Prüfziffersysteme über Quasigruppen

H. Michael Damm

März 1998

Diplomarbeit
am Fachbereich Mathematik und Informatik der
Philipps-Universität Marburg

Betreuer: Prof. Dr. H. Peter Gumm
Zweitgutachter: Prof. Dr. A. Dressler

Prüfziffersysteme über Quasigruppen

Zusammenfassung

Der Begriff *Prüfziffersystem* wurde von H.P. Gumm 1985 eingeführt. Wir untersuchen Prüfziffersysteme über Gruppen und Quasigruppen. Zu jeder Ordnung größer als zwei existiert ein Prüfziffersystem, das alle Einzelfehler und alle Nachbarvertauschungen erkennt. Für den wichtigen Spezialfall der Prüfziffersysteme über Gruppen der Ordnung 10 zeigen wir allerdings, daß diese nicht alle Zwillings-, Sprungzwillingsfehler oder Sprungtranspositionen erkennen.

Bei den Prüfziffersystemen über Quasigruppen werden wir sehen, daß verschiedene Ansätze das Problem ebenfalls nicht lösen können. Dennoch werden wir ein Prüfziffersystem zur Basis 10 angeben, das eine Fehlererkennung von 99,89% aller nicht zufälligen Fehler aufweist.

Inhaltsverzeichnis

Einleitung

Prüfziffern sind unscheinbar und allgegenwärtig. Sie werden von Banken benutzt, um falsch erfaßte Kontonummern oder Bankleitzahlen zu erkennen, der Buchhandel spürt mit ihrer Hilfe falsche ISBN-Nummern auf und schließlich bemerkt der Laserscanner an den Kassen im Supermarkt anhand einer falschen Prüfziffer, daß er den Strichcode der Artikelnummer falsch eingelesen hat.

Die grundlegende Idee besteht darin, daß man aus der vorgegebenen Zahl eine weitere Ziffer berechnet, welche in die Zahl eingebaut wird. Diese Prüfziffer wird so bestimmt, daß Eingabe und Übertragungsfehler erkannt werden können. Dabei wird die errechnete Ziffer mit der Prüfziffer verglichen. Stimmen diese nicht überein, dann wurde die ursprüngliche Zahl verfälscht. Die Prüfziffer wird in der Praxis fast immer an die zu sichernde Zahl angehängt, grundsätzlich spricht aber nichts dagegen, sie in der Mitte einzufügen oder sie an den Anfang zu stellen.

Fehlerstatistik

Um die Qualität eines Prüfzifferverfahrens beurteilen zu können, muß man natürlich zuerst die Art der möglichen Eingabefehler sowie deren Häufigkeit feststellen. Verhoeff [27] hat Ende der sechziger Jahre eine entsprechende Untersuchung mit 6-stelligen Zahlen durchgeführt. Dabei wurde deutlich, daß die sogenannten Einzelfehler, d.h. eine falsch eingegebene Ziffer, am häufigsten vorkommt (siehe Tabelle). Bereits mit großem Abstand folgt die zweithäufigste Fehlerart, nämlich die Vertauschung zweier benachbarter Ziffern (Zahlendreher), vor den anderen möglichen Fehlern.

Fehlerart		Symbol	Häufigkeit
1.	eine falsche Ziffer (Einzelfehler)	$x \to y$	79,0 %
2.	Nachbarvertauschung (Vertauschung einer Ziffer mit der nächsten)	$xy \to yx$	10,2 %
3.	Sprungtransposition (Vertauschung einer Ziffer mit der übernächsten)	$xzy \to yzx$	0,8 %
4.	Zwillingsfehler	$xx \to yy$	0,6 %
5.	phonetische Fehler ($a = 2, ..., 9$)	$a0 \leftrightarrow 1a$	0,5 %
6.	Sprung-Zwillingsfehler	$xzx \to yzy$	0,3 %
7.	sonstige/zufällige Fehler	-	8,6 %

Phonetische Fehler entstehen durch die Verwechslung ähnlich klingender Zahlen, zum Beispiel von „fünfzig" und „fünfzehn". Die Anzahl der Fehler dieses Fehlertyps hängt natürlich von der Sprache ab, d.h. VERHOEFFS Untersuchung gilt genaugenommen nur für die holländische und ähnliche Sprachen wie Deutsch und Englisch.

Im Deutschen existiert eigentlich noch eine weitere Klasse phonetischer Fehler, denn die Zahl 35 (fünf-und-dreißig) wird häufiger mit der 53 verwechselt als z.B. im Englischen (thirty-five). Diese Fehler werden allerdings schon durch die Nachbarvertauschungen abgedeckt und müssen daher nicht gesondert betrachtet werden.

In der Klasse der sonstigen und zufälligen Fehler befinden sich alle sehr seltenen Fehlerarten, wie z.B. $xyx \to yxy$, $wxyz \to xwzy$ oder $xxxx \to yyyy$, sowie Fehler, bei denen kein offensichtlicher Zusammenhang zwischen der korrekten und der fehlerhaften Zahl besteht. Auch wenn kein offensichtlicher Zusammenhang zwischen den Zahlen besteht, kann es trotzdem eine versteckte Verbindung geben, z.B. könnten beide Zahlen zur selben Person gehören, eine ist seine Telefonnummer und die andere seine Kontonummer. Eine andere Möglichkeit besteht darin, daß die korrekte Kundennummer eines anderen Kunden eingegeben wird. Es ist unmöglich jeden dieser Fehler zu erkennen, man kann allerdings erwarten, daß durch die Redundanz des Codes (Zahl + Prüfziffer) eine große Anzahl der zufälligen Fehler erkannt wird.

Eine Fehlerklasse, die nicht weiter betrachtet wird, bildet das Einfügen oder Weglassen einzelner Ziffern. Die Häufigkeit dieser Fehler liegt zwischen zehn und zwanzig Prozent, wobei die letzte Ziffer und die 0 am häufigsten betroffen sind. Es ist also nicht sinnvoll, fehlende Nullen nach der Eingabe automatisch zu ergänzen. Ansonsten fallen fehlende Ziffern anhand der abweichenden Stellenzahl auf.

Mit zunehmender Stellenzahl nimmt sowohl die relative als auch die absolute Häufigkeit von (Mehrfach-)Fehlern zu. Da VERHOEFF die Fehlerstatistik mit sechsstelligen Zahlen ermittelt hat, können die ermittelten Zahlen im allgemeinen nur als Anhaltswerte angesehen werden. So kann, gemäß VERHOEFF, die

Fehlerhäufigkeit von Doppelfehlern (d.h. die Summe der Fehler 2-6) durchaus zwischen zehn und zwanzig Prozent schwanken. Die Fehler verteilen sich auch nicht gleichmäßig auf die einzelnen Stellen, vielmehr sind die letzten beiden Stellen im Vergleich mit den anderen etwa doppelt so häufig betroffen.

Ein weiterer Faktor, der sowohl die absolute als auch die relative Fehlerhäufigkeit beeinflußt, ist die Art der Datenübertragung. Bei der Übermittlung per Telefon ist sicherlich eine andere Fehlerverteilung zu erwarten, als beim Übertragen von hand- oder maschinengeschriebenen Texten.

Kapitel 1

Prüfziffersysteme über Gruppen

In diesem Kapitel werden Prüfziffersysteme untersucht, die auf einer vorgegebenen Gruppe basieren. Die einfachsten Verfahren sind dabei solche, die auf den Restklassenringen $\mathbb{Z}_{10}$,$\mathbb{Z}_{11}$ usw. beruhen, die sogenannten Modulo-Verfahren. Wir werden sehen, daß diese einige Nachteile besitzen und daher in den meisten Fällen in der Praxis nicht benutzt werden sollten. Aus diesem Grund werden wir Prüfziffersysteme basierend auf anderen Gruppen untersuchen. Da es nur zwei Gruppen der Ordnung 10 gibt, nämlich $\mathbb{Z}_{10}$ und die Diedergruppe D_5, sind Prüfziffersysteme basierend auf einer Diedergruppe von besonderem Interesse.

1.1 Modulo-Verfahren

Das einfachste Prüfverfahren für Zahlen mit den Ziffern 0 bis 9 besteht darin, alle Ziffern zu addieren (also die Quersumme zu bilden) und dann den 10er Rest als Prüfziffer anzuhängen. Für die Zahl $x_m x_{m-1} \dots x_1$ mit den Ziffern $x_i \in \mathbb{Z}_{10}$ wird also die Prüfziffer x_0 berechnet durch

$$x_0 \equiv x_m + x_{m-1} + \ldots + x_1 \pmod{10}$$

oder, wenn man + als Gruppenoperation von $\mathbb{Z}_{10}$ ansieht,

$$x_0 = x_m + x_{m-1} + \ldots + x_1.$$

Dieses Verfahren erkennt alle Einzelfehler, da sich beim Ändern einer Ziffer auch die Prüfziffer ändert. Für die Zahl 72201 erhält man z.B. die Prüfziffer 2, denn 7+2+2+0+1=12. Mit angehängter Prüfziffer würde also 722012 abgespeichert. Wenn nun später die Zahl 722212 eingegeben wird, kann man diese Zahl als fehlerhaft erkennen, denn 7+2+2+2+1=14 ergibt die Prüfziffer 4 ungleich 2. Da diese einfache Prüfsumme aber nicht von der Reihenfolge der Ziffern abhängt (Die Gruppe $\mathbb{Z}_{10}$ ist abelsch), wird leider keine einzige Vertauschung erkannt. Eine Eingabe von 272012 statt 722012 kann daher nicht als falsch erkannt werden.

Eine Erweiterung dieses Verfahrens besteht darin, die Prüfziffer nicht aus einer einfachen, sondern aus einer gewichteten Summe der einzelnen Ziffern zu berechnen, d.h.

$$x_0 = a_m x_m + a_{m-1} x_{m-1} + \ldots + a_1 x_1$$

mit $a_i \in \mathbb{Z}_{10}$.

Die Deutsche Post AG benutzt z.B. die Gewichte $a_i = 6$ falls i ungerade und $a_i = 1$ falls i gerade ist, um den Ident- und den Leitcode der Pakete zu sichern. Mit diesen Gewichten können zwar fast alle Nachbarvertauschungen erkannt werden, aber jetzt werden nicht mehr alle Einzelfehler erkannt. Da 6 nicht teilerfremd zu 10 ist, gilt $6 \cdot 5 = 6 \cdot 0$, d.h. es werden an allen ungeraden Positionen Verwechslungen von 5 mit 0, 1 mit 6 und so weiter nicht erkannt.

Auch die Wahl anderer Gewichte führt nicht dazu, daß sowohl alle Einzelfehler als auch alle Nachbarvertauschungen erkannt werden. Um die Einzelfehler erkennen zu können, müssen die Gewichte teilerfremd zu 10 sein. Dies führt aber dazu, daß $(a_i - a_{i-1})$ gerade ist, also ist $(a_i - a_{i-1})$ ein Nullteiler im Ring $\mathbb{Z}_{10}$ und alle Vertauschungen der Form $x_m \ldots x_i x_{i-1} \ldots x_1 \to x_m \ldots x_{i-1} x_i \ldots x_1$ bleiben unerkannt, wenn $(x_i - x_{i-1}) \equiv 5$ (modulo 10).

