universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Gruppen und ihre Wirkungen

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag.rer.nat.)

Verfasserin:	Maria Kranzl
Matrikel-Nummer:	8901529
Studienrichtung (lt. Studienblatt):	UF Mathematik und UF Informatik und Informatikmanagement
Betreuer:	Ao. Univ.-Prof. Dr. Karl Auinger

Wien, im Jänner 2011

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Ziel der Arbeit

Gegenstand dieser Arbeit sind Gruppen, ihre Wirkungen und deren Anwendungen. Das Hauptanliegen ist es, einen Einblick in den fundamentalen und allgemein verbreiteten Charakter der Gruppenwirkungen zu geben; mithilfe von deren Anwendungen sollen darüber hinaus wichtige gruppentheoretische Ergebnisse bewiesen werden. Der Begriff der Gruppenwirkung ist in vielen Bereichen der Wissenschaft vertreten. Mit Wirkungen einer Gruppe auf eine Menge kann man nicht nur Symmetrien beschreiben, sie bilden das Grundkonzept dynamischer Systeme und können als iterativ angewendete Algorithmen verstanden werden.

Allen voran wird das Konzept der Gruppenwirkungen dargestellt mit den beiden zentralen Begriffen *Bahn* und *Stabilisator*. Es soll gezeigt werden, dass die Bahnen einer Gruppenwirkung auf einer Menge eine Partition dieser Menge bilden. Weiters kann jede Bahn bijektiv auf der Menge aller Linksnebenklassen der Gruppe nach dem Stabilisator eines (beliebigen) Elements der Bahn abgebildet werden. Ein Schwerpunkt liegt auf dem sich daraus ergebenden folgenreichen Zusammenhang zwischen Bahn und Stabilisator, aus dem dann die Klassengleichung abgeleitet wird.

Neben der Erläuterung von Gruppenwirkungen ist das zweite Ziel dieser Arbeit, zentrale gruppentheoretische Sätze mit Methoden der Gruppenwirkungen zu beweisen. Eine der Fragestellungen behandelt die Existenz von Untergruppen einer endlichen Gruppe mit vorgegebenen Teilern der Ordnung der Gruppe, eine andere die Zerlegbarkeit einer Gruppe in "einfachere" Bausteine. Die erste Frage hat allgemein eine negative Antwort: es gibt nicht zu jedem Teiler einer Gruppe auch eine Untergruppe mit dieser Ordnung. Zum Beispiel hat die alternierende Gruppe A_4 mit Ordnung 12 keine Untergruppe der Ordnung 6. Ein Ziel dieser Arbeit ist es, hinreichende Bedingungen anzu-

geben, unter welchen die Umkehrung des Satzes von Lagrange gilt. Es wird sich zeigen, dass Gruppen, deren Ordnung eine Primzahlpotenz ist, für jeden Teiler eine Untergruppe mit dieser Ordnung besitzen. Weiters gibt es zu jeder endlichen Gruppe und jeder Primzahlpotenz, die die Ordnung der Gruppe teilt, eine Untergruppe mit dieser Ordnung. Der Satz von Cauchy und die klassischen Sylow-Sätze liefern hier Antworten und sind damit ein grundlegender Beitrag für das Verständnis endlicher Gruppen. Die Sylow-Sätze liefern weiters ein Werkzeug, um sogenannte p-Sylow-Untergruppen und deren Anzahl zu bestimmen. Die Beweise dieser Sätze werden mit speziellen Gruppenwirkungen geführt. Gruppen, die nur sich und die triviale Untergruppe als Normalteiler haben, nennt man einfach. In der Entwicklung der Gruppentheorie hat es viele Jahre gedauert, um alle endlichen einfachen Gruppen zu finden. Sie bilden sozusagen die Bausteine der endlichen Gruppen und sind daher von fundamentaler Bedeutung. Ein weiteres Hauptziel dieser Arbeit ist es, die Einfachheit der alternierenden Gruppe A_n für $n \geq 5$ zu zeigen.

Eine weitere Methode in der Strukturtheorie von Gruppen ist die "Zerlegung" von Gruppen in weniger komplexe Gruppen beziehungsweise die Konstruktion neuer Gruppen aus bestehenden. Eine wichtige Konstruktionsmethode hiefür ist das semidirekte Produkt. Dieses wird im Rahmen der Arbeit ebenfalls erläutert und sein Zusammenhang mit Gruppenwirkungen dargestellt. Es beruht auf der Wirkung einer Gruppe auf einer anderen durch Automorphismen. Die Betrachtung der nicht abelschen Diedergruppe als semidirektes Produkt von zwei zyklischen Gruppen liefert ein instruktives Beispiel.

Es sei schließlich noch auf die Permutationsgruppe S_n hingewiesen, die in dieser Arbeit immer wieder für Beispiele herangezogen wird. Sie spielt eine fundamentale Rolle in der Theorie der endlichen Gruppen, da sie zur Beschreibung von abstrakt gegebenen Gruppen dient. Eine Permutationsgruppe

ist eine Gruppe, die treu auf einer endlichen Menge wirkt, also im wesentlichen eine Untergruppe der S_n für ein geeignetes n. Nach dem Satz von Cayley ist jede endliche Gruppe isomorph zu einer Untergruppe einer Permutationsgruppe. Damit kann jede Gruppe als Permutationsgruppe aufgefaßt werden, wodurch die Möglichkeit gegeben wird, Sätze der abstrakten Gruppentheorie mittels Methoden aus der Theorie der Permutationsgruppen zu beweisen. Von besonderer Bedeutung ist eine spezielle Untergruppe der Permutationsgruppe S_n - die Gruppe der geraden Permutationen, genannt die alternierende Gruppe A_n. Wie bereits erwähnt soll die Einfachheit von A_n für $n \geq 5$ bewiesen werden. Darüber hinaus soll der Beweis erbracht werden, dass A_4 keine Untergruppe der Ordnung 6 haben kann.

Die im Rahmen dieser Arbeit erzielten Resultate werden mit dem Computer Algebra System GAP (vgl. [4]) anhand von praktischen Beispielen validiert. Der Schwerpunkt des Programms liegt auf der Gruppentheorie. Eine ausführliche Beschreibung ist der Online-Hilfe oder Rosebrock (vgl. [9]) zu entnehmen. Der für die Beispiele entwickelte Code ist im Anhang dargestellt.

1.2 Aufbau der Arbeit

Zu Beginn der Arbeit wird im Abschnitt 2.1 erklärt, was man unter der Wirkung einer Gruppe auf eine Menge versteht. Ich führe zwei Definitionen von Gruppenwirkungen ein und zeige, dass diese äquivalent sind. Anschließend stelle ich die Begriffe *Bahn* und *Stabilisator* einer Gruppenwirkung vor und erläutere deren Eigenschaften sowie den fundamentalen Bahn-Stabilisator-Satz. Zur Illustration gebe ich klassische Beispiele wie die Wirkungen einer Gruppe auf sich oder auf ihrer Potenzmenge via Konjugation und Linksmultiplikation oder auf der Menge der Nebenklassen nach einer Untergruppe via Linksmultiplikation.

Aus der Partition der Menge X in die Bahnen unter der Wirkung der Gruppe G und der Gleichung $|O_x| \cdot |G_x| = |G|$ des Bahn-Stabilisator-Satzes wird in Abschnitt 2.2 die verallgemeinerte Klassengleichung $|X| = |X_0| + \sum_{i=1}^{l} |P_i|$ abgeleitet, die dann insbesondere für die Konjugationswirkung die Form der speziellen ("klassischen") Klassengleichung

$$|G| = |Z(G)| + \sum_{i=1}^{l} [G : C_G(x_i)]$$

annimmt, wobei $Z(G)$ das Zentrum von G und $C_G(x)$ den Zentralisator von x in G bezeichnet.

In Abschnitt 2.3 werde ich das Konzept der Gruppenwirkungen im Beweis des Satzes von Cauchy sowie in weiteren Sätzen zu Eigenschaften von p-Gruppen anwenden. Der zweite Teil dieses Abschnittes befasst sich mit dem Thema "Zerlegung" von Gruppen in einfachere Gruppe und der Konstruktion neuer und meist komplexerer Gruppen aus gegebenen. Diese Methode ist für die Analyse der Struktur endlicher Gruppen und damit für deren Klassifizierung fundamental. Sie ist wie folgt definiert: es wirke die Gruppe G auf der Gruppe H durch Automorphismen; dann definiert die Verknüpfung

$(h, g)(k, f) = (h^g k, gf)$ auf dem kartesischen Produkt $H \times G$ eine Gruppe, das sogenannte semidirekte Produkt von H mit G bezüglich der Wirkung von G auf H. Jede Gruppenwirkung durch Automorphismen definiert also ein semidirektes Produkt und umgekehrt. Die nicht kommutative Diedergruppe D_n wird beispielsweise mit dem semidirekten Produkt in zwei kommutative Gruppen "zerlegt": $D_n \cong C_n \rtimes C_2$. Schließlich erläutere ich noch, inwiefern ein semidirektes Produkt ein Spezialfall des algemeineren Konzepts einer *Erweiterung* ist, und zeige, dass eine Gruppe genau dann in ein semidirektes Produkt "zerlegt" werden kann, wenn es sich um eine zerfallende Erweiterung handelt.

Im Abschnitt 2.4 werde ich die klassischen Sylow-Sätze formulieren und gemäß dem Ziel dieser Arbeit mit den Hilfsmitteln der Gruppenwirkungen beweisen. Ich benutze dabei einerseits die Wirkung einer Gruppe auf der Menge von Nebenklassen nach einer Untergruppe per Linkstranslation und andererseits den zentralen Begriff des Normalisators, der mit Hilfe der Konjugationswirkung einer Gruppe auf ihrer Potenzmenge eingeführt wird. Die Resultate dieser Sätze bieten ein Werkzeug, um sogenannte p-Sylow-Untergruppen einer gegebenen Gruppe und deren Anzahl zu bestimmen. Dies führe ich schließlich an der alternierenden Gruppe A_4 und an der Permutationsgruppe S_4 vor.

Die Permutationsgruppen behandle ich im Kapitel 3. Sie spielen in der Gruppentheorie eine zentrale Rolle. Eine Permutationsgruppe ist eine Gruppe, die treu auf einer (endlichen) Menge wirkt. Zentral in diesem Kapitel ist der Nachweis der Einfachheit der alternierenden Gruppe A_n für $n \geq 5$ sowie der Beweis, dass es in der alternierenden Gruppe A_4 keine Untergruppe der Ordnung 6 geben kann. Außerdem werde ich noch beweisen, dass in einer Gruppe G mit Ordnung $|G| = 2^m k$ (wobei k ungerade ist), die Elemente von G mit ungerader Ordnung einen nicht trivialen Normalteiler von G bilden, wenn es ein Element mit Ordnung 2^m gibt. Eine zentrale Idee im Beweis ist,

die abstrakte Gruppe G via Linksmultiplikation als Permutationsgruppe (genauer: als Untergruppe von S_G) zu interpretieren. Damit ist es möglich, den Elementen von G, wie jedem Element der Permutationsgruppe S_n, ein Vorzeichen zuzuordnen, welches dann eine zentrale Rolle in der Argumentation spielt.

Anhang A gliedert sich in vier Abschnitte, die den Abschnitten des Kapitels 2 entsprechen, und bietet zu den dort besprochenen Beispielen die Auflistung der Kommandozeilen-Aufrufe des Computer Algebra Programms GAP (vgl. [4]) inklusive den Ergebnissen.

Die Grafiken in dieser Arbeit habe ich alle eigenhändig mit dem Programm jfig (vgl. [7]) erstellt.

Kapitel 2

Gruppenwirkungen

2.1 Grundlegende Definitionen und Resultate

Dieser Abschnitt widmet sich neben zwei äquivalenten Definitionen von Gruppenwirkungen den beiden Begriffen der Bahn eines Elements unter einer Wirkung und des Stabilisators eines Elements, um im Anschluss den fundamentalen Zusammenhang zu beweisen, dass die Anzahl der Elemente einer Bahn der Anzahl der Nebenklassen des Stabilisators in G entspricht. Es werden weiters elementare Beispiele von Gruppenwirkungen eingeführt. Die Anregungen für diesen Abschnitt basieren auf den Ausführungen von Fischer (vgl. [3] Abschnitt I.§4), Armstrong (vgl. [1] Kapitel 17) und Wolfart (vgl. [11] Abschnitt 2.6).

Folgende Idee ist für Gruppenwirkungen leitend: sei G eine Gruppe und X eine Menge; jedes Gruppenelement $g \in G$ definiere eine Bijektion $X \to X$, welche ebenfalls mit g bezeichnet werde, und zwar so, dass das Einselement 1 von G die identische Abbildung definiert und die Gruppenoperation der Hintereinanderausführung von Abbildungen entspricht.

Die formale Definition lautet: eine (Gruppen)Wirkung von G auf X ist eine Abbildung $\cdot : G \times X \to X$, $(g, x) \mapsto g \cdot x$, die jedem Paar von Elementen $g \in G$ und $x \in X$ ein Element $g \cdot x \in X$ zuordnet, sodass die beiden Eigenschaften

(i) $1 \cdot x = x$ für alle $x \in X$ (wobei 1 das Einselement von G ist) und

(ii) $g \cdot (h \cdot x) = gh \cdot x$ für alle $g, h \in G$ und alle $x \in X$

gelten. Eine andere Möglichkeit, den Begriff der Gruppenwirkung zu definieren ist folgende: Sei S_X die Gruppe aller Bijektionen $X \to X$. Eine Wirkung von G auf X ist ein Homomorphismus $\phi : G \to S_X, g \mapsto \underbrace{(x \mapsto \phi_g(x) = g \cdot x)}_{\phi_g}$.

Bevor ich die Äquivalenz dieser beiden Definitionen zeige, noch ein paar Erläuterungen zur letztgenannten Definition. Jedem Gruppenelement $g \in G$

wird durch ϕ eine Permutation der Elemente von X zugeordnet: $\phi : G \to S_X$, $g \mapsto (x \mapsto \phi_g(x))$. Für das Bild von x unter der Permutation, die g definiert, schreibt man $g \cdot x$ und man sagt: das Gruppenelement g "sendet" x nach $g \cdot x$. Die Bezeichnung "$g \in G$ wirkt auf X" bezieht sich auf alle Elemente der Menge X, das heißt auf die komplette Permutation der Elemente von X. Wichtig ist, dass bei einer Gruppenwirkung jedes Element der Gruppe eine Permutation von Elementen von X derart definiert, dass die Komposition von zwei solchen Permutationen der Verknüpfung in der Gruppe entspricht: für zwei beliebige Elemente $g, h \in G$ entspricht die Komposition der durch g definierten Permutationen mit jener durch h definierten der, die von gh - verknüpft per Gruppenoperation - definiert ist: $\phi_g \circ \phi_h = \phi_{gh}$.

Ich werde im Folgenden zeigen, dass die beiden gegebenen Definitionen von Gruppenwirkungen äquivalent sind.

Einerseits liefert jede Abbildung $G \times X \to X$ mit den Eigenschaften (i) und (ii) einen Homomorphismus $\phi : G \to S_X$ in die Gruppe aller Bijektionen $X \to X$. Zu zeigen ist, a) dass die von einem beliebigen Element g der Gruppe G definierte Abbildung $g : X \to X$ bijektiv ist und b), dass die Abbildung $\phi : G \to S_X$, $g \mapsto (x \mapsto g \cdot x)$ ein Homomorphismus ist. Ad a): Es existiert zu jedem $g : x \mapsto g \cdot x$ eine Umkehrabbildung $g^{-1} : y \mapsto g^{-1} \cdot y$, denn $g^{-1} \cdot (g \cdot x) \overset{(ii)}{=} (g^{-1}g) \cdot x = 1 \cdot x \overset{(i)}{=} x$ für alle $x \in X$ und analog: $g \cdot (g^{-1} \cdot y) = y$ für alle $y \in X$. Das ergibt unmittelbar die Bijektivität der Abbildung von $g : X \to X$. Ad b): Es folgt unmittelbar aus der Eigenschaft (ii) $g \cdot (h \cdot x) = gh \cdot x$, dass für alle $g, h \in G$ gilt: $\phi_g \circ \phi_h = \phi_{gh}$, dass ϕ also ein Homomorphismus ist.

Andererseits existiert umgekehrt zu jedem Gruppenhomomorphismus $\phi : G \to S_X$ von einer Gruppe G in eine Permutationsgruppe S_X eine Abbildung $\cdot : G \times X \to X$, nämlich $(g, x) \mapsto \phi_g(x) =: g \cdot x$. Diese hat die oben genannten Eigenschaften (i) und (ii). Da ϕ ein Homomorphismus ist, gilt:

$\phi(1) = id$, das heißt das Einselement der Gruppe G wird der identischen Abbildung zugeordnet, die jedes $x \in X$ auf x abbildet. Das ergibt Eigenschaft (i): $\phi_1(x) = 1 \cdot x = x$. Ferner folgt aus $\phi_g \circ \phi_h = \phi_{gh}$ für alle $g, h \in G$ die Eigenschaft (ii) $g \cdot (h \cdot x) = \phi_g(\phi_h(x)) = \phi_{gh}(x) = gh \cdot x$ für alle $g, h \in G$ und $x \in X$. Es kann somit jeder Gruppenhomomorphismus von einer beliebigen Gruppe G in eine Permutationsgruppe S_X als Gruppenwirkung von G auf X interpretiert werden und umgekehrt.

Die Eigenschaft (i) in der Definition von Gruppenwirkung ist unabhängig von Eigenschaft (ii), ein Beispiel soll dies verdeutlichen. Sei $X = \{0, 1\}$, G eine beliebige Gruppe und $(g, x) \mapsto 0$ eine konstante Abbildung. Diese Abbildung erfüllt die Bedingung (ii) der Definition. Da ein beliebiges $g \in G$ das Element 1 nicht auf 1 abbildet, ist Eigenschaft (i) verletzt, woraus folgt, dass dies keine Gruppenwirkung ist.

Beispiele.

(1) Eine Gruppe G kann auf ein und derselben Menge X auf unterschiedliche Art und Weisen wirken — es wird i.a. verschiedene Homomorphismen $G \to S_X$ geben. Sei z.B. G die unendliche zyklische Gruppe $\mathbb{Z}$ und $X = \mathbb{R}$ die Menge der reellen Zahlen. Dann kann man eine Wirkung durch Translation definieren: $g \cdot x = g + x$. Es gilt $0 + x = x$ und für alle $g, h \in \mathbb{Z}$ gilt $(g + h) + x = g + (h + x)$. Damit ist ersichtlich, dass es sich hierbei um eine Gruppenwirkung handelt. Die Gruppe $G = \mathbb{Z}$ könnte auf $X = \mathbb{R}$ aber auch durch folgende Vorschrift wirken: $g \cdot x = (-1)^g x$. Aus $(-1)^0 x = 1x = x$ und $(-1)^{g+h} x = (-1)^g (-1)^h x$ folgt, dass man es auch hier mit einer Gruppenwirkung zu tun hat.

(2) Für jede Gruppe G und jede Menge X ist durch $g : x \mapsto x$ für alle $g \in G$ und $x \in X$ eine Wirkung definiert, die *triviale* Wirkung. Die Abbildung ϕ ordnet jedem Element g das neutrale Element von S_X zu - die identische Ab-

bildung, die jedes Elemente aus X wieder auf sich selbst abbildet. Der Kern von ϕ ist bei dieser Wirkung ganz G.

Bemerkung: wirkt eine Gruppe G auf einer Menge X, so wirkt auch jede Untergruppe H von G auf X. Weiters: wirkt die Gruppe G auf der Menge X, dann wirkt G auch auf jeder invarianten Teilmenge. Dabei heißt eine Teilmenge $Y \subseteq X$ *invariant* unter der Wirkung von G, wenn $g \cdot y \in Y$ für alle $g \in G$ und $y \in Y$ gilt.

Wirkt G auf X, dann wirkt wegen

$$\begin{aligned}
\text{(i) } 1 \cdot Z &= \{1 \cdot z \mid z \in Z\} && \text{(wobei 1 das Einselement aus } G \text{ ist)} \\
&= Z \\
\text{(ii) } g \cdot (h \cdot Z) &= g \cdot \{h \cdot z \mid z \in Z\} && \text{für alle } g, h \in G \\
&= \{g \cdot (h \cdot z) \mid z \in Z\} \\
&= \{(gh) \cdot z \mid z \in Z\} \\
&= (gh) \cdot Z
\end{aligned}$$

G in der angegebenen Weise auch auf der Potenzmenge 2^X von X.

Die folgenden beiden Definitionen werden sich als fundamental erweisen: für jedes $x \in X$ heißen

$$O_x := G \cdot x = \{g \cdot x \mid g \in G\}$$

die *Bahn* (oder der *Orbit*) von x unter der Wirkung von G und

$$G_x := \{g \in G \mid g \cdot x = x\}$$

der *Stabilisator* von x. Die Bahn eines Elements ist also die Menge aller Bilder von x unter der Gruppenwirkung von ganz G, also von allen Elementen aus G. Der Stabilisator eines Elements x enthält jene Gruppenelemente aus G,

die x invariant lassen, also stabilisieren. Daher auch die Bezeichnung. Der Stabilisator G_x ist immer eine Untergruppe von G. Denn wegen $1 \cdot x = x$ ist das neutrale Element von G sicher in G_x; seien weiters $g, h \in G_x$, also $g \cdot x = x$ und $h \cdot x = x$. Dann gilt auch $h^{-1} \cdot x = x$ und insgesamt $g \cdot (h^{-1} \cdot x) = g \cdot x = x$. Es ist also auch $gh^{-1} \in G_x$ und es folgt, dass der Stabilisator G_x Untergruppe von G ist.

Sei weiters eine Relation $\sim$ auf X definiert durch

$$x \sim y \Longleftrightarrow \exists g \in G : y = g \cdot x;$$

dann gilt: $\sim$ ist eine Äquivalenzrelation auf X:

- Wenn $x \sim y$ gilt, also $y = g \cdot x$ für ein $g \in G$, dann folgt

  $$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = g^{-1}g \cdot x = 1 \cdot x = x$$

  es gilt also auch $y \sim x$. Die Relation $\sim$ ist symmetrisch.

- Wenn sowohl $x \sim y$ als auch $y \sim z$ gilt, also $g \cdot x = y$ und $h \cdot y = z$ für gewisses $g, h \in G$, dann folgt

  $$hg \cdot x = h \cdot (g \cdot x) = h \cdot y = z$$

  und es gilt also auch $x \sim z$. Die Relation $\sim$ ist transitiv.

- Aus der Eigenschaft $1 \cdot x = x$ ergibt sich unmittelbar die Reflexivität der Relation $\sim$.

Die Äquivalenzklassen dieser Relationen sind genau die Bahnen O_x. Die Bahnen liefern damit eine Zerlegung von X in paarweise disjunkte Teilmengen von X. Jede Bahn ist insbesondere eine invariante Teilmenge. Da die Bahnen eine Partition der Menge X bilden, gilt, dass die Mächtigkeit der Menge X

gleich der Summe über die Kardinalitäten aller Bahnen ist. Mit Hilfe des Stabilisators kann man beschreiben, wann zwei Elemente g und h aus der Gruppe G dieselbe Wirkung $g \cdot x = h \cdot x$ auf ein Element x haben: es ist nämlich

$$\begin{aligned} g \cdot x = h \cdot x &\Leftrightarrow h^{-1}g \cdot x = x \\ &\Leftrightarrow h^{-1}g \in G_x \\ &\Leftrightarrow h^{-1}gG_x = G_x \\ &\Leftrightarrow gG_x = hG_x. \end{aligned}$$

Dies gilt also genau dann, wenn sie in der selben Linksnebenklasse nach dem Stabilisator liegen. Diese Tatsache wird im nachstehenden Satz verwendet.

Wie üblich seien mit $|G|, |G_x|$ und $|O_x|$ die Anzahl der Elemente der Gruppe G, des Stabilisators G_x und der Bahn O_x bezeichnet. Letztere heißt auch die Länge der Bahn. Mit $[G : G_x]$ sei der Index des Stabilisators G_x in der Gruppe G, also die Anzahl der Linksnebenklassen von G nach dem Stabilisator G_x angegeben.

Zwischen Bahn und Stabilisator besteht ein fundamentaler Zusammenhang, der im Bahn-Stabilisator-Satz zusammengefasst ist.

Satz 2.1. *Die Gruppe G wirke auf der Menge X; für jedes $x \in X$ ist die Abbildung $gG_x \mapsto g \cdot x$ eine Bijektion von der Menge G/G_x aller Linksnebenklassen von G nach dem Stabilisator G_x auf die Bahn O_x von x. Ist insbesondere G endlich, dann auch die Bahn O_x und es gilt*

$$|O_x| = [G : G_x] = \frac{|G|}{|G_x|}$$

und daher auch

$$|O_x| \cdot |G_x| = |G|.$$

Beweis. Die Abbildung $G/G_x \to O_x$, $gG_x \mapsto g \cdot x$ ist eine wohldefinierte Bijektion, die in Abbildung 2.1 dargestellt ist.

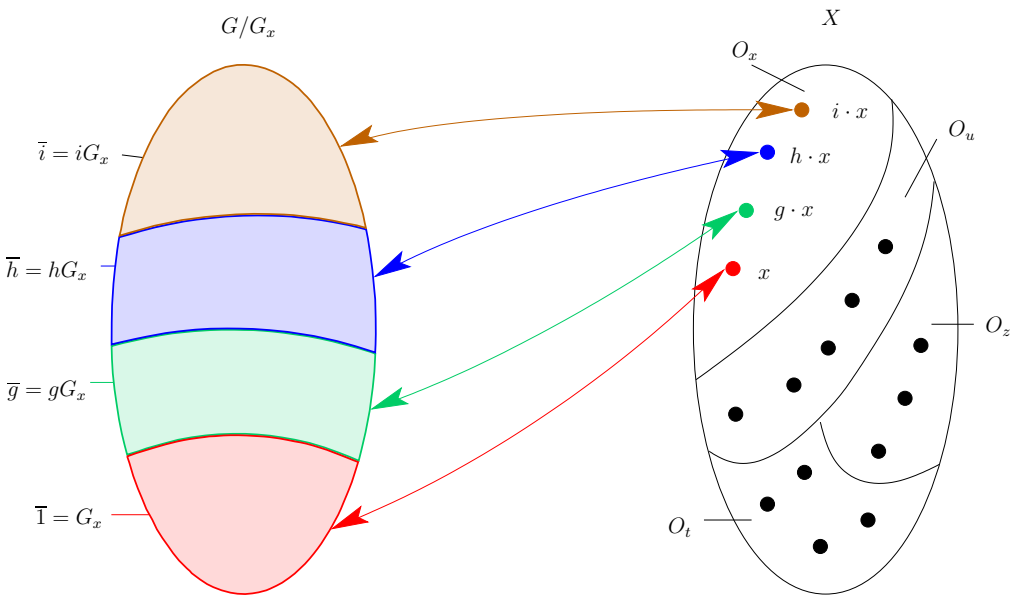

Abbildung 2.1: Bijektive Abbildung $G/G_x \to O_x$

Für $g, h \in G$ mit $gG_x = hG_x$ gilt $h^{-1}g \in G_x$, das heißt $h^{-1}g \cdot x = x$, also auch $h \cdot x = g \cdot x$. Die Abbildung ist also unabhängig von der Wahl des Repräsentanten der Linksnebenklasse und somit wohldefiniert. Umgekehrt haben, wie oben erwähnt, g und h dann dieselbe Wirkung $g \cdot x = h \cdot x$, wenn die Linksnebenklassen gG_x und hG_x von G nach dem Stabilisator G_x gleich sind. Die Abbildung $G/G_x \to O_x$, $gG_x \mapsto g \cdot x$ ist also injektiv. Offensichtlich ist die Abbildung surjektiv, also insgesamt bijektiv. Die Bijektivität dieser Abbildung und die Endlichkeit der Mengen impliziert, dass die Anzahl der Elemente der Bahn eines Elements x gleich dem Index des Stabilisators G_x in der Gruppe G ist, also $|O_x| = [G : G_x]$. Die Gleichheit von $[G : G_x]$ und $\frac{|G|}{|G_x|}$ folgt unmittelbar aus dem Satz von Lagrange. Nach einfacher Umformung folgt insgesamt $|O_x| \cdot |G_x| = |G|$. □

Daraus folgt, dass insbesondere alle Bahnlängen $|O_x|$ Teiler der Gruppenordnung $|G|$ sind.

