

Gruppen unter besonderer Berücksichtigung der Diedergruppen

Thorsten Riedl*

10. Juni 2002

*Facharbeit am Otto-Hahn-Gymnasium Marktredwitz

Inhaltsverzeichnis

Vorwort	iii
Einleitung	1
1 Definitionen und wichtige Eigenschaften von Gruppen	3
2 Untergruppen und Normalteiler	9
3 Nebenklassen und der Satz von Lagrange	10
4 Geometrische Anwendungen	12
4.1 Drehgruppen	12
4.2 Diedergruppen	13
4.2.1 Veranschaulichung an der Diedergruppe D_3	14
4.2.2 Veranschaulichung an der Diedergruppe D_5	15
4.3 Allgemeines über Untergruppen und Normalteiler von Diedergruppen . . .	19
5 Codierungstheorie	25
5.1 Allgemeine Einführung	25
5.1.1 Die ISBN-Codierung und Allgemeines über Prüfzeichencodierungen	26
5.2 Gruppen in der Codierungstheorie	28
5.2.1 Anwendung: Nummerierung der deutschen Geldscheine mit Hilfe von D_5	28
5.2.2 Überprüfen einer Kennnummer	30
6 Ausblick	32

Vorwort

Dieses Dokument wurde mit dem Textsatzprogramm $\text{T}_{\text{E}}\text{X}$ von Prof. Donald E. Knuth und den Erweiterungen $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$ und $\text{BIB}_{\text{E}}\text{X}$ erstellt, sämtliche Abbildungen wurden mit dem ebenfalls von Prof. Donald E. Knuth entwickelten $\text{M}_{\text{E}}\text{T}_{\text{A}}\text{P}_{\text{O}}\text{S}T$ erstellt. Darüberhinaus wurde auch das $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$ -Makrosystem der American Mathematical Society verwendet.

Einleitung

„The Theory of Groups is a branch of mathematics in which one does something to something and then compares the result with the result obtained from doing the same thing to something else, or something else to the same thing.“

James R. Newman in [7]

Die Idee der Gruppe spielt in vielen Naturwissenschaften eine Rolle; in der Physik zum Beispiel kann man mit Hilfe der Gruppentheorie auf Eigenfrequenzen von Molekülen, die um eine Gleichgewichtslage schwingen, schließen. Auch in der Codierungstheorie und in der Kryptographie gewinnt die Gruppentheorie immer mehr an Bedeutung. So codierte die Deutsche Bundesbank seit 1990 die Kennnummern ihrer Geldscheine mit Hilfe der Diedergruppe D_5 des regulären 5-Ecks und in der Kryptographie spielen elliptische Kurven eine wichtige Rolle bei der Verschlüsselung geheimer Daten.

Das Konzept der Gruppe ist in vielen Anwendungen wiederkehrend, und so mancher Physiker, der in seinen Forschungen auf eine Struktur stößt, die er als Gruppe auffassen kann, freut sich darüber, dass sich viele Mathematiker mit Gruppen auseinandergesetzt haben und er auf ihre Erkenntnisse zurückgreifen kann. Es dürfte ihm auch Freude bereiten, dass er diese Erkenntnisse allein mit der Tatsache der Erfüllung von vier Axiomen guten Gewissens verwenden kann. Hier ist es also sehr nützlich, dass wir eine Definition wählen, die „sehr wenige“ Forderungen stellt. Es ist natürlich auch klar, dass hiermit die von vielen Menschen gescholtene „zu hohe Abstraktion“ der Mathematik entsteht, die uns (und vor allem auch unserem Physiker) viele Vorteile beschert. Darüberhinaus findet die Gruppentheorie vielerlei Anwendung in der Lösung von mathematischen Knobeleyen; so lässt sich zum Beispiel mit Hilfe der Gruppen ein Vorgehen finden, mit dem man das Problem des „Rubikwürfels“ lösen kann.

In der vorliegenden Facharbeit wollen wir zunächst auf das Konzept der Gruppe eingehen, einige „eher einfacher“ zu beweisende, aber dennoch wichtige Eigenschaften von Gruppen im Allgemeinen, herleiten, uns danach mit Untergruppen, deren Nebenklassen und Normalteilern beschäftigen; letztere Beschäftigung ist danach unser Handwerkszeug, mit Hilfe dessen wir in der Lage sind, den Satz von Lagrange herzuleiten. Dieser vereinfacht uns später die Suche nach Untergruppen erheblich. In den darauffolgenden Abschnitten setzen wir uns mit den Diedergruppen auseinander und machen uns an ihrem Beispiel auf die Suche nach Untergruppen und Normalteilern. Danach werden

wir unser Augenmerk auf die Codierungstheorie richten, werden fehlererkennende Codes kennenlernen und schließlich auch hier die Gruppentheorie (insbesondere die Diedergruppe D_5) vertreten finden. Abschließend werden wir uns noch einen Ausblick auf weitere Verwendungen der Gruppentheorie genehmigen.

Bei der Erstellung des ersten Kapitels wurde vor allem auf [2] und auf [3] zurückgegriffen, aus denen die Definitionen und Beweise zum Großteil entnommen wurden; bei Kapitel zwei und drei wurde überwiegend [6] verwendet. Kapitel vier ist, bis auf weitere Angaben, eigenständig vom Autor geschaffen worden. Beim Schreiben des fünften Kapitels wurde [9] und [8] verwendet und Kapitel sechs greift auf [11] und [13] zurück.

Wurde eine Definition, ein Satz oder ein Hinweis in Anlehnung an eine Quelle verfasst, so steht der Verweis auf die entsprechende Quelle meist zu Beginn der Definition beziehungsweise des Satzes oder des Hinweises. Die Beweise für diese Sätze und Hinweise wurden dann auch meist an die in den entsprechenden Quellen aufgezeigten angelehnt.

1 Definitionen und wichtige Eigenschaften von Gruppen

Definition 1. (vgl. [2], S.9) Ein Paar (G, \circ) , bestehend aus einer nichtleeren Menge G und einer Abbildung $\circ : G \times G \rightarrow G$, $(a, b) \mapsto a \circ b$ heißt *Gruppe*, wenn gilt:

1. $(a \circ b) \circ c = a \circ (b \circ c)$ (*Assoziativgesetz*)
2. Es gibt ein $e \in G$ (*neutrales Element* von G) mit folgenden Eigenschaften:
 - a) $e \circ a = a$ für alle $a \in G$, (*linksneutrales Element*)
 - b) Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a' \circ a = e$. (*linksinverses Element*)

Manche Mathematiker (und auch viele Physiker) stellen an eine Gruppe nicht nur diese Forderungen, sondern auch die Existenz eines rechtsneutralen Elementes und eines rechtsinversen Elementes, die den zugehörigen linksneutralen beziehungsweise linksinversen gleichen, also ein e , so dass $e \circ a = a \circ e = a$ und nennen e dann einfach neutrales Element. Im Folgenden werden wir jedoch erkennen, dass unsere Forderungen vollkommen ausreichen und wir die soeben angesprochenen weiteren Forderungen aus unseren bisherigen ableiten können.

Hinweis 1. Wir werden in dieser Arbeit manchmal von den vier Gruppenaxiomen sprechen; dabei sehen wir die Abgeschlossenheit der Abbildung \circ bezüglich G als unser erstes Axiom, die Erfüllung des Assoziativgesetzes als zweites, die Existenz eines linksneutralen Elementes als drittes Axiom und die Existenz eines linksinversen als viertes Axiom an.

Hinweis 2. Im Folgenden werden wir, solange keine Mißverständnisse zu befürchten sind, für eine Gruppe (G, \circ) nur G schreiben.

Definition 2. Ist G eine Gruppe und gilt ferner noch das Kommutativgesetz ($a \circ b = b \circ a$ für alle $a, b \in G$), so heißt G *abelsche Gruppe*. Anstatt von „ \circ “ verwendet man dann meist „+“.

Ist G nicht abelsch, so verwendet man neben „ \circ “ oft auch andere Symbole, wie zum Beispiel „ \cdot “ oder „ \oplus “.

Beispiele für Gruppen:

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind abelsche Gruppen (neutrales Element der Addition ist 0 , inverses Element zu \mathbf{a} ist $-\mathbf{a}$), $(\mathbb{N}, +)$ aber nicht, da es in \mathbb{N} keine inversen Elemente bezüglich der Addition in \mathbb{N} gibt.
2. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ sind abelsche Gruppen (mit 1 als neutrales Element und $\frac{1}{\mathbf{a}}$ als inverses Element zu \mathbf{a}).
3. $(\{0\}, +)$ und $(\{1\}, \cdot)$ sind (abelsche) Gruppen.

Bei Verknüpfungen auf „kleinen“ Mengen (wie etwa $(\{0, 1, 2\}, \oplus)$, wobei \oplus in diesem Fall der Addition modulo 3 entsprechen soll) erstellt man häufig Verknüpfungstabellen:

\oplus	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Diese Verknüpfungstafel verrät uns folgendes: $0, 1, 2$ ist bezüglich \oplus abgeschlossen. 0 ist das neutrale Element, 1 das inverse Element zu 2 , 2 das inverse Element zu 1 und 0 das inverse Element zu sich selbst. Die Tatsache, dass die Verknüpfungstafel achsensymmetrisch zu ihrer Hauptdiagonalen ist, bedeutet nichts weiteres als $\mathbf{a} \circ \mathbf{b} = \mathbf{b} \circ \mathbf{a}$ für alle $\mathbf{a}, \mathbf{b} \in \{0, 1, 2\}$, also dass das Kommutativgesetz gilt.

Hinweis 3. Unmittelbar aus der Definition folgen für eine Gruppe G die Eigenschaften (vgl. [2] S. 9f):

1. Sei $e \in G$ linksneutrales Element und $\mathbf{a}, \mathbf{a}' \in G$, so dass $\mathbf{a}' \circ \mathbf{a} = e$. Dann gilt auch $\mathbf{a} \circ \mathbf{a}' = e$. Man nennt \mathbf{a}' dann nur noch ein inverses Element zu \mathbf{a} .
2. Sei $e \in G$ linksneutrales Element. Dann gilt: $\mathbf{a} \circ e = \mathbf{a}$ für alle $\mathbf{a} \in G$ und man nennt e dann ein neutrales Element.
3. Es gibt genau ein neutrales Element $e \in G$.
4. Zu jedem $\mathbf{a} \in G$ gibt es genau ein inverses Element $\mathbf{a}' \in G$ (oft mit \mathbf{a}^{-1} bezeichnet).
5. $(\mathbf{a}^{-1})^{-1} = \mathbf{a}$.
6. $(\mathbf{a} \circ \mathbf{b})^{-1} = \mathbf{b}^{-1} \circ \mathbf{a}^{-1}$.