Auch mit einem noch allgemeineren Ansatz, bei dem statt der Multiplikation mit einem Element a_i eine Permutation auf die einzelnen Ziffern angewendet wird, kann das Problem nicht gelöst werden, denn im Abschnitt „Prüfziffersysteme über abelschen Gruppen" werden wir zeigen, daß über der Gruppe $\mathbb{Z}_{10}$ kein Prüfzifferverfahren existiert.

Die Notwendigkeit, daß sowohl die Gewichte, als auch die Differenzen benachbarter Gewichte Einheiten sein müssen, führt auf den Gedanken, eine Primzahl als Modulus zu benutzen. Die zur 10 nächste Primzahl ist die 11, so daß beim Rechnen in der Gruppe $\mathbb{Z}_{11}$ die Schwierigkeiten bei der Suche nach geeigneten Gewichten zur Fehlererkennung nicht auftreten. Es reicht vielmehr aus, daß benachbarte Gewichte verschieden sind und im Bereich von 1 bis 10 liegen, um alle Einzelfehler und Nachbarvertauschungen zu erkennen.

Ein bekanntes Beispiel einer Modulo-11-Prüfung stellen die Internationalen Standard Buchnummern (ISBN) dar. Eine ISBN hat zehn Ziffern $x_{10} \ldots x_1$ und setzt sich aus vier Abschnitten zusammen, von denen der erste das Land, der zweite den Verlag und der dritte das Buch kennzeichnet. Zuletzt folgt eine Prüfziffer, x_1, die durch die Gleichung

$$10x_{10} + 9x_9 + 8x_8 + \ldots + 2x_2 + x_1 = 0$$

bestimmt wird. Eine gültige ISBN ist z.B. 3-411-04011-4, beim Nachrechnen erhält man: $3 \cdot 10 + 4 \cdot 9 + 1 \cdot 8 + \ldots + 1 \cdot 1 + 4 = 110 \equiv 0 \pmod{11}$.

Das Modulo-11-Verfahren mit den Gewichten 2^i erkennt sogar alle nicht zufälligen Fehler, da die 2 eine primitive zehnte Einheitswurzel ist (vgl. VERHOEFF [27]).

Ein gravierender Nachteil bei den Modulo-11-Verfahren ist, daß beim Rechnen der Rest (die Prüfziffer) 10 heraus kommen kann. Es gibt verschiedene Möglichkeiten, mit diesem Problem umzugehen. Man kann etwa bei einem Rest von 10 ein nicht-numerisches Zeichen als Ersatz nehmen. So wird z.B. bei den ISBN-Prüfziffern ein 'X' als elfte Ziffer benutzt. Eine weitere Möglichkeit besteht darin, alle Zahlen, bei denen als Prüfziffer die 10 entsteht, nicht zu verwenden. Laut ECKER und POCH [9] verfährt die Dresdner Bank auf diese Weise.

Im Normalfall sollen die Prüfziffern allerdings aus den gleichen Ziffern bestehen, wie die zu sichernde Zahl. Häufig möchte man auch nicht auf eine fortlaufende Vergabe der Zahlen verzichten, abgesehen davon, daß die Redundanz durch das Weglassen einiger Zahlen deutlich erhöht wird. In den meisten Fällen ist daher das Modulo-11-Verfahren unbrauchbar. Als Alternative bietet sich die zweite Gruppe mit 10 Elementen an, nämlich die Diedergruppe. Prüfzifferverfahren basierend auf Diedergruppen bieten ebenfalls eine sehr gute Fehlererkennung, z.B. werden die Seriennummern deutscher Banknoten mit diesen gesichert. Wir behandeln diese im Kapitel „Gruppen mit Vorzeichen".

1.2 Verallgemeinerung auf beliebige Gruppen

Bei den Modulo-Verfahren wird von den Restklassenringen $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$ usw. im wesentlichen nur die additive Gruppe benötigt. Die Multiplikation dient nur dazu, eine Permutation der Ziffern zu erzeugen. Für beliebige Gruppen ist es daher sinnvoll, folgende Definition zu treffen (vergleiche SCHULZ [21]):

Definition 1 *Sei $(G, \cdot)$ eine endliche Gruppe der Ordnung n und $m \geq 2$ eine fest gewählte ganze Zahl. Dann ist ein Prüfziffersystem über der Gruppe G definiert durch ein Element $c \in G$ und $m+1$ Permutationen $\tau_m, \ldots, \tau_0$ der Grundmenge G, mit der Eigenschaft $\tau_i \circ \tau_{i-1}^{-1}(x) \cdot y = \tau_i \circ \tau_{i-1}^{-1}(y) \cdot x \Rightarrow x = y$, für $i = 1, \ldots, m$ und alle $x, y \in G$. Zu jeder Zahl $x_m x_{m-1} \ldots x_1$ wird eine Prüfziffer x_0 hinzugefügt, welche die Kontrollgleichung*

$$\tau_m(x_m) \cdot \tau_{m-1}(x_{m-1}) \cdot \ldots \cdot \tau_1(x_1) \cdot \tau_0(x_0) = c$$

erfüllt.

Lemma 1 *1. Für gegebene $x_m, x_{m-1}, \ldots, x_1$ ist die Prüfziffer x_0 eindeutig durch die Kontrollgleichung bestimmt.*

2. Jedes Prüfziffersystem über einer Gruppe erkennt alle Einzelfehler und alle Nachbarvertauschungen.

Beweis zu 1: Da τ_0 eine Permutation ist, ist die Kontrollgleichung eindeutig nach x_0 auflösbar:

$$x_0 = \tau_0^{-1}(\tau_1(x_1)^{-1} \cdot \ldots \cdot \tau_{m-1}(x_{m-1})^{-1} \cdot \tau_m(x_m)^{-1} \cdot c).$$

zu 2: Wenn wir annehmen, daß sowohl $x_m \ldots x_i \ldots x_0$ als auch $x_m \ldots x_i' \ldots x_0$ die Kontrollgleichung erfüllt, dann folgt $\tau_m(x_m) \cdot \ldots \cdot \tau_i(x_i) \cdot \ldots \cdot \tau_0(x_0) = c = \tau_m(x_m) \cdot \ldots \cdot \tau_i(x_i') \cdot \ldots \cdot \tau_0(x_0)$. Nun können sowohl links als auch rechts gleiche Elemente gekürzt werden und es folgt $\tau_i(x_i) = \tau_i(x_i')$ und damit $x_i = x_i'$. Für $x_i \neq x_i'$ können also nicht beide Zahlen $x_m \ldots x_i \ldots x_0$ und $x_m \ldots x_i' \ldots x_0$ die Kontrollgleichung erfüllen, es werden somit alle Einzelfehler erkannt.

Ebenso zeigen wir, daß alle Vertauschungen benachbarter Elemente erkannt werden. Gilt nämlich $\tau_m(x_m) \cdot \ldots \cdot \tau_i(x_i) \cdot \tau_{i-1}(x_{i-1}) \cdot \ldots \cdot \tau_0(x_0) = c = \tau_m(x_m) \cdot \ldots \cdot \tau_i(x_{i-1}) \cdot \tau_{i-1}(x_i) \cdot \ldots \cdot \tau_0(x_0)$, so folgt, nach kürzen der gleichen Elemente auf beiden Seiten, $\tau_i(x_i) \cdot \tau_{i-1}(x_{i-1}) = \tau_i(x_{i-1}) \cdot \tau_{i-1}(x_i)$. Wir setzen $y_{i-1} := \tau_{i-1}(x_{i-1})$ und $y_i := \tau_{i-1}(x_i)$, womit $\tau_i(\tau_{i-1}^{-1}(y_i)) \cdot y_{i-1} = \tau_i(\tau_{i-1}^{-1}(y_{i-1})) \cdot y_i$ folgt. Nach Voraussetzung ist damit $y_i = y_{i-1}$, also $\tau_{i-1}(x_{i-1}) = \tau_{i-1}(x_i)$ und $x_{i-1} = x_i$. Folglich werden alle Nachbarvertauschungen erkannt. □

Bemerkung Es ist für die Erkennung aller Einzelfehler erforderlich, daß die τ_i Permutationen sind. Ebenso ist die Forderung $\tau_i \circ \tau_{i-1}^{-1}(x) \cdot y = \tau_i \circ \tau_{i-1}^{-1}(y) \cdot x \Rightarrow x = y$ nicht nur hinreichend, sondern auch notwendig für die Erkennung aller Nachbarvertauschungen. Gibt es nämlich ein i und $x \neq y$ mit $\tau_i \circ \tau_{i-1}^{-1}(x) \cdot y = \tau_i \circ \tau_{i-1}^{-1}(y) \cdot x$, dann gilt für $x_i := \tau_{i-1}^{-1}(x)$ und $x_{i-1} := \tau_{i-1}^{-1}(y)$ die Gleichung $\tau_i(x_i) \cdot \tau_{i-1}(x_{i-1}) = \tau_i(x_{i-1}) \cdot \tau_{i-1}^{-1}(x_i)$ und $x_i \neq x_{i-1}$. Damit erfüllen aber die Zahlen $x_m \ldots x_i x_{i-1} \ldots x_0$ und $x_m \ldots x_{i-1} x_i \ldots x_0$ die Kontrollgleichung, d.h. es werden nicht alle Nachbarvertauschungen erkannt.

Für weitere Fehlertypen findet man folgende Bedingungen, die für alle $x, y, z \in G$ und alle i erfüllt sein müssen:

Fehlertyp	Bedingungen für die Fehlererkennung
Sprungtranspositionen	$\tau_{i+1} \circ \tau_{i-1}^{-1}(x) \cdot z \cdot y = \tau_{i+1} \circ \tau_{i-1}^{-1}(y) \cdot z \cdot x$ impliziert $x = y$
Zwillingsfehler	$\tau_i \circ \tau_{i-1}^{-1}(x) \cdot x = \tau_i \circ \tau_{i-1}^{-1}(y) \cdot y$ impliziert $x = y$
Sprungzwillingsfehler	$\tau_{i+1} \circ \tau_{i-1}^{-1}(x) \cdot z \cdot x = \tau_{i+1} \circ \tau_{i-1}^{-1}(y) \cdot z \cdot y$ impliziert $x = y$
phonetische Fehler	Für $a = 2, \ldots, n-1$ gilt $\tau_{i+1}(a)\tau_i(0) \neq \tau_{i+1}(1)\tau_i(a)$

Die Bedingungen werden ähnlich wie im obigen Lemma gezeigt. Wir verzichten daher auf einen Beweis.
Da diese Fehlertypen nur sehr selten auftauchen, werden wir uns im folgenden vorrangig mit dem Erkennen der Einzelfehler und der Nachbarvertauschungen beschäftigen. Wie wir sehen, spielen die Permutationen φ, bei denen aus $\varphi(x)\cdot y = \varphi(y)\cdot x$ die Gleichheit von x und y folgt, eine wichtige Rolle. Diese werden anti-symmetrisch genannt (vgl. Kapitel 2). Sie sind erforderlich für die Existenz eines Prüfziffersystems über einer Gruppe. Andererseits kann man mit ihnen auch ein Prüfziffersystem definieren.