Eine Gruppe G wirkt *transitiv* auf X, wenn $\sim$ die Allrelation ist, das heißt wenn die Bahn eines jeden Elements mit X zusammenfällt; wenn es also nur eine Bahn gibt. Das bedeutet: G wirkt transitiv, wenn für alle $x, y \in X$ ein $g \in G$ existiert mit $g \cdot x = y$.

Die Wirkung ist *treu*, wenn der Homomorphismus $G \to S_X$ injektiv ist, das heißt $g \cdot x = x$ für alle $x \in X$ nur für $g = 1$ gilt. Dies ist genau dann der Fall, wenn der Durchschnitt aller Stabilisatoren die triviale Gruppe ist, wenn also nur das Einselement 1 von G als Identität auf X wirkt. Mit anderen Worten: G wirkt treu, wenn G als Untergruppe von S_X aufgefaßt werden kann.

Nach dem Bahn-Stabilisator-Satz gilt dann offensichtlich:

- Wirkt eine Gruppe G transitiv auf der Menge X, dann gilt

$$|G| = |X||G_x|$$

  für jedes $x \in X$.

- Wirkt eine Gruppe G auf einer Menge X transitiv und treu, dann gilt

$$|G| = |X|.$$

Lemma 2.2. *Die Elemente einer Bahn haben konjugierte Stabilisatoren.*

Beweis. Sei G eine Gruppe, die auf X wirke, und seien x und y Elemente derselben Bahn; dann existiert ein $g \in G$, sodass $g \cdot x = y$. Für $h \in G_x$ gilt, dass ghg^{-1} im Stabilisator von y liegt: in der Tat, aus $h \cdot x = x$ folgt mit $g \cdot x = y$, dass $g \cdot (h \cdot x) = y$ gilt und daraus wegen $g^{-1} \cdot y = x$ schließlich $ghg^{-1} \cdot y = y$, insgesamt also $gG_xg^{-1} \subseteq G_y$. Vertauscht man die Rollen von x und y so erhält man $g^{-1}G_yg \subseteq G_x$ und Konjugation mit g ergibt $G_y \subseteq gG_xg^{-1}$, woraus schließlich $gG_xg^{-1} = G_y$ folgt. □

Lemma 2.3. *Wirkt eine Gruppe G transitiv, so sind alle Stabilisatoren von Elementen aus X zu einem beliebigen Stabilisator G_x konjugiert.*

Beweis. Da die Gruppe G laut Voraussetzung transitiv wirkt, gibt es nur eine Bahn. Die Aussage des Satzes folgt also unmittelbar aus dem Lemma 2.2. □

Es folgen einige weitere Beispiele.

Beispiele. (3) Auf jeder Menge X wirkt klarerweise die Permutationsgruppe S_X. Wirke etwa die Permutationsgruppe S_3 auf der Menge $X = \{1, 2, 3\}$, dann sind die Bahnen $O_1 = O_2 = O_3 = \{1, 2, 3\}$ die ganze Menge X. Die Wirkung ist also transitiv. Es ergeben sich die Stabilisatoren $G_1 = \{(1), (2, 3)\}$, $G_2 = \{(1), (1, 3)\}$, $G_3 = \{(1), (2, 3)\}$ und daraus die Indizes $[G : G_1] = [G : G_2] = [G : G_3] = 3$. Da der Durchschnitt aller Stabilisatoren $\{(1)\}$ ist, ist die Wirkung treu.

(4) Jede Gruppe wirkt auf sich selbst (das heißt auf der Menge aller Elemente von G) durch Linksmultiplikation auch Linkstranslation genannt $\cdot : G \times G \to G$: $(g, x) \mapsto g \cdot x = gx$ (oder anders gesagt $\phi : G \to S_G$, $g \mapsto (x \mapsto gx)$). Es wird also die Gruppenverknüpfung von links angewendet. Durch Rechtsmultiplikation kann ebenfalls eine Wirkung definiert werden, nämlich via $g \cdot x := xg^{-1}$; es sind wieder die Bedingungen in der Definition für Gruppenwirkungen erfüllt: $1 \cdot x = x$ für alle $x \in G$ und $g \cdot (h \cdot x) = xh^{-1}g^{-1} = x(gh)^{-1} = (gh) \cdot x$ für alle $g, h, x \in G$. Diese Wirkungen sind transitiv und treu, es gilt sogar, dass alle Stabilisatoren trivial sind. Der korrespondierende Homomorphismus ϕ ist also ein Monomorphismus. Aus dieser Tatsache resultiert der Satz von Cayley (siehe Satz 3.1), der im Kapitel 3 behandelt wird.

Im Anhang A.1 ist der GAP-Code dargestellt, mit dem ich diese Behauptungen per Computer Algebra Programm GAP für die Permutationsgruppe S_3 und die alternierende Gruppe A_4 nachvollzogen habe.

(5) Eine Untergruppe U von G wirke auf G per Linksmultiplikation: $U \times G \to G$, $(u, g) \mapsto ug$. (Es wurde bereits bemerkt, dass jede Wirkung einer Gruppe G auf jede Untergruppe eingeschränkt werden kann.) Es sind also ebenfalls die Bedingungen für eine Gruppenwirkung erfüllt. Die Bahn O_g eines Elements $g \in G$ besteht aus allen Elementen der Form ug mit $u \in U$. Das sind genau die Rechtsnebenklassen Ug von U in G. ($O_g = \{ug \mid u \in U\} = Ug$). Die Menge aller Rechtsnebenklassen $U\backslash G$ bildet die entsprechende Partition von G. Analog ergeben sich für die Wirkung per Rechtsmultiplikation als Bahnen die Linksnebenklassen.

(6) Eine Gruppe G wirkt auf 2^G der Menge aller ihrer Teilmengen durch Linksmultiplikation ($\phi : G \to S_{2^G}$, $g \mapsto g \cdot U = gU$). Diese Gruppenwirkung wird im Abschnitt 2.4 genauer betrachtet.

(7) Sei G eine Gruppe, K eine Untergruppe von G und G/K die Menge aller Linksnebenklassen gK von G nach K; dann wirkt G auf G/K in natürlicher Weise mittels Linksmultiplikation: $\phi : G \to S_{G/K}$, $h \mapsto h \cdot gK = hgK$ für alle $h \in G$ und $gK \in G/K$. Diese Wirkung ist transitiv. Sie wird in Abschnitt 2.4 beim Beweis der Sylow-Sätze zur Anwendung kommen.

Diese Gruppenwirkung soll an folgendem konkreten Beispiel illustriert werden. Sei die Gruppe G gleich der Permutationsgruppe S_3 und die Untergruppe K gleich der alternierenden Gruppe A_3. Die Gruppe G hat also die Elemente
$G = S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ und
$K = A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. Dann besteht die Menge X, da A_3 normal in S_3 ist, aus $\{A_3, aA_3\}$. Sei $H = \{(1), (1\ 2)\}$ eine Untergruppe von G. Dann wirkt H auf X. Folgende Abbildungen sind damit definiert:

- $(1) : A_3 \mapsto A_3,\ (1\ 2)A_3 \mapsto (1\ 2)A_3$
- $(1\ 2) : A_3 \mapsto (1\ 2)A_3,\ (1\ 2)A_3 \mapsto A_3$

Es ist ersichtlich, dass die Bahnen jeweils ganz X sind, also 2 Elemente haben.

Die Wirkung ist also transitiv. Der Stabilisator ist in beiden Fällen trivial. Die Gleichung $|O_x| \cdot |H_x| = |H|$ ergibt $2 \cdot 1 = 2$.

(7) Die prime Restklassengruppe modulo n (i.e. die Einheitengruppe $\mathbb{Z}_n^\times$ von $\mathbb{Z}_n$) wirkt auf dem Ring $\mathbb{Z}_n$ durch Multiplikation von links: $g : x \mapsto gx$ für $g \in \mathbb{Z}_n^\times$ und $x \in \mathbb{Z}_n$ (gilt analog für die Einheitengruppe eines jeden Rings mit 1).

(8) Sei $G = GL(n, K)$ (i.e. die Gruppe der invertierbaren $n \times n$-Matrizen über dem Körper K). Dann wirkt G in nahe liegender Weise auf $X = K^n$ durch Matrixmultiplikation von links. Die Voraussetzungen einer Gruppenwirkung sind für die Abbildung $GL(nK) \times K^n \to K^n$, $(A, x) \mapsto A \cdot x$ gegeben, denn (i) die Einheitsmatrix E bildet das Einselement der Matrixmultiplikation und es gilt daher $E \cdot x = x$ für alle $x \in K^n$. Die Voraussetzung (ii) folgt aus der Assoziativität der Matrixmultiplikation. Sei $o = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ und $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ein beliebiges Element aus $K^n \backslash \{o\}$. Die Bahn O_x von x besteht aus $K^n \setminus \{o\}$: dazu genügt es zu zeigen, dass $O_{e_1} = K^n \setminus \{o\}$, wobei $e_1 = \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix}$ der erste Einheitsvektor ist. Da $x \neq o$, kann x durch geeignete Vektoren $x_2, \ldots, x_n$ zu einer Basis von K^n ergänzt werden. Die Matrix $A = (x, x_2, \ldots, x_n)$ hat dann Rang n, ist also invertierbar und liegt damit in $GL(n, K)$; wegen $Ae_1 = x$ gilt $x \in O_{e_1}$ für jedes beliebige $x \neq o$. Da $Ao = o$ für jede $n \times n$-Matrix, bildet $\{o\}$ eine Bahn für sich. Insbesondere besteht der Stabilisator von o aus ganz $GL(n, K)$. Die Stabilisatoren von $x \neq o$ sind alle zueinander isomorph (Lemma 2.2) und werden im Abschnitt über semidirekte Produkte noch genauer beschrieben (siehe Beispiel (5) in Abschnitt 2.3). Festgehalten sei an dieser Stelle, dass der Stabilisator von e_1 offenbar aus allen invertierbaren $n \times n$-

Matrizen A besteht, für die $Ae_1 = e_1$ gilt; das sind genau jene invertierbaren Matrizen, deren erste Spalte gleich dem ersten Einheitsvektor e_1 ist.

Die Wirkung von $GL(n, K)$ auf K^n ist treu: angenommen für $A \in GL(n, K)$ gelte $Ax = x$ für jedes $x \in K^n$. Dann gilt dies insbesondere für jeden Einheitsvektor e_i: $Ae_i = e_i$ für jedes i. Aber Ae_i ist nichts anderes als die i-te Spalte der Matrix A, also hat A als i-te Spalte genau den i-ten Einheitsvektor e_i. Dies gilt für jedes i, also muß $A = E$ die Einheitsmatrix sein.

Insbesondere wirkt beispielsweise die spezielle orthogonale Gruppe $SO(2, \mathbb{R})$ vom Grad 2 über dem Körper $\mathbb{R}$ via Matrixmultiplikation auf der Euklidischen Ebene $\mathbb{R}^2$. Bekanntlich ist diese Untergruppe von $GL(n, \mathbb{R})$ die Gruppe der orthogonalen Matrizen mit Determinante $+1$, die alle Drehungen um den Ursprung $(0, 0)$ im $\mathbb{R}^2$ beschreiben. Hier ist der Stabilisator des Ursprungs wieder die ganze Gruppe, während der Stabilisator jedes anderen Punktes trivial ist, also die Drehung mit Drehwinkel 0. Die Bahn des Ursprungs ist der Ursprung. Jeder andere Punkt $(x_0, y_0) \in \mathbb{R}^2 \backslash \{(0, 0)\}$ wird auf einer Kreisbahn um den Ursprung bewegt; die Bahn von (x_0, y_0) ist also die Menge $\{(x, y) \mid |(x_0, y_0)| = |(x, y)|\}$.

(9) Jede Gruppe G wirkt auf sich selbst durch Konjugation, definiert durch $g \cdot x := g^{-1}xg$ für alle $g, x \in G$. Es handelt sich dabei tatsächlich um eine Wirkung, denn (i) $1 \cdot x = 1x1 = x$ für alle $x \in G$ und (ii) $h \cdot (g \cdot x) = h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1} = (hg) \cdot x$ für alle $g, h, x \in G$ sind sicherlich erfüllt. Diese Wirkung ist nicht transitiv und treu genau dann, wenn das Zentrum von G trivial ist (siehe den Abschnitt 2.2). Auf dieses Beispiel wird im Abschnitt 2.2 noch genauer eingegangen.

(10) Eine Gruppe G wirkt auf 2^G per Konjugation durch $g \cdot U = g^{-1}Ug$ für $g \in G$ und $U \in 2^G$. Im Abschnitt 2.4 wird dieser Begriff beim Beweis der Sylow-Sätze angewendet.

2.2 Klassengleichung

Üblicherweise wird in Algebralehrbüchern die spezielle Klassengleichung behandelt, die von der im letzten Abschnitt unter Beispiel (9) eingeführten Konjugationswirkung $\cdot : G \times G \to G : (g, x) \mapsto g \cdot x = gxg^{-1}$ ausgeht. Es ist jedoch sinnvoll, die Klassengleichung abstrakt für Gruppenwirkungen herzuleiten, was ich zu Beginn dieses Abschnittes durchführen werde. Anschließend werden die Begriffe Zentrum und Zentralisator definiert und die spezielle Klassengleichung betrachtet. Dieses wichtige Werkzeug wird am Beispiel der Permutationsgruppe S_3, der zyklischen Gruppe $\mathbb{Z}_3$ und der alternierenden Gruppe A_4 illustriert und kommt in den nachstehenden Abschnitten mehrfach direkt und indirekt zur Anwendung.

Sei G eine Gruppe, die auf einer Menge X vermöge $g : x \mapsto g \cdot x$ wirke; sind O_i $(i \in I)$ die Bahnen, dann ist X die Vereinigung der paarweise disjunkten Mengen O_i. Ist X endlich, dann gibt es nur endlich viele Bahnen $O_1, \ldots, O_k$ (die ebenfalls endlich sind) und es gilt offensichtlich

$$|X| = \sum_{i=1}^{k} |O_i|. \tag{2.2.1}$$

Nun soll zwischen zwei Sorten von Bahnen differenziert werden: Seien $P_1, \ldots, P_l$ jene Bahnen, die aus mehr als einem Element bestehen (das heißt $|P_i| > 1$ für alle i) und $Q_1, \ldots, Q_m$ jene Bahnen, die nur aus einem Element bestehen (das heißt $|Q_i| = 1$ für alle i). Setzt man $X_0 := \bigcup_{i=1}^{m} Q_i$, dann gilt: X_0 besteht aus genau den Elementen von X, auf die alle Elemente von G die triviale Wirkung haben. Mit anderen Worten: X_0 besteht genau aus der Menge aller *Fixpunkte* der Wirkung. Aus (2.2.1) folgt nunmehr:

$$|X| = |X_0| + \sum_{i=1}^{l} |P_i|. \tag{2.2.2}$$

Wählt man aus jeder Bahn P_i ein Element x_i und nimmt man zusätzlich an,

dass G ebenfalls endlich ist, so folgt aus Satz 2.1, dass

$$|P_i| \cdot |G_{x_i}| = |G|$$

für alle i gilt. Insgesamt wird damit wegen $\frac{|G|}{|G_{x_i}|} = [G : G_{x_i}]$ die Gleichung (2.2.2) zu

$$|X| = |X_0| + \sum_{i=1}^{l} [G : G_{x_i}]. \tag{2.2.3}$$

Man beachte, dass jeder der Summanden $[G : G_{x_i}] = |P_i|$ größer als 1 ist.

Betrachten wir das bereits im letzen Abschnitt vorgestellte klassische Beispiel (9) der Konjugationswirkung. Die Bahnen bezüglich dieser Wirkung heißen *"Konjugiertenklassen"* von G oder "*Klassen konjugierter Elemente von G*". Dann stellt sich die Frage, was in diesem Fall die Fixpunktmenge X_0 ist. Es gilt:

$$\begin{aligned} X_0 = G_0 &= \{x \in G \mid g \cdot x = x \ \forall g \in G\} \\ &= \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} \\ &= \{x \in G \mid gx = xg \ \forall g \in G\} =: Z(G). \end{aligned}$$

$Z(G)$ heißt das *Zentrum* von G. Für dieses kann festgehalten werden:

(a) Das Zentrum einer Gruppe G ist eine Untergruppe von G, denn: es enthält immer das Einselement 1, weil $1g = g1$ für alle g der Gruppe G gilt. Angenommen z liegt im Zentrum, dann auch z^{-1}: sei $g \in G$ beliebig, dann kommutiert z mit g^{-1}, also $zg^{-1} = g^{-1}z$, also auch $(zg^{-1})^{-1} = (g^{-1}z)^{-1}$, was wiederum $gz^{-1} = z^{-1}g$ impliziert. Weil $g \in G$ beliebig war, liegt z^{-1} ebenfalls im Zentrum. Liegen weiters y, z im Zentrum, dann auch yz, denn für beliebiges $g \in G$ gilt $(yz)g = ygz = g(yz)$.

(b) Das Zentrum einer Gruppe G ist immer eine *charakteristische* Untergruppe von G, das heißt es ist invariant unter allen Automorphismen von G. Sei also $\phi : G \to G$ ein beliebiger Automorphismus und $h \in Z(G)$. Es

muss gezeigt werde, dass $\phi(h)$ mit jedem $x \in G$ kommutiert. Zu gegebenem $x \in G$ gibt es ein (eindeutig bestimmtes) $y \in G$ mit $x = \phi(y)$. Da h im Zentrum liegt, gilt $yh = hy$; Anwendung von ϕ ergibt $x\phi(h) = \phi(y)\phi(h) = \phi(yh) = \phi(hy) = \phi(h)\phi(y) = \phi(h)x$.

(c) Charakteristische Untergruppen sind immer Normalteiler in der Gruppe, denn Normalteiler sind dadurch charakterisiert, dass sie invariant unter allen *inneren* Automorphismen sind. Somit ist klar, was schon aus der Definition folgt, dass das Zentrum einer Gruppe $Z(G)$ Normalteiler in G ist.

(d) Das Zentrum einer Gruppe G besteht per definitionem aus allen Elementen von G, die mit allen Elementen von G kommutieren. Das Zentrum $Z(G)$ ist daher eine abelsche Gruppe.

(e) Das Zentrum $Z(G)$ von G stimmt mit der Gruppe G genau dann überein, wenn die Gruppe G abelsch ist.

(f) Die Elemente des Zentrums sind dadurch charakterisiert, dass die Konjugiertenklassen dieser Elemente einelementig sind, also die Elemente des Zentrums genau die Fixpunkte der Konjugationswirkung sind.

Sei $x \in G$; so stellt sich die Frage, wie man den Stabilisator G_x von x unter der Konjugationswirkung beschreiben kann. Es gilt:

$$\begin{aligned} G_x &= \{g \in G \mid g \cdot x = x\} \\ &= \{g \in G \mid gxg^{-1} = x\} \\ &= \{g \in G \mid gx = xg\} =: C_G(x). \end{aligned}$$

$C_G(x)$ heißt der *Zentralisator von x in G*. Für eine beliebige nichtleere Teilmenge Y von G heißt die Menge

$$C_G(Y) := \{g \in G \mid gy = yg \ \forall y \in Y\}$$

der Zentralisator von Y in G; es gilt:

1. für jede nichtleere Teilmenge Y von G ist $C_G(Y)$ wie jeder Stabilisator eine Untergruppe von G. Insgesamt ist also der Stabilisator (bezüglich der Konjugation) G_x eines Elements x genau der Zentralisator $C_G(x)$.

2. Daraus folgt, dass das neutrale Element der Gruppe in jedem Zentralisator eines Elements bzw. einer Teilmenge enthalten ist, da es mit jedem Element der Gruppe kommutiert.

3. Ein Element x der Gruppe G liegt genau dann im Zentrum, wenn $C_G(x) = G$, das heißt, der Zentralisator umfasst die ganze Gruppe.

4. Das Zentrum ist der Durchschnitt aller Zentralisatoren.

Die Gleichung (2.2.3) wird mit der Gruppenwirkung per Konjugation zu

$$|G| = |Z(G)| + \sum_{i=1}^{l} [G : C_G(x_i)], \tag{2.2.4}$$

wobei über alle Konjugiertenklassen mit mehr als einem Element summiert wird (und $\{x_1, \ldots, x_l\}$ ein Repräsentantensystem dieser Konjugiertenklassen ist). Die Gleichung (2.2.4) (oder eine dazu äquivalente Gleichung) wird in der Literatur üblicherweise als *Klassengleichung* bezeichnet — in diesem Sinn kann (2.2.3) als *verallgemeinerte* Klassengleichung bezeichnet werden.

Abschließend noch drei **Beispiele**.

(1) Die Permutationsgruppe $G = S_3$ wirke auf sich selbst per Konjugation $G \times G \to G, (g, x) \mapsto gxg^{-1}$. Nachstehende Tabelle 2.1 enthält die Konjugiertenklassen und Zentralisatoren unter dieser Wirkung.

Man sieht, es gibt die drei Konjugiertenklassen:
$\{(1)\}$, $\{(1\,2), (1\,3), (2\,3)\}$ und $\{(1\,2\,3), (1\,3\,2)\}$ und kann erkennen, dass jeweils die 2er-Zyklen und die 3er-Zyklen in derselben Konjugiertenklasse sind. Das ist kein Zufall. Näheres dazu im Kapitel 3 über Permutationsgruppen.

x	O_x	$C_G(x)$	$\lvert O_x\rvert\lvert C_G(x)\rvert = \lvert G\rvert$
(1)	$\{(1)\}$	$G = S_3$	$1 \cdot 6 = 6$
(1 2)	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\{(1), (1\ 2)\}$	$3 \cdot 2 = 6$
(1 3)	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\{(1), (1\ 3)\}$	$3 \cdot 2 = 6$
(2 3)	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\{(1), (2\ 3)\}$	$3 \cdot 2 = 6$
(1 2 3)	$\{(1\ 2\ 3), (1\ 3\ 2)\}$	$\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$	$2 \cdot 3 = 6$
(1 3 2)	$\{(1\ 2\ 3), (1\ 3\ 2)\}$	$\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$	$2 \cdot 3 = 6$

Tabelle 2.1: $G = S_3$ wirkt auf sich per Konjugation

Das Zentrum $Z(G)$ von S_3 ist $\{(1)\}$. Die Gruppe $G = S_3$ stimmt also nicht mit dem Zentrum überein. Sie ist daher nicht abelsch. Die Klassengleichung (2.2.4) ergibt wie erwartet $|G| = |Z(G)| + \sum_{i=1}^{l}[G : C_G(x_i)] = 1 + 3 + 2 = 6$.

(2) Wirke die Gruppe $G = (\mathbb{Z}_3, +)$ durch Konjugation auf sich. Nachstehende Tabelle 2.2 enthält die Konjugiertenklassen und Zentralisatoren unter dieser Wirkung.

Element x	O_x	$C_G(x)$	$\lvert O_x\rvert\lvert C_G(x)\rvert = \lvert G\rvert$
$\overline{0}$	$\overline{0}$	$G = \{\overline{0}, \overline{1}, \overline{2}\}$	$1 \cdot 3 = 3$
$\overline{1}$	$\overline{1}$	$G = \{\overline{0}, \overline{1}, \overline{2}\}$	$1 \cdot 3 = 3$
$\overline{2}$	$\overline{2}$	$G = \{\overline{0}, \overline{1}, \overline{2}\}$	$1 \cdot 3 = 3$

Tabelle 2.2: $G = \mathbb{Z}_3$ wirkt auf sich per Konjugation

Das Zentrum $Z(G) = G$, daraus folgt, dass $G = \mathbb{Z}_3$ abelsch ist. Die Klassengleichung (2.2.4) ergibt $|G| = |Z(G)| + \sum_{i=1}^{l}[G : C_G(x_i)] = 3 + 0 = 3$

(3) Die alternierende Gruppe $G = A_4$ wirke auf sich selbst per Konjugation $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$. Die nachstehende Tabelle 2.3 enthält Konjugiertenklassen und Zentralisatoren unter dieser Wirkung. Man sieht, dass es die

x	O_x	$C_G(x)$	$\lvert O_x\rvert\lvert C_G(x)\rvert = \lvert G\rvert$
(1)	(1)	$G = A_4$	$1 \cdot 12 = 12$
(2 3 4)	(2 3 4), (1 2 4), (1 3 2), (1 4 3)	(1)(2 3 4), (2 4 3)	$4 \cdot 3 = 12$
(2 4 3)	(2 4 3), (1 2 3), (1 3 4), (1 4 2)	(1), (2 3 4), (2 4 3)	$4 \cdot 3 = 12$
(1 2)(3 4)	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)	(1), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)	$3 \cdot 4 = 12$
(1 2 3)	(2 4 3), (1 2 3), (1 3 4), (1 4 2)	(1), (1 2 3), (1 3 2)	$4 \cdot 3 = 12$
(1 2 4)	(2 3 4), (1 2 4), (1 3 2), (1 4 3)	(1), (1 2 4), (1 4 2)	$4 \cdot 3 = 12$
(1 3 2)	(2 3 4), (1 2 4), (1 3 2), (1 4 3)	(1), (1 2 3), (1 3 2)	$4 \cdot 3 = 12$
(1 3 4)	(2 4 3), (1 2 3), (1 3 4), (1 4 2)	(1), (1 3 4), (1 4 3)	$4 \cdot 3 = 12$
(1 3)(2 4)	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)	(1), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)	$3 \cdot 4 = 12$
(1 4 2)	(2 4 3), (1 2 3), (1 3 4), (1 4 2)	(1), (1 2 4), (1 4 2)	$4 \cdot 3 = 12$
(1 4 3)	(2 3 4), (1 2 4), (1 3 2), (1 4 3)	(1), (1 3 4), (1 4 3)	$4 \cdot 3 = 12$
(1 4)(2 3)	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)	(1), (1 2)(3 4), (1 3)(2 4), (1 4)(2, 3	$3 \cdot 4 = 12$

Tabelle 2.3: $G = A_4$ wirkt auf sich per Konjugation

folgenden vier Konjugiertenklassen gibt:
$\{(1)\}$, $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\{(2\ 4\ 3), (1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2)\}$, $\{[(2\ 3\ 4), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 3)\}$ Ferner kann man erkennen, dass jeder 3er-Zyklus in einer Konjugiertenklasse der Ordnung 4 liegt. Dies wird allgemein im Kapitel 3 bewiesen und im Beweis, dass es in A_4 keine Untergruppe der Ordnung 6 geben kann, verwendet. Das Zentrum $Z(G)$ von A_4 ist $\{(1)\}$. Die Gruppe $G = A_4$ stimmt also nicht mit dem Zentrum überein. Sie ist daher nicht abelsch. Die Klassengleichung (2.2.4) ergibt wie erwartet $|G| = |Z(G)| + \sum_{i=1}^{l}[G : C_G(x_i)] = 1 + 4 + 3 + 3 = 12$.

Ich habe diese Beispiele mit dem Programm GAP überprüft. Der GAP-Code kann Anhang A.2 entnommen werden. Weiters habe ich im Anhang A.2 den GAP-Code für die Konjugationswirkung der alternierenden Gruppe A_5 und S_4 hinzugefügt.

2.3 Anwendungen und Beispiele

Im ersten Teil dieses Abschnittes werde ich die gewonnenen Erkenntnisse über Gruppenwirkungen, insbesondere die Klassengleichungen des letzten Abschnittes in Anlehnung an Hungerford (vgl. [5] Abschnitt II.5) nutzen, um den Satz von Cauchy und weitere Sätze über Eigenschaften von p-Gruppen abzuleiten. Diese Resultate sind für sich von Bedeutung und dienen weiters der Vorbereitung auf den folgenden Abschnitt über die klassischen Sylow-Sätze. Der Satz von Cauchy besagt, dass in einer endlichen Gruppe G für jeden Primteiler p der Gruppenordnung ein Element von G mit Ordnung p existiert. Dieser Beweis ist von großem Interesse, da hier eine spezielle Gruppenwirkung konstruiert wird, deren Fixpunkte in bijektiver Korrespondenz zu den Elementen x von G stehen, die $x^p = 1$ erfüllen.