Beweise der Eigenschaften:

1. *Beweis.* Wählen wir \mathbf{a}'' mit $\mathbf{a}'' \circ \mathbf{a}' = e$. Dann gilt:
 $\mathbf{a} \circ \mathbf{a}' = e \circ \mathbf{a} \circ \mathbf{a}' = \mathbf{a}'' \circ \mathbf{a}' \circ \mathbf{a} \circ \mathbf{a}' = \mathbf{a}'' \circ e \circ \mathbf{a}' = \mathbf{a}'' \circ \mathbf{a}' = e$ □

2. *Beweis.* $a \circ e = a \circ (a' \circ a) = (a \circ a') \circ a = e \circ a = a.$ □
3. *Beweis.* Wir nehmen an, es gäbe zwei neutrale Elemente von G ($e, e^* \in G$). Dann ist jedoch $e^* = e \circ e^* = e.$
Die beiden neutralen Elemente sind also zwangsläufig gleich. □
4. *Beweis.* Wir nehmen an, es gäbe ein zweites inverses Element a^* neben a' zu a in G . Dann muss jedoch $a^* = a'$ sein: $a^* = a^* \circ e = a^* \circ (a \circ a') = (a^* \circ a) \circ a' = e \circ a' = a'.$ □
5. *Beweis.* Es gilt $(a^{-1})^{-1} \circ a^{-1} = e.$ Es gilt aber auch $a \circ a^{-1} = e.$ Zu a^{-1} gibt es jedoch nur ein inverses Element (\leftarrow vierte Eigenschaft von Gruppen). Also ist $(a^{-1})^{-1} = a.$ □
6. *Beweis.* Es gilt $(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ e \circ b = e.$ Somit ist $(b^{-1} \circ a^{-1})$ das inverse Element zu $(a \circ b).$ Also ist $(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$ □

Satz 1. (vgl. [3], S. 44) Eine nicht leere Menge G mit der Abbildung $\circ : G \times G \rightarrow G$ ist genau dann eine Gruppe, wenn

1. $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G.$ (Assoziativität)
- 2' a) wenn die Gleichung $a \circ c = b$ für jedes $a, b \in G$ mit einem Element von G (c) lösbar ist.
- b) wenn die Gleichung $d \circ a = b$ für jedes $a, b \in G$ mit einem Element von G (d) lösbar ist.

Beweis. „ \Rightarrow “

Sei G eine Gruppe. Dann ist G assoziativ. (1) gilt also. Zu zeigen ist also nur (2' a) und (2' b).

Für (2' a) setzen wir $c = a^{-1} \circ b$; dann ist $a \circ c = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b.$
Für (2' b) setzen wir $d = b \circ a^{-1}$; dann ist $d \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b.$

„ \Leftarrow “

Für G gelte also (1) und (2'). Zu zeigen ist, dass G eine Gruppe ist, also dass G die Definition 1 erfüllt. (1) gilt zweifelsohne. Es bleibt also (2) zu zeigen.

Wir wählen uns nun ein a_0 (G darf also nicht leer sein). Dann gibt es ein $e \in G$, dass die Gleichung $e \circ a_0 = a_0$ erfüllt ist. Nun wählen wir uns ein beliebiges $a \in G$ und dazu ein c , so dass $a_0 \circ c = a.$ Dann ist $e \circ a = e \circ a_0 \circ c = a_0 \circ c = a.$

Nun beweisen wir (2b). Laut (2' b) lässt sich zu jeder Gleichung $d \circ a = b$ für zwei vorgegebene a, b ein d finden, so dass die Gleichung $d \circ a = b$ erfüllt ist. Insbesondere lässt sich ein d zur Gleichung $d \circ a = e$ finden (da ja $e \in G$). Dieses d ist damit das verlangte linksinverse Element zu $a.$ □

Eindeutigkeit der Lösbarkeit der Gleichungen aus (2'a) und (2'b):

Im Folgenden werden wir uns darauf beschränken, dies für (2'a) zu zeigen; für (2'b) könnten wir analog vorgehen.

Gäbe es nun ein c_1 und ein $c_2 \neq c_1$, so dass (2'a) für c_1 und c_2 erfüllt ist, so haben wir $a \circ c_1 = b$ und $a \circ c_2 = b$, also $a \circ c_1 = a \circ c_2$. Wir können uns nun ein inverses Element d zu a suchen (wie oben) und die Gleichung mit diesem von links durchmultiplizieren, womit wir bei $c_1 = c_2$ angelangt sind. Aus unserer Annahme folgt also ein Widerspruch zu ihr. Also muss $c_1 = c_2$: Die Gleichung hat also *höchstens* eine Lösung. Aus dem oberen Satz aber wissen wir bereits, dass jede Gleichung der Form aus 2' *mindestens* eine Lösung besitzt. Die Gleichung muss also eindeutig lösbar sein.

Beim Beweis des vorhergehenden Satzes haben wir gesehen, welche Vorteile uns die bewußte Minimierung unserer Forderungen einbringt. Hätten wir zum Beispiel nun auch noch die Existenz rechtsneutraler und rechtsinverser Elemente gefordert, so hätten wir zwar immer noch die gleiche Struktur, nämlich eine Gruppe, mit der wir uns befassen, jedoch müssen wir für manche Sätze, wie zum Beispiel diesen Satz, viel mehr beweisen. Die Tatsache, dass $(\mathbb{N}, +)$ keine Gruppe darstellt, spiegelt sich zum Beispiel in der Tatsache, dass kein $x \in \mathbb{N}$, welches die Gleichung $1 + x = 0$ erfüllt, wider. Dies ist natürlich nichts anderes als das von uns schon angesprochene Fehlen inverser Elemente bezüglich der Addition in \mathbb{N} . Um jedoch jede Gleichung, die uns begegnen könnte, lösen zu können, haben wir unseren „Zahlbegriff“ immer wieder erweitert: Von \mathbb{N} gelangten wir zunächst nach \mathbb{Q}^+ (Multiplikation) und dann zu \mathbb{Z} (Addition).

Definition 3. Unter der Ordnung einer Gruppe versteht man die Anzahl ihrer Elemente. Für die Ordnung einer Gruppe G schreibt man oft $|G|$.

Definition 4. Geben wir uns eine Menge X vor und betrachten die Menge aller bijektiven Abbildungen von X auf sich selbst. Wir schreiben

$$S(X) = \{f \in \text{Abb}(X, X) : f \text{ bijektiv}\}.$$

Wie wir noch sehen werden, bildet $S(X)$ bezüglich der „Hintereinanderschaltung“ eine Gruppe. Deshalb werden wir $S(X)$ *symmetrische Gruppe der Menge X* nennen. Ist $X = \{1, \dots, n\}$, so schreiben wir für $S(X)$ auch S_n und man nennt jedes Element von S_n eine Permutation der Zahlen $1, \dots, n$. S_n nennt man dann auch Permutationsgruppe. In dieser Arbeit werden wir mit dem Begriff Permutationsgruppe auch Untergruppen von S_n bezeichnen (wie auch in [2], S.36).

Hinweis 4. Elemente σ der symmetrischen Gruppe $S(X)$ schreibt man oft in der Form

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

wobei i_x und j_x Elemente von X sind und ihnen durch σ die Elemente j_x (wiederum von X) zugeordnet werden.

Unter der bereits angesprochenen „Hintereinanderschaltung“ \circ von Permutationen σ, ρ wollen wir, für

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \text{ und } \rho = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

$\pi = \sigma \circ \rho$ mit

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

verstehen. Dabei ist anzumerken, dass diese „Hintereinanderschaltung“ nicht der in der Mathematik verbreiteten Definition entspricht, bei der zunächst die hintere Permutation ausgeführt wird und danach die davor stehende.

Nun wollen wir zeigen, dass $S(X)$ eine Gruppe bezüglich der Hintereinanderausführung unserer Permutationen bildet.

1. Abgeschlossenheit

Wir wollen hier als bekannt voraussetzen, dass die Hintereinanderausführung zweier bijektiver Abbildungen auf der gleichen Menge wieder eine bijektive Abbildung auf dieser Menge ist.

2. Assoziativität

Haben wir drei Permutationen

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}, \rho = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}, \text{ und}$$

$$\pi = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix}, \text{ so haben wir}$$

$$(\sigma \circ \rho) \circ \pi = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} \circ \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix}$$

und

$$\sigma \circ (\rho \circ \pi) = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \circ \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix},$$

also $(\sigma \circ \rho) \circ \pi = \sigma \circ (\rho \circ \pi)$.

3. Existenz eines neutralen Elementes: Die Permutation $e = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ erfüllt unsere Forderungen an das neutrale Element.

4. Existenz inverser Elemente: Zur Permutation $\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$ suchen wir uns die Permutation $\sigma^{-1} = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, die auch eine bijektive Abbildung von X auf X ist. Es gilt nun: $\sigma \circ \sigma^{-1} = e$

2 Untergruppen und Normalteiler

Definition 5. Sei (G, \circ) eine Gruppe und $U \subseteq G$ eine Teilmenge von G . U heißt *Untergruppe* von G , wenn sie selbst eine Gruppe mit \circ bildet.

Hinweis 5. (vgl. [6], S. 10) U ist genau dann eine Untergruppe von G , wenn die Gruppenaxiome 1,3 und 4 für U erfüllt sind, da das Assoziativgesetz ja aufgrund seiner Gültigkeit für G auch für alle Elemente aus U gilt. Man kann an eine Untergruppe also folgende Forderungen stellen:

1. $a \circ b \in U$ für alle $a, b \in U$.
2. $e \in U$.
3. $a^{-1} \in U$ für alle $a \in U$.

Hinweis 6. $\{e\}$ und G selbst sind offensichtlich immer Untergruppen einer Gruppe G . Deshalb bezeichnet man sie als triviale Untergruppen.

Definition 6. ([6], S. 10) Zwei Elemente $a, b \in G$ heißen (über h) *zueinander konjugiert*, wenn es ein $h \in G$ gibt, so dass $b = h \circ a \circ h^{-1}$ beziehungsweise $a = h^{-1} \circ b \circ h = h^{-1} \circ b \circ (h^{-1})^{-1}$.

Definition 7. (vgl. [6], S. 12) Eine Untergruppe H einer Gruppe G wird als *Normalteiler* bezeichnet, wenn für jedes $h \in H$ und jedes $g \in G$ das Produkt $g \circ h \circ g^{-1} \in H$.

Hinweis 7. (vgl. [6], S. 12) Bei abelschen Gruppen sind alle Untergruppen Normalteiler, denn es gilt immer: $g \circ h \circ g^{-1} = g \circ g^{-1} \circ h = h \in H$.

3 Nebenklassen und der Satz von Lagrange

Definition 8. ([6], S. 13) Die *Rechtsnebenklasse* Hg der Untergruppe H einer Gruppe G ist die Menge aller Produkte $h \circ g$, wobei h die gesamte Untergruppe durchläuft und $g \in G$ fix bleibt, also $Hg = \{h \circ g | h \in H\}$.

Analog wird die *Linksnebenklasse* gH dieser Untergruppe H von G definiert.

Hier erkennen wir nun, dass eine Untergruppe H genau dann ein Normalteiler ist, wenn alle Rechtsnebenklassen Hg mit den entsprechenden Linksnebenklassen gH übereinstimmen.

Im Folgenden werden wir uns nur mit den Rechtsnebenklassen beschäftigen. Die folgenden Sätze und Beweise lassen sich aber für die Linksnebenklassen analog formulieren und beweisen.

Hinweis 8. (vgl. [6], S. 14) Da H selbst eine Gruppe ist, muss sie ja auch e enthalten. Damit gibt es für jedes $g \in G$ eine Rechtsnebenklasse von H , nämlich Hg , der g selbst angehört.

Satz 2. Ist $g \in H$ und H Untergruppe von G , so ist $Hg = H$ (vgl. [6], S. 13f)

Beweis. Wir wissen, dass H eine Untergruppe von G ist, also, dass H selbst eine Gruppe darstellt (mit der Verknüpfung \circ aus G). Da H ja abgeschlossen (bezüglich \circ) ist, liegt nun auch $h \circ g$ in H . Auch gilt Satz 1; insbesondere gilt hier 2'b, also, dass jede Gleichung der Form $d \circ a = b$ für jedes $a, b \in H$ mit einem Element $d \in H$ lösbar ist, wenn (H, \circ) eine Gruppe bildet. Wir können nun für unseren Fall $a = g$ setzen und bekommen für jedes beliebige Element $b \in H$ nun ein $d \in H$ geliefert, so dass die Gleichung erfüllt ist. Also liegen alle $h \circ g$ in H und für jedes $b \in H$ lässt sich ein $a \in H$ finden, so dass $a \circ g = b$. Also ist jedes Element von Hg auch Element von H und jedes Element von H liegt auch in Hg : Es gilt also $Hg = H$. \square

Satz 3. (vgl. [6], S.13ff) Zwei Rechtsnebenklassen Hg und Hk der Untergruppe H von G sind entweder gleich (enthalten also die selben Elemente) oder haben kein Element gemeinsam.