Satz 1 *(vgl.* H.P. GUMM [12]*) Sei φ eine anti-symmetrische Permutation der Gruppe G, dann wird durch $\tau_i := \varphi^i$, ein beliebiges Element $c \in G$ sowie der Kontrollgleichung*

$$\varphi^m(x_m)\cdot\varphi^{m-1}(x_{m-1})\cdot\ldots\cdot\varphi(x_1)\cdot x_0 = c$$

ein Prüfziffersystem definiert.

Beweis Es ist $\tau_i \circ \tau_{i-1}^{-1} = \varphi^i \circ \varphi^{-i+1} = \varphi$ und φ erfüllt nach Voraussetzung die geforderte Bedingung. □

1.3 Prüfziffersysteme über abelschen Gruppen

In abelschen Gruppen stehen die anti-symmetrischen Abbildungen in direkter Beziehung zu den von MANN [15] 1942 eingeführten vollständigen Abbildungen. Eine Permutation φ heißt vollständig, wenn $x\cdot\varphi(x) = y\cdot\varphi(y)$ impliziert, daß $x = y$ ist (also wenn $x\cdot\varphi(x)$ wieder eine Permutation ist). Mit Hilfe der vollständigen Abbildungen ist es möglich, orthogonale lateinische Quadrate zu konstruieren.

Lemma 2 *Eine abelsche Gruppe $(G,+)$ besitzt eine vollständige Abbildung genau dann, wenn sie eine anti-symmetrische Abbildung besitzt.*

Beweis Es gilt für alle $x, y \in G$: $\varphi(x) + y = \varphi(y) + x \Leftrightarrow x - \varphi(x) = y - \varphi(y)$. Damit folgt, wenn *inv* die Abbildung $x \mapsto -x$ bezeichnet,

$$\varphi \text{ anti-symmetrisch} \Leftrightarrow inv \circ \varphi \text{ vollständig}$$

und

$$\varphi \text{ vollständig} \Leftrightarrow inv \circ (inv \circ \varphi) \text{ vollständig} \Leftrightarrow inv \circ \varphi \text{ anti-symmetrisch.}$$ □

Die Frage, wann eine endliche abelsche Gruppe eine vollständige Abbildung besitzt, wurde von PAIGE 1947 gelöst.

Theorem 1 *(*PAIGE [18]*) Eine endliche abelsche Gruppe der Ordnung n besitzt eine vollständige und damit eine anti-symmetrische Abbildung genau dann, wenn n ungerade ist oder wenn G mindestens zwei verschiedene Involutionen enthält (also die 2-Sylowgruppe von G nicht zyklisch ist).*

Beweis 1) Falls n ungerade ist, dann ist $\varphi = (x \mapsto 2x)$ eine anti-symmetrische Permutation, denn aus $2x = 2y$ oder aus $x + x + y = y + y + x$ folgt direkt $x = y$. 2) Der Fall n gerade wird konstruktiv bewiesen. Um den Beweis des Theorems zu vereinfachen, zeigen wir allerdings zunächst einige Lemmata.

Im folgenden sei $n = n(G)$ die Ordnung der Gruppe G und die Summe aller Elemente der Gruppe werde mit $p = p(G)$ bezeichnet, d.h.

$$p(G) = \sum_{x \in G} x.$$

Weiterhin sei δ eine Permutation von G und $\eta = (x \mapsto x + \delta(x))$ eine abgeleitete Abbildung. Die Ordnung von η, bezeichnet mit $O(\eta)$, sei die Anzahl der verschiedenen Elemente $\eta(x)$, für $x \in G$.

Lemma 3 *Wenn G nicht genau ein Element der Ordnung 2 besitzt, dann ist $p(G) = 0$, ansonsten ist $p(G)$ das einzige Element der Ordnung 2.*

Beweis Sei S die eindeutig bestimmte Untergruppe, die aus dem neutralen Element und allen Elementen der Ordnung 2 der Gruppe G besteht. Wenn die Ordnung von $a \in G$ größer als 2 ist, dann ist $a \neq -a$ und deshalb kommen a und $-a$ in der Summe $p(G)$ vor, folglich gilt $p(G) = p(S)$.

Hat S die Ordnung 1, dann ist $p(S) = 0$. Hat S die Ordnung 2, d.h. $S = \{0, g\}$, dann ist $p(S) = 0 + g = g$ und $p(S)$ ist das einzige Element von S (und damit auch von G) der Ordnung 2.

Es bleibt der Fall, daß die Ordnung von S größer als 2 ist. Dann hat S die Ordnung 2^k, $k > 1$ und die k Erzeugenden $g_1, \ldots, g_k$. Jedes Element von S hat eine eindeutige Darstellung der Form $n_1 g_1 + n_2 g_2 + \ldots + n_k g_k$ mit $n_i \in \{0, 1\}$. Folglich ist $p(S) = \sum(n_1 g_1 + n_2 g_2 + \ldots + n_k g_k)$, wobei über die verschiedenen Tupel $(n_1, \ldots, n_k)$ mit $n_i \in \{0, 1\}$ summiert wird. Es gibt 2^k solche Tupel, wobei an jeder Position der Wert 0 genau $2^k/2 = 2^{k-1}$-mal vorkommt. Also ist $p(S) = 2^{k-1} \cdot (g_1 + \ldots + g_k)$ und weil $k > 1$ ist, erhalten wir $p(S) = 0$. □

Lemma 4 *Eine notwendige Bedingung für $O(\eta) = n(G)$ ist, daß $p(G) = 0$.*

Korollar 1 *Wenn $p(G) \neq 0$ ist, dann ist $O(\eta) < n(G)$ für alle Permutationen δ.*

Beweis Angenommen, es existiert eine Permutation δ mit $O(\eta) = n(G)$, d.h. η ist ebenfalls eine Permutation. Die Elemente von G werden mit x_i bezeichnet $(i = 1, 2, \ldots, n)$. Es ist

$$\sum_{i=1}^{n} \eta(x_i) = \sum_{i=1}^{n} (x_i + \delta(x_i)) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} \delta(x_i)$$

und es folgt, da η und δ bijektiv sind, $p = p + p$ bzw. $p = 0$. □

Lemma 5 *Wenn für ein δ $O(\eta) \leq n - 2$, wobei $n = n(G)$, dann existiert ein δ' mit $O(\eta') > O(\eta)$.*

Korollar 2 *Es existiert ein δ mit $O(\eta) \geq n(G) - 1$.*

Beweis Sei δ eine Permutation für die $O(\eta) = r \leq n - 2$ gilt. Die Elemente von G werden mit x_i, $i = 1, \ldots, n$, bezeichnet, dabei seien $\eta(x_i)$, $i = 1, \ldots, r$ die r verschiedenen Elemente von $\eta(x)$ mit $x \in G$. Existieren $h, k > r$ mit $x_h + \delta(x_k) \neq \eta(x_i)$ für alle $i \leq r$, dann wird das Problem gelöst durch $\delta'(x_h) := \delta(x_k)$, $\delta'(x_k) := \delta(x_h)$ und $\delta'(x) := \delta(x)$ sonst. Also nehmen wir an, daß dies nicht der Fall sei.

Da $\eta(x_{r+1}) = \eta(x_i)$ für ein $i \leq r$, können wir ohne Beschränkung der Allgemeinheit annehmen, daß $\eta(x_{r+1}) = \eta(x_1)$ ist. Ist $x_1 + \delta(x_{r+2}) \neq \eta(x_i)$, für alle $i \leq r$, dann können wir $\delta'(x_1) := \delta(x_{r+2})$, $\delta'(x_{r+2}) := \delta(x_1)$ und $\delta'(x) := \delta(x)$ sonst setzen, um ein δ' mit $O(\eta') > r$ zu konstruieren (wenigstens sind dann die Elemente $\eta'(x_1), \ldots, \eta'(x_{r+1})$ paarweise verschieden). Aber wenn $x_1 + \delta(x_{r+2}) = \eta(x_i)$ für ein $i \leq r$ gilt, dann können wir o.B.d.A. annehmen, daß $x_1 + \delta(x_{r+2}) = \eta(x_2)$ $(i \neq 1$, denn $x_1 + \delta(x_{r+2}) \neq x_1 + \delta(x_1) = \eta(x_1))$.

Es gilt $x_2 + \delta(x_1) \neq \eta(x_1), \eta(x_2)$. Wenn $x_2 + \delta(x_1) \neq \eta(x_i)$, für alle $i \leq r$, können wir δ ändern durch $\delta'(x_1) := \delta(x_{r+2})$, $\delta'(x_2) := \delta(x_1)$, $\delta'(x_{r+2}) := \delta(x_2)$ und wir erhalten ein δ' mit $O(\eta') > r$ (auch hier sind wenigstens die Elemente $\eta'(x_1), \ldots, \eta'(x_{r+1})$ paarweise verschieden). Andernfalls können wir ohne Einschränkung der Allgemeinheit annehmen, daß $x_2 + \delta(x_1) = \eta(x_3)$ ist.

In dieser Weise fahren wir fort: Nehmen wir an, wir hätten die Stelle erreicht, wo

$$x_1 + \delta(x_{r+2}) = \eta(x_2), \qquad x_{i+1} + \delta(x_i) = \eta(x_{i+2}), \qquad i = 1, 2, \ldots, k \tag{1.1}$$

gilt. Hieraus erhalten wir die Gleichungen

$$\eta(x_1) + \delta(x_{r+2}) = \eta(x_{i+1}) + \delta(x_i), \qquad i = 1, 2, \ldots, k+1. \tag{1.2}$$

Dies zeigen wir durch Induktion: Es ist $\eta(x_1) + \delta(x_{r+2}) = x_1 + \delta(x_1) + \delta(x_{r+2}) = x_1 + \delta(x_{r+2}) + \delta(x_1) = \eta(x_2) + \delta(x_1)$ und für $1 \leq j \leq k$ gilt $\eta(x_{j+1}) + \delta(x_j) = x_{j+1} + \delta(x_{j+1}) + \delta(x_j) = x_{j+1} + \delta(x_j) + \delta(x_{j+1}) = \eta(x_{j+2}) + \delta(x_{j+1})$.

Nun gilt $x_{k+2}+\delta(x_{k+1}) \neq \eta(x_i)$ für alle $i \leq k+2$, denn andernfalls folgt mit 1.2 $\eta(x_i)+\delta(x_{k+2}) = x_{k+2}+\delta(x_{k+1})+\delta(x_{k+2}) = \eta(x_{k+2})+\delta(x_{k+1}) = \eta(x_i)+\delta(x_{i-1})$, bzw. $\delta(x_{k+2}) = \delta(x_{i-1})$, was unmöglich ist, da $i \leq k+2$.