Im zweiten Teil dieses Abschnittes werden Gruppen in semidirekte Produkte "zerlegt" bzw. auf diese Art neue Gruppen konstruiert. Dies dient der Analyse der Struktur dieser Gruppen. Ein Schwerpunkt dieses Abschnittes liegt in der Erläuterung der Diedergruppe D_n. Verschiedene Interpretationen von D_n - geometrische, als Permutationsgruppe und als semidirektes Produkt der Gruppe der komplexen n-ten Einheitswurzeln mit der zweielementigen zyklischen Gruppe - liefern ein besseres Verständnis der Methode des semidirekten Produktes und den Bezug zu Gruppenwirkungen. Man wird sehen, dass eine Gruppenwirkung durch Automorphismen aus den beiden beteiligten Gruppen die neue Gruppe, das semidirekte Produkt, definiert. Die Frage, wann man Gruppen "zerlegen" oder zusammensetzen kann, führt letztlich zu dem Begriff der zerfallenden Erweiterung. Die Ideen für den zweiten Teil dieses Abschnittes beruhen auf Fischer (vgl. [3] Abschnitt I.§3) und Armstrong (vgl. [1] Kapitel 23).

Beginnen werde ich mit einem einfachen Lemma, das in der Folge mehr-

fach zur Anwendung kommen wird. Es seien, wie im letzten Abschnitt bei der allgemeinen Klassengleichung (2.2.2), X_0 die Vereinigung der Menge der einelementigen Bahnen, also die Menge der Fixpunkte der Wirkung, und P_i jene Bahnen, die aus mehr als einem Element bestehen. Im folgenden bezeichne p eine beliebige Primzahl.

Lemma 2.4. *Eine Gruppe mit Ordnung p^n wirke auf einer endlichen Menge X. Dann gilt*

$$|X| \equiv |X_0| \pmod{p}$$

Beweis. Nach (2.2.2) gilt $|X| = |X_0| + \sum |P_i|$ und laut Bahn-Stabilisator-Satz (Satz 2.1) teilt jede Bahnlänge die Gruppenordnung $|G|$. Laut Voraussetzung ist $|G| = p^n \equiv 0 \pmod{p}$ und daher auch $|P_i| \equiv 0 \pmod{p}$. Es folgt $|X| \equiv |X_0| \pmod{p} + \sum 0 \pmod{p}$ und somit die Aussage des Satzes. □

Eine Gruppe G heiße *p-Gruppe*, falls die Ordnung $\mathrm{ord}(g)$ eines jeden Elements g von G (endlich und) eine Potenz von p ist. Der nun folgende Satz von Cauchy impliziert dann, dass eine endliche Gruppe G genau dann eine p-Gruppe ist, wenn ihre Ordnung $|G|$ eine Potenz von p ist.

Satz 2.5. *Sei F eine endliche Gruppe deren Ordnung $|F|$ von p geteilt wird; dann besitzt F ein Element der Ordnung p.*

Beweis. Man konstruiere eine spezielle Gruppenwirkung, deren Fixpunkte in bijektiver Korrespondenz zu der Menge aller Elemente von G mit Ordnung 1 oder p stehen. Indem man zeigt, dass die Mächtigkeit von X_0 größer 1 ist, hat man die Existenz eines Elements mit Ordnung p also die Aussage des Satzes bewiesen.

Es sei $X = \{(g_1, \ldots, g_p) \in F^p = F \times \cdots \times F \mid g_1 \cdots g_p = 1\}$ die Menge der geordneten p-Tupel von Elementen der Gruppe F, bei denen die Multiplikation der entsprechenden Gruppenelemente das Einselement ergibt. Man lasse

die zyklische Gruppe $G := (\mathbb{Z}_p, +)$ auf X vermöge zyklischer Vertauschung wirken: $\mathbb{Z}_p \times X \to X$, $(\overline{k}, (g_1, \ldots, g_p)) \mapsto \overline{k} \cdot (g_1, \ldots, g_p)$, mit

$$\overline{k} \cdot (g_1, \ldots, g_p) = (g_{1+k}, g_{2+k}, \ldots, g_p, g_1, \ldots, g_k).$$

Das heißt, jede Komponente des p-Tupels wird bei der zyklischen Vertauschung mit $\overline{1}$ durch die nächstfolgende und die letzte durch die erste Komponente des Tupels ersetzt. Der Faktor $\overline{k} \in \mathbb{Z}_p$ bedeutet, dass diese Ersetzung k-mal angewendet wird. Die Fixpunktmenge X_0 unter dieser Wirkung enthält dann genau jene p-Tupel, die von allen $\overline{k} \in \mathbb{Z}_p$ fixiert werden, das heißt für welche $\overline{k} \cdot (g_1, g_2, \cdots, g_p) = (g_1, g_2, \cdots, g_p)$ für alle $\overline{k} \in \mathbb{Z}_p$ gilt. Das bedeutet, dass sich bei diesen Tupeln durch keine zyklische Vertauschung etwas ändert. Das sind somit genau jene Tupel, bei denen $g_1 = g_2 = \cdots = g_p$ gilt, die also die Form $(g, \ldots g)$ haben und deren Eintragungen g daher $g^p = 1$ erfüllen müssen. Falls $g \neq 1$, muss g die Ordnung p haben. Indem im Folgenden bewiesen wird, dass $|X_0| > 1$ gilt, hat man die Behauptung des Satzes nachgewiesen. Dies erfolgt in mehreren Schritten. Es wird gezeigt, dass (i) die Kardinalität der Menge X, auf der die Gruppe $\mathbb{Z}_p$ wirkt, durch p geteilt wird; (ii) die soeben definierte Abbildung $\mathbb{Z}_p \times X \to X$ per zyklischer Vertauschung wohldefiniert und tatsächlich eine Gruppenwirkung ist; (iii) die Ordnung der Menge $|X_0| > 1$ ist. (i): Die Komponenten g_i der p-Tupel $(g_1, \ldots, g_p)$ der Menge X sind Elemente aus F. Es kann zu jedem $(p-1)$-Tupel $(g_1, \ldots, g_{p-1})$ von Elementen $g_i \in F$ *genau ein* Element $g_p \in F$ gewählt werden, sodass $g_1 \cdots g_{p-1} g_p = 1$ gilt, nämlich $g_p = (g_1 \cdots g_{p-1})^{-1} = (g_{p-1})^{-1} \cdots g_1^{-1}$. Daraus folgt, dass $|X| = |F|^p$ und daher p ein Teiler von $|X|$ ist. (ii): Es muss gezeigt werden, dass für ein beliebiges p-Tupel $(g_1, \ldots, g_p)$ aus X das Bild $(g_{1+k}, g_{2+k}, \ldots, g_p, g_1, \ldots, g_k) = \overline{k} \cdot (g_1, \ldots, g_p)$ unter der Wirkung wieder Ele-

ment in X ist. Dies folgt aus

$$\begin{aligned}(g_{1+k}g_{2+k}\cdots g_p)(g_1\cdots g_k) = \\ &= \underbrace{\big((g_1\cdots g_k)^{-1}(g_1\cdots g_k)\big)}_{=1,\text{ da die Elemente invers sind}} g_{1+k}g_{2+k}\cdots g_p)(g_1\cdots g_k) = \\ &= (g_1\cdots g_k)^{-1}\underbrace{\big((g_1\cdots g_k)(g_{1+k}g_{2+k}\cdots g_p)\big)}_{=1\text{ weil }x\in X}(g_1\cdots g_k) = \\ &= (g_1\cdots g_k)^{-1}(g_1\cdots g_k) = 1\end{aligned}$$

Damit ist die Wohldefiniertheit der gegebenen Abbildung überprüft.
Es gilt klarerweise $\overline{0}\cdot(g_1,\ldots,g_p) = (g_1,\ldots,g_p)$ für alle $(g_1,\ldots,g_p)\in X$ (wobei $\overline{0}$ wie üblich das neutrale Element der zyklischen Gruppe $\mathbb{Z}_p$ ist) und

$$\begin{aligned}\overline{k_1}\cdot(\overline{k_2}\cdot(g_1,\ldots,g_p)) &= \overline{k_1}\cdot(g_{1+k_2},g_{2+k_2},\ldots,g_p,g_1,\ldots,g_{k_2}) = \\ &= (g_{1+k_1+k_2},g_{2+k_1+k_2},\ldots,g_p,g_1,\ldots,g_{k_1+k_2}) = \\ &= \overline{k_1+k_2}\cdot(g_1,\ldots,g_p)\end{aligned}$$

für alle $\overline{k_1},\overline{k_2}\in\mathbb{Z}_p$ und alle $(g_1,\ldots,g_p)\in X$. Alle Voraussetzungen für eine Gruppenwirkung sind demnach erfüllt.

(iii): Zu beweisen ist noch, dass $|X_0|$ die Ordnung der Fixpunktmenge größer 1 ist. Wie erwähnt haben die Elemente von X_0 die Form $(g,\ldots,g)$. Die Menge X_0 ist nicht leer, da $(1,1,\ldots,1)\in X_0$. Es gilt also $|X_0|\geq 1$. Aber $|X_0|$ ist nicht nur größer gleich sondern echt größer als 1. Dies folgt aus Lemma 2.4, denn erstens ist die Ordnung von $G=\mathbb{Z}_p$ gleich p und X endlich (es sind also die Voraussetzungen des Lemmas erfüllt) und zweitens ist die Kardinalität von X durch p teilbar, wie in (i) gezeigt wurde. Insgesamt ist also die Kardinalität von X_0 durch p teilbar und nachdem 1 nicht durch p teilbar ist, muss $|X_0|>1$ sein. □

Dieser Beweis ist ein schönes Beispiel für eine Anwendung einer Gruppenwirkung. Nachdem gezeigt wurde, dass es sich tatsächlich um eine Gruppen-

wirkung handelt, musste nur noch abgeleitet werden, dass $|X|$ durch p teilbar ist, um dann mit Lemma 2.4 auf die Behauptung des Satzes zu schließen. Der Trick dieses Beweises liegt allein in der Idee dieser speziellen Gruppenwirkung. Dieser Satz wird von vielen Autoren kompliziert mit Hilfe der Sylow-Sätze bewiesen.

Daraus folgt, wie schon angekündigt

Lemma 2.6. *Eine endliche Gruppe G ist genau dann eine p-Gruppe, wenn ihre Ordnung $|G|$ eine Potenz von p ist.*

Beweis. Sei G eine p-Gruppe und q eine Primzahl, die die Gruppenordnung $|G|$ teilt. Laut Satz von Cauchy besitzt dann G ein Element mit Ordnung q. Da G eine p-Gruppe ist, muss per definitionem aber jedes Element eine Potenz von p sein. Dies ist nur erfüllt, wenn $p = q$ gilt. Damit ist die Ordnung von G eine Potenz von p. Ist umgekehrt die Ordnung von G eine Potenz von p und $x \in G$, dann ist nach dem Satz von Lagrange die Ordnung von $\langle x \rangle$ ebenfalls eine Potenz von p, also ist die Ordnung von x eine Potenz von p. □

Mit Lemma 2.4 vom Beginn dieses Abschnittes kann man auch nachstehendes Resultat ableiten.

Satz 2.7. *Das Zentrum $Z(G)$ jeder endlichen p-Gruppe G ist nichttrivial (das heißt es besitzt außer dem 1-Element noch andere Elemente).*

Beweis. Eine p-Gruppe G wirke auf sich durch Konjugation. Da das Zentrum $Z(G)$ von G zumindest das Einselement enthält, ist die Ordnung $|Z(G)| \geq 1$. Die Aussage des Lemmas 2.4 wird unter dem Spezialfall der Konjugationswirkung zu $|G| \equiv |Z| \pmod{p}$. Da die Ordnung von G laut Voraussetzung durch p teilbar ist, ist auch die Ordnung des Zentrums durch p teilbar. Da 1 nicht durch p teilbar ist, folgt die Behauptung des Satzes, dass $|Z(G)| > 1$ ist. □

Bekanntlich ist jede Gruppe mit Ordnung p zyklisch und daher abelsch; nun kann man sofort ableiten, dass jede Gruppe mit Ordnung p^2 abelsch ist.

Korollar 2.8. *Jede Gruppe der Ordnung p^2 ist abelsch.*

Beweis. Sei G eine Gruppe mit Ordnung p^2. Da das Zentrum $Z := Z(G)$ Untergruppe von G ist, kann nach dem Satz von Lagrange $|Z|$ die Werte 1, p oder p^2 annehmen. Laut Satz 2.7 ist $|Z| \neq 1$, der erste Wert kann also ausgeschlossen werden. Ist $Z = G = p^2$, dann ist G abelsch.
Bleibt noch der Fall, dass Z genau p Elemente hat, das heißt $Z \neq G$. Die Faktorgruppe G/Z hätte laut Lagrange dann ebenfalls p Elemente, wäre also zyklisch der Ordnung p. Es wird sich zeigen, dass auch dieser Fall ausgeschlossen werden kann, da G/Z zyklisch die Gleichheit von Z und G impliziert, was der Voraussetzung dieses Falls widerspricht. Sei nämlich xZ ein erzeugendes Element von G/Z; dann ist

$$G/Z = \{Z, xZ, x^2Z, \ldots, x^{p-1}Z\}$$

und daher

$$G = Z \cup xZ \cup x^2Z \cup \cdots \cup x^{p-1}Z. \tag{2.3.1}$$

Ist weiters z ein erzeugendes Element von Z, dann ist $Z = \{1, z, z^2, \ldots, z^{p-1}\}$. Aus Gleichung (2.3.1) folgt daher, dass sich jedes Element von G in der Form $x^i z^j$ für geeignete $i, j \in \{0, \ldots, p-1\}$ darstellen lässt. Seien etwa a, b beliebige Elemente aus G, die zu den Nebenklassen x^kZ und x^iZ gehören, dann gilt $a = x^k z^j$ und $b = x^i z^l$ und daher

$$\begin{aligned} ab &= x^k z^j x^i z^l \\ &= x^{k+i} z^{j+l} \\ &= x^i z^l x^k z^j \\ &= ba \end{aligned}$$

Zwei derartige Elemente müssen also kommutieren, weil z mit jedem Element kommutiert. Damit wäre aber G kommutativ, ein Widerspruch zur Annahme $Z(G) \neq G$. Somit ist der Fall $Z = p$ ausgeschlossen und es bleibt nur der Fall $Z = G = p^2$, woraus die Kommutativität von G folgt. □

Es folgt nun der zweite Teil dieses Abschnitts, über semidirekte Produkte, beginnend mit einer Definition. Die Gruppe G wirke auf X und diese Menge sei nun ebenfalls mit einer Gruppenstruktur ausgestattet; dann wirkt G auf X *durch Automorphismen* (von links), wenn für jedes $g \in G$, $g : X \to X$ ein Gruppenautomorphismus von X ist. Mit anderen Worten: das Bild des Homomorphismus $\phi : G \to S_X$, $g \mapsto \phi_g$, der die Wirkung von G auf X definiert, liegt in der Automorphismengruppe $\mathrm{Aut}(X)$. Die Elemente aus G permutieren also die Elemente aus X entsprechend dem zugehörigen Automorphismus. In diesem Fall ist es bequem, die Notation $g : x \mapsto {}^g x$ zu verwenden. Wirkt eine Gruppe G auf einer Gruppe H durch Automorphismen, dann bildet die Menge der geordneten Paare $H \times G$ mit der Operation

$$(h, g)(k, f) = (h{}^g k, gf)$$

eine Gruppe, das *semidirekte Produkt* $H \rtimes G$ von H mit G (bezüglich der gegebenen Wirkung von G auf H). Bei diesem Produkt setzt sich die erste Koordinate folgendermaßen zusammen: es wird auf die erste Koordinate des zweiten Faktors k der Automorphismus $\phi_g : k \mapsto {}^g k$ angewandt, der durch die zweite Koordinate des ersten Faktors definiert wird. Das Resultat davon wird dann von links mit der ersten Koordinate h des ersten Faktors multipliziert. Das Einselement dieser Gruppe $H \rtimes G$ ist $(1_H, 1_G)$, für die Inversenbildung gilt

$$(h, g)^{-1} = ({}^{g^{-1}}h^{-1}, g^{-1}).$$

Die Assoziativität folgt aus

$$\begin{aligned}
\big((h,g)(h',g')\big)(h'',g'') &= (h{}^{g}h', gg')(h'',g'') \\
&= (h{}^{g}h'{}^{gg'}h'', gg'g'') \\
&= (h{}^{g}h'{}^{g}({}^{g'}h''), gg'g'') \\
&\qquad \text{da } \phi_g \text{ ein Automorphismus ist, gilt } {}^{g}h_1{}^{g}h_2 = {}^{g}(h_1h_2) \\
&= (h{}^{g}({}^{g'}h'{}^{g'}h''), gg'g'') \\
&= (h,g)({}^{g'}h'{}^{g'}h'', g'g'') \\
&= (h,g)\big((h',g')(h'',g'')\big).
\end{aligned}$$

Somit wird aus beiden Gruppen H und G mit einem Homomorphismus ϕ von G in die Automorphismengruppe von H eine neue Gruppe $H \rtimes G$ konstruiert. In der üblichen Notation des semidirekten Produkts $H \rtimes G$, die rechts vom Produktzeichen $\rtimes$ die Gruppe G und links die Gruppe H schreibt, auf die die Gruppe G durch Automorphismen wirkt, wird ausgedrückt in welche Richtung der Homomorphismus geht. Wichtig ist, die Reihenfolge $H \rtimes G$ festzuhalten, denn im Allgemeinen ist $H \rtimes G$ eine ganz andere Gruppe als $G \rtimes H$. Ich werde später zeigen, dass nur einer, nämlich der linke Faktor H von $H \rtimes G$, immer einen Normalteiler im semidirekten Produkt bildet. Es sei noch erwähnt, dass in der Literatur auch das umgekehrte Produktzeichen $\ltimes$ zu finden ist, das andeutet, dass der rechte Faktor ein Normalteiler im semidirekten Produkt ist, und die linke Gruppe auf der rechten durch Automorphismen von rechts wirkt. Siehe dazu Beispiel (5).

Im Folgenden wird zur Charakterisierung des semidirekten Produkts die Projektion $\pi\colon H \rtimes G \to G$, $(h,g) \mapsto g$ vom semidirekten Produkt auf die zweite Komponente des kartesischen Produkts verwendet. Aus der Definition der Verknüpfung im semidirekten Produkt sieht man unmittelbar, dass diese Abbildung ein Homomorphismus ist. Es ist wichtig zu beachten, dass nur die

Projektion auf die zweite Komponente nicht aber die Projektion auf die erste Komponente ein Homomorphismus ist.

Des weiteren wird die sogenannte kanonische Injektion $H \to H \rtimes G$, $h \mapsto (h, 1_G)$, auch "Einbettung" genannte Abbildung verwendet, die ebenfalls einen Homomorphismus darstellt. Der Kern dieses Homomorphismus ist klarerweise $\{1_H\}$ und das Bild ist $H \times \{1_G\}$. Analoges gilt für die Einbettung $G \to H \rtimes G$, $g \mapsto (1_H, g)$.

Das folgende Lemma charakterisiert nun das semidirekte Produkt. Vorausgesetzt sind die beiden Gruppen H und G, sowie ein beliebiger Homomorphismus von G in die Automorphismengruppe von H und die damit definierte Gruppe des sogenannten äusseren semidirekten Produktes $F = H \rtimes G$.

Lemma 2.9. *Für die Gruppe $F = H \rtimes G$ gilt*

1. $H \trianglelefteq F$
2. $G \leq F$
3. $H \cap G = \{1_F\}$
4. $F = HG$,

wobei jeweils H mit $H \times \{1_G\}$ und G mit $\{1_H\} \times G$ identifiziert wird.

Beweis. 1. Die Menge $H \times \{1_G\} = \{(h, 1_G) \mid h \in H\}$ ist eine Untergruppe von F, die via $h \mapsto (h, 1_G)$ zu H isomorph ist. Sie bildet einen Normalteiler in $H \rtimes G$, denn die Projektionsabbildung $\pi : H \times G \to G$, $(h, g) \mapsto g$ auf die zweite Komponente ist, wie erwähnt, ein Homomorphismus von $H \rtimes G$ nach G, dessen Kern genau $H \times \{1_G\}$ ist.

2. Analoge Überlegungen zur kanonischen Injektion $G \to \{1_H\} \times G$, $g \mapsto (1_H, g)$ zeigen, dass die Menge $\{1_H\} \times G$ eine Untergruppe von F isomorph zu G ist.

3. Es ist klar, dass für $h \in H$ und $g \in G$, $(h, 1_G) = (1_H, g)$ ausschließlich für $h = 1_H$ und $g = 1_G$ gelten kann, also $(H \times \{1_G\}) \cap (\{1_H\} \times G) = \{(1_H, 1_G)\}$ gilt.

4. Für beliebige $h \in H$ und $g \in G$ gilt $(h, 1_G)(1_H, g) = (h^{1_G} 1_H, 1_G g) = (h, g)$, also $HG = (H \times \{1_G\})(\{1_H\} \times G) = F$. □

Umgekehrt kann unter bestimmten Voraussetzungen eine Gruppe als semidirektes Produkt dargestellt werden, die Gruppe kann sozusagen "zerlegt" werden. In diesem Fall wird eine spezielle natürliche Gruppenwirkung induziert - G wirkt auf H per Konjugation. Daher verwendet man die Bezeichnung inneres semidirektes Produkt. Der folgende Satz gibt Auskunft darüber, unter welchen Voraussetzungen dies möglich ist.

Satz 2.10. *Gibt es in einer Gruppe F einen Normalteiler H und eine Untergruppe G mit $F = HG$ und $H \cap G = \{1\}$, dann ist F isomorph zum semidirekten Produkt $H \rtimes G$, wobei G auf H durch Konjugation wirkt.*

Beweis. Zunächst ist festzuhalten, dass jedes $f \in F$ eine *eindeutige* Darstellung als $f = hg$ mit $h \in H$ und $g \in G$ besitzt. Die Voraussetzung $F = HG$ besagt, dass für jedes $f \in F$ *mindestens* so eine Darstellung existiert. Angenommen für ein f gäbe es zwei solcher Darstellungen: $f = h_1 g_1 = h_2 g_2$. Dann würde $h_2^{-1} h_1$ klarerweise in H und $g_2 g_1^{-1}$ in G liegen, da beides Untergruppen von F sind. Aber $h_1 g_1 = h_2 g_2$ impliziert $h_2^{-1} h_1 = g_2 g_1^{-1}$, die folglich beide im Durchschnitt von H und G liegen müssten, der wie erwähnt gleich 1_F ist. Daher ist $h_1 = h_2$ und $g_1 = g_2$. Damit kann eine Abbildung $\Psi : F \to H \times G$ durch $f = hg \mapsto (h, g)$ definiert werden, die nach obiger Überlegung (wohldefiniert und) bijektiv ist.

Da H ein Normalteiler von F ist, ist H eine invariante Menge unter der Konjugationswirkung von F (F wirkt also nicht nur auf sich selbst sondern

auch auf H durch Konjugation). Diese Wirkung können wir auf die Untergruppe G einschränken. Damit wirkt G auf H durch Konjugation (in F!). Jede solche Konjugationsabbildung $h \mapsto ghg^{-1}$ ist ein Automorphismus von H. Das semidirekte Produkt $H \rtimes G$ sei nun bezüglich dieser Wirkung definiert.

Oben wurde schon eine Bijektion $\Psi : F \to H \rtimes G$ definiert; es muss noch überprüft werden, dass Ψ tatsächlich ein Homomorphismus (und damit ein Isomorphismus) ist. Dazu seien $f_1, f_2 \in F$, wobei $f_1 = h_1 g_1$ mit $h_1 \in H$ und $g_1 \in G$ und $f_2 = h_2 g_2$ mit $h_2 \in H$ und $g_2 \in G$. Dann gilt

$$\begin{aligned}
\Psi(f_1 f_2) &= \Psi(h_1 g_1 h_2 g_2) \\
&= \Psi(h_1 g_1 h_2 (g_1^{-1} g_1) g_2) \\
&= \Psi(h_1 (g_1 h_2 g_1^{-1}) g_1 g_2) \\
&= (h_1 (g_1 h_2 g_1^{-1}), g_1 g_2) \\
&= (h_1{}^{g_1} h_2, g_1 g_2) \\
&= (h_1, g_1)(h_2, g_2) \\
&= \Psi(h_1 g_1)\Psi(h_2 g_2) \\
&= \Psi(f_1)\Psi(f_2).
\end{aligned}$$

□

Die Struktur eines semidirekten Produktes $H \rtimes G$ ist wesentlich abhängig von der Struktur der einzelnen beteiligten Gruppen und vor allem von der Wirkung der einen Gruppe auf der anderen. Dies soll an ein paar elementaren Beispielen illustriert werden.

Beispiele. (1) Das semidirekte Produkt ist genau dann ein direktes Produkt, wenn die Wirkung trivial ist. Wählt man die triviale Wirkung, also den Homomorphismus $\Phi : H \to \mathrm{Aut}(N)$, $h \mapsto \mathrm{id}_N$, dann ist die Verknüpfung im

semidirekten Produkt

$$(n,h)(n',h') = (n{}^h n', hh') = (nn', hh').$$

Damit ist das semidirekte Produkt $N \rtimes H$ bezüglich dieser trivialen Gruppenwirkung gleich dem direkten Produkt $N \times H$. Im umgekehrten Fall sei $N \times H$ das direkte Produkt von N mit H, dann ist auch H Normalteiler, das heißt $\{1_N\} \rtimes H \trianglelefteq N \rtimes H$ und es gilt $(n,1)(1,h)(n,1)^{-1} = (1,h)$. Laut Verknüpfungsregel im semidirekten Produkt ist aber

$$(n,1)(1,h)(n,1)^{-1} = (n,h)(n^{-1},1) = (n\ {}^h n^{-1}, h)$$

Daraus folgt, dass $n\ {}^h n^{-1} = 1$, bzw. $n = {}^h n$, das heißt, die Wirkung ist trivial.

Man sieht: Jedes direkte Produkt $N \times H$ ist auch ein semidirektes. Das semidirekte Produkt ist also eine Verallgemeinerung des direkten. Bis auf Isomorphien ist es das einzige semidirekte Produkt, in dem beide beteiligten Gruppen $N \times \{1_H\}$ und $\{1_N\} \times H$ Normalteiler sind. Ansonsten gilt beim semidirekten die schwächere Voraussetzung, dass nur eine Untergruppe ein Normalteiler ist.

Seien beispielsweise $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ und $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ zwei zyklische Gruppen. Welche semidirekten Produkte $\mathbb{Z}_2 \rtimes \mathbb{Z}_3$ und $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$ können mit diesen Komponenten gebildet werden? Im ersten Fall $\mathbb{Z}_2 \rtimes \mathbb{Z}_3$ gibt es nur das direkte Produkt $\mathbb{Z}_2 \times \mathbb{Z}_3$, da $\mathrm{Aut}(\mathbb{Z}_2)$ nur aus der identischen Abbildung besteht und daher nur ein Homomorphismus $\mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2)$ existiert, nämlich der triviale.

Im Anhang findet sich unter A.3 zu diesem Beispiel der GAP-Code, mit dem ich das Ergebnis nachvollzogen habe.

(2) Andrerseits gibt es zwei verschiedene semidirekte Produkte der Form $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$, eine abelsche und eine nicht abelsche Gruppe. Die Automorphismengruppe der Restklassengruppe $\mathbb{Z}_3$ besteht aus zwei Elementen. Dementsprechend kann man zwei Fälle unterscheiden. Im ersten Fall wählt man den

trivialen Automorphismus, der analog zu Beispiel (1) in der trivialen Wirkung und damit im direkten Produkt $\mathbb{Z}_3 \times \mathbb{Z}_2$ resultiert, das isomorph zur zyklischen Gruppe $\mathbb{Z}_6$ ist. Im zweiten Fall kommt der einzige nicht-triviale Automorphismus von $\mathbb{Z}_3$ ins Spiel: $\mathbb{Z}_3$ hat die beiden Automorphismen $\mathrm{id} : x \mapsto x$ und $- : x \mapsto -x$. In diesem Fall ist es zweckmäßig, die additive Gruppe $\mathbb{Z}_3$ durch die Restklassen $\{\overline{-1}, \overline{0}, \overline{1}\}$ zu beschreiben, $\mathbb{Z}_2$ mit der multiplikativen Gruppe $\{\overline{1}, \overline{-1}\}$ zu identifizieren (dies ist genau die Einheitengruppe von $\mathbb{Z}_3$) und die Wirkung von $\{\overline{-1}, \overline{1}\}$ auf $\mathbb{Z}_3$ durch ${}^{x}y := xy$ darzustellen. Auf der Menge $\{\overline{-1}, \overline{0}, \overline{1}\} \times \{\overline{-1}, \overline{1}\}$ erhält man durch die Definition:

$$(x_1, y_1)(x_2, y_2) := (x_1 + y_1 x_2, y_1 y_2)$$

die Gruppenstruktur von $\mathbb{Z}_3 \rtimes C_2$. Diese Gruppe ist, wie wir noch sehen werden, zur Diedergruppe D_3 und ebenso zur Permutationsgruppe S_3 isomorph.

