/E$. Ersetze M durch sein minimales Konjugiertes unter der Operation von $N_D(F) \times N_C(E)$.
11. [Eigenschaftstests] Berechne $N := N_{C \wr S_{Länge}}(M)$. Ist $Länge = m$ und erfüllt N nicht die notwendigen Eigenschaften aus (IV.3.5), so gehe zu Schritt 15. (Ansonsten wird dieser Normalisator im nächsten Schleifendurchlauf in Schritt 8. benötigt, die Berechnung ist also nicht unnütz.)
12. [Invariantentest] Bestimme Konjugationsinvarianten von M gemäß (14). Stimmen diese mit den Invarianten eines $H \in Subpotenzen(Länge)$ überein, so gehe zu Schritt 14. Ist dies nicht der Fall und stimmen sie sogar mit den Invarianten von keinem $H \in Vorläufig$ überein, so setze $Vorläufig := Vorläufig \cup \{M\}$. Gehe zu Schritt 15.
13. [Kollision mit vorläufig kanonischem Element] Es sei $H \in Vorläufig$ derjenige Vertreter (es gibt nur einen!), der bezüglich der Konjugationsinvarianten mit M übereinstimmt.
Setze $Vorläufig := Vorläufig \setminus \{H\}$. Bestimme mit Algorithmus (100) den kanonischen Vertreter von H und teste damit implizit, ob H kanonisch ist. Ist dies der Fall, so setze $Subpotenzen(Länge) := Subpotenzen(Länge) \cup \{H\}$.
14. [Kanonizitätstest für M] Bestimme mit Algorithmus (100) den kanonischen Vertreter von M und teste damit implizit, ob M kanonisch ist. Ist dies der Fall, so setze
$Subpotenzen(Länge) := Subpotenzen(Länge) \cup \{M\}$.
15. [Schleifenende] Ende der Schleifen aus den Schritten 5,8,9 und 10.
16. [Eine Länge komplett]
Setze $Subpotenzen(Länge) := Subpotenzen(Länge) \cup Vorläufig$. Gehe zu Schritt 4.

Ist der Algorithmus beendet, so enthält $Subpotenzen(m)$ die Kanonischen Repräsentantensystem der W-Klassen von Subpotenzen von A von Länge m (die die Bedingungen aus (IV.3.5) erfüllen).

IV.3.7. In Fortsetzung von IV.2.13 soll jetzt die Konstruktion von Erweiterungen der Subpotenz $B := S_3 \perp S_3$ mit $A := S_3$ beschrieben werden. Zunächst (dies geschieht eigentlich ganz zu Beginn des Algorithmus) werden die Faktorgruppen und nötigen Automorphismen bestimmt: Es ist $C = N_{S_3}(A) = A$ und $\mathcal{E} = \{E_1 = \langle\rangle, E_2 = \langle a \rangle, E_3 = A\}$. Dann ist $N_C(E_i) = C$ und $ANK_{E_i} = \{\mathrm{id}\}$ für $i \in \{1, 2, 3\}$, da alle Automorphismen der (Faktor)gruppen bereits durch Konjugation mit C induziert sind. Weiterhin stellen wir fest, daß jede Faktorgruppe eine treue primitive Darstellung besitzt, es ist also $\mathit{primFaktDst} = 1$. Wir springen jetzt mit dem gegebenen B in Schritt 5 des Algorithmus. Da A auflösbar und $\mathit{primFaktDst} = 1$ ist, bestimmen wir Repräsentanten der maximalen Untergruppen von B als

$$\begin{aligned}\mathcal{U} =&\{\langle(a,1),(1,a)\rangle, \langle(b,b),(1,a)\rangle, \langle(b,b),(a,1)\rangle,\\ &\langle(b,b)(a,a)\rangle, \langle(b,b),(a,a')\rangle\},\end{aligned}$$

die uns die Normalteiler (in gleicher Reihenfolge)

$$\begin{aligned}\mathcal{F} =&\{F_1 = \langle(a,1),(1,a)\rangle, F_2 = \langle(1,a)\rangle, F_3 = \langle(a,1)\rangle,\\ &F_4 = \langle(a,a)\rangle, F_5 = \langle(a,a')\rangle\} \cup \{F_6 = B\}\end{aligned}$$

liefern. Nun ist $D := N_{C \wr S_2}(B) = C \wr S_2 = \langle(a,1),(b,1),(1,a),(1,b),\overline{(1,2)}\rangle$, und wir stellen fest, daß lediglich F_1,F_2,F_5 und F_6 klein unter D sind. Wir durchlaufen also diese Normalteiler:

Zu F_1 ist E_2 der einzige Normalteiler mit isomorpher Faktorgruppe. Da $ANK_{E_2} = \mathrm{id}$ ist, konstruieren wir nur ein subdirektes Produkt, und zwar $M_1 := \langle(a,1,1),(1,a,1),(1,1,a),(b,b,b)\rangle$ von Ordnung 54. Wir stellen fest, daß M_1 bereits minimal unter $N_D(F_1) \times N_C(E_2)$ ist. Wir gehen davon aus, daß B die erste Subpotenz von Länge 2 ist, die wir in der Schleife in Schritt 5 durchlaufen. Die Listen *Subpotenzen*$_3$ und *Vorläufig* sind daher leer. Wir merken uns daher M_1 in *Vorläufig*.

Zu F_2 ist E_1 der einzige Normalteiler mit isomorpher Faktorgruppe. Da $ANK_{E_1} = \mathrm{id}$ ist, ist $M_2 := \langle(a,1,a),(1,a,1),(b,b,b)\rangle$ das einzige zu konstruierende subdirekte Produkt. Auch M_2 ist bereits minimal unter $N_D(F_2) \times N_C(E_1)$. Da $|M_2| \neq |M_1|$ merken wir uns auch M_2 in *Vorläufig*.

Zu F_5 ist ebenfalls E_1 der einzige Normalteiler mit isomorpher Faktorgruppe und $M := \langle(1,a,a),(a,1,1),(b,b,b)\rangle$ das einzige zu konstruierende subdirekte Produkt. Der minimale Vertreter von M unter $N_D(F_5) \times N_C(E_1)$ ist $M_3 := \langle(a,1,a),(1,a,1),(b,b,b)\rangle$, was zufälligerweise gleich M_2 ist (Dies tritt auf, weil unsere Beispiele so klein sind). Wir stellen beim Invariantentest fest, daß M_3 mit einem Vertreter aus *Vorläufig* (und zwar M_2) in den Invarianten übereinstimmt. Wir müssen also zunächst M_2 auf Kanonizität testen, und stellen fest, daß es nicht kanonisch ist. (Der kanonische Vertreter von M_2 ist $\langle(a,a,1),(1,1,a),(b,b,b)\rangle$ und wird beim Ergänzen von $\mathrm{Diag}(S_3,S_3)$ erhalten.) Wir entfernen also M_2 aus der Liste *Vorläufig*.

Nun ist in Schritt 14 noch M_3 auf Kanonizität zu testen, natürlich (gleiche Gruppe) ist auch M_3 nicht kanonisch, und wird verworfen.

Als letztes betrachten wir $F_6 = B$. Der entsprechende Normalteiler ist E_3, die Subpotenz das direkte Produkt $M_4 := \langle (a,1,1),(1,a,1),(1,1,a),(b,b,1),(1,1,b)\rangle$. M_4 ist bereits klein unter $N_D(F_6) \times N_C(E_3)$, und wird ebenfalls in *Vorläufig* gespeichert.

Es verbleiben zunächst also M_1 und M_4. In der Tat sind beide Vertreter kanonisch und werden, nachdem auch die übrigen Subpotenzen von Länge 2 durchlaufen wurden, in *Subpotenzen*$_3$ übernommen. Würden wir in Schritt 11 auf Transitivität des Normalisators testen, so würden M_2, M_3 und M_4 noch vor den Kanonizitätstests verworfen.

IV.3.8. An dieser Stelle bietet es sich an, kurz auszuführen, wie man (mit im wesentlichen denselben Methoden) ein Repräsentantensystem der intransitiven Gruppen – und somit alle Untergruppen von S_n – bestimmen kann (Diese Listen werden jedoch schnell sehr lang und liefern nur wenig neue Information, so daß in diesem Kontext von der Ausführung abgesehen werden soll). Die Vorgehensweise lehnt sich dabei an II.2.5 an.

Ist G intransitiv auf $\Omega = \{1, \ldots, n\}$, so können wir G in der symmetrischen Gruppe so konjugieren, daß die Bahnen $\{\Omega_i\}$ in absteigender Länge angeordnet sind, die Projektionen auf die Bahnen jeweils der kanonische Vertreter der Klasse transitiver Gruppen sind und ansonsten bezüglich einer fest gewählten Anordnung $\preceq$ auf den Klassen transitiver Gruppen gilt, daß für $i < j$ mit $|\Omega_i| = |\Omega_j|$ gilt, daß $G|_{\Omega_i} \preceq G|_{\Omega_j}$ gilt.

Gruppen dieser Gestalt konnen wir nun so konstruieren, indem wir zunächst jeweils diejenigen Ω_i zusammenfassen, auf die G mit gleichem Bild projiziert. Die Projektion auf die Vereinigung dieser Ω_i ist dann eine Subpotenz von $G|_{\Omega_i}$. Solche Subpotenzen konstruieren wir wie beschrieben, wobei lediglich die Tests aus (IV.3.5) in Schritt 11 entfallen.

Die Subpotenzen zu verschiedenen transitiven Gruppen werden dann iteriert zu subdirekten Produkten zusammengefügt. Da die Projektionen mit verschiedenen Bildern aufgrund obiger Anordnungsbedingung nicht mehr vertauscht werden dürfen, beschränkt sich Konjuugation dabei auf den in II.2.7 betrachteten Fall. Wir können die subdirekten Produkte demnach mittels Satz (32) beschreiben.

Mittels einer Schleife über die möglichen Bahnlängen und -projektionen werden so alle intransitiven Gruppen konstruiert.

IV.4. Transitivitätsbedingungen

Bei der vorangegangenen Beschreibung wurde im wesentlichen nicht benutzt, daß eine Subpotenz Basis einer transitiven Gruppe sein soll. Der Konstruktionsprozeß soll nun so modifiziert werden, daß die Transitvitätsbedingungen aus Abschnitt III.4 berücksichtigt sind.

IV.4.1. Zunächst wiederholen wir einige notwendige Kriterien dafür, Basis einer transitiven Gruppe zu sein.

(107) LEMMA: Es sei M Subpotenz, die Basis einer transitiven Gruppe ist. Dann sind die M_i konjugiert und M ist in Parität.

<u>Beweis:</u> Unmitelbar aus (70) und (84). □

Wir können diese Tests durchführen, bevor wir den Normalisator von M in S_n (oder einem entsprechenden Kranzprodukt) berechnen. Weit interessanter sind für uns jedoch Aussagen, die uns gestatten, zu untersuchen, ob eine Subpotenz M von Länge k Anfangsstück einer Subpotenz in Parität sein kann, da wir damit den Konstruktionsbaum bereits an den Ästen, und nicht erst an den Zweigen beschneiden können.

Das 1. Anfangsstückkriterium (85) ist bereits von dieser Art, doch gibt es nur eine untere Schranke für die Signatur einer Ergänzung von M in Parität an. Diese Signatur legt jedoch wiederum Einträge dieser Ergänzung fest, welche allerdings ihrerseits wieder Einfluß auf die Signaturen bekommen können. Wir wollen daher eine Vorgehensweise beschreiben, die versucht, daraus die minimale Länge einer Ergänzung in Parität abzuschätzen. Stellen wir dann im Konstruktionsprozeß fest, daß wir eine Subpotenz erzeugt haben, für die die Länge einer Ergänzung in Parität größer als die zu erzeugende Länge m ist, so kann diese Subpotenz nicht zu einer für unsere Zwecke brauchbaren Subpotenz führen und folglich – ohne sie auch nur auf Kanonizität getestet zu haben – ignoriert werden.

IV.4.2. Zu einer Subpotenz M von Länge k betrachten wir die Matrix I der Blockkernprojektionsklassen $[M_i^j]$ von M. (Um Isomorphietests zu vermeiden, benutzen wir in der Praxis die Ordnungen der Normalteiler, siehe (73).) Um Aussagen über Ergänzungen von M zu erhalten, wollen wir diese Blockkernprojektionsklassenmatrix[1] erweitern, um mögliche Matrizen von Erweiterungen in Parität zu erhalten. Die Begriffe „Signatur" und „in Parität" seien in offensichtlicher Weise auf solche Matrizen ausgeweitet.

Wir wollen – soweit möglich – I zu einer $m \times m$-Matrix L ergänzen, die mögliche Matrix einer M ergänzenden Subpotenz in Parität ist. L soll also symmetrisch und in Parität sein, außerdem muß $\operatorname{sign}_i(I) \mid \operatorname{sign}(L)$ gelten.

Die möglichen Signaturen von L müssen nach (85) alle Vielfachen s von $\operatorname{kgV}_i(\operatorname{sign}_i(I))$ mit $\deg(s) \leq m$ durchlaufen.

Zu einem solchen s soll nun L mit $\operatorname{sign}(L) = s$ konstruiert werden. Dazu seien

$$r_i = \begin{cases} s / \operatorname{sign}_i(I) & \text{für } 1 \leq i \leq k \text{ und} \\ s & \text{sonst} \end{cases}$$

die Signaturen, die die möglichen zusätzlichen Einträge von L angeben. Die Eigenschaft, Matrix einer Subpotenz zu sein, erzwingt außerdem die folgenden Ergänzungs- und Endregeln:

- E1 Das Bild eines Kerns ist trivial: $L_{i,i} = [1]$,
- E2 Symmetrie: $L_{i,j} = L_{j,i}$.
- E3 Wird der Eintrag $L_{i,j} := [x]$ gesetzt, so wird r_i durch $r_i - 1 \cdot [w]$ ersetzt. (Aufgrund E2 muß dann auch $L_{j,i} := [x]$ gesetzt und r_j durch $r_j - 1 \cdot [x]$ ersetzt werden.)
- F1 Ergeben sich r_i's, die keine Signaturen sind (d.h. die negative Einträge besitzen), so kann der bisherige Ansatz nicht zu einer möglichen Matrix führen.
- E4 Besitzt r_i nur einen Primteiler (das heißt nach (80), daß $r_i = n \cdot [N]$ für ein $[N] \in \mathcal{N}$) so sind damit alle übrigen Einträge einer Zeile (auf diesen Wert) festgelegt.

[1] Die deutsche Sprache gestattet solche Wortungetüme. Der Lesbarkeit halber sei in diesen Abschnitten aber jetzt nur noch von „Matrix" die Rede.

Während die Indizes $\{1, \dots, k\}$ durch I bereits festgelegt sind, haben wir bei den übrigen Indizes Wahlfreiheit (die Kanonizität von Subpotenzen verbietet zwar Bahnvertauschungen, uns geht es aber nur um die potentielle Transitivität des Normalisators, die davon natürlich nicht beeinflusst wird). Daher dürfen wir ohne Beschränkung der Allgemeinheit auch noch die folgende Regel anwenden:

E5 Sind in einer Zeile (Spalte) alle Einträge zu bisher festgelegten Indizes festgelegt, so können wir an einer beliebigen noch nicht belegten Stelle dieser Zeile (Spalte) einen weiteren Eintrag (soweit durch das entsprechende r_i erlaubt) beliebig ansetzen und damit den entsprechenden Index festlegen.

Um nach solchen Festlegungen möglichst viele Folgerungen aus E4 zu erhalten, empfiehlt es sich, hierbei einen Eintrag zu wählen, der das entsprechende r_i in geringster Multiplizität teilt.

Mit diesen Regeln versuchen wir nun ein L mit $\mathrm{sign}(L) = s$ zu konstruieren. Mit Regeln E4 und E5 bestimmen wir, welche Einträge gesetzt werden. Das Setzen der Einträge geschieht dann mit Regeln E2 und E3. Diagonaleinträge sind nach E1 stets gleich [1]. Die Endregel F1 kann den Prozeß dabei womöglich abbrechen und die Unmöglichkeit einer entsprechenden Ergänzung zeigen.

Eine zweite Endregel können wir für den Fall, daß L vollständig konstruiert ist, angeben, diese folgt unmittelbar aus Lemma (77):

F2 Sind für einen Matrixeintrag X nicht alle der $\sim_X$-Klassen auf $\{1, \dots, m\}$ von gleicher Ordnung, so kann – da diese ein Blocksystem bilden müssen – L nicht Matrix einer Ergänzung mit transitiv operierendem Normalisator sein.

Diese Regel läßt sich natürlich auch dann anwenden, wenn – zur partiellen Konstruktion der transitiven Gruppen – die erlaubten Imprimitivitätsgebiete der Blockoperation bereits a priori eingeschränkt sind.

Gestatten diese Regeln nur eine partielle Konstruktion, so kann im Prinzip eine Backtrack-Suche mit probeweisen Einträgen in L (und Abbruch eines Zweiges, falls eine der Endbedingungen verletzt ist) alle möglichen Ergänzungen erzeugen. Da dies in der Praxis recht aufwendig ist, aber nur geringe zusätzliche Informationen liefert, verzichten wir darauf und nehmen in diesem Fall an, daß eine Ergänzung von M in Parität mit Signatur s existiert. (Mit anderen Worten: Wir verwerfen M nicht.)

(108) Bemerkung (Anfangsstückkriterium 2): Indem wir die möglichen s nun nach aufsteigendem Grad solange durchlaufen, bis wir die Existenz einer Ergänzung in Parität nicht mehr ausschließen können, erhalten wir eine untere Schranke für den Grad von Ergänzungen in Parität.

(109) Beispiel: In Fortsetzung von (105) betrachten wir nun fünffache Subpotenzen von S_3. Im naïven Konstruktionsprozeß werden dann alle 23 Subpotenzen von Länge 4 konstruiert und erweitert, während letztendlich nur 5 fünffache Subpotenzen verbleiben, die die Bedingungen aus IV.3.5 erfüllen. Bestimmt man jedoch für die (zuvor erhaltenen) Subpotenzen von Länge 4 jeweils Schranken für den minimalen Grad einer Erweiterung in Parität, und verwirft Subpotenzen, deren Schranke größer als 5 Bahnen ist, so verbleiben

nach einem Test auf das kgV der Signaturen nur 11 Subpotenzen, die weiterhin zu behandeln sind. Nach Anwendung des oben beschriebenen Algorithmus sind sogar nur 8 der 23 Subpotenzen von Länge 4 weiter zu behandeln. Als Beispiel betrachten wir die Subpotenz (in der Notation aus IV.2.13)

$$M = \langle (b,b,1,1),(a,a,1,1),(1,1,b,b),(1,1,a,1),(1,1,1,a)\rangle = \mathrm{Diag}(S_3,S_3)\times(S_3 \perp S_3).$$

Diese hat Ordnung 108. Die Matrix zu M ist (wir geben statt Normalteilerklassen nach (73) die Ordnung der Normalteiler an):

$$\begin{pmatrix} 1 & 1 & 6 & 6 \\ 1 & 1 & 6 & 6 \\ 6 & 6 & 1 & 3 \\ 6 & 6 & 3 & 1 \end{pmatrix},$$

woraus wir sofort ersehen, daß M nicht in Parität ist. Das kgV der Signaturen ist $2\cdot\mathbf{1}+1\cdot\mathbf{3}+2\cdot\mathbf{6}$, es besitzt Grad 5. Wir können also allein aufgrund des 1. Anfangsstückkriteriums (85) nicht ausschließen, daß M eine Erweiterung von Grad 5 in Parität besitzt. Nun wollen wir aber versuchen, eine solche Erweiterung zu konstruieren: Da die Signatur einer solchen Erweiterung durch das kgV bereits bestimmt ist, sind für alle Zeilen und Spalten die fehlenden Einträge vorgegeben, der Eintrag der rechten unteren Ecke muß wegen Regel E1 gleich 1 sein. Dies liefert

$$\begin{pmatrix} 1 & 1 & 6 & 6 & 3 \\ 1 & 1 & 6 & 6 & 3 \\ 6 & 6 & 1 & 3 & 1 \\ 6 & 6 & 3 & 1 & 1 \\ 3 & 3 & 1 & 1 & 1 \end{pmatrix},$$

was sich offenbar nicht in Parität befindet. Erst bei der Konstruktion von Subpotenzen von Länge 6 müssten wir M zunächst berücksichtigen: Der oben angegebene Algorithmus konstruiert für die potentielle Signatur $2\cdot\mathbf{1}+1\cdot\mathbf{3}+3\cdot\mathbf{6}$ die (partielle) Matrix (Nullen bezeichnen bisher nicht festgelegte Einträge)

$$\begin{pmatrix} 1 & 1 & 6 & 6 & 3 & 6 \\ 1 & 1 & 6 & 6 & 0 & 0 \\ 6 & 6 & 1 & 3 & 0 & 0 \\ 6 & 6 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

die ohne Backtrack mit obigen Regeln nicht mehr verbesserbar ist, weshalb hier die Existenz einer Erweiterung in Parität nicht mehr ausgeschlossen werden kann.

Überlegt man etwas, so stellt man fest, daß an Stelle (2,5) eine 6 stehen muß, da die 3 in der fünften Spalte bereits vergeben ist. (Algorithmisch wäre eine passende Regel aber schwierig zu formulieren, man müsste die einzelnen Einträge der Matrix durchlaufen und Zeilen und Spaltenrestriktionen gleichzeitig betrachten, was aufwendig ist. Daher wurde auf eine solche Regel verzichtet.) Ausprobieren liefert dann in der Tat eine Matrix in Parität, und zwar

$$\begin{pmatrix} 1 & 1 & 6 & 6 & 3 & 6 \\ 1 & 1 & 6 & 6 & 6 & 3 \\ 6 & 6 & 1 & 3 & 1 & 6 \\ 6 & 6 & 3 & 1 & 6 & 1 \\ 3 & 6 & 1 & 6 & 1 & 6 \\ 6 & 3 & 6 & 1 & 6 & 1 \end{pmatrix}.$$

Ein Backtrack hätte also in der Tat keine Verbesserung mehr geliefert.)

IV.4.3. Unabhängig von der Eliminierung nicht möglicher Anfangsstücke können wir die Signaturen auch dazu benutzen, die Menge der bei der weiteren Konstruktion zu berücksichtigenden Faktorgruppen zu verkleinern. Dazu betrachten wir eine Subpotenz M von Länge m wieder als subdirektes Produkt des Anfangsstückes $\underleftarrow{M}_{m-1}$ mit A. Nach (66) ist $E = M^m \pi_m$ der dazugehörige Normalteiler von A. Aus Bemerkung (61) folgt dann $E \subseteq \bigcap_{j \lneqq m} M_j^m$.

Angenommen sei nun, daß M in Parität ist und Signatur s besitzt. Dann bestimmt s (da stets $M_m^m = \langle 1 \rangle$ ist) die $[M_j^m]$ für alle $j \lneqq m$, wodurch die möglichen E eingeschränkt werden.

Ist nun s bereits durch die Signaturen von $\underleftarrow{M}_{m-1}$ eindeutig bestimmt (als kgV der Signaturen, beziehungsweise – falls $\underleftarrow{M}_{m-1}$ bereits in Parität ist – nach Untersuchung potentieller Signaturvielfacher wie in IV.4.2 beschrieben), so ist der Schnitt E der M_j^m dadurch stark eingeschränkt. So muß zum Beispiel seine Ordnung den ggT der Ordnungen der M_j^m teilen. Weitere Einschränkungen können sich aus dem Verband der Normalteiler von A ergeben.

IV.5. Moduln

IV.5.1. Ist A abelsch, so existiert eine besonders große Anzahl an subdirekten Produkten. In diesem Fall ist aber auch M abelsch. Die Konjugation mit Nebenklassenrepräsentanten induziert daher eine Operation der Faktorgruppe $T = G\varphi = G/M$ auf M; das heißt einen Homomorphismus $\alpha \colon T \to \operatorname{Aut}(M)$, $t \mapsto t\alpha$. Diesen Homomorphismus kennen wir aber a priori nicht, wenn wir die möglichen M erst suchen.

Nach Satz (37) bettet G außerdem in das Kranzprodukt $H \wr T$ ein (hierbei sei die sich natürlich ergebende Permutationsdarstellung von T bei Operation von G auf den Bahnen gewählt), wobei $H = \operatorname{Stab}_G(B_1)\psi \leq N_{S_l}(A) = C$ sei. Dies liefert einen anderen Homomorphismus $\beta \colon T \to \operatorname{Aut}(H^{\times m})$, $t \mapsto t\beta$, unter dem $A^{\times m}$ offenbar invariant ist. Diesen Homomorphismus kennen wir, sobald wir T kennen.

Nun sei angenommen, daß die folgende Bedingung erfüllt ist:

(110)

$$T\beta \text{ induziert } T\alpha, \text{ das heißt} \qquad \begin{array}{ccc} M & \overset{\iota}{\hookrightarrow} & A^{\times m} \leq H^{\times m} \\ t\alpha \downarrow & & \downarrow t\beta \\ M & \overset{\iota}{\hookrightarrow} & A^{\times m} \leq H^{\times m} \end{array} \qquad \text{kommutiert für alle } t \in T,$$

wobei ι die Einbettung von M in $A^{\times m}$ sei. Diese Bedingung impliziert also insbesondere, daß M unter $T\beta$ invariant ist. Die nachfolgenden Beispiele illustrieren diese Bedingung:

(111) BEISPIEL: Es sei

$$G = \langle (1,5)(2,6), (1,8,2,7)(3,5,4,6) \rangle \cong [2^2]4$$

transitiv von Grad 8 und von Ordnung 16. Dann ist

$$\mathcal{B} = \{\{1,2\},\{3,4\},\{5,6\},\{7,8\}\}$$

Blocksystem von G. (Der Name der Gruppe gemäß Anhang A entspricht nicht diesem Blocksystem!) Die Operation von G auf $\mathcal{B}$ ist

$$T = G\varphi = \langle (1,3), (1,4)(2,3) \rangle \cong D_8(4).$$

Der Kern dieser Operation ist

$$M = \langle (1,2)(3,4)(5,6)(7,8) \rangle,$$

Diese Gruppe besitzt nur triviale Automorphismen. Der Homomorphismus α ist also die Abbildung, der jedem $t \in T$ den trivialen Automorphismus von M zuordnet.

Gleichzeitig bettet G in

$$2 \wr T = W = \langle (1,2), K \rangle \text{ mit } K = \langle (1,5)(2,6), (1,7)(2,8)(3,5)(4,6) \rangle$$

ein. Ist

$$A^{\times 4} = \langle (1,2), (3,4), (5,6), (7,8) \rangle$$

der Basisnormalteiler von W, so ist durch das Komplement K der folgende Homomorphismus $\beta\colon T \to \mathrm{Aut}(A^{\times 4})$:

$$\begin{array}{rcl} (1,3) & \mapsto & \left(a \mapsto a^{(1,5)(2,6)} \mid a \in A^{\times 4}\right), \\ (1,4)(2,3) & \mapsto & \left(a \mapsto a^{(1,7)(2,8)(3,5)(4,6)} \mid a \in A^{\times 4}\right) \end{array}$$

definiert. Die Gruppe M ist unter $T\beta$ invariant und auf dieser Gruppe induziert jedes $t\beta$ den trivialen Automorphismus. Für jedes $t \in T$ ist also $t\beta|_M = t\alpha$, Bedingung (110) also erfüllt.

Die Bedingung (110) ist aber nicht stets erfüllt:

(112) BEISPIEL: Es sei

$$\begin{array}{rcl} G & = & \langle (1,18,14,11,7,6,3,16,13,10,9,5,2,17,15,12,8,4), \\ & & (2,3)(4,16)(5,17)(6,18)(7,14)(8,13)(9,15)(11,12) \rangle \end{array}$$

eine transitive Gruppe von Grad 18 und Ordnung 108. Die Partition

$$\mathcal{B} = \{\{1,2,3\},\{4,5,6\},\{7,8,9\},\{10,11,12\},\{13,14,15\},\{16,17,18\}\}$$

bildet ein Blocksystem von G. Die Operation auf den Blöcken ist also

$$T = \langle (1,6,5,4,3,2), (2,6)(3,5) \rangle.$$

Der Kern der Operation ist

$$\begin{aligned} M &= \langle (4,5,6)(7,9,8)(13,14,15)(16,17,18), \\ &\qquad (1,2,3)(7,9,8)(10,11,12)(16,17,18) \rangle \end{aligned}$$

von Ordnung 9. Der Stabilisator des Blockes $\{1,2,3\}$ ist

$$\begin{aligned} U &= \langle (1,2)(4,16,6,18,5,17)(7,13,8,15,9,14)(10,11), \\ &\qquad (2,3)(4,17,6,16,5,18)(7,15,8,14,9,13)(11,12) \rangle \end{aligned}$$

es ist also

$$H = U\psi = \langle (1,2),(2,3) \rangle.$$

Die Gruppe G bettet damit in

$$C_3 \wr T \cong W = \langle (1,2),(2,3),K \rangle$$

ein, wobei

$$\begin{aligned} T \cong K &= \langle (1,16,13,10,7,4)(2,17,14,11,8,5)(3,18,15,12,9,6), \\ &\qquad (4,16)(5,17)(6,18)(7,13)(8,14)(9,15) \rangle \end{aligned}$$

das Basiskomplement ist. Unter Konjugation mit K bleibt M aber nicht invariant. Der Konjugationshomomorphismus $\alpha\colon T \to \mathrm{Aut}(M)$ ist also nicht durch Konjugation mit K induziert.

Ist Bedingung (110) erfüllt, so impliziert dies, daß M unter der Operation von $T\beta$ – die wir a priori kennen – invariant ist. Als transitive Gruppe enthält T auch eine minimal transitive Untergruppe $\hat{T}$. Offenbar ist M dann auch unter $\hat{T}\beta$ invariant.

In diesem Fall erhalten wir M somit als unter der Operation von $\hat{T}\beta$ invarianten Untermodul von $A^{\times m}$.

IV.5.2. Sei nun eine Bahnlänge m und eine Operation A des Basisnormalteilers vorgegeben, für die wir a priori wissen, daß für jede transitive Gruppe, die ein entsprechendes Blocksystem mir Kern $\leq A^{\times m}$ besitzt (wir bezeichnen diese Klasse im folgenden mit $\mathcal{Q}$) die Bedingung (110) erfüllt sein wird. In diesem Fall durchlaufen wir mit $\hat{T}$ ein Repräsentantensystem der S_m-Klassen minimal transitiver Gruppen von Grad m und bestimmen für jedes $\hat{T}$ die unter $\hat{T}\beta$ invarianten Untergruppen von $A^{\times m} \leq A \wr \hat{T}$. Wir bezeichen ein Repräsentantensystem der $W = C \wr S_m$-Klassen dieser Untergruppen mit $\mathcal{I}$.

Ist nun $G \in \mathcal{Q}$ und $M \lhd G$ der Basisnormalteiler von G zu dem Blocksystem, desbezüglich G in $\mathcal{Q}$ ist, so ist M unter W zu einem Repräsentanten aus $\mathcal{I}$ konjugiert.

In diesem Fall umfasst $\mathcal{I}$ folglich ein Repräsentantensystem der Basisnormalteiler von Gruppen aus $\mathcal{Q}$. Wir brauchen diese Basisnormalteiler also nicht als Subpotenzen von A zu konstruieren, sondern erhalten ein Repräsentantensystem ihrer W-Klassen, indem wir diejenigen Untergruppen aus $\mathcal{I}$ auswählen, deren Normalisator in S_n transitiv auf $\{1,\ldots,n\}$ operieren. In dieser Situation liefert zu jedem $M \in \mathcal{I}$ dasjenige $\hat{T}$, unter dem M invariant ist, auch gleich einen nichttrivialen Anteil des Normalisators, der zur Verkürzung der Normalisatorberechnung benutzt werden kann.

IV.5.3. Die Bedingung (110) ist zum Beispiel erfüllt, wenn A in H zentral ist.

(113) LEMMA: Sei $A \leq Z(H)$. Dann gilt (110) für alle Subpotenzen M von A und alle T.

Beweis: Da $A \leq Z(H)$ ist auch

$$A^{\times m} \leq Z(H^{\times m}). \tag{114}$$

Die Gruppe M sei eine Subpotenz von A und G eine transitive Gruppe mit Basisnormalteiler M. Die durch Operation auf den Bahnen erhaltene Faktorgruppe G/M sei mit T bezeichnet. Für die Nebenklassen aus T in G sei ein Repräsentantensystem $\mathcal{A} = \{a_t\}_{t \in T} \subset G$ gewählt. Ausserdem bette G in $H \wr T$ ein, die Elemente des Basiskomplements seien mit $\{b_t\}_{t \in T}$ bezeichnet. Der Homomorphismus α bezeichnet Konjugation mit a_t, der Homomorphismus β Konjugation mit b_t. Da $M = H^{\times m} \cap G$ ist $\mathcal{A}$ auch ein Repräsentantensystem für die Nebenklassen von $H^{\times m}$ in $\langle G, H^{\times m} \rangle \leq H \wr T$, wobei wegen $T = G\varphi$ Gleichheit gilt. Somit ist $b_t = h_t a_t$ mit $h_t \in H^{\times m}$. Damit gilt aber für alle $m \in M$ und alle $t \in T$:

$$m^{t\alpha} = m^{a_t} = m^{h_t^{-1} b_t} = (m^{h_t^{-1}})^{b_t} \overset{(114)}{=} m^{b_t} = m^{t\beta},$$

was zu beweisen war. □

Da in den von uns betrachteten Fällen A nach III.2.4 transitiver Normalteiler der primitiven (da $\mathcal{B}$ minimal gewählt wurde) Gruppe H ist, tritt die Bedingung $A \leq Z(H)$ nur in solchen Fällen ein, wenn $A = H$ abelsch und primitiv und somit isomorph Z_p ist. Die Bedingung $A = H$ ist nach (49) zum Beispiel erfüllt, wenn $\mathrm{ggT}(|\mathrm{Stab}_T(1)|, [N_{S_l(A)} : A]) = 1$ gilt.

Da wir nach III.2.5 davon ausgehen können, daß T minimal transitiv ist, so erhalten wir damit die Aussage:

(115) LEMMA: Sind m und A derart, daß für alle minimal transitiven Gruppen $\hat{T}$ von Grad m die Ordnungen der Punktstabilisatoren $\left|\mathrm{Stab}_{\hat{T}}(1)\right|$ teilerfremd zu $[N_{S_l}(A) : A]$ sind (zum Beispiel wenn $\hat{T}$ regulär ist), so ist die Bedingung (110) für jede transitive Gruppe vom Grad m erfüllt.

(116) FOLGERUNG: Ist m prim, so ist die Voraussetzung von (115) erfüllt.

Beweis: Ist T transitiv von Primzahlgrad m, so enthält T ein Element t von Ordnung m, das durch einen m-Zykel dargestellt werden muß. Die zyklische Gruppe $\langle t \rangle$ ist somit (bis auf Konjugation) die einzige minimal transitive Gruppe von Grad m. Sie operiert regulär. □

Schließlich gilt offensichtlich:

(117) BEMERKUNG: Ist $l = 2$, so ist $A = H$ und damit (110) erfüllt.

IV.5.4. Wir beschreiben nun, wie wir in diesen Fällen die möglichen M als unter der Operation der $\hat{T}$ invariante Untergruppen von $A^{\times m}$ erhalten. Auch wenn die bisher hierbei betrachteten A zyklisch sind, werden wir dies nicht voraussetzen, um später auch andere Fälle betrachten zu können.

Wir durchlaufen mit $\hat{T}$ ein Vertretersystem der minimal transitiven Gruppen von Grad m, betrachten für jedes $\hat{T}$ dessen Operation auf $A^{\times m}$ durch Bahnpermutation, und bestimmen mit dem in V.8 beschriebenen Verfahren die unter dieser Operation von $\hat{T}$ invarianten Untergruppen von $A^{\times m}$.

(118) BEMERKUNG: Die Suche nach invarianten Untergruppen liefert alle Untergruppen, die unter der Operation eines Komplementes invariant sind. Als Basis kommen aber nur solche Gruppen in Frage, die bei Einschränkung auf einen (und aufgrund der Invarianzeigenschaft dann auf alle) der Bahnen mit Bild A projizieren. Dies bedeutet insbesondere, daß die Ordnung der Untergruppe von $|A|$ geteilt werden muß. Ist A zyklisch von Primzahlordnung, so ist diese Bedingung trivialerweise erfüllt.

Solche Bedingungen werden uns in dem in Abschnitt V.8 beschriebenen Algorithmus helfen, den Konstruktionsbaum in seinen Zweigen stark zu beschneiden. Erst durch diese Ergänzung wird die Invariantensuche für nicht zyklisches A wirklich praktikabel.

Allerdings liefern mehrere T möglicherweise die gleichen Untergruppen, auch können einige der erhaltenen Untergruppen noch in S_n konjugiert sein. Nach Lemma (94) sind diese Gruppen dann aber bereits in $W = C \wr S_m$ konjugiert.