Ist $x_{k+2}+\delta(x_{k+1}) \neq \eta(x_i)$ für alle $i \leq r$, dann setzen wir $\delta'(x_1) := \delta(x_{r+2})$, $\delta'(x_{i+1}) := \delta(x_i)$, $i = 1, 2, \ldots, k+1$, $\delta'(x_{r+2}) := \delta(x_{k+2})$ und erhalten eine Permutation δ' mit $O(\eta') > r$.

Gilt dagegen $x_{k+2}+\delta(x_{k+1}) = \eta(x_i)$ für ein $i \leq r$, dann können wir o.B.d.A. annehmen, daß $i = k+3$ gilt und wir können die Gleichung $x_{k+2}+\delta(x_{k+1}) = \eta(x_{k+3})$ zu den Gleichungen 1.1 dazunehmen. In jedem Fall erreichen wir, da $O(\eta)$ endlich ist, eine Summe $x_j+\delta(x_{j-1}) \neq \eta(x_i)$ für alle $i \leq r$. Damit ist der Beweis des Lemmas abgeschlossen. Das Korollar ist offensichtlich. □

Wir zeigen nun den verbleibenden Fall des Theorems.
Sei die Ordnung von G gerade (d.h. G hat wenigstens ein Element der Ordnung 2). Besitzt G eine vollständige Abbildung, dann folgt mit Lemma 4, daß $n(G) = 0$ ist und mit Lemma 3, daß G mindestens zwei Elemente der Ordnung 2 besitzt.

Hat G wenigstens zwei Involutionen, dann ist $p = p(G) = 0$. Durch das Korollar können wir annehmen, daß eine Permutation δ existiert mit $O(\eta) \geq n-1$. Mit $\eta(x_i)$, $i = 1, \ldots, n-1$ bezeichnen wir $n-1$ Elemente, die paarweise verschieden sind und mit z das verbleibende Element der Gruppe. Dann gilt

$$\sum_{i=1}^{n-1}(x_i+\delta(x_i)) = \sum_{i=1}^{n-1}\eta(x_i).$$

Wir erhalten $p-x_n+p-\delta(x_n) = p-z$ und damit $x_n+\delta(x_n) = z$, also ist $O(\eta) = n$ und G besitzt die vollständige Abbildung δ. □

Im folgenden geben wir einige Ergebnisse von SIEMON [23] wieder:

Satz 2 *(SIEMON)*

1. *Die identische Abbildung $x \mapsto x$ einer endlichen Gruppe der Ordnung n ist genau dann vollständig, wenn n ungerade ist.*

2. *Ist $\mathbb{Z}_n$ eine zyklische Gruppe der Ordnung n, dann ist die durch $f(x) := x^k$ definierte Abbildung genau dann vollständig, wenn $ggT(k,n) = 1$ und $ggT(k+1,n) = 1$.*

Beweis zu 1) Sei n ungerade, $n = 2k+1$, dann gilt $x^{2k+2} = x = (x^{k+1})^2$ also ist x^2 surjektiv und, da G endlich ist, damit auch injektiv. Folglich ist $x \mapsto x$ eine vollständige Abbildung.

Ist dagegen n gerade, dann besitzt G ein Element a der Ordnung 2, somit ist $a^2 = e = e^2$ und x^2 ist nicht injektiv, also auch keine Permutation.

zu 2) Die Eigenschaft $ggT(k,n) = 1$ bzw. $ggT(k+1,n) = 1$ ist äquivalent zu x^k bzw. x^{k+1} injektiv. Daraus folgt die Behauptung. □

Bemerkung

1. Ist $ggT(k,n) = 1$, dann ist die Abbildung $f(x) := x^k$ ein Automorphismus von $\mathbb{Z}_n$.

2. Für n gerade gibt es kein k das die Bedingung $ggT(k,n) = ggT(k+1,n) = 1$ erfüllt, denn entweder ist k oder $k+1$ gerade.

Theorem 2 *(SIEMON) Eine Gruppe G der Ordnung $n = 4k+2$, $k \geq 1$, besitzt keine vollständige Abbildung und, falls G abelsch ist, auch keine anti-symmetrische Abbildung.*

Mit etwas mehr Theorie können wir den Beweis von SIEMON deutlich verkürzen, wir verschieben ihn daher auf den Abschnitt „Gruppen mit Vorzeichen".

Korollar 3 *Eine zyklische Gruppe $\mathbb{Z}_n$ der Ordnung n besitzt eine vollständige bzw. anti-symmetrische Abbildung genau dann, wenn n ungerade ist.*

Beweis Der Fall n ungerade wurde bereits gezeigt. Ist n gerade, dann ist $n/2$ das einzige Element der Ordnung 2 in $\mathbb{Z}_n$, also besitzt $\mathbb{Z}_n$ keine vollständige Abbildung.

Korollar 4 *Über den Gruppen $\mathbb{Z}_{2k}$, $k \geq 1$, insbesondere über $\mathbb{Z}_{10}$, existiert kein Prüfziffersystem.*
Über Gruppen der Ordnung $n = 4k+2$, $k \geq 1$ existiert kein Prüfziffersystem, das alle Zwillings- oder Sprungzwillingsfehler erkennt.

Die Gruppe $\mathbb{Z}_{10}$ eignet sich also grundsätzlich nicht dazu, ein Prüfziffersystem zu definieren. Für die Erkennung der Zwillings- und Sprungzwillingsfehler benötigen wir eine vollständige Abbildung (siehe Tabelle Seite 14, $\tau_{i-1} \circ \tau_i^{-1}$ bzw. $z \cdot \tau_{i-1} \circ \tau_{i+1}^{-1}$ sind vollständige Abbildungen), daher können diese Fehler in Gruppen der Ordnung $n = 4k+2$, insbesondere $n = 10$, nicht erkannt werden.

Für den nicht abelschen Fall ist bislang noch keine vollständige Lösung bekannt. 1950 bewies BATEMANN [2], daß alle unendlichen Gruppen eine vollständige Abbildung besitzen. Also haben alle unendlichen abelschen Gruppen eine anti-symmetrische Abbildung. HALL und PAIGE [14] haben 1955 gezeigt, daß in S_n $(n > 3)$, A_n $(n > 3)$ und auflösbaren Gruppen mit nicht-zyklischer 2-Sylowgruppe eine vollständige Abbildung existiert. Sie zeigten außerdem, daß eine endliche Gruppe mit zyklischer 2-Sylowgruppe keine vollständige Abbildung besitzt und vermuteten, daß in jeder endlichen Gruppe mit nicht-zyklischer 2-Sylowgruppe eine vollständige Abbildung existiert.

Wir werden später zeigen, daß die Diedergruppe D_5 mit 10 Elementen eine anti-symmetrische Abbildung besitzt. Nach Theorem 2 besitzt sie aber keine vollständige Abbildung, d.h. im nicht abelschen Fall unterscheiden sich die beiden Begriffe voneinander.

Zum Abschluß dieses Abschnittes sei noch angemerkt, daß man auf dem direkten Produkt $G_1 \times G_2$ der Gruppen G_1 und G_2 (nicht notwendig abelsch) mit den vollständigen Abbildungen g_1 und g_2 in natürlicher Weise eine vollständige Abbildung definieren kann.

Lemma 6 *Sind g_1, g_2 vollständige Abbildungen der Gruppen G_1 bzw. G_2, dann ist $f = (x, y) \mapsto (g_1(x), g_2(y))$ eine vollständige Abbildung von $G_1 \times G_2$.*

Beweis Daß f bijektiv ist, ergibt sich aus der Bijektivität von g_1 und g_2. Ebenso folgt aus der Vollständigkeit von g_1 und g_2, daß $(x, y) \cdot f(x, y) = (x \cdot g_1(x), y \cdot g_2(y))$ eine Permutation und damit vollständig ist. □

Kapitel 2

Anti-symmetrische Abbildungen

Eine Gruppe läßt die Definition eines Prüfziffersystems genau dann zu, wenn sie eine anti-symmetrische Abbildung besitzt (siehe Kapitel 1). In diesem Kapitel beschäftigen wir uns daher ausführlich mit der Existenz, den Eigenschaften und der Konstruktion von anti-symmetrischen Abbildungen.

Definition 2 *(*Gallian [10]*) Eine Permutation φ einer Gruppe $(G, \cdot)$ heißt anti-symmetrisch, wenn für alle $x, y \in G$ gilt*

$$\varphi(x) \cdot y = \varphi(y) \cdot x \quad \Rightarrow \quad x = y.$$

Die Menge aller anti-symmetrischen Abbildungen einer Gruppe G werde mit $Ant(G)$ bezeichnet.

Bemerkung $Ant(G)$ ist für eine Gruppe G der Ordnung $n > 1$ keine Untergruppe von S_n, da die Identität nicht anti-symmetrisch ist. Es gilt nämlich für beliebige $x \neq e$

$$Id(x) \cdot e = x \cdot e = e \cdot x = Id(e) \cdot x.$$

Aus der Eigenschaft $\varphi(x) \cdot y = \varphi(y) \cdot x \Rightarrow x = y$ folgt nicht, daß φ injektiv ist, z.B. wird sie von $\varphi(x) := e$ erfüllt. Da solche Funktionen nicht alle Einzelfehler erkennen, meinen wir mit dem Begriff „anti-symmetrische Abbildung" daher immer eine anti-symmetrische Permutation.

In der Literatur (z.B. Verhoeff [27]) wird der Begriff „anti-symmetrisch" auch für Permutationen mit der Eigenschaft $y \cdot \varphi(x) = x \cdot \varphi(y) \Rightarrow x = y$ benutzt. Diese können aber bijektiv auf die anti-symmetrischen Permutationen gemäß Definition 2 abgebildet werden:

Lemma 7 *Ist φ eine Permutation mit $y \cdot \varphi(x) = x \cdot \varphi(y) \Rightarrow x = y$, dann ist φ^{-1} anti-symmetrisch.*

Beweis Es gelte $\varphi^{-1}(x) \cdot y = \varphi^{-1}(y) \cdot x$. Wir setzen $\tilde{x} := \varphi^{-1}(x), \tilde{y} := \varphi^{-1}(y)$ und es folgt $\tilde{x} \cdot \varphi(\tilde{y}) = \tilde{y} \cdot \varphi(\tilde{x})$. Nach Voraussetzung ist damit $x = y$. □

2.1 Gruppen mit anti-symmetrischen Abbildungen

In diesem Abschnitt präsentieren wir eine Arbeit von GALLIAN und MULLIN [10], welche sich mit der Existenz anti-symmetrischer Abbildungen beschäftigt. In Kapitel 1 haben wir den direkten Zusammenhang zwischen vollständigen und anti-symmetrischen Abbildungen bei abelschen Gruppen gezeigt. Diese Arbeit überträgt die wesentlichen Ergebnisse von HALL und PAIGE [14] bzgl. vollständiger Abbildungen bei nicht-abelschen Gruppen auf anti-symmetrische Abbildungen.