Beweis. Wir nehmen nun an, Hg und Hk hätten ein gemeinsames Element, also $h_1 \circ g = h_2 \circ k$. Durch „Multiplikation“ der Gleichung mit h_2^{-1} von links und mit g^{-1} von rechts gelangen wir nun zu: $h_2^{-1} \circ h_1 \circ g \circ g^{-1} = h_2^{-1} \circ h_2 \circ k \circ g^{-1}$, also $h_2^{-1} \circ h_1 = k \circ g^{-1}$.

Die linke Seite dieser Gleichung ist ja selbst Element von H und somit natürlich auch die rechte Seite $k \circ g^{-1}$; wenn wir nun die Rechtsnebenklasse $H(k \circ g^{-1})$ bilden (und mit Hilfe des vorangehenden Satzes) folgt nun: $H(k \circ g^{-1}) = H$.

Bilden wir nun die beiden Rechtsnebenklassen $H(k \circ g^{-1})g = Hg$, so gelangen wir zum Ziel: $Hk = Hg$. \square

Hinweis 9. Die Mächtigkeit $|Hg|$ von Hg ist gleich der Mächtigkeit $|H|$ von H , da für jedes $h_1 \circ g = d$ kein $h_2 \circ g = d$ ($h_1, h_2 \in H$, $h_1 \neq h_2$), da sonst wieder $h_1 = h_2$ folgen würde.

Der folgende Satz wird uns später bei der Suche nach Untergruppen besonders hilfreich sein, da er eine Aussage über die Ordnung einer Untergruppe macht und uns die Arbeit erspart, nach Untergruppen (außer den trivialen) von Gruppen bestimmter Ordnungen, wie zum Beispiel Primzahlen, zu suchen, da er solche nicht zulässt.

Satz 4. Satz von Lagrange (vgl. [6], S.15f)

Die Ordnung M jeder Untergruppe H einer endlichen Gruppe G ist ein Teiler der Ordnung N der Gruppe G .

Beweis. Wir haben gesehen, dass jedes Element g von G in mindestens einer Rechtsnebenklasse Hg von einer Untergruppe H vorkommt, wenn es aber in mehreren Rechtsnebenklassen vorkommt, sind diese zwangsläufig gleich. Die Gruppe zerfällt also in Rechtsnebenklassen. Dabei hat jede Rechtsnebenklasse die Ordnung M der Untergruppe H , bezüglich der sie gebildet wurde. Die Anzahl L der verschiedenen Rechtsnebenklassen muss also multipliziert mit der Ordnung M der Untergruppe H wieder die Ordnung von G ergeben, da dieses Produkt die Anzahl der verschiedenen Elemente von G ergibt. Dabei ist offensichtlich $L \in \mathbb{N}$. Wenn wir die Ordnung von G mit N benennen, erhalten wir die Gleichung

$$L \cdot M = N, \tag{3.1}$$

die aussagt, dass M ein Teiler von N sein muss. \square

4 Geometrische Anwendungen

4.1 Drehgruppen

Wenn wir ein reguläres n -Eck mit den Eckpunkten p_1, \dots, p_n um ein ganzzahliges Vielfaches k des Winkels $\frac{2\pi}{n}$ um seinen Mittelpunkt drehen, so erhalten wir ein n -Eck, das zu dem ursprünglichen n -Eck deckungsgleich ist.

Wir können eine Drehung um den Winkel $\frac{2\pi k}{n}$ auch durch k -faches Anwenden der Drehung um $\frac{2\pi}{n}$ erreichen. Wir werden also die Drehung um $\frac{2\pi}{n}$ mit d und die Drehung um $\frac{2\pi k}{n}$ mit d^k bezeichnen.

Offensichtlich gilt

$$d^k \circ d^l = d^{k+l} \quad (4.1)$$

und

$$d^{n+k} = d^k, \quad (4.2)$$

wobei die Abbildung \circ die Hintereinanderausführung von Drehungen ist. Die Menge aller dieser Drehungen $\{d^0, d^1, \dots, d^{n-1}\}$ bildet bezüglich der Hintereinanderausführung dieser Drehungen eine Gruppe:

- **Abgeschlossenheit**
Seien d^k und d^l zwei beliebige Elemente unserer Drehgruppe. Dann ist ihre Verknüpfung $d^k \circ d^l = d^{k+l}$ wieder Element der Drehgruppe, wenn $k+l < n$. Ist $k+l \geq n$, so gilt ja $d^{k+l} = d^{k+l-n}$.
- **Assoziativität** (vgl [10], S. 20) Geben wir uns drei beliebige Abbildungen M , N und O , die die Punkte P , Q , R und S wie folgt abbilden: $P \xrightarrow{M} Q$, $Q \xrightarrow{N} R$ und $R \xrightarrow{O} S$. Dann ist aber $P \xrightarrow{(MN)} R$ und $R \xrightarrow{O} S$, aber auch $P \xrightarrow{M} Q$ und $Q \xrightarrow{(NO)} S$, also $P \xrightarrow{(MN)O} S$ und $P \xrightarrow{M(NO)} S$. Damit ist $(MN)O = M(NO)$ für beliebige Abbildungen, die Punkte wieder auf Punkte abbilden.
- **Existenz eines neutralen Elementes**
Es gilt $d^0 \circ d^k = d^{0+k} = d^k$. Also ist d^0 das neutrale Element für jedes d^k . Die Drehung d^0 ist die Drehung um 0° , lässt also die Punkte des n -Ecks fest.

- Existenz inverser Elemente

Es gilt $d^{n-k} \circ d^k = d^0$. Also ist zu einem beliebigen Element d^k der Drehgruppe das Inverse als d^{n-k} gegeben.

4.2 Diedergruppen

Betrachten wir nun die Menge aller Deckbewegungen der regulären n -Ecks.

Wir wollen nun wieder mit d^k die k -fache Drehung des n -Ecks um den Winkel $\frac{2\pi}{n}$ bezeichnen und mit s eine Spiegelung an einer festen Spiegelachse. Im Folgenden werden wir mit s die Spiegelung an der Spiegelachse durch den Punkt p_1 und den Umkreismittelpunkt unseres n -Ecks bezeichnen.

Betrachten wir nur die Drehungen d^k um den Mittelpunkt, so erkennen wir eine Drehgruppe wieder; für die Drehungen gelten also die beiden Regeln, die wir im vorherigen Abschnitt aufgeführt haben.

Darüberhinaus erkennen wir, dass $s^2 = e$, da zwei Spiegelungen an einer festen Achse das n -Eck unberührt lassen.

Wir können alle Spiegelungen an den Symmetrieachsen auf eine Drehung und eine Spiegelung an einer festen Symmetrieachse zurückführen, da eine Spiegelung nur den Drehsinn des n -Ecks ändert und wir deshalb das an einer festen Achse gespiegelte n -Eck einfach durch eine Drehung mit dem an einer anderen Achse gespiegelten n -Eck zur Deckung bringen können. Hier erkennen wir, dass $s \circ d^k = d^{-k} \circ s = d^{n-k} \circ s$.

Insbesondere mit unserer festen Spiegelung s können wir jede Spiegelung darstellen, indem wir unser n -Eck zunächst so drehen, dass der Punkt p_1 an der Stelle steht, an der wir ihn auch nach der Spiegelung haben wollen. Die Spiegelung s (durch p_1 und den Mittelpunkt des n -Ecks) lässt dabei p_1 fix, da dieses sich ja auf der Spiegelachse befindet. Die restlichen Punkte sind danach eindeutig durch den Drehsinn, der sich durch die Spiegelung geändert hat, festgelegt.

Nun stellt sich die Frage, ob diese Menge von Deckbewegungen die Gruppenaxiome bezüglich der Hintereinanderausführung erfüllt.

1. Abgeschlossenheit.

Einen Teil des Nachweises haben wir schon bei den Drehgruppen gebracht. Nun wollen wir nur noch zeigen, dass

$$\text{a) } (d^k \circ s) \circ (d^l \circ s) \in D_n \text{ und dass}$$

$$\text{b) } d^k \circ (d^l \circ s) \in D_n$$

für k und l mit $0 \leq k \leq n$ und $0 \leq l \leq n$. $(d^k \circ s) \circ d^l \in D_n$ folgt direkt aus $d^k \circ (d^l \circ s) \in D_n$.

Zu a)

$$d^k \circ (d^l \circ s) = (d^k \circ d^l) \circ s = d^{k+l} \circ s.$$

$d^{k+l} \circ s$ liegt aber in D_n , da $d^{k+l} \in D_n$ für $0 \leq k+l \leq n$ und für $k+l \geq n$ gilt $d^{k+l} = d^{k+l-n}$, welches wegen $k \leq n$ und $l \leq n$ kleiner als $2n$ ist.

Zu b)

$$(d^k \circ s) \circ (d^l \circ s) = d^k \circ (s \circ d^l) \circ s = d^k \circ d^{-l} \circ s \circ s = d^k \circ d^{-l} = d^{k-l} \in D_n$$

2. Assoziativität.

Der Beweis, den wir beim Nachweis des Assoziativgesetzes bei den Drehgruppen geführt haben, lässt sich hier auch ohne Weiteres anwenden.

3. Existenz eines neutralen Elements.

Die Drehung d^0 um 0° um den Mittelpunkt lässt das Dreieck fest.

4. Existenz inverser Elemente.

Wir haben auch hier bei den Drehgruppen schon eine gewisse Vorarbeit geleistet. Jetzt brauchen wir uns nur noch um die Inversen zu $d^k \circ s$ kümmern. Es sticht ins Auge, dass $(d^k \circ s) \circ (d^k \circ s) = d^k \circ (s \circ s) \circ d^{-k} = d^{k-k} = d^0 = e$, also dass eine Spiegelung ihr eigenes Inverses ist, was auch rein intuitiv klar ist.

Definition 9. Die *Diedergruppe* D_n ist die Gruppe der n Drehungen und n Spiegelungen der Ebene, die ein reguläres n -Eck in sich überführen.

4.2.1 Veranschaulichung an der Diedergruppe D_3

Im Folgenden sehen wir alle Fälle, die auftreten können, wenn wir ein Dreieck durch Drehungen und Spiegelungen der Ebene, in der es liegt, wieder in ein solches Dreieck überführen. Dabei sind die Elemente unserer Diedergruppe die Überführungen des Ausgangsdreiecks in die jeweiligen anderen Dreiecke.

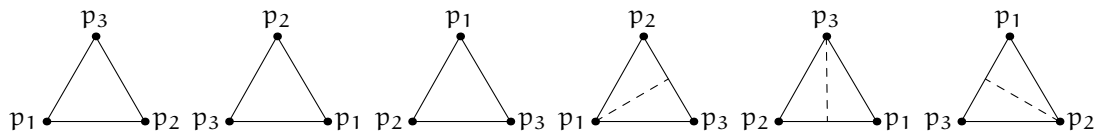


Abbildung 4.1: Die Drehungen und Spiegelungen des gleichseitigen Dreiecks

Untergruppen der Diedergruppe D_3

Untergruppen von D_3 können nach dem Satz von Lagrange nur die Mächtigkeiten 1, 2, 3 und 6 haben, da die Mächtigkeit von D_3 gleich 6 ist. Wir wollen im Folgenden mit H_{ij} eine Untergruppe von D_3 bezeichnen, wobei i die Mächtigkeit dieser Untergruppe bezeichnet und j nur der Nummerierung dient.

Als Untergruppe mit der Mächtigkeit 1 kommt nur $H_1 = \{e\}$ in Frage, da das Einselement in jeder Gruppe vorhanden sein muss.