Im Anhang findet sich dazu unter A.3 der GAP-Code, mit dem dieses Ergebnis nachvollzogen werden kann.

(3) Die *Diedergruppe* D_n ist ein Beispiel einer nicht abelschen Gruppe, die in ein semidirektes Produkt von zwei abelschen Gruppen "zerlegt" werden kann. Dies ist die Gruppe aller Symmetrien eines regelmäßigen n-Ecks in der Euklidischen Ebene. Es werden regelmäßige Polygone unter der Annahme, dass der Mittelpunkt im 0-Punkt der Ebene und die Ecke 1 im Punkt $(1, 0)$ auf der x-Achse liegt, betrachtet. Durch die Elemente der Diedergruppe werden die Ecken des n-Ecks wieder in Ecken übergeführt, sodass benachbarte Ecken benachbart bleiben und der Nullpunkt festgehalten wird. Die Polygone werden demnach durch die Symmetrien aus D_n deckungsgleich in sich abgebildet. Die Diedergruppe wird von zwei Symmetrien erzeugt, z.B. von der Drehung δ um den Winkel $2\pi/n$ und der Spiegelung σ um die x-Achse. Der Zusammenhang wird anhand der Diedergruppen D_4 oder D_7 in Abbildung 2.2 und Abbildung 2.3 veranschaulicht. Die Drehung δ erzeugt eine zyklische Gruppe der Ord-

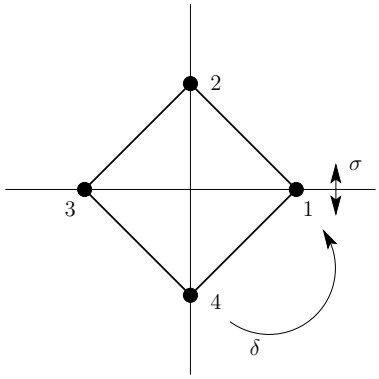

Abbildung 2.2: Diedergruppe D_4 als Symmetriegruppe des Quadrats

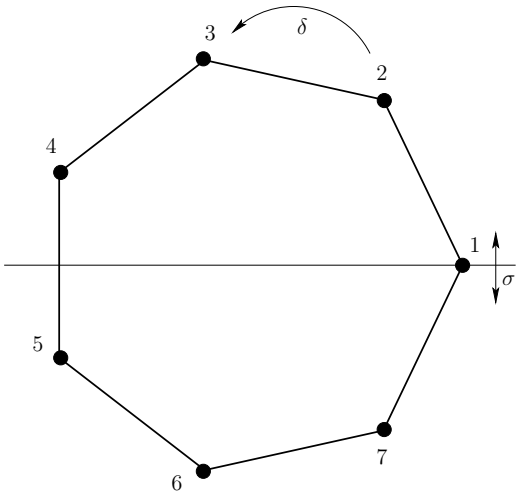

Abbildung 2.3: Diedergruppe D_7 als Symmetriegruppe des Sieben-Ecks

nung n und es gilt $(\delta^k)^{-1} = \delta^{k-n}$. Die Spieglung σ hat indessen Ordnung 2 und es gilt $\sigma^{-1} = \sigma$. Man erhält somit $C_n = \langle\delta\rangle = \{1, \delta, \delta^2, \ldots, \delta^{n-1}\}$ und $C_2 = \langle\sigma\rangle = \{1, \sigma\}$ (wobei C_i die zyklische Gruppe mit Ordnung i bezeichnet).

Ein n-Eck lässt n Spiegelungen an n Spiegelachsen zu. Folgende Spiegelachsen sind möglich: falls n ungerade ist, geht durch jede Ecke und durch die Mitte der gegenüberliegenden Kante genau ein Spiegelungsachse und dies sind alle Spiegelungsachsen. Falls n gerade ist, gibt es durch je zwei gegenüberliegende Ecken eine Spiegelungsachse und durch die Mitte von zwei gegenüberliegenden Kanten eine Spiegelungsachse — dies sind wiederum alle Spiegelungsachsen. Dies wird an den Achsen des Sieben-Ecks und des Quadrats ersichtlich (siehe Abbildung 2.4 und Abbildung 2.5). Insgesamt ergeben sich $2n$ Symmetrie-Operationen - n Drehungen und n Spiegelungen. Die Diedergruppe D_n hat somit Ordnung $2n$.

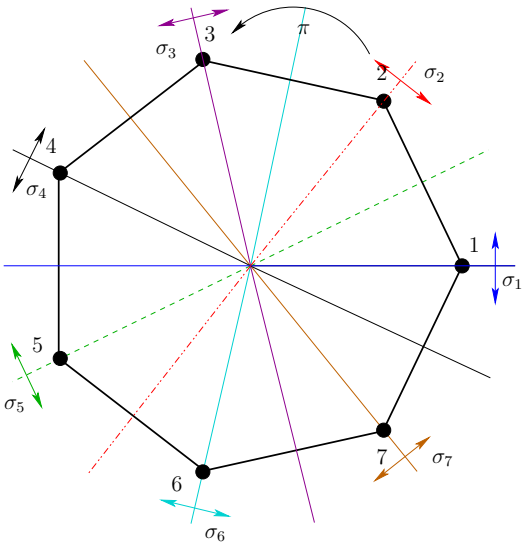

Abbildung 2.4: Spiegelachsen des Sieben-Ecks

Ich werde im Folgenden zeigen, dass die Diedergruppe D_n isomorph ist zum inneren semidirekten Produkt $\langle\delta\rangle \rtimes \langle\sigma\rangle$. Dies erfolgt mittels des Satzes

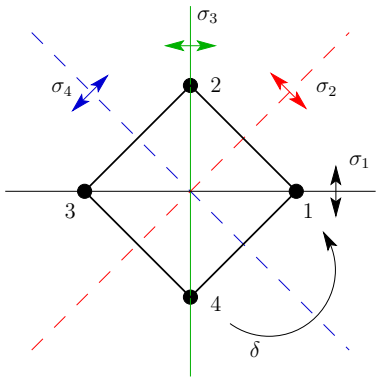

Abbildung 2.5: Spiegelachsen des Quadrats

2.10. Die zyklische Gruppe der Drehungen $\langle\delta\rangle$ ist normal in der Diedergruppe, denn die Drehungen $\langle\delta\rangle$ in D_n sind genau die Symmetrien, die die Orientierung erhalten und daher ist jede Konjugierte einer Drehung wieder eine Drehung und somit ist $\langle\delta\rangle \trianglelefteq D_n$. Klarerweise ist $\langle\sigma\rangle$ eine Untergruppe von D_n und es gilt $\langle\delta\rangle \cap \langle\sigma\rangle = \{1\}$. Da die Nebenklasse $\langle\delta\rangle\sigma$, aus n verschiedenen Elementen besteht, und jedes dieser Elemente die Orientierung des n-Ecks ändert, besteht $\langle\delta\rangle\langle\sigma\rangle = \langle\delta\rangle \cup \langle\delta\rangle\sigma$ aus allen $2n$ Elementen von D_n, daher gilt $D_n = \langle\delta\rangle\langle\sigma\rangle$. Daraus folgt die Isomorphie der Diedergruppe mit dem inneren semidirekten Produkt $\langle\delta\rangle \rtimes \langle\sigma\rangle$. Es wirkt die Spiegelungsgruppe $\langle\sigma\rangle = \{1, \sigma\}$ auf der Drehgruppe $\langle\delta\rangle = \{1, \delta, \delta^2, \cdot, \delta^{n-1}\}$ durch Konjugation. Einfache geometrische Überlegungen ergeben, dass $\sigma\delta^k\sigma^{-1} = (\delta^k)^{-1} = \delta^{n-k}$, das heißt die Spiegelung ordnet jeder Drehung die inverse Drehung zu. Die Inversion ist, wie gezeigt, auf der zyklischen, und daher abelschen Gruppe der Drehungen ein Automorphismus.

Mit dem erklärten Homomorphismus

$$\phi : \langle\sigma\rangle \to \mathrm{Aut}(\langle\delta\rangle), \sigma : \delta^k \mapsto {}^{\sigma}\delta^k = \sigma\delta^k\sigma^{-1} = (\delta^k)^{-1} = \delta^{k-n}$$

erhält man die Gruppenstruktur der Diedergruppe und es ergeben sich die für

die Struktur definierenden Relationen $\delta^n = \sigma^2 = (\delta\sigma)^2 = id$. Man kann die Elemente der Diedergruppe auch explizit angeben und erhält

$$D_n = \{id, \delta, \delta^2, \cdots, \delta^{n-1}, \sigma, \delta\sigma, \delta^2\sigma, \cdots, \delta^{n-1}\sigma\}$$

Mit Hilfe der Interpretation der Ecken des regelmäßigen n-Ecks als multiplikative Gruppe der komplexen n-ten Einheitswurzeln kann noch eine andere Interpretation dieser Gruppe gegeben werden. Die Ebene, in der das n-Eck liegt, wird mit der komplexen Zahlenebene identifiziert und als Ecken der n-Ecke werden die n-ten Einheitswurzeln angenommen, also $x = e^{\frac{2\pi ki}{n}}$ mit $k = 0, 1, \cdots, n-1$. Die Drehung definiert man als $\delta(x) = e^{\frac{2\pi ki}{n}}x$ und die Spiegelung an der reellen Achse $\sigma(x) = x^{-1} = \overline{x}$. Das Konjugierte einer Drehung ist die inverse Drehung

$$\begin{aligned}
\sigma\delta^k\sigma^{-1}(x) &= \sigma\delta^k(x^{-1}) \\
&= \sigma(\delta^k(x^{-1})) \\
&= (\delta^k(x^{-1}))^{-1} \\
&= (e^{\frac{2\pi ki}{n}}x^{-1})^{-1} \\
&= (e^{\frac{2\pi ki}{n}})^{-1}x \\
&= (\delta^k)^{-1}(x)
\end{aligned}$$

Insgesamt kann die Diedergruppe D_n daher auch als das semidirektes Produkt $\left\langle e^{\frac{2\pi i}{n}} \right\rangle \rtimes \langle\sigma\rangle$ angesehen werden, wobei σ die konjugiert-komplexe Konjugation bezeichnet.

Eine weitere Interpretation der Diedergruppe D_n ist die als Untergruppe von S_n. Um das geometrisch zu veranschaulichen, nummeriere man die Ecken der Polygone durch. Jede Symmetrie des n-Ecks aus D_n kann dann als eine Permutation aufgefasst werden. Die Drehung δ um $2\pi/n$ wird mit der zyklischen Permutation $\delta = (12\cdots n)$ identifiziert und die Spiegelung σ um die

x-Achse mit $\sigma = (1)(2\ n)(3\ n-1)(4\ n-2)\cdots$ (siehe dazu Abbildung 2.2 und Abbildung 2.3).

Im Anhang findet sich dazu unter A.3 der GAP-Code, mit dem ich die Ergebnisse für $D_7 \cong C_7 \rtimes C_2$ und für $D_5 \cong C_5 \rtimes C_2$ überprüft habe. Es gilt nur für $n = 3$, dass $D_n = C_n \rtimes C_2$ isomorph ist zur Permutationsgruppe S_n, im Allgemeinen gilt das nicht. Bemerkung: da die Untergruppe $\langle\sigma\rangle$ in D_n nicht normal ist, ist die Diedergruppe kein direktes Produkt.

(4) Sei E die Euklidische Ebene (oder allgemeiner ein Euklidischer Raum) mit der zugehörigen Metrik. Dann lässt sich die Gruppe aller *Isometrien* von E, i.e. aller Bijektionen von E, die die Abstände zwischen je zwei Punkten fix lassen, als semidirektes Produkt $E \rtimes O$ darstellen, wobei E (genauer: die abelsche Gruppe des Vektorraums E) mit der Gruppe aller *Translationen* von E identifiziert wird, O die Gruppe aller orthogonalen Transformationen von E bezeichnet und O auf E in natürlicher Weise auf E wirkt.

(5) Ein ähnliches Beispiel liefert der Stabilisator eines beliebigen Vektors $x \in K^n$, $x \neq o$ unter der Wirkung der allgemeinen linearen Gruppe $GL(n, K)$. Es wurde bereits darauf hingewiesen, dass $K^n \setminus \{o\}$ eine Bahn dieser Wirkung bildet und der Stabilisator des ersten Einheitsvektors e_1 aus allen invertierbaren Matrizen besteht, deren erste Spalte gleich e_1 ist. Mit anderen Worten: der Stabilisator besteht aus allen invertierbaren $n \times n$-Matrizen der Form

$$\begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix},$$

wobei a ein beliebiger Zeilenvektor mit $n-1$ Eintragungen in K, 0 der Nullvektor in K^{n-1} und A eine $(n-1) \times (n-1)$-Matrix über K ist. Wegen

$$\det \begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix} = \det A$$

muss A zusätzlich invertierbar sein. Sei K_{n-1} die Menge aller Zeilenvektoren

über K mit $n-1$ Eintragungen. Dann ist jedenfalls die Abbildung

$$\begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix} \mapsto (A, a) \tag{2.3.2}$$

eine Bijektion zwischen dem Stabilisator von e_1 und der Menge $GL(n-1, K) \times K_{n-1}$. Beachtet man weiters, dass nach den Regeln der Matrixmultiplikation die Gleichung

$$\begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & B \end{pmatrix} = \begin{pmatrix} 1 & b + aB \\ 0 & AB \end{pmatrix} \tag{2.3.3}$$

gilt, so haben wird abgeleitet, dass der Stabilisator von e_1 als semidirektes Produkt

$$GL(n-1, K) \ltimes K_{n-1}$$

dargestellt werden kann, worunter wir hier die Menge $GL(n-1, K) \times K_{n-1}$ mit der Verknüpfung

$$(A, a)(B, b) = (AB, aB + b)$$

verstehen wollen. Die Gleichung (2.3.3) sagt dann, dass die Bijektion (2.3.2) ein Gruppenisomorphismus ist.

(6) Die beiden vorhergehenden Beispiele, sowie das unter Punkt (2) betrachtete semidirekte Produkt $\mathbb{Z}_3 \rtimes C_2$ können als konkrete Beispiele eines allgemeinen Konstruktionsprinzip interpretiert werden: das sogenannte *Holomorph* einer Gruppe G. Als dieses bezeichnet man das semidirekte Produkt $G \rtimes \mathrm{Aut}(G)$ von G mit seiner Automorphismengruppe (und der natürlichen Wirkung von Aut(G) auf G).

Es wurde bereits geklärt (Satz 2.10), wie die Struktur einer Gruppe beschaffen ist, die als semidirektes Produkt von zwei Untergruppen dargestellt werden kann. Semidirekte Produkte sind Spezialfälle von sogenannten *Erweiterungen*, die wie folgt definiert sind.

Eine Gruppe F heißt eine *Erweiterung* einer Gruppe H durch eine Gruppe G, wenn F einen Normalteiler (isomorph zu) H besitzt, sodass deren Faktorgruppe F/H (isomorph zu) G ist. Es stellt sich die Frage, wie jene Erweiterungen charakterisiert werden können, die von semidirekten Produkten stammen. Innerhalb der Menge aller Erweiterungen einer Gruppe H durch eine Gruppe G gibt es die "zerfallenden" (splitting extensions). Das sind genau jene Erweiterungen F, für die es einen Homomorphismus $\iota : G \to F$ gibt, sodass für die kanonische Projektion $\pi : F \to G$ gilt: $\pi\iota = \mathrm{id}_G$. Die Abbildung ι ist also ein Rechtsinverses der kanonischen Projektion. Das nachstehende Lemma zeigt, dass es sich hier gerade um semidirekte Produkte handelt. Man hat damit ein Kriterium dafür gefunden, dass eine Erweiterung von einem semidirekten Produkt stammt.

Lemma 2.11. *Sei F eine Erweiterung der Gruppe H durch die Gruppe G; genau dann ist diese Erweiterung zerfallend, wenn F zu einem semidirekten Produkt $H \rtimes G$ isomorph ist.*

Beweis. Sei F eine zerfallende Erweiterung von H durch G; es ist zu zeigen, dass $F \cong H \rtimes G$. Es soll also von den Eigenschaften einer zerfallenden Erweiterung auf die Charakterisierung des semidirekten Produktes (siehe Satz 2.10) geschlossen werden. Zu beweisen ist also 1. $H \trianglelefteq F$, 2. $G \leq F$, 3. $H \cap G = \{1_F\}$ und 4. $F = HG$.

1. Laut Voraussetzung ist F Erweiterung und damit ist H Normalteiler von F.

2. Für eine zerfallende Erweiterung F von H durch G ist die Abbildung ι: $G \to F$ injektiv, weil aus $\iota(g_1) = \iota(g_2)$ für $g_1, g_2 \in G$ mit $\pi\iota = \mathrm{id}_G$ folgt, dass $g_1 = \pi\iota(g_1) = \mathrm{id}_G = \pi\iota(g_2) = g_2$ also $g_1 = g_2$ gelten muss. Mit der Injektivität von ι folgt, dass G isomorph ist zu dem Bild $\iota(G)$ von G. Da ι ein Homomorphismus ist, ist $\mathrm{Im}(\iota) = \iota(G)$ Untergruppe von F. Somit gilt $\iota(G) \cong G \leq F$.

3. Da F laut Voraussetzung Erweiterung ist, gilt $F/H \cong G$, das heißt, die Projektion $\pi : F \to G$ entspricht dem kanonischen Homomorphismus von F in die Faktorgruppe F/H. Nach dem Homomorphiesatz gilt $\mathrm{Ker}(\pi) = H$, also wird jedes Element aus H durch π auf das Einselement abgebildet; es gilt also $\pi\iota(g) = 1$, genau dann, wenn $\iota(g) \in H$. Solch ein Element g aus H kann nur 1 sein, weil sonst die Eigenschaft der zerfallenden Erweiterung $\pi\iota = \mathrm{id}_G$, das heißt $\pi\iota(g) = g$ nicht erfüllt wäre. Somit ist der Durchschnitt von G und H trivial.
4. Sei $f \in F$ beliebig und $g = \pi(f)$; dann ist $\iota(g)^{-1}f \in H$, denn

$$\pi(\iota(g)^{-1}f) = \pi\iota(g^{-1})\pi(f) = g^{-1}g = 1$$

und daher

$$f = \iota(g) \cdot \iota(g)^{-1}f \in \iota(G)H \cong GH = HG.$$

Insgesamt ist also F zu dem semidirekten Produkt $H \rtimes \iota(G)$ isomorph.

Sei umgekehrt $F = H \rtimes G$ ein semidirektes Produkt. Wir wissen schon, dass $H \cong H \times \{1_G\}$ ein Normalteiler in $H \rtimes G$ ist, der zugleich der Kern der kanonischen Projektion $\pi : H \rtimes G \to G$ von $H \rtimes G$ auf G ist. Weiters ist $\iota : G \to H \rtimes G$, $g \mapsto (1_H, g)$ offenbar ein Homomorphismus mit $\pi\iota = \mathrm{id}_G$. Damit ist $F = H \rtimes G$ eine zerfallende Erweiterung von H durch G. □

Ein Beispiel einer nicht zerfallenden Erweiterung ist die zyklische Gruppe $\mathbb{Z}_{p^2}$ für eine Primzahl p. Diese ist (nicht zerfallende) Erweiterung von $\mathbb{Z}_p$ durch $\mathbb{Z}_p$. Denn $\langle\overline{p}\rangle = \{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{(p-1)p}\}$ ist eine Untergruppe von $\mathbb{Z}_{p^2}$ isomorph zu $\mathbb{Z}_p$ (und klarerweise ein Normalteiler). Weiters ist $\mathbb{Z}_{p^2}/\langle\overline{p}\rangle$ eine Gruppe mit p Elementen, die notwendigerweise isomorph zu $\mathbb{Z}_p$ ist. Sei nun $\iota : \mathbb{Z}_{p^2}/\langle\overline{p}\rangle \to \mathbb{Z}_{p^2}$ ein beliebiger nichttrivialer Homomorphismus. Jedes Element $\overline{x} + \langle\overline{p}\rangle$ mit $\overline{x} \neq \overline{0}$ muss auf ein Element mit Ordnung p abgebildet werden, also gilt $\iota(\mathbb{Z}_{p^2}/\langle\overline{p}\rangle) \subseteq \langle\overline{p}\rangle$ (es gilt sogar $=$). Sei $\pi : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}/\langle\overline{p}\rangle$ die kanonische

Projektion. Da das Bild von ι im Kern von π enthalten ist, ist $\pi\iota$ konstant $\overline{0}$, der triviale Endomorphismus, also $\pi\iota \neq id_{\mathbb{Z}_{p^2}/\langle\overline{p}\rangle}$.

2.4 Sylow-Sätze

In diesem Abschnitt will ich die klassischen Sylow-Sätze beweisen. Sie geben Auskunft über die Existenz von Untergruppen von Primzahlpotenzordnung, sowie über deren Anzahl und Zusammenhang. In der Literatur gibt es verschiedene Beweise, teilweise mit kombinatorischen Überlegungen. Ich will, dem Konzept dieser Arbeit folgend, den Beweis mit Gruppenwirkungen aus Hungerford (vgl. [5] Abschnitt II.5) führen. Hierzu wird der Begriff des Normalisators benötigt, der gleich zu Beginn dieses Abschnittes mit Hilfe einer speziellen Gruppenwirkung erläutert wird.

Es wirke eine endliche Gruppe G auf der Menge 2^G der Teilmengen von G durch Konjugation: $G \times 2^G \to 2^G$, $(g, X) \mapsto gXg^{-1}$ mit $g \in G$ und $X \in 2^G$ der Potenzmenge von G. Die Bahn O_X einer Teilmenge X unter dieser Wirkung besteht aus

$$\{gXg^{-1} \mid g \in G\}$$

allen zu X konjugierten Teilmengen von G.

Eine Untergruppe X von G ist genau dann ein Normalteiler in G, wenn die zugehörige Bahn O_X nur die Untergruppe selbst enthält, wenn also $gXg^{-1} = X$ für alle $g \in G$ gilt. Die Menge

$$N_G(X) := \{g \in G \mid gXg^{-1} = X\}$$

heißt der *Normalisator von X in G* und ist genau der Stabilisator von X bezüglich dieser Wirkung. Es gilt

(a) auch umgekehrt $N_G(X) = \{g \in G \mid g^{-1}Xg = X\}$;

(b) für jede Menge X ist wie jeder Stabilisator der Normalisator $N_G(X) \leq G$ eine Untergruppe von G;

(c) ist X nicht nur Teilmenge sondern eine Untergruppe von G, dann folgt aus der Definition des Normalisators von X in G, dass $X \trianglelefteq N_G(X)$ Normalteiler im Normalisator von X in G ist. Entsprechend dem Begriff des Normalisators ist $N_G(X)$ die größte Untergruppe N von G, in welcher X eine normale Untergruppe ist (das heißt: ist N eine Untergruppe von G mit $X \trianglelefteq N$, dann ist $N \subseteq N_G(X)$);

(d) der Normalisator $N_G(X)$ einer Untergruppe X stimmt mit der Gruppe G genau dann überein, wenn $X \trianglelefteq G$ Normalteiler von G ist. Wie bereits erwähnt, enthält dann die Bahn O_X nur X selbst.

Im Folgenden sei p immer eine fix gewählte Primzahl. Um den ersten sogenannten Sylow-Satz zu beweisen, wird folgendes Lemma benötigt:

Lemma 2.12. *Sei G eine endliche Gruppe und H eine p-Untergruppe von G (das heißt eine Untergruppe, die eine p-Gruppe ist). Dann gilt:*

$$[G : H] \equiv [N_G(H) : H] \ (\mathrm{mod} p).$$

Beweis. Sei $X := \{gH \mid g \in G\}$ die Menge aller Linksnebenklassen von G nach H. Die p-Untergruppe H wirke auf X vermöge Linksmultiplikation h: $gH \mapsto hgH$. Dann gilt $|X| = [G : H]$ und $|X| \equiv |X_0| \ (\mathrm{mod} p)$ (Satz 2.4 gilt, da die p-Gruppe H auf der endlichen Menge X wirkt).
Es ist zu beweisen, dass $X_0 = N_G(H)/H$, dass also die einelementigen Bahnen gleich den Linksnebenklassen des Normalisators von H in G nach H sind. Daraus folgt $|X_0| = [N_G(H) : H]$ und damit die Aussage des Satzes. Die Menge X_0 unter dieser Wirkung ist

$$X_0 = \{gH \mid hgH = gH \ \forall h \in H\}$$

die Menge der Linksnebenklassen gH, auf die alle $h \in H$ die triviale Wirkung haben. Es wird sich zeigen, dass eine Nebenklasse gH genau dann in X_0 liegt,

wenn g im Normalisator von H in G liegt. Wegen

$$hgH = gH \Leftrightarrow g^{-1}hgH = H \Leftrightarrow g^{-1}hg \in H$$

gilt $gH \in X_0$ genau dann, wenn $g^{-1}hg \in H$ für alle $h \in H$, das heißt $g^{-1}Hg \subseteq H$, was äquivalent ist zu $g^{-1}Hg = H$ (weil H und $g^{-1}Hg$ gleich viele Elemente besitzen). Insgesamt ergibt sich aus der Definition des Normalisators $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$ also

$$gH \in X_0 \Leftrightarrow g^{-1} \in N_G(H) \Leftrightarrow g \in N_G(H),$$

das heißt

$$X_0 = \{gH \mid g \in N_G(H)\}.$$

Daraus folgt, dass $X_0 = N_G(H)/H$ die Menge der Linksnebenklassen von $N_G(H)$ nach H gilt, also $|X_0| = [N_G(H) : H]$, woraus die Behauptung folgt. □

Damit kann nun der erste Sylow-Satz bewiesen werden.

Satz 2.13. *Sei G eine endliche Gruppe mit Ordnung $|G| = p^n r$, wobei $(p, r) = 1$. Für jedes $i \in \{0, 1, \ldots, n\}$ gibt es eine Untergruppe H von G der Ordnung p^i; ist $i < n$, dann ist H normal in einer Untergruppe K mit Ordnung p^{i+1}.*

Beweis. Mit Induktion nach i.
Induktionsannahme: Sei $i = 0$, dann gibt es eine Untergruppe H (die triviale Untergruppe) mit Ordnung $|H| = p^0 = 1$. Als eine unmittelbare Konsequenz des Satzes von Cauchy (Satz 2.5) besitzt G ein Element g mit Ordnung p und daher eine zyklische Gruppe $K = \langle g \rangle$ mit Ordnung p. Die Untergruppe H ist (trivialer) Normalteiler von K.
Induktionsschritt: Sei $i \in \{1, \ldots, n-1\}$ und H eine Untergruppe von G der Ordnung p^i. Es ist zu zeigen, (i) es gibt eine Untergruppe $K \leq G$, in

welcher H Normalteiler ist und (ii) die Ordnung von K ist p^{i+1}. (i). Da H p-Untergruppe von G ist, gilt nach Lemma 2.12 $[G : H] \equiv [N_G(H) : H] \pmod{p}$; und da weiters $[G : H] = \frac{|G|}{|H|} = \frac{p^n r}{p} = p^{n-i} r$ durch p teilbar ist, ist also auch $[N_G(H) : H] = |N_G(H)/H|$ durch p teilbar. Daraus folgt, dass $N_G(H)/H$ nach dem Satz von Cauchy (Satz 2.5) eine Untergruppe U der Ordnung p hat. Nach dem Homomorphiesatz ist für den kanonischen Homomorphismus $\pi : N_G(H) \to N_G(H)/H$ die Menge $K := \pi^{-1}(U)$ eine Untergruppe von $N_G(H)$, die H enthält und selber in $N_G(H)$ enthalten ist (K ist trivialerweise auch eine Untergruppe von G). (Siehe dazu Abbildung 2.6.) Da H Normalteiler in $N_G(H)$ ist, ist H umsomehr Normalteiler in K.