Auch hier ersetzen wir darum wieder jede Untergruppe durch einen (im folgenden definierten) kanonischen Vertreter, und eliminieren Duplikate aus der Liste der kanonischen Vertreter. Diese Liste enthält dann Vertreter aller zu betrachtenden Subpotenzen.

Da die Konstruktion hier jedoch nicht bahnweise geschieht, ist die Definition der Kanonizität aus IV.2.2 an dieser Stelle nicht sinnvoll. Wir werden statt dessen einen anderen Kanonizitätsbegriff, der sich auf solche Untergruppen bezieht, definieren:

Kanonisierungsalgorithmus für kleine Gruppen

Es sei im folgenden $V \leq W$ eine Untergruppe von W, für die ein (einfach berechenbarer) kanonischer Vertreter unter W definiert werden soll. Dabei sei vorausgesetzt, daß V noch so klein ist, daß es möglich ist alle Elemente von V im Speicher zu halten. (In der von uns bisher betrachteten Situation ist V invariante Untergruppe von $A^{\times m}$ und W Kranzprodukt. Hierfür ist diese Bedingung erfüllt, so m nicht zu groß ist.)

Es sei $No = N_W(V)$. Ist der Normalisatorindex $[W : No]$ klein (d.h. die W-Bahnen kurz) so kann man einfach alle Konjugierten von V bestimmen und unter diesen einen minimalen (bezüglich einer beliebig definierten Ordnung, siehe V.1) Vertreter als kanonischen Repräsentanten von V auswählen.

Ist der Normalisatorindex dagegen groß, so soll ein kanonischer Vertreter von V elementweise konstruiert werden. Dabei benutzen wir, daß V hinreichend klein ist, um noch alle Elemente auflisten zu können.

(119) BEMERKUNG: Reguläre Gruppen sind nach Folgerung (10) genau dann in der vollen symmetrischen Gruppe konjugiert wenn sie isomorph sind. Sind diese Gruppen von kleiner Ordnung (was ein kleiner Grad automatisch impliziert), so reduziert sich der Isomorphietest meist auf die Untersuchung einiger weniger Invarianten. Ist V regulär und W die volle

symmetrische Gruppe, so empfiehlt es sich, die Gruppe anhand eines Kataloges (vergleiche [Neu1967]) zu identifizieren und eine standardisierte reguläre Permutationsgruppe von diesem Isomorphietyp als kanonischen Vertreter zu wählen.

IV.5.5. Nun wollen wir den Prozeß beschreiben, der elementweise einen – nur von der W-Klasse von V abhängigen – Vertreter dieser Klasse bestimmt. Wir wählen ein nichttriviales Element r_1 aus V aus, und suchen den minimalen Vertreter (bezüglich einer vorher definierten totalen Ordnung auf W. Für Permutationsgruppen kann man zum Beispiel Basebilder vergleichen, siehe V.1) Vertreter s_1 seiner W-Bahn. Bei Konjugation von r_1 auf s_1 geht V in eine Untergruppe V_2 über. Diese Untergruppe V_2 ist dabei bis auf Konjugation mit dem Zentralisator $C_W(s_1)$ bestimmt.

Unter den von s_1 verschiedenen Elementen von V_2 sei nun ein weiteres Element r_2 ausgewählt. Der minimale Vertreter seiner $C_W(s_1)$-Bahn sei s_2. Soll V, beziehungsweise V_2 so konjugiert werden, so daß r_1 auf s_1 und (das Urbild von) r_2 auf s_2 abgebildet wird, so ist das Bild V_3 bis auf Konjugation mit $C_{C_W(s_1)}(s_2)$ bestimmt. Das nächste Element r_3 wird nun so aus V_3 ausgewählt, daß es nicht im Erzeugnis $\langle s_1, s_2\rangle$ liegt.

Iteriert man diesen Prozeß bis die s_i ein Erzeugendensystem des Bildes bilden, so gelangt man schließlich zu einer zu V konjugierten Untergruppe U. Diese ist bis auf Konjugation mit Elementen, die alle Erzeuger zentralisieren, und damit eindeutig bestimmt. Allerdings ist sie von der Wahl der r_i abhängig. Um auch hiervon unabhängig zu werden (beziehungsweise die r_i so auszuwählen, daß die erhaltenen s_i unabhängig vom ursprünglichen V sind), teilen wir die Elemente von V, aus denen r_1 ausgewählt wird, in Klassen unter dem Normalisator $No = N_W(V)$ ein. Diese Klassen werden bezüglich Größe ansteigend sowie Zykelstruktur angeordnet. Beide Eigenschaften sind konjugationsinvariant, die Anordnung ist es somit ebenso. r_1 wird aus der ersten Klasse ausgewählt (Wir nehmen zunächst einmal an, daß diese „erste" Klasse durch die Anordnung bereits eindeutig gegeben ist). Diese Repräsentantenwahl beeinflußt dann offensichtlich nicht den minimalen Vertreter s_1. Nun wird No durch den Normalisator von V_2 im Zentralisator $C_W(s_1)$ ersetzt und eine neue Klasseneinteilung der zur Auswahl von r verbleibenden Elemente vorgenommen. Der Repräsentant r_2 wird nun wiederum aus der ersten Klasse ausgewählt. Dieses Vorgehen wird entsprechend zur Auswahl der weiteren r_i iteriert.

Sind zu einem Zeitpunkt mehrere Klassen von gleicher Ordnung und gleicher Zykelstruktur (und die „erste" Klasse somit nicht eindeutig), so müssen sie simultan berücksichtigt werden: Für jede Klasse wird ein Bild $\hat{s}_i$ bestimmt. Das minimale (bezüglich der gewählten Ordnung) Element darunter wird als s_i ausgewählt. Dies erzwingt ein minimales s_i, unabhängig von der Anordnung der Klassen.

Ein Problem tritt dabei nur auf, wenn *mehrere* Klassen zum selben minimalen Element führen („die Klassen fusionieren"). In diesem Fall müßten beide Möglichkeiten simultan weiterverfolgt und das letzendlich kleinere Ergebnis gewählt werden. Da dies zu einer aufwendigen Aufspaltung des Algorithmus führt, empfiehlt es sich in solchen Fällen die fusionierenden Klassen zunächst zu ignorieren und die r_i – so möglich – aus den verbleibenden oder nachrangigeren Klassen zu wählen. Dieser Fall tritt unabhängig von der Wahl des ursprünglichen V ein, die Entscheidung beeinflußt folglich nicht das Ergebnis des Prozesses. Da die Klassen durch Konjugation mit einer Teilmenge der operierenden Gruppe gebildet werden, ist die Auswahl des Klassenvertreters bei der Bestimmung des minimalen Konjugierten unerheblich; alle führen zum selben Ergebnis:

(120) SATZ: Wird V durch ein W-konjugiertes ersetzt, so ergeben sich die gleichen s_i. Das damit erhaltene U kann somit als kanonischer Vertreter der Konjugiertenklasse angesehen werden.

Fusionieren alle Klassen, so verbleibt (wenn man keine Rekursion einführen möchte) bei kleinem Index $[W : V]$ immer noch, den kanonischen Vertreter als minimales Element der W-Bahn von V zu definieren[2].

Die primäre Auswahl kleiner Klassen zu Beginn bedeutet, daß nur wenige Elemente auf Minimalität getestet zu werden brauchen. Im Verlaufe des Algorithmus verkleinert sich andererseits der iterierte Zentralisator sehr schnell, so daß die ursprüngliche Klassenlänge dann sekundär wird.

(121) BEMERKUNG: Da die von uns betrachteten Untergruppen recht klein sind, ist der Hauptaufwand bei dieser Kanonisierung die anfängliche Normalisatorberechnung.

(122) BEMERKUNG: Dieser Kanonisierungsalgorithmus kann zwar im Prinzip auf beliebige (Permutations)gruppen angewandt werden. Im allgemeinen Fall wird jedoch die Elementanzahl oder die Bahnlänge zu groß sein, als daß das Verfahren hierfür praktikabel wäre.

(123) BEMERKUNG: In der (hier unter anderem betrachteten) Situation, in der die Gruppe ein Vektorraum ist, genügt es natürlich, die Operation von W projektiv durchzuführen. Dies verringert die zu betrachtenden Bahnlängen.

IV.6. Weitere Invarianzfälle

IV.6.1. Es sollen einige weitere Fälle untersucht werden, in denen sich die möglichen Subpotenzen als invariant unter einer Operation der Faktorgruppe T auf $A^{\times m}$ herausstellen. Um überhaupt eine solche Operation zu erhalten, nehmen wir an, daß ein transitives G über M zerfällt, es gebe also ein Komplement K mit $G = M \rtimes K$.

Betten wir G nun wiederum nach (37) in $Z = C \wr T$ ein, so gilt $C^{\times m} \geq A^{\times m} \geq M = G \cap C^{\times m}$. Folglich schneidet K trivial mit $C^{\times m}$. Andererseits ist $G = \langle M, K \rangle$ und damit $Z = \langle C^{\times m}, K \rangle$. Die Gruppe K ist also Komplement zu $C^{\times m}$ in Z und M ist unter der Konjugationsoperation von K invariant. Da $A^{\times m}$ in $C^{\times m}$ normal ist und offensichtlich unter der reinen Bahnpermutationsoperation von T invariant bleibt ist auch $A^{\times m} \lhd Z$. Somit läßt sich die Operation von $K \leq Z$ auf $A^{\times m}$ einschränken und M ist somit ebenfalls invariante Untergruppe von $A^{\times m}$.

In diesem Falle können wir bei vorgegebenem T Repräsentanten für die möglichen M dadurch erhalten, daß wir ein Repräsentantensystem $\{K_i\}$ der Komplementklassen zu $C^{\times m}$ in $C \wr T$ bestimmen, und zu jedem K_i die unter der Konjugationsoperation invarianten Untergruppen von $A^{\times m}$ bestimmen.

[2]Damit konnten bisher alle auftretenden Fälle behandelt werden

Auch hier liefert das Komplement K_i wieder einen nichttrivialen Normalisatoranteil, der zur Backtrackverkürzung bei der Normalisatorberechnung verwandt werden kann.

IV.6.2. Ist A auflösbar, so können die möglichen M wiederum, wie in IV.5.4 beschrieben, als invariante Untergruppen bestimmt werden. Dabei sind lediglich statt der einzelnen $\hat{T}$ auch Repräsentanten K_i der übrigen Komplementklassen zu berücksichtigen, falls mehrere existieren. (Im nichtauflösbaren Fall ist dagegen der Grad l von A bereits größer so daß $\mathcal{B}$ nur aus relativ wenigen Bahnen besteht. Auch besitzen solche Gruppen nur verhältnismäßig wenige Normalteiler und Automorphismen, so daß der iterative Konstruktionsprozeß für Subpotenzen dort weniger zeitkritisch ist.) Von den so erhaltenen Gruppen können wiederum einige – wie bereits in IV.5.4 bemerkt – konjugiert sein. Hierfür gelten die Kriterien aus (14) (Diese unterscheiden im abelschen Fall nicht so gut, weshalb wir sie dort nicht explizit erwähnt haben). Sind solche Gruppen klein genug, daß die Elementliste im Speicher gehalten werden kann, so kann mittels des Algorithmus aus (IV.5.4) wiederum der kanonische Repäsentant bestimmt werden.

IV.6.3. Nun soll ein Kriterium angegeben werden, wann für jede transitive Gruppe G, die M als Basis besitzt, ein Komplement in G zu M existiert. Zunächst einmal können wir gemäß III.2.5 davon ausgehen, daß $T = G\varphi$ minimal transitiv ist, da sich beim Übergang von G zu $H \leq G$ mit $M \lhd H$ und $H\varphi$ minimal transitive Untergruppe von $G\varphi$ die Basis M selber nicht ändert.

Sind nun $|A|$ und $|T|$ teilerfremd, so existiert nach dem Satz von SCHUR und ZASSENHAUS [Hup1967, I.18.1] ein solches Komplement.

Gilt sogar, daß $\mathrm{ggT}(|C|, |T|) = 1$, so folgt bei Anwendung von SCHUR/ZASSENHAUS auf das Kranzprodukt aufgrund der ebenfalls (unter Verwendung des Satzes von FEIT und THOMPSON folgenden [Hup1967, Satz I.18.3]) gelieferten Konjugation aller Komplemente, daß T als einziger Repräsentant einer Komplementklasse berücksichtigt werden muß. Da wir G jedoch nur in $C \wr T$ und nicht notwendigerweise in $A \wr T$ einbetten können, folgt dies nicht schon falls $|A|$ und $|T|$ teilerfremd sind.

Ist T in regulärer Darstellung, so liefert ein Satz von P. M. NEUMANN, C. H. HOUGHTON und J. A. H. SHEPPERD [Neu1964] ebenfalls die Konjugation aller Komplemente im Kranzprodukt.

Existieren mehrere Klassen von Komplementen, so genügt es natürlich, nur Repräsentanten ihrer Klassen unter Konjugation mit $N_{S_n}(A^{\times m}) = C \wr S_m$ zu betrachten, da diese Konjugation nur zu in $C \wr S_m$ konjugierten Klassen invarianter Untergruppen führt.

IV.6.4. Wir wollen noch eine Variante der beschriebenen Situation betrachten. Dabei sei nicht angenommen, daß ein transitives G über einem Basisnormalteiler M zerfällt, sondern daß dies nur für einen Faktor von M gilt: Die Gruppe A sei Erweiterung des transitiven p-Normalteilers N (wobei p eine Primzahl ist) mit der Faktorgruppe F, wobei p nicht die Ordnung von F teilt. Mit anderen Worten: N ist die normale p-Sylowgruppe von A. Wir können dann $A^{\times m}$ als Erweiterung von $N^{\times m}$ mit $F^{\times m}$ auffassen. Jeder Subpotenz M von A läßt sich dementsprechend ein N-Anteil $M_N := M \cap N^{\times m} \lhd M$ zuordnen. Dann ist M_N die p-Sylowgruppe von M, also insbesondere charakteristisch.

Nun sei G eine transitive Gruppe, die M als Basis bezüglich des Blocksystems $\mathcal{B}$ besitzt. Dann ist folglich $M_N \lhd G$. Zusätzlich sei angenommen, daß $|G/M|$ und $|F|$ teilerfrend sind. Folglich existiert ein Komplement $H/M_N \leq G/M_N$ zu M/M_N. Dessen Urbild unter dem natürlichen Homomorphismus zu M_N sei mit H bezeichnet. Diese Untergruppe H permutiert die Bahnen aus $\mathcal{B}$, so wie G es tut, also insbesondere transitiv. Andererseits projiziert M auf jede Bahn mit Bild A. Da $N \leq A$ existiert folglich für jedes $u \in N$ und für jede Bahn ein Element der Form $e = (\ldots, u, \ldots) \in M \leq A^{\times m}$, das bei Projektion auf die betreffenden Bahn das Bild u liefert. Da $\mathrm{ggT}(|N|, |F|) = 1$ können wir ohne Einschränkung annehmen, daß auch die Einträge zu den übrigen Bahnen aus N sind. Dies bedeutet, daß das Element e aus M_N ist, was wiederum impliziert, daß M_N auf jede Bahn mit Bild N projiziert. Daher ist M_N auf allen Bahnen aus $\mathcal{B}$ transitiv (da N transitiv gewählt war).

Folglich ist H eine transitive Gruppe von gleichem Grad wie G, deren Basis zum Blocksystem $\mathcal{B}$ gleich M_N ist. Als Normalteiler von G ist M natürlich auch unter der Konjugationsoperation von $H \lneqq G$ invariant.

Geht es um die Konstruktion der möglichen M, so können wir nach III.2.5 wiederum annehmen, daß $G\varphi \cong G/M$ minimal transitiv von Grad m ist. Um die obigen Überlegungen anwenden zu können, setzen wir voraus, daß für alle minimal transitiven T von Grad m die Ordnungen $|T|$ und $|F|$ teilerfremd sind.

Dann existiert nach obigen Überlegungen für jedes transitive G mit minimal transitiver Blockoperation T eine echte transitive Untergruppe $H \leq G$, deren Basis zum Blocksystem $\mathcal{B}$ eine Subpotenz von N ist.

(124) Beispiel: Diese Voraussetzungen sind für eine ganze Reihe primitiver Gruppen vom affinen Typ erfüllt. Als (kleinstes) Beispiel soll der Fall $A = S_3$ mit $l = 3$ dienen. Hier ist $p = 3$, $N = A_3$ und $F = C_2$. Ist nun $m = 9$, so sind alle minimal transitiven Gruppen von Grad 9 regulär. Also ist $\mathrm{ggT}(|T|, |F|) = 1$ für jedes minimal transitive T von Grad 9.

Wir nehmen nun an, daß wir *alle* Gruppen, die eine Subpotenz von N als Basis besitzen, bereits bestimmt haben. Die Menge dieser Gruppen sei mit $\mathcal{H}$ bezeichnet. Dabei seien insbesondere auch solche Gruppen, die einem anderen Blocksystem zugehörig sind, eingeschlossen. Bestimmen wir alle Gruppen von Grad $n = lm$, so ist diese letzte Annahme nicht unvernünftig. Aus den Gruppen aus $\mathcal{H}$ wählen wir eine Teilmenge $\mathfrak{H}$ aus, so daß jedes $H \in \mathcal{H}$ eine Untergruppe besitzt, die permutationsäquivalent zu einer Gruppe $H' \in \mathfrak{H}$ ist.

Dann ist jedes mögliche M (bis auf Äquivalenz) unter einem $H \in \mathfrak{H}$ bezüglich der natürlichen Konjugationsoperation von H invariant. Haben wir ein mögliches $\mathfrak{H}$ bestimmt (was im wesentlichen mit Methoden aus IV.11.2 geschehen kann), so können wir mit den bereits beschriebenen Invarianzmethoden daraus ein Repräsentantensystem der möglichen M bestimmen. Eine Betrachtung von Komplementen kann entfallen, da nicht die Blockoperation, sondern die natürliche Permuattionsoperation der $H \in \mathfrak{H}$ betrachtet wird.

IV.6.5. Es stellt sich die Frage ob die Bestimmung der als Basisnormalteiler möglichen Subpotenzen von A auch in weiteren Fällen auf Invarianz dieser Basisnormalteiler unter gewissen, von der Permutationsdarstellung der möglichen Faktorgruppen induzierten, Automorphismen zurückgespielt werden kann. So ist in [But1993] angenommen, daß im Falle eines Blocksystems von m Blöcken mit m prim die Gruppe G stets ein nur aus

p-Zykeln bestehendes Element f (welches als p-Zykel auf den Blöcken operiert) besitzt, die Kerne also als unter solchen Operationen invariante Untergruppen bestimmt werden können. Diese Annahme ist aber nicht haltbar, wie das folgende Beispiel zeigt:

(125) BEISPIEL: Es sei

$$\begin{aligned} G = \langle &(2,4,6,8,10,12,14), \\ &(1,6,13,8)(2,9,12,5)(3,4,11,10)(7,14), \\ &(1,11,9)(2,4,8)(3,5,13)(6,12,10), \\ &(1,13)(2,12)(3,11)(4,10)(5,9)(6,8)\rangle \end{aligned}$$

vom Typ $[\frac{1}{6}{}_{-}F_{42}(7)^2]2_2$ die 22. transitive Gruppe von Grad 14 (gemäß der Anordnung in [But1993], zur Nomenklatur siehe Anhang A). Diese Gruppe hat Ordnung 588. Dann ist

$$\{\{1,3,5,7,9,11,13\},\{2,4,6,8,10,12,14\}\}$$

das einzige Blocksystem von G. Der Kern M der Darstellung auf den Blöcken hat Index 2. Der Kern dieser Darstellung ist eine Subpotenz von Länge 2 der primitiven Gruppe $F_{42}(7)$ von Grad 7, die gemeinsame Faktorgruppe ist abelsch von Ordnung 6, wobei allerdings – dies erklärt das Minuszeichen – der nichttriviale Automorphismus von Z_6 dazwischengeschaltet wurde.

Nachrechnen in GAP liefert, daß G nur zwei Konjugiertenklassen außerhalb M besitzt, die Repräsentanten beider Klassen haben Ordnung 4. Die Gruppe ist also nicht semidirektes Produkt mit Normalteiler M, sondern die zweite Potenz jedes Elementes von $G \setminus M$ liegt in M.

G besitzt also insbesondere kein Element f mit oben beschriebenen Eigenschaften.

Nichtsdestotrotz stellt sich heraus, daß die Listen in [But1993] korrekt sind. So enthält der Normalisator $N = N_{S_{14}}(M)$ des Kernes ein Element f mit beschriebenen Eigenschaften. Dieses Element liegt aber nicht in G. Ähnliche Beobachtungen kann man bei anderen Graden machen:

(126) BEISPIEL: Es sei $m = 6$ und $A = S_3$. Die minimal transitiven Gruppen von Grad 6 sind $C(6)$,$D_6(6)$, beide von der Ordnung 6, $A_4(6)$ von der Ordnung 12 und $F_{36}(6)$ von der Ordnung 36. Wir können also nicht von der Existenz von Komplementen ausgehen. Eine Verwendung des angegebenen Algorithmus liefert 22 unter einem Basiskomplement der Kranzprodukte invariante Untergruppen von $S_3^{\times 6}$. Von diesen besitzen 4 einen Normalisator in S_n, der ein Blocksystem mit Blöcken von Ordnung 2 besitzt. Die hierzu gehörenden transitiven Gruppen werden daher bei Blockgröße 2 erhalten, es verbleiben also 18 Gruppen. Eine Konstruktion der möglichen Basen als Subpotenzen von S_3 (wobei Gruppen, deren Normalisator Blöcke von Ordnung 2 besitzt, bereits im Konstruktionsprozess ausgesondert wurden) liefert genau diese 18 Typen. Auch hier hätte die Invarianzmethode (obgleich ihre Anwendung nicht gerechtfertigt ist) ein korrektes Ergebnis geliefert.

Diese Beobachtungen führen unmittelbar zu der Frage, ob man die Fälle, in denen man die Kerne auf diese Weise als invariante Untergruppen erhält, a priori erkennen, und den Algorithmus in solchen Fällen entsprechend verkürzen kann.

IV.6.6. Gibt es transitive Gruppen G mit minimal transitiver Blockoperation $T = G\varphi$, für die nicht notwendigerweise ein Komplement zum Basisnormalteiler $M \lhd G$ existiert, so ist der – im allgemeinen schnellere – Zugang, die möglichen Basisnormalteiler als invariante Untergruppen zu erhalten, nicht mehr möglich. In diesem Fall kann man das Vorgehen aus III.2.5 überspitzen, und statt einer minimal transitiven Gruppe T eine – nicht mehr transitive – Untergruppe $U \leq T$ betrachten, so daß das volle Urbild $M \leq F \leq G$ von U unter $\varphi|_G$ über M zerfällt. Dann ist jedes M zu T invariant unter U. Gute Kandidaten für U sind Sylowgruppen oder π-Hallgruppen zu geeigneten Primzahlen, so daß $\operatorname{ggT}|A|, |U| = 1$ gilt.

Bestimmt man nun alle U-invarianten Untergruppen von $A^{\times m}$, so kann es jedoch sein, daß einige der dabei erhaltenen invarianten M keine transitive Operation gestatten. Daher können – zusätzlich zu den Filtern aus Bemerkung (118) – diejenigen M ignoriert werden, für die der Normalisator nicht transitiv auf den Bahnen von M operiert. Dies kann zunächst mit den Kriterien aus Abschnitt IV.4 geschehen, wodurch in vielen Fällen bereits eine Normalisatorberechnung eingespart werden kann. Operiert der Normalisator transitiv, so ist die Vorgehensweise wieder wie im Fall der Invarianz unter einer transitiven Gruppe.

Natürlich könnte man auch versuchen, für U die triviale Gruppe zu setzen, und alle Untergruppen der direkten Potenz von A auf transitive Operation des Normalisators zu testen. Dies wird aber für gewöhnlich durch die schiere Fülle an Untergruppen unmöglich gemacht:

(127) BEISPIEL: Das direkte Produkt $S_4 \times S_4 \times S_4$ besitzt 6558 Klassen von Untergruppen, deren Ordnung durch 24 teilbar ist (was nach (118) eine notwendige Einschränkung ist). Eine Untersuchung all dieser Gruppen auf transitive Normalisatoroperation wäre bereits recht aufwendig. Hingegen sind Subpotenzen der Länge 3 von S_4 noch ohne Probleme auszurechnen.

Dieses Beispiel zeigt bereits, daß es nicht sinnvoll sein kann, U zu klein zu wählen.

IV.7. Verwendung von Blocksystemen der Faktorgruppe

Sind alle minimal transitiven Gruppen von Grad m imprimitiv, so folgt aus Corollar (89), daß alle möglichen Kerne M als verschachtelte Subpotenz darstellbar sind. Wir wollen diese Eigenschaft dazu benutzen, um in diesem Fall die Konstruktion der M zu vereinfachen.

Es sei O eine (möglichst klein gewählte) Menge natürlicher Zahlen, so daß jede minimal transitive Gruppe von Grad m ein Blocksystem mit Blöcken von Ordnung $o \in O$ besitzt. Existieren mehrere Alternativen für O, so sei diejenige gewählt, für die die $o \in O$ möglichst klein sind, um die Automorphismengruppen klein zu halten.

Die möglichen M sind folglich verschachtelte Subpotenz von einer Stufe aus O. Konstruieren wir also alle (Konjugiertenklassen von) verschachtelten Subpotenzen von Stufen aus O, so schöpfen wir damit die Klassen möglicher M aus. Probleme ergeben sich alleine daraus, daß eine Subpotenz auf ganz verschiedene Weise verschachtelt sein kann. Zunächst soll aber beschrieben werden, wie die bisherigen Algorithmen an die Konstruktion verschachtelter Subpotenzen adaptiert werden können:

IV.7.1. Um ein Repräsentantensystem der verschachtelten Subpotenzen von Stufe o zu erhalten, benötigen wir zunächst eine Liste aller möglichen Projektionen Y der zu bestimmenden Basisnormalteiler auf die Vereinigung von Bahnen, die durch einen Block indiziert sind. Diese erhalten wir als Subpotenzen von A von Länge o, die wie in IV.3 konstruiert werden, wobei lediglich der Filterung von Gruppen mit feineren Blocksystemen entfällt, während die sonstigen Transitivitätstests aufgrund (93) durchgeführt werden.

Für jedes Y werden nun die Subpotenzen von m/o Kopien von Y konstruiert. Hierfür können wiederum die Methoden aus IV.3 benutzt werden. Prinzipiell könnten auch die Invarianzmethoden aus IV.5 verwendet werden (letzteres für die möglichen Operationen minimal transitiver Gruppen von Grad m auf Blöcken von Ordnung o). Da die Operation des Urbilds des zu Y gehörenden Blockstabilisators auf Y allerdings nicht a priori bekannt ist, scheint dies im wesentlichen nur im Fall praktikabel zu sein, daß m/o zu $(lo)!$ (die Operation des Urbildes des Blockstabilisators operiert treu auf lo Punkten) teilerfremd ist.

Bei dieser Konstruktion fordern wir wiederum eine mögliche transitive Operation auf den Kopien von Y. Die Bedingungen aus IV.4 übertragen sich für die jeweils zu Blöcken zusammengefassten Bahnen.

Gleichzeitig können wir die konstruierten Gruppen aber immer noch als Subpotenzen von A auffassen und auch diesbezüglich die Blockprojektionsmatrix ausrechnen. Auch hierauf können die Bedingungen aus IV.4 angewandt werden. Dies liefert im allgemeinen einen besseren Filter, da diese (größere) Matrix feiner unterscheidet. Dabei müssen wir lediglich berücksichtigen, daß die Länge der Subpotenzen sich zwischen den beiden Interpretationen um einen Faktor o ändert.

Die in IV.3.5 erwähnten Bedingungen müssen dagegen leicht modifiziert werden. Transitive Operation des Normalisators betrifft den Normalisator N von M in S_n (beziehungsweise $C \wr S_m$), nicht den beim verschachtelten Konstruktionsprozeß entstehenden (möglicherweise kleineren) Normalisator in $N_{S_{lo}}(Y) \wr S_{m/o}$. Insofern ist eine Berechnung beider Normalisatoren notwendig.

Anstatt nur kleinere Blocksysteme zu betrachten, muß getestet werden, ob die Gruppe auf andere Weise bereits als verschachtelte Subpotenz konstruiert wurde. Dies ist aufwendiger und soll im folgenden untersucht werden.

IV.7.2. Da von den Bahnen des Normalisators N von M nicht notwendigerweise auf mögliche Verschachtelungen geschlossen werden kann, müssen wir potentiell alle möglichen Partitionen untersuchen. Davon gibt es sehr viele:

(128) Lemma: Es gibt

$$\frac{n!}{(k!)^{n/k}\left(\frac{n}{k}\right)!}$$

Partitionen von m Punkten in k-elementige Teilmengen.

Beweis: Wir wählen die ersten k Punkte für den ersten Block aus, dann die nächsten k Punkte aus den verbliebenen Punkten und so weiter. Dies gibt

$$\binom{m}{k}\cdot\binom{m-k}{k}\cdots\binom{k}{k}=\prod_{i=0}^{k-1}\binom{m-ik}{k}=\prod_i\frac{(n-ik)!}{k!(n-ik-k)!}$$
$$=\prod_i\frac{(n-ik)!}{k!(n-(i+1)k)!}\quad\overset{\text{Teleskopprodukt}}{=}\quad\frac{n!}{(k!)^{n/k}}$$

Möglichkeiten. Da die Anordnung der Blöcke jedoch nicht interessiert, ist schließlich durch $(n/k)!$ zu teilen. □

Offensichtlich liefern zwei Partitionen aber dieselbe Gruppe, wenn sie unter der Operation des Normalisators aufeinander abgebildet werden. Folglich genügt es, ein Repräsentantensystem der Normalisatorklassen der Partitionen zu betrachten, die sich aus der Operation R des Normalisators auf den Bahnen $\mathcal{B}$ von M ergeben.

IV.7.3. Da wir nach Partitionen suchen, bezüglich derer M als Verschachtelung konstruiert werden kann, brauchen wir nur solche zu betrachten, für die jeweils die Restriktion von M auf die Vereinigung aller durch Blöcke induzierten Teilmengen von Bahnen vom gleichen Typ ist.

Um den Fall mehrerer möglicher Partitionen zu behandeln, benutzen wir, wie schon in (41), Anordnungen:

(129) DEFINITION: Eine Partitionierung $\mathcal{C}$ von $\mathcal{B}$ heiße *schön* für M, wenn gilt:

- S1 M wird als Verschachtelung bezüglich $\mathcal{C}$ erhalten.
- S2 M wird nicht als Verschachtelung bezüglich eines Blocksystems mit kleineren Blökken erhalten.
- S3 Unter allen verbleibenden Partitionen gleicher Ordnung ist der Typ der Operation von M auf einem Block für $\mathcal{C}$ minimal.
- S4 Unter allen verbleibenden Partitionen ist die kanonische Form von M minimal als Subpotenz des kanonischen Vertreters der Subpotenz, die Bild der Restriktion von M auf die Bahnen zu einem Blocks aus $\mathcal{C}$ ist.

(130) BEMERKUNG: Liefern zwei Partitionen in Bedingung S4 die gleiche kanonische Form, so liegen diese Partitionen in einer Bahn unter dem Normalisator von M. Eine schöne Partitionierung ist insofern M als Verschachtelung eindeutig zugeordnet. Berücksichtigt man bei der Konstruktion nur verschachtelte Subpotenzen, die zu schönen Blocksystemen der Gruppe gehören, so entledigt man sich der in IV.7.1 erwähnten Duplikate.

IV.7.4. Für die Konstruktion benötigen wir damit noch einen Test, ob ein – beziehungsweise welches – Blocksystem schön ist. Zu einem gegebenen M betrachten wir alle möglichen Stufen in Reihenfolge von wachsendem o und brechen den folgenden Prozeß ab, sobald Bedingungen S1, S3 und S4 erfüllt sind (dies erfüllt S2). Als nächstes bestimmen wir ein Repräsentantensystem der N-Bahnen auf Partitionen in Blöcke von Ordnung o und wählen (um S1 zu erfüllen) daraus diejenigen aus, die auf allen durch Blöcke indizierten Bahnmengen mit gleichem Typ operieren. Diesen Typ bestimmen wir anhand der Liste aller möglichen Z durch Filterung nach Konjugationsinvarianten gemäß (14). Verbleiben mehrere Kandidaten, so müssen die Projektionen gemäß IV.2.14 kanonisiert werden, der Typ wird dann durch direkte Suche des kanonisierten Konjugierten in der Liste ermittelt.

Verbleiben dabei Partitionen zu verschiedenen Typen von Y, so werden (für Bedingung S3) nur diejenigen zum minimalen Typ weiter betrachtet. Ist dieser minimale Typ kleiner als der, zu dem die Verschachtelung konstruiert wurde, so kann diese Verschachtelung verworfen werden.

Für jede verbleibende Partitionierung $\mathcal{C}$ wird (durch Kanonisierung der einzelnen Projektionen) M jeweils per Konjugation in die in IV.2.1 definierte Normalform gebracht und nachfolgend (bezüglich $\mathcal{C}$) wie in IV.2.14 kanonisiert. Das Bild dieser Kanonisierung ist die kanonische Form zu $\mathcal{C}$. (Ist $\mathcal{C}$ das Blocksystem zu dem M als Verschachtelung konstruiert wurde, so können all diese Kanonisierungen entfallen.)

Die minimale kanonische Form (da wir ein Repräsentantensystem der Normalisatorbahnen gewählt haben, kann es nach (130) nur eine minimale geben), die zur kleinstmöglichen Blockgröße gefunden wird, bestimmt das schöne Blocksystem für M.

IV.7.5. Konstruiert man Subpotenzen als Verschachtelungen, so stellt man in der Praxis fest, daß es – insbesondere für kleine m – aufwendiger ist, Verschachtelungen zu konstruieren, als direkt Subpotenzen zu konstruieren. Der Grund hierfür ist, daß bei Verwendung von Verschachtelungen Subpotenzen von größeren Gruppen (die ihrerseits wieder Subpotenz sind) konstruiert werden müssen. Dabei wachsen insbesondere die Automorphismengruppen der Faktorgruppen sehr schnell. Diese Automorphismengruppen sind aber nach Satz (32) Teil einer Parametrisierung der Subpotenzen als subdirekte Produkte. Nun kann die folgende Situation auftreten:

Es sei Y Subpotenz von A, der Einfachheit halber von Länge 2. (Für größere Längen gibt es analoge Beispiele.) Es sollen Subpotenzen von Y von Länge l_1 konstruiert werden um Subpotenzen von A von Länge $2l_1$zu erhalten. Wir betrachten nun die Situation der Ergänzung einer Subpotenz B von Y von kleinerer Länge l_1-1, die als Anfangsstück dienen soll. Würden wir Subpotenzen von A konstruieren, so würden wir zunächst alle möglichen subdirekten Produkte von B und A konstruieren (diese sind Subpotenzen von Länge $2l_1-1$), und von diesen viele gemäß der Transitivitätsbedingungen aus IV.4 verwerfen. Von den verbleibenden Gruppen würden wiederum subdirekte Produkte mit A gebildet.

Bildet man dagegen sofort subdirekte Produkte von B mit Y, so sorgt die größere Automorphismengruppe dafür, daß zunächst *mehr* Subpotenzen konstruiert werden. Betrachten wir diese aber wieder als Subpotenzen von A, so stellt sich heraus, daß viele davon Erweiterungen von solchen Subpotenzen von Länge $2l_1 - 1$ sind, die verworfen worden wären. Das größere Y bewirkt also, daß *seltener* Transitivitätstests durchgeführt werden und dementsprechend der Konstruktionsbaum nicht so wirksam beschnitten wird.

Dies führt insbesondere bei kleinen m zu Problemen. Für größere m ist es aber so, daß die Konstruktion der Subpotenzen als Verschachtelungen insgesamt weniger Anfangsstücke kleinerer Längen erzeugt und dadurch den Konstruktionsprozess beschleunigt.

Konsequenterweise ist es schwierig, für gegebenes A und m zu entscheiden, ob Subpotenzen als Verschachtelungen konstruiert werden sollen. Die Entscheidung hierüber muß unter anderem die Ordnungen der Automorphismengruppen von Faktorgruppen der Subpotenzen Y, sowie die Effizienz der Algorithmen zum Rechnen in diesen Automorphismengruppen berücksichtigen und muß im Zweifelsfall von Benutzer getroffen werden. Als Regel soll hier nur festgehalten werden, daß für $m = 4$ keine Verschachtelungen konstruiert werden, da sich in diesem Fall der beschriebene Nachteil besonders extrem auswirkt.

IV.8. Bestimmen aller Kerne

In diesem Abschnitt soll die Beschreibung der Konstruktion der möglichen Kerne damit abgeschlossen werden, daß beschrieben wird, wie letzendlich die in den vorangegangenen Abschnitten beschriebenen Methoden ausgewählt werden, um alle möglichen Kerne für Blocksysteme einer vorgegebenen Ordnung zu erhalten. Zu Beginn bestimmen wir die möglichen Projektionen A. Wie gehabt sei $n = l \cdot m$, das Blocksystem bestehe aus m Blöcken von Ordnung l.