Es lassen sich auch Untergruppen mit der Mächtigkeit 2 finden: $H_{21} = \{e, s\}$, $H_{22} = \{e, d \circ s\}$, $H_{23} = \{e, d^2 \circ s\}$. Diese bestehen jeweils aus dem Einselement und einem anderem Element aus D_3 , das sein eigenes Inverses ist (sonst benötigten wir auch noch dieses in unserer Untergruppe). Diese Forderung erfüllen unsere Spiegelungen, wie wir oben beim Nachweis der Existenz inverser Elemente erkannt haben. Drehungen können diese Forderung (bis auf $d^0 = e$) aber nicht erfüllen, da wir $d^{-1} = d^2$ und $d^{-2} = d^1$ haben.

Diese kommen nun bei der Suche nach Untergruppen mit der Mächtigkeit 3 zu tragen, da wir hier keine Spiegelungen verwenden können: Wenn wir eine Spiegelung verwenden würden, bräuchten wir noch eine Spiegelung, damit wir die Mächtigkeit von 3 erhalten, denn das Inverse des letzten Elements muss ja auch in unserer Untergruppe vorhanden sein. Die Verknüpfung von zwei (verschiedenen) Spiegelungen würde uns aber insgesamt eine Drehung liefern (die nicht mit d^0 übereinstimmt, da die zwei Spiegelungen ja verschieden sind, also nicht ihre gegenseitigen Inversen sind). Hier wäre also in diesem Fall die Abgeschlossenheit nicht gegeben. Wir müssen uns also für zwei inverse Drehungen entscheiden. Hier kann also folgender Fall auftreten, $H_{31} = \{e, d^1, d^2\}$, der nichts anderes als die Drehgruppe des regulären Dreiecks darstellt.

Als Untergruppe mit der Mächtigkeit 6 finden wir nur $H_6 = G$ selbst.

Normalteiler von D_3

Hier sind offensichtlich auf jeden Fall die Untergruppen H_1 und $H_6 = G$ Normalteiler, da hier ja für $H_1 = \{e\}$ immer $g \circ e \circ g^{-1} = g \circ g^{-1} = e \in H_1$ und für $H_6 = G$ ist natürlich auch für jedes $h \in H$ die Forderung $g \circ h \circ g^{-1} \in H$, da $H = G$ und G abgeschlossen ist.

Nun können wir die Untergruppen der Mächtigkeit 2 betrachten: Hier gilt für $H_{21} = \{e, s\}$ offensichtlich $d \circ s \circ d^{-1} = d \circ d \circ s = d^2 \circ s \notin H_{21}$ und für $H_{22} = \{e, d \circ s\}$ können wir $d \circ (d \circ s) \circ d^{-1} = d \circ d \circ d \circ s = e \circ s = s \notin H_{22}$ feststellen. Für $H_{23} = \{e, d^2 \circ s\}$ finden wir wieder $d \circ (d^2 \circ s) \circ d^{-1} = d \circ d^2 \circ d \circ s = d \circ s \notin H_{23}$.

Nun untersuchen wir noch $H_3 = \{e, d, d^2\}$: Hier haben wir auch hier für jedes $g \in H$ ja die Normalteilerforderung schon wegen der Tatsache erfüllt, dass H selbst eine Gruppe ist. Für $g \notin H$, $g \in G$, also alle Spiegelungen $d^x \circ s$ haben wir $d^x \circ s \circ d^y \circ d^x \circ s = (d^x \circ s)^2 \circ d^{-y} = e \circ d^{-y} \in H_3$. Damit ist neben den trivialen Untergruppen auch H_3 ein Normalteiler von D_3 .

4.2.2 Veranschaulichung an der Diedergruppe D_5

Ähnlich zum letzten Beispiel können wir hier die Elemente unserer Diedergruppe durch die Fünfecke darstellen, die aus dem Ausgangsfünfeck durch Elemente dieser Diedergruppe entstanden sind. Gemäß unserer Regeln, dass hier $d^5 = e = s^2$ und $d^k \circ s = s \circ d^{-k}$, können wir nun eine Verknüpfungstafel erstellen:

\circ	d^0	d^1	d^2	d^3	d^4	s	$d^1 \circ s$	$d^2 \circ s$	$d^3 \circ s$	$d^4 \circ s$
d^0	d^0	d^1	d^2	d^3	d^4	s	$d^1 \circ s$	$d^2 \circ s$	$d^3 \circ s$	$d^4 \circ s$
d^1	d^1	d^2	d^3	d^4	d^0	$d^1 \circ s$	$d^2 \circ s$	$d^3 \circ s$	$d^4 \circ s$	s
d^2	d^2	d^3	d^4	d^0	d^1	$d^2 \circ s$	$d^3 \circ s$	$d^4 \circ s$	s	$d^1 \circ s$
d^3	d^3	d^4	d^0	d^1	d^2	$d^3 \circ s$	$d^4 \circ s$	s	$d^1 \circ s$	$d^2 \circ s$
d^4	d^4	d^0	d^1	d^2	d^3	$d^4 \circ s$	s	$d^1 \circ s$	$d^2 \circ s$	$d^3 \circ s$
s	s	$d^4 \circ s$	$d^3 \circ s$	$d^2 \circ s$	$d^1 \circ s$	d^0	d^4	d^3	d^2	d^1
$d^1 \circ s$	$d^1 \circ s$	s	$d^4 \circ s$	$d^3 \circ s$	$d^2 \circ s$	d^1	d^0	d^4	d^3	d^2
$d^2 \circ s$	$d^2 \circ s$	$d^1 \circ s$	s	$d^4 \circ s$	$d^3 \circ s$	d^2	d^1	d^0	d^4	d^3
$d^3 \circ s$	$d^3 \circ s$	$d^2 \circ s$	$d^1 \circ s$	s	$d^4 \circ s$	d^3	d^2	d^1	d^0	d^4
$d^4 \circ s$	$d^4 \circ s$	$d^3 \circ s$	$d^2 \circ s$	$d^1 \circ s$	s	d^4	d^3	d^2	d^1	d^0

Wir sehen also, dass die Diedergruppe vollständig durch unsere drei Regeln festgelegt ist und (da die Gruppentafel nicht symmetrisch zur Hauptdiagonalen ist), dass die Diedergruppe D_5 nicht abelsch ist. Dies können wir für alle D_n mit $n > 2$ zeigen, denn damit D_n abelsch ist, müsste für jedes $d^k \in D_n$ die Gleichung $d^k \circ s = s \circ d^k$ erfüllt sein, und mit unseren Regeln folgt nun $d^k = d^{-k}$. Dies ist offensichtlich zum Beispiel für $k = 1$ nie erfüllt (— solange $n \geq 3$).

Nun stellen wir die Fünfecke dar, die wir durch die Drehungen unserer Diedergruppe D_5 aus dem Ausgangsfünfeck erhalten:

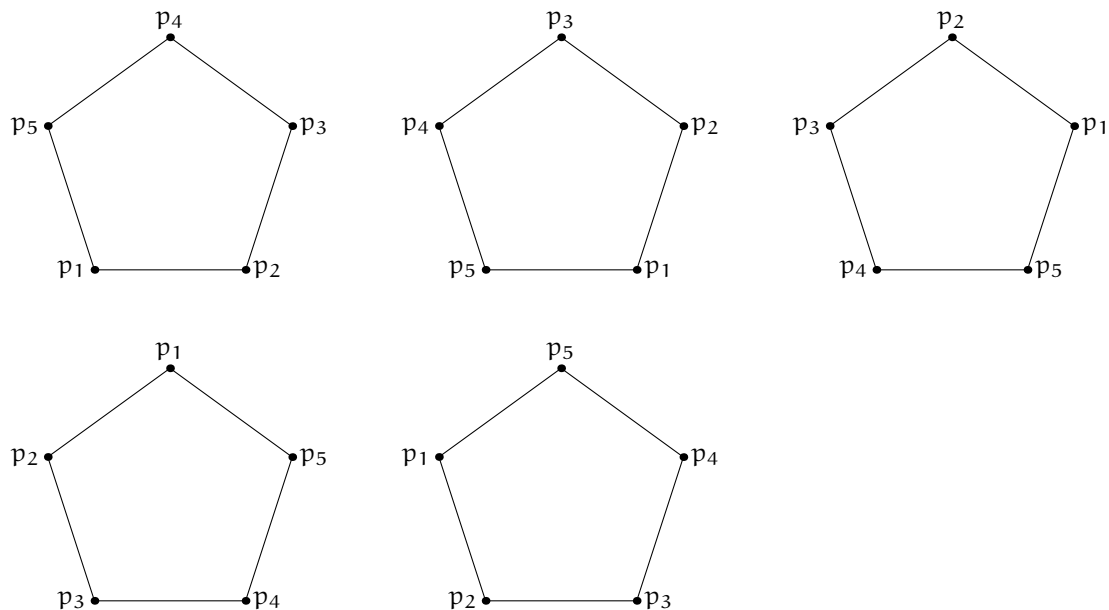


Abbildung 4.2: Die Drehungen eines regulären 5-Ecks

Nun wenden wir uns den Fünfecken zu, die durch Spiegelungen (an unserer festen Achse durch den Punkt p_1 und dem Mittelpunkt des Fünfecks) aus unserem Urfünfeck hervorgegangen sind. Dabei sind die Spiegelachsen, die wir durch die Hintereinanderausführung von Drehungen und Spiegelungen durch unsere feste Achse darstellen können, gestrichelt eingezeichnet.

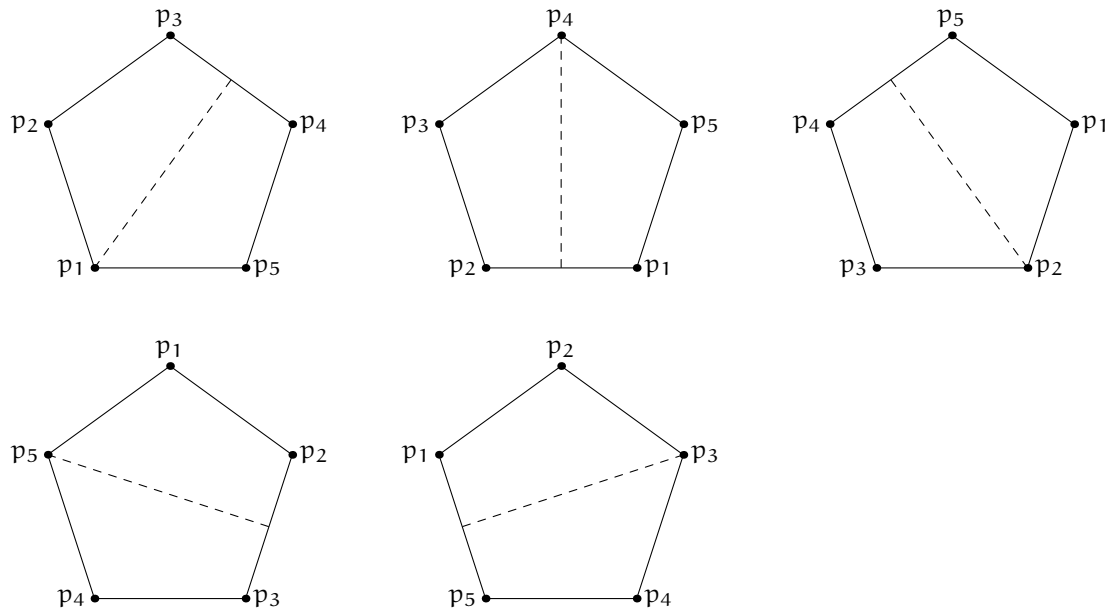


Abbildung 4.3: Die Spiegelungen eines regulären 5-Ecks

Da wir unsere Gruppenelemente ja auch als Vertauschung der Eckpunkte ansehen können, können wir unsere Gruppenelemente nun als Permutationen schreiben:

$$e: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, d: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, d^2: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

$$d^3: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, d^4: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},$$

$$s: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}, d \circ s: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}, d^2 \circ s: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix},$$

$$d^3 \circ s: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}, d^4 \circ s: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Wie wir erkennen können, gilt auch hier, wenn wir die Permutation, die der Drehung entspricht mit R und die, die der Spiegelung entspricht mit M bezeichnen, $R^5 = e = M^2$. Wir wollen für die Komposition von Permutationen das Zeichen „ \cdot “ wählen.