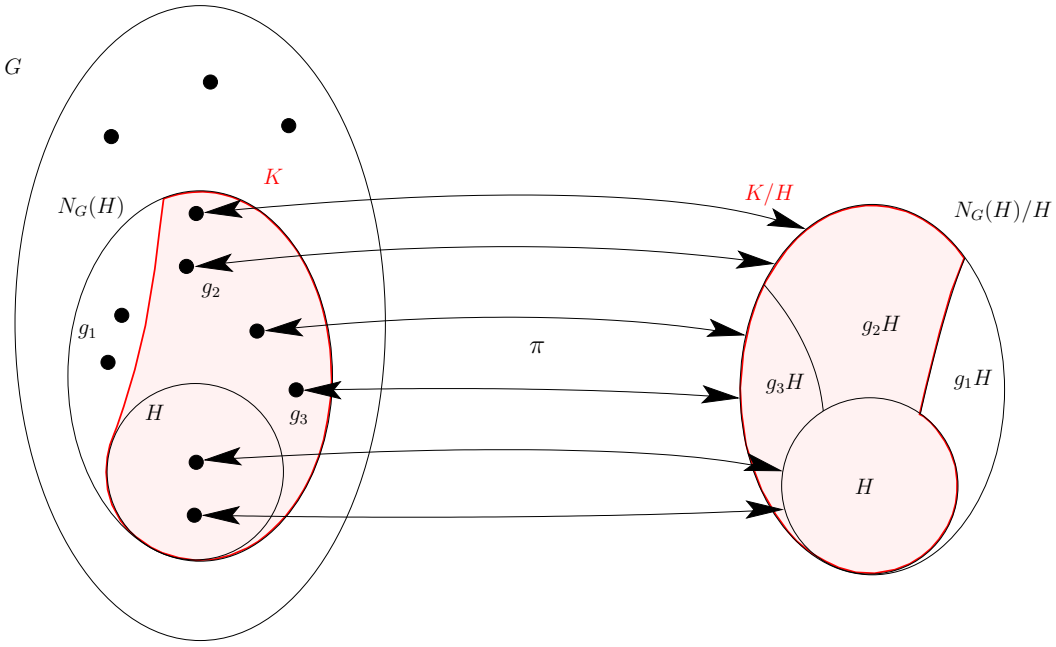

Abbildung 2.6: Kanonische Abbildung π: $N_G(H) \to N_G(H)/H$

(ii) Wegen $K/H \cong \pi\pi^{-1}U = U$ gilt $[K : H] = |H/K| = |U| = p$. Nach dem Satz von Lagrange folgt nun $|K| = [K : H]|H| = pp^i = p^{i+1}$. □

Ist $|G| = p^n r$ mit $(n, r) = 1$, so heißt jede Untergruppe von G mit Ordnung

p^n eine *p-Sylow-Untergruppe* von G. Die Ordnung einer p-Sylow-Untergruppe ist also die höchste p-Potenz, die die Gruppenordnung $|G|$ teilt. Laut Satz von Lagrange kann eine p-Untergruppe keine Ordnung größer als p^n haben, die p-Sylow-Untergruppen werden daher auch als maximale p-Untergruppen bezeichnet. Sie liegen in keiner echt größeren p-Untergruppe.

Es wurde also gezeigt

(i) dass jede endliche Gruppe zu jedem Primteiler p ihrer Ordnung eine p-Sylow-Untergruppe besitzt;

(ii) dass jede p-Untergruppe von G in einer p-Sylow-Untergruppe enthalten ist;

(iii) dass zu jeder Primzahlpotenz, die die Gruppenordnung teilt, eine Untergruppe mit dieser (Primzahlpotenz) Ordnung existiert.

Bemerkungen:
1. Eine Gruppe G kann mehr als eine p-Sylow-Untergruppe zu einer Primzahl p besitzen. Dazu nachstehendes Lemma.
2. Sylow-Untergruppen zu verschiedenen Primzahlen haben trivialen Durchschnitt, denn überhaupt hat zu zwei verschiedenen Primzahlen p und q, jede p-Untergruppe mit jeder q-Untergruppe trivialen Durchschnitt.

Lemma 2.14. *Sei P eine beliebige p-Sylow-Untergruppe, dann ist auch jede konjugierte Gruppe gPg^{-1} eine p-Sylow-Untergruppe in der Gruppe G.*

Beweis. Sei $|G| = p^n r$ mit $(p, r) = 1$. Für jedes $g \in G$ ist die Konjugationsabbildung $x \mapsto gxg^{-1}$ ein Automorphismus von G, der jede p-Sylowuntergruppe von G (i.e. jede Untergruppe mit p^n Elementen) wieder in eine solche überführt. □

Der zweite Sylow-Satz besagt, dass umgekehrt je zwei p-Sylow-Untergruppen konjugiert, also insbesondere isomorph sind. Es können also keine anderen als die zueinander konjugierten p-Sylow-Untergruppen existieren. Sie bilden eine Konjugiertenklasse von Untergruppen. Ist P etwa eine beliebige p-Sylow-Untergruppe, dann ist $\{gPg^{-1} \mid g \in G\}$ die Menge aller p-Sylow-Untergruppen in G.

Satz 2.15. *Sei G eine endliche Gruppe, P eine p-Sylow-Untergruppe und H eine beliebige p-Untergruppe; dann existiert ein Element $g \in G$ mit $g^{-1}Hg \subseteq P$. Insbesondere sind je zwei p-Sylow-Untergruppen von G zueinander konjugiert und daher isomorph.*

Beweis. Sei $|G| = p^n q$ mit $(p, q) = 1$ und $X = \{gP \mid g \in G\}$ die Menge aller Linksnebenklassen von G nach P. Die Gruppe H wirke auf X durch Linksmultiplikation: $h : gP \mapsto hgP$. Da P p-Sylow-Untergruppe (also $|P| = p^n$) und p laut Voraussetzung q nicht teilt, ist $|X| = [G : P] = \frac{|G|}{|P|} = \frac{p^n q}{p^n} = q$ nicht durch p teilbar. Also wird auch $|X_0|$ laut Satz 2.4 (da die p-Untergruppe H auf der endlichen Menge X wirkt) nicht durch p geteilt und daher muss $X_0 \neq \emptyset$ gelten. Es existiert daher eine Nebenklasse gP, für die $hgP = gP$ für alle $h \in H$ gilt, das heißt es ist $g^{-1}hg \in P$ für alle $h \in H$, und damit existiert ein $g \in G$ mit $g^{-1}Hg \subseteq P$. Ist H selber eine p-Sylow-Untergruppe, dann ist nach Lemma 2.14 $g^{-1}Hg$ ebenfalls eine p-Sylow-Untergruppe und die Inklusion $g^{-1}Hg \subseteq P$ kann nur bei Gleichheit erfüllt sein. □

Als Folgerung erhält man

Korollar 2.16. *Die Anzahl der p-Sylow-Untergruppen ist ein Teiler von $|G|$; genauer ist diese Anzahl bestimmt durch den Index $[G : N_G(P)]$ für eine beliebige p-Sylow-Untergruppe P.*

Beweis. Sei P eine p-Sylow-Untergruppe von G. Man lässt G auf der Potenzmenge 2^G durch Konjugation wirken: $g : X \mapsto gXg^{-1}$ für $X \subseteq G$. Nach Satz 2.15 besteht die Menge aller p-Sylow-Untergruppen genau aus der Bahn O_P von P unter dieser Wirkung. Die Anzahl der Elemente dieser Bahn ist laut Satz 2.1 $[G : G_P]$, sicher ein Teiler von $|G|$. Wie zu Beginn dieses Abschnitts erwähnt, ist der Stabilisator G_P genau der Normalisator $N_G(P)$ von P in G. □

Im dritten Sylow-Satz wird schließlich die Anzahl der p-Sylow-Untergruppen noch näher bestimmt.

Satz 2.17. *Die Anzahl der p-Sylow-Untergruppen von G ist kongruent zu* $1 \pmod{p}$.

Beweis. Sei P eine p-Sylow-Untergruppe von G. G wirke auf 2^G durch Konjugation. Wegen $P \leq N_G(P) \leq G$ gilt laut Satz von Lagrange

$$[G : P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|}\frac{|N_G(P)|}{|P|} = [G : N_G(P)][N_G(P) : P]$$

und daher a fortiori

$$[G : P] \equiv [G : N_G(P)][N_G(P) : P] \pmod{p}.$$

Nach Lemma 2.12 gilt

$$[G : P] \equiv [N_G(P) : P] \pmod{p},$$

also auch

$$[G : P] \equiv [G : N_G(P)][G : P] \pmod{p}.$$

Wegen $[G : P] = \frac{|G|}{|P|} = \frac{p^n r}{p^n} = r \not\equiv 0 \pmod{p}$ muss $[G : N_G(P)] \equiv 1 \pmod{p}$ gelten (da man im Restklassenkörper $\mathbb{Z}/(p)$ durch die Restklasse $\overline{[G : P]}$ kürzen kann). Nach Korollar 2.16 ist das genau die Anzahl der p-Sylow-Untergruppen von G. □

Das nachstehende einfache Lemma wird bei nachfolgenden Beispielen benutzt.

Lemma 2.18. *Eine endliche Gruppe G besitzt genau dann eine einzige p-Sylow-Untergruppe P zu einem Primteiler p von $|G|$, wenn P ein Normalteiler von G ist.*

Beweis. Hat eine Gruppe G nur eine einzige p-Sylow-Untergruppe P, dann gilt $P \trianglelefteq G$, denn sei $g \in G$, dann ist laut Lemma 2.14 auch gPg^{-1} die konjugierte eine p-Sylow-Untergruppe. G hat aber laut Voraussetzung nur eine einzige p-Sylow-Untergruppe, daher gilt $gPg^{-1} = P$ für alle $g \in G$, das heißt, P ist Normalteiler von G. Umgekehrt ist ein Normalteiler gerade dadurch charakterisiert, dass er außer sich selbst keine konjugierten Untergruppen besitzt. □

Daraus folgt offensichtlich, dass abelsche Gruppen eindeutig bestimmte p-Sylow-Untergruppen haben.

Abschließend wird die Anwendung der Sylow-Sätze an einfachen Beispielen praktisch vorführt. Zuerst werde ich nachweisen, dass eine Gruppe mit Ordnung 15 zwei Normalteiler besitzt. Anschließend soll die Anzahl der 2- und der 3-Sylow-Untergruppen der alternierenden Gruppe A_4 sowie der Permutationsgruppen S_4 und S_5 bestimmt werden.

Beispiele.

(1) Eine Gruppe G mit $|G| = 15$ besitzt zwei Normalteiler. Sie enthält 3- und 5-Sylow-Untergruppen, da $15 = 3 \cdot 5$. Die Anzahl der 3-Sylow-Untergruppen $n_3 = 1$, denn nur für 1 gilt $n_3 \equiv 1 \pmod 3$ und $n_3 \mid 15$. Ebenso ist die Anzahl der 5-Sylow-Untergruppen $n_5 = 1$, da nur für 1 gilt $n_5 \equiv 1 \pmod 5$ und $n_5 \mid 15$ gilt. Nachdem diese beiden p-Sylow-Untergruppen die einzigen bezüglich p sind, gibt es genau diese beiden Normalteiler.

(2) Die nachstehende Tabelle 2.4 zeigt die Elemente der alternierenden Gruppe A_4 und deren Ordnung. Man sieht, dass sie ein Element mit Ordnung 1, drei Elemente der Ordnung 2 und acht Elemente der Ordnung 3 enthält.

ELEMENT	ORDNUNG
(1)	1
(1,2)(3,4)	2
(1,3)(2,4)	2
(1,4)(2,3)	2
(2,3,4)	3
(2,4,3)	3
(1,2,3)	3
(1,2,4)	3
(1,3,2)	3
(1,3,4)	3
(1,4,2)	3
(1,4,3)	3

Tabelle 2.4: Die Elemente der alternierenden Gruppe A_4 und deren Ordnung

Da 2^2 und 3 die höchsten Potenzen sind, die $|A_4| = 12 = 2^2 \cdot 3$ teilen, besitzt A_4 gemäß dem erstem Sylow-Satz (Satz 2.13) 2-Sylow-Untergruppen der Ordnung $2^2 = 4$ und 3-Sylow-Untergruppen der Ordnung $3^1 = 3$. Nach dem dritten Sylow-Satz (Satz 2.17) ist die Anzahl der 2-Sylow-Untergruppen $n_2 \equiv 1 \pmod 2$. Demnach ist $n_2 \in \{1, 3, 5, ...\}$. Weiters teilt n_2 nach Korollar 2.16 die Gruppenordnung $|A_4| = 12$ und könnte daher aus $\{1, 2, 3, 4, 6\}$ sein. Es bleiben als mögliche Kandidaten für n_2 die Elemente der Schnittmenge $\{1, 3\}$ übrig.

Analog ist nach Satz 2.17 die Anzahl der 3-Sylow-Untergruppe $n_3 \equiv$

1 (mod3), also $n_3 \in \{1, 4, 7, \ldots\}$. Laut Korollar 2.16 gilt $n_3 \mid 12 = |A_4|$ und es ist daher $n_3 \in \{1, 2, 3, 4, 6\}$. Der Durchschnitt ist in diesem Fall $\{1, 4\}$.

Es kann jedoch nicht gleichzeitig $n_2 = 3$ und $n_3 = 4$ gelten. Angenommen, $n_3 = 4$. Der Durchschnitt von je zwei zyklischen Untergruppen mit Primzahlordnung ist trivial. Daraus folgt, dass die vier zyklischen Untergruppen der Ordnung 3 zusammen $4 \cdot 2 = 8$ nicht-triviale Elemente besitzen müssen. Bleiben höchstens $12 - 8 = 4$ Elemente für die 2-Sylow-Untergruppen (die Ordnung 4 haben müssen), von welchen es daher nicht mehr als eine geben kann.

Da es in A_4 genau 3 Elemente der Ordnung 2 gibt, ist die 2-Sylow-Untergruppe $P_2 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ damit bestimmt. Diese einzige 2-Sylow-Untergruppe P_2 ist daher in A_4 ein Normalteiler. Es handelt sich um die Klein'sche Vierergruppe V_4.

Eine 3-Sylow-Untergruppe von A_4 ist sicherlich zyklisch mit Ordnung 3. Jede solche Untergruppe besteht aus einem beliebigen 3-Zyklus, dem zugehörigen inverse 3-Zyklus und dem 1-Element. Somit ist klar, dass es vier 3-Sylow-Untergruppen gibt:

- $\{(1), (2,3,4), (2,4,3)\}$
- $\{(1), (1,2,3), (1,3,2)\}$
- $\{(1), (1,2,4), (1,4,2)\}$
- $\{(1), (1,3,4), (1,4,3)\}$

(3) Die Ordnung der Permutationsgruppe S_4 ist $24 = 2^3 \cdot 3$. S_4 hat daher 2-Sylow-Untergruppen mit Ordnung 8 und 3-Sylow-Untergruppen mit Ordnung 3. Um die Anzahl n_2 der 2-Sylow-Untergruppen zu bestimmen, wähle man eine beliebige Untergruppe der Ordnung 8 etwa

$$P_8 = \{(1), (3\ 4), (1\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 4)(2\ 3)\}$$

und bestimme den Normalisator $N_{S_4}(P_2)$ von P_2 in S_4. Er entspricht P_2 selbst, hat also Kardinalität 8. Nach Korollar 2.16 ist also die Anzahl der 2-Sylow-Untergruppen

$$n_2 = [S_4 : N_{S_4}(P_2)] = \frac{|S_4|}{|N_{S_4}(P_2)|} = \frac{24}{8} = 3$$

Analog ist

$$n_3 = [S_4 : N_{S_4}(P_3)] = \frac{|S_4|}{|N_{S_4}(P_3)|} = \frac{24}{6} = 4$$

Wobei P_3 eine beliebige Untergruppe von S_4 mit Ordnung 3 ist.

Diese Ergebnisse wurden mit Unterstützung des Algebra-Programms GAP ermittelt. Die Befehle finden sich für die Permutationsgruppen S_4 und S_5 im Anhang unter A.4.

Kapitel 3

Permutationsgruppen

3.1 Grundlegendes

In diesem Abschnitt stehen einleitend zentrale Definitionen sowie Aussagen zu elementaren Eigenschaften von Permutationsgruppen, aus denen schnell der Zusammenhang von Permutationsgruppen zu Gruppenwirkungen ersichtlich wird. Der Satz von Cayley ist theoretisch äußerst wertvoll. Er besagt, dass jede endliche Gruppe G mit Ordnung $|G| = n$ zu einer Untergruppe einer Permutationsgruppe S_n isomorph ist. Das heißt, man kann die Theorie der Permutationsgruppen auf jede beliebige Gruppe anwenden. Es folgt daraus jedoch nicht, dass man sich auf die Analyse der Permutationsgruppen beschränken kann. Wenn es praktisch um den Nachweis spezieller Eigenschaften von Gruppen geht, dann wird ersichtlich, dass mit wachsendem n die Struktur der Permutationsgruppen S_n sehr schnell kompliziert wird und die Betrachtung einer Gruppe als Untergruppe der Permutationsgruppe die Analyse erschwert anstatt sie zu erleichtern. Es wird sich zeigen, dass mit der Betrachtung der Gruppenelemente einer abstrakten Gruppe als Permutationsgruppe beispielsweise der Zyklentyp der Permutation Informationen über das Signum und die Konjugiertenklasse des Elements liefert, die in der Folge zur Analyse der Gruppenstruktur beitragen. Ich habe mich in diesem Kapitel an Rotman (vgl. [10] Abschnitt 3.), Robinson (vgl. [8] Abschnitt 1.2), Cigler (vgl. [2] Abschnitt V.5.) und Ledermann (vgl. [6] Kapitel VII) orientiert.

Einleitend die Definition der Permutationsgruppe: für jede Menge X ist die Menge S_X aller bijektiven Funktionen zusammen mit der Komposition $\circ$ von Funktionen bekanntlich ein Gruppe, die genau dann nicht abelsch ist, wenn $|X| > 2$. Im folgenden werde die Menge X immer als endlich vorausgesetzt. Jede Untergruppe U von S_X heißt *Permutationsgruppe*. Eine Permutationsgruppe wirkt per definitionem auf X. Diese Wirkung ist treu (vgl. Beispiel (4) unter Abschnitt 2.1). Umgekehrt kann man auch sagen, dass eine Gruppe,

die treu auf einer endlichen Menge wirkt, eine Permutationsgruppe ist. Da es auf die Bezeichnung der Elemente der Menge nicht ankommt, nimmt man für eine endliche Menge X meist $X = \{1, 2, ..., n\}$ mit $n = |X|$ an. Eine Permutationsgruppe $G \leq S_n$ heißt dann Permutationsgruppe *vom Grad n*. Jedem Element $\sigma \in S_n$ entspricht eine Anordnung $\sigma(1)\sigma(2)\ldots\sigma(n)$ der Menge X. Da es $n!$ Möglichkeiten gibt, die Elemente der Menge X anzuordnen, hat die volle Permutationsgruppe S_n $n!$ Elemente.

Der folgende Satz von Cayley benutzt die bereits in Beispiel (4) unter Abschnitt 2.1 gezeigte treue Gruppenwirkung der Linksmultiplikation einer beliebigen Gruppe auf sich und zeigt, dass sich jede endliche Gruppe als Gruppe von Permutationen auffassen lässt.

Satz 3.1. *Jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe der Permutationsgruppe S_n.*

Beweis. Die Linkstranslation einer Gruppe G auf sich ist eine treue Gruppenwirkung, der die Wirkung definierende Homomorphismus ist also injektiv und G ist isomorph zu seinem Bild in der Permutationsgruppe S_G, somit ist G isomorph zu einer Untergruppe von S_G und da S_G für $|G| = n$ isomorph zu S_n ist, ist G auch isomorph zu einer Untergruppe von S_n. □

Sei G eine beliebige Gruppe und $\varphi : G \to S_X$ ein Homomorphismus, dann heißt φ *Darstellung von G als Permutationsgruppe auf X*. Man sieht, dass die Darstellung einer Gruppe G als Permutationsgruppe auf einer Menge X nichts anderes als eine Gruppenwirkung von G auf X ist und umgekehrt. Man kann daher diese Ausdrücke synonym verwenden. Dies ist, wie bereits einleitend erwähnt, bis zu einem gewissen Grad eine nützliche Technik, um Gruppen zu analysieren. Wenn man die Gruppenelemente einer abstrakten Gruppe als Permutationen interpretiert, kann man beispielsweise die Zyklenstruktur der

Elemente in S_G betrachten und darüber Aussagen über das Signum der Elemente in S_G oder die Konjugiertenklasse eines Elements in S_G gewinnen. Dies liefert dann einen Beitrag zur Analyse der Gruppenstruktur. Insbesondere der letzte Satz des Kapitels (Satz 3.14) wird dazu ein Beispiel aufzeigen.

Für eine Permutation σ auf X bezeichnet die Menge $\{x \in X \mid \sigma(x) \neq x\}$ die *Trägermenge* oder den *Träger* von σ. Die Permutation (1 3 5)(2 6) hat beispielsweise die Trägermenge $\{1, 2, 3, 5, 6\}$. Zwei Permutationen heißen *disjunkt*, wenn die Trägermengen disjunkt sind.

Lemma 3.2. *Zwei disjunkte Permutationen kommutieren.*

Beweis. Seien σ und π disjunkte Permutationen und x in der Trägermenge von π. Dann ist $\pi(x)$ ebenfalls in der Trägermenge von π; denn wäre dem nicht so, dann wäre $\pi(\pi(x)) = \pi(x)$ und Anwendung von π^{-1} ergäbe $\pi(x) = x$, ein Widerspruch. Nun gilt $\sigma(\pi(x)) = \pi(x)$, weil $\pi(x)$ nicht im Träger von σ liegen kann. Anderseits gilt $\sigma(x) = x$, also auch $\pi(\sigma(x)) = \pi(x)$. Für jedes x im Träger von π gilt also

$$\sigma(\pi(x)) = \pi(x) = \pi(\sigma(x)).$$

Analog gilt für jedes y im Träger von σ, dass

$$\sigma(\pi(y)) = \sigma(y) = \pi(\sigma(y)).$$

Falls z weder im Träber von σ noch im Träger von π liegt, gilt

$$\sigma(\pi(z) = z = \pi(\sigma(z)).$$

Insgesamt gilt also $\sigma(\pi(u)) = \pi(\sigma(u))$ für jedes u des Definitionsbereichs. □

Eine Permutation π heißt ein *Zyklus* oder *zyklische Permutation der Länge* l , wenn der Träger von π eine l-elementige Menge $\{a_1, \ldots, a_l\}$ ist und (für eine

geeignete Anordnung $a_1, a_2, \ldots$ der Elemente des Trägers) $\pi(a_1) = a_2, \pi(a_2) = a_3, \ldots, \pi(a_l) = a_1$ gilt.

Ich werde nun den Zusammenhang von Zyklen einer Permutation und Bahnen einer Gruppenwirkung erläutern. Man lasse die Gruppe $G = \langle\pi\rangle$, $\pi \in S_n$, auf der Menge $X = \{1, \ldots, n\}$ wirken. Dies entspricht der nachstehenden Vorgangsweise, die beschreibt, wie man alle Zyklen $\rho_1, \ldots \rho_m$ einer beliebigen Permutation π erhält. Man beginnt mit $i_1 = 1$ und berechnet der Reihe nach $\pi(1), \pi^2(1)$ und folgende, bis zur ersten Potenz π^{k_1}, die angewandt auf 1 wieder 1 ergibt. So erhält man den ersten Zyklus $\rho_1 = (1\ \pi(1)\ \ldots\ \pi^{k_1-1}(1))$ der Länge k_1. Den nächsten Zyklus beginnt man mit dem ersten $i_2 \in X$, das noch nicht im vorigen Zyklus vorkam, und wiederholt die Berechnung von $\pi(i_2), \pi^2(i_2)$, usw. bis $\pi^{k_2}(i_2)$ wieder i_2 ergibt. Der Zyklus $\rho_2 = (i_2\ \pi(i_2)\ \ldots\ \pi^{k_2-1}(i_2))$ hat die Länge k_2. Dieser Vorgang wird fortgesetzt bis kein Element aus X mehr übrig ist. Die Trägermenge $\{i_j, \pi(i_j), \ldots, \pi^{k_j-1}(i_j)\}$ eines Zyklus ρ_j hat k_j Elemente.

In der Sprache der Gruppenwirkungen heißt das, dass die von π erzeugte Untergruppe $\langle\pi\rangle$ von S_n auf der Menge $X = \{1, \ldots, n\}$ wirkt. Dann ist die Menge $\{i, \pi(i), \ldots, \pi^{k-1}(i)\}$ die Bahn O_i von i unter der Wirkung von $\langle\pi\rangle$. Die Zyklen einer beliebigen Permutation entsprechen also den Bahnen. Diese Tatsache wird im folgenden Satz benutzt, zuvor noch eine dafür benötigte Definition.

Seien $\rho_1, \ldots, \rho_m$ die disjunkten Zyklen der Permutation π (wie oben beschrieben), so nennt man die Darstellung $\pi = \rho_1 \cdots \rho_m$ die *Zyklenzerlegung* der Permutation π. Diese ist bis auf die Reihenfolge eindeutig bestimmt.

Satz 3.3. *Jede Permutation $\pi \in S_n$ besitzt eine (bis auf die Reihenfolge) eindeutig bestimmte Zyklenzerlegung.*

Beweis. Bahnen bilden eine disjunkte Zerlegung der Menge $\{1, \ldots, n\}$, die den

Trägermengen der Zyklen entsprechen. Weil umgekehrt die Zyklenzerlegung einer beliebigen Permutation $\sigma \in G$ immer den Bahnen unter $\langle \pi \rangle$ entspricht, folgt die Eindeutigkeit der Zyklenzerlegung. □

Sei $\pi = \rho_1 \cdots \rho_m$ die Produktdarstellung einer Permutation in elementfremde Zyklen ρ_i; angenommen, diese haben die Längen $l_1 \leq l_2 \leq \cdots \leq l_m$, so bezeichnet die geordnete Zahlenfolge $(l_1, \cdots, l_m)$ den *Zyklentyp* der Permutation π. Zum Beispiel hat $(1\ 3\ 5)(2\ 6) = (2)(2\ 6)(1\ 3\ 5)$ den Zyklentyp $(1, 2, 3)$. Zwei Permutationen sind also vom selben Zyklentyp, wenn sie dieselbe Anzahl von 1er-Zyklen, 2er-Zyklen, etc. haben. Der Zyklentyp einer Permutation π ist deshalb von Interesse, weil er einfach zu bestimmen ist und weil er die folgenden Invarianten der Permutation π bestimmt:

- die Konjugiertenklasse O_π in S_n
- das Signum $\operatorname{sgn}(\pi)$
- die Ordnung $\operatorname{ord}(\pi)$

Dies soll nun gezeigt werden. Wobei der nächste Satz nicht nur besagt, dass der Zyklentyp einer Permutation π die Konjugiertenklasse O_π bestimmt, sondern dass auch die umgekehrte Aussage gilt.

Satz 3.4. *Zwei Permutationen σ, π sind in S_n genau dann konjugiert, wenn sie vom selben Zyklentyp sind.*

Beweis. Seien σ und π zueinander konjugiert, so sind π und σ vom selben Zyklentyp, denn sei $\sigma = (a_1\ a_2\ \cdots\ a_k)$ eine zyklische Permutation (das heißt $\sigma(a_i) = a_{i+1 \pmod k}$) und sei τ eine beliebige Permutation. Dann gilt:

- $\tau\sigma\tau^{-1}(\tau(a_i)) = \tau(a_{i+1 \pmod k})$
- $\tau\sigma\tau^{-1}(b) = b$ falls $b \notin \{\tau(a_1), \ldots, \tau(a_k)\}$

Daraus folgt $\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2)\cdots\tau(a_k)) =: \pi$. Das Konjugierte eines Zyklus ist also wieder ein Zyklus gleicher Länge. Sei nun $\sigma = \rho_1\rho_2\ldots\rho_m$ das Produkt disjunkter Zyklen der Länge $l_1, l_2, \ldots, l_m$. Dann ist

$$\tau\sigma\tau^{-1} = \tau\rho_1\tau^{-1} \cdot \tau\rho_2\tau^{-1}\cdots\tau\rho_m\tau^{-1}.$$

Wie oben gezeigt, ist $\tau\rho_i\tau^{-1}$ eine zyklische Permutation mit derselben Zyklenlänge wie ρ_i. Weiters sind die Zyklen $\tau\rho_i\tau^{-1}$ paarweise disjunkt, da dies für die Zyklen ρ_i gilt. Das Konjugierte eines Produktes disjunkter Zyklen ergibt also wieder disjunkte Zyklen derselben Länge. Also haben konjugierte Elemente insgesamt denselben Zyklentyp.