(131) ALGORITHMUS: Bestimme alle Kerne zu Blockgröße $l = n/m$.

1. [Gruppen kleinerer Grade] Setze $minops :=$ Menge der minimal transitiven Gruppen von Grad m (siehe IV.11.2) und

2 [Bestimmen aller möglichen Blockprojektionen]

$$\textit{mögliche\_A} := \bigcup_{P \in prim} \left\{ N \lhd P \mid [P:N] \;\Big|\; |\mathrm{Stab}_T(1)| \text{ für ein } T \text{ transitiv von Grad } m \right\}$$

3 [Schleife] Für jedes $A \in \textit{mögliche\_A}$ bestimme die Kerne zu A mittels Algorithmus (132)

Schritt 2 berücksichtigt dabei die Indexbedingung aus (49). Die folgenden beiden Algorithmen beschreiben nun im wesentlichen die Methodenauswahl zur Konstruktion der Subpotenzen. Hierbei sollte man jedoch die Bemerkungen aus IV.7.5 im Hinterkopf behalten: Die angegebenen Heuristiken haben sich in den behandelten Fällen als brauchbar erwiesen, jedoch ist es möglich, daß sie für höhere Grade geändert werden müssten. Insbesondere die Entscheidung, ob es sich lohnt, Invarianz unter echten Untergruppen zu benutzen, dürfte hiervon betroffen sein.

(132) ALGORITHMUS: Bestimme die Kerne zu A

1. [lokaler Normalisator] Berechne $C := N_{S_l}(A)$.
2. Wenn A primitiv ist, dann setze $erlaubteT := minops$ und gehe zu Schritt 4, ansonsten
3. [Minimal mögliche Blockoperationen] Setze $minprim$:= Menge der minimal primitiven U mit $A < U \leq C$. Setze $erlaubteT$:= Repräsentantensystem derjenigen T von Grad m, für die ein $U \in minprim$ existiert, so daß $[U:A] \;\big|\; |\mathrm{Stab}_T(1)|$. Setze $minErlaubte$:= diejenigen $T \in erlaubteT$ die bis auf Äquivalenz minimal bezüglich Inklusion sind (mit den gleichen Methoden wie in IV.11.2).
4. [Zentraler Fall] Falls A abelsch ist und für alle $T \in minops$ gilt, daß

$$\mathrm{ggT}(|\mathrm{Stab}_T(1)|, [C:A]) = 1 \quad \text{ist,}$$

dann bestimme die Kerne als unter $minops$ invariante Moduln gemäß IV.5. Ende.

5. [Komplementfall] Falls für alle $T \in minops$ gilt, daß $\mathrm{ggT}(|T|, |A|) = 1$ ist, dann setze $Operanden := minops$ und gehe zu 7.

6. [partielle Komplemente] Teste mit Algorithmus (133), ob es sich lohnt, Invarianz unter nichttransitiven Untergruppen zu benutzen. Wenn nicht, dann gehe zu 8. Ansonsten erhält man aus diesem Test eine Liste $intransops$ intransitiver Gruppen.
   Setze $Operanden{:=}intransops$.
7. [Invariante Untergruppen] Für jedes $T \in Operanden$ bestimme ein Repräsentantensystem der $C \wr S_l = N_{S_n}(A^{\times m})$-Klassen von Komplementen zu $C^{\times m}$ in $C \wr T$. Für jeden der Repräsentanten T' dieser Komplementklassen bestimme die unter T' invarianten Untergruppen von $A^{\times m}$ und bestimme deren kanonische Vertreter gemäß IV.6. Dies sind Vertreter der möglichen Kerne. Ende.
8. [Test auf Verschachtelungen] Bestimme für alle $T \in minops$ die Ordnungen möglicher Blocksysteme. Ist $m = 4$, oder ist eines der T primitiv, oder sollen keine Verschachtelungen benutzt werden (siehe IV.7.5), so gehe zu 12.
9. Bestimme eine Menge O natürlicher Zahlen, so daß jedes $T \in minops$ ein nichttriviales Blocksystem mit Blöcken einer Ordnung $o \in O$ besitzt (siehe IV.7).
10. Es sei $maxO := \max_{o \in O} o$. Bestimme alle Subpotenzen von A von Länge bis zu $maxO$, ohne dabei auf eine mögliche transitive Operation zu achten.
11. Bestimme die Kerne als Verschachtelungen für alle Stufen $o \in O$ für alle in 10 erhaltenen Subpotenzen von Länge o gemäß IV.7. Ende.
12. Bestimme die Kerne als Subpotenzen von A von Länge m.

In Schritt 5 und Schritt 8 würde es genügen, nur solche $T \in minops$ zu berücksichtigen, so daß für jedes $\tilde{T} \in erlaubteT$ bis auf Äquivalenz ein $T \leq \tilde{T}$ gewählt ist. Dies bringt aber kaum Verbesserungen und erschwert die Beschreibung.

(133) Algorithmus: Bestimme für gegebene A, $C = N_{S_l}(A)$ und vorgegebene minimal transitive Blockoperationen $minops$, ob es sich lohnt, Invarianz unter intransitiven Untergruppen zu betrachten, und bestimme in diesem Fall auch eine Liste $intransops$ der zu benutzenden intransitiven Untergruppen.

1. [Koprime Teiler] Bestimme für jedes $T \in erlaubteT$ die Menge P_T derjenigen Primzahlen, die $|T|$, aber nicht $|A|$ teilen.
2. [Gleiche Primteiler] Wenn für ein $T \in erlaubteT$ die Menge P_T leer ist, dann lohnt es sich nicht (nur triviale Untergruppe möglich). Ende.
3. [intransitive Untergruppen] Bestimme für jedes T eine Untergruppe $S_T \leq T$, so daß jeder Primteiler von $|S|$ in P_T liegt: Ist T auflösbar, so wähle die P_T-Hallgruppe, ansonsten die größte p-Sylowgruppe für ein $p \in P_T$. Setze $intransops := \{S_T\}$.
4. [Test] Wenn jedes $S_T \in intransops$ höchstens 3 Bahnen auf $\{1, \ldots, m\}$ besitzt, dann lohnt es sich, Invarianz unter den Gruppen aus $intransops$ zu benutzen.

IV.9. Konstruktion der Gruppen aus den Normalteilern

Zu einer gegebenen Subpotenz M einer Gruppe A soll nun ein Repräsentantensystem der dazugehörigen transitiven Gruppen bestimmt werden (so es solche gibt). Wir setzen wiederum $C = N_{S_l}(A)$, $W = C \wr S_m$ und $N = N_W(M)$. Die Operation von N auf der Menge $\mathcal{B}$ der Bahnen von M sei mit φ, der Kern mit $K = \operatorname{Kern} \varphi$ bezeichnet. Die zu M gehörigen transitiven Gruppen $G \geq M$ erhält man gemäß III.3.1 über N/M-Klassen von Komplementen S/M zu K/M, wobei $K \leq S \leq N$ und $S\varphi \leq N\varphi$ transitiv auf $\mathcal{B}$ sei. Gruppen, die mehrere „gleichartige" Blocksysteme besitzen, werden nach III.3.3 möglicherweise mehrfach erzeugt. Für diese müssen dann nachfolgend noch Konjugationstests durchgeführt werden.

Die Vorgehensweise der Konstruktion der G ist entsprechend III.2.6. Wir geben die notwendigen Schritte kurz im Zusammenhang an und führen sie danach expliziter aus.

(134) ALGORITHMUS: Konstruktion aller aus M hervorgehenden transitiven Gruppen.

1 Bestimme den Normalisator $N = N_W(M)$. Ist dieser nicht transitiv, oder erlaubt er Blocksysteme mit kleineren Blöcken als die Bahnlänge von M, so braucht dieses M nach IV.3.5 nicht berücksichtigt zu werden.

2 Bestimme den Kern K der Operation von N auf der Menge $\mathcal{B}$ der Blöcke.

3 Berechne Repräsentanten der Konjugiertenklassen transitiv auf $\mathcal{B}$ operierender Untergruppen $S/K \leq N/K$.

4 Berechne Komplementklassen zu K/M in S/M und deren Fusion unter $N_{N/M}(S/M)$ (siehe IV.9.7).

5 Wähle aus den so erhaltenen Gruppen diejenigen aus, denen $\mathcal{B}$ zugehörig ist.

6 Wenn $\mathcal{B}$ mehreren Gruppen zugehörig ist, die jeweils mehrerere Blocksysteme mit zu M äquivalentem Kern und äquivalenter Faktorgruppe besitzen, so müssen diese Gruppen aufgrund III.3.3 nachfolgend noch auf Konjugation getestet werden.

Die Normalisatorberechnung für Schritt 1) ist genauer in V.6 beschrieben; Schritt 2) wirft keine Probleme auf und kann mit Standardalgorithmen durchgeführt werden.

IV.9.1. Für Schritt 3) wird zunächst die Operation R von N auf $\mathcal{B}$ bestimmt. Zu diesem R sollen nun die Konjugiertenklassen transitiver Untergruppen bestimmt werden. Wir können nach Schritt 1) annehmen, daß R transitiv operiert.

Ist R klein, so läßt sich ohne Probleme der Untergruppenverband bestimmen, und aus diesem ein Repräsentantensystem der transitiv operierenden Untergruppen bestimmen.

(135) BEMERKUNG: In der Praxis stellt sich bei der Bestimmung der transitiven Gruppen bis Grad 30 heraus (siehe VI.2), daß R entweder kleiner als 5000 ist, oder aber in eine der Klassen fällt, für die im folgenden explizit Klassenrepräsentanten der transitiven Untergruppen bestimmt werden.

Die Untergruppen S erhält man schließlich als volle Urbilder der transitiven Untergruppen unter dem vom Blockhomomorphismus induzierten Homomorphismus $\bar{\varphi}$.

IV.9.2. Es verbleibt somit, das Problem für große transitive Untergruppen der S_m zu lösen. Für S_m selbst setzen wir die Existenz einer solchen Liste bereits nach III.1.1 voraus, zur Behandlung anderer großer Untergruppen betrachten wir zunächst die maximalen Untergruppen von S_m:

(136) SATZ ([LPS1987]): Es sei U maximale Untergruppe von S_m. Dann ist U von einer der folgenden Gestalten:

a) $S_a \times S_b$ mit $m = a + b$ und $a \neq b$;

b) $S_a \wr S_b$ mit $m = a \cdot b$, $a, b > 1$ Kranzprodukt wie in II.3.2;
c) $AGL_a(p)$ mit $m = p^a$ und p Primzahl;
d) $V^{\times a}(\mathrm{Out}\, V \times S_a)$ mit V nichtabelsch einfach, $a \geq 2$ und $m = |V|^{a-1}$
e) $S_a \wr S_b$ in "product action", $m = a^b$, $a \geq 5$ und $b > 1$;
f) $V \lhd U \leq \mathrm{Aut}(V)$ mit V nichtabelsch einfach, $\neq A_m$ und U operiert primitiv.
g) A_m.

Gruppen in Fall a) sind intransitiv, Fall d) kann erst bei Grad 60 und Fall e) erst bei Grad 25 auftreten, die beide jenseits unseres angesetzten Suchraumes liegen. Die vorkommenden affinen Gruppen sind allesamt hinreichend klein, daß die Klassen transitiven Untergruppen durch Bestimmung des Untergruppenverbandes gewonnen werden können. Wir wollen diese Fälle daher nicht gesondert berücksichtigen.

(137) BEMERKUNG: Eine Inspektion der einfachen Gruppen zeigt, daß Fall f für $n \leq 15$ nur für die folgenden V eintreten kann (zur Namensgebung siehe Anhang A):

$$L(6), L(7), L(8), L(9), A_5(10), L(10), L(11), M(11), A_5(12), L(2,11),$$
$$M_{11}(12), M(12), L(13), L_7(14), L(14), A_5(15), A_6(15), A_7(15), L(15).$$

Von diese Gruppen sind nur 7 von Ordnung größer 1000. Außerdem listet der ATLAS [CCN$^+$1985] die maximalen Untergruppen dieser Gruppen auf, so daß es genügt, für diese maximalen Untergruppen zunächst die transitiven Untergruppen zu bestimmen und lediglich eine nachträgliche Fusion unter der Gruppe durchzuführen. Ähnliches gilt dann für die möglichen U. Ebenso kann man im Prinzip auch für größere n verfahren.

Schließlich sei bemerkt, daß für beliebiges m der Index in S_m primitiver Gruppen, welche nicht A_m enthalten, mindestens $\left[\frac{n+1}{2}\right]!$ ist [Bor1889]. Die größten der zu berücksichtigen Untergruppen werden daher zumeist Kranzprodukte sein.

IV.9.3. Das folgende Lemma gestattet, die Klassen transitiver Untergruppen von Normalteilern von kleinem Index zu bestimmen, sofern diese für die Gruppe bekannt sind:

(138) LEMMA: Es sei $\mathcal{L}$ ein Repräsentantensystem der Klassen transitiver Untergruppen von G und $H \lhd G$ mit $[G:H] = p$ prim. Es sei

$$\mathcal{K} = \bigcup_{\substack{L \in \mathcal{L} \\ L \leq H}} \bigcup_{t \in Y_L} L^t \qquad \text{mit} \qquad Y_L = \begin{cases} \{id_G\} & \text{falls } N_G(L) \not\leq H, \\ X(H \backslash G) & \text{sonst,} \end{cases}$$

wobei $X(H\backslash G)$ ein Repräsentantensystem von $H\backslash G$ sei. Dann ist $\mathcal{K}$ Repräsentantensystem der Klassen transitiver Untergruppen von H.

<u>Beweis:</u> Es sei $L \in \mathcal{L}$. Da $H \lhd G$ sind entweder alle, oder keine Konjugierten von L Untergruppen von H. Die G-Klasse von L steht in Bijektion zu $N_G(L)\backslash G$, die H-Klasse in Bijektion zu $N_H(L)\backslash H$. Ist $N_G(L) \not\leq H$, so ist (da $[G:H]$ prim) $\langle N_G(L), H\rangle = G$ und damit (Isomorphiesatz)

$$[N_G(L) : N_H(L)] = [G:H] = p.$$

Also ist $[G : N_G(L)] = [H : N_H(L)]$ und damit $\left|L^G\right| = \left|L^H\right|$, die G-Klasse also gleich der H-Klasse.

Andernfalls ist $N_G(L) = N_H(L)$, die H-Klasse also kleiner als die G-Klasse. In diesem Fall faktorisiert das Vertretersystem $N_G(L)\backslash G$ durch H, Konjugation mit Repräsentanten aus $X(H\backslash G)$ liefert Vertreter der verschiedenen H-Klassen. □

Dieses Lemma liefert als Anwendung unmittelbar die Klassen transitiver Untergruppen der alternierenden Gruppen:

(139) Folgerung (Klassen transitiver Untergruppen von A_m): Es sei $T \leq S_m$ transitiv. Dann enthält A_m Konjugiertenklassen vom Typ T genau dann, wenn T gerade (even) ist. A_m enthält eine Konjugiertenklasse genau dann, wenn der Normalisator von T in S_m ungerade Elemente enthält. (Ansonsten existieren zwei Klassen, die bei Konjugation mit einem ungeraden Element in S_m ineinander übergehen.)

IV.9.4. Da die übrigen interessierenden maximalen Untergruppen allesamt Kranzprodukte sind, klassifizieren wir die Konjugiertenklassen ihrer transitiven Untergruppen. Dabei seien x und y natürliche Zahlen mit $xy = m$. Es sei $Z = S_x \wr S_y$. Das der Kranzproduktstruktur von Z entsprechende Blocksystem von Z sei $\mathcal{B}$.

(140) Satz: Es sei T transitiv von Grad m. Dann stehen die Z-Konjugiertenklassen von Untergruppen $V \leq Z$, die äquivalent zu T sind, in Bijektion zu den Bahnen von $Q = N_{S_m}(T)$ auf den Blocksystemen von T mit Blöcken von Ordnung x.

Repräsentanten der Klassen erhält man durch Konjugation von T mit solchen Elementen, die jeweils ein Blocksystem aus der Bahn auf $\mathcal{B}$ abbilden.

Beweis: Aus dem Einbettungssatz von Krasner und Kaloujnine (37) folgt, daß Z genau dann zu T äquivalente Untergruppen besitzt, wenn T ein passendes Blocksystem besitzt. Die Menge aller zu T äquivalenter Untergruppen V von Z entspricht den verschiedenen Einbettungen von T in Z. Wir nehmen daher ohne Beschränkung der Allgemeinheit an, daß (durch geeigntete Konjugation, beziehungsweise feste Wahl einer Einbettung) bereits $T \leq Z$ gilt.

Nun seien $T' \leq Z$ eine weitere Untergruppe und $g \in S_m$ mit $T^g = T'$. Z induziert auf T und T' jeweils das Blocksystem $\mathcal{B}$. Daher ist $\mathcal{C} = \mathcal{B}^{(g^{-1})}$ ebenfalls Blocksystem von T. Da Z als volles Kranzprodukt Stabilisator von $\mathcal{B}$ in S_n ist, ist $g \in Z$ genau dann, wenn $\mathcal{B} = \mathcal{C}$ gilt.

Zu zwei Blocksystemen $\mathcal{C}$ und $\mathcal{C}'$ von T mit Blöcken von Ordnung x seien $h, h' \in S_m$ mit

$$\mathcal{C}^h = \mathcal{B}, \qquad \mathcal{C}'^{h'} = \mathcal{B}. \tag{141}$$

Ist nun $q \in Q$ ein T normalisierendes Element und $\mathcal{C}^q = \mathcal{C}'$ so ist

$$\mathcal{B} = \mathcal{C}'^{h'} = \mathcal{C}^{qh'} = \mathcal{B}^{(h^{-1}qh')}$$

und somit $z = h^{-1}qh' \in Z$. Damit ist

$$T^{h^z} = T^{hz} = T^{qh'} = \overset{q\in Q}{=} T^{h'},$$

Die Bilder von T unter h und h' sind also unter Z konjugiert.

Sind umgekehrt T^h und $T^{h'}$ in Z mittels $z \in Z$ konjugiert und $\mathcal{C}$ und $\mathcal{C}'$ gemäß (141) definiert, so folgt mit analoger Rechnung daß $\mathcal{C}^{hzh'^{-1}} = \mathcal{C}'$ gilt und $hzh'^{-1} \in Q$ ist.

Ist also

$$\mathcal{T} = \{T^g \mid T^g \leq Z, \quad g \in S_m\}$$

die Menge aller in S_m zu T konjugierten Untergruppen von Z, so entsprechen die Z-Bahnen auf $\mathcal{T}$ den Q-Bahnen auf den Blocksystemen von T. Ist $\mathcal{B}_1, \ldots, \mathcal{B}_r$ ein Repräsentantensystem der Q-Bahnen und $g_i \in S_m$ mit $\mathcal{B}_i^{g_i} = \mathcal{B}$, so sind die $T_i = T^{g_i}$ ein Repräsentantensystem der Z-Bahnen auf $\mathcal{T}$, was zu zeigen war. □

IV.9.5. Mit Hilfe dieses Satzes wollen wir nun auch die Klassen transitiver Untergruppen weiterer großer Kranzprodukte (oder ihrer maximalen Untergruppen) beschreiben. So sind zum Beispiel eine Reihe großer Untergruppen des Kranzproduktes (wie etwa $S_x \wr A_y$) in $S_x \wr S_y$ normal, so daß hierfür Lemma (138) anwendbar ist.

(142) Bemerkung: Ist $X \leq S_x$ und $Y \leq S_y$, so bettet $X \wr Y$ (bei der Konstruktion dieses Kranzproduktes fassen wir Y explizit als Permutationsgruppe auf $\{1, \ldots, y\}$ auf, auch wenn einige Punkte von Y festgelassen werden) in natürlicher Weise in Z ein: Wir betten den Basisnormalteiler $X \times \cdots \times X$ komponentenweise in $S_x \times \cdots \times S_x$ ein und bilden das Erzeugnis mit Y, das als Teilmenge des Basiskomplements S_y aufgefasst wird.

Um die Schreibweise zu vereinfachen, definieren wir:

(143) Definition: Ist $T \leq S_\Omega$ transitiv, $\mathcal{C}$ eine Partition von Ω, $X \leq S_\Gamma$ für ein $\Gamma \in \mathcal{C}$ und $Y \leq S_{\mathcal{C}}$, so nennen wir T vom *Blocktyp* $(\mathcal{C}, X, Y)$, falls

i) $\mathcal{C}$ ein Blocksystem von T ist.
ii) Die Operation von T auf dem Blocksystem $\mathcal{C}$ äquivalent zu einer Untergruppe von Y ist und
iii) die Operation eines Blockstabilisators von T auf seinem Block äquivalent zu einer Untergruppe von X ist.

(144) Bemerkung: Aufgrund Bedingung i) und der Transitivität von T ist die Auswahl des Blockes $\Gamma \in \mathcal{C}$ irrelevant.

(145) Bemerkung: Die Aussage von Satz (37) besagt, daß ein transitives $T \leq S_m$ genau dann zu einer Untergruppe von $X \wr Y$ äquivalent ist, wenn es für ein Blocksystem $\mathcal{C}$ vom Blocktyp $(\mathcal{C}, X, Y)$ ist.

Beweis: Ist T von diesem Blocktyp, so folgt die Aussage unmittelbar aus (37) und der Einbettung von Kranzprodukten nach (142). Um die Umkehrung zu sehen, wählt man $\mathcal{C}$ als das zum Kranzprodukt gehörige Blocksystem. □

Die folgende Definition sieht sehr technisch aus, soll aber im wesentlichen in Fortsetzung von (36) nur eine Normalform für transitive Untergruppen eines Kranzproduktes definieren.

(146) DEFINITION: Es seien $X \leq S_x$ und $Y \leq S_y$ transitive Permutationsgruppen, $\mathfrak{R}_X$ sei ein Repräsentantensystem der X-Klassen transitiver Untergruppen von X und $\mathfrak{R}_Y$ ein ebensolches für Y. Das Kranzprodukt $X \wr Y$ operiere gemäß (36) und wir erhalten so einerseits eine Bijektion ϖ des Blocksystems $\mathcal{B}$ des Kranzproduktes zu $\{1, \ldots, y\}$, andererseits für jedes $\mathrm{B} \in \mathcal{B}$ eine Bijektion ς_{B} von B zu $\{1, \ldots, x\}$. Eine transitive Untergruppe $T \leq X \wr Y$ heiße *sauber* bezüglich $(\mathcal{B}, \mathfrak{R}_X, \mathfrak{R}_Y)$, wenn gilt:

- Die Operation von T auf $\mathcal{B}$ ist bezüglich ϖ aus $\mathfrak{R}_Y$.
- Für jeden Block $\mathrm{B} \in \mathcal{B}$ ist die Operation des Blockstabilisators T_{B} auf B bezüglich ς_{B} aus $\mathfrak{R}_X$.

In Erweiterung von (143) sagen wir von einer transitiven Gruppe T sie sei *sauber vom Blocktyp* $(\mathcal{B}, X, Y, \mathfrak{R}_X, \mathfrak{R}_Y)$, wenn T vom Blocktyp $(\mathcal{B}, X, Y)$ und außerdem sauber bezüglich $(\mathcal{B}, \mathfrak{R}_X, \mathfrak{R}_Y)$ ist.

(147) BEMERKUNG: Offenbar besitzt jede transitive Untergruppe von $X \wr Y$ auch ein sauberes $X \wr Y$-Konjugiertes.

Nun sei $\widehat{S_y}$ das Basiskomplement in Z. Die Abbildung

$$\phi\colon Z \to \widehat{S_y} \tag{148}$$

sei über den natürlichen Homomorphismus bezüglich des Basisnormalteilers von Z definiert.

Als Permutationsgruppen sind S_y und $\widehat{S_y}$ ungleich, aber in offensichtlicher Weise äquivalent. Ist $T \subset S_y$, so sei im folgenden mit $\widehat{T}$ die entsprechende Teilmenge von $\widehat{S_y}$ bezeichnet. Mit $\widehat{\ }\colon S_y \to \widehat{S_y}$ bezeichnen wir also die Einbettung des Basiskomplementes S_y in das Kranzprodukt $Z = S_x \wr S_y$.

(149) DEFINITION: Es sei $H \leq G$ Permutationsgruppen und $\mathfrak{R}_H$ ein Repräsentantensystem der H-Klassen transitiver Untergruppen von H. Zu jedem $T \in \mathfrak{R}_H$ sei $\mathrm{nvs}(G, H, T)$ ein fest gewähltes Vertretersystem der Linksnebenklassen $N_G(T)/N_H(T)$. Dann setzen wir

$$\mathrm{NVS}(G, H, \mathfrak{R}_H) = \bigcup_{T \in \mathfrak{R}_H} \mathrm{nvs}(G, H, T).$$

(150) LEMMA: Es seien $V_x \leq S_x$ und $V_y \leq S_y$ transitiv. Für $i \in \{x, y\}$ gelte

(151) Sind $T, U \leq V_i$ unter S_i konjugiert, so sind T und U bereits unter V_i konjugiert.

Des weiteren sei $\mathfrak{R}_i$ ein Repräsentantensystem der V_i-Klassen transitiver Untergruppen von V_i. Wir setzen

$$\mathcal{X} = \mathrm{NVS}(S_x, V_x, \mathfrak{R}_x) \quad \text{und} \quad \mathcal{Y} = \mathrm{NVS}(S_y, V_y, \mathfrak{R}_y).$$

Weiterhin sei $W_V = V_x \wr V_y \leq Z$ gemäß (142). Ist $T \leq W_V$ eine transitive Gruppe, so besitzt jede Z-Klasse von Untergruppen von Z äquivalent zu T, die vom Blocktyp $(\mathcal{B}, V_x, V_y)$ sind, einen Repräsentanten in W_V. Ist T ein solcher Klassenrepräsentant, der nach (147) sauber bezüglich $(\mathcal{B}, \mathfrak{R}_x, \mathfrak{R}_y)$ gewählt sei, so ist jede Untergruppe $T_1 \leq W_V$ der Z-Klasse von T unter W_V zu einem Vertreter aus

$$\mathcal{R}_{T, V_x, V_y} = \{T^z \mid z \in \mathcal{X}^y \cdot \widehat{\mathcal{Y}} \subset W_V\}$$

konjugiert. Dabei bezeichne $\widehat{\mathcal{Y}}$ die Menge $\mathcal{Y}$ als Teilmenge von $\widehat{S_y}$ und $\mathcal{X}^y$ diejenigen Elemente aus dem Basisnormalteiler, die in jeder der y Komponenten einen Eintrag aus $\mathcal{X}$ besitzen.

Beweis: Es sei $T_1 \leq Z$ äquivalent zu T vom Blocktyp $(\mathcal{B}, V_x, V_y)$. Dann existiert nach Satz (37) ein $s \in S_m$, so daß $T_1^s \in W_V$ gilt. Da T_1 vom Blocktyp $(\mathcal{B}, V_x, V_y)$ ist, zeigt der Beweis von (37) aber auch, daß s in diesem Fall das Blocksystem $\mathcal{B}$ festlassen muß, also bereits in Z liegt. Jede der zu betrachtenden Z-Klassen besitzt also einen Repräsentanten in W_V.

Nun sei ein T sauber und $T_1 \leq W_V$ aus derselber Z-Klasse, es gibt also ein $z \in Z$ mit $T^z = T_1$. Gemäß der Zerlegung des Kranzproduktes als semidirektes Produkt sei $z = st$ mit $s \in (S_x)^y$ und $t = z\phi \in \widehat{S_y}$ dargestellt (dabei sei $\phi\colon Z \to \widehat{S_y}$ wie in (148) definiert). Damit ist

$$T_1\phi = (T^z)\phi = (T\phi)^{z\phi} = (T\phi)^t.$$

Die Blockoperationen sind also in $\widehat{S_y}$ konjugiert. Nach Voraussetzung (151) gibt es also ein $v \in \widehat{V_y} \leq \widehat{S_y}$, so daß $(T\phi)^t = (T\phi)^v = T_1\phi \leq \widehat{S_y}$ gilt. Also ist $t/v \in N_{\widehat{S_y}}(T\phi)$. Nun war T vom Blocktyp $(\mathcal{B}, V_x, V_y)$, es ist also $T\varphi \leq \widehat{V_y}$. Gemäß Definition (149) enthält $\mathcal{Y}$ ein Vertretersystem der Linksnebenklassen $N_{S_y}(U)/N_{V_y}(U)$ für jedes transitive $U \in \mathfrak{R}_y$. Wir transferieren $\mathcal{Y}$ in das Basiskomplement und erhalten dort die Menge $\widehat{\mathcal{Y}}$, die dann (da T sauber ist) ein Vertretersystem der Linksnebenklassen $N_{\widehat{S_y}}(T\phi)/N_{\widehat{V_y}}(T\phi)$ enthält. Damit muß $t \in \widehat{\mathcal{Y}} \cdot \widehat{V_y}$ gelten. Wir setzen nun $T_2 = T_1^{t^{-1}}$, also ist $T^s = T_2$.

Nun betrachten wir die Basisnormalteiler $U \lhd T$ und $U_2 \lhd T_2$ bezüglich des Blocksystems $\mathcal{B}$. Da dieses von s festgelassen wird, müssen diese Gruppen aufeinander abgebildet werden. Es gilt also $U^s = U_2$. Ist $\mathrm{B} \in \mathcal{B}$ ein Block und $\psi\colon (S_x)^y \to S_x$ der Einschränkungshomomorphismus dazu, so ist

$$U_2\psi = (U^s)\psi = (U\psi)^{s\psi},$$

wobei $s\psi$ die B-Komponente von s ist. Da T und T_2 transitiv sind, sind auch $U\psi$ und $U_2\psi$ transitive Untergruppen von V_x. Wie oben folgt aus (151), daß $s\psi \in \mathcal{X} \cdot V_x$ gilt.

Damit ist $z \in \mathcal{X}^y \cdot (V_x)^y \cdot \widehat{\mathcal{Y}} \cdot \widehat{V_y}$. Da $\widehat{\mathcal{Y}}$ lediglich die Komponenten permutiert, kommutiert es mit ${V_x}^y$. Folglich ist

$$z \in \mathcal{X}^y \cdot \widehat{\mathcal{Y}} \cdot (V_x)^y \cdot \widehat{V_y} = \mathcal{X}^y \cdot \widehat{\mathcal{Y}} \cdot W_V.$$

Damit ist T_1 unter W_V zu einem Verteter aus $\mathcal{R}_{T,V_x,V_y}$ konjugiert, was zu zeigen war. $\square$

Die Bedingung (151) sieht zunächst technisch aus, ist aber von einer ganzen Reihe großer transitiver Gruppen (wie zum Beispiel $L(7)$) erfüllt. Die Klassen transitiver Untergruppen von Kranzprodukten $X \wr Y$ dieser Gruppen bestimmen sich dann wie folgt: Nach (145) werden diejenigen Gruppen bestimmt, die als Permutationsgruppe in das Kranzprodukt eingebettet werden können. Satz (140) parametrisiert dann die Klassen äquivalenter Untergruppen im Kranzprodukt der entsprechenden vollen symmetrischen Gruppen. Für diejenigen Klassen, deren Repräsentanten vom Blocktyp $(\mathcal{B}, X, Y)$ sind, wird (bezüglich Repräsentantenwahl in X und Y) ein sauberer Repräsentant T in $X \wr Y$ bestimmt. Klassenrepräsentanten erhält man dann durch Fusion der Bildmenge $\mathcal{R}_{T,X,Y}$ unter $X \wr Y$.

IV.9.6. Auch wenn mit (135) die für uns relevanten Fälle transitiver Blockoperationen abgedeckt sind, stellt sich natürlich die Frage, ob man allgemeinere Aussagen über die Typen von Blockoperationen machen kann. Neben dem rein theoretischen Interesse könnte man solche Aussagen womöglich auch bei der Berechnung von Normalisatoren intransitiver Gruppen gewinnbringend benutzen.

Im einzelnen seien zwei Fragen erwähnt:

1. Es sei T eine transitive Gruppe von Grad m. Gibt es dann eine intransitive Gruppe M mit m Bahnen von Länge l, so daß $N = N_{S_{l \cdot m}}(M)$ auf den Bahnen von M transitiv äquivalent zu T operiert?
2. Inwieweit bleibt das Ergebnis aus 1. gültig, wenn man l einschränkt?

Als Antwort können wir zunächst festhalten, daß Frage 2 für kleines l negativ zu beantworten ist (in (135) haben wir ja bereits gesehen, daß für kleine l und eine Reihe von m nicht jede transitive Permutationsgruppe als Operation des Normalisators einer Subpotenz auf den Bahnen der Subpotenz erhalten). Zu Frage 1 sei bemerkt, daß zumindestens die symmetrischen Gruppen, beziehungsweise Kranzprodukte der symmetrischen Gruppen stets auftreten:

(152) Beispiel: Es seien l und m natürliche Zahlen und A eine beliebige transitive Gruppe von Grad l. Weiter sei $D_1 = A^{\times m}$ und D_2 die Diagonale in D_1. Dann operieren $N_1 := N_{S_{lm}}(D_1)$ und $N_2 := N_{S_{lm}}(D_2)$ als symmetrische Gruppe auf den Bahnen von D_1 und D_2.

Ist n eine weitere natürliche Zahl und $D = D_2^{\times n}$, so operiert $N := N_{S_{lmn}}(D)$ auf den Bahnen von D als Kranzprodukt $S_m \wr S_n$.

<u>Beweis:</u> Nach (39) ist $N_1, N_2 \leq N_{S_l}(A) \wr S_m$. Man sieht sofort, daß in beiden Fällen das natürliche Basiskomplement des Kranzproduktes die betreffende Gruppe normalisiert.

Ebenso sieht man sofort, daß N die Partitionierung in Diagonalfaktoren von A respektieren muß (vergleiche (77)), während die Diagonalfaktoren, sowie die Komponenten innerhalb eines Diagonalfaktors jeweils mit der vollen symmetrischen Gruppe permutiert werden dürfen. □

(Für iterierte Kranzprodukte symmetrischer Gruppen kann man ähnliche, jedoch aufwendigere, Konstruktionen durchführen.)

Auch wenn die Vermutung geäußert sei, daß Frage 1 letztendlich eine positive Antwort besitzt, genügen die vorliegenden Ergebnisse nicht, hier genauere Aussagen zu treffen.

Transitive Gruppen als Komplementklassen

IV.9.7. In Schritt 4) müssen wir zum ersten Mal in der Faktorgruppe N/M rechnen. Dies ist im allgemeinen nicht ohne Probleme (siehe V.2), es sei aber an dieser Stelle zunächst angenommen, daß eine geeignete Darstellung der Faktorgruppe zur Verfügung steht. Eine genauere Beschreibung zur Ermittlung einer solchen Darstellung wird in V.2.1 gegeben. Die Faktorgruppe N/K ergibt sich durch die transitive Operation auf den Blöcken, womit automatisch eine kleine Permutationsdarstellung dieser Faktorgruppe zur Verfügung steht.

In der Faktorgruppe S/M sind Komplemente zu K/M zu finden. Ist S/M aufösbar, so existiert hierfür ein effizienter Algorithmus, der zum Beispiel in [CNW1990] beschrieben ist. De facto läßt sich dieser Algorithmus auf die Situation eines auflösbaren K/M ausweiten. Eine genauere Beschreibung des Vorgehens findet sich in V.3.

Es verbleibt der Fall eines nicht auflösbaren K/M. In diesem Fall muß explizit nach Erzeugendensystemen für Komplemente gesucht werden. Dies geschieht mit der in V.5 beschriebenen Backtrack-Suche.

Eine — im Falle von $S < N$ mögliche — zusätzliche Konjugation der Komplemente in N/M muß schließlich durch einen Konjugationstest in der Faktorgruppe entschieden werden. Da $K \lhd N$, bleibt S bei Konjugation der Komplemente fest, die Konjugation findet de facto also in $N_{N/M}(S/M)$ statt und läßt sich damit im Falle auflösbarer Normalteiler auf den in V.3 behandelten Fall zurückspielen.

Diese Suche nach konjugierten Komplementen mag zunächst aufwendig erscheinen, stellt in der Praxis jedoch nur ein verhältnismäßig geringes Problem dar. Im Falle elementar abelscher Normalteiler verwendet [RP1989] in ähnlicher Situation (allerdings unter alleiniger Berücksichtigung minimal transitiver Operationen auf den Blöcken) die 2-Cohomologiegruppe, um alle Erweiterungen zu klassifizieren. Die hier (zur Komplementberechnung) verwendete 1-Cohomologiegruppe scheint im Vergleich dazu einfacher zu berechnen.