Wenn wir nun noch zeigen können, dass $R^k \cdot M = M \cdot R^{-k}$, haben wir alle unsere Gesetze, die unsere Diedergruppe festlegen, auch für unsere Permutationsgruppe gezeigt.

Wir könnten dies nun für alle möglichen k einzeln nachweisen, können es jedoch auch induktiv zeigen:

1. Induktionsanfang

Für $k = 1$ ist unsere Vermutung erfüllt:

$$M \cdot R^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = R \cdot M$$

2. Induktionsschritt

Wir gehen nun davon aus, dass unsere Vermutung bereits für ein bestimmtes $k = n$ erfüllt ist und versuchen, aus dieser Tatsache allgemein abzuleiten, dass sie dann auch für $k = n + 1$ erfüllt ist.

$R^{n+1} \cdot M = R \cdot R^n \cdot M = R \cdot M \cdot R^{-n} = M \cdot R^{-1} \cdot R^{-n} = M \cdot R^{-(n+1)}$. Dabei haben wir allerdings im vorletzten Schritt auch noch unseren Induktionsanfang verwendet.

Aus der Tatsache, dass unsere Vermutung für $k = 1$ gilt, können wir nun mit Hilfe unseres Induktionsschritts folgern, dass sie dann auch für $k = 1 + 1 = 2$ gelten muss, aus dieser Tatsache dann wiederum die Gültigkeit für $k = 3$ folgern und so fort.

Das Prinzip der vollständigen Induktion ist in der Mathematik sehr verbreitet und findet vor allem Anwendung, wenn man eine Vermutung für alle natürlichen Zahlen (über dem Induktionsanfang) zeigen will, in unserem Beispiel hat es uns aber nur drei oder vier Rechnungen erspart, da wir für $k \geq 5$ mit Hilfe der ersten Regel wieder zu $k < 5$ kommen würden.

Die Tatsache, dass wir eine Permutationsgruppe finden konnten, die sich genauso verhält wie unsere Diedergruppe ist kein Zufall; in der Gruppentheorie existiert der Satz von Cayley ([2] S.36), der uns garantiert, dass zu jeder endlichen Gruppe ein Isomorphismus zu einer Permutationsgruppe existiert.

Definition 10. Ein *Isomorphismus* von einer Gruppe G auf eine Gruppe G' ist eine Art „Wörterbuch“ ([1] S.95), eine Abbildung Φ , die folgende Eigenschaften (vgl. [4] S.2) zu erfüllen hat:

1. Für $a \neq b$ gilt $\Phi(a) \neq \Phi(b)$ (mit $a, b \in G$).
2. Für jedes Element aus G' gibt es ein $a \in G$, so dass sich dieses Element in der Form $\Phi(a)$ schreiben lässt.

3. Φ erhält uns Produkte:

$$\Phi(ab) = \Phi(a)\Phi(b)$$

Anschaulich ist ein Isomorphismus eine Abbildung, die die Struktur unserer Gruppentafel unverändert lässt; zwei zueinander isomorphe Gruppen unterscheiden sich nur in ihren Bezeichnungen.

In unserem Fall haben wir als Elemente von D_5 , wie wir der Verknüpfungstafel entnehmen können, nur solche der Form $d^x \circ s^y$ mit $x \in \{0, 1, 2, 3, 4, 5\}$ und $y \in \{0, 1\}$. Wir haben nun ein Φ gefunden, dass ein solches Element auf $R^x \cdot M^y$ abbildet.

Für zwei verschiedene Elemente a, b aus D_5 folgt hier offensichtlich auch, dass $\Phi(a) \neq \Phi(b)$. Außerdem finden wir auch für jedes $k = R^x \cdot M^y$ aus unserer Permutationsgruppe ein Element $a \in D_5$, nämlich $a = d^x \circ s^y$ mit $\Phi(a) = k$. Nun können wir noch sehen, dass wir für $a, b \in D_5$ nach einigen Fallunterscheidungen (y, w gerade/ungerade) genau zu $\Phi(a \circ b) = \Phi(d^x \circ s^y \circ d^z \circ s^w) = \Phi(a) \cdot \Phi(b)$ gelangen.

Untergruppen der Diedergruppe D_5

Auch hier können wir alle Untergruppen betrachten. D_5 hat die Ordnung 10. Es kommen also nur Untergruppen der Ordnung 1, 2, 5 und 10 in Frage.

Als Untergruppe H_1 haben wir wieder $\{e\}$.

Für H_{2i} mit $|H_{2i}| = 2$ kommen wir nach gleichem Vorgehen wie bei der Diedergruppe D_3 zu:

$$H_{21} = \{e, s\}, H_{22} = \{e, d \circ s\}, H_{23} = \{e, d^2 \circ s\}, H_{24} = \{e, d^3 \circ s\} \text{ und } H_{25} = \{e, d^4 \circ s\}.$$

Für H_5 mit $|H_5| = 5$ finden wir nun wieder $H_5 = \{e, d, d^2, d^3, d^4\}$.

Letztendlich gibt es nur die eine Möglichkeit für H_{10} , nämlich $H_{10} = D_5$.

Normalteiler von D_5

Als Normalteiler finden wir hier wieder (nach analogem Vorgehen wie bei der Normalteilerversuche bei D_3) die trivialen Untergruppen und $\{e, d, d^2, d^3, d^4\}$.

4.3 Allgemeines über Untergruppen und Normalteiler von Diedergruppen

Neben den trivialen Untergruppen $H_1 = \{e\}$ und $H_{(2n)} = D_n$ selbst, hat jede Diedergruppe auf jeden Fall n Untergruppen H_{2j} mit den Elementen e und $d^j \circ s$; da jede Spiegelung ihr eigenes Inverses ist, ist jedes H_{2j} abgeschlossen, und auch das neutrale Element (e) und die inversen Elemente sind alle vorhanden (da ja jedes Element von H_{2j} sein eigenes Inverses ist).

Nun haben wir auf jeden Fall noch H_n , das eine zyklische Untergruppe mit dem erzeugenden Element d von D_n darstellt.

Eine zyklische Gruppe ist eine Gruppe, die von einem einzigen Element erzeugt wird, also eine Gruppe, in der ein Element a existiert, so dass sich jedes Gruppenelement g als $g = a^k$ (mit einem $k \in \mathbb{N}$) schreiben lässt. Man schreibt für eine solche Gruppe oft $\langle a \rangle$, wenn man mit a das erzeugende Element bezeichnet.

Diese zyklische Untergruppe H_n ist abgeschlossen (da jede Potenz von d darin enthalten ist und wir nur solche aus Verknüpfung von Potenzen von d erhalten können), enthält $e = d^n$ und zu jedem d^k sein Inverses d^{n-k} .

Es sticht auch ins Auge, dass diese Untergruppe abelsch ist, also dass $d^l \circ d^m = d^m \circ d^l$ gilt, denn o. B. d. A. können wir $l \geq m$ wählen; damit haben wir dann $d^l \circ d^m = d^m \circ d^{l-m} \circ d^m = d^m \circ d^l$.

Diese Untergruppe ist neben $\{e\}$ und D_n immer ein Normalteiler von D_n , da wir ja mit $a \circ h \circ a^{-1}$, mit $h \in H_n$ und $a \in D_n$ für $a \in H_n$ ja selbstverständlich wieder ein $h' \in H_n$ erhält und für $a \notin H_n$ ja a eine Spiegelung sein muss; dann ist aber $a \circ h \circ a^{-1} = a \circ a \circ h^{-1} = h^{-1} \in H_n$.

Damit haben wir Untergruppen erfasst, die jede Diedergruppe haben muss, auch diejenigen, bei denen n Primzahl ist, da wir bisher Untergruppen mit den Ordnungen $1, 2, n$ und $2n$ betrachtet haben.

Betrachten wir nun Diedergruppen, bei denen n nicht Primzahl ist, also durch eine natürliche Zahl t ($t \neq 1$) teilbar ist. Dann können wir eventuell Untergruppen der Ordnungen t bzw. $2t$ finden. Suchen wir zunächst die Untergruppen der Ordnung t . Hier haben wir offensichtlich $\langle d^{\frac{n}{t}} \rangle$, wieder eine abelsche zyklische Untergruppe, die auch wieder Normalteiler ist:

Die Normalteilerforderung lautet für diese Untergruppe:

$$d^x \circ s^y \circ d^{ru} \circ (d^x \circ s)^{-1} \in H_t, \text{ mit } u = \frac{n}{t} \text{ und } r \in \mathbb{N}.$$

Nun machen wir eine Fallunterscheidung:

1. Fall: $y=0$

$$d^x \circ d^{ru} \circ d^{-x} = d^{ru} \in H_t$$

2. Fall: $y=1$

$$d^x \circ s \circ d^{ru} \circ (d^x \circ s)^{-1} = d^x \circ s \circ d^{ru} \circ (d^x \circ s) = d^x \circ s \circ s \circ d^{-ru} \circ d^{-x} = d^{-ru} \in H_t$$

Analog können wir für H_u vorgehen, wobei wir dann auch wieder einen Normalteiler bekommen mit $H_u = \langle d^t \rangle$.

Als Untergruppen H_{2t} haben wir hier natürlich die Diedergruppen des regulären t -Ecks.

Die Normalteilerforderung lautet für diesen Fall:

$$d^x \circ s^y \circ d^{ru} \circ s^z \circ (d^x \circ s^y)^{-1} \in H_{2t}$$

Für $z = 0$ sind wir wieder beim oberen Fall gelandet, von dem wir nichts zu befürchten haben, da wir dort ja die Normalteilerforderung erfüllt sahen.

Nun betrachten wir den Fall $z = 1$ und werden wieder eine Fallunterscheidung durchführen müssen:

1. Fall: $y=0$

$$d^x \circ d^{ru} \circ s \circ d^{-x} = d^x \circ d^{ru} \circ d^x \circ s = d^{ru+2x} \circ s$$

2. Fall: $y=1$

$$d^x \circ s \circ d^{ru} \circ s \circ (d^x \circ s)^{-1} \circ d^{-x} \circ d^{ru} \circ d^{-x} \circ s \circ s = s \circ d^{ru-2x} = d^{2x-ru} \circ s$$

Damit unsere Untergruppe H_{2t} also ein Normalteiler ist, muss $ru+2x = au$ und $2x-ru = bu$ mit $a, b \in \mathbb{Z}$ für alle $x \in \{0, 1, \dots, n\}$. Diese beiden Gleichungen können wir nun durch u teilen und gelangen so zu $r + 2\frac{x}{u} = a$ und $2\frac{x}{u} - r = b$. Für $u = 2$ sind $a, b \in \mathbb{Z}$ (der Fall $u = 1$ hat für uns ja keine weitere Bedeutung). Alle u , die uns einen Normalteiler bringen, müssen insbesondere die Gleichungen für $x = 1$ erfüllen:

$$r + \frac{2}{u} = a \quad \text{und} \quad \frac{2}{u} - r = b$$

Hier sehen wir also, dass wir nur für $u = 2$ eine Untergruppe, die eine Diedergruppe ist, als Normalteiler haben. Dies ist dann $D_{\frac{n}{2}}$; für $\frac{n}{t} = u$ haben wir aber die Diedergruppe D_t und D_u als Untergruppen. Um eine Untergruppe zu haben, die wieder eine Diedergruppe und auch Normalteiler ist, muss eine Diedergruppe D_n also ein n besitzen, das durch 2 teilbar ist.