2.1.1 Beispiele

Definition 3 *Unter der* Diedergruppe der Ordnung $2n$ *versteht man die Gruppe* $D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$, *wobei* a, b *zwei erzeugende Elemente sind, die den Relationen* $a^n = e$ *(und* $a^m \neq e$ *für* $1 \leq m < n$*),* $b^2 = e \neq b$ *und* $ab = ba^{-1}$ *genügen. (Abkürzende Schreibweise:* $D_n =< a, b | a^n = b^2 = e, ab = ba^{-1} >$*).*

Theorem 3 *Die folgenden Gruppen besitzen anti-symmetrische Abbildungen:*

1. $D_n =< a, b | a^n = b^2 = e, ab = ba^{-1} >$, $n \geq 3$ *(die Diedergruppe der Ordnung* $2n$*)*
2. $Q_n =< a, b | a^{2n} = b^4 = e, b^2 = a^n, ab = ba^{-1} >$, $n \geq 2$
   (die verallg. Quaternionengruppe der Ordnung $4n$*)*
3. $SD_n^+ =< a, b | a^{4n} = b^2 = e, ab = ba^{2n+1} >$, n *gerade (Semi-Diedergruppe der Ordnung* $8n$*)*
4. $SD_n^- =< a, b | a^{4n} = b^2 = e, ab = ba^{2n-1} >$, n *gerade (Semi-Diedergruppe der Ordnung* $8n$*)*

Beweis 1) Die folgende Abbildung ist anti-symmetrisch: Wenn n ungerade ist, sei $\varphi(a^i) = a^{2-i}$ und $\varphi(ba^i) = ba^i$. Wenn n gerade ist, d.h. $n = 2k$, wird φ definiert durch:

$$\begin{array}{llll} \varphi(e) = b & \varphi(a) = e & & \\ \varphi(a^i) = a^{1-i} & \text{für } 2 \leq i \leq k & \varphi(a^i) = ba^{1-i} & \text{für } k+1 \leq i \leq n-1 \\ \varphi(ba^i) = a^{i+1} & \text{für } 0 \leq i \leq k-1 & \varphi(ba^i) = ba^{i+1} & \text{für } k \leq i \leq n-2 \\ \varphi(ba^{n-1}) = ba & & & \end{array}$$

2) Wir definieren φ durch

$$\begin{aligned}
\varphi(e) &= e \qquad \varphi(a^i) = ba^{-i} \quad \text{für } 1 \le i \le n \\
\varphi(a^i) &= a^{-i} \quad \text{für } n+1 \le i \le 2n-1 \\
\varphi(ba^i) &= ba^{i+1} \quad \text{für } 0 \le i \le n-2 \\
\varphi(ba^i) &= a^{i+1} \quad \text{für } n-1 \le i \le 2n-2 \qquad \varphi(ba^{2n-1}) = b
\end{aligned}$$

3) Wir definieren φ durch

$$\begin{aligned}
\varphi(a^i) &= a^{4n-1-i} \quad \text{für } 0 \le i \le 2n-1 \\
\varphi(a^i) &= ba^{4n-1-i} \quad \text{für } 2n \le i \le 4n-1 \\
\varphi(ba^i) &= ba^{4n-i} \quad \text{für } 1 \le i \le 2n \qquad \varphi(b) = e \\
\varphi(ba^i) &= a^{4n-i} \quad \text{für } 2n+1 \le i \le 4n-1
\end{aligned}$$

4) Wir definieren φ durch

$$\begin{aligned}
\varphi(a^i) &= a^{4n-1-i} \quad \text{für } 0 \le i \le 2n-1 \\
\varphi(a^i) &= ba^{4n-1-i} \quad \text{für } 2n \le i \le 4n-1 \\
\varphi(ba^i) &= a^i \quad \text{für } 0 \le i \le 2n-1 \\
\varphi(ba^i) &= ba^i \quad \text{für } 2n \le i \le 4n-1
\end{aligned}$$

zu 1) Daß die genannte Permutation für ungerades n anti-symmetrisch ist, zeigen wir im Abschnitt „Beispiele", Seite 58. Im Fall n gerade müssen wir eine Vielzahl verschiedener Fälle unterscheiden. Dazu sei $0 \le i \le k-1$ und $k \le j \le n-2$. Wir zeigen exemplarisch $\varphi(x)y \neq \varphi(y)x$ für einige $x \neq y$.

	x	y	$\varphi(x)y$		$\varphi(y)x$
a.	e	a^{i+1}	ba^{i+1}	$\neq$	a^{-i}
b.	e	a^{j+1}	ba^{j+1}	$\neq$	ba^{-j}
c.	e	ba^i	a^i	$\neq$	a^{i+1}
d.	a^{i+1}	ba^j	$a^{-i}ba^j = ba^{j+i}$	$\neq$	$ba^{j+1}a^{i+1}$
e.	ba^j	ba^{n-1}	$ba^{j+1}ba^{n-1} = a^{n-j-2}$	$\neq$	$baba^j = a^{j-1}$

Bei b. folgt aus $j+1 = n-j$ die Gleichung $2j+1 = 2k$, Widerspruch (da n gerade). Bei d. können die beiden Seiten nur gleich sein, falls $n = 2$ ist. Dann kommt dieser Fall allerdings nicht vor, da kein j existiert mit $1 \le j \le 0$. Und schließlich folgt bei e. aus $n-j-2 = j-1$ die Gleichung $2k-1 = 2j$, Widerspruch.

Die anderen Fälle und Behauptungen können analog gezeigt werden. □

2.1.2 Existenztheoreme

Theorem 4 *Sei G eine Gruppe und a ein Element von G. Die Abbildung $\varphi(x) = x^{-1}a$ ist genau dann anti-symmetrisch, wenn a mit keinem Element der Ordnung 2 kommutiert.*

Beweis Sei $\varphi(x) = x^{-1}a$ anti-symmetrisch. Offensichtlich ist φ für jedes a eine Permutation. Es ist also ausreichend zu untersuchen für welche a gilt: $x \neq y \Rightarrow \varphi(x)y \neq \varphi(y)x$. Angenommen es existieren verschiedene x und y s.d. $\varphi(x)y = \varphi(y)x$ oder äquivalent dazu $x^{-1}ay = y^{-1}ax$ gilt. Multiplikation von links mit y und von rechts mit x^{-1} ergibt

$$(yx^{-1})a(yx^{-1}) = a. \tag{2.1}$$

Wir setzen $z := yx^{-1}$. Es folgt $a^2z = zazaz = za^2$ und mit Induktion

$$a^{2n}z = za^{2n} \qquad \text{für alle } n \tag{2.2}$$

Wenn die Ordnung von a gerade ist, z.B. $2m$, dann hat a^m die Ordnung 2 und kommutiert mit a. Wenn andererseits die Ordnung von a ungerade, d.h. $2k+1$ ist, dann folgt mit 2.2:

$$za = za^{2(k+1)} = a^{2(k+1)}z = az$$

Also kommutiert z mit a. Benutzt man diese Eigenschaft zusammen mit 2.1, dann erhält man

$$zaz = z^2a = a.$$

Folglich hat $z = yx^{-1}$ die Ordnung 2 und kommutiert mit a. Dies zeigt, daß $\varphi(x) := x^{-1}a$ eine anti-symmetrische Abbildung ist, wenn a mit keinem Element der Ordnung 2 kommutiert.

Um den Beweis abzuschließen, nehmen wir an, daß a mit einem Element z der Ordnung 2 kommutiert. Es folgt, daß $\varphi(x) := x^{-1}a$ nicht anti-symmetrisch ist, denn es gilt:

$$\varphi(z)e = z^{-1}a = za = az = e^{-1}az = \varphi(e)z$$

und $z \neq e$. □

Korollar 5 *Alle Gruppen mit ungerader Ordnung besitzen eine anti-symmetrische Abbildung.*

Beweis Da eine Gruppe mit ungerader Ordnung kein Element der Ordnung 2 besitzt, ist $\varphi(x) := x^{-1}a$ eine anti-symmetrische Abbildung für alle a. □

Korollar 6 *Für alle $n > 2$ besitzen die symmetrischen Gruppen S_n und die alternierenden Gruppen A_n anti-symmetrische Abbildungen.*

Beweis Wenn n ungerade ist, ist jeder n-Zykel in A_n und kommutiert mit keinem Element der Ordnung 2. Ist n gerade so gilt dies für jeden $(n-1)$-Zykel. □

Korollar 7 *Wenn eine endliche Gruppe ein Element a besitzt, dessen Zentralisator $Z(a)$ ungerade Ordnung hat, dann besitzt die Gruppe eine anti-symmetrische Abbildung.*

Beweis Wenn die Ordnung von $Z(a) = \{x \in G | xa = ax\}$ ungerade ist, dann kommutiert a mit keinem Element der Ordnung 2. □

2.1.3 Erweiterungstheoreme

Theorem 5 *Sei G eine Gruppe mit Normalteiler H und es existieren anti-symmetrische Abbildungen φ auf H und ψ auf G/H, dann existiert eine anti-symmetrische Abbildung γ auf G. Kurz gesagt: Die Klasse der Gruppen mit anti-symmetrischen Abbildungen ist gegen Erweiterung abgeschlossen.*

Beweis Seien $u_1H, \ldots, u_rH$ die Elemente von G/H. Wir definieren die Abbildung $\psi^* : \{u_1, \ldots, u_r\} \to \{u_1, \ldots, u_r\}$ durch die Bedingung

$$\psi^*(u_i)H = \psi(u_iH). \tag{2.3}$$

Da jedes Element von G eindeutig als Produkt $g = hu$ geschrieben werden kann, wobei $h \in H$ und $u = u_i$ für ein i, ist die Abbildung $\gamma : G \to G$, $\gamma(g) = \gamma(hu) := \psi^*(u)\varphi(h)$ wohldefiniert. Wir zeigen nun, daß γ anti-symmetrisch ist. Seien $g = hu$ und $g' = h'u'$ Elemente von G, dann folgt aus $\gamma(g)g' = \gamma(g')g$:

$$\psi^*(u)\varphi(h)h'u' = \psi^*(u')\varphi(h')hu. \tag{2.4}$$

Durch Multiplikation mit H erhält man $\psi^*(u)Hu'H = \psi^*(u')HuH$. Mit 2.3 folgt $\psi(uH)u'H = \psi(u'H)uH$ und damit, weil ψ anti-symmetrisch ist, $uH = u'H$ bzw. $u = u'$, da die Repräsentanten fest gewählt sind. Nun wird aus 2.4 die Gleichung

$$\psi^*(u)\varphi(h)h'u = \psi^*(u)\varphi(h')hu.$$

Nach kürzen von $\psi^*(u)$ und u bleibt die Gleichung $\varphi(h)h' = \varphi(h')h$, woraus, wegen der Anti-Symmetrie von φ, $h = h'$ folgt und insgesamt $g = g'$. Also ist γ eine anti-symmetrische Abbildung. □

Definition 4 *([3]) Seien $(G, \cdot, ^{-1}, e)$ und $(X, +, -, 0)$ Gruppen und $\pi : G \to Aut(X)$ ein Gruppenhomomorphismus. Das semi-direkte Produkt von X und G relativ zu π wird definiert durch:*

$$X \times_\pi G = \{(x, a) | x \in X, a \in G\}$$

mit der Operation $(x_1, a_1)(x_2, a_2) = (x_1 + \pi(a_1)[x_2], a_1a_2)$, *für* $x_1, x_2 \in X$ *und* $a_1, a_2 \in G$.