IV.9.8. Der Zugehörigkeitstest ist wiederum einfach: Für jede der erhaltenen Gruppen werden alle Blocksysteme bestimmt. Ist das Blocksystem $\mathcal{B}$ der Konstruktion nicht minimal, so ist Bedingung Z1 (die Minimalität, Seite 34) verletzt. Für die Blocksysteme gleicher Ordnung werden daraufhin die jeweiligen Kerne (die Normalteiler M) bestimmt. Ist einer von diesen kleiner als der Kern zu $\mathcal{B}$, so erfüllt $\mathcal{B}$ nicht Z2. Für die verbleibenden Blocksysteme wird der Typ der Operation eines Blockstabilisators auf seinem Block bestimmt, welcher für Z3 minimal sein muß. Schließlich muß für Z4 der Permutationsisomorphietyp der Operation auf den Blöcken für $\mathcal{B}$ ebenfalls minimal sein. Ist eine dieser drei Bedingungen verletzt, so ist $\mathcal{B}$ nicht zugehörig, und die Gruppe wird noch auf andere Weise konstruiert werden. Auf gleiche Weise werden damit implizit auch die anderen G zugehörigen Blocksysteme bestimmt.

Nehmen wir also an, daß neben $\mathcal{B}$ eine Reihe weiterer zugehöriger Blocksysteme von G verbleiben (in diesem Abschnitt ist im weiteren nur noch von zugehörigen Blocksystemen die Rede, weshalb dieser Zusatz ab jetzt implizit verstanden sei). Nach Satz (54) muß somit nun die Minimalität der Kernklasse $[M]$ getestet werden. Dies geschieht (wir definieren die Ordnung auf genau diese Weise) zunächst durch einen Vergleich des Permutationsisomorphietyps der Operation des Blockstabilisators auf seinem Block. Dieser soll minimal sein. Die $[M]$ mit minimalem Blockoperationstyp werden dann vermöge eines Vergleichs ihrer kanonischen Repräsentanten verglichen.

IV.9.9. Im Zugehörigkeitstest wird daher zunächst für jedes M der Typ der Operation auf einem Block bestimmt. Ist dieser für den Kern M_0, über den G konstruiert wurde, nicht minimal, so kann G nicht in $\mathcal{G}_{M_0}$ liegen und wird folglich verworfen. Ansonsten liefert dies eine Filterung der im weiteren zu betrachtenden Kerne. Für die verbliebenen Kerne bestimmen wir nun die kanonischen Vertreter:

Wurden die Subpotenzen nicht als Verschachtelung konstruiert, so wird M wie in IV.2.14 in die in IV.2.1 definierte Form gebracht und dann mit Algorithmus (100) – beziehungsweise IV.5.4, falls die Subpotenzen als invariante Untergruppen bestimmt wurden – kanonisiert. (Da die Operation des Blockstabilisators für alle Blocksysteme gleich ist, sind die Kerne aller Blocksysteme vom selben „Kanonisierungstyp“).

Wurden die Subpotenzen dagegen als Verschachtelung konstruiert, so ist das schöne Blocksystem auf den Bahnen von M nach IV.7.4 zu konstruieren und M dementsprechend zu kanonisieren.

Der Normalteiler M_0, zu dem G konstruiert wurde, ist bereits kanonisch.

Ist das Minimum der kanonischen Vertreter der möglichen M kleiner als M_0, so kann G ebenfalls nicht in $\mathcal{G}_{M_0}$ liegen. G wird also noch auf eine andere Weise konstruiert werden und wird daher nicht in die Liste aufgenommen.

Es verbleibt damit der Fall aus III.3.3 und es ist möglich, daß G mehrfach zu M_0 konstruiert wurde, wobei das konjugierende Element M_0 nicht festläßt. Wir führen daher eine separate Merkliste solcher Gruppen zu M_0 und testen, ob G zu einer dieser Gruppen konjugiert ist. Ist dies nicht der Fall, so wird G in die Liste der transitiven Gruppen aufgenommen und gleichzeitig in dieser Merkliste notiert.

(153) Bemerkung: Dies ist die einzige Stelle, an der ein Konjugationstest der konstruierten transitiven Gruppen durchgeführt werden muß. Er tritt aber nur sehr selten auf, siehe (177)

Die nach diesem Test verbliebenen Gruppen können damit als Vertreter aus $\mathcal{G}_{M_0}$ angesehen werden und werden folglich in die Liste der transitiven Gruppen aufgenommen.

IV.10. Aufblasungen

Zur Gesamtheit der imprimitiven Gruppen fehlen diejenigen Gruppen, die nach Lemma (45) als Aufblasungen erhalten werden. Die Konstruktion dieser Gruppen geschieht genau nach diesem Lemma: Ist die Blocksystemordnung m und Blockordnung l gegeben, so durchlaufen wir das Repräsentantensystem $\mathfrak{R}_m$ der transitiven Gruppen von Grad m. Zu einer Gruppe $T \in \mathfrak{R}_m$ bestimmen wir den Punktstabilisator S und dessen maximale Untergruppen $\{V_i\}$ von Index l. Die Aufblasungen selber erhält man daraus durch Operation auf den Nebenklassen.

Ist der Punktstabilisator auflösbar, so kann die Bestimmung der V_i wiederum mittels der Methoden aus [Eic1993] geschehen. Da l aber (insbesondere wenn m und damit auch $|S|$ größer wird) meist recht klein ist, ist in jedem Fall das nachfolgende Lemma recht nützlich.

(154) Lemma: Es sei $l \leq 4$. Es sei $H = G^l \lhd G$ das l-te Glied der Kommutatorreihe von G (wobei die Indizes so gewählt seien, daß $G^1 = G$, $G^{i+1} = [G^i, G^i]$ gilt). Dann liegt jede Untergruppe von G von Index l über H.

Beweis: Es sei $V \leq G$ von Index l. Dann liefert die Darstellung auf den Nebenklassen von V einen Homomorphismus $\alpha\colon G \to S_l$. Für $l \leq 4$ ist S_l auflösbar mit Kommutatorlänge l. Damit ist die Kommutatorlänge von $\operatorname{Bild}\alpha$ maximal l. Nach dem Homomorphiesatz gilt gleiches dann für die Kommutatorlänge von $G/\operatorname{Kern}\alpha$, also ist $H = G^l \leq \operatorname{Kern}\alpha$, was zu zeigen war. □

Es genügt also, die Untergruppen von passendem Index im homomorphen Bild zu suchen und die V_i dann als Urbilder zu erhalten.

Die Untergruppen V_i müssen danach nur unter der Automorphismengruppe fusioniert werden. Dabei kann jedoch, wie in III.2.3 erwähnt, die Berechnung der Automorphismengruppe auf diejenigen Fälle beschränkt werden, in denen die Aufblasung zwei gleichartige Blocksysteme besitzt. Diese Information erhält man wiederum beim Zugehörigkeitstest wie in IV.9.8: Das Blocksystem muß minimal für die Aufblasung sein, die Operation auf den Blöcken vom minimal möglichen Typ unter den Blocksystemen gleicher Ordnung mit trivialem Kern.

IV.11. Listen

IV.11.1. Die primitiven Gruppen schließlich sind bereits für Grad ≤ 50 bestimmt und können der Liste von C. SIMS (welche bis Grad 20 in [Sim1970] publiziert ist und sich ansonsten in GAP[S$^+$1995] findet) entnommen werden (die Liste der Gruppen bis Grad 1000 von J. DIXON und B. MORTIMER [DM1988] gibt keine expliziten Erzeuger an).

Um nun alle transitiven Gruppen eines gegebenen Grades n zu erhalten, bestimmen wir zu jedem nichttrivialen Teiler l von n als möglicher Blockgröße die imprimitiven Gruppen mit entsprechendem Blocksystem von Ordnung $m = n/l$. Die Aufblasungen erhält dabei man wie im vorangegangenen Abschnitt beschrieben.

Zum Erhalt der übrigen Gruppen bestimmen wir nun die möglichen M. Dazu betrachten wir zunächst die minimal transitiven Gruppen von Grad m und bestimmen deren Punktstabilisatoren. Die möglichen A sind dann nach (49) und III.2.5 die Normalteiler primitiver Gruppen von Grad l, deren Index die Ordnung eines der Punktstabilisatoren teilt. Zu jedem dieser A bestimmen wir den Normalisator C. Aus dieser Information über die minimal transitiven Gruppen können wir nun, wie in IV.5 und IV.6.3 beschrieben, feststellen, ob die möglichen M als invariante Untergruppen erhalten werden können. Ist dies nicht der Fall, so erhalten wir die möglichen M wie in IV.3 beschrieben. Zu jedem der M ermitteln wir schließlich die transitiven Gruppen entsprechend der Beschreibung in IV.9. Nach Satz (57) erhalten wir hieraus insgesamt alle transitiven Gruppen von Grad n.

IV.11.2. Um den Konstruktionsprozeß dann iteriert für höhere Grade durchführen zu können, benötigen wir noch eine Liste der minimal transitiven Gruppen eines Grades. Diese können wir aus der Liste aller transitiven Gruppen recht einfach bestimmen. Die folgende Vorgehensweise wird in Grundzügen bereits von G. ROYLE [Roy1987] vorgeschlagen: Die Liste der transitiven Gruppen wird durchlaufen. Dabei wird für jede Gruppe getestet, ob echte transitive Untergruppen gefunden werden können. Ist dies der Fall, so kann die Gruppe nicht minimal transitiv sein. Im folgenden sind eine Reihe Tests beschrieben, die nach Rechenaufwand geordnet sind.

(155) ALGORITHMUS: Teste, ob die Gruppe T minimal transitiv ist. Liefert einer der folgenden Tests eine transitive echte Untergruppe, so ist T nicht minimal transitiv.

1. [Zufällige Untergruppen] Bestimme eine Reihe (typischerweise 30) von jeweils von zwei zufälligen Elementen aus T erzeugten Untergruppen von T und teste, ob diese echte Untergruppen und transitiv sind.
2. [Primitivitätstest] Ist T imprimitiv so gehe zu Schritt 3, ist T einfach, so gehe zu Schritt 6, sonst halte an (Normalteiler primitiver Gruppen sind transitiv).
3. [Minimale Operation des Faktors] Für alle Blocksysteme der Gruppe untersuche, ob die Operation auf den Blöcken minimal transitiv ist. Ansonsten gibt es nach (III.2.5) echte transitive Untergruppen.
4. [Minimale Basis] Suche nach Untergruppen der Basis, die auf allen Blöcken transitiv operieren, und untersuche deren Erzeugnis mit Nebenklassenvertretern der Basisfaktorgruppenerzeuger auf Transitivität.
5. [auflösbarer Fall] Ist T auflösbar, so bestimme die maximalen Untergruppen mittels der Methode aus [Eic1993]. Teste sie auf Transitivität, halte an.
6. [Verbandsberechnung] Bestimme den Untergruppenverband und suche nach nichttrivialen transitiven Untergruppen.

Die nach Test 4. verbleibenden Gruppen sind meist bereits minimal transitiv und damit so klein, daß die Berechnung der maximalen Untergruppen, beziehungsweise des Untergruppenverbandes keine Probleme aufwirft.

Der Beweis von Folgerung (116) zeigte bereits, daß für primes n jeweils die zyklische Gruppe C_p die einzige minimal transitive Grupe ist.

IV.12. Konstruktion partieller Listen

Da die Anzahl transitiver Gruppen für höhere Grade sehr stark ansteigt, ist es dort nicht mehr sinnvoll, komplette Listen zu erstellen. Vielmehr möchte man nur noch Aufzählungen aller Gruppen mit gewissen Eigenschaften erstellen. Sind diese Eigenschaften „permutationsartig“, so läßt sich der hier beschriebene Algorithmus an die alleinige Konstruktion solcher Gruppen anpassen.

IV.12.1. Offensichtlich sind die Reduktionen, falls nur Gruppen mit bestimmter Blockgröße oder sogar bestimmter Operation des Blockstabilisators (oder des Kerns) auf einem Block gesucht werden; in diesem Fall wird lediglich der entsprechende Teil des Konstruktionsbaumes durchlaufen. Dabei muß allerdings der Zugehörigkeitstest insoweit verändert werden, als daß eine Gruppe, die ein kleineres Blocksystem besitzt, nun nicht auch noch zu diesem konstruiert wird. Die Minimalitätsbedingungen in IV.9.8 sind dementsprechend so abzuändern, daß nur Minimalität bezüglich derjenigen Blocksysteme/Operationen betrachtet wird, für die Gruppen konstruiert werden. Auch der Konstruktionsprozeß der subdirekten Produkte ändert sich in IV.3.5 analog.

Werden nur Gruppen mit vorgegebener Operation T auf den Blöcken gesucht, so sind zunächst alle möglichen Kerne dieser Blockoperation modulo Konjugation zu konstruieren. Eine Betrachtung der minimal transitiven Untergruppen von T kann dabei entscheiden, ob in diesem speziellen Fall – auch wenn es im allgemeinen für diese Blockgröße nicht zulässig ist – die möglichen Kerne als Invariante Untergruppen oder Verschachtelungen konstruiert werden.

Unter diesen Kernen sind diejenigen auszuwählen, für die die Operation des Normalisators auf den Blöcken eine Untergruppe äquivalent zu T besitzt. Für ein Repräsentantensystem dieser Untergruppen ist dann wie in IV.9 beschrieben zu verfahren. Beim Zugehörigkeitstest sind dann nur noch Blocksysteme mit gleicher Operation auf den Blöcken zu berücksichtigen.

Werden nur Gruppen gewisser Ordnung gesucht, so kann man hieraus und aus der Ordnung der transitiven Gruppen kleinerer Grade zunächst zu jeder Blockgröße die möglichen Ordnungen der Kerne M bestimmen (ist $G = M.T$, so ist $|G| = |M| \cdot |T|$). Bei der Kernbestimmung brauchen dann nur Subpotenzen passender Ordnung und zu jeder Subpotenz nur Blockoperationen passender Ordnung berücksichtigt zu werden. Da alle Fälle des Konstruktionsbaumes durchlaufen werden, braucht der Zugehörigkeitstest nicht modifiziert zu werden.

Für andere Eigenschaften läßt sich der Konstruktionsprozeß nicht reduzieren. Falls möglich, sollte man die zu suchende Teilklasse in die oben beschriebenen Klassen einbetten. Ansonsten können lediglich Konjugationstests für G/M und G'/M (vergleiche IV.9.7) sowie die Zugehörigkeitstest entfallen, sofern G (und G') nicht die gewünschte Eigenschaft besitzen.

KAPITEL V

Hilfsalgorithmen

In diesem Kapitel sollen eine Reihe von Algorithmen, beziehungsweise Modifikationen und Heuristiken für bekannte Algorithmen, beschrieben werden, die für den Konstruktionsprozeß von Bedeutung sind, jedoch auch für sich selbst stehend Nutzanwendungen haben können.

V.1. Anordnung von Permutationsgruppen

An verschiedenen Stellen der vorangegangenen Kapitel geschah die Auswahl kanonischer Vertreter letzlich durch Anordnung von Gruppen und Auswahl des kleinsten Vertreters. In diesem Abschnitt soll eine – relativ schnell berechenbare – Anordnung für Permutationsgruppen vorgestellt werden, die hierfür benutzt wird. Die Idee für eine solche Anordnung dürfte seit längerem bekannt sein (Ansätze finden sich bereits in [Sim1971b, Hol1984]); so ist sie zum Beispiel im System GAP [S^+1995] implementiert. Da aber meines Wissens eine Beschreibung bisher nirgendwo publiziert wurde, sei sie der Vollständigkeit halber gegeben.

In einer (endlichen) Permutationsgruppe G berechnen wir iteriert Stabilisatoren

$$G_1, G_{[1,2]}, \ldots, G_{\tilde{B}} = \langle 1 \rangle,$$

wobei $\tilde{B} = [1, 2, \ldots, n]$ ist. Nun eliminieren wir aus $\tilde{B}$ Punkte, die bereits vom Stabilisator der vorangegangenen Punkte stabilisiert werden; das heißt solche $1 < k \leq n$, bereits von $G_{[1,\ldots,k-1]}$ festgelassen werden. Damit erhalten wir die lexikographisch kleinste unverkürzbare Base $B_k(G)$ von G. (Eine *Base* ist eine Menge von Punkten, so daß jedes Element der Gruppe durch die Bilder der Basepunkte eindeutig gegeben ist [Sim1971b].)

Elemente von G können damit bezüglich der Listen ihrer Basebilder lexikographisch verglichen werden, die Identität ist dabei das kleinste Element. Ist $U \leq G$, so kann man für $g \in G$ den „Divisionsrest“ beim Enthaltenseinstest in U bezüglich $B_k(U)$ als kanonischen Vertreter der Nebenklasse Ug wählen, da er als kleinstes Element der Nebenklasse vom Repräsentanten unabhängig ist [Sim1971a].

V.1.1. Mit Hilfe dieser Methoden konstruieren wir nun ein „kleinstes“ Erzeugendensystem E (eine Folge von Erzeugern) für G wie folgt:

Wir initialisieren

$$U := \langle\rangle \leq G, \qquad E := \emptyset.$$

Nun wählen wir das kleinste (bezüglich lexikographischer Ordnung der Basebilder) Element $g \in G \setminus U$ aus und setzen

$$U := \langle U, g \rangle, \qquad E := E \cup \{g\}.$$

Diesen Prozeß iterieren wir, bis $U = G$ gilt (was irgendwann der Fall sein muß, da U stets wächst). Offenbar ist E stets ein Erzeugendensystem des aktuellen U. Das letzendlich erhaltene E ist somit Erzeugendensystem von G und enthält die kleinstmöglichen Elemente für ein Erzeugendensystem (wobei jedoch keine Elemente angefügt werden, die bereits im Erzeugnis der vorangegangenen Elemente liegen). Das System ist nur von G, nicht jedoch von der ursprünglichen Erzeugermenge abhängig. Wir nennen dieses E daher das *kleinste Erzeugendensystem* für G.

Durch Vergleich der jeweils kleinsten Erzeugendenfolgen können wir damit eine Anordnung auf der Menge der Permutationsgruppen definieren. Alternativ – und in der Praxis schneller – kann auch zunächst eine Anordnung gemäß Ordnung der Gruppen erfolgen und nur bei gleicher Ordnung auf Vergleich der kleinstmöglichen Erzeugendensysteme zurückgegriffen werden. Dies liefert ebenso eine totale Ordnung.

(156) BEMERKUNG: In Hinblick auf den Beweis von Lemma (94) sei bemerkt, daß die so konstruierte Ordnung „verschiebungsinvariant“ ist, das heißt, sie ist unter Punktersetzungen $i \mapsto i + j$ für festes j invariant.

Um eine Aufzählung der Elemente aus $G \setminus U$ zu vermeiden, gehen wir in der Praxis bei der Konstruktion von E etwas anders vor: Ein Element ist umso kleiner, je größer das Anfangsstück der Base ist, das es festläßt. Sind $G > S_1 > S_2 > \cdots S_l > \langle\rangle$ die der Base entsprechenden iterierten Stabilisatoren, so liegen die Erzeuger aus E somit, soweit möglich, in kleinen S_i (das heißt i ist groß). Ist $E_i = E \cap S_i$, so erhalten wir E_{i-1} folglich durch Ergänzen von E_i zum kleinsten Erzeugendensystem von S_{i-1}. (E ist somit auch ein starkes Erzeugendensystem [Sim1971b].)

Die E_i zu E_{i-1} ergänzenden Elemente müssen den i-ten Basepunkt bewegen, sie sind gemäß der Definition der Ordnung umso kleiner, je kleiner das Bild dieses Basepunktes ist. Die Bilder stehen dabei in Bijektion zu den Nebenklassen $S_i \backslash S_{i-1}$. Ist $O_i = i^{(S_{i-1})}$ die Bahn des i-ten Basepunktes unter S_{i-1}, so muß das erste E_i ergänzende Element $e_{i,1}$ aus der Nebenklasse zu $\min(O_i)$ gewählt werden, das kleinstmögliche Element ist dann das kleinste Element aus dieser Nebenklasse, und wird wie oben beschrieben bestimmt. (Dabei sei bemerkt, daß Base- und Stabilisatorkettenanteil in den S_i jeweils auch einer kleinstmöglichen Base von S_i entsprechen, eine erneute Stabilisatorkettenberechnung kann entfallen.)

Da S_i Punktstabilisator ist, liegen alle Elemente aus S_{i-1}, die i auf einen Punkt in der Bahn von i unter $U := \langle e_{i,1}, S_i\rangle$ abbilden, bereits in U. Der nächste Erzeuger $e_{i,2}$ muß i folglich auf einen anderen Punkt der Bahn abbilden und wird somit als kleinstes Element der Nebenklasse zu $\min(O_i \setminus i^U)$ gewählt. Dies wird iteriert, bis $i^U = O_i$ gilt. Nach dem Bahnensatz ist dann $S_{i-1} = \langle E_{i-1}\rangle$ mit $E_{i-1} := E \cup \{e_{i,1}, \ldots, e_{i,m_i}\}$ und der Prozeß kann induktiv fortgesetzt werden.

V.2. Faktorgruppendarstellungen

Im nächsten Abschnitt soll versucht werden, zu einer Gruppe G (im allgemeinen einer Permutationsgruppe) und einem Normalteiler $N \lhd G$ eine Gruppe H, in der effizient gerechnet werden kann (zum Beispiel eine Permutationsgruppe), nebst einem Morphismus

$\varphi\colon G \to H$ mit $\operatorname{Kern}\varphi = N$ zu bestimmen. Bevor wir dies aber versuchen, soll zunächst bemerkt werden, daß dieses Problem in manchen Fällen nur sehr schlechte Lösungen besitzen kann. P. NEUMANN gibt in [Neu1986] als Beispiel eine Gruppe von Grad 80 an, die eine Faktorgruppe mit minimaler Permutationsdarstellung von Grad 2^{21} besitzt.

Der allgemeine Fall einer Faktorgruppe mit größerer minimaler Permutationsdarstellung als die Gruppe selber wird von D. EASDOWN und C. PRAEGER in [EP1988] untersucht, wobei ebenfalls eine Reihe von Beispielen angegeben wird.

All diesen Beispielen gemein ist, daß die Faktorgruppe auflösbar mit großen abelschen Normalfaktoren ist und aus diesem Grunde keine kleine Permutationsdarstellung besitzt.

V.2.1. Ist die Faktorgruppe G/N auflösbar, so kann in dieser am effizientesten mit Hilfe einer Ag-Präsentation gerechnet werden. Der Algorithmus von C. SIMS zur Bestimmung einer Ag-Präsentation einer Permutationsgruppe [Sim1990] kann dazu so abgeändert werden, daß er nur modulo des Normalteilers N rechnet, und damit eine solche Präsentation der Faktorgruppe (nebst einem Epimorphismus) liefert. Darüberhinaus bricht der Algorithmus im Falle einer nicht auflösbaren (Faktor)gruppe mit einer Fehlermeldung ab und kann somit implizit auch als Auflösbarkeitstest benutzt werden.

Für uns bedeutet dies, daß eine Permutationsdarstellung der Faktorgruppe nur benötigt wird, wenn die Faktorgruppe nicht auflösbar ist. Dies schließt obige (Gegen)beispiele aus.

Selbst wenn aber eine treue Permutationsdarstellung der Faktorgruppe von kleinem Grad existiert, müssen wir diese erst finden, um sie dann praktisch verwenden zu können. Im allgemeinen bedeutete dies wohl Bestimmung des Untergruppenverbandes von G/N, was bei weitem zu aufwendig ist. Daher soll das Ziel lediglich ganz pragmatisch sein, zu einem gegebenen N (mit nicht auflösbarer Faktorgruppe) eine treue Permutationsdarstellung dieser Faktorgruppe von akzeptablem Grad zu finden. Akzeptabel bedeutet dabei, daß der Aufwand der Suche einer solchen Darstellung nicht den Gewinn durch die Möglichkeit, eine kleinere Darstellung benutzen zu können, überwiegen sollte. Ziel dieses Abschnittes kann es daher nur sein, eine Reihe von Heuristiken zur Bestimmung verhältnismäßig einfach zu erhaltender Permutationsdarstellungen der Faktorgruppe, unter denen dann die kleinstmögliche ausgewählt wird, anzugeben.

V.2.2. Zunächst seien angelehnt an [Neu1986] eine Reihe von Fällen aufgeführt, in denen eine geeignete Operation der Gruppe eine Darstellung der Faktorgruppe liefert:

1. N ist punktweiser Stabilisator einer Teilmenge der Bahnen von G.
2. N ist mengenweiser Stabilisator aller Blöcke eines Blocksystems von G.
3. N ist abelsch und selbstzentralisierend.
4. N ist direktes Produkt und Schnitt der Normalisatoren der direkten Faktoren.

In 1. können wir dann die Operation auf den von N festgelassenen Bahnen, in 2. die Operation auf den Blöcken verwenden. In 3. ist N abelsch und damit meist nicht signifikant größer als der Grad von G (ist N zum Beispiel transitiv, so muß N regulär sein), wir können auf den nichttrivialen Elementen von N (beziehungsweise einer Teilmenge) per Konjugation operieren. In 4 schließlich operieren wir auf den direkten Faktoren per Konjugation.

Anhand der Bahnen von N kann getestet werden, ob Fall 1 oder 2 eintritt; aus den Zentralisatoren der Elemente von N (so N abelsch ist), beziehungsweise den Normalisatoren von Normalteilern in N läßt es sich für die anderen beiden Fälle ersehen.

Betrachten wir nun solche Operationen so wird es sich allerdings oftmals ergeben, daß N zwar Untergruppe des Kerns ist (dies ergibt sich automatisch aus der Konstruktion der Operation, die ja auf von N festgelassenen Objekten stattfindet), jedoch der Kern M der Operation echt größer ist (dies tritt bezüglich Blockoperation zum Beipiel immer dann auf, wenn in III.2.6 der Kern K echt größer als die zu normalisierende Subpotenz ist). Ist S Stabilisator der Operation (hier sei transitive Operation angenommen, ansonsten sind Stabilisatoren für alle Bahnen zu betrachten), so enthält S also nicht nur N, sondern auch bereits K. In diesem Fall kann man offenbar S zumindestens durch diejenige Untergruppe T von S ersetzen, die von N und denjenigen Erzeugern von S erzeugt wird, welche nicht in $M \setminus N$ liegen. Dann betrachten wir die Operation auf den Nebenklassen von T. Dies garantiert zwar nicht, daß der Kern dieser Darstellung nun N ist; auch ist T im allgemeinen kleiner als nötig. In einer ganzen Reihe von Fällen stellt sich aber heraus, daß dies akzeptable Darstellungsgrade liefert.

V.2.3. Als weitere Alternative kann eine zufällige Suche nach Untergruppen dienen, deren Kern gleich N ist. Dazu wird N solange mit zufälligen Elementen aus G erweitert, wie sich eine echte Untergruppe von G ergibt, deren Kern nicht größer als N ist.

Als brauchbare Heuristik hat es sich dabei herausgestellt, N mit einem zufälligen Element aus G zu einer Untergruppe $N \leq U < G$ zu erweitern, so daß der Kern von U gleich N ist und dann (wir können annehmen daß G/N nicht zyklisch ist) nach einem weiteren zufälligen Element $r \in G$ zu suchen, so daß $V = \langle U, r \rangle$ wiederum Kern N besitzt. Dabei kann der rechnerisch aufwendige Test auf den Kern von V entfallen, wenn der Index $[G : V]$ so klein ist, daß eine treue Darstellung von G/N von diesem Grad bereits aus Ordnungsgründen nicht möglich ist. Für die meisten r wird $\langle U, r \rangle = G$ gelten, dies kann aber meist verhältnismäßig schnell mit einem Random-Schreier-Sims Algorithmus getestet werden.

Dieser Test wird 15 mal (ein Wert der sich in der Praxis als ausreichend erwiesen hat) iteriert und die Untergruppe V von kleinstem Index ausgewählt.

Ergibt sich dabei bei einem Test eine treue Darstellung von Grad kleiner 100, so lohnt es sich meistens nicht mehr zu versuchen, einen noch kleineren Grad durch weitere Zufallssuche zu erreichen, da der Gewinn dabei im Verhältnis zu den Kosten zu gering ist.

Haben wir schließlich eine treue Permutationsdarstellung erhalten, so empfiehlt es sich, abschließend noch nach Blocksystemen mit trivialem Kern zu suchen [SS1994]. In vielen Fällen gelingt es damit nochmals, den Grad der Permutationsdarstellung zu verringern. Da auf Punkten und nicht auf Nebenklassen operiert wird, ist eine solche Suche auch effektiver, als ein Versuch, die als Stabilisator dienende Untergruppe zu vergrößern.

Die Methode verallgemeinert sich offensichtlich auf die Suche nach mehreren Untergruppen, deren Kerne sich in N schneiden, dies liefert dann eine intransitive Permutationsdarstellung der Faktorgruppe.

V.2.4. Ist der Normalteiler N verhältnismäßig klein, so gibt es für Permutationsgruppen einen direkten Zugang zu Untergruppen, die zumindestens als Kandidaten für die V's des vergangenen Abschnittes gewählt werden können.

Es sei B eine Base für N. Dann schneidet der Stabilisator $S := G_{[B]}$ trivial mit N. S ist also Komplement zu N im Erzeugnis $\langle N, S\rangle$. Wir wählen nun ein Repräsentantensystem $\{\omega_i\}$ der Bahnen von S, die von Länge größer 1 sind. Es sei $S_i := \mathrm{Stab}_S(\omega_i)$. Dann ist die Permutationsdarstellung von S auf der Vereinigung der Nebenklassen aller S_i treu. Dementsprechend hat $\langle N, S\rangle/N$ eine treue Darstellung auf den Nebenklassen der Untergruppen $U_i := \langle N, S_i\rangle$. Die Darstellung von G/N auf den Nebenklassen dieser Untergruppen muß daher ebenfalls treu sein. Ist B klein (zum Beispiel für reguläres N), so führt dies zu Darstellungen der Faktorgruppe von akzeptablem Grad.

V.2.5. Um von einer Untergruppe letztendlich zu einer Permutationsdarstellung zu gelangen, benötigen wir abschließend noch eine Routine, die die Permutationsdarstellung auf den Nebenklassen der Untergruppe liefert. Dazu repräsentieren wir die Nebenklassen durch die in V.1 definierten kleinsten Repräsentanten. Da uns die Entsprechung zwischen Punkten und Nebenklassen hier nicht interessiert, können wir darauf verzichten, die Vertretermenge zu Beginn auszurechnen. Statt dessen bauen wir das Vertretersystem als Bahn des trivialen Elementes (das kanonischer Vertreter der Untergruppe ist) unter der durch Multiplikation und nachfolgende Kanonisierung gegebenen Operation auf, und erhalten dabei implizit auch die Permutationsdarstellung auf den Nebenklassen.

Während dieses Algorithmus muß schließlich ein Vertretersystem der Nebenklassen (die Bahn) im Speicher gehalten werden. Ist der Index der Untergruppe oder der Grad der Permutationsdarstellung von G groß, so ist dies aus Speicherplatzgründen nicht mehr möglich. In diesem Falle speichern wir statt der Gruppenelemente in der Bahn jeweils nur die Bilder der kleinsten Base von G unter dem Gruppenelement. Die Operation ändert sich dann entsprechend in

1. Bestimmung des Nebenklassenvertreters aus seinen Basebildern durch Multiplikation geeigneter Transversalenelemente der Stabilisatorkette.
2. Multiplikation dieses Vertreters mit dem operierenden Gruppenelement.
3. Bestimmung des kanonischen Nebenklassenvertreters des Produktes.
4. Abbilden der Base mit diesem kanonischen Vertreter.

Das Aus- und Einpacken der Gruppenelemente in Basebilder erhöht die Rechenzeit, allerdings ist für die meisten nicht-symmetrischen Gruppen eine Base erheblich kürzer als der Grad, pro Nebenklasse sind meist nur eine Handvoll Zahlen anstelle einer Permutation von hohem Grad zu speichern.

V.2.6. Da wir die Darstellung der Faktorgruppe letzendlich stets durch Operation der Gruppe auf einer geeigneten Menge erhalten, liefert uns die Konstruktion implizit stets die Bilder der Erzeuger von G unter dem Homomorphismus $\varphi\colon G \to H$. Da wir beliebige Elemente aus G durch abdividieren „entlang der Stabilisatorkette" in Worte aus den Erzeugern zerlegen können, das Wort in den Bildern der Erzeuger ausgewertet also das Bild des Gruppenelementes unter φ sein muß, lassen sich Bilder (und durch duales Vorgehen in H auch Urbildrepräsentanten) unter φ bestimmen [LGPS1991]

Abschließend sei nochmals erwähnt, daß die hier beschriebene Vorgehensweise sicherlich noch weit vom Optimum entfernt ist. Für den Zweck der Konstruktion transitiver Gruppen von verhältnismäßig kleinem Grad reicht sie aber aus.

V.3. Komplemente und Cohomologie

Für elementar abelsche Normalteiler lassen sich die Konjugiertenklassen von Komplementen durch die 1-Cohomologiegruppe beschreiben [Hup1967, Satz 17.1]: Es sei H eine Gruppe, die über dem elementar abelschen Normalteiler $N \lhd H$ mit Komplement K zerfällt. Jedes Komplement zu N läßt sich dann in der Form

$$\{k \cdot k\gamma \mid k \in K\}$$

für eine dem Komplement zugehörige Abbildung $\gamma\colon K \to N$ darstellen. Wählen wir einen Nebenklassenvertreter $k \in K$ aus dem fest gewählten Komplement, so schreiben wir $k \cdot n$ mit $n \in N$ explizit als Produkt, um die Zerlegung anzudeuten. Die Komplementeigenschaft bedingt, daß

$$(k \cdot k\gamma) \cdot (l \cdot l\gamma) = kl \cdot (kl)\gamma$$

gilt, und γ damit die Bedingung

$$(kl)\gamma = (k\gamma)^l l\gamma, \qquad \forall k, l \in K \tag{157}$$

erfüllen muß. Analog folgt, daß jede derartige Funktion γ ein Komplement definiert, die Komplemente stehen somit in Bijektion zu den *1-Cozykeln*

$$Z^1(K, N) = \{\gamma\colon K \to N \mid \gamma \text{ erfüllt } (157)\}.$$

Zur Konjugation von Komplementen genügt es – da ein Komplement ja ein Repräsentantensystem von H/N bildet – Konjugation mit N zu betrachten. Konjugieren wir das Komplement $\{k \cdot k\gamma\}$ mit dem Element $n \in N$, so erhalten wir wegen

$$(k \cdot k\gamma)^n = k^n (k\gamma)^n \overset{N \text{ abelsch}}{=} k \cdot (k\gamma) \cdot n^{-k} n$$

das Komplement zur Abbildung $\gamma \cdot \kappa_n$, wobei $\kappa_n\colon k \mapsto n^{-k}n$ sei. Konjugation entspricht somit Multiplikation der Abbildung γ mit einer Abbildung aus den *1-Coränder*n

$$B^1(K, N) = \{\kappa_n\colon K \to N, k \mapsto n^{-k}n \mid n \in N\},$$

die Konjugiertenklassen von Komplementen stehen in Bijektion zu den Elementen der *1-Cohomologiegruppe* $H^1(K, N) = Z^1(K, N)/B^1(K, N)$. Ist eine Präsentation der Faktorgruppe bekannt, so kann man mit Methoden aus [CNW1990] die Gruppen Z^1, B^1 und H^1 mittels linearer Algebra durch Lösen eines homogenen Gleichungssystems bestimmen. Ein dazugehörendes inhomogenes Gleichungssystem gestattet, ein einzelnes Komplement zu berechnen.

V.3.1. Hierauf aufbauend, wird in [CNW1990] ein Verfahren zur Bestimmung von Komplementen in auflösbaren Gruppen beschrieben. De facto genügt dafür aber, daß der Normalteiler N auflösbar ist.

Zur Bestimmung der 1-Cohomologiegruppe und der Komplemente benötigt man dann lediglich eine Präsentation der ursprünglichen Faktorgruppe und eine Normalreihe durch den Normalteiler mit elementar abelschen Faktoren (nebst zugehörigen Homomorphismen). Für Permutationsgruppen kann eine Präsentation, wie in [Neu1982] beschrieben, bestimmt werden. Eine Normalreihe erhält man aus folgendem Lemma:

(158) LEMMA: Es sei $N \lhd H$ und $M \lhd N$ mit $S := N/M$ einfach. Dann ist $L := \bigcap_{h \in H} M^h$ normal in H und N/L elementar (das heißt direktes Produkt) vom Typ S.

Beweis: Als Schnitt einer H-Bahn ist L normal, die Faktorgruppe ist per Konstruktion subdirektes Produkt von Kopien von S und, da S einfach ist, folglich elementar. □

Da N auflösbar ist, lassen sich maximale Normalteiler M mit abelscher Faktorgruppe leicht bestimmen (zum Beispiel durch Suche in der Kommutatorfaktorgruppe oder auch Umwandlung in eine AgGruppe), iterierte Anwendung der Konstruktion des Lemmas liefert eine Normalreihe durch N mit elementar abelschen Faktoren.

Epimorphismen auf die Faktorgruppe erhält man schließlich mit den Methoden aus V.2.1.

V.3.2. Wir kehren zum Fall eines elementar abelschen N zurück. Nun sei $\varphi\colon H \to H$ ein Automorphismus, der N festläßt. Folglich muß φ die Konjugiertenklassen von Komplementen untereinander permutieren. Diese Operation soll auf H^1 beschrieben werden.