Wir können uns nun die Frage stellen, ob die schon von uns gefundenen Untergruppen *alle* Untergruppen einer Diedergruppe D_n sind. Um diese Frage beantworten zu können, versuchen wir noch ein paar allgemeine Sachverhalte zu zeigen:

Im Allgemeinen können wir erkennen, dass eine Untergruppe, die sowohl Drehungen als auch Spiegelungen enthält, die gleiche Anzahl an Drehungen (mit $d^n = d^0$ als Drehung) wie an Spiegelungen enthalten muss.

Beweis. Wir haben mit Hilfe unserer Rechenregeln schon erkannt, dass die Verknüpfung zweier Spiegelungen immer eine Drehung ist. Da wir mit H ja eine Untergruppe haben wollen, sollte diese aber die Gruppenaxiome, also auch Satz 1 erfüllen. Es muss also zu jeder Spiegelung genau so viele von ihr verschiedene Spiegelungen geben, wie wir Drehungen haben:

Jede Gleichung $a \circ b = c$ muss für eine vorgegebene Spiegelung a und einer beliebigen Drehung c eindeutig lösbar sein, d. h. es muss genau ein $b \in H$ (welches wiederum eine Spiegelung sein muss, da die Verknüpfung von a und b sonst wieder eine Spiegelung wäre) geben, das die Gleichung für eine vorgegebene Drehung c erfüllt. Gehen wir nun alle in H existierenden Drehungen c durch, so erhalten wir auch genauso viele Spiegelungen b . Wir haben also mindestens so viele Spiegelungen wie Drehungen in unserer Untergruppe H .

Hätten wir noch eine weitere Spiegelung $b' \in H$, die wir damit noch nicht erfasst haben, dann könnten wir $a \circ b'$ bilden und würden damit wieder eine Drehung erhalten, die in H enthalten sein muss, denn wir wollen ja mit H eine Untergruppe von D_n . Zu jeder in H enthaltenen Drehung c haben wir aber schon die zugehörige Spiegelung b gesucht, so dass dann $b = b'$ folgt.

□

Eine Untergruppe, die Spiegelungen und Drehungen enthält, muss also von beiden die gleiche Anzahl enthalten. Insbesondere alle Untergruppen, die Spiegelungen enthalten (und natürlich auch $d^0 = d^n = e$ enthalten müssen), müssen also auch die gleiche Anzahl an Drehungen wie an Spiegelungen enthalten.

Stellen wir nun weitere Überlegungen an:

Jede Untergruppe von D_n , die eine Drehung d^m enthält, muss auch (da sie sonst keine Gruppe darstellt) alle Potenzen von d^m enthalten.

Untersuchen wir nun Allgemein $\langle d^m \rangle$:

Wir können nun

$$(d^m)^k \circ d^r = d^n \text{ betrachten.}$$

Nun folgt: $m \cdot k + r \equiv 0 \pmod{n}$, da $d^p = d^q$ nur für $p \equiv q \pmod{n}$ erfüllt ist (denn wäre nun nicht $p \equiv q \pmod{n}$, so müßte $d^{p-q} \equiv d^0 \pmod{n}$ und wir hätten damit zwei verschiedene neutrale Elemente, was wir jedoch schon in Kapitel 1 ausgeschlossen haben). r werden wir im Folgenden als Rest bezeichnen.

Um zwei gleiche Reste (für verschiedene k) zu bekommen, brauchen wir also:

$$m \cdot k + r \equiv m \cdot k' + r \pmod{n}$$

und damit $mk \equiv mk' \pmod{n}$.

Ist m nun teilerfremd zu n , so haben wir also nur $k \equiv k' \pmod{n}$ für k von 1 bis n , das die Gleichung erfüllt und damit genau n verschiedene Reste. $\langle d^m \rangle$ muss also in diesem Fall gleich $\langle d \rangle$ sein.

Bezeichnen wir mit a den größten gemeinsamen Teiler von m und n , so haben wir mit allen Potenzen von d^m immer auch eine Potenz von d^a (also $\langle d^m \rangle \subseteq \langle d^a \rangle$), haben also in unserer Menge höchstens $\frac{n}{a}$ verschiedene Elemente und es folgt die Forderung $a \cdot \frac{m}{a}k \equiv a \cdot \frac{m}{a}k' \pmod{n}$; da a der größte gemeinsame Teiler von m und n ist, ist $\frac{m}{a}$ teilerfremd zu n (denn wenn es einen Teiler t mit n gemeinsam hätte, hätten wir at als größten gemeinsamen Teiler von m und n). Damit haben wir für $k, k' \pmod{n}$ Werte von 1 bis $\frac{n}{a}$ und nun also $\frac{n}{a}$ verschiedene Reste. Mit $\frac{n}{a}$ vielen verschiedenen Resten haben wir auch $\frac{n}{a}$ viele verschiedene Elemente in $\langle d^m \rangle$. Wir wissen bereits, dass $\langle d^m \rangle \subseteq \langle d^a \rangle$ und können nun folgern, dass $\langle d^m \rangle = \langle d^a \rangle$.

Betrachten wir nun eine Untergruppe H , die zwei verschiedene Drehungen d^l und d^k enthält:

Diese Untergruppe muss nun auch wieder alle Potenzen von d^l und d^k enthalten, also $\langle d^k \rangle \subseteq H$ und $\langle d^l \rangle \subseteq H$. Bezeichnen wir mit a den größten gemeinsamen Teiler von k und n und mit b den größten gemeinsamen Teiler von l und n , so muss also auch $\langle d^a \rangle \subseteq H$ und $\langle d^b \rangle \subseteq H$.

Mit $d^a \in H$ und $d^b \in H$ müssen natürlich auch alle $d^{\alpha \cdot a + \beta \cdot b}$ in H liegen (für ganze α, β) In [5] (S. 13f) wird der erweiterte Euklidische Algorithmus behandelt, der es uns ermöglicht, zu zwei vorgegebenen natürlichen Zahlen a, b zwei ganze Zahlen α, β zu finden, so

dass $\alpha \cdot a + \beta \cdot b = g$, wobei g der grösste gemeinsame Teiler von a und b ist, zu finden. Wir haben also auch $d^g \in H$. Wir können auch erkennen, dass jegliche Kombination $\alpha \cdot a + \beta \cdot b$ auch ein Vielfaches von g sein muss, dass es also keine Kombination gibt, die sich nicht als Potenz von d^g darstellen lässt. Damit haben wir nun also $H = \langle d^g \rangle$. Nun wissen wir bereits, dass $\langle d^g \rangle$ nichts anderes ist als $\langle d^p \rangle$, wobei p der größte gemeinsame Teiler von n und g ist.

Haben wir nun mehrere solch „verschiedene“ Drehungen in einer Menge, die nur aus Drehungen bestehen und eine Untergruppe bilden soll, so lässt sich das obige Verfahren (für zwei Drehungen) sukzessiv anwenden, so dass wir schließlich bei der zyklischen Untergruppe $\langle d^x \rangle$ landen, wobei x der größte gemeinsame Teiler aller Potenzen und n ist.

Haben wir nun eine Untergruppe von D_n , die eine Spiegelung enthält (und mindestens eine Drehung: $e = d^n = d^0$), so muss diese, wie wir bereits gezeigt haben, genauso viele Drehungen wie Spiegelungen enthalten.

Betrachten wir zuerst alle Drehungen, die in dieser Menge vorhanden sein sollen. Da diese miteinander verknüpft wieder Drehungen ergeben, die auch wieder in unserer Menge sein sollen, wir zu jeder Drehung auch eine Inversdrehung fordern, weil wir ja keine Spiegelung haben, die das Inverse einer Drehung darstellt, sondern nur das Inverse zu sich selbst, und $d^0 = e$ in unserer Menge haben wollen, da wir dies auch nicht unter den Spiegelungen finden, muss die Menge unserer Drehungen selbst auch wieder eine Untergruppe von D_n darstellen. Eine solche Untergruppe muss, wie wir gerade gesehen haben, die Form $\langle d^a \rangle$ haben (mit a als Teiler von n) und die Untergruppe enthält damit $\frac{n}{a}$ Drehungen.

Suchen wir uns nun eine Spiegelung $d^x \circ s$ beliebig, die wir in dieser gemischten Untergruppe haben wollen. Dann lässt sich diese Spiegelung als $d^{k \cdot a + r} \circ s$, mit einem festen k , schreiben, und da wir alle $d^{l \cdot a}$ in unserer Menge haben, muss damit ja auch die Deckbewegung $d^{l \cdot a + k \cdot a + r} \circ s = d^{(l+k) \cdot a + r} \circ s$ in dieser Menge sein, wobei wir für $l + k$ wieder $\frac{n}{a}$ verschiedene Werte (natürlich $(\text{mod } n)$) erhalten und für $k + l = n$ auch $d^r \circ s$ in unserer Untergruppe finden.

Nun haben wir auch $\frac{n}{a}$ verschiedene Spiegelungen und damit keinen Platz mehr für weitere. Die Abgeschlossenheit macht uns hier auch keine Probleme, da die Verknüpfung von Spiegelungen uns wieder zu e führt und wir mit der Verknüpfung von Drehungen und Spiegelungen auch keine Probleme haben.

Für ein festes a bekommen wir also so viele verschiedene Untergruppen dieser Art, wie wir uns verschiedene k wählen können; dies sind a Stück (von 0 bis $a - 1$ beziehungsweise von 1 bis a).

Für jede dieser Untergruppen können wir $d^r \circ s = s'$, das ja auch in ihr liegen muss, und $d^a = d'$ setzen und haben dann offensichtlich mit dieser Umbenennung einen Isomorphismus zu der Diedergruppe $D_{\frac{n}{a}}$.

Damit haben wir dann für jedes a , das n teilt, a zu $D_{\frac{n}{a}}$ isomorphe Untergruppen. Kehren wir nun zu unserem Anliegen zurück: Wir wollten zeigen, dass wir mit unserem zyklischen Untergruppen $\langle d^a \rangle$ und unseren Diedergruppen D_a alle Untergruppen von

D_n betrachtet haben, wenn q ein Teiler von n ist.

Dieses Problem lösen wir folgendermaßen: Wir versuchen, Untergruppen zu bauen. Um eine Untergruppe zu erhalten, brauchen wir zunächst ein Element, das in ihr liegt. Ist dies eine Drehung, so erhalten wir eine zyklische Untergruppe $\langle d^q \rangle$. Geben wir nun weitere Drehungen hinzu, so wird sich an der Tatsache, dass wir eine zyklische Untergruppe der Form $\langle d^x \rangle$ haben, wie wir sukzessiv zeigen können, nichts ändern.

Gehen wir nun von einer Spiegelung aus, oder geben wir zu einer Drehgruppe Spiegelungen hinzu, so kommen wir, wie wir gesehen haben, zu einer Diedergruppe $D_{\frac{n}{q}}$.

Nun können wir auch sehen, dass es diese Untergruppen für jeden Teiler q von n gibt, da wir für jeden Teiler q die Möglichkeit haben, uns Dreh- und Diedergruppen zu konstruieren, denn wenn q ein Teiler von n ist, so finden wir eine Drehung, die einen Exponenten besitzt, der als größten gemeinsamen Teiler q mit n gemeinsam hat, zum Beispiel d^q selbst. Diese Drehung erzeugt dann eine zyklische Untergruppe $\langle d^q \rangle$ (beziehungsweise mit einer Spiegelung eine Diedergruppe $D_{\frac{n}{q}}$).

Allgemein haben wir auch schon gezeigt, dass alle zyklischen Untergruppen $\langle d^q \rangle$ Normalteiler von D_n sind und für die Untergruppen, die Diedergruppen darstellen, nur $D_{\frac{n}{2}}$ einen Normalteiler von D_n darstellt.