Proposition 1 *1. Das semi-direkte Produkt* $X \times_\pi G$ *ist eine Gruppe.*

2. *Die Menge* $\{(x, a) \in X \times_\pi G | x = 0\}$ *ist eine Untergruppe von* $X \times_\pi G$, *welche isomorph zu* G *ist.*

3. *Die Menge* $N = \{(x, a) \in X \times_\pi G | a = e\}$ *ist ein Normalteiler von* $X \times_\pi G$, *die isomorph zu* X *ist und* $(X \times_\pi G)/N$ *ist isomorph zu* G.

Beweis zu 3.: Es ist klar, daß X isomorph zu N ist. Definiere $\varphi : X \times_\pi G \to G$ durch $\varphi(x, a) = a$, dann ist φ ein Homomorphismus mit $\varphi(X \times_\pi G) = G$ und $Kern(\varphi) = N$. Der Homomorphiesatz zeigt nun $(X \times_\pi G)/N \cong G$. □

Korollar 8 *Wenn* A *und* B *Gruppen mit anti-symmetrischen Abbildungen sind und* $\pi : G \to Aut(X)$ *ein Gruppenhomomorphismus ist, dann besitzt das semi-direkte Produkt* $A \times_\pi B$ *eine anti-symmetrische Abbildung.*

Beweis $A \times_\pi B$ hat eine Untergruppe isomorph zu A und die Faktorgruppe $(A \times_\pi B)/A$ ist isomorph zu B. Mit dem Erweiterungstheorem folgt nun die Behauptung.

Korollar 9 *Sind* A *und* B *Gruppen mit anti-symmetrischen Abbildungen, dann besitzt das direkte Produkt* $A \times B$ *eine anti-symmetrische Abbildung.*

Beweis Spezialfall vom vorherigen Korollar, wobei π alle Elemente auf die Identität abbildet.

2.1.4 Einfache Gruppen

Die einfachen Gruppen spielen angesichts Theorem 5 eine entscheidende Rolle bei der Bestimmung der endlichen Gruppen mit anti-symmetrischen Abbildungen. Die Klassifikation der einfachen Gruppen (GORENSTEIN [11]) zeigt, daß jede endliche einfache Gruppe von einem der folgenden Typen ist: eine zyklische Gruppe mit Primzahlordnung, eine alternierende Gruppe, ein Mitglied einer von sechzehn Familien vom Lie-Typ oder eine von 26 sporadischen Gruppen.

Theorem 6 *Jede endliche einfache Gruppe, außer* $\mathbb{Z}_2$, *besitzt eine anti-symmetrische Abbildung.*

Beweis Die zyklischen und alternierenden Gruppen werden von Korollar 5 und Korollar 6 abgedeckt. Mit dem Atlas der endlichen Gruppen [7] kann man verifizieren, daß in allen 26 sporadischen einfachen Gruppen der Zentralisator der Elemente mit maximaler Primzahlordnung ungerade Ordnung hat und diese Gruppen daher eine anti-symmetrische Abbildung besitzen (Korollar 7). Korollar 7 kann auch

auf die Lie-Gruppen angewendet werden, da LYONS, SOLOMON und SEITZ [10, Gallian] gezeigt haben, daß jede einfache Lie-Gruppe ein Element besitzt, dessen Zentralisator ungerade Ordnung hat. □

2.1.5 Verallgemeinerte Diedergruppen

Definition 5 *Sei G eine abelsche Gruppe. Die verallgemeinerte Diedergruppe $dih(G)$ wird definiert durch das semi-direkte Produkt $G \times_\pi \mathbb{Z}_2$, wobei $\pi(0) = id$ und $\pi(1) = inv$.*

Beispiel Die Diedergruppe D_n ist das semi-direkte Produkt von $\mathbb{Z}_n$ und $\mathbb{Z}_2$: $D_n = \mathbb{Z}_n \times_\pi \mathbb{Z}_2$.

Lemma 8 *Für zwei abelsche Gruppen A und B gilt: $dih(A \times B) \cong A \times_\gamma dih(B)$, wobei $\gamma(b, 0) = id$ und $\gamma(b, 1) = inv$.*

Beweis Die Abbildung $\psi : \mathrm{dih}(A \times B) \to A \times_\gamma \mathrm{dih}(B)$, $\psi((a, b), z) = (a, (b, z))$, mit $a \in A$, $b \in B$ und $z \in \mathbb{Z}_2$ ist ein Isomorphismus. □

Theorem 7 *Sei G eine nicht-triviale abelsche Gruppe, dann besitzt $dih(G)$ eine anti-symmetrische Abbildung.*

Beweis Fallunterscheidung:
1. Fall: Ist G eine zyklische Gruppe der Ordnung n, dann gilt $\mathrm{dih}(G) \cong D_n$ und G hat demnach eine anti-symmetrische Abbildung.
2. Fall: Hat G ungerade Ordnung und ist nicht zyklisch, dann kann man G faktorisieren in eine zyklische Gruppe Z_m und eine Gruppe H mit ungerader Ordnung. Es folgt mit Hilfe von Lemma 8:

$$\mathrm{dih}(G) \cong \mathrm{dih}(H \times Z_m) \cong H \times_\gamma \mathrm{dih}(Z_m).$$

H besitzt eine anti-symmetrische Abbildung (H hat ungerade Ordnung) und es gilt $\mathrm{dih}(Z_m) \cong D_m$. Mit Korollar 8 folgt, daß $\mathrm{dih}(G)$ eine anti-symmetrische Abbildung besitzt.
3. Fall: Ist G eine nicht-zyklische 2-Gruppe, dann gilt $G \cong Z_{2^{i_1}} \times Z_{2^{i_2}} \times \ldots \times Z_{2^{i_s}}$ mit $s \geq 2$. Folglich hat das Zentrum $Z(\mathrm{dih}(G))$ die Ordnung 2^s und ist isomorph zu $H = Z_2 \times Z_2 \times \ldots \times Z_2$. Da H abelsch ist und wenigstens zwei Involutionen enthält, besitzt H eine vollständige und damit eine anti-symmetrische Abbildung. Der Quotient $\mathrm{dih}(G)/Z(\mathrm{dih}(G))$ ist isomorph zu $\mathrm{dih}(Z_{2^{(i_1-1)}} \times Z_{2^{(i_2-1)}} \times \ldots \times Z_{2^{(i_s-1)}})$ und besitzt, durch Induktion nach dem Maximum von i_j nachweisbar, eine anti-symmetrische Abbildung und wir können mit Korollar 8 folgern, daß G eine anti-symmetrische Abbildung besitzt.
4. Fall: Nun habe G gerade Ordnung, sei aber keine 2-Gruppe, dann kann man G in

zwei nicht-triviale Gruppen faktorisieren: eine Gruppe H mit ungerader Ordnung und eine 2-Gruppe N. Es folgt, daß

$$\mathrm{dih}(G) \cong \mathrm{dih}(H \times N) \cong H \times_\gamma \mathrm{dih}(N).$$

H und $\mathrm{dih}(N)$ haben anti-symmetrische Abbildungen also auch $\mathrm{dih}(G)$. □

Wir adaptieren nun die Argumente von HALL und PAIGE [14] zur Charakterisierung der endlichen p-Gruppen, die eine vollständige Abbildung besitzen, um zu zeigen, daß die selbe Charakterisierung auch für anti-symmetrische Abbildungen gilt.

Theorem 8 *Eine nicht-triviale endliche p-Gruppe hat eine anti-symmetrische Abbildung genau dann, wenn sie keine zyklische 2-Gruppe ist.*

Beweis Sei G eine nicht-triviale endliche p-Gruppe. Wenn p ungerade ist, dann hat G eine anti-symmetrische Abbildung. Wenn G eine zyklische 2-Gruppe ist, dann wissen wir durch das Resultat von PAIGE, Theorem 1 (Seite 16), daß G keine vollständige und damit auch keine anti-symmetrische Abbildung besitzt. Der Fall, daß G eine nicht-zyklische abelsche 2-Gruppe ist wurde ebenfalls von PAIGE gezeigt. Deshalb können wir uns auf den Fall beschränken, daß G eine nicht-abelsche 2-Gruppe ist mit der Ordnung 2^n.

Besitzt G eine zyklische Untergruppe der Ordnung 2^{n-1} dann ist bekanntlich G entweder eine Diedergruppe, eine verallgemeinerte Quaternionen-Gruppe oder eine Semi-Diedergruppe (PAIGE [14]). Nach Theorem 3 haben diese Gruppen eine anti-symmetrische Abbildung.

Also nehmen wir an, daß G keine zyklische Untergruppe der Ordnung 2^{n-1} hat. Wenn G genau ein Element der Ordnung 2 enthält, dann wäre sie eine verallgemeinerte Quaternionen-Gruppe und hätte eine zyklische Untergruppe der Ordnung 2^{n-1} (siehe PAIGE [14]), im Widerspruch zu unserer Annahme. Also hat G wenigstens zwei Elemente der Ordnung 2 und wenigstens eins davon im Zentrum. Diese beiden Elemente erzeugen eine 4-Gruppe V. Wenn V in zwei verschiedenen maximalen Untergruppen M_1 und M_2 enthalten ist, dann ist $M_1 \cap M_2 = K \supset V$ ein Normalteiler von G und sowohl K als auch G/K sind nicht zyklisch. Also haben, mit Induktion, K und G/K anti-symmetrische Abbildungen und, mit dem Erweiterungstheorem, damit auch G.

Wir nehmen daher an, daß V in genau einer maximalen Untergruppe M_1 enthalten ist. Weil G nicht zyklisch ist, enthält sie eine weitere maximale Untergruppe M_2 (PAIGE [14]). Wenn $M_1 \cap M_2$ nicht zyklisch ist, dann stellt sie eine normale nicht-zyklische Untergruppe K mit nicht-zyklischer Quotientengruppe dar und wir können mit Induktion schließen, daß G eine anti-symmetrische Abbildung besitzt.

Nun sei $M_1 \cap M_2$ zyklisch. Es muß M_1 eine Gruppe der Ordnung 2^{n-1} sein, die eine zyklische Untergruppe der Ordnung 2^{n-2} und die 4-Gruppe V enthält.