Ist $k \in K$, so ist $(Nk)\varphi = Nh$ mit $h \in K$, wir definieren die induzierte Operation $\bar{\varphi}$ auf dem Komplement vermöge $(Nk)\varphi =: N(k\bar{\varphi})$. Schließlich setzen wir $m_{k,\varphi} \in N$ als $m_{k,\varphi} := k\varphi/(k\bar{\varphi})$, es gilt also $k\varphi = k\bar{\varphi}m_{k,\varphi}$.

Damit ist

$$(k \cdot k\gamma)\varphi = k\bar{\varphi}m_{k,\varphi}(k\gamma)\varphi = k\bar{\varphi} \cdot (k\bar{\varphi})\delta$$

mit $\delta\colon K \to N$ vermöge

$$k\delta := m_{k(\bar{\varphi}^{-1}),\varphi}(k(\bar{\varphi}^{-1})\gamma)\varphi$$

definiert. Da φ Komplemente permutiert, muß $\delta \in Z^1(K, N)$ sein.

Diese Operation ist *keine* Operation durch Homomorphismen. Insbesondere bleibt B^1 nicht fest. Allerdings werden (da die Konjugiertenklassen von Komplementen, entsprechend Nebenklassen von B^1, permutiert werden müssen) die Nebenklassen von B^1 permutiert. Repräsentanten der φ-fusionierten Konjugiertenklassen erhält man somit als Repräsentantensystem der Bahnen auf den Nebenklassen.

Um diese Operation explizit durchzuführen, bestimmt man zunächst eine Basis von B^1 (wir fassen Z^1 als Zeilenraum auf) in Hermite-Normalform. In jeder Nebenklasse von B^1 in Z^1 gibt es dann genau einen Vertreter, dessen Einträge in den Komponenten Null ist, zu denen die Basis von B^1 Stufen besitzt. Aus einem beliebigen Nebenklassenvertreter können wir diesen ausgezeichneten Vertreter der Nebenklasse durch Subtraktion der Basisvektoren erhalten. Die Operation auf den Nebenklassen wird dann so durchgeführt, daß zunächst ein Repräsentant abgebildet, und für die Nebenklasse des Bildes dann der oben definierte ausgezeichnete Repräsentant berechnet wird.

V.3.3. Als nächstes betrachten wir den Fall einer Einbettung $H \lhd F$, wobei auch $N \lhd F$ gelte. Mittels Bahnrepräsentanten der durch F-Konjugation induzierten Operation auf $H^1(K,N)$ erhalten wir ein Repräsentantensystem der F-Klassen von Komplementen zu N in H.

Ist N nicht elementar abelsch, so können wir die Konstruktion aus [CNW1990] entsprechend modifizieren: Wir wählen mittels (158) eine F-Normalreihe von N mit elementar abelschen Faktoren und wenden dann die folgende Modifikation von [CNW1990, Satz 4.2] an:

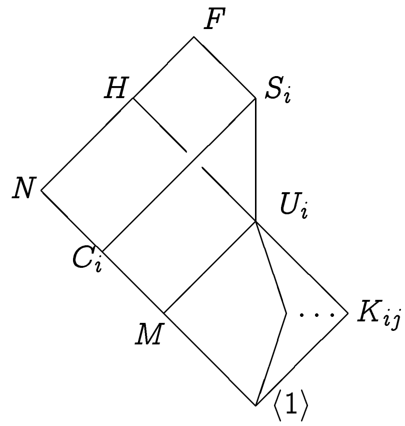


BILD 1. Komplemente und ihre epimorphen Bilder

(159) SATZ: Es sei F eine Gruppe, $H, N, M \lhd F$ mit $H > N > M$, M elementar abelsch. $\{U_1/M, \dots, U_k/M\}$ sei ein Repräsentantensystem der F-Klassen von Komplementen zu N/M in H/M. Zu jedem $i \in \{1, \dots, k\}$ sei S_i das volle Urbild des Normalisators in der Faktorgruppe $N_{F/M}(U_i/M)$. Schließlich sei $\mathcal{L}_i$ ein Repräsentantensystem der S_i-Klassen von Komplementen K_{ij} zu M in U_i (siehe Bild 1). Dann ist $\bigcup_{i=1}^k \mathcal{L}_i$ ein Repräsentantensystem der F-Klassen von Komplementen zu M in H.

<u>Beweis:</u> Wie in [CNW1990] unter Berücksichtigung der zusätzlichen Operation von $N_F(U_i)$. □

Die Vorgehensweise bei der Berechnung ist dann wiederum wie in [CNW1990] beschrieben, wobei lediglich die Operation aus V.3.2 anstelle der affinen Operation des genannten Artikels (letzteres ist der Fall, da durch die Operation von F der Normalisator nicht notwendigerweise gleich dem Zentralisator ist) verwendet werden muß.

V.4. Hauptreihen in Permutationsgruppen

Für den allgemeinen Fall einer Komplementberechnung werden wir auch Normalreihen durch nicht auflösbare Normalteiler benötigen. Da der Aufwand dazu nur geringfügig größer ist, sei hier die Berechnung einer Hauptreihe beschrieben.

Gegeben sei eine Gruppe G und ein Normalteiler $H \lhd G$. Wir wollen eine G-Kompositionsreihe für H bestimmen. (Im Fall G=H ergibt sich eine Hauptreihe für G.) $U \lhd$

H sei ein maximaler Normalteiler von H, der Faktor H/U ist also einfach. Ein solches U kann zum Beispiel mit den Methoden zur Bestimmung von Kompositionsreihen [Neu1986, Luk1987, BS1992] berechnet werden, wobei der iterierte Verfeinerungsprozeß zu einfachen Faktoren jeweils nur auf die Faktorgruppe angewandt werden muß. Nach (158) ist $L = \bigcap_{g\in G} U^g \leq H$ normal in G und H/L elementar vom Typ H/U. (Für Freunde der Komplexizitätstheorie sei angemerkt, daß L als Schnitt von sich gegenseitig normalisierenden Gruppen in polynomialer Zeit berechnet werden kann [CFL1989].) Ist H/U nicht abelsch, so ist H/L bereits ein G-Kompositionsfaktor:

(160) Satz: Ist $H \lhd G$ und $U \lhd H$ mit $S = H/U$ einfach und nichtabelsch und ist $L = \bigcap_{g\in G} U^g$, so existiert kein Normalteiler $N \lhd G$ mit $L \lneqq N \lneqq H$.

<u>Beweis:</u> Wir können durch Übergang zur Faktorgruppe ohne Beschränkung der Allgemeinheit annehmen daß $L = 1$ ist. Nach (158) ist H elementar, es sei $H = S^{\times r}$. Es sei $\langle 1\rangle \lneqq N \lhd H$ ein nichttrivialer Normalteiler von H, also existiert $1 \neq n \in N$. Gemäß der Zerlegung als direktes Produkt ist $n = (s_1, s_2, \ldots, s_r)$. Da $1 \neq n$ ist (bei geeigneter Numerierung ohne Beschränkung der Allgemeinheit) $s_1 \neq 1$. Da S einfach und nicht abelsch ist, existiert ein $t \in S$ mit $s_1^t \neq s_1$. Damit ist auch der Quotient

$$n^{(t,1,\ldots,1)}/n = (s_1^t/s_1, s_2/s_2, \ldots, s_r/s_r) = (s_1^t/s_1, 1, \ldots, 1)$$

in N enthalten, wobei $s_1^t/s_1 \neq 1$ gelten muß. Durch weitere Konjugation erhalten wir Elemente der Form $(r, 1, \ldots, 1)$, wobei r die Klasse von s_1^t/s_1 in S durchläuft. Das Erzeugnis dieser Elemente ist ein nichttrivialer Normalteiler in $(S, 1, \ldots, 1)$ und damit – da S einfach – gleich diesem direkten Faktor. Durch iteriertes Anwenden dieses Arguments folgt, daß ein nichttrivialer Normalteiler von N direktes Produkt von mehreren der konstituierenden direkten Faktoren sein muß.

Dies gilt insbesondere für den Normalteiler U. Dieser – und seine G-Konjugierten U^g – müssen aus Ordnungsgründen jeweils direktes Produkt von $r-1$ der S_i sein. Nach Definition operiert G transitiv auf diesen Gruppen und damit auch auf deren normalen Komplementen S_i selber. Ist also $N \lhd G$ und eines der $S_i \leq N$ – nach obigem notwendige Bedingung für ein nichttriviales N – so müssen folglich alle $S_j \leq N$ sein. Damit ist $N = H$, also H minimaler Normalteiler. □

Ist H/U dagegen abelsch, so ist H/L ein Modul für G, für den mit MeatAxe-Methoden [Par1984] eine Kompositionsreihe bestimmt werden kann (wie in [Rón1990] gezeigt, ist auch dies in polynomialer Zeit möglich). Die vollständigen Urbilder der Untermoduln aus dieser Reihe bilden dann eine nicht weiter verfeinerbare Normalteilerreihe durch H/L.

In beiden Fällen ist damit eine Hauptreihe bis L bestimmt. Indem man nun das Vorgehen mit $H_{\text{neu}} = L$ iteriert, erhält man letzlich eine G-Hauptreihe für H.

Soll eine Hauptreihe durch einen vorher gewählten Normalteiler $M \lhd G$, $M \leq H$ gelegt werden, so ist, solange die Reihe nicht bei M angelangt ist, der maximaler Normalteiler $U \lhd H$ jeweils über M zu wählen (zum Beispiel als vollständiges Urbild des ersten Gliedes einer Kompositionsreihe von H/M). In diesem Fall wird $M \leq L = \bigcap U^g$ gelten, die Reihe muß aus Ordnungsgründen also irgendwann M erreichen.

Im Nachhinein habe ich festgestellt, daß die Grundstruktur eines solchen Algorithmus bereits in [KL1990] beschrieben ist, allerdings aufsteigend anstelle absteigend. Da die dortige Beschreibung aber eher kursorisch ist, schien es mir sinnvoll, diesen Abschnitt beizubehalten.

V.5. Morpheus

Im Verlaufe der Berechnungen benötigen wir mehrfach die Automorphismengruppe einer Gruppe sowie einen konstruktiven (das heißt eine explizite Abbildung liefernden) Isomorphietest. Diese Probleme sind recht verwandt; so könnte man zum Beispiel nach Isomorphismen zwischen A und B suchen, indem man nach Automorphismen von $A \times B$ sucht, die A und B vertauschen. Im folgenden soll daher ein Algorithmus beschrieben werden, der mit leichten Veränderungen der Eingabeparameter sowohl die Automorphismengruppe, als auch Isomorphismen bestimmen kann. In Folge werden wir ihn darüber hinaus auch noch zur Komplementbestimmung und zur Suche nach Faktorgruppen von vorgegebenem Isomorphietyp benutzen. Im Grundgerüst handelt es sich um eine Suche nach möglichen Morphismen, weshalb die Routine auf den Namen „Morpheus" getauft sei[1]. Der permim Algorithmus aus [HR1992] benutzt im wesentlichen dieselben Ideen, er wird dort allerdings nur als G-Quotient Algorithmus verwandt.

An die Gruppen wird lediglich die Bedingung gestellt, daß in diesen gerechnet werden kann (im wesentlichen die Berechnung von Konjugiertenklassen sowie der Test, ob eine auf einer Erzeugermenge gegebene Abbildung sich zu einem Homomorphismus fortsetzen läßt). Sind die Gruppen dagegen von speziellerer Gestalt, so existiert eine Reihe von effizienteren Algorithmen, die es dann anzuwenden lohnt: Die Automorphismengruppe einer abelschen Gruppe wird in [Sho1928] beschrieben und ist im wesentlichen eine leicht modifizierte Matrixgruppe. Als solche kann sie aus Operationen, die den elementaren Umformungen eines Gleichungssystems entsprechen, konstruiert werden. Einen konstruktiven Isomorphismustest für abelsche Gruppen erhält man unmittelbar aus der Darstellung beider Gruppen in Normalform als direktes Produkt zyklischer Gruppen.

Für p-Gruppen liefert der Erzeugungsalgorithmus [New1977, O'B1990] gleichzeitig Automorphismen [O'B1995] und ein kanonisches Erzeugendensystem der Quotienten. Läßt man den Algorithmus daher mit einer Präsentation einer endlichen p-Gruppe laufen, so erhält man deren Automorphismengruppe; der Vergleich kanonischer Erzeugendensysteme gestattet einen einfachen Isomorphietest [O'B1994]. Algorithmen dieser Art wurden von E. O'Brien [O'B1990] und M. Wursthorn [Wur1993] implementiert.

Auf diesen Ideen aufbauend, entwickelte M. Smith in [Smi1994] einen Algorithmus der sogar die Automorphismengruppe einer auflösbaren Gruppe bestimmt. Auch hier sollte die Berechnung kanonischer Erzeugendensysteme und damit ein Isomorphietest möglich sein.

Der hier beschriebene Algorithmus wird daher vor allem für den Fall nicht auflösbarer Grupen Verwendung finden. Diese besitzen im allgemeinen weniger äußere Automorphismen als auflösbare oder gar nilpotente Gruppen. So braucht zum Beispiel der „worst case"

[1] Dabei ist die Assoziation eines „zum einschlafen langsamen" Algorithmus nicht notwendigerweise beabsichtigt

einer elementar abelschen Gruppe, die minimal n Erzeuger hat und die komplette $GL(n,p)$ als äußere Automorphismengruppe besitzt, nicht behandelt zu werden.

V.5.1. Gegeben sei eine Gruppe A mit Erzeugendensystem $\{a_i\}$ sowie eine Gruppe B. Zu a_i sei $B_i \subset B$ eine Menge von Gruppenelementen auf die a_i potentiell abgebildet werden kann. Schließlich sei vorausgesetzt, daß die Möglichkeit besteht, eine Präsentation für A in den a_i auf vorgegebenen Elementen (potentiellen Bildern unter Morphismen) aus B auszuwerten. Für Permutationgruppen A bedeutet dies im wesentlichen eine Zerlegung der Schreiererzeuger von A gemäß einer Stabilisatorkette (genaueres ist in [Neu1982] beschrieben) und Auswerten der so erhaltenen Worte in den gewählten Bildern in B. Für AgGruppen wird zunächst ein induziertes Erzeugendensystem aus den a_i bestimmt, wobei die Erzeugerbilder simultan mit umgeformt werden. Zu einem IGS (das ja selber wieder ein PCGS ist) kann eine Präsentation schließlich durch einfaches Auswerten und Zerlegen von p-Potenzen und Kommutatoren bestimmt werden.

Da B eine Gruppe ist und die Verkettung eines Morphismus mit einem inneren Automorphismus stets wieder einen Morphismus liefert (wobei sich Injektivität etc. übertragen) können wir ohne Einschränkung annehmen, daß die B_i jeweils Vereinigungen von Konjugiertenklassen (als Bahnen der inneren Automorphismengruppe) sind:

$$B_i = \bigcup_{r_{i,j}} \bigcup_{g \in B} r_{i,j}^g.$$

Die Suche nach möglichen Morphismen, die a_i in B_i abgebilden, geschieht nun, indem ein Suchbaum mit iterierten Schleifen durchlaufen wird: Da die Bildtupel nur modulo innerer Automorphismen durchlaufen werden sollen, dürfen wir die Bilder beliebig konjugieren. Dabei steht uns zunächst ganz B zur Konjugation zur Verfügung. Wir können daher annehmen, daß a_1 auf eines der $r_{1,j}$ abgebildet wird. Diese $r_{1,j}$ werden in einer Schleife durchlaufen. Damit ist die Konjugation auf $C_B(r_{1,j})$ eingeschränkt.

Sind nun die Bilder der ersten $i-1$ Erzeuger vorgegeben und die Konjugation auf $C \leq B$ eingeschränkt, so sind für die Bilder von a_i nicht nur die $r_{i,j}$, sondern die C-Bahnen auf deren Klassen zu betrachten. Die Auswahl der Klassen geschieht wiederum mittels einer Schleife, die j auswählt. Die C Bahnen auf $r_{i,j}^B$ entsprechen – bei Konjugation mit den Repräsentanten – nach (4) den Doppelnebenklassen $C_B(r_{i,j})\backslash B/C$, die in einer weiteren Schleife durchlaufen werden und damit jeweils das Bild $b_i = r_{i,j}^b$ vorgeben. Die Konjugation wird dann für das Bild des nächsten Erzeugers auf $C_C(b_i)$ eingeschränkt.

Sind schließlich Bilder b_i für alle a_i ausgewählt, so wird durch Auswerten einer Präsentation von A in den a_i auf den b_i festgestellt, ob $a_i \mapsto b_i$ einen Homomorphismus liefert. Zusätzlich werden je nach der geplanten Anwendung weitere Bedingungen wie Injektivität getestet. Je nach Aufwendigkeit dieser Tests empfiehlt es sich zur Beschleunigung in einigen Fällen, diese bereits vor dem Homomorphietest – der im Falle einer negativen Antwort dann entfallen kann – durchzuführen. Ist der Homomorphietest – wie bei Permutationsgruppen – selbst recht aufwendig, so empfiehlt es sich darüber hinaus, zunächst eine Reihe von Testrelationen (Ordnungen einiger Produkte in den a_i) in den b_i auszuwerten, um mögliche Morphismen weiter einzuschränken.

Je nach geplanter Anwendung werden diese iterierten Schleifen nun so lange durchlaufen, bis ein Morphismus gefunden wurde; beziehungsweise alle Bildtupel getestet wurden.

Ist die Erzeugerzahl größer als 2, so lohnt es sich, bereits nach der Auswahl von i Bildern ($i \geq 2$) diese auf Erfüllung von Relationen zwischen der ersten i Erzeugern zu testen. Ist eine dieser Relationen nicht erfüllt, so kann der Suchbaum an dieser Stelle direkt beschnitten werden, da es keine möglichen Bilder für a_j ($j > i$), gibt, durch die ein Homomorphismus definiert würde.

Die Idee einer solchen Suche durch Elementtupel ist nicht neu, sondern findet sich bereits in [FN1970], dort allerdings ohne die Reduktion auf Repräsentanten modulo Konjugation.

V.5.2. Da in allen (später betrachteten) Anwendungen von MORPHEUS die Menge der zu testenden Bildtupel von der Anzahl und den Ordnungen der a_i abhängt, empfiehlt es sich bei größeren Gruppen ein Erzeugendensystem mit kleiner potentieller Bildmenge zu suchen. Das heißt im allgemeinen: die Erzeugeranzahl ist minimal und die Ordnungen der Erzeuger sind möglichst klein.

Dies kann zum einen durch eine Zufallssuche nach erzeugenden Elementen kleiner Ordnung geschehen. Ist diese nicht erfolgreich, so kann für Gruppen, für die die Konjugiertenklassen bekannt oder einfach zu bestimmen sind, ein solches Erzeugendensystem explizit mit Morpheus selber gesucht werden.

Dies geschieht in einer Schleife über die Erzeugerzahl n (die mit der leicht zu bestimmenden minimalen Erzeugendenanzahl der Kommutatorfaktorgruppe, beziehungsweise 2 im perfekten Fall, gestartet wird[2]).

Bei gegebenem n geschieht die Suche nach einem n-Erzeugendensystem mittels MORPHEUS selber. Hier ist A die freie Gruppe auf n Erzeugern und B die zu untersuchende Gruppe, die B_i sind jeweils alle nichttrivialen Klassen. Nebenbedingung ist, daß die Menge der b_i ganz B erzeugt, während der Morphismustest trivial wird. Abgebrochen wird, sobald ein Erzeugendensystem gefunden wurde. Dabei sind die Klassen in den B_i entsprechend Präferenz (z. B. primär kleine Elementordnungen) angeordnet, das erste gefundene Erzeugendensystem ist also relativ „gut“.

V.5.3. Die zweite Anwendung ist die Bestimmung der Automorphismengruppe einer Gruppe A. Hier ist $B := A$ und $\{a_i\}$ ein Erzeugendensystem von A. B_i ist die Vereinigung derjenigen Klassen, in die a_i unter einem möglichen Automorphismus abgebildet werden könnte. Dies sind Klassen von gleicher Ordnung und gleicher Repräsentantenordnung. Als untere Approximation können hierbei die rationalen Klassen dienen, die dann nur noch bezüglich gleicher Element- und Klassenordnungen fusioniert werden müssen. In [FN1970] wird eine weitergehende Einschränkung der Klassenfusionen vorgeschlagen, die iteriert Normalisatoren und Zentralisatoren der von den Klassenrepräsentanten erzeugten Untergruppen betrachtet. Unter Automorphismen müssen die vorkommenden Größen

[2]Zyklische Gruppen können aufgrund der geringen Zahl möglicher Abbildungen durch direkte Tests behandelt werden

und Eigenschaften (wie abelsch, zyklisch etc.) dieser Gruppen gleich bleiben. Die Bestimmung einer solchen – besseren – Fusion wird für größere Gruppen jedoch selber aufwendig. Andererseits sind diese Verbesserungen insbesondere für nilpotente Gruppen, welche verhältnismäßig viele Klassen und Automorphismen besitzen, lohnend. Da wir jedoch annehmen können, daß die hier betrachteten Gruppen nicht einmal auflösbar sind, kann auf eine solche Verbesserung verzichtet werden.

Nebenbedingung an die Morphismen sind offenbar Injektivität und Surjektivität.

Die Suche mittels Morpheus findet nun Repräsentanten für jede Nebenklasse in der äußeren Automorphismengruppe. Um letzlich die gesamte Automorphismengruppe zu erhalten, muß die so erhaltene Menge somit um ein Erzeugendensystem der innerern Automorphismen – Konjugationsmorphismen zu den Erzeugern von A – ergänzt werden.

Da die betrachteten Gruppen nicht auflösbar sind, ist die äußere Automorphismengruppe meist verhältnismäßig klein. Nichtsdestotrotz kann sich in einigen Fällen ein für die weitere Verarbeitung unangenehm großes Repräsentantensystem ergeben. Daher kann es sich lohnen, redundante Erzeuger der Automorphismengruppe herauszuwerfen. Hierzu ist es nötig, in dieser zu rechnen. Dazu verwenden wir die (offenbar treue) Permutationsdarstellung von $\mathrm{Aut}(A)$ auf der Vereinigung der B_i, sofern diese von akzeptabel kleinem Grad ist.

Ganz unabhängig davon verwenden wir diese Permutationsdarstellung auch für Nebenklassenberechnungen in der Automorphismengruppe, die in IV.3.3 durchgeführt werden müssen.

V.5.4. Im Falle der Suche nach Isomorphismen sind A und B zwei Gruppen (für die die Möglichkeit der Isomorphie bereits zuvor anhand Ordnung und Klassenordnungen getestet wurde). Wie bei der Automorphismenbestimmung werden wiederum die möglichen Bildermengen B_i bestimmt, Nebenbedingung ist wiederum Injektivität und Surjektivität. Die Schleife wird abgebrochen, sobald ein Isomorphismus gefunden wurde. Da das Produkt eines Iso- mit einem Automorphismus stets wiederum Isomorphismus ist, braucht die dabei womöglich gegebene Auswahl eines inneren Automorphismus nicht beachtet zu werden; gibt es einen Isomorphismus, so würde ein entsprechender Repräsentant modulo innerer Automorphismen auch gefunden.

V.5.5. Als nächstes betrachten wir die Suche nach Komplementen eines Normalteilers. Dazu sei G eine Gruppe und $N \lhd G$. Ist U Komplement zu N, so existiert ein Monomorphismus $\varphi\colon G/N \hookrightarrow G$ mit $\mathrm{Bild}\,\varphi = U$. Bezeichnen wir den natürlichen Homomorphismus zu N mit ν, so können wir annehmen, daß $\varphi\nu = \mathrm{id}_{G/N}$ gilt.

Wir setzen somit $A = G/F$, $\{a_i\}$ gleich einem Erzeugendensystem von A und B_i gleich dem vollständigen Urbild der Klasse a_i^A unter ν. (Ist N auflösbar, so kann man, wie in [MN1989] beschrieben, affine Methoden zur Berechnung dieser Urbilder verwenden. In diesem Fall empfiehlt es sich jedoch, Komplementklassen mit cohomologischen Methoden zu bestimmen, siehe V.3.) Nebenbedingung an die Morphismen ist die Injektivität sowie, daß $\mathrm{Bild}\,\varphi$ trivial mit N schneidet.

Die Suche liefert Erzeugendensysteme modulo Konjugation. Ist man dagegen – wie meist – an Repräsentanten der Klassen von Komplementen interessiert, so müssen die so erhaltenen Untergruppen noch nachfolgend auf Konjugation getestet werden.

Analog dem Vorgehen in [CNW1990] kann in Fällen, in denen N nicht minimaler Normalteiler ist, die Berechnung „faktorisiert" werden. Dazu bestimmt man, wie in V.4 beschrieben, eine Hauptreihe durch N und wendet für die einzelnen Hauptfaktoren M [CNW1990, Satz 4.2] an. (Dies ist Satz (159) für $F = H$ und daraus folgender Beobachtung daß $S_i/M = N_{H/M}(U_i/M) = C_{H/M}(U_i/M)$ gilt). Die Bestimmung der Komplemente zu den Hauptfaktoren geschieht dann im elementar abelschen Fall mit cohomologischen Methoden (siehe V.3), im nicht abelschen Fall mit der oben beschriebenen Suche nach Erzeugendensystemen. In diesem Fall ist dann N elementar einfach nichtabelsch, die vollen Urbilder der betreffenden Faktorgruppenklassen können meist recht schnell durch eine Zufallssuche mit Konjugationstests bestimmt werden.

V.5.6. Als letzte Anwendung sei eine Suche nach Faktorgruppen von bestimmtem Isomorphietyp – also ein G-Quotient Algorithmus (wie er auch ursprünglich bei [HR1992] vorkommt) – beschrieben. Hier ist A die Gruppe, für die Quotienten isomorph G gesucht werden sollen, $\{a_i\}$ ein Erzeugendensystem von A mit Elementen möglichst kleiner Ordnung und $B = G$. Ist $A \twoheadrightarrow G$ ein Epimorphismus, so muß a_i auf ein Element abgebildet werden, dessen Ordnung $|a_i|$ teilt, und dessen Klassenlänge Teiler der Klassenlänge von a_i in A ist. (Letzteres gilt, da $C_A(a_i)N/N \leq C_{A/N}(a_iN)$ und damit $|C_A(a_i)| \;\Big|\; |N| \cdot \left|C_{A/N}(a_iN)\right|$ gilt. Damit ist

$$\left|(a_iN)^{A/N}\right| = \frac{|A|}{|N| \cdot \left|C_{A/N}(a_iN)\right|} = \frac{|A|}{\mathrm{const} \cdot |C_A(a_i)|} = \frac{1}{\mathrm{const}} \left|a_i^A\right|,$$

also $\left|(a_iN)^{a/N}\right| \;\Big|\; \left|a_i^A\right|$.)

Diese beiden Bedingungen definieren die B_i. Bedingung an die Morphismen ist in diesem Falle die Surjektivität. Da wiederum nur nach Erzeugertupeln gesucht wird, kann – im Falle nichttrivialer äußerer Automorphismen von B – der gleiche Quotient mehrfach gefunden werden. Daher müssen die gefundenen Epimorphismen noch entsprechend ihren Kernen klassifiziert werden.

Ist G abelsch, so kann diese Suche durch die Kommutatorfaktorgruppe A/A' faktorisiert werden.

V.6. Normalisatoren

Im Verlaufe des Algorithmus sind immer wieder Normalisatoren zu berechnen. Dies geschieht für gewöhnlich mit Backtrack-Methoden, die in Grundlagen von C. Sims [Sim1971b] stammen und zum Beispiel in [But1991] beschrieben sind. Erhebliche Verbesserungen stammen von J. Leon [Leo1991]. Verwendet wurde eine Implementation von H. Theissen [The1996], die weitere Beschneidungen des Suchbaumes hinzufügt.

Die in dieser Arbeit vorliegende spezielle Situation der Normalistoren in der vollen symmetrischen Gruppe (beziehungsweise vollen Kranzprodukten) macht jedoch weitere Verbesserungen notwendig, um die Normalisatorberechnungen in akzeptabler Zeit durchführen zu können: Die Kriterien aus III.4.7 gestatten zunächst, die volle symmetrische Gruppe durch eine bisweilen erheblich kleinere Untergruppe in Form eines (möglicherweise iterierten) Kranzproduktes zu ersetzen, in der bereits der gesamte Normalisator liegen muß. Auch dann noch treten allerdings insbesondere bei elementar abelschen Gruppen Probleme auf. Diese beruhen darauf, daß für diese Gruppen einerseits kaum Kriterien zur Verfügung stehen, den Suchbaum der Backtrack-Suche a priori zu beschneiden, andererseits der Normalisator klein ist und die damit implizit gegebene Suchbaumbeschneidung durch bereits gefundene Normalisatoranteile auch nur geringe Auswirkungen hat.

Andererseits ist der Zentralisator einer Untergruppe als iterierter Zentralisator der Erzeuger erheblich einfacher zu berechnen (auch hierzu sind wiederum die bereits oben zitierten Werke als Referenzen zu nennen). Weiterhin gilt für jede Untergruppe $U \leq G$, daß Konjugation mit $N_G(U)$ einen Homomorphismus nach $\mathrm{Aut}(U)$ liefert. Der Kern dieses Homomorphismus ist $C_G(U)$. Wir können somit $N_G(U)/C_G(U)$ als Untergruppe von $\mathrm{Aut}(U)$ auffassen[Hup1967, Satz I.4.5].

V.6.1. Weiterhin nehmen wir an, daß $\mathrm{Aut}(U)$ nebst der Operation auf U bereits bekannt ist. Dies ist zum Beispiel für abelsche Gruppen der Fall, bei denen sich im wesentlichen Produkte linearer Gruppen ergeben (In [Hal1959, Abschnitt 6.2], beziehungsweise [Sho1928] wird dies explizit ausgeführt). Im Falle elementar abelscher Gruppen ergibt sich jeweils die volle lineare Gruppe $GL_n(p)$.

In dieser Automorphismengruppe soll nun die Untergruppe derjenigen Automorphismen, die vom Normalisator in der S_n induziert sind, möglichst gut durch eine Gruppe $V \leq \mathrm{Aut}(U)$ approximiert werden. Dies wird zwar auch die Verwendung von Backtrack-Algorithmen erfordern, dafür ist für kleine U die Automorphismengruppe, in der gesucht wird, kleiner als die symmetrische Gruppe (beziehungsweise das iterierte Kranzprodukt, in dem der Normalisator liegen muß). Tabelle 1 mag hierbei der Orientierung dienen.

Selbst wenn die Automorphismengruppe größer ist, ergibt sich in nicht zu extremen Fällen dadurch ein Vorteil, daß die Gruppe „nicht so symmetrisch ist“, Beschneidungen des Suchbaumes daher oft effektiver wirken.

Ist U transitiv, so könnte das Kriterium aus Lemma (7) benutzt werden, um B zu approximieren: B muß die Klasse des Punktstabilisators festlassen. Die hier natürlich vor allem interessierenden abelschen Gruppen sind in transitiver Darstellung aber regulär, so daß dies dort keine Verbesserung ergibt. Eine Verallgemeinerung von Lemma (7) auf intransitive Gruppen ist dagegen recht aufwendig, da dann nicht nur die Punktstabilisatoren, sondern auch die zu den Bahnprojektionen gehörende subdirekte Struktur berücksichtigt werden muß.

Statt dessen soll benutzt werden, daß Konjugation die Zykelstruktur eines Elementes nicht verändern kann. Wir teilen die nichttrivialen Elemente von U in Klassen gemäß ihrer Zykelstruktur ein. Der Normalisator muß also diese Bahneinteilung respektieren, und wir können V als Stabilisator dieser Partitionierung wählen.

Dies geschieht wie folgt: Wir betrachten U in regulärer Darstellung und die Operation A der Automorphismengruppe auf den Elementen von U. Beide Gruppen seien als Permutationsgruppen aufgefasst. In dieser Permutationsdarstellung entspricht das Einselement e von U dem Fixpunkt von A und jedes $u \in U$ dem Bild dieses Fixpunktes unter u. Der

1	$GL(1,2)$	11232	$GL(3,3)$	185794560	$S(2) \wr S(9)$
2	$GL(1,3)$	13200	$GL(2,11)$	479001600	$S(12)$
2	$S(2)$	20160	$GL(4,2)$	955514880	$S(4) \wr S(5)$
4	$GL(1,5)$	26208	$GL(2,13)$	1410877440	$S(3) \wr S(7)$
6	$GL(1,7)$	28800	$S(5) \wr S(2)$	2124276000	$GL(3,11)$
6	$S(3)$	31104	$S(3) \wr S(4)$	2239488000	$S(6) \wr S(3)$
6	$GL(2,2)$	40320	$S(8)$	3251404800	$S(8) \wr S(2)$
8	$S(2) \wr S(2)$	46080	$S(2) \wr S(6)$	3715891200	$S(2) \wr S(10)$
10	$GL(1,11)$	78336	$GL(2,17)$	4976640000	$S(5) \wr S(4)$
12	$GL(1,13)$	82944	$S(4) \wr S(3)$	6227020800	$S(13)$
16	$GL(1,17)$	123120	$GL(2,19)$	9726417792	$GL(3,13)$
18	$GL(1,19)$	267168	$GL(2,23)$	20158709760	$GL(6,2)$
22	$GL(1,23)$	362880	$S(9)$	67722117120	$S(3) \wr S(8)$
24	$S(4)$	645120	$S(2) \wr S(7)$	81749606400	$S(2) \wr S(11)$
28	$GL(1,29)$	682080	$GL(2,29)$	87178291200	$S(14)$
30	$GL(1,31)$	892800	$GL(2,31)$	111203278848	$GL(3,17)$
48	$GL(2,3)$	933120	$S(3) \wr S(5)$	116064000000	$GL(4,5)$
48	$S(2) \wr S(3)$	1036800	$S(6) \wr S(2)$	137594142720	$S(4) \wr S(6)$
72	$S(3) \wr S(2)$	1488000	$GL(3,5)$	263363788800	$S(9) \wr S(2)$
120	$S(5)$	3628800	$S(10)$	304812862560	$GL(3,19)$
168	$GL(3,2)$	7962624	$S(4) \wr S(4)$	475566474240	$GL(5,3)$
384	$S(2) \wr S(4)$	9999360	$GL(5,2)$	768144384000	$S(7) \wr S(3)$
480	$GL(2,5)$	10321920	$S(2) \wr S(8)$	1307674368000	$S(15)$
720	$S(6)$	10368000	$S(5) \wr S(3)$	1719443554752	$GL(3,23)$
1152	$S(4) \wr S(2)$	24261120	$GL(4,3)$	1961990553600	$S(2) \wr S(12)$
1296	$S(3) \wr S(3)$	33592320	$S(3) \wr S(6)$	2985984000000	$S(5) \wr S(5)$
2016	$GL(2,7)$	33784128	$GL(3,7)$	3656994324480	$S(3) \wr S(9)$
3840	$S(2) \wr S(5)$	39916800	$S(11)$	6449725440000	$S(6) \wr S(4)$
5040	$S(7)$	50803200	$S(7) \wr S(2)$		

TABELLE 1. Ordnungen einiger Automorphismengruppen

Stabilisator einer Teilmenge $Z \subset U$ in der Automorphismengruppe ist dann im Permutationskontext genau der Stabilisator der Bildmenge e^Z in A. Iterierte Anwendung auf alle Bahnen liefert uns V. Da der Aufwand der Berechnung eines Mengenstabilisators mit der Größe der Menge wächst, empfiehlt es sich, die Klassen der Größe nach geordnet zu betrachten, damit die Berechnung der Stabilisatoren großer Mengen in möglichst kleinen Gruppen erfolgt.

Die Stabilisatorberechnung geschieht ebenfalls über einen Backtrack, für den wiederum auf [But1991, Leo1991, The1996] verwiesen wird. Kennen wir a priori bereits einen Normalisatoranteil, so können wir dessen Operation auf U zur Verkürzung der Suche diesem Stabilisatorbacktrack übergeben.

V.6.2. Probleme ergeben sich bei dieser Vorgehensweise, wenn die Klassen, für die Mengenstabilisatoren berechnet werden, zu groß sind. Hierbei ist insbesondere die Größe der kleinsten Klasse relevant, da ihr Stabilisator in der vollen Automorphismengruppe A berechnet wird. Die weiteren Stabilisatoren werden dann in Gruppen berechnet, die durch die bereits vorangegangenen Stabilisatorberechnungen bereits signifikant kleiner als A sind, wodurch die Auswirkung der Klassenordnungen hierbei geringer ist. Als Faustregel hat sich dabei bewährt, daß für $|U| \lesssim 5000$ die Ordnung der kleinsten Klasse 15 nicht überschreiten sollte.