Seien umgekehrt zwei Permutationen σ und π vom selben Zyklentyp gegeben, dann konstruiere man eine Permutation $\gamma : a_{ij} \mapsto b_{ij}$, wobei sich die a_{ij} und b_{ij} folgendermaßen aus den aufsteigend nach Zyklenlänge sortierten Elementen von π und σ ergeben:

$$\begin{array}{cccccccccc}
\pi & (a_{11}) & \cdots & (a_{k_1 1}) & (a_{12}a_{22}) & \cdots & (a_{k_2 1}a_{k_2 2}) & \cdots & (a_{31}a_{32}a_{33}) & \cdots \\
 & \downarrow & & \downarrow & \downarrow\ \downarrow & & \downarrow\ \downarrow & & \downarrow\ \downarrow\ \downarrow & \\
\sigma & (b_{11}) & \cdots & (a_{k_1 1}) & (b_{12}b_{22}) & \cdots & (b_{k_2 1}b_{k_2 2}) & \cdots & (b_{31}b_{32}b_{33}) & \cdots
\end{array}$$

Da π und σ denselben Zyklentyp haben ist diese Definition möglich. Es gilt dann klarerweise $\sigma = \gamma\pi\gamma^{-1}$ und σ und π sind also konjugiert. □

Die Aussage dieses Satzes soll an zwei kurzen Beispiele verdeutlicht werden, die leicht nachzurechnen sind.

1. Sei $\sigma = (1\ 3\ 4)$ und $\tau = (2\ 3\ 5)(4\ 6)$, dann ist
   $\tau\sigma\tau^{-1} = (\tau(3)\ \tau(4)\ \tau(1)) = (5\ 6\ 1) =: \pi$

2. Sei $\alpha = (4)(1\ 3)(2\ 5\ 6)$ und $\beta = (6)(2\ 4)(3\ 1\ 5)$. Dann kann man ein $\gamma = (4\ 6\ 5\ 1\ 2\ 3)$ definieren, sodass $\gamma\alpha\gamma^{-1} = \beta$.

Um die Signum-Funktion einzuführen, ist noch folgende Definitionen nötig. Eine *Transposition* ist eine Permutation, die genau zwei Elemente i und j vertauscht und alle anderen fix läßt; die übliche Notation für diese Transposition ist $(i\ j)$. Jede zyklische Permutation kann durch Komposition von Transpositionen erhalten werden, denn $(a_1 \dots a_l) = (a_1\ a_l)(a_1\ a_{l-1}) \dots (a_1\ a_2)$. Da jede Permutation die Hintereinanderausführung von zyklischen Permutationen ist, gilt dies dann sogar für jede Permutation. Die Permutationsgruppe S_n wird also von ihren Transpositionen erzeugt. (Es gilt sogar, dass die $n-1$ Transpositionen $(1\ 2), (2\ 3), \dots, (n-1\ n)$ die Gruppe S_n erzeugen.)

Ein Paar (i, j) mit $i < j$ und $\pi(i) > \pi(j)$ heißt *Inversion* der Permutation π. Mit $\mathrm{inv}(\pi)$ bezeichnet man die Gesamtzahl der Inversionen von π. Sei $i < j$; was sind die Inversionen der Transposition $(i\ j)$? Es sind dies offenbar genau die Paare:

$$\{(i,k) \mid i < k < j\} \cup \{(k,j) \mid i < k < j\} \cup \{(i,j)\}.$$

Die Anzahl der Inversionen von $(i\ j)$ ist somit $2|\{k \mid i < k < j\}| + 1$, was unabhängig von der Wahl von i und j eine ungerade Zahl ist.

Die *Signum*-Funktion auf der Menge der Permutation ist folgendermaßen definiert:

$$\mathrm{sgn}(\pi) := \prod_{i<j} \frac{\pi(j) - \pi(i)}{j - i}.$$

Im Nenner dieses Bruchs stehen natürliche Zahlen, im Zähler ganze Zahlen, die sich von denen im Zähler höchstens um das Vorzeichen unterscheiden. Die Anzahl der negativen Zahlen im Zähler ist genau der Anzahl der Inversionen von π, es gilt also: $\mathrm{sgn}(\pi) = (-1)^{\mathrm{inv}(\pi)}$. Sei beispielsweise $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$;

dann ist

$$\begin{aligned}\operatorname{sgn}(\pi) &= \frac{4-1}{2-1}\frac{3-1}{3-1}\frac{2-1}{4-1}\frac{3-4}{3-2}\frac{2-4}{4-2}\frac{2-3}{4-3} = \frac{3-4}{4-3}\frac{2-4}{4-2}\frac{2-3}{3-2} \\ &= (-1)(-1)(-1) = -1.\end{aligned}$$

Der Wert der Signum-Funktion, auch *Vorzeichen* der Permutation genannt, zeigt somit, ob eine Permutation eine gerade oder eine ungerade Anzahl von Inversionen besitzt. Entsprechend nennt man eine Permutation *gerade* oder *ungerade*. Die wichtigste Eigenschaft der Signum Funktion ist die folgende.

Satz 3.5. *Die Funktion* $\operatorname{sgn} : S_n \to \{1, -1\}$ *ist ein Homomorphismus.*

Beweis.

$$\begin{aligned}\operatorname{sgn}(\pi\sigma) &= \prod_{i<j} \frac{(\pi\sigma)(j) - (\pi\sigma)(i)}{j-i} \\ &= \prod_{i<j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{\sigma(j) - \sigma(i)} \frac{\sigma(j) - \sigma(i)}{j-i} \\ &= \prod_{i<j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{\sigma(j) - \sigma(i)} \operatorname{sgn}(\sigma) \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)\end{aligned}$$

□

Folgendes ist festzuhalten.

1. Das Produkt von zwei geraden oder zwei ungeraden Permutationen ergibt eine gerade Permutation, während das Produkt von einer geraden mit einer ungeraden eine ungerade Permutation ist.

2. Für jede Permutation σ gilt $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma)^{-1} = \operatorname{sgn}(\sigma^{-1})$.

3. Es gilt: $\operatorname{sgn}(\sigma^{-1}\pi\sigma) = \operatorname{sgn}(\sigma^{-1})\operatorname{sgn}(\pi)\operatorname{sgn}(\sigma) = \operatorname{sgn}(\pi)$. Das heißt, die Funktion sgn ist auf jeder Konjugiertenklasse konstant.

4. Jede Transposition $(i\ j)$ ist eine ungerade Permutation, wie weiter oben gezeigt wurde. Hat eine Permutation π eine Darstellung als Produkt von t Transpositionen, so gilt $t \equiv \mathrm{inv}(\pi) \pmod 2$

5. Den Kern der Signumfunktion bezeichnet man als die *alternierende Gruppe* $A_n := \mathrm{Ker}(\mathrm{sgn}) = \{\sigma \in S_n : \mathrm{sgn}(\sigma) = +1\}$, sie besteht genau aus den geraden Permutationen.

Für sie gilt folgende wichtige Aussage.

Satz 3.6. *Die alternierende Gruppe A_n ist Normalteiler von S_n mit Ordnung $\frac{1}{2}n!$.*

Beweis. Die alternierende Gruppe A_n ist per definitionem der Kern der Signumfunktion $\mathrm{sgn} : S_n \to \{1, -1\}$. Da es eine ungerade Permutation α gibt, ist die Signumfunktion surjektiv, das heißt, $\mathrm{sgn}(S_n) = \{1, -1\}$. Nach dem Homomorphiesatz ist daher $A_n \trianglelefteq S_n$ und die Faktorgruppe S_n/A_n is isomorph zum Bild $\{1, -1\}$. Da alle Nebenklassen dieselbe Kardinalität haben, gilt $|A_n| = |\alpha A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. □

Es ergibt sich eine nützliches Beobachtung über Untergruppen der S_n.

Lemma 3.7. *Die Gruppe G sei Untergruppe von S_n; wenn G eine ungerade Permutation enthält, dann ist $|G|$ gerade und G entählt $\frac{1}{2}|G|$ gerade und $\frac{1}{2}|G|$ ungerade Elemente.*

Beweis. Die Gruppe G enthält laut Voraussetzung eine ungerade Permutation

α. Dann gilt

$$\begin{aligned} G &= G \cap S_n && && \text{wegen } G \leq S_n \\ &= G \cap (A_n \cup \alpha A_n) && && \text{wegen Satz 3.6} \\ &= (G \cap A_n) && \cup\ (G \cap \alpha A_n) \\ &= \underbrace{(G \cap A_n)}_{\substack{\text{gerade} \\ \text{Permutationen} \\ \text{in } G}} && \cup\ \underbrace{\alpha(G \cap A_n)}_{\substack{\text{ungerade} \\ \text{Permutationen} \\ \text{in } G}} \end{aligned}$$

Es gibt also in G eine Untergruppe mit Index 2 (nämlich $G \cap A_n$), welche aus genau den geraden Permutationen von G besteht; die zweite Nebenklasse nach dieser Untergruppe besteht genau aus den ungeraden Permutationen von G. Da alle Nebenklassen dieselbe Kardinalität haben, sind die Hälfte der Elemente gerade Permutationen und die andere ungerade. □

Der folgende Satz zeigt, dass der Zyklentyp einer Permutation ihre Ordnung und ihr Vorzeichen bestimmt.

Satz 3.8. *1. Für eine zyklische Permutation σ der Länge m gilt* $\operatorname{ord}(\sigma) = m$ *und* $\operatorname{sgn}(\sigma) = (-1)^{m-1}$. *Eine zyklische Permutation ist also genau dann gerade, wenn die Zyklenlänge ungerade ist.*
2. Hat die kanonische Zerlegung einer Permutation σ ausschließlich Zyklen derselben Länge l, dann ist $\operatorname{ord}(\sigma) = l$ *und es gilt*

$$\sigma \text{ ist gerade} \Leftrightarrow \text{Zyklenlänge ist ungerade oder Zyklenanzahl gerade}$$

und damit auch

$$\sigma \text{ ist ungerade} \Leftrightarrow \text{Zyklenlänge ist gerade und Zyklenanzahl ungerade .}$$

Dieser Sachverhalt ist in Tabelle 3.1 zusammengefasst.
3. Ist $\pi = \rho_1 \cdots \rho_m \in S_n$ die kanonische Zerlegung von π in elementfremde

l in S_G gerade ungerade	# in S_G gerade ungerade	sgn
U	U	+1
U	G	+1
G	U	-1
G	G	+1

Tabelle 3.1: Zusammenhang Zyklenlänge, Zyklenanzahl und Signum

Zyklen $\rho_1, \ldots, \rho_m$ *mit Längen* $l_1, \ldots, l_m$*, dann ist* $\mathrm{ord}(\pi) = \mathrm{kgV}(l_1, \ldots, l_m)$.

Beweis. 1. Sei $\pi = (a_1\ a_2\ \ldots a_l)$ eine zyklische Permutation der Länge l. Für jedes $k < l$ gilt $\pi^k(a_1) = a_k \neq a_1$, also ist $\pi^k \neq id$; anderseits gilt $\pi^l(a_i) = a_i$ für jedes a_i aus dem Träger von π, also gilt $\pi^l = id$ und $\mathrm{ord}(\pi) = l$. Weiter oben wurde bereits erwähnt, dass ein Zyklus der Länge l als Produkt von $l-1$ Transpositionen dargestellt werden kann, also gilt $\mathrm{sgn}(\pi) = (-1)^{l-1}$.

2. Angenommen, die kanonische Zyklenzerlegung von π ist $\pi = \rho_1 \cdots \rho_k$ und alle Zyklen ρ_i haben Länge l. Dann ist $\pi^l = (\rho_1 \cdots \rho_k)^l = \rho_1^l \cdots \rho_k^l = id$, die die Zyklen ρ_i kommutieren, und $\pi^t \neq id$ für alle $t < l$. Damit ist $\mathrm{ord}(\pi) = l$. Jeder Zyklus ρ_i kann als Produkt von $l-1$ Transpositionen dargestellt werden, also kann π als Produkt von $k(l-1)$ Transpositionen dargestellt werden. Diese Zahl ist offenbar genau dann gerade, wenn zumindest eine der beiden Zahlen k oder $l-1$ gerade ist, also k gerade oder l ungerade ist, was die erste der beiden Äquivalenzen beweist. Die zweite ist zur ersten äquivalent.

3. Sei $l := \mathrm{kgV}(l_1, \ldots, l_m)$; wegen $l_i \mid l$ gilt $\rho_i^l = id$ für jedes i. Da die Zyklen ρ_i kommutieren, sieht man wie oben, dass

$$\pi^l = (\rho_1 \cdots \rho_m)^l = \rho_1^l \cdots \rho_m^l = id.$$

Daraus ergibt sich $\mathrm{ord}(\pi) \mid l$.

Sei umgekehrt a_i aus dem Träger von ρ_i; dann gilt $\pi(a_i) = \rho_i(a_i)$ und für $k \in \mathbb{N}$ ist daher

$$\pi^k(a_i) = a_i \Leftrightarrow \rho_i^k(a_i) = a_i \Leftrightarrow l_i \mid k.$$

Für $k = \text{ord}(\pi)$ ergibt sich daraus $l_i \mid \text{ord}(\pi)$ für alle i und damit auch $l \mid \text{ord}(\pi)$. □

Beispiel.

Am Beispiel der Permutationsgruppe S_3 soll nun einerseits der soeben angesprochene Zusammenhang von Zyklentyp, Signum und Ordnung eines Elements gezeigt werden und andererseits soll die Betrachtung der Elemente als Untergruppe von S_{S_3} erläutert werden. Die Gruppe wirke also auf sich selbst durch Linksmultiplikation. Die gesamte Wirkung eines Elementes $a \in G = S_3$ per Linksmultiplikation auf alle Elemente $x \in S_3$ lässt sich in Zyklenschreibweise darstellen.

Sei z.B. $a = (1\ 2)$, so ergeben sich die Zyklen $((1)(1\ 2))$ $((1\ 3)(1\ 3\ 2))$ $((2\ 3)(1\ 2\ 3))$. Alle Zyklen haben Zyklenlänge $l = 2$. Abbildung 3.1 zeigt, wie so

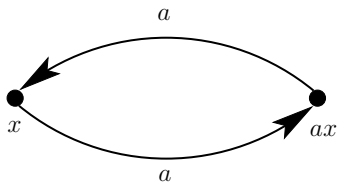

Abbildung 3.1: Zyklen der Länge 2 aus S_3 in S_{S_3}

ein Zyklus aussieht. Da die Zyklen alle die gleiche Länge haben und eindeutig sowie paarweise disjunkt sind, ist die Zyklenanzahl $\#$ von a in S_{S_3} gleich 3. Allgemein enthält ein Zyklus, in dem ein Element a wiederholt auf x wirkt, die Elemente $(x\ ax\ a^2x\ \ldots a^{l-1}x)$ mit Zyklenlänge $l = \text{ord}(a)$. Abbildung 3.2 zeigt solch einen Zyklus. Man sieht, dass die l-te Anwendung von a auf x wieder x ist.

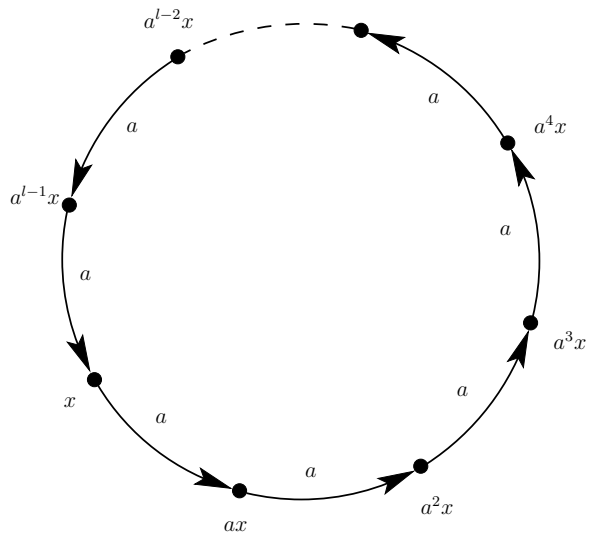

Abbildung 3.2: Ein Zyklus von $a \in G$ aufgefasst als Element in S_G

Es ergibt sich die in Tabelle 3.2 angegebene Wirkung mit der entsprechenden Zyklenstruktur in S_{S_3}.

Man sieht, dass die Ordnung des Elements in der Gruppe G gleich der Zyklenlänge l in S_G ist und die Zyklenanzahl $\# = \frac{|G|}{l}$, da die Zyklen alle gleiche Länge haben. Nun soll bestimmt werden, ob dem Element in S_G eine gerade oder eine ungerade Permutation entspricht. Dazu betrachtet man die Zyklenstruktur des Elements in S_G. Laut Satz 3.8 ist ein Element a genau dann eine ungerade Permutation (das heißt $\operatorname{sgn}(a) = -1$), wenn die Zyklenlänge l gerade und die Zyklenanzahl $\#$ ungerade ist. Dies kann in Tabelle 3.3 abgelesen werden. Es ist zu erkennen, dass das Signum in S_G gleich dem Signum in G ist.

$a \in G$	ord(a) in G	Wirkung von a auf G	l in S_G	# in S_G
(1)	1	((1)) ((1 2)) ((1 3)) ((1 2 3)) ((1 3 2)) ((2 3))	1	6
(1 2)	2	((1)(1 2)) ((1 3)(1 3 2)) ((2 3)(1 2 3))	2	3
(1 3)	2	((1)(1 3)) ((1 2)(1 2 3)) ((2 3)(1 3 2))	2	3
(2 3)	2	((1)(2 3)) ((1 2)(1 3 2)) ((1 3)(1 2 3))	2	3
(1 2 3)	3	((1 3)(1 2)(2 3)) ((1)(1 3 2)(1 2 3))	3	2
(1 3 2)	3	((1 3)(2 3)(1 2)) ((1)(1 2 3)(1 3 2))	3	2

Tabelle 3.2: $G = S_3$ aufgefasst als Untergruppe von S_{S_3}

$a \in G$	sgn(a) in G	ord(a) $= l$ in S_G	# Zyklen in S_G	l gerade ungerade	# gerade ungerade	sgn(a) in S_G
(1)	+1	1	6	U	G	+1
(1 2)	-1	2	3	G	U	-1
(1 3)	-1	2	3	G	U	-1
(1 2 3)	+1	3	2	U	G	+1
(1 3 2)	+1	3	2	U	G	+1
(2 3)	-1	2	3	G	U	-1

Tabelle 3.3: $G = S_3$: Zyklenanzahl, Zyklenlänge und Signum in S_{S_3}

3.2 Einfachheit der A_n für $n \geq 5$

Ich beginne diesen Abschnitt mit zwei Lemmata als Vorbereitung auf den Hauptsatz dieses Abschnitts.

Lemma 3.9. *Für $n \geq 3$ wird die alternierende Gruppe A_n wird von 3er-Zyklen erzeugt.*

Beweis. Sei $\sigma \in A_n$. Dann ist σ laut Definition gerade, insbesondere ist σ (in S_n) ein Produkt einer geraden Anzahl von Transpositionen. Es ist daher zu zeigen, dass jedes Produkt von zwei Transpositionen Produkt von 3er-Zyklen ist. Seien $a, b, c \in \{1, \ldots, n\}$ verschiedene Zahlen. Dann gilt

- für gleiche 2er-Zyklen: $(a\ b)(a\ b) = id = (a\ b\ c)^3$
- für 2er-Zyklen mit einem gleichen Element: $(a\ b)(a\ c) = (a\ c\ b)$
- für disjunkte 2er-Zyklen: $(a\ b)(c\ d) = (a\ d\ c)(a\ b\ c)$

□

Satz 3.10. *Für $n \geq 5$ sind in der alternierenden Gruppe A_n alle 3er-Zyklen zueinander konjugiert.*

Beweis. Per definitionem sind zwei Elemente σ und ρ zueinander in einer Gruppe G konjugiert, wenn ein $\pi \in G$ existiert, sodass $\pi\sigma\pi^{-1} = \rho$. Seien $\sigma = (a_1\ a_2\ a_3)$ und $\rho = (b_1\ b_2\ b_3)$ zwei 3er-Zyklen. Dann sind sie laut Satz 3.4 in S_n konjugiert. Das heißt, es gibt ein $\pi \in S_n$, sodass $\pi\sigma\pi^{-1} = \rho$. Die Behauptung des Satzes lautet aber, dass die beiden Permutationen σ und ρ nicht nur in S_n sondern auch in A_n konjugiert sind. Dies ist also zu überprüfen. Wenn $\pi \in A_n$, dann sind die beiden Elemente in A_n konjugiert und wir sind fertig. Ist allerdings $\pi \notin A_n$, dann wählt man $c \neq d \in \{1, \ldots, n\}$ mit $c, d \notin \{a_1, a_2, a_3\}$ (an dieser Stelle wird verwendet, dass $n \geq 5$). Die Transposition

$(c\ d)$ ist disjunkt zu ρ, also gilt $(c\ d)\rho(c\ d) = \rho$. Wegen $(c\ d)^{-1} = (c\ d)$ ergibt sich aus $\pi\sigma\pi^{-1} = \rho = (c\ d)\rho(c\ d)$ insbesondere

$$\rho = (c\ d)\pi\sigma\pi^{-1}(c\ d)^{-1} = ((c\ d)\pi)\sigma((c\ d)\pi)^{-1}.$$

Da π ungerade ist, ist $(c\ d)\pi$ gerade, und ρ und σ sind in konjugiert in A_n. □

Eine Gruppe $G \neq \{1\}$ heißt *einfach*, wenn sie außer G und $\{1\}$ keine Normalteiler besitzt. Insbesondere heißt dies, dass G keine Erweiterung einer nicht-trivialen Untergruppe durch eine nicht-triviale Gruppe ist. Die endlichen einfachen Gruppen bilden quasi die Bausteine der endlichen Gruppen. Man kann eine gegebene Gruppe darüber beschreiben, dass man sie aus einfachen Gruppen zusammensetzt. Daher ist es von Interesse, die endlichen einfachen Gruppen zu identifizieren. Der folgende Satz ergibt die elementarste einfache Gruppe.

Lemma 3.11. *Eine abelsche Gruppe ist genau dann einfach, wenn sie zyklisch und ihre Ordnung prim ist.*

Beweis. Jede (zyklische) Gruppe G mit Primzahlordnung ist einfach: ist H Untergruppe von G, dann gilt $|H|$ teilt $|G|$. Da $|G|$ prim, kann die Ordnung von H nur 1 oder $|G|$ sein. Das heißt $H = \{1\}$ oder $H = G$, insbesondere hat G keinen nicht-trivialen Normalteiler.

Sei umgekehrt G abelsch und einfach und $x \in G$, $x \neq 1$. Da $\langle x\rangle$ ein Normalteiler ist, gilt $\langle x\rangle = G$. Also ist G zyklisch und wird von jedem seiner Elemente $\neq 1$ erzeugt. Dies ist nur möglich, wenn G Primzahlordnung hat. □

Die einzigen einfachen abelschen Gruppen sind also die zyklischen Gruppen C_p von Primzahlordnung p.

Für A_4 gilt: die Klein'sche Vierergruppe $V_4 = \{id, (12)(34), (13)(24), (14)(23)\}$ ist Normalteiler von A_4, weil sie mit jedem Element $(ab)(cd)$ auch jedes konju-

gierten Elemente enthält. Die alternierende Gruppe A_4 ist also nicht einfach. Sehr wohl aber die alternierende Gruppe A_5, was der nächste Satz zeigt.

Satz 3.12. *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Beweis. Angenommen, die alternierende Gruppe A_n enthalte einen von $\{1\}$ verschiedenen Normalteiler N. Es soll gezeigt werden, dass dieser für $n \geq 5$ ganz mit A_n zusammenfallen muss. Es genügt zu zeigen, dass N einen 3er-Zyklus enthält; denn dann enthält N (da Normalteiler) auch jeden konjugierten und damit (laut Satz 3.10) jeden beliebigen 3er-Zyklus. (Bemerkung: Hier geht ein, dass $n \geq 5$ sein muss.) Aus Satz 3.9 folgt dann schließlich, dass der gewählte Normalteiler N mit ganz A_n übereinstimmt und A_n somit einfach sein muss.
Bleibt der Beweis, dass der Normalteiler N einen 3er-Zyklus enthält. Man wähle eine beliebige Permutation π aus dem Normalteiler N, wobei $\pi \neq 1$ sein soll. Die gewählte Permutation π kann keine Transposition sein, denn sonst wäre π ungerade und nicht Element aus A_n. Wenn π ein 3er-Zyklus ist, dann ist nichts mehr zu beweisen. Also muss π mindestens 4 Elemente bewegen und eine der folgenden Formen haben:

1) $\pi = (a\ b\ c\ d \ldots) \ldots$ - das heißt, die Zyklenzerlegung der Permutation π enthält mindestens einen Zyklus der Länge ≥ 4;

2) $\pi = (a\ b\ c)(d\ e \ldots) \ldots$ - das heißt die Permutation π hat einen Zyklus der Länge 3;

3) $\pi = (a\ b)(c\ d) \ldots$ - das heißt, die Permutation π enthält zwei Zyklen der Länge 2.

Es wird schließlich die entscheidende Voraussetzung, dass N Normalteiler (und damit auch Untergruppe) von A_n ist, benutzt. Da $N \leq A_n$ ist neben dem

Element π auch das inverse Element $\pi^{-1} \in N$ und, da $N \trianglelefteq A_n$, liegt auch jedes zu π^{-1} konjugierte Element, sowie das Produkt von π mit jedem konjugierten Element von π^{-1} im Normalteiler N. Zu einem beliebigen π müsste also auch $\pi(\rho\pi^{-1}\rho^{-1}) \in N$ sein, wobei ρ aus A_n beliebig gewählt werden kann.

1) Sei $\rho = (a\,b\,c)$, dann ist $\rho^{-1} = (a\,c\,b)$ und es gilt $\pi\rho\pi^{-1} = (\pi(a)\,\pi(b)\,\pi(c)) = (b\;c\;d)$ und $\pi(\rho\pi^{-1}\rho^{-1}) = (\pi\rho\pi^{-1})\rho^{-1} = (b\;c\;d)(a\;c\;b) = (a\;d\;b)$ also ein 3er-Zyklus aus N.

2) Sei $\rho = (a\;b\;d)$, dann ist $\pi\rho\pi^{-1} = (b\;c\;e), \rho^{-1} = (d\;b\;a)$ und $\pi(\rho\pi^{-1}\rho^{-1}) = (b\;c\;e)(d\;b\;a) = (a\;d\;c\;e\;b)$, damit hat man wieder eine Permutation wie im Fall 1) und findet wieder einen 3er-Zyklus in N.

3) Sei $e \neq a, b, c, d$ und $\rho = (a\;c\;e)$. Dann ist $\pi\rho\pi^{-1} = (b\;d\;\pi(e))$ und $\rho^{-1} = (a\;e\;c)$. Wenn $\pi(e) = e$, dann ist $\pi\rho\pi^{-1}\rho^{-1} = (b\;d\;e)(a\;e\;c) = (a\;b\;d\;e\;c)$. Das entspricht dann dem Fall 1). Wenn $\pi(e) \neq e$, sei $\pi(e) = f$, dann ist $f \notin \{a, b, c, d, e\}$ und $\pi\rho\pi^{-1}\rho^{-1} = (bdf)(eca)$ und somit gilt Fall 2).

□

A_5 ist die kleinste einfache nicht-abelsche alternierende Gruppe (A_3 ist zyklisch mit Ordnung 3, also ebenfalls einfach, aber abelsch). Folgende besonderen Eigenschaften dieser Gruppe sollen an dieser Stelle, kurz aufgezeigt werden: sie ist überhaupt die kleinste einfache nicht-abelsche Gruppe. Es gilt sogar, dass jede einfache Gruppe der Ordnung $60 = |A_5|$ isomorph zu A_5 ist. Ferner ist A_5 der einzige nicht triviale Normalteiler von S_5, dies gilt auch für alle A_n mit $n \geq 5$.

3.3 Weiterführende Resultate

Der letzte Abschnitt zeigt anhand von zwei weiteren Sätzen die nützlichen Beweismethoden der Gruppenwirkungen.

Für jede endliche abelsche Gruppe (Hauptsatz über endlich-erzeugte abelsche Gruppen aus Cigler (vgl. [2] Abschnitt IV.1.)) und jede endliche p-Gruppe (Satz 2.13) gilt die Umkehrung des Satzes von Lagrange: zu jedem Teiler d der Gruppenordnung gibt es eine Untergruppe mit Ordnung d. Diese Behauptung gilt aber nicht für beliebige endliche Gruppen, es wird gezeigt, dass die alternierende Gruppe A_4 ein Gegenbeispiel ist. Diese hat Ordnung 12, besitzt aber keine Untergruppe der Ordnung 6.