Damit haben wir also alle Untergruppen und Normalteiler einer Diedergruppe D_n gefunden.

5 Codierungstheorie

5.1 Allgemeine Einführung

Um uns genauer mit der Codierungstheorie auseinanderzusetzen, müssen wir zunächst einige wichtige Begriffe klären.

Im Allgemeinen bestehen Daten aus Elementen eines bestimmten *Alphabets*, einer Menge von Zeichen, werden mit Hilfe einer Codierung in eine Folge von Elementen eines (meist anderen) Alphabets transformiert; eine Folge von Elementen (oder auch *Buchstaben*) eines Alphabets nennt man auch ein *Wort* (über dem Alphabet A). Im Besonderen nennt man eine injektive Abbildung der Elemente eines Alphabets A auf Wörter über einem Alphabet B eine *Codierung*. Eine Abbildung g ist *injektiv*, falls $f(a) = f(b)$ nur für $a = b$ erfüllt ist, also wenn keine zwei verschiedenen Elemente der Definitionsmenge von g , dieselben Bilder haben. Nun kann man aber mit Hilfe einer Codierung auch ganze Wörter, die aus einem Alphabet gebildet werden können, codieren, indem man nacheinander jedes Element des Alphabets, aus dem das Wort gebildet wurde, codiert. Auch eine solche Abbildung, die, durch sukzessive Codierung der Elemente eines Alphabets, Wörter wieder auf Wörter über ein anderes Alphabet abbildet, nennt man auch Codierung. Dabei ist die Abbildung jedoch nicht mehr unbedingt injektiv. Es kann zum Beispiel folgender Fall auftreten (wobei g eine Codierung ist): $g(a) = y$, $g(b) = z$ und $g(c) = yz$ ($ab \neq c$). Nun folgt (durch unsere sukzessive Codierung g'), dass $g'(ab) = g(a)g(b) = yz = g(c)$. Wenn für alle Elemente a des Alphabets A jedoch alle Bilder $g(a)$ die gleiche Länge n haben, so kann man eindeutig aus jedem gegebenen möglichen Bild zuerst die ersten n Zeichen betrachten; und dann kann man ja wegen der Injektivität von g auf a schließen. Dieses Verfahren kann man fortsetzen, bis man das Ende des Bildworts erreicht hat. (vgl. [9], S. 32)

Die Verwendung von Codierungen hat in der Praxis viele Vorteile; es gibt Codes, wie den ISBN-Code, den wir noch genauer kennenlernen werden, die es uns ermöglichen, eine Aussage zu treffen, ob uns bei einer Übertragung der codierten Daten ein Fehler unterlaufen ist. Darüberhinaus ermöglicht es uns die Codierungstheorie, Daten zu komprimieren: Das Wort `aaaaaaaaabhgop`, das wir aus dem uns bekannten Alphabet bilden können, lässt sich zum Beispiel in das Wort `Za9bhgop` transformieren, wobei wir den Buchstaben `Z` als Indikator verwenden (er sollte also von Anfang an als solcher reserviert sein und nicht in unserem Urwort vorkommen) und uns mit den darauffolgenden

Zeichen angibt, dass an dieser Stelle neunmal der Buchstabe a eingefügt werden soll. In der Praxis gibt es auch noch andere Kompressionstechniken, wie zum Beispiel die „statistische Codierung“, bei der häufig zu erwartende Symbole durch kurze Codewörter und seltenere Symbole durch längere Codewörter beschrieben werden. ([9], S. 41)

Diese und ähnliche Kompressionstechniken ermöglichen es uns im Computerbereich, Dateien auf Datenträgern platzsparend zu lagern oder ermöglichen uns erst, dass Dateien auf einen Datenträger passen und natürlich auch einen schnelleren (und mit Hilfe von fehlererkennenden Codes auch sichereren) Datenaustausch über Netzwerkverbindungen. Mit Hilfe der Codierungstheorie kann man diese Daten auch verschlüsseln, so dass sie nur Personen, die über die zum Entschlüsseln wichtigen Informationen verfügen, wieder entschlüsseln und damit lesen können. (vgl. [9], S. 40f)

5.1.1 Die ISBN-Codierung und Allgemeines über Prüfzeichencodierungen

Ein Beispiel für einen fehlererkennenden Code ist die Codierung mit Hilfe der ISBN (International Standard Book Number). „Von westlichen Verlagen herausgegebene Bücher werden seit einiger Zeit mit Nummern versehen, aus denen Land, Verlag und Buch zu identifizieren sind.“ ([9] S.56) Das Buch [9] von Ralph Har do Schulz zum Beispiel hat die ISBN 3 – 528 – 06419 – 6, wobei die 3 für das Land, die 528 für den Verlag und die 06419 für den Artikel stehen. Die 6 ist eine Prüfziffer, die es uns (unter Umständen) erlaubt, eine Aussage über die Richtigkeit der Nummer zu machen: Erfüllt die Prüfziffer eine bestimmte Kontrollgleichung nicht, so können wir uns sicher sein, dass ein Fehler aufgetreten ist, erfüllt sie diese aber, dann können wir immer noch keine genaue Aussage darüber treffen, ob sie richtig ist. Eine gültige ISBN-Nummer $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10}$ muss die Prüfgleichung

$$a_{10} \equiv \sum_{i=1}^9 i \cdot a_i \pmod{11}$$

erfüllen. Man verwendet hier die Summe modulo 11, was zur Folge hat, dass auch der Fall $a_{10} = 10$ auftreten kann; wir müssen also unser Alphabet $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, aus dem wir die endgültige Nummer bilden wollen, um eine Stelle erweitern. Man hat als Symbol für die 10 den Buchstaben X gewählt. Es stellt sich nun die Frage, ob die Verwendung der Summe modulo 11, die uns zwingt, unser Alphabet zu erweitern, uns auch irgendwelche Vorteile verschafft. Dies tut sie, da bei einem Einzelfehler in der j -ten Stelle die Summe folgendermaßen aussieht (vgl. auch [9], S. 59):

$$\sum_{i=1, i \neq j}^9 i \cdot a_i + j \cdot a'_j = \sum_{i=1}^9 i \cdot a_i - j \cdot a_j + j \cdot a'_j \equiv a_{10} + j \cdot (a'_j - a_j) \pmod{11} \quad (5.1)$$

Damit ein solcher Fehler erkannt werden kann, darf der Term $j \cdot (a'_j - a_j)$ allerdings nicht durch 11 teilbar sein. Dieser Fall kann jedoch gar nicht eintreten, da 11 eine Primzahl

ist: Das Produkt $j \cdot (a'_j - a_j)$ besteht aus den Faktoren j und $a'_j - a_j$; j kann sich ja nur zwischen 1 und 9 bewegen, hat also auf jeden Fall keinen Teiler $t \neq 1$ mit 11 gemeinsam und auch der Betrag des zweiten Faktors kann sich zwischen 1 und 9 bewegen (wir gehen davon aus, dass $a'_j \neq a_j$, also dass ein Fehler aufgetreten ist) und wir wissen, dass $-a \pmod{n} = n - a \pmod{n}$. Also kann das gesamte Produkt gar kein Vielfaches von 11 sein, da 11 keinen Teiler $t \neq 1$ mit einem Faktor gemeinsam hat. Ein einzelner Fehler der ersten neun Stellen wird also auf diese Weise erkannt, was bei Verwendung von $(\text{mod } 10)$ nicht gewährleistet hätte sein können, zum Beispiel wenn der Fall $j = 2$ und $a'_j - a_j = 5$ eintritt. Allgemein können wir aus Gleichung 5.1 erkennen, dass es, wenn wir nicht modulo 11 rechnen, sondern allgemein modulo k (wobei k allerdings größer sein sollte als das größte a_i) notwendig für die Erkennung von Einzelfehlern ist, dass alle i teilerfremd zu k sind und diese Forderung auch hinreichend für die Erkennung von Einzelfehlern ist (vgl. auch [9], S. 59).

Die Prüfgleichung kann nun auch anders formuliert und verallgemeinert werden:

$$\sum_{i=1}^9 i \cdot a_i - a_{10} \equiv 0 \pmod{11}, \quad (5.2)$$

und noch allgemeiner können wir, da wir ja die Teilerfremdheit zu einem allgemeinen k nicht für alle $i \in \{1, \dots, n\}$ garantieren können, die folgende Gleichung

$$\sum_{i=1}^n \omega_i \cdot a_i \equiv c \pmod{k} \quad (5.3)$$

als Prüfgleichung wählen. (vgl. [9], S. 59)

In unserem Fall ist $\omega_i = i$ für $i \neq 10$ und $\omega_{10} = -1$. Wir können nun von Gleichung 5.2 ausgehend (analog zur ersten Form) erkennen, dass Einzelfehler auch in der zehnten Stelle erkannt werden können.

Unsere allgemeine Gleichung 5.3 findet in der Praxis vor allem für $k = 10$ (mit ω_i ungerade und $\omega_i \neq 5$) und $k = 11$ Anwendung, wobei sich allerdings gezeigt hat, dass für $k = 11$ mehr Fehlertypen erkannt werden können als mit $k = 10$, dass hier jedoch, wie wir schon gesehen haben, eine Erweiterung des Alphabets notwendig ist (vgl. [9], S. 61).

Man kann die Abbildung von i auf den Rest von $\omega_i \cdot i$ bei Division (in unserem Fall) durch 11 als eine Permutation auffassen (vgl. auch [9] S.59) und den Begriff der Prüfzeichencodierung auf Gruppen ausweiten; den Nachweis, dass wir es hier mit Permutationen zu tun haben, werden wir hier allerdings nicht erbringen, die Tatsache, dass hier wieder 11 verschiedene Reste auftreten und für keine zwei i aus unserem Alphabet gleiche Reste auftreten, könnten wir aber wieder ähnlich zu dem Beweis, dass $\langle d^m \rangle = \langle d^a \rangle$ für den Fall, dass a der größte gemeinsame Teiler von n und m ist, den wir bei unserer Untergruppensuche geführt haben, und auch allgemein für den Fall, dass w_i teilerfremd zu k ist, zeigen.

In unserem Beispiel haben wir für $\omega_i = 8$ die folgenden Reste bei Division mit 11 und erkennen sofort, dass wir es hier mit einer Permutation zu tun haben, wobei wir allerdings das Alphabet um die 10 erweitern.

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 8 & 5 & 2 & 10 & 7 & 4 & 1 & 9 & 6 & 3 \end{pmatrix}$$

5.2 Gruppen in der Codierungstheorie

[9] definiert die Prüfzeichencodierung über einer Gruppe folgendermaßen ([9], S.61):

Definition 11. Sei A ein Alphabet und $G = (A, \cdot)$ eine Gruppe mit zugrundeliegender Menge A . Dann ist eine Prüfzeichen-Codierung über der Gruppe G definiert durch n Permutationen $\delta_1, \dots, \delta_n$ von A , ein Element $c \in G$ zusammen mit der Kontrollgleichung

$$\prod_{i=1}^n \delta_i(a_i) = c.$$

Man kann erkennen, dass die Verwendung von Permutationen äußerst sinnvoll ist, da diese ja bijektive Abbildungen einer Menge A auf sich selbst sind. Haben wir nun einen Einzelfehler in der j -ten Stelle vorliegen, so ist mit $a_j \neq a'_j$ dann nämlich ja auch $\delta_j(a_j) \neq \delta_j(a'_j)$. Da die anderen $a_i \in A$ mit $i \neq j$ ja alle gleichbleiben, bleiben damit auch alle $\delta_i(a_i)$ gleich. Nun kann es in einer Gruppe aber nicht vorkommen, dass $k \circ x \circ l = k \circ y \circ l$ für $x \neq y$ (wir könnten nämlich auf beiden Seiten von links mit k^{-1} und von rechts mit l^{-1} operieren). Damit ist das gesamte Produkt der linken Seite unserer Kontrollgleichung mit Einzelfehler auf keinem Fall gleich dem gültigen Produkt ohne Einzelfehler.