Ist dies nicht der Fall, so soll versucht werden, eine feinere Klassenunterteilung zu bestimmen, als die durch die Zykelstruktur gegebene. Diese Unterteilung soll die vom Normalisator induzierten Konjugiertenklassen immer noch umfassen, aber möglichst gut approximieren. Um die anfangs durch die Zykelstruktur gegebenen Klassen weiter aufzuspalten, untersuchen wir, wie oft Produkte von Klassenrepräsentanten in die einzelnen Klassen fallen:

Es sei $U = \biguplus U_i$ eine Unterteilung in Klassen, die vom Normalisator $N_G(U)$ invariant gelassen wird. In unserer Situation sind dies also anfangs die durch die Zykelstruktur gegebenen Klassen. Für festes j und k testen wir nun für jedes $u \in U_j$, wie oft das Produkt uv in welche Klasse U_i fällt, wenn v die Klasse U_k durchläuft. Für $u \in U_j$ sei $c_{k,i}(u)$ gleich der Anzahl der $v \in U_k$, so daß $uv \in U_i$ ist. (Würden wir die $c_{k,i}(u)$ über $u \in U_j$ summieren, so erhielten wir Strukturkonstanten der von den Klassensummen aufgespannten Unteralgebra der Gruppenalgebra über einem beliebigen Ring).

Nun sei $n \in N_G(U)$ gegeben. Durchläuft v die Klasse U_k, so durchläuft auch v^n die Klasse U_k, da sie unter $N_G(U)$ invariant ist. Aus dem gleichen Grund ist $uv \in U_i$ genau dann, wenn $(uv)^n \in U_i$ ist. Dies bedeutet, daß für $u \in U_j$ und für alle k und i gilt, daß $c_{k,i}(u) = c_{k,i}(u^n)$ ist.

Mit anderen Worten: Sind $u, u' \in U_j$, so können u und u' nur dann in der selben Normalisatorklasse liegen, wenn für alle k und alle i gilt, daß $c_{k,i}(u) = c_{k,i}(u')$ ist. Berechnen wir also die $c_{k,i}(u)$, so können wir durch Vergleich der Werte womöglich einige der Klassen weiter aufspalten. Ergibt sich eine Aufspaltung, so ergeben sich natürlich bezüglich der aufgespaltenen Klassen neue Werte für die $c_{k,i}(u)$, weshalb das Verfahren solange iteriert werden kann, bis sämtliche der Koëffizienten keine neuerlich Aufspaltung liefern.

In der Praxis stellt sich heraus, daß dieses Verfahren insbesondere in den Fällen, in denen alle durch die Zykelstruktur gegebenen Klassen groß sind, signifikante Verbesserungen liefert. Der Laufzeitgewinn der Mengenstabilisatorberechnung wiegt dabei die Kosten der Berechnung der Multiplikationskoëffizienten auf.

V.6.3. Ist U elementar abelsch, so könnten wir theoretisch V zunächst dadurch approximieren, daß wir zu jeder der Klassen in U den Unterraum bestimmen, der von den Elementen dieser Klasse erzeugt wird, und als V den Stabilisator dieser Unterräume – also eine reduzible Matrixgruppe – wählen. Gemeinhin sind diese Unterräume allerdings gleich U, so daß sich hierdurch keinerlei Ersparnis ergibt.

In V bestimmen wir nun die Untergruppe derjenigen Automorphismen, die vom Normalisator induziert wurden. Ist ein Automorphismus gegeben, so suchen wir zunächst ein

Element, das den ersten Erzeuger auf sein Bild abbildet und bilden alle Erzeuger damit ab. Im Zentralisator des ersten Bildes wird diese Suche dann für (das Bild des) zweiten Erzeugers iteriert bis schließlich ein Element gefunden wurde, das alle Erzeuger gemäß dem Automorphismus abbildet oder – dadurch daß kein solches Element gefunden werden konnte – gezeigt wurde, daß der Automorphismus nicht von der S_n induziert ist. Die Untergruppe $\overline{N_G(U)}$ der entsprechenden Elemente kann dann mittels dieses Tests wieder in einer Backtrack-Suche gefunden werden. Es stellt sich heraus, daß V dabei meist sehr nah an (oder gleich) dieser Gruppe ist, so daß keinerlei Vorkehrungen zur Suchbaumbeschneidung getroffen zu werden brauchen. Für den hier besonders interessierenden Fall derjenigen Gruppen, die mögliche Basis einer transitiven Gruppe sind, ist sogar zu vermuten, daß Gleichheit gilt:

(161) VERMUTUNG: Es sei p prim, $W = N_{S_p}(C_p) \wr S_m$ das Kranzprodukt zur natürlichen Permutationsdarstellung der S_m und $D = C_p^{\times m}$ die darin liegende direkte Potenz der zyklischen Gruppe von Ordnung p. Diese operiert intransitiv mit m Bahnen. Es sei $U \leq D$, so daß U auf jeder Bahn von D nichttrivial operiert. Ist $\alpha \in \mathrm{Aut}(U)$ derart, daß α die Zykelstruktur aller Elemente aus U erhält, so gibt es ein $n \in N_W(U)$ so daß $u\alpha = u^n$ für alle $u \in U$ gilt.

In der Anwendung ist natürlich U vorgegeben und D und n werden dann passend gewählt.

Schließlich sei erwähnt, daß die Berechnung von Normalisatoren abelscher Gruppen auch in anderen Fällen den Aufwand der Normalisatorberechnung reduzieren kann:

(162) BEMERKUNG: Es sei $G \leq P$ und $N \lhd G$ charakteristisch und abelsch (solche N gibt es zum Beispiel stets, wenn G auflösbar ist). Dann ist $N_P(G) \leq N_P(N)$. Ist N einfach zu berechnen (z.B. als Glied der Kommutatorreihe), so liefert dies oft eine kleinere Obergruppe des Normalisators, in der die eigentliche Normalisatorberechnung für G erheblich schneller abläuft.

V.7. Kanonische Klassenvertreter in auflösbaren Gruppen

Konjugationstests sind das duale Problem zur Bestimmung des Normalisators. Ist dabei mehrfach Konjugiertheit zu denselben Vertretern zu testen, so empfiehlt es sich, kanonische Klassenvertreter zu definieren und den Konjugiertheitstest durch Vergleich der kanonischen Vertreter beider Gruppen durchzuführen. Die Bestimmung solcher kanonischen Vertreter kann oftmals ganz analog zur Bestimmung des Normalisators vorgenommen werden, indem nicht nach normalisierenden Elementen, sondern nach Elementen gesucht wird, die auf einen „kleinstmöglichen" Vertreter abbilden. Probleme treten dabei aber dann auf, wenn der Algorithmus auch lokale Berechnungen in Untergruppen oder Faktorgruppen durchführt. In diesem Fall ist nicht garantiert, daß sich die gewählte Ordnung auch in die lokale Situation übertragen läßt. Damit wird jedoch die lokale Bestimmung eines „kleinsten" Vertreters unmöglich gemacht. Bei der Normalisatorberechnung ist das Bild (eben die Gruppe selber) dagegen bereits bekannt, so daß sich das Problem der Auswahl des Bildes nicht stellt.

Für auflösbare Gruppen existiert bereits ein effizienter Algorithmus zur Bestimmung des Normalisators einer Untergruppe [GS1990, CNW1990]. Bestandteil desselben ist zum einen die Berechnung in homomorphen Bildern der Gruppe – es gilt offenbar $N_G(U)N/N \leq N_{G/N}(UN/N)$ – die eine Obergruppe des Normalisators liefert. Zum anderen wird eine Berechnung in Untergruppen durchgeführt – für $N \lhd G$ ist $N_G(U) \leq N_G(U \cap N)$. Letzteres läßt sich für elementar abelsche Normalteiler N mit cohomologischen Methoden auf eine lineare Operation zurückführen, was dem Algorithmus besondere Effizienz gibt. Allerdings läßt sich ein Vergleich von Gruppen nicht auf diese lineare Situation (in der die konkreten Realisierungen womöglich von der Auswahl einer Basis abhängig sind) übertragen. Da die ursprünglichen Artikel [GS1990] und [CNW1990] nicht auf diese Probleme eingehen, soll hier eine Abwandlung des Algorithmus vorgestellt werden, die es gestattet, kanonische Klassenvertreter zu berechnen.

V.7.1. Motivation war hierbei insbesondere, daß das zu den Berechnungen verwendete System GAP [S+1995] den Konjugiertheitstest noch durch eine generische Routine durchführte, die im wesentlichen die gesamte Bahn ausrechnete und dabei keine besonderen Eigenschaften auflösbarer Gruppen verwandte, was für praktische Zwecke völlig unzureichend war. Insofern ist der im folgenden beschriebene Algorithmus weniger als neue Idee, sondern als praxisbezogene Interpretation vermutlich bekannter Ideen zu verstehen.

Gegeben sei eine auflösbare Gruppe G (die wir nach [LNS1984] als mit einem Ag-System versehen annehmen). Zu einer Untergruppe $U \leq G$ soll ein Konjugiertes $U^{g_U} \leq G$ angegeben werden, welches unabhängig von der Auswahl von U ist; das heißt, das gleiche Verfahren soll für U^h das gleiche Konjugerte $(U^h)^{g_{U^h}} = U^{g_U}$ liefern.

Grundlage ist die gewählte Ordnung auf den Untergruppen (der kanonische Vertreter wird als unter dieser Ordnung kleinstes Element seiner Klasse ausgewählt): Es gelte $U \preceq V$ genau dann, wenn $\mathrm{CGS}(U) \leq \mathrm{CGS}(V)$ gilt, letzterer Vergleich sei als lexikographischer Vergleich von Listen aus Exponentenmatrizen verstanden. Diese Ordnung überträgt sich auf Faktorgruppen zu Normalteilern aus der Ag-Reihe:

(163) Lemma: Es sei $N \lhd G$ Normalteiler in der Ag-Reihe und $U, V \leq G$. Ist $U \preceq V$, so ist auch $UN/N \preceq VN/N$.

Beweis: Da N Normalteiler in der Ag-Reihe ist, erhält man ein CGS für UN/N aus einem CGS für U durch „Abschneiden" der Exponentenvektoren. Dies ist mit der lexikographischen Anordnung verträglich, die die Vektoren komponentenweise vergleicht. □

Dies bedeutet, daß für Normalteiler aus der Reihe das Homomorphieprinzip bezüglich des natürlichen Homomorphismus $\bar{\ }: G \to G/N$ angewandt werden darf: Ist $\bar{g}$ das konjugierende Element in G/N, das UN/N auf den kanonischen Vertreter $\tilde{U}/N$ in G/N abbildet, so ist $\tilde{U}/N$ auch Bild des kanonischen Vertreters U' von U unter dem natürlichen Homomorphismus: $U'N/N = \tilde{U}/N$. Dies impliziert aber: Ist g ein Urbild von $\bar{g}$ und ist A das vollständige Urbild von $N_{G/N}(\tilde{U}/N)$, so ist U' gleich dem kleinsten (gemäß der Anordnung bezüglich eines von G induzierten CGS) Konjugierten von U^g unter der (meist kleineren) Gruppe A.

V.7.2. Um hieraus ein induktives Verfahren zu gewinnen (welches über die Normalteiler in der Ag-Reihe absteigt), benötigen wir noch eine Bestimmung des kleinsten Konjugierten von U unter A (wobei $AN/N = N_{G/N}(UN/N)$ gilt). Naïve Vorgehensweise wäre hier ein Bahnalgorithmus. In der Tat sind die hier auftretenden Bahnen meist von sehr viel geringerer Länge als die Bahn von U unter G. Nichtsdestotrotz ist die Operation und der notwendige Vergleich der Bilder aufwendig.

Der Normalisatoralgorithmus reduziert an dieser Stelle die Berechnung durch Übergang zu Untergruppen. Wie oben dargelegt ist dieses Vorgehen bei der Suche nach einem kanonischen Repräsentanten jedoch nicht statthaft, da eine Übertragung der Anordnung nicht möglich ist. Aus diesem Grunde nutzen wir die – schnelle – Normalisatorberechnung, um die Bestimmung der Bahn zu verkürzen: Die Bahn von U entsteht durch Konjugation von U mit einem Vertretersystem der Nebenklassen ${}_A\backslash N_A(U)$. Dabei sind lediglich $[A : N_A(U)]$ Konjugationen anstelle der bei einem Bahnenalgorithmus notwendigen $[A : N_A(U)]\cdot m$ (wobei m die Erzeugeranzahl von A sei) Konjugationen und Gruppenvergleiche notwendig. Diese Ersparnis macht in der Praxis die zusätzliche Normalisatorberechnung wieder wett.

Zur Fortführung des Algorithmus wird schließlich dasjenige Element der Bahn mit kleinstem CGS gesucht. Ist g das zugehörige konjugierende Element, so ist $N_A(U)^g$ der für den nächsten Schritt benötigte Normalisator von U^g in A.

(164) ALGORITHMUS: Bestimme das kanonische G-Konjugierte V von $U \leq G$.

1. [Initialisierung] Bestimme eine Reihe $E_i \lhd G$ mit elementar abelschen Faktoren. Setze $i := 1$, $V := U$, $No := G$, $g := 1_G$.
2. [Hebe zum nächstgrößeren Faktor] Inkrementiere $i := i + 1$. Setze $F := G/E_i$. Der natürliche Homomorphismus sei mit $\bar{}: G \to F$ bezeichnet.
3. [Konjugiere lokal minimal] Berechne $M := N_{\overline{No}}(\bar{V})$ und bestimme ein Vertretersystem R der Nebenklassen ${}_M\backslash^{No}F$. Bestimme das $r \in R$, für das das Bild $(\bar{U})^r$ minimal wird.
4. [Ändere Konjugiertes] Bestimme ein Urbild s für r. Setze $V := V^s$, $g := gs$. Setze No gleich dem vollständigen Urbild von M^r.
5. [Schleife über Hauptfaktoren] Wenn $E_i \gneqq \langle 1 \rangle$, dann gehe zu Schritt 2.

Endet der Algorithmus, so ist V der kanonische Vertreter, No der Normalisator von V und g ein Element, das U auf V konjugiert.

V.8. Invariante Untergruppen

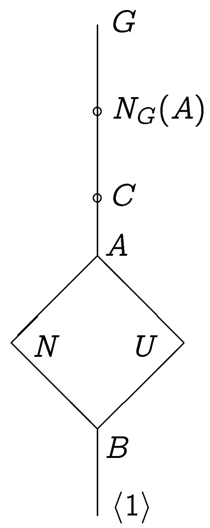
In diesem Abschnitt soll ein Algorithmus beschrieben werden, der die unter einer Menge von Automorphismen invarianten Untergruppen einer auflösbaren Gruppe bis auf Konjugation bestimmt.

Dazu sei G eine (auflösbare) Gruppe und $H \leq \mathrm{Aut}(G)$ eine Gruppe von Automorphismen.

Zur Einführung betrachten wir zunächst den Fall eines trivialen H und beschreiben einen Algorithmus, der Repräsentanten der Konjugiertenklassen aller Untergruppen von G liefert. Die Konstruktion geschieht dabei induktiv über die Faktoren nach Normalteilern in einer Hauptreihe. Der einzelne Rechenschritt besteht dann darin, aus den Untergruppen einer Faktorgruppe G/N die Untergruppen von G zu bestimmen. Da wir G als auflösbar annehmen, genügt es, elementar abelsche Normalteiler zu betrachten. Dies soll zunächst geschehen.

V.8.1. Wir betrachten eine beliebige Untergruppe $U \leq G$ und einen abelschen Normalteiler $N \lhd G$. Dann ist N in U enthalten, U in N enthalten oder $B := N \cap U$ ist eine echte Untergruppe von N und $A := \langle N, U \rangle$ eine echte Obergruppe von N.
In letzterem Fall ist B als Schnitt von U mit N normal in U. Da N abelsch ist, ist B auch normal in U. Folglich ist $B \lhd A$. Das Bild U/B ist damit Komplement zu N/B in A/B. Da $N \lhd G$ ist, folgt

(165) $$N_G(U) \leq N_G(B) \qquad \text{und} \qquad N_G(U) \leq N_G(A).$$



Kennen wir also alle Untergruppen oberhalb N und alle Untergruppen von N, so ist jede Untergruppe von G, die nicht bereits in einer dieser beiden Mengen enthalten ist, als Komplement zu N/B in A/B zu erhalten, wobei $B \leq N \leq A$, $B \lhd A$ gilt.
Jetzt betrachten wir zwei in G konjugierte Untergruppen U und U'. Dann sind auch $A = \langle N, U \rangle$ und $A' = \langle N, U' \rangle$ unter G konjugiert. Gilt sogar $A = A'$, so sind $B = N \cap U$ und $B' = N \cap U'$ unter $N_G(A)$ konjugiert. Ist außerdem $B = B'$, so sind U und U' sogar unter $C = N_G(A) \cap N_G(B) \geq A$ konjugiert. Die Faktoren U/B und U'/B sind also unter C/B konjugierte Komplemente zu N/B in A/B.

Wollen wir nur ein Repräsentantensystem der G-Klassen von Untergruppen erhalten, so genügt es folglich, bei der Konstruktion der Komplemente jeweils nur Klassenrepräsentanten zu berücksichtigen:

(166) Lemma: Es sei $N \lhd G$ abelsch. Weiterhin sei $\mathfrak{A}$ ein Repräsentantensystem der Konjugiertenklassen von Untergruppen, die N echt enthalten und $\mathfrak{B} \ni N$ ein solches der in N enthaltenen Untergruppen. Zu $A \in \mathfrak{A}$ sei $\mathfrak{B}_A$ ein Repräsentantensystem der $N_G(A)$-Klassen von Untergruppen, die echt unter N liegen und in A normal sind. Zu $B \in \mathfrak{B}_A$ sei $C_{A,B} = N_G(A) \cap N_G(B)$ und $\mathfrak{U}_{A,B}$ ein Repräsentantensystem der vollen Urbilder der $C_{A,B}$-Klassen von Komplementen zu N/B in A/B. Dann ist jede Untergruppe von G zu genau einem Vertreter aus

$$R := \mathfrak{A} \cup \mathfrak{B} \cup \bigcup_{A \in \mathfrak{A}} \bigcup_{B \in \mathfrak{B}_A} \mathfrak{U}_{A,B}$$

konjugiert. R ist also ein Repräsentantensystem der Untergruppen von G.

Beweis: Die Untergruppen die N enthalten, oder in N enthalten sind, sind zu jeweils genau einem Vertreter aus $\mathfrak{A}$ oder $\mathfrak{B}$ konjugiert. Wir brauchen also nur noch Untergruppen $U \leq G$ zu betrachten, für die beides nicht gilt.

Ist nun eine solche Untergruppe U gegeben, so sei ohne Beschränkung der Allgemeinheit angenommen, daß U bereits so konjugiert ist, daß $A := \langle N, U \rangle$ in $\mathfrak{A}$ liegt. Dann ist $B' = U \cap N$ unter $N_G(A)$ zu einem $B \in \mathfrak{B}_A$ konjugiert. Ohne Beschränkung der Allgemeinheit können wir weiterhin annehmen, daß bereits $B = B'$ gilt. Dann ist U/B Komplement zu N/B in A/B, beziehungsweise gibt es ein $C_{A,B}$-Konjugiertes von U so daß $U \in \mathfrak{U}_{A,B}$ ist.

Umgekehrt zeigt obige Betrachtung, daß U nur zu höchstens einem Vertreter aus R konjugiert sein kann, woraus die Behauptung folgt. $\square$

(167) BEMERKUNG: Da $B \leq U$ und $B \lhd C$, besitzt der bei der Komplementfusion implizit erhaltene Normalisator $N_{C/B}(U/B)$ das volle Urbild $N_C(U)$, das wegen (165) gleich dem Normalisator $N_G(U)$ ist.

V.8.2. Ist G auflösbar, so existiert eine Normalreihe $G = N_0 \geq N_1 \geq \cdots \geq N_n$ mit elementar abelschen Faktoren. Rechnet man induktiv modulo dieser Faktoren, so kann man im i-ten Schritt annehmen, daß ein Repräsentantensystem aller Untergruppen von G/N_{i-1} – und damit aller Untergruppen über N_{i-1} – bekannt ist und die Konjugiertenklassen aller Untergruppen von G/N_i bestimmt werden sollen. Dann ist $N_{i-1}/N_i \lhd G/N_i$ elementar abelsch und eine einfache Basisabzählung der Basen von möglichen Teilräumen liefert alle Untergruppen von N_{i-1}/N_i.

Die Parametrisierung aus Lemma (166) liefert dann ein Repräsentantensystem aller Untergruppen von G/N_i, mit dem die Berechnung im nächsten Schritt fortgesetzt werden kann.

Da N_{i-1}/N_i elementar abelsch ist, ist N/B stets ein Vektorraum. Die notwendige Bestimmung der Klassen von Komplementen reduziert sich somit im wesentlichen auf eine Berechnung der 1-Kohomologiegruppe und die Bestimmung der C/B-Klassen von Komplementen. Letzteres ist bereits in V.3.2 beschrieben.

Nach (167) erhält man dabei gleichzeitig die für den nächsten Schritt benötigten Normalisatoren als Stabilisatoren.

V.8.3. Im Gegensatz zu dem üblicherweise verwandten cyclic extension Algorithmus, der in [Neu1960, Mni1992] beschrieben ist, baut dieser Algorithmus die Gruppen nicht von unten, sondern von oben auf. Da die Untergruppen jeweils aus ihren Schnitten mit einer elementar abelschen Reihe konstruiert werden, sei dieses Vorgehen „elementary abelian extension“, kurz Eae, getauft. Per Konstruktion erhält man zu den Untergruppen nicht nur eine Subnormalreihe, sondern sogar eine elementar abelsche Reihe.

Zusätzlich genügt es, auf jeder Stufe jeweils nur Repräsentanten der Konjugiertenklassen von Gruppen im Speicher zu behalten und man muß nicht eine komplette Liste der „Zuppos“ speichern. Des weiteren entfallen eine ganze Reihe an sonst notwendigen Konjugationstests. Insbesondere bei größeren Gruppen sollte Eae daher gegenüber cyclic extension im Vorteil sein. Tabelle 2 zeigt die Laufzeiten einiger Beispiele. Diese unterstützen die Vermutung.

Im Nachhinein stellte sich heraus daß ein ähnlicher Algorithmus auch von M. SLATTERY implementiert wurde. Seine Beobachtungen decken sich mit den hier gemachten [Sla].

Ein weiterer Vorteil für Eae zeigt sich, wenn nur nach Untergruppen mit gewissen Eigenschaften gesucht werden soll (als Beispiel mag die – hier im Hintergrund stehende – Suche nach invarianten Untergruppen dienen): In der Gruppentheorie interessierende Eigenschaften gehen oft auf Faktorgruppen, aber nicht immer auf Untergruppen über. Insofern läßt

Gruppe	$\|G\|$		#Klassen	t_{Eae}	t_{CE}
$M_{12}.2M6$ $= 3_+^{1+2} : D_8$	348	$= 2^7 3$	135	139	46
$\frac{1}{2}[3^4 : 2^2]_c D_4 = T_{12}N_{209}$	1296	$= 2^4 3^4$	370	212	307
Borel$(GL_3(4))$	1728	$= 2^6 3^3$	298	156	244
$A_4^{\times 3}$	1728	$= 2^6 3^3$	543	280	581
$N_{PGL_3(23)}(\mathrm{Syl}_{11})$	2904	$= 2^3 3 \cdot 11^2$	43	22	52
Borel$(SL_4(3))$	5832	$= 2^3 3^6$	1867	1009	4926
$ThM11$ $= 7^2 : (3 \times 2S_4)$	7056	$= 2^4 3^2 7^2$	70	45	110
Borel$(GL_2(41))$	65600	$= 2^6 5^2 41$	592	761	8309

Zeiten sind in Sekunden auf einem 50Mhz 486PC unter FreeBSD Unix

TABELLE 2. Laufzeitvergleich zur Verbandsberechnung

sich der Algorithmus mit relativ geringem Aufwand auf die Suche nach solchen eigenschaftsbestimmten Untergruppen aufrüsten. Sofern es von diesen nur hinreichend wenige gibt, funktioniert dies selbst in solchen Fällen, in denen der gesamte Untergruppenverband aufgrund seiner Größe nicht mehr bestimmt werden kann.

Nicht verschwiegen werden soll der größte Nachteil von Eae gegenüber cyclic extension: Ist eine Gruppe nicht auflösbar, so gelingt es cyclic extension dennoch, die Untergruppen zu konstruieren, sofern nur das auflösbare Residuum (der kleinste Normalteiler mit auflösbarer Faktorgruppe) in einer Bibliothek identifiziert wird, und dadurch alle perfekten Untergruppen des auflösbaren Residuums identifiziert werden können. Dies ist bei Eae nicht möglich, da dieser insgesamt eine auflösbare Struktur der Gruppe benötigt[3]. Ist eine Gruppe – was in der Praxis recht häufig geschieht – jedoch mit einem großen auflösbaren Normalteiler und nicht auflösbarer Faktorgruppe versehen, so kann man natürlich zunächst den Untergruppenverband der Faktorgruppe mittels cyclic extension bestimmen, und diesen dann mittels Eae auf die gesamte Gruppe ausweiten. Dabei genügt es dann, die perfekten Untergruppen der Faktorgruppe zu kennen, was erheblich wahrscheinlicher ist, als die – für cyclic extension benötigte – Kenntnis *aller* perfekten Untergruppen.

V.8.4. Wir kehren nun zum Fall eines nichttrivialen H zurück. Bestimmt werden sollen jetzt die Untergruppen von G, die unter H invariant sind. Dies soll wiederum nur bis auf Konjugation in G geschehen. Der Einfachheit der Darstellung halber betten wir G und H in das semidirekte Produkt $G \rtimes H$ ein, so daß H per Konjugation auf G operiert und wir Elemente aus G mit solchen aus H multiplizieren können.

Es stellt sich aber das Problem, daß mit $U \leq G$ unter H invariant nicht auch U^g für $g \in G$ unter H invariant sein muß. Deshalb definieren wir

(168) DEFINITION: Eine *Konjugiertenklasse von H-invarianten Untergruppen* besteht — so welche existieren – aus den H-invarianten Untergruppen einer G-Konjugiertenklasse.

[3]Eine theoretisch mögliche Erweiterung auf den Fall eines nicht auflösbaren N soll hier nicht weiter untersucht werden.

Jedoch gilt: Ist U unter H invariant, so ist U^g unter $g^{-1}Hg$ invariant. Ist auch U^g unter H invariant, so ist U somit ebenfalls gHg^{-1}-invariant. Wir nennen (da mit dem Inversen, beziehungsweise „von der anderen Seite" operiert wird) ein solches Bild der operierenden Gruppe auch das *Jugierte* von H.

V.8.5. Dies wirft das Problem auf, wann zu $U \leq G$ ein $g \in G$ existiert, so daß U^g unter H invariant ist. Wir betrachten zunächst den Fall eines U, das Komplement zu einem H-invarianten Normalteiler $N \lhd G$ ist. Die Elemente aus G sind also eindeutig in der Form $g = un$ mit $u \in U$ und $n \in N$ darstellbar. Da U sich selbst normalisiert, genügt es mit $n \in N$ zu konjugieren, und es gilt:

$$u^n = n^{-1}un = u \cdot [u, n] = u \cdot (n^{-1})^u \cdot n.$$

Das mit n konjugierte Komplement zu U besteht also aus Produkten $u \cdot [u, n]$. Invarianz eines konjugierten Komplementes unter φ bedeutet dann, daß es zu jedem $u \in U$ ein $v \in U$ gibt, so daß

$$(u[u, n])\varphi = v[v, n] \tag{169}$$

gilt. Dabei ist v durch die induzierte Operation auf G/N bereits bestimmt, es gilt $uN\bar{\varphi} = vN$ und folglich ist $u\varphi = vm$ mit $m \in N$. Damit übersetzt sich (169) zu

$$vm[vm, n\varphi] = v[v, n], \qquad \text{bzw.} \qquad m[vm, n\varphi] = [v, n].$$

Nehmen wir jetzt zusätzlich an, daß N elementar abelsch ist, so kommutieren m und $n\varphi$, und wir erhalten

$$m[v, n\varphi] = [v, n];$$

beziehungsweise in additiver Schreibweise, bei der v' und φ' die entsprechenden induzierten Automorphismen von N seien:

$$m - n(\varphi'v') + n\varphi' = -(n)v' + n.$$

Das gesuchte konjugierende Element n ist also eine Lösung des Gleichungssystems:

$$n(1 - v' + \varphi'v' - \varphi') = m. \tag{170}$$

Ist n Lösung von (170) so folgt umgekehrt die Invarianz des Komplementes nach (169) und wir erhalten somit:

(171) Lemma: Ist N elementar abelsch, so existiert ein N-Konjugiertes von U, das unter H invariant ist, genau dann, wenn das Gleichungssystem

$$n(1 - \varphi')(1 - v') = n(1 - v' + \varphi'v' - \varphi') = m, \qquad u\varphi = vm,$$

wobei u ein Erzeugendensystem von U und φ eines von H durchläuft (wodurch v und m impliziert werden), eine nichttriviale Lösung n besitzt. Diese Lösung ist dann ein konjugierendes Element.

V.8.6. Nun soll die Situation von Lemma (166) auf invariante Untergruppen erweitert werden. Es sei N ein H-invarianter Normalteiler und $U \leq G$ unter H invariant. Dann sind $A = \langle N, U\rangle$ und $B = U \cap N$ ebenfalls H-invariant.

(172) LEMMA: Ist $V \leq G$ unter H invariant, so auch $N_G(V)$

Beweis: Sei $\varphi \in H$ und $g \in N_G(V)$. Dann ist (indem wir G und H in das semidirekte Produkt $G \rtimes H$ einbetten, können wir annehmen, daß φ auch per Konjugation operiert)

$$V^{(g\varphi)} = ((V\varphi^{-1})^g)\varphi \overset{V\varphi^{-1}=V}{=} (V^g)\varphi = V$$

und folglich $g\varphi \in N_G(V)$. □

Damit sind auch $N_G(A)$ und $N_G(B)$ und deren Schnitt C unter H invariant, und U/B ist ein unter der induzierten Operation auf C/B invariantes Komplement.

Sind U und U' konjugiert und unter H invariant, so sind ebenfalls wie oben die dazugehörigen A, A' und B, B' konjugiert und unter H invariant. Jedoch folgt aus Konjugiertheit nicht auch Invarianz: Ist U ein invariantes Komplement zu A und B und sind A' und B' Konjugierte dieser Gruppen, so gibt es zwar auch dort Komplemente, die zu konjugierten Untergruppen von U gehören. Selbst wenn A' und B' unter H invariant sind, so sind diese Komplemente jedoch nicht notwendigerweise invariant unter H:

(173) BEISPIEL: Es sei

$$G = S_4(4) = \langle (1, 2, 3, 4), (1, 2)\rangle \quad \text{und} \quad N = V_4 = \langle (1, 2)(3, 4), (1, 3)(2, 4)\rangle \lhd G.$$

Es sei $\varphi \in \mathrm{Aut}(G)$ der innere Automorphismus zu $(1, 2)(3, 4)$ und $H = \langle\varphi\rangle \leq \mathrm{Aut}(G)$. Dann ist $G/N \cong S_3$ und φ operiert auf G/N trivial. Die drei konjugierten 2-Sylowgruppen der Faktorgruppe $U_1/N = \langle N, (3, 4)\rangle/N$, $U_2/N = \langle N, (1, 3)\rangle/N$ und $U_3/N = \langle N, (2, 3)\rangle/N$ sind also allesamt unter dem induzierten (trivialen) Automorphismus der Faktorgruppe invariant. Jedoch besitzt U_1 mit $\langle(1, 2)\rangle$ und $\langle(3, 4)\rangle$ zwei unter φ invariante Komplemente zu N in U_1, die eine Konjugiertenklasse von Komplementen bilden, während dies für U_2 und U_3 nicht gilt. Für U_2 zum Beispiel sind die entsprechenden Komplemente $\langle(1, 3)\rangle$ und $\langle(2, 4)\rangle$, von denen keines unter φ invariant ist.

Wählen wir nun Repräsentanten für A und B aus, so genügt es daher nicht, nur zu diesen beiden Gruppen nach invarianten Komplementen zu suchen, sondern wir müssten im Prinzip auch alle Konjugierten von A und B betrachten. Dies widerspricht natürlich der Idee der Auswahl von Repräsentanten.

Statt A und B mit g zu konjugieren und dort nach H-invarianten Komplementen zu suchen, können wir aber auch nach unter jugierten Operationen $H^{g^{-1}}$ invarianten Komplementen suchen, und diese dann wieder mit g konjugieren, um die eigentlichen invarianten Untergruppen zu erhalten.

Es soll nun untersucht werden, mit welchen Elementen g die Operation von H jugiert werden muß, damit die Suche nach gHg^{-1}-invarianten Untergruppen schließlich zu einem Repräsentantensystem aller H-invarianter Untergruppen führt.

V.8.7. Ist $u \in N_G(H)$, so liefern g und gu offenbar dieselben Jugierten von H. Wir brauchen daher für die jugierenden Elemente g nur jeweils einen Vertreter aus jeder Linksnebenklasse $G/N_G(H)$ zu berücksichtigen.

Wir wählen nun zunächst einen Repräsentanten für A aus, der unter H invariant ist (de facto werden wir ein Repräsentantensystem der A aus dem vorangegangenen Schritt erhalten). Dann ist die Untergruppe A genau dann unter $H^{(g^{-1})}$ invariant, wenn sie für $n \in N_G(A)$ unter $H^{(ng)^{-1}}$ invariant ist. Wir wählen somit ein Repräsentantensystem $\{t_i\}$ der Doppelnebenklassen $N_G(A)\backslash G/N_G(H)$, für die A^{t_i} unter H invariant (beziehungsweise äquivalent: A unter $H^{t_i^{-1}}$ invariant) ist.

Nun sind diejenigen $B \leq N$ zu bestimmen, die unter A normal sind und unter mindestens einer der jugierten Gruppen $H^{t_i^{-1}}$ invariant sind. Zu diesem Zwecke betrachten wir alle unter H invarianten Untergruppen von N und wählen aus deren Bildern unter allen $t_i{}^{-1}$ diejenigen aus, die normal in A sind. Für diese bestimmen wir wie oben ein Repräsentantensystem der $N_G(A)$ Klassen.

Für einen Repräsentanten B sei wiederum $C = N_G(A) \cap N_G(B)$ und $\{s_j\}$ ein Repräsentantensystem der Nebenklassen $C\backslash N_G(A)$.

Jedes Paar $s_j t_i$ bestimmt nun ein konjugierendes Element g modulo C und $N_G(H)$. Da B unter $H^{((s_j t_i)^{-1})}$ invariant sein soll, betrachten wir nur noch solche Paare $s_j t_i$, für die dies gilt.

Schließlich suchen wir in der Faktorgruppe A/B Komplemente zu N/B, die unter der induzierten Operation von mindestens einem der $H^{(s_j t_i)^{-1}}$ invariant sind. Dies geschieht (da N/B elementar abelsch ist), indem zunächst ein Repräsentantensystem der Konjugiertenklassen von Komplementen von N/B in A/B über die 1-Cohomologiegruppe bestimmt wird.

Zu jedem dieser Repräsentanten untersuchen wir nun, ob dieser ein N-Konjugiertes besitzt, das unter der induzierten Operation eines der $H^{(s_j t_i)^{-1}}$ invariant ist. Dies kann – nebst Bestimmung eines konjugierenden Element $n \in N$ – mittels Lemma (171) geschehen. Existiert ein solches n, so ist $ns_j t_i$ ein Element, welches das Urbild U des Komplements auf eine H-invariante Untergruppe U' konjugiert, so daß deren A' und B' zur Klasse von A und B gehören.

Die Komplemente, für die ein solches n existiert, werden schließlich auf lokale Konjugation in C/B getestet. Dabei lohnt es sich nicht, dies wie im gewöhnlichen Fall bereits durch eine Operation auf der Cohomologiegruppe durchzuführen, da bei bereits reduzierter Repräsentantenauswahl dann eine größere Menge an jugierten Abbildungen betrachtet werden müsste.

Die so erhaltenen Repräsentanten werden abschließend mit den passenden $ns_j t_i$ konjugiert, um letzlich invariante Untergruppen zu erhalten.

Umgekehrt liefert Konjugation jeder invarianten Gruppe mit geeignetem $(s_j t_i)^{-1}$ ein unter den $s_j t_i$-jugierten Abbildungen invariantes Komplement in C/B. Wir erhalten also auf diese Weise Repräsentanten aller invarianten Gruppen. Wie oben sind solche Gruppen in G konjugiert, falls die zugehörigen Komplemente unter C/B konjugiert sind. Fassen wir zusammen:

(174) LEMMA: Es sei $N \lhd G$ abelsch und unter H invariant und $\mathfrak{A}$ ein Repräsentantensystem der unter H invarianten Untergruppen, die N enthalten. Zu $A \in \mathfrak{A}$ sei $\mathfrak{B}_A$ ein Repräsentantensystem der $N_G(A)$-Klassen von Untergruppen, die echt unter N liegen, in A normal sind und für einen Doppelnebenklassenvertreter x von $N_G(A)\backslash G/N_G(H)$ unter einem jugierten $H^{x^{-1}}$ invariant sind, für das gilt, daß A unter $H^{x^{-1}}$ invariant ist. Zu $B \in \mathfrak{B}_A$ sei $\mathfrak{U}_{A,B}$ wie in Lemma (166) definiert.