Satz 3.13. *Die alternierende Gruppe A_4 hat keine Untergruppe der Ordnung 6.*

Beweis. Ich nehme indirekt an, dass H Untergruppe der alternierenden Gruppe A_4 mit Ordnung $|H| = 6$ ist und beweise, dass dies zu einem Widerspruch führt. Ich werde zuerst die Anzahl der Elemente von H, die einen 3er-Zyklus darstellen, bestimmen und dann die, die Ordnung 2 haben. Zusammen mit dem Einselement der Untergruppe ergeben sich zwingend mehr als 6 Elemente, was der Annahme widerspricht. Zuerst also zu den Elementen, die einen 3er-Zyklus darstellen. Es wird in drei Schritten gezeigt, dass H vier 3er-Zyklen enthalten muss:
1) Es existiert mindestens ein 3er-Zyklus α in H;
2) Der Zentralisator $C_{A_4}(\alpha)$ von α in der alternierenden Gruppe A_4 hat Ordnung 3;
3) Nach dem Bahn-Stabilisator-Satz (Satz 2.1) folgt für die Konjugationswirkung, dass die Konjugiertenklasse $C(\alpha)$ in der alternierenden Gruppe A_4 vier Elemente enthält. Alle vier Elemente sind 3er-Zyklen und liegen in der Unter-

gruppe H.

ad 1) A_4 hat 12 Elemente (siehe Tabelle 2.4), davon sind acht 3er-Zyklen. Da H Kardinalität 6 hat, muss mindestens ein 3er-Zyklus α in H liegen.

ad 2) Um den Zentralisator $C_{A_4}(\alpha)$ von α in A_4 zu bestimmen, wird zuerst der Zentralisator $C_{S_4}(\alpha)$ von α in S_4 bestimmt, der, wie sich zeigen wird, genau mit dem Zentralisator $C_{A_4}(\alpha)$ übereinstimmt. Die Konjugiertenklasse $C(\alpha)$ von α in S_4 besteht laut Satz 3.4 aus allen 3er-Zyklen und hat somit Ordnung $|C(\alpha)| = 8$. Mit dem Bahn-Stabilisator-Satz (Satz 2.1) ergibt dies die Kardinalität des Zentralisators $C_{S_4}(\alpha)$ von α in S_4: $|C_{S_4}(\alpha)| = \frac{|S_4|}{|C(\alpha)|} = \frac{12}{8} = 3$. Das heißt, es gibt nur drei Elemente in S_4, die mit α kommutieren: α, $\alpha^{-1} = \alpha^2$ und 1. Da alle drei Elemente in A_4 enthalten sind, stimmt der Zentralisator $C_{S_4}(\alpha)$ in S_4 mit dem Zentralisator $C_{A_4}(\alpha)$ in A_4 überein und der Zentralisator $C_{A_4}(\alpha)$ von α in A_4 hat Ordnung 3.

3) Mit der Ordnung des Zentralisator $C_{A_4}(\alpha)$ von α in A_4 und der Ordnung von A_4 erhält man mit Hilfe des Bahn-Stabilisator-Satzes (Satz 2.1) die Ordnung der Konjugiertenklasse $C(\alpha)$ in A_4: $|C(\alpha)| = \frac{|A_4|}{|C_{A_4}(\alpha)|} = \frac{12}{3} = 4$. Alle vier Elemente der Konjugiertenklasse $C(\alpha)$ in A_4 liegen in der Untergruppe H, weil diese normal ist. (Die Normalität von H in A_4 ergibt sich aus der Tatsache, dass der Index laut Satz von Lagrange $[A_4 : H] = \frac{12}{6} = 2$ ist.)

Die Untergruppe H enthält bisher das Einselement und vier 3er-Zyklen, also insgesamt fünf Elemente. H kann keinen weiteren 3er-Zyklus enthalten, denn hätte H einen fünften 3er-Zyklus, so würde es damit aber auch dessen gesamte Konjugiertenklasse also weitere vier Elemente beinhalten und H könnte nicht mehr Ordnung 6 haben.

Laut Satz von Cauchy (Satz 2.5) muss H ein Element β der Ordnung 2 haben. Da β eine gerade Permutation ist, hat es die Form $\beta = (a\ b)(c\ d)$. Der

3er-Zyklus $(a\ c\ b)$ liegt in A_4. Da H normal in A_4 ist, muss mit β auch das konjugierte Element $(a\ c\ b)\beta(a\ c\ b)^{-1} = (c\ a)(b\ d)$ in H liegen. Dieses stimmt nicht mit β überein. Damit hätte H mehr als sechs Elemente. □

Zuletzt soll ein Satz bewiesen werden, der einige interessante Anwendungen besitzt. Die Beweistechnik ist hervorzuheben. Diese besteht darin, dass die gegebene Gruppe G als Untergruppe von S_G via Linksmultiplikation betrachtet werden. Das bedeutet, dass man wie im Satz von Cayley (Satz 3.1) den injektiven Homomorphismus $G \to S_G$, der jedem $g \in G$ die Bijektion $g(.) : G \to G, x \mapsto gx$ von G zuordnet, betrachtet. Das Bild unter diesem Homomorphismus ist eine Untergruppe von S_G, die isomorph mit G ist. Am Zyklentyp in der Elemente von S_G kann man dann mit Satz 3.8 ablesen, ob es sich um eine gerade oder eine ungerade Permutation in S_G handelt. Im Anschluss an den Beweis des Satzes wird an den Gruppen A_4 und C_{12} exemplarisch die Aussage des Satzes verdeutlicht.

Satz 3.14. *Sei G eine Gruppe mit Ordnung $|G| = 2^m k$, wobei k ungerade sein soll; wenn G ein Element mit Ordnung 2^m hat, dann bilden die Elemente von G mit ungerader Ordnung einen nicht trivialen Normalteiler von G.*

Beweis. Man betrachte die gegebene Gruppe G als Untergruppe von S_G via Linksmultiplikation. Jedes Element g von G wird mit der Permutation $g : x \mapsto gx$ in S_G identifiziert und in Zyklenform notiert. Der Beweis wird zuerst für $m = 1$ und dann allgemein für beliebige $m \geq 1$ geführt.

1. Sei $m = 1$, das heißt die Ordnung der gegebenen Gruppe ist $|G| = 2k$. Es wird gezeigt (i) es existiert eine Untergruppe G_1, deren Ordnung $|G_1| = k$ ist; (ii) diese Untergruppe G_1 enthält genau die Elemente ungerader Ordnung; (iii) diese Untergruppe G_1 ist Normalteiler in G.

ad (i): Laut Voraussetzung existiert ein Element $a \in G$ mit $\mathrm{ord}(a) = 2$. Die Ordnung von a entspricht wie gezeigt genau der Zyklenlänge von a - aufgefasst

als Element in S_G. Weiters stimmt das Produkt aus Zyklenlänge und Zyklenanzahl mit der Ordnung der Gruppe G überein. Da die Ordnung der Gruppe $2k$ ist, ist das Element a in S_G ein Produkt aus k Zyklen der Länge 2; weil k laut Voraussetzung ungerade, ist nach Satz 3.8 a eine ungerade Permutation. Mit dieser ungeraden Permutation kann man Satz 3.7 anwenden und erhält genau k ungerade und k gerade Permutationen. Die geraden Permutationen bilden laut Lemma 3.6 eine Untergruppe mit Ordnung k, die im folgenden mit G_1 bezeichnet wird.

ad (ii): Diese Untergruppe G_1 enthält genau die Elemente ungerader Ordnung, denn sei b ein beliebiges Element mit $\text{ord}(b) = l$, dann stimmt, wie gehabt, die Zyklenlänge von b dargestellt als Element in S_G mit der Ordnung von b überein. Da die Ordnung von G mit $|G| = 2k$ nicht durch 4 teilbar ist, kann die Zyklenlänge und die Zyklenanzahl nicht gleichzeitig gerade sein. Es folgt mit Lemma 3.8: die Permutation b ist genau dann gerade in S_G, wenn die Zyklenlänge ungerade ist und genau dann ungerade in S_G, wenn die Zyklenlänge gerade ist. Die Untergruppe G_1 enthält (siehe (i)) k gerade Permutationen, die somit alle ungerade Ordnung haben.

ad (iii): Da genau die Hälfte der Elemente in G_1 liegen, ist der Index $[G : G_1]$ von G_1 in G gleich 2. Die Untergruppe G_1 ist daher ein Normalteiler in G. Für den Fall $m = 1$ ist die Aussage des Satzes also bewiesen.

2. Sei $m \geq 1$, so ist die Ordnung von G also $|G| = 2^m k$. Es wird gezeigt (i) es existiert eine Untergruppe G_m, deren Ordnung $|G_m| = k$ ist; (ii) diese Untergruppe G_m enthält genau die Elemente ungerader Ordnung; (iii) diese Untergruppe G_m ist Normalteiler in G.

ad (i): Man kreiere eine absteigende Folge von ineinander geschachtelten Untergruppen, die jeweils die geraden Permutationen der übergeordneten Gruppe enthalten, wobei die Untergruppen jeweils als Permutationsgruppe

der übergeordneten Gruppe aufgefasst werden.

	G	$\geq$	G_1	$\geq$	G_2	$\geq$	$\cdots$	$\geq$	G_{m-1}	$\geq$	G_m
Ordnung :	$2^m k$		$2^{m-1}k$		$2^{m-2}k$				$2^1 k$		k

Die Argumentation, dass es eine Untergruppe G_1 gibt, ist analog zu 1. ($m = 1$) geführt. Laut Voraussetzung des Satzes existiert ein Element $a \in G$ mit $\text{ord}(a) = 2^m$. Die Ordnung des Elements a entspricht genau der Zyklenlänge von a - aufgefasst als Element in S_G. Da die Zyklen alle disjunkt sind, gilt: das Produkt aus Zyklenlänge und Zyklenanzahl entspricht der Ordnung der Gruppe G. Da die Gruppe G $2^m k$ Elemente hat, ist das Element a in S_G ein Produkt aus k Zyklen der Länge 2^m; weil k laut Voraussetzung ungerade, ist nach Satz 3.8 a eine ungerade Permutation. Mit dieser ungeraden Permutation kann man Satz 3.7 anwenden und erhält genau $2^{m-1}k$ gerade und $2^{m-1}k$ ungerade Permutationen. Die geraden Permutationen bilden laut Lemma 3.6 eine Untergruppe G_1 mit Ordnung $2^{m-1}k$.

Bevor dieser Vorgang wiederholt werden kann, muss gezeigt werden, dass in der Untergruppe G_1 ein Element mit Ordnung 2^{m-1} existiert, das dann - aufgefasst als Element in S_{G_1} - aus k Zyklen der Länge 2^{m-1} besteht und somit eine ungerade Permutation in S_{G_1} darstellt, sodass die nächste Untergruppe aus geraden Permutationen analog zur übergeordneten Untergruppe gebildet werden kann. Da die Hälfte der Elemente von G in G_1 liegen, hat G_1 Index 2 in G. Daraus folgt, dass die Faktorgruppe G/G_1 von G nach G_1 isomorph zu $\mathbb{Z}_2$ ist. Für jedes $b \in G$ gilt (in der Faktorgruppe G/G_1), dass $G_1 = (bG_1)^2 = b^2 G_1$. Insbesondere folgt daraus, dass $b^2 \in G_1$ für jedes $b \in G$. Sei a ein Element aus G mit Ordnung 2^m, dann ist also $a^2 \in G_1$ und es gilt $a^{2^m} = 1$. Aus $a^{2^m} = (a^2)^{2^{m-1}}$ folgt, dass die Ordnung von a^2 gleich 2^{m-1} ist.

Die Folge der Untergruppen kann somit fortgesetzt und die Argumente können rekursiv wiederholt werden. Man betrachte also die gefundene Gruppe

G_1 mit Ordnung $2^{m-1}k$ (k ungerade) als Untergruppe von S_{G_1} via Linksmultiplikation. Die geraden Permutationen bilden eine Untergruppe G_2 usw.

ad (ii): In der Untergruppe G_1 liegen, wie gezeigt, jene Elemente aus G, die in S_G gerade Permutationen darstellen. Nach Satz 3.8 muss ein Element ungerader Ordnung eine gerade Permutation in S_G sein, also in G_1 liegen. Dies folgt auch aus folgendem unabhängigen Argument: sei $b \in G$, $b \notin G_1$. Wir betrachten $\langle b \rangle$, die von b erzeugte zyklische Untergruppe von G und den Quotientenhomomorphismus $\pi : G \to G/G_1$, eingeschränkt auf $\langle b \rangle$. Da $b \notin G_1$ ist $\pi(\langle b \rangle) = \langle bG_1 \rangle$. Aus dem Homomorphiesatz folgt $|\langle b \rangle| = |\mathrm{Ker}(\pi|_{\langle b \rangle})| \cdot |\langle bG_1 \rangle|$. Wegen $2 = |\langle bG_1 \rangle|$ gilt also $2 \mid |\langle b \rangle| = \mathrm{ord}(b)$. Ein Element mit ungerader Ordnung kann daher nicht außerhalb von G_1 liegen.

Diese Argumente werden rekursiv auf die Folge der verschachtelten Untergruppen angewendet. Die innerste dieser Untergruppen G_m enthält dann nur mehr die Elemente ungerader Ordnung.

ad (iii): Bleibt zu zeigen, dass $G_m \trianglelefteq G$: die Untergruppe G_m bestehend aus der Menge aller Elemente ungerader Ordnung, ist sogar eine charakteristische Untergruppe von G, da die Ordnung eines Elements unter jedem Automorphismus also insbesondere unter jeder Konjugation invariant ist. Daraus folgt die Normalteiler-Eigenschaft von G_m in G.

□

Nachstehend werde ich in Anlehnung an den soeben gegebenen Beweis des Satzes 3.14 illustrieren, dass die zyklische Gruppe C_{12} eine Untergruppe der Elemente ungerader Ordnung hat.

Die Gruppe C_{12} besitzt mit den beiden Elementen x^3 und x^9, die beide Ordnung 4 haben, ungerade Permutationen in $S_{C_{12}}$. (Siehe Tabelle 3.4). Die Gruppe C_{12} hat eine Untergruppe G_1 mit den geraden Permutationen in S_{G_1} (siehe Tabelle 3.5), die selbst, wieder betrachtet als Untergruppe von S_{G_1}, das

$x \in G$	ord(x) $= l$ in S_G	# Zyklen in S_G	l in S_G gerade ungerade	# in S_G gerade ungerade	sgn(x)
1	1	3	U	U	+1
x	12	1	G	U	-1
x^2	6	1	G	U	-1
x^3	4	3	G	U	-1
x^4	3	1	U	U	+1
x^5	12	1	G	U	-1
x^6	2	3	G	U	-1
x^7	12	1	G	U	-1
x^8	3	1	U	U	+1
x^9	4	3	G	U	-1
x^{10}	6	1	G	U	-1
x^{11}	12	1	G	U	-1

Tabelle 3.4: $G = C_{12}$ aufgefasst als Untergruppe von $S_{C_{12}}$

Element x^6 mit Ordnung 2 beinhaltet, eine ungerade Permutation. Die geraden Permutationen von G_1 bilden selbst wieder eine Untergruppe G_2 (siehe Tabelle 3.6).

Tabelle 3.7 zeigt ebenfalls das aus dem Zyklentyp sich ergebende Signum der Elemente der alternierenden Gruppe A_4. Man sieht, dass A_4 klarerweise keine ungeraden Permutationen in S_{A_4} enthält. Sie besitzt kein Element mit Ordnung 4, das mit einer gerade Zyklenlänge und einer ungerade Zyklenanzahl $\# = 3$ notwendigerweise ungerade wäre. Die Elemente mit Ordnung 3 bilden daher keinen Normalteiler.

Der Beweis von Satz 3.14 zeigt, dass mit der Betrachtung der Gruppe als treue Gruppenwirkung, die Gruppe als Untergruppe der Permutationsgruppe

$x \in G$	ord(x) $= l$ in S_G	# Zyklen in S_G	l in S_G gerade ungerade	# in S_G gerade ungerade	sgn(x)
1	1	3	U	U	+1
x^2	6	1	G	U	-1
x^4	3	1	U	U	+1
x^6	2	3	G	U	-1
x^8	3	1	U	U	+1
x^{10}	6	1	G	U	-1

Tabelle 3.5: $G = G_1 \leq C_{12}$ aufgefasst als Untergruppe von S_{G_1}

$x \in G$	ord(x) $= l$ in S_G	# Zyklen in S_G	l in S_G gerade ungerade	# in S_G gerade ungerade	sgn(x)
1	1	3	U	U	+1
x^4	3	1	U	U	+1
x^8	3	1	U	U	+1

Tabelle 3.6: $G = G_2 \leq G_1 \leq C_{12}$ aufgefasst als Untergruppe von S_{G_2}

aufgefasst werden kann. Mit dem Zyklentyp der Elemente, aufgefasst als Elemente der Permutationsgruppe, erhält man das Signum und die Ordnung, die entscheidend sind bei der Ableitung der Aussage des Satzes. Es handelt sich also abschließend um ein elegantes Beispiel für den Nutzen von Gruppenwirkungen für die Beweisführung.

$x \in G$	ord(x) $= l$ in S_G	# Zyklen in S_G	l in S_G gerade oder ungerade	# in S_G gerade oder ungerade	sgn(x)
(1)	1	12	U	G	+1
(2 3 4)	3	4	U	G	+1
(2 4 3)	3	4	U	G	+1
(1 2)(3 4)	2	6	G	G	+1
(1 2 3)	3	4	U	G	+1
(1 2 4)	3	4	U	G	+1
(1 3 2)	3	4	U	G	+1
(1 3 4)	3	4	U	G	+1
(1 3)(2 4)	2	6	G	G	+1
(1 4 2)	3	4	U	G	+1
(1 4 3)	3	4	U	G	+1
(1 4)(2 3)	2	6	G	G	+1

Tabelle 3.7: $G = A_4$ aufgefasst als Untergruppe von S_{A_4}

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] Armstrong, Mark A.: *Groups and Symmetry (Undergraduate Texts in Mathematics)*. Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2nd edition, January 1988. 14, 32

[2] Cigler, Johann: *Körper - Ringe - Gleichungen*. Spektrum Akademischer Verlag, 1995. 66, 85

[3] Fischer, Gerd: *Lehrbuch der Algebra: Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern*. Vieweg+Teubner, 1. Auflage, 2008. 14, 32

[4] The GAP Group: *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008. `http://www.gap-system.org`. 8, 11

[5] Hungerford, Thomas W.: *Algebra (Graduate Texts in Mathematics)*. Springer, January 1996. 32, 54

[6] Ledermann, Walter: *Einführung in die Gruppentheorie*. Vieweg Friedr. + Sohn Verlag, September 1996. 66

[7] Norman Hendrich, University of Hamburg, Department of Informatics: *jfig, Tutorial and User-Guide, Version 3.08*, 2006. `http://tams-www.informatik.uni-hamburg.de/applets/jfig`. 11

[8] Robinson, Derek J.S.: *A Course in the Theory of Groups: 2nd Ed.* Secaucus, New Jersey, U.S.A.: Springer Verlag, 2nd edition edition, 1996. 66

[9] Rosebrock, Stephan: *Geometrische Gruppentheorie.* Vieweg+Teubner Verlag, Januar 2004. 8

[10] Rotman, Joseph J.: *Theory of Groups: An Introduction, 2nd ed.* Allyn and Bacon, 2nd edition, 1973. 66

[11] Wolfart, Jürgen: *Vieweg Studium, Nr.86, Einführung in die Zahlentheorie und Algebra.* Vieweg Verlagsgesellschaft, September 1996. 14

Anhang A

GAP-Code

A.1 Beispiele zu Abschnitt 2.1

Die Permutationsgruppe S_3 wirkt auf sich selbst durch Rechtsmultiplikation

```
gap> S3:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> Elements(S3);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> Size(S3);
6
gap> IsAbelian(S3);
false
gap> E_S3:=Elements(S3);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> OrbitStabilizer(S3,E_S3[1],OnRight);
rec( orbit := [ (), (1,2,3), (1,2), (1,3,2), (2,3),
    (1,3) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(S3,E_S3[2],OnRight);
rec( orbit := [ (2,3), (1,2), (1,2,3), (1,3), (),
    (1,3,2) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(S3,E_S3[3],OnRight);
rec( orbit := [ (1,2), (1,3), (), (2,3), (1,3,2),
    (1,2,3) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(S3,E_S3[4],OnRight);
```

```
rec( orbit := [ (1,2,3), (1,3,2), (2,3), (), (1,3),
    (1,2) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(S3,E_S3[5],OnRight);
rec( orbit := [ (1,3,2), (), (1,3), (1,2,3), (1,2),
    (2,3) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(S3,E_S3[6],OnRight);
rec( orbit := [ (1,3), (2,3), (1,3,2), (1,2), (1,2,3),
    () ],
  stabilizer := Group(()) )
gap> IsTransitive(S3,S3,OnRight);
true
gap> IsRegular(S3,S3,OnRight);
true
```

Die alternierende Gruppe A_4 wirkt auf sich selbst durch Rechtsmultiplikation

```
gap> g:=Group((1,3,2),(2,4,3));
Group([ (1,3,2), (2,4,3) ])
gap> Size(g);
12
gap> Elements(g);
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4),
    (1,3,2), (1,3,4),
  (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
gap> A4:=AlternatingGroup(4);
Alt( [ 1 .. 4 ] )
```

```
gap> IsomorphismGroups(g,A4);
[ (1,3,2), (2,4,3) ] -> [ (1,2,3), (2,3,4) ]
gap> IsSimple(A4);
false
gap> IsAbelian(A4);
false
gap> E_A4:=Elements(A4);
E_A4:=Elements(A4);
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4),
  (1,3,2), (1,3,4),
  (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
gap> OrbitStabilizer(A4,E_A4[1],OnRight);
rec( orbit := [ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),
  (2,4,3), (1,4,2),
    (1,2,3), (1,3,4), (2,3,4), (1,3,2), (1,4,3),
      (1,2,4) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[2],OnRight);
rec( orbit := [ (2,3,4), (1,2,4), (1,3,2), (1,4,3), (),
  (1,4)(2,3), (1,2)(3,4),
    (1,3)(2,4), (2,4,3), (1,3,4), (1,4,2), (1,2,3) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[3],OnRight);
rec( orbit := [ (2,4,3), (1,2,3), (1,3,4), (1,4,2),
  (2,3,4), (1,4,3),
    (1,2,4), (1,3,2), (), (1,3)(2,4), (1,4)(2,3),
      (1,2)(3,4) ],
```

```
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[3],OnRight);
rec( orbit := [ (2,4,3), (1,2,3), (1,3,4), (1,4,2),
   (2,3,4), (1,4,3),
       (1,2,4), (1,3,2), (), (1,3)(2,4), (1,4)(2,3),
          (1,2)(3,4) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[4],OnRight);
rec( orbit := [ (1,2)(3,4), (), (1,4)(2,3), (1,3)(2,4),
   (1,4,2), (2,4,3),
       (1,3,4), (1,2,3), (1,3,2), (2,3,4), (1,2,4),
          (1,4,3) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[5],OnRight);
rec( orbit := [ (1,2,3), (2,4,3), (1,4,2), (1,3,4),
   (1,4,3), (2,3,4),
       (1,3,2), (1,2,4), (1,3)(2,4), (), (1,2)(3,4),
          (1,4)(2,3) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[6],OnRight);
rec( orbit := [ (1,2,4), (2,3,4), (1,4,3), (1,3,2),
   (1,4)(2,3), (), (1,3)(2,4),
       (1,2)(3,4), (1,3,4), (2,4,3), (1,2,3), (1,4,2) ],
  stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[7],OnRight);
rec( orbit := [ (1,3,2), (1,4,3), (2,3,4), (1,2,4),
   (1,2)(3,4), (1,3)(2,4),
```

```
        (), (1,4)(2,3), (1,4,2), (1,2,3), (2,4,3),
           (1,3,4) ],
   stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[8],OnRight);
rec( orbit := [ (1,3,4), (1,4,2), (2,4,3), (1,2,3),
    (1,2,4), (1,3,2),
        (2,3,4), (1,4,3), (1,4)(2,3), (1,2)(3,4), (),
           (1,3)(2,4) ],
   stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[9],OnRight);
rec( orbit := [ (1,3)(2,4), (1,4)(2,3), (), (1,2)(3,4),
    (1,2,3), (1,3,4),
        (2,4,3), (1,4,2), (1,4,3), (1,2,4), (2,3,4),
           (1,3,2) ],
   stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[10],OnRight);
rec( orbit := [ (1,4,2), (1,3,4), (1,2,3), (2,4,3),
    (1,3,2), (1,2,4),
        (1,4,3), (2,3,4), (1,2)(3,4), (1,4)(2,3),
           (1,3)(2,4), () ],
   stabilizer := Group(()) )
gap> OrbitStabilizer(A4,E_A4[11],OnRight);
rec( orbit := [ (1,4,3), (1,3,2), (1,2,4), (2,3,4),
    (1,3)(2,4), (1,2)(3,4),
        (1,4)(2,3), (), (1,2,3), (1,4,2), (1,3,4),
           (2,4,3) ],
   stabilizer := Group(()) )
```

```
gap> OrbitStabilizer(A4,E_A4[12],OnRight);
rec( orbit := [ (1,4)(2,3), (1,3)(2,4), (1,2)(3,4), (),
    (1,3,4), (1,2,3),
        (1,4,2), (2,4,3), (1,2,4), (1,4,3), (1,3,2),
            (2,3,4) ],
   stabilizer := Group(()) )
gap> IsTransitive(A4,A4,OnRight);
true
gap> IsRegular(A4,A4,OnRight);
true
```

A.2 Beispiele zu Abschnitt 2.2

Konjugiertenklassen, Zentralisatoren und Zentrum von der Permutationsgruppe S_3

```
gap> S3:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> Elements(S3);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> Size(S3);
6
gap> Orbit(S3,(1,2));
[ (1,2), (2,3), (1,3) ]
gap> Orbit(S3,(1));
[ 1, 3, 2 ]
gap> Orbit(S3,(1,3));
[ (1,3), (1,2), (2,3) ]
gap> Orbit(S3,(2,3));
[ (2,3), (1,3), (1,2) ]
gap> Orbit(S3,(1,2,3));
[ (1,2,3), (1,3,2) ]
gap> Orbit(S3,(1,3,2));
[ (1,3,2), (1,2,3) ]
gap> C_S3:=ConjugacyClasses(S3);
[ ()^G, (1,2)^G, (1,2,3)^G ]
gap> List(C_S3, i -> Elements(i));
[ [ () ], [ (2,3), (1,2), (1,3) ], [ (1,2,3), (1,3,2) ]
  ]
gap> List(C_S3, i -> Size(i));
```

```
[ 1, 3, 2 ]
gap> Cent_S3:=Centralizer(S3,(1,2));
Group([ (1,2) ])
gap> Elements(Cent_S3);
[ (), (1,2) ]
gap> Cent_S3:=Centralizer(S3,(1,3));
Group([ (1,3) ])
gap> Elements(Cent_S3);
[ (), (1,3) ]
gap> Cent_S3:=Centralizer(S3,(2,3));
Group([ (2,3) ])
gap> Elements(Cent_S3);
[ (), (2,3) ]
gap> Cent_S3:=Centralizer(S3,(1,2,3));
Group([ (1,2,3) ])
gap> Elements(Cent_S3);
[ (), (1,2,3), (1,3,2) ]
gap> Cent_S3:=Centralizer(S3,(1,3,2));
Group([ (1,3,2) ])
gap> Elements(Cent_S3);
[ (), (1,2,3), (1,3,2) ]
gap> Cent_S3:=Centralizer(S3,());
Group([ (1,3), (2,3) ])
gap> Elements(Cent_S3);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> Z_S3:=Centre(S3);
Group(())
```

```
gap> Size(Z_S3);
1
gap> Elements(Z_S3);
[ () ]
```