Demnach muß M_1 entweder eine Diedergruppe, eine Semi-Diedergruppe oder eine abelsche Gruppe sein. In jedem Fall können wir

$$M_1 =< a, b | a^{2^{n-2}} = b^2 = e, ba = a^k b >$$

schreiben, wobei k gleich $-1, 2^{n-3} \pm 1$ oder 1 ist, abhängig davon, ob M_1 einer Dieder-, Semi-Dieder- oder einer abelschen Gruppe entspricht, und es ist $M_1 \cap M_2 =< a >$. Sei c ein Element von M_2 aber nicht von M_1. Da $< a >$ normal in M_2 ist, muß $c^2 = a^r$ gelten, wobei r gerade ist, da sonst c die Ordnung 2^{n-1} hat, was wir ausgeschlossen haben. Weil $< a >$ normal in G ist, erhalten wir $cb = bca^s$ für ein s.

Sei H die Untergruppe $< a^2, b >$. Eine einfache Rechnung zeigt, daß H mit den Elementen a, c und ac kommutiert, wenn s gerade ist. Also ist H ein Normalteiler in G. H ist nicht zyklisch, also wissen wir durch Induktion, daß H eine anti-symmetrische Abbildung hat und der Quotient $G/H \cong Z_2 \times Z_2$ hat ebenfalls eine anti-symmetrische Abbildung. Mit dem Erweiterungstheorem folgt nun, daß G eine anti-symmetrische Abbildung besitzt.

Es bleibt der Fall, daß s ungerade ist. Wir untersuchen die Untergruppe, die durch cb erzeugt wird. Wir haben

$$(cb)^2 = cbcb = cb^2ca^s = c^2a^s = a^{s+r}, \qquad \text{wobei } s + r \text{ ungerade ist.}$$

Also hat $(cb)^2$ die Ordnung 2^{n-2}, was $ord(cb) = 2^{n-1}$ impliziert. Aber dies widerspricht unserer Annahme, daß G keine zyklische Untergruppe der Ordnung 2^{n-1} besitzt. Damit haben wir die Behauptung bewiesen. □

Korollar 10 *Eine endliche nilpotente Gruppe mit trivialer oder nicht-zyklischer 2-Sylow-Untergruppe hat eine anti-symmetrische Abbildung.*

Beweis Eine endliche nilpotente Gruppe ist das direkte Produkt ihrer Sylow-Untergruppen. Die p-Sylow-Untergruppen mit ungeradem p haben gemäß Theorem 8 eine anti-symmetrische Abbildung. Da die 2-Sylow-Untergruppe trivial oder nicht-zyklisch ist, hat sie ebenfalls eine anti-symmetrische Abbildung. Demnach hat auch das direkte Produkt, also G, eine anti-symmetrische Abbildung. □

Die obengenannten Theoreme reichen aus, um zu zeigen, daß alle nicht-abelschen Gruppen der Ordnung kleiner als 36 eine anti-symmetrische Abbildung besitzen, mit Ausnahme der Gruppe $< a, b | a^3 = b^8 = e, ab = ba^2 >$ der Ordnung 24, wobei bei dieser Gruppe ebenfalls gezeigt werden kann, daß sie eine besitzt.

Da es keinen Anhaltspunkt gibt, daß eine nicht-abelsche Gruppe keine anti-symmetrische Abbildung besitzt, vermuten GALLIAN und MULLIN, daß alle nicht-abelschen Gruppen eine anti-symmetrische Abbildung besitzen.

2.2 Invarianten von $Ant(G)$

Wir untersuchen nun welche Transformationen die Menge der anti-symmetrischen Abbildungen einer Gruppe invariant lassen.

Satz 3 *Sei $\varphi(x)$ eine anti-symmetrische Abbildung einer Gruppe $(G,\cdot)$, dann ist auch die Abbildung $a \cdot \varphi(x \cdot b)$, $a, b \in G$, anti-symmetrisch.*

Beweis Aus $(a \cdot \varphi(x \cdot b)) \cdot y = (a \cdot \varphi(y \cdot b)) \cdot x$ folgt mit dem Assoziativgesetz und der Kürzungsregel $\varphi(x \cdot b) \cdot y = \varphi(y \cdot b) \cdot x$. Die Gleichung wird nun von rechts mit b durchmultipliziert, also gilt $\varphi(x \cdot b) \cdot y \cdot b = \varphi(y \cdot b) \cdot x \cdot b$ und es folgt, da φ anti-symmetrisch ist, $x \cdot b = y \cdot b$ und damit $x = y$. Also ist $a \cdot \varphi(x \cdot b)$ anti-symmetrisch. □

Satz 4 *Wenn $\varphi(x)$ eine anti-symmetrische Abbildung der Gruppe $(G,\cdot)$ ist, dann ist für jedes $c \in G$ auch $\varphi(c \cdot x) \cdot c$ anti-symmetrisch.*

Beweis Es gilt, da φ anti-symmetrisch ist: $\varphi(c \cdot x) \cdot c \cdot y = \varphi(c \cdot y) \cdot c \cdot x \Rightarrow c \cdot x = c \cdot y \Rightarrow x = y$. □

Mit $l_a = (x \mapsto a \cdot x)$ werde die Linksmultiplikation und mit $r_b = (x \mapsto x \cdot b)$ die Rechtsmultiplikation bezeichnet. Die Transformationen $L_a = (\varphi \mapsto l_a \circ \varphi)$, $R_b = (\varphi \mapsto \varphi \circ r_b)$ und $M_c = (\varphi \mapsto r_c \circ \varphi \circ l_c)$ bilden jeweils eine Gruppe mit der Verknüpfung $\circ$, die isomorph zu G ist.

Satz 5 *(Verhoeff [27]) Sei φ eine anti-symmetrische Abbildung und ψ ein Automorphismus, dann ist auch $\psi \circ \varphi \circ \psi^{-1}$ anti-symmetrisch.*

Beweis Aus $\psi \circ \varphi \circ \psi^{-1}(x) \cdot y = \psi \circ \varphi \circ \psi^{-1}(y) \cdot x$ folgt mit $y = \psi(\psi^{-1}(y))$ und $x = \psi(\psi^{-1}(x))$, daß $\psi(\varphi(\psi^{-1}(x)) \cdot \psi^{-1}(y)) = \psi(\varphi(\psi^{-1}(y)) \cdot \psi^{-1}(x))$ gilt. Nachdem wir ψ auf beiden Seiten gekürzt haben, folgt aus der Anti-Symmetrie von φ, daß $\psi^{-1}(x) = \psi^{-1}(y)$ ist und damit $x = y$. □

Auch hier bilden die Transformationen $T_\psi = (\varphi \mapsto \psi \circ \varphi \circ \psi^{-1})$ eine Gruppe. Diese ist isomorph zur Automorphismen-Gruppe $Aut(G)$.

Bemerkung Satz 4 läßt sich auch mit Satz 5 und 3 beweisen. Dazu setzt man $\psi(x) := c^{-1}xc$ und $a = b = c$.

Andere Möglichkeiten, wie aus einer vorgegebenen anti-symmetrischen Abbildung weitere konstruiert werden können, findet man im Abschnitt „Automorphismen und Anti-Automorphismen" sowie im Kapitel „Gruppen mit Vorzeichen".

2.3 Äquivalenzklassen

Auf der Menge der anti-symmetrischen Abbildungen einer Gruppe definieren wir in diesem Abschnitt eine Äquivalenzrelation. Diese ermöglicht es uns, eine Übersicht über alle anti-symmetrischen Abbildungen einer Gruppe zu gewinnen.

Mit 0 bezeichnen wir im folgenden das neutrale Element der Gruppe. Weiterhin sei φ ein Automorphismus der Gruppe G und l_a bzw. r_a die Links- bzw. Rechtsmultiplikation mit dem Element $a \in G$.
Die genannten Abbildungen haben folgende Eigenschaften:

1. $l_a \circ l_b = l_{a \cdot b}, \quad r_a \circ r_b = r_{b \cdot a}, \quad l_a^{-1} = l_{a^{-1}}, \quad r_a^{-1} = r_{a^{-1}}$.
2. $l_a \circ r_b = r_b \circ l_a$.
3. $\varphi \circ l_b = l_{\varphi(b)} \circ \varphi, \quad \varphi \circ r_a = r_{\varphi(a)} \circ \varphi$.

Die ersten beiden Eigenschaften folgen aus dem Assoziativgesetz, für die letzte gilt: $\varphi \circ l_b(x) = \varphi(b \cdot x) = \varphi(b) \cdot \varphi(x) = l_{\varphi(b)} \circ \varphi(x)$ und $\varphi \circ r_a(x) = \varphi(x \cdot a) = \varphi(x) \cdot \varphi(a) = r_{\varphi(a)} \circ \varphi(x)$.

Die Äquivalenzklassen werden nun wie folgt definiert:

Definition 6 *Seien f, g Permutationen. f und g heißen äquivalent, $f \sim g$, wenn Elemente $a, b \in G$ und ein Automorphismus φ existieren, so daß gilt:*

$$f = l_b \circ \varphi^{-1} \circ g \circ \varphi \circ r_a.$$

Die Relation $\sim$ bildet eine Äquivalenzrelation auf der Menge der Permutationen:

1. $\sim$ ist reflexiv: $f = l_0 \circ Id \circ f \circ Id \circ r_0$
2. $\sim$ ist symmetrisch: $f = l_b \circ \varphi^{-1} \circ g \circ \varphi \circ r_a$ genau dann, wenn

$$\begin{aligned} g &= \varphi \circ l_b^{-1} \circ f \circ r_a^{-1} \circ \varphi^{-1} \\ &\underset{1.,2.}{=} \varphi \circ l_{b^{-1}} \circ f \circ \circ r_{a^{-1}} \circ \varphi^{-1} \\ &\underset{3.}{=} l_{\varphi(b^{-1})} \circ \varphi \circ f \circ \varphi^{-1} \circ r_{\varphi(a^{-1})} \end{aligned}$$

   Also: $f \sim g$ impliziert $g \sim f$.

3. $\sim$ ist transitiv: Sei $f = l_{b_1} \circ \varphi_1^{-1} \circ g \circ \varphi_1 \circ \circ r_{a_1}$ und $g = l_{b_2} \circ \varphi_2^{-1} \circ h \circ \varphi_2 \circ r_{a_2}$, dann folgt

$$\begin{aligned} f &= l_{b_1} \circ \varphi_1^{-1} \circ l_{b_2} \circ \varphi_2^{-1} \circ h \circ \varphi_2 \circ r_{a_2} \circ \varphi_1 \circ r_{a_1} \\ &\underset{3.}{=} l_{b_1} \circ l_{\varphi_1^{-1}(b_2)} \circ (\varphi_2 \circ \varphi_1)^{-1} \circ h \circ (\varphi_2 \circ \varphi_1) \circ r_{\varphi_1(a_2)} \circ r_{a_1} \\ &\underset{1.}{=} l_{b_1 \varphi_1^{-1}(b_2)} \circ (\varphi_2 \circ \varphi_1)^{-1} \circ h \circ (\varphi_2 \circ \varphi_1) \circ r_{a_1 \varphi_1(a_2)} \end{aligned}$$

Damit ist $f \sim g, g \sim h \Rightarrow f \sim h$ gezeigt.

Aus dem vorherigen Abschnitt können wir das folgende Korollar ableiten.