Zu $A \in \mathfrak{A}$ sei $\{t_i\}$ ein Repräsentantensystem der Doppelnebenklassen $N_G(A)\backslash G/N_G(H)$, für die A unter $H^{t_i^{-1}}$ invariant ist. Zu $b \in \mathfrak{B}_A$ sei $\{s_j\}$ ein Repräsentantensystem der Nebenklassen $(N_G(A) \cap N_G(B))\backslash N_G(A)$ und

$$K_B = \{s_j t_i \mid B \quad \text{invariant unter} \quad H^{(s_j t_i)^{-1}}\}.$$

Zu $U \in \mathfrak{U}_{A,B}$ sei

$$n_U := \begin{cases} ng & \begin{array}{l}\text{falls ein } n \in N \text{ und ein } g \in K_B \text{ existieren,}\\ \text{so daß } U/B \text{ unter } H^{(ng)^{-1}} \text{ invariant ist;}\end{array} \\ & \\ 0 & \text{sonst.} \end{cases}$$

Ist schließlich $\mathfrak{B}$ ein Repräsentantensystem der G-Klassen invarianter Untergruppen in N, dann ist

$$R := \mathfrak{A} \cup \mathfrak{B} \cup \bigcup_{A\in\mathfrak{A}} \bigcup_{B\in\mathfrak{B}_A} \bigcup_{\substack{U\in\mathfrak{U}_{A,B}\\ 0\neq n_U}} U^{n_U}$$

ein Repräsentantensystem der G-Klassen von unter H invarianten Untergruppen.

(175) BEMERKUNG: Mit den $s_j t_i$ betrachten wir zu jedem B Repräsentanten der Doppelnebenklassen $C_{A,B}\backslash G/N_G(H)$. Die zu Repräsentanten $s_j t_i$ und $s_k t_l$ gehörenden Klassen können dabei noch fusionieren. Offenbar braucht man zu jeder Klasse nur jeweils einen Repräsentanten zu berücksichtigen. Wie in [Lau1982] gezeigt, fusionieren solche Klassen dann und nur dann, wenn $t_i = t_l$ gilt, die Fusion findet dann unter $\mathrm{Stab}_{N_G(H)}(N_G(A)t_i) = N_G(H) \cap N_G(A)^{t_i}$ statt.

V.8.8. Wir erweitern damit jetzt die Konstruktion aus Abschnitt V.8.2 auf die Bestimmung von Repräsentanten der invarianten Untergruppen. Eine G-Normalreihe mit elementar abelschen Faktoren erhalten wir wiederum durch iterierte Anwendung von (158)

Für die elementar abelschen Faktoren der Reihe können dann mit Hilfe der MeatAxe [LMR1994] jeweils alle invarianten Untermoduln bestimmt werden. Diese liefern $\mathfrak{B}$ und die $\mathfrak{B}_A$. Die Suche nach invarianten Komplementen, wie in V.8.7 beschrieben, liefert dann die Untergruppen $U \in \mathfrak{U}_{A,B}$, für die $n_U \neq 0$ ist. Konjugation dieser Untergruppen mit n_U liefert dann die nach Lemma (174) noch fehlenden Untergruppen oberhalb des i-ten Normalteilers. Die induktive Vorgehensweise ist ansonsten wie in V.8.2.

(176) BEMERKUNG: Da die Berechnung von Doppelnebenklassen nach dem Verfahren von M.SLATTERY [Sla1992] (eine genauere Beschreibung findet sich in [Hul1993, Abschnitt

2.5.3]) ebenfalls induktiv geschieht, kann man bei der notwendigen Bestimmung der Doppelnebenklassen jeweils die im vorangegangenen Schritt bestimmte Information weiterverwenden.

V.8.9. Da der Konstruktionsprozeß über eine Kette von wachsenden Faktoren voranschreitet, sind in jedem neuen Schritt mehr Komplementfälle zu untersuchen. Andererseits lassen sich dabei – insbesondere im letzten Schritt – die Eigenschaften der potentiellen Komplemente bereits recht genau beschreiben.

Bisweilen – so zum Beispiel nach (118) im hier eigentlich interessierenden Fall – sind nur solche Untergruppen von Interesse, die weitere Einschränkungen, so z.B. Teilereigenschaften der Ordnung, erfüllen. Ist nun bereits a priori klar, daß gewisse Komplementberechnungen nur noch zu nicht interessierenden Gruppen führen werden, so brauchen sie natürlich nicht mehr ausgeführt zu werden.

Insbesondere im letzten Schritt können so oft eine ganze Reihe kleine Untergruppen, die unter A daher viele Komplementklassen bilden, welche unter der Operation von $N(A) \cap N(B)$ dann jedoch wieder fusionieren, ignoriert werden, was zur starken Beschleunigung des Algorithmus führt.

KAPITEL VI

Katalog

Der in den vorangegangenen Kapiteln beschriebene Algorithmus ist vom Autor in GAP implementiert worden. Für viele Teilprobleme (wie zum Beispiel Stabilisator- oder Konjugiertenklassenberechnungen, im wesentlichen alles, was nicht in den vorangegangenen Kapiteln explizit beschrieben wurde) wurden die Funktionen benutzt, die bereits durch die GAP-Bibliothek zur Verfügung gestellt sind. Darüberhinaus wurde in einigen Fällen eine separate Implementation des Mengenstabilisators für Permutationsgruppen verwandt, die von J. LEON stammt [Leo1991].

Mittels dieses Programmes wurden Repräsentantensysteme für die transitiven Gruppen bis Grad 30 berechnet. (Da 31 eine Primzahl ist, waren alle Gruppen dieses Grades bereits vorher bekannt.) Diese Listen sollen – nachdem sie nochmals auf Korrektheit überprüft worden sind – der Allgemeinheit sowohl als Gruppenbibliothek in GAP, als auch als einfache Erzeugerlisten, zur Verfügung gestellt werden[1]. Auf einen Abdruck im Rahmen dieser Arbeit wurde verzichtet, da zum einen die zum Teil sehr umfangreichen Listen ein mehrbändiges Werk erforderlich gemacht hätten. (Selbst bei kompakter Darstellung kann man nur etwa 30-40 Gruppen mit Permutationserzeugern auf einer Seite abdrucken. Alleine Grad 24 hätte dann über 500 Seiten benötigt.) Zum anderen können derart umfangreiche Listen wohl kaum noch sinnvoll von Hand benutzt werden und sollten daher auch direkt in rechnerlesbarer Form vorliegen. Schließlich bedeutet die Erzeugung solcher Listen einen nicht unerheblichen Aufwand. Er soll erst dann unternommen werden, wenn die Zuverlässigkeit der Listen durch eine Reihe zusätzlicher Tests bestätigt worden ist.

Neben reinen Erzeugerlisten sollen auch Tabellen angegeben werden, die es gestatten, Fehler (auch wenn solche nicht intendiert sind) aufzuspüren, beziehungsweise die Listen mit unabhängig gewonnenen zu vergleichen. Hierzu geben wir im wesentlichen die vorkommenden Basen, sowie die Anzahl der aus ihnen hervorgehenden transitiven Gruppen an. Da die Bestimmung der Basen für gewöhnlich auch den Großteil der Berechnungen ausmacht, wäre notfalls auch eine Neuberechnung, die von diesen Listen von Basen ausgeht, mit verhältnismäßig geringem Aufwand möglich.

VI.0.10. Der Aufwand der Berechnung wächst exponentiell. Für die Grade 8, 9 und 10 benötigt ein 133Mhz Pentium PC unter FreeBSD je nur zwei bis drei Minuten. Grad 12 benötigt etwa eine halbe Stunde, Grad 16 etwa drei Stunden. Die Grade 18 oder 20 können in je etwa ein bis zwei Tagen durchgeführt werden. Die höheren Grade benötigen teilweise bereits mehrere Tage für die Gruppen zu einzelnen Blockoperationen A.

[1] Für diesbezügliche Nachfragen ist der Autor per eMail erreichbar: `Alexander.Hulpke@math.rwth-aachen.de`

Die Rechnungen für Grad 24 haben sich dabei als besonders aufwendig herausgestellt. Dadurch war es in der bis zur Abgabe der Arbeit zur Verfügung stehenden Zeit (und mit der zur Verfügung stehenden Rechnerausstattung) nicht möglich, die Gruppen zu einem Blocksystem mit Blöcken von Ordnung 3 und einer Operation A von Typ S_3 zu bestimmen. Eine solche Berechnung ist nach Abgabe der Arbeit nachgeholt worden[2]. Da eine sequentielle Berechnung alleine dieses Falls wohl mehrere Wochen benötigen würde, soll dabei versucht werden, den Konstruktionsalgorithmus für Subpotenzen unter GAP-MPI [Coo1996] zu parallelisieren, und die Rechenzeit auf einem Pool von Workstations damit wieder in akzeptable Bereiche zu rücken.

VI.1. Korrektheit der Ergebnisse

Wie in der Einleitung beschrieben, ist die Geschichte der Klassifikation transitiver Gruppen auch eine Geschichte der Korrekturen und Irrtümer. Viele dieser Fehler beruhen zwar sicherlich darauf, daß bei der Behandlung umfangreicher Fallunterscheidungen „von Hand“ Dinge übersehen wurden. Fehler dieser Art sollten einem Computer nicht unterlaufen. Die große Zahl der benutzten Algorithmen und Implementationen, die – über die in dieser Arbeit beschriebenen Verfahren hinaus, deren Implementation aus etwa 3000 Zeilen Code besteht – insbesondere auch einen Großteil der GAP-Bibliothek umfassen, macht es aber unumgänglich, sich Gedanken über mögliche Fehlerquellen sowie deren Aufspürung und Beseitigung zu machen. Die möglichen Fehlerquellen kann man grob wie folgt aufzählen:

a) Fehler bei der Übertragung der Ergebnisse in Listen: Diese sollten unwahrscheinlich sein, da die Übertragung soweit möglich automatisiert durchgeführt wurde.
b) Konzeptuelle Fehler: Die benutzten Algorithmen sind in den vorangegangenen Kapiteln ausführlich dargestellt und begründet. Ich hoffe, den Leser bis hierhin von der Korrektheit derselben überzeugt zu haben.
c) Fehler bei der Implementation des beschriebenen Algorithmus
d) Fehler in anderen verwendeten Algorithmen oder deren Implementationen in GAP
e) Compiler- und Betriebssystemfehler
f) Hardwarefehler

Mögliche Fehler können im wesentlichen zwei Auswirkungen haben:

1. Mehrere der erhaltenen Repräsentanten sind konjugiert.
2. Die Repräsentanten decken nicht alle Klassen ab.

Fehler der ersten Art sind verhältnismäßig harmlos und leicht zu entdecken: Zunächst kann man mit Konjugationsinvarianten (siehe (14)) für die allermeisten der erhaltenen Repräsentanten Konjugation ausschließen, lediglich für die verbliebenen sehr ähnlichen Paare ist ein Konjugationstest in der symmetrischen Gruppe durchzuführen.

Fehler der zweiten Art sind ungleich schwieriger zu entdecken. Hier kann man zum einen versuchen, bekannte Gruppen in den Listen zu finden. Zum anderen kann man versuchen, die Fehler der Typen c)-f) durch Änderung der benutzten Software oder Hardware aufzuspüren. Dies ist am einfachsten bei Fehlern der Sorten e) und f), da dies einfach

[2] Siehe Kapitel VII.

durch erneute Berechnungen auf einem anderen Computer geschehen kann. Fehlertypen c) und d) sind hierbei erheblich unangenehmer, da dies teilweise erheblichen Aufwand für Neuimplementationen bedeuten würde. Um dieses zu vermeiden bieten sich zwei Auswege: Zunächst kann man Parameter der Algorithmen ändern (zum Beispiel die benutzte Anordnung der Gruppen, oder auch die Initialisierung des Zufallsgenerators), was dafür sorgt, daß andere Repräsentanten gewählt werden. Dies bedeutet, daß die einzelnen Teilalgorithmen mit anderen Eingabewerten laufen. Konzeptuelle Fehler der Implementationen lassen sich hiermit natürlich nicht aufspüren.

Der andere Ausweg ist, eine Reihe von kritischen Algorithmen lediglich „dumm" – das heißt auf sehr elementarer Ebene – zu implementieren. Solche Implementationen sind gemeinhin einfacher auf ihre Korrektheit überprüfbar, leider benötigen sie zumeist auch signifikant mehr Speicherplatz und Rechenzeit, dies kann aber womöglich durch eine Parallelisierung ausgeglichen werden. Stichprobenweise mögen solche Tests allerdings auch sonst verwendbar sein.

Durch Verwendung solcher Tests sollte es zumindestens möglich sein, die Korrektheit der Listen soweit menschenmöglich nachzuweisen. Dies ist für die berechneten Ergebnisse zum großen Teil noch durchzuführen, wobei noch zu entscheiden ist, welchen Aufwand man hierzu treiben möchte. Dem kritischen Leser sei unbenommen, eine erneute, vollkommen unabhängige, Klassifikation durchzuführen, und das Ergebnis mit den vom Autor erhaltenen Listen zu vergleichen.

VI.2. Beobachtungen

An verschiedenen Stellen der Arbeit wurde die Behandlung einiger Einzelfälle mit der Bemerkung abgeschlossen, daß diese in der Praxis nicht, oder nur selten, auftreten. Diese Behauptungen sollten tunlichst anhand der Ergebnisse belegt werden, weshalb hier eine Reihe an Ergebnissen, die man aus den nachfolgend angegebenen Listen folgern kann, angegeben werden sollen:

1. Aufblasungen stellen nur ein Minorität der transitiven Gruppen eines Grades dar.
2. Die Mehrzahl aller Gruppen wird zu kleinen Blocksystemen erhalten.
3. Die Blockoperationen der Normalisatoren erfüllen die Bedingungen aus (135). Allerdings treten mit wachsender Blockanzahl (beziehungsweise steigender Komplexizität der Subpotenzen) immer mehr „mittelgroße" Blockoperationen auf.
4. Die Anzahl transitiver Gruppen von Grad n steigt mit wachsender Teilerzahl von n sehr stark an. Für Grad 32 sind mehrere hunderttausend Gruppen zu vermuten.
5. Ist (in den Bezeichnungen aus III.2.6) $S\varphi \leq R$ eine transitive Untergruppe der Operation $R = N\varphi$ des Normalisators $N = N_{S_n}(M)$ auf den Bahnen von M, so besitzt das Urbild S/M meist mindestens ein Komplement zu K/M, das heißt, die meisten transitiven Untergruppen $S\varphi$ führen auch zu einer transitiven Gruppe von Grad n, die M als Basis besitzt. (Hierbei ist zu berücksichtigen, daß nach VI.3.1 die Tabellen Gruppen nur bei zugehörigen Blocksystemen aufführen, in Wahrheit sind daher noch mehr Einträge ungleich Null.)

Mit Ausnahme von Punkt 3 scheint wahrscheinlich, daß diese Aussagen auch für höhere Grade gelten werden.

(177) BEMERKUNG: Betrachtet man die erhaltenen Gruppen selber (diese Information kann man nicht direkt den nachfolgend abgedruckten Tabellen entnehmen, sondern muß die Listen der Gruppen untersuchen), so stellt man fest, daß nur eine Minderheit (typischerweise weniger als 5 Prozent) der Gruppen zwei zugehörige Blocksysteme besitzen. Für diese Gruppen müssen bei der Konstruktion aufwendige Konjugationstests durchgeführt werden; da sie selten auftreten macht dies aber keine Schwierigkeiten.

VI.3. Beschreibung der Listen

In den folgenden Abschnitten finden sich Listen, die die transitiven Gruppen von Grade 16 beschreiben. Auf eine erneute Aufnahme der Gruppen bis Grad 15 wurde verzichtet, Listen dieser Gruppen finden sich in [CHM]. Auf die Gruppen dieser Grade wird zum Teil mit Nummern verwiesen. Diese Nummern sind für jeden Grad separat vergeben. Die Anordnung entspricht dabei [CHM] und sollte mit [BM1983, But1993] übereinstimmen. Die gleiche Anordnung wird in GAP (und vermutlich auch in Magma) benutzt.

Entsprechende Listen bis Grad 30 wurden ebenfalls erstellt. Ein Abdruck hätte allerdings den Umfang dieser Arbeit mehr als verdoppelt, sie können auf Wunsch vom Autor bezogen werden. Die Anzahlen für die einzelnen Grade finden sich in Tabelle 1 in Kapitel I.

Die Listen sind innerhalb eines Grades nach Blockgröße und Blockoperation (ein transitiver Normalteiler einer primitiven Gruppe, in den vorangegangenen Kapiteln mit A bezeichnet) geordnet. Zu jeder Blockoperation werden die auftretenden Basen (zuvor mit M bezeichnet) angegeben und mit einem Buchstaben als Namen gekennzeichnet. Zu jeder Basis ist ihre Größe, der Typ der (transitiven) Operation des Normalisators auf den Bahnen (NTyp), sowie die Anzahl transitiver Gruppen, die diese Gruppe als Basis besitzen, notiert.

Darauf folgt eine Tabelle, deren Zeilen den möglichen Operationen auf den Blöcken entsprechen.

Die Spalten der Tabelle entsprechen den zuvor angegebenen Basen, die Spalte $\emptyset$ entspricht dabei der trivialen Basis. Die in dieser Spalte angegebenen Gruppen sind daher Aufblasungen.

Die Tabelleneinträge geben dann die Anzahl transitiver Gruppen mit entsprechender Basis und Blockoperation an. Die Spaltensummen sind daher gleich den bei den Basen angegebenen Anzahlen.

Abschließend ist zur Vollständigkeit noch die Anzahl primitiver Gruppen (entsprechend der Angaben von C. SIMS, siehe I.1.2) und die Gesamtanzahl angegeben.

VI.3.1. Um den Tabellenumfang akzeptabel zu halten, wurde jede transitive Gruppe nur *einmal* aufgenommen, und zwar entsprechend eines ihr zugehörigen Blocksystems. Zum Beispiel (vergleiche (43)) ist $V_4 \wr S_4$ bezüglich des zugehörigen Blocksystems von Ordnung 2 mit Basis von Ordnung 16 (Basis D) sowie Operation $[2^4]S_4 = 2 \wr S_4$ der Faktorgruppe auf den Blöcken (Typ 44) gezählt. Zum Blocksystem mit Blöcken von Ordnung 4 besitzt $V_4 \wr S_4$ eine Basis, die äquivalent zu Basis F bei Blockordnung 4 ist. Zu dieser Basis existiert (laut Tabelle) eine transitive Gruppen mit Blockoperation S_4. Dies ist die

Gruppe

$$[V_4^4]S(4)_{24} = \langle (1,2)(3,4), (1,8,4,6)(2,5,3,7)(10,11)(13,15),$$
$$(1,8,12,15,4,5,9,16)(2,7,10,14,3,6,11,13)\rangle\,,$$

aber diese besitzt kein Blocksystem mit Blöcken von Ordnung 2.

VI.4. Grad 16

VI.4.1. Blockgröße 2.

Operation Typ 1, $S2$:

$A = \langle (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)\rangle$

$|A| = 2$ NTyp: 50 90 Gruppen

$B = \langle (1,2)(3,4)(5,6)(7,8), (9,10)(11,12)(13,14)(15,16)\rangle$

$|B| = 4$ NTyp: 47 195 Gruppen

$C = \langle (1,2)(3,4)(9,10)(11,12), (5,6)(7,8)(13,14)(15,16), (9,10)(11,12)(13,14)(15,16)\rangle$

$|C| = 8$ NTyp: 44 390 Gruppen

$D = \langle (1,2)(3,4), (5,6)(7,8), (9,10)(11,12), (13,14)(15,16)\rangle$

$|D| = 16$ NTyp: 44 190 Gruppen

$E = \langle (1,2)(7,8)(11,12)(13,14), (3,4)(7,8)(9,10)(13,14), (5,6)(7,8)(9,10)(11,12), (9,10)(11,12)(13,14)(15,16)\rangle$

$|E| = 16$ NTyp: 48 148 Gruppen

$F = \langle (1,2)(7,8)(11,12)(13,14), (3,4)(5,6)(11,12)(15,16), (5,6)(7,8)(13,14)(15,16), (5,6)(7,8), (9,10)(11,12)\rangle$

$|F| = 32$ NTyp: 44 303 Gruppen

$G = \langle (1,2)(7,8), (3,4)(7,8), (5,6)(7,8), (9,10)(11,12), (9,10)(13,14), (11,12)(15,16)\rangle$

$|G| = 64$ NTyp: 47 176 Gruppen

$H = \langle (1,2)(9,10), (3,4)(13,14), (5,6)(9,10), (5,6)(15,16), (7,8)(9,10), (7,8)(13,14), (9,10)(11,12)\rangle$

$|H| = 128$ NTyp: 50 155 Gruppen

$I = \langle (1,2), (3,4), (5,6), (7,8), (9,10), (11,12), (13,14), (15,16)\rangle$

$|I| = 256$ NTyp: 50 50 Gruppen

Anzahlen:

	∅	A	B	C	D	E	F	G	H	I
1	0	2	2	2	2	0	2	2	2	1
2	0	3	6	11	4	9	10	5	3	1
3	0	2	3	5	2	9	6	2	2	1
4	0	1	4	10	3	8	10	5	3	1
5	0	0	2	4	2	2	4	2	2	1
6	1	4	4	4	4	0	4	4	4	1
7	1	0	3	4	4	0	4	4	3	1
8	1	1	4	4	4	0	4	4	4	1
9	1	8	18	46	8	22	26	10	6	1
10	1	1	15	28	8	14	10	6	3	1
11	1	1	7	20	4	4	20	8	6	1
12	0	1	0	2	2	2	2	0	1	1
13	0	3	2	3	2	5	2	1	2	1
14	0	2	2	2	1	5	2	1	2	1
15	2	0	5	8	6	0	8	6	6	1
16	2	0	4	8	6	0	8	5	3	1
17	1	0	2	8	4	0	8	4	4	1
18	1	4	28	40	6	16	8	5	4	1
19	1	4	6	16	4	10	8	4	4	1
20	2	0	4	11	6	4	10	5	3	1
21	0	0	6	11	6	0	12	9	3	1
22	1	2	4	22	4	4	22	5	4	1
23	1	1	0	2	4	0	2	0	2	1
24	1	7	2	14	4	8	2	2	4	1
25	0	1	0	0	0	2	0	0	1	1
26	3	0	4	10	8	0	12	8	6	1
27	5	0	4	6	12	0	12	8	4	1
28	2	0	8	12	8	0	8	8	4	1
29	3	4	8	39	8	8	12	8	6	1
30	3	0	4	6	8	0	8	8	4	1
31	2	0	4	8	8	0	20	8	4	1
32	0	1	0	2	2	2	5	0	1	1
33	0	4	6	0	0	2	0	1	2	1
34	0	4	4	0	0	2	0	1	2	1
35	7	0	8	12	16	0	16	16	8	1
36	0	1	0	0	0	1	0	0	1	1
37	0	2	0	0	0	1	0	0	1	1
38	1	0	0	1	4	0	4	0	2	1
39	1	1	0	6	4	4	4	0	2	1
40	1	0	0	1	4	0	4	0	2	1
41	1	8	4	0	0	2	0	2	4	1
42	0	2	2	0	0	0	0	1	2	1
43	1	2	0	0	0	0	0	0	2	1
44	3	0	0	2	8	0	4	0	4	1
45	1	3	2	0	0	0	0	2	3	1
46	1	2	2	0	0	0	0	2	2	1
47	3	4	2	0	0	0	0	4	4	1
48	0	2	0	0	0	2	0	0	1	1
49	0	1	0	0	0	0	0	0	1	1
50	1	1	0	0	0	0	0	0	2	1

VI.4.2. Blockgröße 4.

Operation Typ 2, $E(4) = 2[x]2$:

$A = \langle(1,3)(2,4)(5,7)(6,8)(9,11)(10,12)(13,15)(14,16),$
$(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)\rangle$

$|A| = 4$ NTyp: 5 4 Gruppen

$B = \langle(1,3)(2,4)(5,7)(6,8)(13,16)(14,15),$
$(1,2)(3,4)(9,11)(10,12)(13,15)(14,16),$
$(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)\rangle$

$|B| = 8$ NTyp: 5 7 Gruppen

$C = \langle(1,3)(2,4)(9,11)(10,12)(13,16)(14,15),$
$(1,2)(3,4)(9,10)(11,12)(13,15)(14,16),$
$(5,8)(6,7)(9,12)(10,11)(13,16)(14,15),$
$(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)\rangle$

$|C| = 16$ NTyp: 5 6 Gruppen

$D = \langle(1,4)(2,3)(9,12)(10,11)(13,16)(14,15), (1,2)(3,4)(13,16)(14,15),$
$(5,7)(6,8)(9,12)(10,11)(13,14)(15,16),$
$(5,6)(7,8)(9,10)(11,12)(13,16)(14,15), (9,10)(11,12)(13,14)(15,16)\rangle$

$|D| = 32$ NTyp: 5 6 Gruppen

$E = \langle(1,3)(2,4)(9,10)(11,12)(13,16)(14,15),$
$(1,2)(3,4)(9,11)(10,12)(13,16)(14,15),$
$(5,7)(6,8)(9,10)(11,12)(13,16)(14,15),$
$(5,6)(7,8)(9,11)(10,12)(13,16)(14,15), (9,12)(10,11)(13,16)(14,15),$
$(9,11)(10,12)(13,15)(14,16)\rangle$

$|E| = 64$ NTyp: 5 4 Gruppen

$F = \langle(1,4)(2,3), (1,2)(3,4)(13,16)(14,15), (5,7)(6,8)(13,16)(14,15),$
$(5,6)(7,8), (9,11)(10,12), (9,10)(11,12), (13,16)(14,15), (13,15)(14,16)\rangle$

$|F| = 256$ NTyp: 5 2 Gruppen

Operation Typ 4, $A4$:

$G = \langle(1,4)(2,3)(5,8)(6,7)(9,12)(10,11)(13,16)(14,15),$
$(2,3,4)(6,7,8)(10,11,12)(14,15,16)\rangle$

$|G| = 12$ NTyp: 5 3 Gruppen

$H = \langle(1,4,3)(5,8,7)(10,11,12)(13,14,16),$
$(1,4,2)(5,7,8)(9,10,11)(14,16,15),$
$(1,3,2)(5,7,6)(10,11,12)(13,16,15)\rangle$

$|H| = 48$ NTyp: 5 5 Gruppen

$I = \langle(1,4)(2,3)(9,12)(10,11), (2,3,4)(6,7,8)(9,11,10)(13,15,14),$
$(5,8)(6,7)(9,12)(10,11), (9,10)(11,12)(13,14)(15,16)\rangle$

$|I| = 192$ NTyp: 5 11 Gruppen

$J = \langle(1,4)(2,3), (2,3,4)(6,7,8)(10,11,12)(13,15,14), (5,8)(6,7),$
$(9,12)(10,11), (13,15)(14,16)\rangle$

$|J| = 768$ NTyp: 5 11 Gruppen

$$K = \langle (1,4,3)(5,8,7)(9,12,11)(13,16,15),$$
$$(1,3,2)(5,7,6)(9,12,10)(14,16,15),$$
$$(2,4,3)(5,6,7)(9,11,12)(13,16,14)\rangle$$

$|K| = 2304$ NTyp: 3 8 Gruppen

$$L = \langle (1,4,3)(5,7)(6,8)(9,11)(10,12)(13,16,14),$$
$$(1,2,4)(5,7)(6,8)(9,12,10)(13,16,15), (2,4,3)(5,7,8)(13,14)(15,16)\rangle$$

$|L| = 6912$ NTyp: 5 13 Gruppen

$$M = \langle (1,4)(2,3), (2,3,4), (5,8)(6,7), (5,7,6), (9,12)(10,11), (9,11,10),$$
$$(13,16)(14,15), (13,15,14)\rangle$$

$|M| = 20736$ NTyp: 5 7 Gruppen

Operation Typ 5, $S4$:

$$N = \langle (1,4,3,2)(5,8,7,6)(9,12,11,10)(13,16,15,14),$$
$$(1,2)(5,6)(9,10)(13,14)\rangle$$

$|N| = 24$ NTyp: 5 1 Gruppe

$$O = \langle (1,4,2)(5,8,6)(9,11,12)(13,15,16),$$
$$(1,4,3,2)(6,8)(9,11)(13,14,15,16),$$
$$(1,2)(5,8,6,7)(9,10)(13,16,14,15)\rangle$$

$|O| = 384$ NTyp: 5 5 Gruppen

$$P = \langle (1,4,3)(5,7,6)(9,10,12)(13,15,14),$$
$$(1,3,2)(6,7,8)(10,11,12)(13,15,14), (1,2,3,4)(6,8)(9,11)(14,16)\rangle$$

$|P| = 1536$ NTyp: 5 5 Gruppen

$$Q = \langle (1,3,4,2)(5,6,8,7)(9,12,11,10)(13,15),$$
$$(1,2,4,3)(5,8)(9,11,12,10)(13,14,16,15),$$
$$(3,4)(5,7,6,8)(10,11)(14,15)\rangle$$

$|Q| = 4608$ NTyp: 3 9 Gruppen

$$R = \langle (1,4)(5,7,8,6)(9,12,10,11)(13,16,15,14), (1,4)(6,8)(9,12)(13,14),$$
$$(1,3,2)(5,6,7)(9,12,11)\rangle$$

$|R| = 4608$ NTyp: 5 5 Gruppen

$$S = \langle (1,4,2,3)(5,6)(10,11)(13,16),$$
$$(1,3)(2,4)(5,7)(6,8)(9,10)(11,12)(13,16)(14,15),$$
$$(1,2,3,4)(5,7)(9,11,10)(13,14,16)\rangle$$

$|S| = 9216$ NTyp: 3 3 Gruppen

$T = \langle (1,4)(7,8)(10,11)(13,14), (2,3)(7,8)(10,11)(13,14),$
$(3,4)(7,8)(11,12)(13,14), (5,8,6)(13,14,15), (6,7,8)(10,12,11),$
$(9,12)(10,11), (13,15)(14,16)\rangle$

$|T| = 13824$ NTyp: 5 5 Gruppen

$U = \langle (1,4)(7,8)(10,11)(13,14), (2,3)(7,8)(10,11)(13,14),$
$(3,4)(7,8)(10,11)(13,14), (5,6,7)(13,15,14), (9,10,11), (10,12,11),$
$(14,15,16)\rangle$

$|U| = 41472$ NTyp: 5 14 Gruppen

$V = \langle (1,4)(5,6)(9,12,11)(13,14)(15,16), (1,3,2,4)(5,6,7,8)(9,10)(14,16),$
$(6,8,7)(9,12,11)(13,15,14)\rangle$

$|V| = 82944$ NTyp: 3 8 Gruppen

$W = \langle (1,3,2,4)(5,8,7)(9,11)(13,15,14),$
$(1,2,4,3)(5,6,7,8)(9,10)(11,12)(13,15,16),$
$(2,4,3)(5,8,6)(10,11)(13,16,14,15)\rangle$

$|W| = 165888$ NTyp: 5 11 Gruppen

$X = \langle (1,4), (2,3), (3,4), (5,8), (6,8), (7,8), (9,12), (9,11), (9,10), (13,16), (13,14),$
$(15,16)\rangle$

$|X| = 331776$ NTyp: 5 5 Gruppen

Anzahlen:

	$\emptyset$	A	B	C	D	E	F	G	H	I	J	K	L
1	0	0	0	0	0	0	0	0	1	2	2	2	2
2	0	0	0	0	0	0	0	0	1	2	2	2	2
3	0	0	0	0	0	0	0	0	1	4	4	4	4
4	0	2	3	3	2	2	1	1	1	1	1	0	2
5	0	2	4	3	4	2	1	2	1	2	2	0	3

	M	N	O	P	Q	R	S	T	U	V	W	X
1	1	0	1	1	2	1	1	1	2	2	2	1
2	1	0	1	1	3	1	1	1	4	2	2	1
3	2	0	1	1	4	1	1	1	4	4	4	1
4	1	0	1	1	0	1	0	1	2	0	1	1
5	2	1	1	1	0	1	0	1	2	0	2	1

VI.4.3. Blockgröße 8.

Operation Typ 25, $E(8):7 = F_{56}(8)$**:**

$$A = \langle(1,7,8,4,2,3,5)(9,15,16,12,10,11,13),$$
$$(1,5,7,6,2,3,8)(9,11,10,13,14,16,12),$$
$$(1,3,6,5,8,2,7)(9,12,11,16,15,13,14)\rangle$$

$|A| = 448$ NTyp: 1 1 Gruppe

$$B = \langle(1,6,2,8,4,3,7)(9,10,13,11,15,16,14),$$
$$(1,6,7,2,5,4,8)(9,14,12,10,15,13,11)\rangle$$

$|B| = 448$ NTyp: 1 1 Gruppe

$$C = \langle(1,5)(2,7)(3,4)(6,8)(9,14,12,10,15,13,11),$$
$$(1,5,7,6,2,3,8)(9,10,14,12,11,13,16)\rangle$$

$|C| = 3136$ NTyp: 1 1 Gruppe

Operation Typ 36, $E(8):F_{21}$**:**

$$D = \langle(1,6,7,5,8,2)(3,4)(9,16,15)(10,13,14),$$
$$(1,2,4,7,6,8,3)(9,10,12,15,14,16,11)\rangle$$

$|D| = 1344$ NTyp: 1 1 Gruppe

$$E = \langle(1,5,3)(2,6,8)(9,16,12)(11,15,13),$$
$$(3,7,4)(5,8,6)(9,15,14,10,13,11)(12,16)\rangle$$

$|E| = 1344$ NTyp: 1 1 Gruppe

$$F = \langle(1,4,7)(2,3,8)(9,12,16,13,11,14)(10,15),$$
$$(1,3,4)(2,7,6)(9,15,12,11,16,13)(10,14),$$
$$(1,3)(2,6)(4,5)(7,8)(9,16,10,13,15,12,11)\rangle$$

$|F| = 9408$ NTyp: 1 1 Gruppe

$$G = \langle(1,2,3,4,5,6,7)(9,10,15,11,16,13,12),$$
$$(2,8,7)(3,5,4)(9,12,15,13,11,10)(14,16)\rangle$$

$|G| = 9408$ NTyp: 1 1 Gruppe

$$H = \langle(1,8)(2,6,3,4,5,7)(9,10,13)(11,12,16),$$
$$(1,6,3,8,2,4,5)(9,11,16)(12,14,13),$$
$$(1,2,7,3,8,5,4)(9,16)(10,15,13,12,11,14)\rangle$$

$|H| = 28224$ NTyp: 1 1 Gruppe

Operation Typ 37, $L(8) = PSL(2,7)$**:**

$$I = \langle (1,4,6,8,5,7,3)(9,12)(10,16)(11,15)(13,14),$$
$$(1,2,8,5,6,4,3)(9,14,15,13)(10,16,12,11)\rangle$$

$|I| = 28224$ NTyp: 1 1 Gruppe

Operation Typ 43, $L(8):2 = PGL(2,7)$**:**

$$J = \langle (1,4,5,8,6,7,3,2)(9,12)(10,11)(13,15),$$
$$(1,2,3)(4,7,8)(9,15,12,16,10,14,13)\rangle$$

$|J| = 56448$ NTyp: 1 2 Gruppen

$$K = \langle (1,6,3,7,5,4,8,2)(9,13,16,10,14,12,15,11),$$
$$(1,2,4)(3,6,5)(9,12,11,10,13,14,16,15)\rangle$$

$|K| = 112896$ NTyp: 1 1 Gruppe

Operation Typ 48, $E(8):L_7 = AL(8)$**:**

$$L = \langle (1,6)(2,7,3,4)(9,13,16,11)(10,15,12,14),$$
$$(1,4)(2,3,8,5)(9,12,10,13)(11,16,14,15)\rangle$$

$|L| = 1344$ NTyp: 1 1 Gruppe

$$M = \langle (1,8,4,2)(3,6,5,7)(9,11,13,12)(10,14,15,16),$$
$$(1,2,5,7)(3,4)(9,15,10,14)(11,12,13,16)\rangle$$

$|M| = 10752$ NTyp: 1 1 Gruppe

$$N = \langle (1,6,2,7,5,3,8)(9,16,13,12,11,14,15),$$
$$(1,4,3,8,5,6,2)(9,10,16,14,12,15,11)\rangle$$

$|N| = 10752$ NTyp: 1 1 Gruppe

$$O = \langle (1,3,6,8)(2,4,5,7)(9,13,14,11,12,10)(15,16),$$
$$(2,5,4)(3,8,7)(9,15)(10,16,14,13,11,12)\rangle$$

$|O| = 1806336$ NTyp: 1 1 Gruppe

Operation Typ 49, A_8**:**

$$P = \langle (1,8,5)(2,4,6,3,7)(9,12)(10,11,16)(14,15),$$
$$(1,8,7,5,6,3)(2,4)(9,15,14,10,13,12)(11,16)\rangle$$

$|P| = 406425600$ NTyp: 1 1 Gruppe

Operation Typ 50, S_8:

$$Q = \langle (1,6,8,4,7,5,3,2)(9,13,14,16,10,15,12,11),$$
$$(1,2,6,7,8,3)(9,12,16,14)(10,15)(11,13)\rangle$$

$|Q| = 812851200$ NTyp: 1 2 Gruppen

$$R = \langle (1,5,3,2,8)(6,7)(9,13,14)(10,12,16,11),$$
$$(1,5,2,4)(3,8,6,7)(9,15,12,11,16)(10,14)\rangle$$

$|R| = 1625702400$ NTyp: 1 1 Gruppe

Anzahlen:

	$\emptyset$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	0	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1

Primitiv: 22

Gesamt:1954

KAPITEL VII

Epilog: Ergänzungen nach Abgabe der Arbeit

Nach Abgabe der Arbeit im April 1996 wurde das in Kapitel VI skizzierte Programm zur Überprüfung und Vervollständigung der Listen begonnen. Bis zum Zeitpunkt der Drucklegung im August 1996 ergaben sich dabei die folgenden Ergänzungen und Korrekturen:

VII.0.4. In der Liste der transitiven Gruppen bis Grad 18 wurde ein Duplikatpaar entdeckt. Entgegen der ursprünglichen Angaben gibt es nur 983 Gruppen dieses Grades. Dieser Fehler konnte auf ein Problem bei der Implementation der Komplementberechnung zurückgeführt werden. Das korrigierte Programm liefert jetzt 983 Gruppen.