Konjugiertenklassen, Zentralisatoren und Zentrum von der zyklischen Gruppe C_3

```
gap> C3:=CyclicGroup(3);
<pc group of size 3 with 1 generators>
gap> Elements(C3);
[ <identity> of ..., f1, f1^2 ]
gap> Size(C3);
3
gap> E_C3:=Elements(C3);
[ <identity> of ..., f1, f1^2 ]
gap> Orbit(C3,E_C3[1]);
[ <identity> of ... ]
gap> Orbit(C3,E_C3[2]);
[ f1 ]
gap> Orbit(C3,E_C3[3]);
[ f1^2 ]
gap> C_C3:=ConjugacyClasses(C3);
[ <identity> of ...^G, f1^G, f1^2^G ]
gap> Elements(C_C3[1]);
[ <identity> of ... ]
gap> List(C_C3, i -> Elements(i));
[ [ <identity> of ... ], [ f1 ], [ f1^2 ] ]
gap> List(C_C3, i -> Size(i));
```

```
[ 1, 1, 1 ]
gap> Cent_C3:=Centralizer(C3,E_C3[1]);
<pc group of size 3 with 1 generators>
gap> Elements(Cent_C3);
[ <identity> of ..., f1, f1^2 ]
gap> Cent_C3:=Centralizer(C3,E_C3[2]);
<pc group of size 3 with 1 generators>
gap> Elements(Cent_C3);
[ <identity> of ..., f1, f1^2 ]
gap> Cent_C3:=Centralizer(C3,E_C3[3]);
<pc group of size 3 with 1 generators>
gap> Elements(Cent_C3);
[ <identity> of ..., f1, f1^2 ]
gap> Z_C3:=Centre(C3);
<pc group of size 3 with 1 generators>
gap> Size(Z_C3);
3
gap> Elements(Z_C3);
[ <identity> of ..., f1, f1^2 ]
```

Konjugiertenklassen, Zentralisatoren und Zentrum von der alternierenden Gruppe A_4

```
gap> A4:=AlternatingGroup(4);
Alt( [ 1 .. 4 ] )
gap> E_A4:=Elements(A4);
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4),
  (1,3,2),
  (1,3,4), (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
```

```
gap> i:=1;
1
gap> for i  in [1..12]  do
> Print( i, " " );
> Print(Elements(Centralizer(A4,E_A4[i])));
> Print( "   " );
> Print(Size(Centralizer(A4,E_A4[i])));
> Print("\n");
> i:=i+1;
> od;
1 [ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4),
   (1,3,2),
   (1,3,4), (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
      12
2 [ (), (2,3,4), (2,4,3) ]    3
3 [ (), (2,3,4), (2,4,3) ]    3
4 [ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    4
5 [ (), (1,2,3), (1,3,2) ]    3
6 [ (), (1,2,4), (1,4,2) ]    3
7 [ (), (1,2,3), (1,3,2) ]    3
8 [ (), (1,3,4), (1,4,3) ]    3
9 [ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    4
10 [ (), (1,2,4), (1,4,2) ]    3
11 [ (), (1,3,4), (1,4,3) ]    3
12 [ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    4
gap> i:=1;
1
```

```
gap> for i  in [1..12]  do
> Print( i, " " );
> Print(Elements(Orbit(A4,E_A4[i])));
> Print( "    " );
> Print(Size(Orbit(A4,E_A4[i])));
> Print("\n");
> i:=i+1;
> od;
1 [ () ]    1
2 [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ]    4
3 [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ]    4
4 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    3
5 [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ]    4
6 [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ]    4
7 [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ]    4
8 [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ]    4
9 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    3
10 [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ]    4
11 [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ]    4
12 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    3
gap> ConjugacyClasses(A4);
[ ()^G, (1,2)(3,4)^G, (1,2,3)^G, (1,2,4)^G ]
gap> Elements(ConjugacyClasses(A4));
[ ()^G, (1,2,4)^G, (1,2,3)^G, (1,2)(3,4)^G ]
gap> List(ConjugacyClasses(A4), i -> Elements(i));
[ [ () ], [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ],
  [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ],
```

```
  [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ] ]
gap> List(ConjugacyClasses(A4), i -> Size(i));
[ 1, 3, 4, 4 ]
                                                    ^
gap> Elements(Centre(A4)); Size(Centre(A4));
[ () ]
1
```

Konjugiertenklassen, Zentralisatoren und Zentrum von der alternierenden Gruppe A_5

```
gap> A5:=AlternatingGroup(5);
Alt( [ 1 .. 5 ] )
gap> E_A5:=Elements(A5);
[ (), (3,4,5), (3,5,4), (2,3)(4,5), (2,3,4), (2,3,5),
    (2,4,3),
  (2,4,5), (2,4)(3,5), (2,5,3), (2,5,4), (2,5)(3,4),
      (1,2)(4,5),
  (1,2)(3,4), (1,2)(3,5), (1,2,3), (1,2,3,4,5),
      (1,2,3,5,4),
  (1,2,4,5,3), (1,2,4), (1,2,4,3,5), (1,2,5,4,3),
      (1,2,5),
  (1,2,5,3,4), (1,3,2), (1,3,4,5,2), (1,3,5,4,2),
      (1,3)(4,5),
  (1,3,4), (1,3,5), (1,3)(2,4), (1,3,2,4,5),
      (1,3,5,2,4),
  (1,3)(2,5), (1,3,2,5,4), (1,3,4,2,5), (1,4,5,3,2),
      (1,4,2),
```

```
  (1,4,3,5,2), (1,4,3), (1,4,5), (1,4)(3,5),
     (1,4,5,2,3),
  (1,4)(2,3), (1,4,2,3,5), (1,4,2,5,3), (1,4,3,2,5),
     (1,4)(2,5),
  (1,5,4,3,2), (1,5,2), (1,5,3,4,2), (1,5,3), (1,5,4),
  (1,5)(3,4), (1,5,4,2,3), (1,5)(2,3), (1,5,2,3,4),
     (1,5,2,4,3),
   (1,5,3,2,4), (1,5)(2,4) ]

gap> i:=1;
1
gap> for i in [1..60] do
> Print( i, " " );
> Print(Elements(Centralizer(A5,E_A5[i])));
> Print( "   " );
> Print(Size(Centralizer(A5,E_A5[i])));
> Print("\n");
> i:=i+1;
> od;
gap> i:=1;
1
gap> for i in [1..60] do
> Print( i, " " );
> Print(Elements(Orbit(A5,E_A5[i])));
> Print( "   " );
> Print(Size(Orbit(A5,E_A5[i])));
> Print("\n");
```

```
> i:=i+1;
> od;


gap> ConjugacyClasses(A5);
[ ()^G, (1,2)(3,4)^G, (1,2,3)^G, (1,2,3,4,5)^G,
    (1,2,3,5,4)^G ]
gap> Elements(ConjugacyClasses(A5);
Syntax error: ) expected in *errin* line 91
Elements(ConjugacyClasses(A5);
                                 ^
gap> Elements(ConjugacyClasses(A5));
[ ()^G, (1,2,3)^G, (1,2)(3,4)^G, (1,2,3,4,5)^G,
    (1,2,3,5,4)^G ]
gap> List(ConjugacyClasses(A4), i -> Elements(i));
[ [ () ], [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ],
  [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ],
  [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ] ]
gap> List(ConjugacyClasses(A5), i -> Elements(i));
[ [ () ],
  [ (2,3)(4,5), (2,4)(3,5), (2,5)(3,4), (1,2)(4,5),
      (1,2)(3,4), (1,2)(3,5), (1,3)(4,5), (1,3)(2,4),
      (1,3)(2,5), (1,4)(3,5), (1,4)(2,3), (1,4)(2,5),
      (1,5)(3,4), (1,5)(2,3), (1,5)(2,4) ],
  [ (3,4,5), (3,5,4), (2,3,4), (2,3,5), (2,4,3),
    (2,4,5),
      (2,5,3), (2,5,4), (1,2,3), (1,2,4), (1,2,5),
        (1,3,2),
```

```
        (1,3,4), (1,3,5), (1,4,2), (1,4,3), (1,4,5),
            (1,5,2),
        (1,5,3), (1,5,4) ],
    [ (1,2,3,4,5), (1,2,4,5,3), (1,2,5,3,4), (1,3,5,4,2),
        (1,3,2,5,4), (1,3,4,2,5), (1,4,3,5,2),
            (1,4,5,2,3),
        (1,4,2,3,5), (1,5,4,3,2), (1,5,2,4,3),
            (1,5,3,2,4) ],
    [ (1,2,3,5,4), (1,2,4,3,5), (1,2,5,4,3), (1,3,4,5,2),
        (1,3,2,4,5), (1,3,5,2,4), (1,4,5,3,2),
            (1,4,2,5,3),
        (1,4,3,2,5), (1,5,3,4,2), (1,5,4,2,3),
            (1,5,2,3,4) ] ]
gap> List(ConjugacyClasses(A4), i -> Size(i));
[ 1, 3, 4, 4 ]
gap> List(ConjugacyClasses(A5), i -> Size(i));
[ 1, 15, 20, 12, 12 ]
gap> Elements(Centre(A5)); Size(Centre(A5));
[ () ]
1
```

Konjugiertenklassen, Zentralisatoren und Zentrum von der Permutatinsgruppe S_4

```
gap> S4:=SymmetricGroup(4);
Sym( [ 1 .. 4 ] )
gap> E_S4:=Elements(S4);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2),
  (1,2)(3,4),
```

```
   (1,2,3), (1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2),
      (1,3,4,2),
   (1,3), (1,3,4), (1,3)(2,4), (1,3,2,4), (1,4,3,2),
      (1,4,2),
   (1,4,3), (1,4), (1,4,2,3), (1,4)(2,3) ]

gap> i:=1;
1
gap> for i in [1..24] do
> Print( i, " " );
> Print(Elements(Centralizer(S4,E_S4[i])));
> Print( "    " );
> Print(Size(Centralizer(S4,E_S4[i])));
> Print("\n");
> od;
1 [ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2),
     (1,2)(3,4), (1,2,3), (1,2,3,4), (1,2,4,3), (1,2,4),
     (1,3,2), (1,3,4,2), (1,3), (1,3,4), (1,3)(2,4),
     (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4),
     (1,4,2,3), (1,4)(2,3) ]    24
2 [ (), (3,4), (1,2), (1,2)(3,4) ]    4
3 [ (), (2,3), (1,4), (1,4)(2,3) ]    4
4 [ (), (2,3,4), (2,4,3) ]    3
5 [ (), (2,3,4), (2,4,3) ]    3
6 [ (), (2,4), (1,3), (1,3)(2,4) ]    4
7 [ (), (3,4), (1,2), (1,2)(3,4) ]    4
8 [ (), (3,4), (1,2), (1,2)(3,4),
```

```
    (1,3)(2,4), (1,3,2,4), (1,4,2,3), (1,4)(2,3) ]    8
9 [ (), (1,2,3), (1,3,2) ]    3
10 [ (), (1,2,3,4), (1,3)(2,4), (1,4,3,2) ]    4
11 [ (), (1,2,4,3), (1,3,4,2), (1,4)(2,3) ]    4
12 [ (), (1,2,4), (1,4,2) ]    3
13 [ (), (1,2,3), (1,3,2) ]    3
14 [ (), (1,2,4,3), (1,3,4,2), (1,4)(2,3) ]    4
15 [ (), (2,4), (1,3), (1,3)(2,4) ]    4
16 [ (), (1,3,4), (1,4,3) ]    3
17 [ (), (2,4), (1,2)(3,4), (1,2,3,4),
     (1,3), (1,3)(2,4), (1,4,3,2), (1,4)(2,3) ]    8
18 [ (), (1,2)(3,4), (1,3,2,4), (1,4,2,3) ]    4
19 [ (), (1,2,3,4), (1,3)(2,4), (1,4,3,2) ]    4
20 [ (), (1,2,4), (1,4,2) ]    3
21 [ (), (1,3,4), (1,4,3) ]    3
22 [ (), (2,3), (1,4), (1,4)(2,3) ]    4
23 [ (), (1,2)(3,4), (1,3,2,4), (1,4,2,3) ]    4
24 [ (), (2,3), (1,2)(3,4), (1,2,4,3),
     (1,3,4,2), (1,3)(2,4), (1,4), (1,4)(2,3) ]    8
```

```
gap> i:=1;
1
gap> for i in [1..24] do
> Print( i, " " );
> Print(Elements(Orbit(S4,E_S4[i])));
```

```
> Print( "    " );
> Print(Size(Orbit(S4,E_S4[i])));
> Print("\n");
> od;
1 [ () ]    1
2 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]    6
3 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]    6
4 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
    (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
5 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
    (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
6 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]    6
7 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]    6
8 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    3
9 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
    (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
10 [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
     (1,3,2,4), (1,4,3,2), (1,4,2,3) ]    6
11 [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
     (1,3,2,4), (1,4,3,2), (1,4,2,3) ]    6
12 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
     (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
13 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
     (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
14 [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
     (1,3,2,4), (1,4,3,2), (1,4,2,3) ]    6
15 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]    6
```

```
16 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
     (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
17 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    3
18 [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
     (1,3,2,4), (1,4,3,2), (1,4,2,3) ]    6
19 [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
     (1,3,2,4), (1,4,3,2), (1,4,2,3) ]    6
20 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
     (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
21 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
     (1,3,2), (1,3,4), (1,4,2), (1,4,3) ]    8
22 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]    6
23 [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
     (1,3,2,4), (1,4,3,2), (1,4,2,3) ]    6
24 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]    3
```

```
gap> ConjugacyClasses(S4);
[ ()^G, (1,2)^G, (1,2)(3,4)^G, (1,2,3)^G, (1,2,3,4)^G ]
gap> Elements(ConjugacyClasses(S4));
[ ()^G, (1,2)^G, (1,2,3)^G, (1,2)(3,4)^G, (1,2,3,4)^G ]
gap> List(ConjugacyClasses(S4), i -> Size(i));
[ 1, 6, 3, 8, 6 ]
gap> List(ConjugacyClasses(S4), i -> Elements(i));
[ [ () ], [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ],
  [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ],
  [ (2,3,4), (2,4,3), (1,2,3), (1,2,4),
```

```
      (1,3,2), (1,3,4), (1,4,2), (1,4,3) ],
   [ (1,2,3,4), (1,2,4,3), (1,3,4,2),
      (1,3,2,4), (1,4,3,2), (1,4,2,3) ] ]
gap> Elements(Centre(S4)); Size(Centre(S4));
[ () ]
1
```

A.3 Beispiele zu Abschnitt 2.3

Semidirektes Produkt $\mathbb{Z}_2 \rtimes \mathbb{Z}_3$ entspricht dem direkten Produkt $\mathbb{Z}_2 \times \mathbb{Z}_3$

```
gap> C3:=CyclicGroup(3);
<pc group of size 3 with 1 generators>
gap> C2:=CyclicGroup(2);
<pc group of size 2 with 1 generators>
gap> Aut_C2:=AutomorphismGroup(C2);
<group with 1 generators>
gap> Size(Aut_C2);
1
gap> Elements(Aut_C2);
[ IdentityMapping( <pc group of size 2 with 1
    generators> ) ]
gap> PHI:=GroupHomomorphismByImages(C3, Aut_C2,
GeneratorsOfGroup(C3), GeneratorsOfGroup(Aut_C2));
[ f1 ] -> [ [ f1 ] -> [ f1 ] ]
gap> Sem_C2_C3:=SemidirectProduct(C3,PHI,C2);
<pc group of size 6 with 2 generators>
gap> Dir_C2_C3:=DirectProduct(C2,C3);
<pc group of size 6 with 2 generators>
gap> IsomorphismGroups(Sem_C2_C3,Dir_C2_C3);
[ f2, f1 ] -> [ f1, f2 ]
```

Semidirektes Produkt $\mathbb{Z}_3 \rtimes \mathbb{Z}_2 \cong S_3$

```
gap> C3:=CyclicGroup(3);
<pc group of size 3 with 1 generators>
```

```
gap> C2:=CyclicGroup(2);
<pc group of size 2 with 1 generators>
gap> Aut_C3:=AutomorphismGroup(C3);
<group with 1 generators>
gap> GeneratorsOfGroup(C3);
[ f1 ]
gap> GeneratorsOfGroup(Aut_C3);
[ [ f1 ] -> [ f1^2 ] ]
gap> Elements(Aut_C3);
[ IdentityMapping( <pc group of size 3 with 1
    generators> ),
  [ f1 ] -> [ f1^2 ] ]
gap> Size(Aut_C3);
2
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C3,
GeneratorsOfGroup(C2), GeneratorsOfGroup(Aut_C3));
[ f1 ] -> [ [ f1 ] -> [ f1^2 ] ]
gap> Sem_C3_C2:=SemidirectProduct(C2,PHI,C3);
<pc group of size 6 with 2 generators>
gap> Dir_C2_C3:=DirectProduct(C2,C3);
<pc group of size 6 with 2 generators>
gap> IsomorphismGroups(Sem_C3_C2,Dir_C2_C3);
fail
gap> S3:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> IsomorphismGroups(Sem_C3_C2,S3);
[ f1, f2 ] -> [ (2,3), (1,2,3) ]
```

Semidirektes Produkt $\mathbb{Z}_7 \rtimes \mathbb{Z}_2 \cong D_7$

```
gap> C2:=CyclicGroup(2);
<pc group of size 2 with 1 generators>
gap> GeneratorsOfGroup(C2);
[ f1 ]
gap> C7:=CyclicGroup(7);
<pc group of size 7 with 1 generators>
gap> Aut_C7:=AutomorphismGroup(C7);
<group with 1 generators>
gap> E_AutC7:=Elements(Aut_C7);
[ IdentityMapping( <pc group of size 7 with 1
    generators> ),
  Pcgs([ f1 ]) -> [ f1^2 ], [ f1 ] -> [ f1^3 ], Pcgs([
      f1 ]) -> [ f1^4 ],
  Pcgs([ f1 ]) -> [ f1^5 ], Pcgs([ f1 ]) -> [ f1^6 ] ]
gap> Size(Aut_C7);
6
gap> GeneratorsOfGroup(Aut_C7);
[ [ f1 ] -> [ f1^3 ] ]
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C7,
     Gen_C2,[E_AutC7[1]]);
[ f1 ] -> [ IdentityMapping( <pc group of size 7 with 1
    generators> ) ]
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C7,
     Gen_C2,[E_AutC7[2]]);
fail
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C7,
```

```
    Gen_C2,[E_AutC7[3]]);
fail
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C7,
    Gen_C2,[E_AutC7[4]]);
fail
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C7,
    Gen_C2,[E_AutC7[5]]);
fail
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C7,
    Gen_C2,[E_AutC7[6]]);
[ f1 ] -> [ Pcgs([ f1 ]) -> [ f1^6 ] ]
gap> SemDir:=SemidirectProduct(C2,PHI,C7);
<pc group of size 14 with 2 generators>
gap> Elements(SemDir);
[ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2,
  f2^3, f1*f2^3, f2^4,
  f1*f2^4, f2^5, f1*f2^5, f2^6, f1*f2^6 ]
gap> Size(SemDir);
14
gap> D14:=DihedralGroup(14);
<pc group of size 14 with 2 generators>
gap> IsomorphismGroups(SemDir,D14);
[ f1, f2 ] -> [ f1, f2 ]
gap> NormalSubgroups(D14);
[ Group([ ]), Group([ f2 ]), <pc group of size 14 with
  2 generators> ]
gap> List(Elements(NormalSubgroups(D14)),Elements);
```

```
[ [ <identity> of ... ],
  [ <identity> of ..., f2, f2^2, f2^3, f2^4, f2^5, f2^6
    ],
  [ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2,
    f2^3, f1*f2^3, f2^4,
     f1*f2^4, f2^5, f1*f2^5, f2^6, f1*f2^6 ] ]
gap> List(Elements(NormalSubgroups(D14)),Size);
[ 1, 7, 14 ]
```

Semidirektes Produkt von $\mathbb{Z}_5 \rtimes \mathbb{Z}_2 \cong D_5$

```
gap> C2:=CyclicGroup(2);
<pc group of size 2 with 1 generators>
C5:=CyclicGroup(5);
<pc group of size 5 with 1 generators>
gap> Aut_C5:=AutomorphismGroup(C5);
<group with 1 generators>
gap> GeneratorsOfGroup(Aut_C5);
[ [ f1 ] -> [ f1^2 ] ]
gap> E_AutC5:=Elements(Aut_C5);
[ IdentityMapping( <pc group of size 5 with 1
   generators> ),
  [ f1 ] -> [ f1^2 ], Pcgs([ f1 ]) -> [ f1^3 ], Pcgs([
    f1 ]) -> [ f1^4 ] ]
gap> Size(Aut_C5);
4
gap> PHI:=GroupHomomorphismByImages(C2, Aut_C5,
    Gen_C2,[E_AutC5[4]]);
[ f1 ] -> [ Pcgs([ f1 ]) -> [ f1^4 ] ]
```

```
gap> SemDir:=SemidirectProduct(C2,PHI,C5);
<pc group of size 10 with 2 generators>
gap> Elements(SemDir);
[ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2,
    f2^3, f1*f2^3, f2^4,
  f1*f2^4 ]
gap> Size(SemDir);
10
gap> D10:=DihedralGroup(10);
<pc group of size 10 with 2 generators>
gap> IsomorphismGroups(SemDir,D10);
[ f1, f2 ] -> [ f1, f2 ]
gap> List(Elements(NormalSubgroups(D10)),Size);
[ 1, 5, 10 ]
gap> List(Elements(NormalSubgroups(D10)),Elements);
[ [ <identity> of ... ], [ <identity> of ..., f2, f2^2,
    f2^3, f2^4 ],
  [ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2,
      f2^3, f1*f2^3, f2^4,
      f1*f2^4 ] ]
```

A.4 Beispiele zu Abschnitt 2.4

p-Sylow-Gruppen der Permutationsgruppe S_4

```
gap> S4:=SymmetricGroup(4);;
gap> Size(S4);
24
gap> Elements(S4);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2),
  (1,2)(3,4), (1,2,3),
  (1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2), (1,3,4,2),
    (1,3), (1,3,4),
  (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3),
    (1,4), (1,4,2,3),
  (1,4)(2,3) ]
gap> SYL4_2:=SylowSubgroup(S4,2);
Group([ (1,2), (3,4), (1,3)(2,4) ])
gap> Size(SYL4_2);
8
gap> Elements(SYL4_2);
[ (), (3,4), (1,2), (1,2)(3,4), (1,3)(2,4), (1,3,2,4),
  (1,4,2,3), (1,4)(2,3) ]
gap> N:=Normalizer(S4,SYL4_2);
Group([ (1,4)(2,3), (3,4), (1,2) ])
gap> Size(N);
8
gap> Elements(N);
[ (), (3,4), (1,2), (1,2)(3,4), (1,3)(2,4), (1,3,2,4),
  (1,4,2,3), (1,4)(2,3) ]
```

```
gap> Index(S4,N);
3
gap> SYL4_3:=SylowSubgroup(S4,3);
Group([ (1,2,3) ])
gap> Size(SYL4_3);
3
gap> Elements(SYL4_3);
[ (), (1,2,3), (1,3,2) ]
gap> N:=Normalizer(S4,SYL4_3);
Group([ (1,2,3), (2,3) ])
gap> Size(N);
6
gap> Elements(N);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> Index(S4,N);
4
```

p-Sylow-Gruppen der Permutationsgruppe S_5

```
gap> S5:=SymmetricGroup(5);;
gap> P3:=Subgroup(S5,[ (2,3,4), (2,4,3)]);
Group([ (2,3,4), (2,4,3) ])
gap> Size(P3);
3
gap> N3:=Normalizer(S5,P3);
Group([ (2,3,4), (1,5), (3,4) ])
gap> Elements(N3);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,5),
  (1,5)(3,4), (1,5)(2,3),(1,5)(2,3,4), (1,5)(2,4,3),
```

```
    (1,5)(2,4) ]
 gap> Size(N3);
12
gap> Index(S5,N3);
10

gap> S5:=SymmetricGroup(5);;
gap> SYL5_2:=SylowSubgroup(S5,2);;
gap> Size(SYL5_2);
8
gap> Elements(SYL5_2);
[ (), (3,4), (1,2), (1,2)(3,4), (1,3)(2,4), (1,3,2,4),
    (1,4,2,3), (1,4)(2,3) ]
gap> N:=Normalizer(S5,SYL5_2);
Group([ (1,4)(2,3), (3,4), (1,2) ])
gap> Index(S5,N);
15
```

Anhang B

Zusammenfassung

Thema dieser Diplomarbeit sind Gruppen und ihre Wirkungen. Gruppenwirkungen beruhen auf der Idee, dass jedes Element einer Gruppe G eine Bijektion von einer Menge X auf sich definiert und zwar so, dass das Einselement 1 von G die identische Abbildung definiert und die Gruppenoperation der Hintereinanderausführung von Abbildungen entspricht. Die Bahn O_x eines Elements bezüglich einer Gruppenwirkung ist die Menge aller Bilder von x unter dieser Wirkung von G. Die Bahnen liefern eine Zerlegung von X in paarweise disjunkte Teilmengen von X. Der Stabilisator G_x eines Elements x enthält jene Gruppenelemente aus G, die x invariant lassen. Es gilt die fundamentale Bahn-Stabilisator-Gleichung:

$$|O_x| \cdot |G_x| = |G|.$$

Daraus ergibt sich die allgemeine Klassengleichung

$$|X| = |X_0| + \sum_{i=1}^{l} [G : G_{x_i}],$$

wobei X_0 genau aus den Elementen von X besteht, auf die alle Elemente von G die triviale Wirkung haben.

Neben der Erläuterung von Gruppenwirkungen liegt der zweite Schwerpunkt dieser Arbeit auf dem Beweis folgender gruppentheoretischer Resultate, die mit Hilfe des Konzepts der Gruppenwirkungen geführt werden.

- Nach dem Satz von Cauchy existiert zu jedem Primteiler p der Ordnung $|F|$ einer endlichen Gruppe F ein Element in F mit Ordnung p und folglich auch eine zyklische Untergruppe $U = \langle g \rangle$ mit $|U| = p$.

- Eine gegebene Gruppenwirkung einer Gruppe auf einer anderen durch Automorphismen definiert eine neue Gruppe, die semidirektes Produkt genannt wird. Ein derartiges semidirektes Produkt ist ein Spezialfall einer sogenannten Gruppenerweiterung. Abstrakt können semidirekte Produkte als "zerfallende Erweiterungen" charakterisiert werden.

- Die Sylow-Sätze geben Auskunft über eine hinreichende Bedingung für die Existenz von Untergruppen mit Primzahlpotenzordnung, sowie über deren Zusammenhang. Ferner liefern sie ein mächtiges Werkzeug, um sogenannte p-Sylow-Untergruppen und deren Anzahl praktisch zu bestimmen.

- Die alternierende Gruppe A_4 enthält keine Untergruppe mit Ordnung 6.

- Die alternierende Gruppe A_n ist für $n \geq 5$ einfach.

Anhang C

Abstract

The objective of this diploma thesis is to discuss the concept of groups acting on sets. An action of a group G on a set X is a homomorphism from G to the permutation group S_X. The set of all images under a given group-action of a specific point x is called the orbit O_x. The stabilizer G_x of an element x in X is the set of elements in G which leave x fixed. The orbit-stabilizer-theorem states the fundamental property:

$$|O_x| \cdot |G_x| = |G|.$$

This implies the general class equation

$$|X| = |X_0| + \sum_{i=1}^{l} [G : G_{x_i}]$$

where X_0 consists of all elements of X on which the whole group G is acting trivially (that is, X_0 is comprised of the fixed points of the action of G).

Apart from the explanation of group actions, the second focus of this thesis is to prove the following important results of group theory using the concept of group-actions.

- As a result of the Cauchy Theorem a finite group G contains an element

of prime order p if p divides the order G. In this case there exists a cyclic subgroup $U = \langle g \rangle$ with order $|U| = p$.

- An action of a group on another by automorphisms results in yet another group, the *semidirect product*. The class of these form a special case of group extensions. Abstractly, within the class of all extensions, splitting extensions are characterized as those coming form semidirect products.
- The Sylow theorems inform about sufficient conditions for the existence of subgroups having prime power order. Moreover it gives a powerful tool to determine the so-called p-Sylow-subgroups and to count them.
- The alternating group A_4 does not contain a subgroup of order 6.
- The alternating group A_n is simple, if $n \geq 5$.

Lebenslauf

Maria Kranzl

Persönliche Daten

Geburtsdatum: 29.2.1968
Geburtsort: Wien
Staatsangehörigkeit: Österreich

Ausbildung

1978–1986	Neusprachliches Gymnasium, Franklinstraße 26, 1210 Wien
1986–1989	Ausbildung zur Diplomkrankenschwester, Kaiserin Elisabeth Spital, 1150 Wien
1992–1995	Abendkolleg für EDV und Organisation, HTL-Spengergasse, 1050 Wien
Seit 2002	Studium Lehramt Mathematik und Informatik an der Universität Wien

---

Berufliche Tätigkeiten

1989–1994	Kaiserin Elisabeth Spital Intensivstation
1994–1995	Alcatel Austria Softwareentwicklung
1995–dato	Bank Austria Konzern verschiedenste EDV-Projekte