Dies bedeutet, dass wir mit einer Prüfzeichencodierung über einer Gruppe immer alle Einzelfehler erkennen können (vgl. [9], S. 62).

5.2.1 Anwendung: Nummerierung der deutschen Geldscheine mit Hilfe von D_5

Die Idee der Gruppe wird auch in der Codierungstheorie angewendet: Mit Hilfe der Diedergruppe D_5 des regelmäßigen 5-Ecks wurden zum Beispiel die Geldscheine, die die Deutsche Bundesbank seit Herbst 1990 ausgegeben hat, nummeriert.

Zu diesem Zweck können wir die Elemente von D_5 mit den Ziffern $0, 1, \dots, 9$ wie folgt codieren (vgl. [9], S. 64):

$d^i \mapsto i; d^i s \mapsto i + 5$, wobei d die Drehung um 72° und s eine Spiegelung an einer festen Symmetrieachse des regelmäßigen 5-Ecks ist. Wir können jetzt also eine codierte Gruppentafel erstellen, die auch in [9] (S. 65) abgebildet ist:

.	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Dabei verwendete die Deutsche Bundesbank auch Buchstaben in ihren Kennnummern, die sich wie folgt in eine unserer Ziffern $0, 1, \dots, 9$ überführen lassen (vgl. [9], S. 65):

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

Eine solche (11-stellige) Kennnummer $a_1 a_2 \dots a_{10} a_{11}$ muss die folgende Prüfgleichung erfüllen:

$$T(a_1)T^2(a_2)T^3(a_3)T^4(a_4)T^5(a_5)T^6(a_6)T^7(a_7)T^8(a_8)T^9(a_9)T^{10}(a_{10})a_{11} = 0, \quad (5.4)$$

wobei die Permutation T folgendermaßen aussieht ([9], S. 66):

$$T = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$$

Desweiteren ergibt sich für die Potenzen von T , wie sie zum Beispiel auch in [9] (S.66) aufgelistet sind

$$\begin{aligned} T^2 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 0 & 3 & 7 & 9 & 6 & 1 & 4 & 2 \end{pmatrix}, & T^3 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 1 & 6 & 0 & 4 & 3 & 5 & 2 & 7 \end{pmatrix}, \\ T^4 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 5 & 3 & 1 & 2 & 6 & 8 & 7 & 0 \end{pmatrix}, & T^5 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 8 & 6 & 5 & 7 & 3 & 9 & 0 & 1 \end{pmatrix}, \\ T^6 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 3 & 8 & 0 & 6 & 4 & 1 & 5 \end{pmatrix}, & T^7 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 0 & 4 & 6 & 9 & 1 & 3 & 2 & 5 & 8 \end{pmatrix}, \end{aligned}$$

und schließlich

$$T^8 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = \text{id.}$$

Diese Permutation T wurde von Verhoeff [12] mit Hilfe von Computern gefunden (vgl.[8],

S.13) und erfüllt, wie auch wir durch Ausprobieren aller möglichen x, y zeigen könnten, folgende Bedingung für alle $x, y \in \{0, 1, \dots, 9\}$ mit $x \neq y$:

$$x \cdot T(y) \neq y \cdot T(x)$$

Dies bedeutet, dass eine Vertauschung zweier (verschiedener) benachbarter Ziffern (außer der beiden letzten) erkannt werden kann, denn dann muss ja

$$T(a_1) \cdot \dots \cdot T^i(a_i) \cdot T^{i+1}(a_{i+1}) \cdot \dots \cdot a_{11} \neq T(a_1) \cdot \dots \cdot T^i(a_{i+1}) \cdot T^{i+1}(a_i) \cdot \dots \cdot a_{11}.$$

Also muss (nach sukzessivem Kürzen von Links und Rechts: Wir haben ja $T^{-k} = T^{8-k}$) $T^i(a_i) \cdot T^{i+1}(a_{i+1}) \neq T^i(a_{i+1}) \cdot T^{i+1}(a_i)$ gelten. Setzen wir nun $T^i(a_i) = x$ und $T^i(a_{i+1}) = y$ (man beachte, dass damit $x, y \in \{0, 1, \dots, 9\}$ liegen), so gelangen wir nun mit Hilfe von

$$T^i(a_i) \cdot T^{i+1}(a_{i+1}) = T^i(a_i) \cdot T(T^i(a_{i+1}))$$

und von

$$T^i(a_{i+1}) \cdot T^{i+1}(a_i) = T^i(a_{i+1}) \cdot T(T^i(a_i))$$

zur Forderung

$$x \cdot T(y) \neq y \cdot T(x) \quad (\text{vgl. [9], S. 62}).$$

Leider kann uns eventuell die Vertauschung der letzten beiden Ziffern entgehen, da ja der Term $T^{10}(a_{10}) \cdot a_{11}$ nicht die Form $T^i(a_i) \cdot T^{i+1}(a_{i+1})$ hat, die wir bei der Erstellung unserer Forderung verwendet haben.

Desweiteren lassen sich, wie wir schon für alle Prüfzeichencodierungen über Gruppen gezeigt haben, hier auch alle Einzelfehler erkennen; mit Hilfe der Diedergruppe D_5 ist es uns also gelungen, eine Codierung zu finden, die es uns ermöglicht, die beiden (nach [9] (S. 58), wo die Ergebnisse der Untersuchung der relativen Häufigkeiten der verschiedenen Fehlertypen in [12] aufgelistet sind) häufigsten Fehlertypen sehr sicher zu erkennen.

5.2.2 Überprüfen einer Kennnummer

Konkret können wir jetzt an einem Beispiel überprüfen, ob wir einen gültigen Geldschein besitzen: Die Kennnummer eines 10-DM Scheines lautet GL1445302A7. Wir können jetzt auf die codierte Nummer schließen. Diese lautet nun 24144530207; die Prüfgleichung

$$T(2) \cdot T^2(4) \cdot T^3(1) \cdot T^4(4) \cdot T^5(4) \cdot T^6(5) \cdot T^7(3) \cdot T^8(0) \cdot T^9(2) \cdot T^{10}(0) \cdot 7 = 0$$

muss also erfüllt sein. Diese linke Seite der Prüfgleichung lautet nach Anwenden der Permutationen

$$7 \cdot 7 \cdot 9 \cdot 1 \cdot 5 \cdot 0 \cdot 6 \cdot 0 \cdot 7 \cdot 5 \cdot 7,$$

nach Vereinfachen mit Hilfe unserer codierten Gruppentafel

$$0 \cdot 8 \cdot 5 \cdot 6 \cdot 2 \cdot 7,$$

einer weiteren Vereinfachung

$$8 \cdot 4 \cdot 9,$$

und schließlich

$$9 \cdot 9 = 0,$$

womit die Prüfgleichung erfüllt ist, also unsere Kennnummer existiert.

6 Ausblick

Die Gruppentheorie hat jedoch auch noch weitere Anwendungen gefunden. Auf der Idee der Gruppe beruht zum Beispiel auch die Galois¹-theorie:

Galois ordnete jeder Gleichung eindeutig eine Permutationsgruppe zu, aus deren Struktur er Aussagen über die Struktur der Lösungen der Gleichungen treffen konnte ([13], S. 75). Aus seiner Theorie konnte er einerseits wieder das damals schon bekannte Lösungsverfahren für Gleichungen vierten Grades ableiten und andererseits kann man darauf schließen, dass Gleichungen mit höherem Grad als vier im Allgemeinen nicht mehr (durch sogenannte Radikale) lösbar sind.

Die Gruppentheorie spielt auch eine entscheidende Rolle beim gerade erst gefundenen Beweis von „Fermats letztem Satz“², der besagt, dass die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine ganzzahligen Lösungen besitzt. Wir kennen eine ähnliche Gleichung bereits als Satz des Pythagoras (für $n = 2$), die jedoch ganzzahlige Lösungen, die sogenannten „pythagoreischen Zahlentripel“ — von denen es unendlich viele gibt (vgl. [11], S. 347f)— besitzt. Es ist verwunderlich, dass es solche Zahlentripel für $n \geq 3$ offenbar gar nicht mehr geben kann.

Über diesen Satz, den er selbst gefunden hat, als er versuchte, den Satz des Pythagoras abzuwandeln und auf diesem Weg noch etwas über pythagoreische Zahlentripel herauszufinden, machte Pierre de Fermat neben seiner berühmten Vermutung in seine Ausgabe des Buches *Arithmetica* von Diophantos auch noch eine weitere Randnotiz vgl. [11] S. 85ff) :

„Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.“ ([11], S. 87)

Diese Randnotiz bedeutet (frei) übersetzt:

„Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist dieser Rand hier zu schmal, um ihn zu fassen.“ ([11], S. 87)

Mit dieser Randnotiz bewegte Fermat die Welt der Mathematik für mehr als 300 Jahre, bis endlich Andrew Wiles³ im Jahre 1994 einen Beweis für diesen Satz veröffentlichte, bei dem er unter Anderem auf Galois-Gruppen zurückgriff (vgl. [11], S. 264).

¹Evariste Galois (1811-1832) war ein bedeutender französischer Mathematiker, der, wie auch Niels H. Abel, wichtige Erkenntnisse über die Auflösbarkeit algebraischer Gleichungen fand.

²Pierre de Fermat (1601-1665) war neben seiner Tätigkeit als Richter auch ein wichtiger Mathematiker.

³Andrew Wiles ist Mathematikprofessor in Princeton.

Der Beweis selbst ist zu komplex (und auch zu lang), um in dieser Facharbeit ausführlich behandelt zu werden, doch dieser kleine Ausblick dürfte den Leser von der zentralen Stellung der Gruppentheorie in der modernen Mathematik überzeugt haben.

Literaturverzeichnis

- [1] ADLER, IRVING: *Gruppen in der Neuen Mathematik*. Vieweg, Braunschweig, 1974.
- [2] FISCHER, G. und R. SACHER: *Einführung in die Algebra*. B.G. Teubner, Stuttgart, 3. überarbeitete Auflage, 1983.
- [3] FISCHER, GERD: *Lineare Algebra*. Vieweg, Braunschweig/Wiesbaden, 11., verbesserte Auflage, 1997.
- [4] KARGAPOLOV, M. I. and JU. I. MERTLJAKOV: *Fundamentals of the Theory of Groups*, volume 62 of *Graduate texts in mathematics*. Springer Verlag, New York, 1979.
- [5] KNUTH, DONALD E.: *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming*. Addison Wesley, third edition, 1997.
- [6] LUCHA, WOLFGANG und FRANZ F. SCHÖBERL: *Gruppentheorie - Eine Einführung für Physiker*, Band 697 der Reihe *BI Hochschultaschenbuch*. BI Wissenschaftsverlag, Mannheim, 1993.
- [7] NEWMAN, JAMES R. (editor): *The World of Mathematics*. Simon and Schuster, New York, 1956.
- [8] SCHULZ, RALPH HARDO: *Prüfziffern und Teilbarkeit*. Der Mathematikunterricht, September 1990.
- [9] SCHULZ, RALPH HARDO: *Einführung in die Codierungstheorie*. Vieweg, Braunschweig, 1991.
- [10] SIELAFF, KLAUS: *Einführung in die Theorie der Gruppen*. Diesterweg Salle, Frankfurt am Main, 5. Auflage, 1971.
- [11] SINGH, SIMON: *Fermats letzter Satz*. dtv, München, 6. Auflage, 2000.
- [12] VERHOEFF, J.: *Error detecting Decimal Codes*, volume 29 of *Math. Centre Tracts*. Math. Centrum Amsterdam, 1969.
- [13] WUSSING, H.: *Die Genesis des abstrakten Gruppenbegriffs*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1969.