VII.0.5. Die Gruppen bis Grad 23 wurden nochmals ab initio neu konstruiert um eventuelle Auswirkungen von in der Zwischenzeit durchgeführten Korrekturen am benutzten Programmpaket GAP festzustellen. Mit Ausnahme der im vorangegangenen Abschnitt erwähnten Korrektur für Grad 18 ergaben sich keine Änderungen.

Die dabei gewonnenen Informationen lassen wiederum die Identifikation einer transitiven Gruppe vom gegebenen Grad mit dem Katalog zu.

VII.0.6. Die noch fehlenden Berechnungen für Grad 24 konnten fertiggestellt werden. Die Konstruktion der zu betrachtenden Subpotenzen von S_3 von Stufe 8 benötigte etwa 12 Tage auf einem 133Mhz Pentium PC. Die Ermittlung der daraus entstehenden transitiven Gruppen konnte dann in weniger als einem Tag durchgeführt werden. Dabei ergaben sich 2454 transitive Gruppen, deren zugehöriges Blocksystem von diesem Typ ist. Damit gibt es insgesamt 26813 transitive Gruppen von Grad 24.

Aufgrund dieser hohen Anzahl wird sich der Test auf Duplikate, beziehungsweise die Erstellung von Identifikationsinformation, als schwierig erweisen, da es nicht mehr möglich ist, sämtliche Daten zum gleichen Zeitpunkt im Speicher zu halten.

VII.0.7. Eine erneute Konstruktion der Gruppen der Grade 24-30 und ein Duplikattest für diese Gruppen ist bisher nicht durchgeführt worden. Dies soll vor einer endgültigen Publikation der Listen trotz der oben erwähnten Schwierigkeiten jedoch noch geschehen.

ANHANG A

Namen für transitive Permutationsgruppen

Im Verlaufe der Arbeit wurden mehrfach Gruppen mit Namen bezeichnet. Das hierbei zugrundelegende Schema dürfte noch nicht allgemein bekannt sein und einiger Erläuterungen bedürfen. Hierzu sei ein Abschnitt einer vorläufigen Version eines Artikels von J. Conway, J. McKay und dem Verfasser [CHM] angefügt, in dem dieses Schema beschrieben wird. (Die Arbeit umfasst darüberhinaus Listen der transitiven Gruppen bis Grad 15, denen Namen und „schöne“ Erzeuger gegeben werden. Diese Listen sollen hier aus Platzgründen entfallen.)

A.1. Taxonomy

In this section we present a scheme for assigning names to transitive permutation groups, based on their permutational structure. Whereas the goal of assigning an unique name to each individual transitive permutation group cannot be achieved for all degrees, the scheme presented is powerful enough for individual naming of all groups of degree up to 15. Conversely we do not attempt to give names so explicit that one can deduce a generating set for every group based solely on its name. It should be possible, however, to identify the group belonging to a name in a list of representatives of the transitive groups without having to determine the correspondence of the whole list to the catalogue printed here.

As we need to distinguish between *permutation isomorphism types* and *names* we denote names or parts of names used by enclosing them thus: $\langle\!\langle G \rangle\!\rangle$.

A.1.1. Modifications to ATLAS notation. As a basis we use the notation of the ATLAS [CCN$^+$1985] to which we refer also for the names and definitions of the simple groups. The name of a group reflects its subnormal structure written from left to right in ascending order. The subnormal series is chosen to be compatible with permutational structures, namely kernels of block operations.

Direct products are denoted by '$\times$', split extensions by ':' and nonsplit extensions by '$\cdot$'. A dot itself '.' is used only to separate a normal subgroup and its factor without giving further information about the extension structure.

To such a name, additional information is added in brackets to denote permutation specific information. A group name followed by a number n in round brackets '(n)' denotes that the group operates transitively on n points, respectively that a point stabilizer has index n in the group. Square brackets '$[,]$' denote normal structures corresponding to permutational concepts.

Curly brackets '$\{,\}$' give further information("hints") towards the construction. For example, several nonisomorphic transitive representations of one group might be distinguished by a hint towards the point stabilizer of the form $\langle\langle X(n\{stab\})\rangle\rangle$. We explain the hints given after a description of the basic names (A.1.5).

A.1.2. Natural names. Some families of groups containing one member for each degree are given natural names. A name of the form $\langle\langle X(n)\rangle\rangle$ denotes the n-th member of this family as a permutation group on n points. The same group is denoted by $\langle\langle X_n\rangle\rangle$ if it occurs as an abstract group but not necessarily with this action. Exceptions are dihedral and Frobenius groups for which traditionally the *size* is indicated by an index. Thus $\langle\langle D(4)\rangle\rangle = \langle\langle D_8(4)\rangle\rangle$ is the dihedral group of size 8. We sum up the names used in the following list:

A	Alternating	F	Frobenius	E	Elementary
S	Symmetric	AL	Affine linear	C	Cyclic
M	Mathieu	D	Dihedral		

In addition we use $\langle\langle L(n)\rangle\rangle$ to denote groups derived from linear groups as defined in table 1.

TABLE 1. The permutation groups $L(n)$

Name	Size	Type
$L(6)$	60	$PSL(2,5) = A_5(6)$
$L(7)$	168	$PSL(3,2)$
$L(8)$	168	$PSL(2,7)$
$L(9)$	504	$PSL(2,8)$
$L(10)$	360	$PSL(2,9)$
$L(11)$	660	$PSL(2,11)(11)$
$L(12)$	660	$PSL(2,11)$
$L(13)$	5616	$PSL(3,3)$
$L(14)$	1092	$PSL(2,13)$
$L(15)$	20160	$PSL(4,2) = A_8(15)$

A.1.3. Group products. If G acts transitively on Ω, and H on Δ, the direct product has a transitive representation on $\Omega \times \Delta$. This is denoted by $\langle\langle G[\times]H\rangle\rangle$.

A subdirect product (see [Rem1930]) corresponding to two epimorphisms $\alpha\colon G \twoheadrightarrow F$ and $\beta\colon H \twoheadrightarrow F$ with $|F| = m$ is denoted by $\langle\langle G[\frac{1}{m}]H\rangle\rangle$. If several subdirect products exist, further information is given in hints towards the epimorphisms: $\langle\langle G\{\alpha\}[\frac{1}{m}]\{\beta\}H\rangle\rangle$. If F is abelian, there is a special subdirect product of n copies of G, which is the "augmentation ideal" construction

$$\langle\langle \tfrac{1}{m}(G^n)\rangle\rangle = \{(g_1,\dots,g_n) \mid g_1^{\alpha_1}\cdot\dots\cdot g_n^{\alpha_n} = 1_F\}$$

Again a hint, $\langle\!\langle \frac{1}{m}\{\alpha\}G^n \rangle\!\rangle$, can be given to the defining homomorphism(s).

We need to describe intransitive actions of (iterated) (sub)direct products: as an intransitive permutation group $G \times H$ — and therefore all subdirect products of G with H — can be represented on the disjoint union $\Omega \uplus \Delta$.

We now take a group A acting on Ω and consider the direct product $A^m = A_1 \times \cdots \times A_m$ acting on $\Omega_1 \uplus \cdots \uplus \Omega_m$. If U is a subgroup of A then $\langle\!\langle U^m \rangle\!\rangle$ is the direct product, acting with each component U_i in the same way on Ω_i. For $k < m$ the group $\langle\!\langle U^k \rangle\!\rangle$ also acts on all orbits in the same way. If $u \in U^k$ acts as u_i on Ω_i (and thus $u = \prod u_i$), then $u_i = u_j^{\alpha_{i,j}}$ where $\alpha_{i,j}$ is a permutation isomorphism (depending only on U^k and not on u) mapping U_j to U_i. So, as an intransitive group, the augmentation ideal is denoted by $\langle\!\langle A^{m-1} \rangle\!\rangle$.

Analogous rules apply to groups of the form $\langle\!\langle U^j.V^k \rangle\!\rangle$ when $U.V$ is a subgroup of A.

A.1.4. Imprimitive constructions. By the embedding theorem [KK1951] imprimitive groups can be embedded into suitable wreath products. We will use these wreath products to describe imprimitive groups: let C be a transitive group of degree l and H a permutation group of degree m, then the wreath product $C \wr H = W$ is a semidirect product $C^m \rtimes H$ with H acting on C^m by permuting the m components according to the permutation action. We denote the complement to C^m in W by $\hat{H}$. It is an intransitive group, acting on l orbits with H acting simultaneously on the points. When embedding an imprimitive group into W, the kernel K of the action on the blocks embeds into C^m as an intransitive group acting on every orbit like a normal subgroup A of C.

For an intransitive subgroup, $\langle\!\langle K \rangle\!\rangle$ of C^m, as defined in the last section $\langle\!\langle [K]H \rangle\!\rangle$ is the split extension $\langle K, \hat{H} \rangle$; so the permutational wreath product $A \wr H$ is denoted by $\langle\!\langle [A^m]H \rangle\!\rangle$.

When there are epimorphisms $\beta\colon K \twoheadrightarrow F$ and $\gamma\colon H \twoheadrightarrow F$ and $|F| = m$, then $\langle\!\langle \frac{1}{m}[K]H \rangle\!\rangle$ is the subgroup of $[K]H$ consisting of those elements kh for which $k^\beta = h^\gamma$. Again hints can be placed before the groups to give information about β and γ, leading to names of the form $\langle\!\langle \frac{1}{m}\{\beta\}[K]\{\gamma\}H \rangle\!\rangle$.

Other groups with the same action H on the blocks may differ in the part of H for which a complement in $\hat{H}$ exists. This complementable part is called the "bodily part" of H. A group of this type will be called $\langle\!\langle [K]H\{bodily\} \rangle\!\rangle$.

Similarly the kernel of the block operation may partially intersect with the K given in the name (the reason being that the proper kernel is not readily described). This leads to the indication of a bodily part of K and names of the form $\langle\!\langle [K\{bodily\}]H\{bodily\} \rangle\!\rangle$.

When the index of the bodily part suffices to distinguish groups, it is given as an index to the group names, for example $\langle\!\langle [K_i]H_j \rangle\!\rangle$. Instead of writing a number, a division sign '$\div$' can be used as an index to denote "fractional part" if this suffices to distinguish the groups. The bodily part of H is maximized if several possible embeddings exist.

The groups 17-20 of degree 10 may serve as examples: we take subdirect products of the Frobenius group $F(5)$ of order 20 and degree 5 with itself in which we "glue" together the factor groups of order 4. We arrange the points 0-9 in the following scheme

$$\begin{matrix} 0 & 2 & 4 & 6 & 8 \\ 5 & 7 & 9 & 1 & 3 \end{matrix}$$

with both factors of the subdirect product acting on one row to get orbits (which will become block systems of a transitive group later) via congruences. According to this scheme, the standard subdirect product is

$$5^2 : 4 = \langle (0,2,4,6,8), (5,7,9,1,3), (2,4,8,6)(7,9,3,1) \rangle.$$

If we apply the outer automorphism of the factor group, we get another subdirect product. Its intersection with $5^2 : 4$ has size 50. In other words: the bodily part has index 2. Thus the group is

$$5^2 : 4_2 = \langle (0,2,4,6,8), (5,7,9,1,3), (2,4,8,6)(7,1,3,9) \rangle.$$

We extend these two intransitive groups by a factor group of order 2 so that the extension becomes transitive. The standard element of order 2, permuting the blocks, is the complement of the wreath product:

$$a = (0,5)(2,7)(4,9)(6,1)(8,3).$$

Extending both subdirect products by this element gives the groups $[5^2 : 4]2$ and $[5^2 : 4_2]2$.

For both subdirect products we take an element x of the direct product not in the subdirect product such that $(xa)^2$ is contained in the subdirect product. Then extending the subdirect products by xa, we get a group that is transitive while its order has doubled, therefore, the subdirect product is the base group of this new group. The factor group 2 is not bodily as otherwise x would be in the base group. Taking $x = (2,8)(4,6)(7,9,3,1)$ we get the third group $[5^2 : 4]2_2$, for the other subdirect product $x = (7,3)(1,9)$ yields the fourth group $[5^2 : 4_2]2_2$. (Instead of writing $[5^2 : 4_2]2_2$ we could have written $[5^2 : 4_2]2_{\div}$ instead, but there is no advantage in doing so).

A.1.5. Hints. Hints are given only if they are necessary to distinguish different groups arising from the same general construction. A hint usually relates to the kernel of an homomorphism, the point stabilizer, or a bodily part. If the index of this subgroup suffices, it is given as an index. If there are two epimorphisms, one which is associated with the identity mapping of the image and one associated with a unique non-identity automorphism of the image, they are distinguished by indices '$+$' and '$-$'. (An omitted index always reading as '$+$'.)

We use single (non-capital) letter abbreviations for other frequent hints referring to subgroups. When standing alone these are written without surrounding hint brackets.

c	central or cyclic	d	odd or dihedral
e	even or elementary		
i	intransitive	t	transitive

The first three letters are reminiscent of the proper normal subgroups of the dihedral group, $D_8(4)$, of order 8, that can be denoted by $4c = \langle(1,2,3,4)\rangle$, $4d = \langle(1,3),(2,4)\rangle$, $4e = \langle(1,2)(3,4),(1,3)(2,4)\rangle$ and $2c = \langle(1,3)(2,4)\rangle$.

A hint of the form $\{n\langle ind\rangle\}$ after the group name indicates that the group has index $\langle ind\rangle$ in its normalizer in the full symmetric group.

Literaturverzeichnis

[Aca1858] *Grand prix de mathématiques*, C. R. Acad. Sci. Paris, 1858, 302–303.

[AR1993] Ahmad Al-Rhayyel, *On transitive subgroups of S_{18}*, J. Inform. Optim. Sci. **15** (1993), no. 3, 289–308.

[Ask1890a] E. H. Askwith, *On possible groups of substitutions that can be formed with eight letters*, Quart. J. Pure Appl. Math. **24** (1890), 263–331, Errata: [Ask1893], Corrigendum in [Höl1892].

[Ask1890b] E. H. Askwith, *On possible groups of substitutions that can be formed with three, four, five, six and seven letters respectively*, Quart. J. Pure Appl. Math. **24** (1890), 111–167, Errata: [Ask1890a].

[Ask1893] E. H. Askwith, *On groups of substitutions that can be formed with nine letters*, Quart. J. Pure Appl. Math. **26** (1893), 79–128.

[Atk1984] Michael D. Atkinson (ed.), *Computational group theory*, Academic press, 1984.

[Ben1912] Elizabeth R. Bennett, *Primitive groups with a determination of the primitive groups of degree 20*, Amer. J. Math. **34** (1912), 1–20.

[Bir1994] Bryan Birch, *Noncongruence subgroups, covers and drawings*, The Grothendieck Theory of Dessins d'Enfants (Leila Schneps, ed.), London Mathematical Society Lecture Note Series, no. 200, Cambridge University Press, 1994, pp. 25–46.

[BM1983] Gregory Butler and John McKay, *The transitive groups of degree up to 11*, Comm. Algebra **11** (1983), 863–911.

[Bor1889] Alfred Borchert, *Über die Zahl der verschiedenen Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. **33** (1889), 584–590.

[BS1992] Robert Beals and Ákos Seress, *Structure forest and composition factors for small base groups in nearly linear time*, Proceedings of the 24^{th} ACM Symposium on Theory of Computing, ACM Press, 1992, pp. 116–125.

[Bur1897] W[illiam] Burnside, *Theory of groups of finite order*, 1st ed., Cambridge University Press, 1897.

[Bur1898] Heinrich Burckhardt, *Endliche discrete Gruppen*, Encyclopädie der mathematischen Wissenschaften (W. F. Meyer, ed.), Band I, erster Teil, B. G. Teubner, Leipzig, 1898, pp. 208–226.

[Bur1911] W[illiam] Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge University Press, 1911, Nachdruck Dover, New York, 1955.

[But1991] G[regory] Butler, *Fundamental algorithms for permutation groups*, Lecture Notes in Computer Science, Band 559, Springer, Heidelberg, 1991.

[But1993] Greg[ory] Butler, *The transitive groups of degree fourteen and fifteen*, J. Symb. Comput. **16** (1993), 413–422.

[BV1909] H[einrich] Burckhardt and H. Vogt, *Sur les groupes finis discontinus*, Encyclopédie des sciences mathématiques pures et appliquées (Jules Molk, ed.), Band Tome I, Vol. 1, Fasc. 4, Gauthier–Villars (Édition Française), 1909, pp. 546–565.

[Cam1981] Peter J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[Cau1845] Augustin L. Cauchy, *Recherche du nombre des valeurs que peut aquérire une fonction transitive ou intransitive qui ne renferme pas plus de six variables*, C. R. Acad. Sci. Paris **21** (1845), 1363–1369,1401–1409, ibid., **22**(1846),2–31.

[Cay1891] Arthur Cayley, *On the substitution groups for two, three, four, five, six, seven, and eight letters*, Quart. J. Pure Appl. Math. **25** (1891), 71–88,137–155.

[CCN+1985] J[ohn] H. Conway, R[obert] T. Curtis, S[imon] P. Norton, R[ichard] A. Parker, and R[obert] A. Wilson, ATLAS *of finite groups*, Oxford University Press, 1985.

[CFL1989] Gene Cooperman, Larry Finkelstein, and Eugene M. Luks, *Reduction of group constructions to point stabilizers*, Proceedings 1989 ACM-SIGSAM, 1989, pp. 351–356.

[CHM] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, in preparation ().

[CNW1990] Frank Celler, Joachim Neubüser, and Charles R. B. Wright, *Some remarks on the computation of complements and normalizers in soluble groups*, Acta Appl. Math. **21** (1990), 57–76.

[Coh1993] Henri Cohen, *A course in computational algebraic number theory*, Springer, Heidelberg, 1993.

[Col1893a] Frank N. Cole, *List of the substitution groups of nine letters*, Quart. J. Pure Appl. Math. **26** (1893), 372–388.

[Col1893b] Frank N. Cole, *Note on the substitution groups of six, seven, and eight letters*, Bull. New-York Math. Soc. **2** (1893), 184–190.

[Col1893c] Frank N. Cole, *The transitive substitution-groups of nine letters*, Bull. New-York Math. Soc. **2** (1893), 250–258.

[Col1895] Frank N. Cole, *List of the transitive substitution groups of ten and eleven letters*, Quart. J. Pure Appl. Math. **27** (1895), 39–50, Corrigendum in [Mil1895b].

[Coo1996] Gene Cooperman, *GAP/MPI: Faciliating Parallelism*, College of Computer Science, Northeastern University, Boston, MA 02115, 1996.

[CP1993] J[ohn] Cannon and C[atherine] Playoust, *An Introduction to MAGMA*, School of Mathematics and Statistics, University of Sydney, 1993.

[Dav1996] J[ames] H. Davenport, *Galois groups and the simplification of polynomials*, `http://www.bath.ac.uk/~masjhd/Galois.dvi`, 1996.

[DM1988] John D. Dixon and Brian Mortimer, *The primitive permutation groups of degree less than 1000*, Math. Proc. Cambridge Philos. Soc. **103** (1988), 213–238.

[Eic1993] Bettina Eick, *PAG-Systeme im Computeralgebrasystem GAP*, Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1993.

[EP1988] David Easdown and Cheryl E. Praeger, *On minimal faithful permutation representations of finite groups*, Bull. Austral. Math. Soc. **38** (1988), 207–220.

[FN1970] Volkmar Felsch and Joachim Neubüser, *On a programme for the determination of the automorphism group of a finite group*, In Leech [Lee1970], pp. 59–60.

[Gey1993] Helmut Geyer, *Programme zur Berechnung der Galoisgruppen von Polynomen 8. und 9. Grades*, Preprint 93-10, IWR Heidelberg, 1993.

[Gor1982] Daniel Gorenstein, *Finite simple groups*, Plenum Press, 1982.

[Gou1889] É. Goursat, *Sur les substitutions orthogonales et les diviseurs régulières de l'espace*, Ann. Sci. École Norm. Sup. (3) **6** (1889), 9–102.

[GS1990] Stephan P. Glasby and Michael C. Slattery, *Computing intersections and normalizers in soluble groups*, J. Symb. Comput. **9** (1990), 637–651.

[Hal1959] Marshall Hall, Jr, *The theory of groups*, Macmillan, 1959.

[Hil1893] David Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370.

[Höl1892] Otto Hölder, *Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen*, Math. Ann. **40** (1892), 55–88.

[Hol1984] D[erek] F. Holt, *The calculation of the Schur multiplier of a permutation group*, In Atkinson [Atk1984], pp. 307–319.

[HR1992] Derek F. Holt and Sarah Rees, *Testing for isomorphism between finitely presented groups*, Groups, Combinatorics and Geometry (Martin W. Liebeck and Jan Saxl, eds.), LMS Lecture Notes Series, Band 165, Cambridge University Press, 1992, pp. 459–475.

[Hul] Alexander Hulpke, *Galois groups over the rationals*, in preparation ().

[Hul1993] Alexander Hulpke, *Zur Berechnung von Charaktertafeln*, Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1993.

[Hup1967] B[ertram] Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften, Band 134, Springer, Heidelberg, 1967.

[HY1979] Koichiro Harada and Hiroyoshi Yamaki, *The irreducible subgroups of* $\mathrm{GL}_n(2)$ *with* $n \leq 6$, C. R. Math. Rep. Acad. Sci. Canada **1** (1979), 75–78.

[IT1986] V. I. Il'in and A. S. Takamakov, *Primitive simple permutation groups of small degrees*, Algebra and Logic **25** (1986), 167–171.

[Jor1870] Camille Jordan, *Traité des substitutions et des équations algébriques*, Gauthier–Villars, 1870.

[Jor1871a] Camille Jordan, *Sur la classification des groupes primitifs*, C. R. Acad. Sci. Paris **73** (1871), 853–857.

[Jor1871b] Camille Jordan, *Sur la résolution des équations les unes par les autres*, C. R. Acad. Sci. Paris **72** (1871), 283–290.

[Jor1872] Camille Jordan, *Sur l'énumeration des groupes primitifs pour les dix-sept premiers degrés*, C. R. Acad. Sci. Paris **75** (1872), 1754–1757.

[Jor1874] Camille Jordan, *Sur deux points de la théorie des substitutions*, C. R. Acad. Sci. Paris **79** (1874), 1149–1151.

[Kir1862] T. P. Kirkman, *The complete theory of groups, being the solution of the mathematical prize question of the French academy for 1860*, Proc. Manchester Lit. Phil. Soc. **3** (1862), 133–152, 161–162, Errata: ibid., **4**(1865),171–172.

[KK1951] Marc Krasner and Leo [A.] Kaloujnine, *Produit complet des groupes de permutations et problème d'extension de groupes II*, Acta Sci. Math. (Szeged) **14** (1951), 39–66.

[KL1990] William M. Kantor and Eugene M. Luks, *Computing in quotient groups*, Proceedings of the 22$^{\text{nd}}$ ACM Symposium on Theory of Computing, Baltimore, ACM Press, 1990, pp. 524–563.

[Kuh1904] Harry W. Kuhn, *On imprimitive substitution groups*, Amer. J. Math. **26** (1904), 45–102.

[Lau1982] Reinhard Laue, *Computing double coset representatives for the generation of solvable groups*, EUROCAM '82 (Jacques Calmet, ed.), Lecture Notes in Computer Science, Band 144, Springer, Heidelberg, 1982.

[Lee1970] John Leech (ed.), *Computational problems in abstract algebra*, Pergamon press, 1970.

[Leo1991] Jeffrey S. Leon, *Permutation group algorithms based on partitions, I: theory and algorithms*, J. Symb. Comput. **12** (1991), 533–583.

[LGPS1991] Charles R. Leedham-Green, Cheryl E. Praeger, and Leonard H. Soicher, *Computing with group homomorphisms*, J. Symb. Comput. **12** (1991), 527–532.

[LMR1994] Klaus Lux, Jürgen Müller, and Michael Ringe, *Peakword Condensation and Submodule Lattices: An Application of the Meat-Axe*, J. Symb. Comput. **17** (1994), 529–544.

[LNS1984] Reinhard Laue, Joachim Neubüser, and Ulrich Schoenwaelder, *Algorithms for finite soluble groups and the SOGOS system*, In Atkinson [Atk1984], pp. 105–135.

[LPS1987] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), 365–383.

[LPS1988] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A **44** (1988), 389–396.

[Luk1987] Eugene M. Luks, *Computing the composition factors of a permutation group in polynomial time*, Combinatorica **7** (1987), 87–89.

[Mar1901] Emilie N. Martin, *On the imprimitive substitution groups of degree fifteen and the primitive substitution groups of degree eighteen*, Amer. J. Math. **23** (1901), 259–286.

[Mat1858] Émile Mathieu, *Sur le nombre des valeurs que peut aquérire une fonction de n lettres, quand on y permute ses lettres de toutes manières possibles*, C. R. Acad. Sci. Paris **46** (1858), 1047–1050,1208–1209.

[Mat1861] Émile Mathieu, *Sur létude des fonctions de plusieurs qualités*, J. Math. Pures Appl.(2) **6** (1861), 241–323.

[Mat1873] Émile Mathieu, *Sur la fonction cinq fois transitive de 24 quantités*, J. Math. Pures Appl.(2) **18** (1873), 25–46, cf. [Mat1861].

[Mat1987] B[ernd] Heinrich Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Mathematics, Band 1284, Springer, Heidelberg, 1987.

[Mat1992] Thomas W. Mattman, *The computation of Galois groups over function fields*, Master's thesis, McGill University, 1992.

[Mil1894a] George A. Miller, *Note on substitution groups of eight and nine letters*, Bull. New-York Math. Soc. **3** (1894), 242–245.

[Mil1894b] George A. Miller, *Note on substitution groups of eight letters*, Bull. New-York Math. Soc. **3** (1894), 168–169, Errata: [Mil1894a].

[Mil1895a] George A. Miller, *Note on the transitive substitution groups of degree twelve*, Bull. Amer. Math. Soc. **1** (1894/1895), no. 2, 255–258.

[Mil1895b] George A. Miller, *On the non-primitive substitution groups of degree ten*, Bull. Amer. Math. Soc. **1** (1894/1895), 67–72.

[Mil1895c] George A. Miller, *Intransitive substitution groups of ten letters*, Quart. J. Pure Appl. Math. **27** (1895), 99–118.

[Mil1896a] George A. Miller, *On the lists of all substitution groups that can be formed with a given number of elements*, Bull. Amer. Math. Soc. **2** (1895/1896), no. 2, 138–145.

[Mil1896b] George A. Miller, *List of transitive substitution groups of degree twelve*, Quart. J. Pure Appl. Math. **28** (1896), 193–231, Errata: ibid., **29**(1898),249.

[Mil1897a] George A. Miller, *On the primitive substitution groups of degree fifteen*, Proc. London Math. Soc **28** (1897), 533–544.

[Mil1897b] George A. Miller, *Sur l'énumération des groupes primitifs dont le degré est inférieur à 17*, C. R. Acad. Sci. Paris **124** (1897), 1505–1508.

[Mil1898a] George A. Miller, *On the primitive substitution groups of degree sixteen*, Amer. J. Math. **20** (1898), 229–241.

[Mil1898b] George A. Miller, *On the transitive substitution groups of degree thirteen and fourteen*, Quart. J. Pure Appl. Math. **29** (1898), 224–249.

[Mil1899] George A. Miller, *Note on Burnside's Theory of Groups*, Bull. Amer. Math. Soc. **5** (1898/1899), no. 2, 249–251.

[Mil1900a] George A. Miller, *On the primitive substitution groups of degree ten*, Quart. J. Pure Appl. Math. **31** (1900), 228–233.

[Mil1900b] George A. Miller, *On the transitive substitution groups of degree seventeen*, Quart. J. Pure Appl. Math. **31** (1900), 49–57.

[Mil1935] George A. Miller, *Historical note on the determination of all the permutation groups of low degrees*, The Collected Works of George Abram Miller, Band 1, University of Illinois Press, 1935, pp. 1–9.

[ML1901] George A. Miller and G. H. Ling, *List of the intransitive substitution groups of degree eleven*, Quart. J. Pure Appl. Math. **32** (1901), 342–368.

[MN1989] M[atthias] Mecky and J[oachim] Neubüser, *Some remarks on the computation of conjugacy classes of soluble groups*, Bull. Austral. Math. Soc. **40** (1989), no. 2, 281–292.

[Mni1992] Jürgen Mnich, *Untergruppenverbände und auflösbare Gruppen in GAP*, Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1992.

[Neu1960] Joachim Neubüser, *Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine*, Numer. Math. **2** (1960), 280–292.

[Neu1964] Peter M. Neumann, *On the structure of standard wreath products of groups*, Math. Z. **84** (1964), 343–373.

[Neu1967] Joachim Neubüser, *Die Untergruppenverbände der endlichen Gruppen von Ordnung* ≤ 100 *mit Ausnahme der Ordnungen 64 und 96*, Habilitationsschrift, Kiel, 1967.

[Neu1982] J[oachim] Neubüser, *An elementary introduction to coset table methods in computational group theory*, Groups – St. Andrews 1981, Proceedings Conference St. Andrews, 1981 (Colin M. Campbell and Edmund F. Robertson, eds.), LMS Lecture Notes Series, Band 71, Cambridge University Press, 1982, pp. 1–45.

[Neu1986] Peter M. Neumann, *Some algorithms for computing with finite permutation groups*, Groups – St Andrews 1985 (Edmund F. Robertson and Colin M. Campbell, eds.), Cambridge University Press, 1986, pp. 59–92.

[New1977] M[ichael] F. Newman, *Determination of groups of prime-power order*, Group theory, Proc. Miniconf., Austral. Nat. Univ., Canberra, 1975 (R. A. Bryce, J. Cossey, and M[ichael] F. Newman, eds.), Lecture Notes in Mathematics, Band 573, Springer, Heidelberg, 1977, pp. 73–84.

[O'B1990] E[amonn] A. O'Brien, *The p-group generation algorithm*, J. Symb. Comput. **9** (1990), 677–698.

[O'B1991] E[amonn] A. O'Brien, *The groups of order* 256, J. Algebra **143** (1991), 219–235.

[O'B1994] E[amonn] A. O'Brien, *Isomorphism testing for p-groups*, J. Symb. Comput. **17** (1994), 133–147.

[O'B1995] E[amonn] A. O'Brien, *Computing automorphism groups of p-groups*, Proceedings of CANT '92 (Wieb Bosma and Alf J. van der Poorten, eds.), Kluwer, 1995, pp. 83–90.

[Oli1993] Michel Olivier, *Groupe de Galois des polynômes de degre 7,8 et 9*, preprint, Université Bordeaux I, CeReMaB, 1993.

[Par1984] Richard Parker, *The Computer Calculation of Modular Characters (the* MeatAxe*)*, In Atkinson [Atk1984], pp. 267–274.

[Pfe1996] Götz Pfeiffer, *The subgroups of M_{24} or how to compute the table of marks of a finite group*, in Vorbereitung, 1996.

[Pog1980] B. A. Pogorelov, *Primitive permutation groups of low degree*, Algebra and Logic **19** (1980), 230–254, 278–296.

[Pog1982] B. A. Pogorelov, *Primitive permutation groups of degree $n \in \overline{\{51, 64\}}$*, Eighth All-Union Symposium on Group Theory, Abstracts of Reports, Institute of Mathematics, Academy of Sciences of the UkrSSR, Kiev, 1982, p. 98.

[Rem1930] Robert Remak, *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte*, J. Reine Angew. Math. **163** (1930), 1–44.

[Rón1990] Lajos Rónyai, *Computing the structure of finite algebras*, J. Symb. Comput. (1990), 355–373.

[Roy1987] Gordon F. Royle, *The transitive groups of degree twelve*, J. Symb. Comput. **4** (1987), 255–268.

[RP1989] Gordon F. Royle and Cheryl E. Praeger, *Constructing the vertex-transitive graphs of order 24*, J. Symb. Comput. **8** (1989), 309–326.

[Ruf1799] P. Ruffini, *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto*, Bologna, 1799, 2 Bände.

[S+1995] Martin Schönert et al., *GAP 3.4, patchlevel 3*, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1995.

[Sco1980] Leonard L. Scott, *Representations in characteristic p*, The Santa Cruz conference on finite groups, Proc. Sympos. Pure Math., Band 37, American Mathematical Society, Providence, RI, 1980, Corrigendum in [LPS1988], pp. 318–331.

[Ser1850] J.-A. Serret, *Mémoire sur les fonctions de quatre, cinc et six lettres*, J. Math. Pures Appl. **15** (1850), no. 1, 45–70.

[Sho1928] Kenjiro Shoda, *Über die Automorphismen einer endlichen Abelschen Gruppe*, Math. Ann. **100** (1928), 674–686.

[Sho1992] Mark W. Short, *The primitive soluble permutation groups of degree less than 256*, Lecture Notes in Mathematics, Band 1519, Springer, Heidelberg, 1992.

[Sim1970] Charles C. Sims, *Computational methods in the study of permutation groups*, In Leech [Lee1970], pp. 169–183.

[Sim1971a] Charles C. Sims, *Computation with permutation groups*, Second Symposium on Symbolic and Algebraic Manipulation, Los Angeles 1971 (S. R. Petrick, ed.), ACM Press, 1971, pp. 23–28.

[Sim1971b] Charles C. Sims, *Determining the conjugacy classes of a permutation group*, Computers in Algebra and Number theory (Garrett Birkhoff and Marshall Hall, Jr, eds.), American Mathematical Society, Providence, RI, 1971, pp. 191–195.

[Sim1990] Charles C. Sims, *Computing the order of a solvable permutation group*, J. Symb. Comput. **9** (1990), 699–705.

[Sla] Michael C. Slattery, personal communication.

[Sla1992] Michael C. Slattery, *Double cosets and transversals in finite soluble groups*, Computational Group Theory. Bericht der Tagung vom 7. bis 13. Juni in Oberwolfach, 1992.

[SM1985] Leonard [H.] Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

[Smi1994] Michael J. Smith, *Computing automorphisms of finite soluble groups*, Ph.D. thesis, Australian National University, Canberra, 1994.

[SS1994] Martin Schönert and Ákos Seress, *Finding blocks of imprimitivity in small base groups in nearly linear time*, Proc. ISSAC '94, ACM Press, 1994.

[Sta1973] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[Stu1993] Bernd Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, Band 1, Springer, Wien, 1993.

[SvdW1928] O. Schreier and B. L. van der Waerden, *Die Automorphismen der projektiven Gruppen*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 303–322.

[The1996] Heiko Theißen, *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen (Arbeitstitel)*, Dissertation, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, in Vorbereitung 1996.

[TW1988] Tang Shou Wen and Wang Jie, *The primitive permutation groups of degrees 21 to 30 (Titel aus dem Chinesischen übersetzt)*, Beijing Daxue Xuebao **24** (1988), 269–276.

[Val1995] Annick Valibouze, *Computation of the galois groups of the resolvent factors for the direct and inverse galois problems*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Gèrard Cohen, Marc Giustini, and Teo Mora, eds.), Lecture Notes in Computer Science, Band 948, Springer, Heidelberg, 1995, pp. 456–468.

[vdW1971] B. L. van der Waerden, *Algebra*, Springer, Heidelberg, 1971.

[Ver1883] G. Veronese, *Interprétations géométriques de la théorie des substitutions de n lettres particulièrement pour $n = 3, 4, 5, 6$ en relation avec les groupes de l'hexagramme mystique*, Ann. Mat. Pura Appl. **11** (1883), no. 2, 92–236.

[Wie1960] Helmut Wielandt, *Über den Transitivitätsgrad von Permutationsgruppen*, Math. Z. **74** (1960), 297–298.

[Wur1993] Martin Wursthorn, SISYPHOS*, computing in modular group algebras, version 0.5*, Math. Inst. B, 3. Lehrstuhl, Universität Stuttgart, 1993.

Index