Korollar 11 *Seien $f, g \in S_n$ mit $f \sim g$, dann gilt*

$$f \text{ anti-symmetrisch} \Leftrightarrow g \text{ anti-symmetrisch.}$$

Beispiel Die Diedergruppe D_5 besitzt 34040 anti-symmetrische Abbildungen. Es können 3040 von $x^{-1} \cdot a$ abgeleitet werden (siehe Satz 21, Seite 53). Für die restlichen 31000 anti-symmetrischen Abbildungen erhalten wir folgende Repräsentanten der Äquivalenzklassen:

1. Diese 15 Permutationen erzeugen 30000 anti-symmetrische Abbildungen (rechts: Zyklenschreibweise):

$$\begin{array}{lcl}
[0215637894] & = & (21)(53)(67894) \\
[0215638974] & = & (21)(53)(68794) \\
[0215647938] & = & (21)(5467983) \\
[0215694378] & = & (21)(59873)(64) \\
[0215748396] & = & (21)(5473)(896) \\
[0215748936] & = & (21)(5479683) \\
[0215794638] & = & (21)(5983)(764) \\
[0215867394] & = & (21)(5673)(894) \\
[0215874936] & = & (21)(5796483) \\
[0215897436] & = & (21)(5967483) \\
[0245678931] & = & (246835791) \\
[0245718936] & = & (247968351) \\
[0256714893] & = & (251)(647893) \\
[0256743918] & = & (2547981)(63) \\
[0257918436] & = & (251)(749683)
\end{array}$$

2. Die Permutation $[0215643978] = (21)(5463)(987)$ erzeugt die restlichen 1000 anti-symmetrischen Abbildungen.

Bemerkung Mit $[a_0 a_1 \ldots a_9]$ meinen wir die Permutation $x \mapsto a_x$, d.h.

$$[a_0 a_1 \ldots a_9] = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{pmatrix}.$$

Dieses Beispiel zeigt auch, daß die Klassen nicht unbedingt gleich groß sein müssen.

2.4 Automorphismen und Anti-Automorphismen

In diesem Abschnitt untersuchen wir einen Spezialfall, nämlich anti-symmetrische Automorphismen bzw. Anti-Automorphismen. Automorphismen sind bekanntlich bijektive Permutationen einer Gruppe $\varphi : G \to G$ mit $\varphi(xy) = \varphi(x)\varphi(y)$. Der Begriff „Anti-Automorphismus" wird dagegen nicht so häufig benutzt, er wird aber ganz ähnlich definiert:

Definition 7 *Eine bijektive Abbildung $\psi : G \to G$ einer Gruppe G heißt* Anti-Automorphismus*, wenn für alle $x, y \in G$ gilt: $\psi(xy) = \psi(y)\psi(x)$. Ein Anti-Automorphismus oder ein Automorphismus heißt* fixpunktfrei*, wenn für alle $x \neq 0$ gilt: $\psi(x) \neq x$.*

Die folgenden Eigenschaften eines Anti-Automorphismus werden genauso gezeigt wie bei einem Automorphismus:

1. $\psi(0) = 0$
2. $\psi(x)^{-1} = g(x^{-1})$
3. $ord(\psi(x)) = ord(x)$

Bemerkung Da für einen (Anti-)Automorphismus ψ immer $\psi(0) = 0$ gilt, ist es sinnvoll, bei der Definition von „fixpunktfrei" die Stelle $x = 0$ auszuschließen.

Die Menge der Automorphismen einer Gruppe können wir bijektiv auf die Menge der Anti-Automorphismen abbilden. Es gilt nämlich

$$\varphi \text{ ist ein Automorphismus} \quad \Leftrightarrow \quad \varphi \circ inv \text{ ist ein Anti-Automorphismus}$$

Ist φ ein Automorphismus, dann gilt

$$\varphi \circ inv(xy) = \varphi((xy)^{-1}) = \varphi(y^{-1}x^{-1}) = \varphi(y^{-1})\varphi(x^{-1}) = \varphi \circ inv(y)\varphi \circ inv(x^{-1})$$

und $\varphi \circ inv$ ist ein Anti-Automorphismus. Ist andererseits $\varphi \circ inv$ ein Anti-Automorphismus, dann haben wir

$$\varphi(xy) = \varphi((y^{-1}x^{-1})^{-1}) = \varphi \circ inv(x^{-1})\varphi \circ inv(y^{-1}) = \varphi(x)\varphi(y)$$

und φ ist ein Automorphismus.

Wenn wir also die Automorphismen einer Gruppe kennen, dann können wir auch ohne weiteres alle Anti-Automorphismen dieser Gruppe bestimmen.

Ist ψ ein Anti-Automorphismus, so ist für zwei beliebige Automorphismen φ_1, φ_2 auch $\varphi_1 \circ \psi \circ \varphi_2$ ein Anti-Automorphismus:

$$\begin{aligned} \varphi_1 \circ \psi \circ \varphi_2(xy) &= \varphi_1 \circ \psi(\varphi_2(x)\varphi_2(y)) = \varphi_1(\psi(\varphi_2(y))g(\varphi_2(x))) \\ &= \varphi_1(\psi(\varphi_2(y)))\varphi_1(\psi(\varphi_2(x))) \\ &= \varphi_1 \circ \psi \circ \varphi_2(y)\varphi_1 \circ \psi \circ \varphi_2(x) \end{aligned}$$

Das Gleiche gilt auch, wenn φ_1 und φ_2 zwei Anti-Automorphismen sind.

Wie man leicht sieht, gilt außerdem: Sind ψ_1, ψ_2 Anti-Automorphismen, dann ist $\psi_1 \circ \psi_2$ ein Automorphismus.
Ist ψ ein (fixpunktfreier) Anti-Automorphismus, dann ist auch ψ^{-1} ein (fixpunktfreier) Anti-Automorphismus:

$$\psi^{-1}(xy) = \psi^{-1}(\psi(\psi^{-1}(x))\psi(\psi^{-1}(y))) = \psi^{-1}(\psi(\psi^{-1}(y)\psi^{-1}(x))) = \psi^{-1}(y)\psi^{-1}(x)$$

und

$$\psi(x) = x \qquad \Leftrightarrow \qquad x = \psi^{-1}(x).$$

Damit haben wir gezeigt, daß die Menge der Anti-Automorphismen zusammen mit den Automorphismen eine Gruppe bildet. Gibt es einen Anti-Automorphismus der auch ein Automorphismus ist, so folgt

$$xy = \psi(\psi^{-1}(x))\psi(\psi^{-1}(y)) = \psi(\psi^{-1}(y)\psi^{-1}(x)) = yx$$

und die Gruppe ist abelsch. In einer abelschen Gruppe sind Anti-Automorphismen auch Automorphismen, während in einer nicht-abelschen Gruppe kein Anti-Automorphismus ein Automorphismus ist.

Mit Hilfe der Anti-Automorphismen finden wir eine zusätzliche Möglichkeit, aus einer vorgegebenen anti-symmetrischen Abbildung eine weitere zu konstruieren.

Satz 6 *Sei φ eine anti-symmetrische Abbildung und ψ ein Anti-Automorphismus, dann ist auch $\psi \circ \varphi^{-1} \circ \psi^{-1}$ anti-symmetrisch.*

Beweis Es gelte $\psi\circ\varphi^{-1}\circ\psi^{-1}(x)y = \psi\circ\varphi^{-1}\circ\psi^{-1}(y)x$. Wir setzen $\tilde{x} := \varphi^{-1}\circ\psi^{-1}(x)$ und $\tilde{y} := \varphi^{-1} \circ \psi^{-1}(y)$, womit $\psi(\tilde{x})\psi(\varphi(\tilde{y})) = \psi(\tilde{y})\psi(\varphi(\tilde{x}))$ folgt. Wir nutzen die Eigenschaft aus, daß ψ ein Anti-Automorphismus ist, um $\psi(\varphi(\tilde{y})\tilde{x}) = \psi(\varphi(\tilde{x})\tilde{y})$ zu erhalten. In dieser Gleichung kürzen wir ψ. Aus der resultierenden Gleichung folgt $\tilde{x} = \tilde{y}$, denn $\varphi \in Ant(G)$. Da $\varphi^{-1} \circ \psi^{-1}$ bijektiv ist, haben wir damit $x = y$, und der Satz ist bewiesen. □

Wir untersuchen nun, wann ein (Anti-)Automorphismus anti-symmetrisch ist.

Satz 7 *Ein Anti-Automorphismus ist genau dann anti-symmetrisch, wenn er fixpunktfrei ist.*

Beweis Sei ψ ein fixpunktfreier Anti-Automorphismus und es gelte $\psi(x)y = \psi(y)x$. Die Gleichung wird von links mit $\psi(y)^{-1}$ und von rechts mit y^{-1} durchmultipliziert, es folgt $\psi(y^{-1})\psi(x) = \psi(xy^{-1}) = xy^{-1}$. Da ψ fixpunktfrei ist, muß

$xy^{-1} = 0$, bzw. $x = y$ gelten. Also ist ψ anti-symmetrisch. Wenn andererseits ψ einen Fixpunkt $x \neq 0$ besitzt, dann gilt $\psi(0)x = x = \psi(x) = \psi(x)0$ und ψ ist nicht anti-symmetrisch. □

Satz 8 *Sei φ ein Automorphismus. φ ist genau dann anti-symmetrisch, wenn für alle $y \in G$ gilt: $y^{-1}\varphi(z)y$ ist fixpunktfrei.*

Beweis Die Gleichung $\varphi(x)y = \varphi(y)x$ ist äquivalent zu $\varphi(y^{-1})\varphi(x) = xy^{-1}$ bzw. $\varphi(y^{-1}x) = x(y^{-1}x)x^{-1}$. Mit $z := y^{-1}x$ ist dies äquivalent zu $\varphi(z) = yzy^{-1}$ bzw. $y^{-1}\varphi(z)y = z$. □

Lemma 9 *Sei ψ ein Anti-Automorphismus und φ ein (Anti-)Automorphismus, dann gilt:*

$$\psi \textit{ fixpunktfrei} \quad \Leftrightarrow \quad \varphi^{-1} \circ \psi \circ \varphi \textit{ fixpunktfrei}$$

Beweis Es ist $\psi(x) = x$ äquivalent zu $\varphi^{-1}(\psi(\varphi(\varphi^{-1}(x)))) = \varphi^{-1}(x)$. □

Wir können nun Satz 4 von GALLIAN und MULLIN etwas anders formulieren:

Satz 9 *Der Anti-Automorphismus $\psi(x) := a^{-1}x^{-1}a$ ist genau dann fixpunktfrei, wenn x^{-1} und $a^{-1}xa$ keinen gemeinsamen Fixpunkt $x \neq 0$ besitzen.*

Beweis $\psi(x)$ fixpunktfrei $\Leftrightarrow$ $\psi(x)$ anti-symmetrisch $\Leftrightarrow$ $a\psi(x) = x^{-1}a$ anti-symmetrisch $\Leftrightarrow$ a kommutiert mit keinem Element der Ordnung 2 $\Leftrightarrow$ für alle $x \neq 0$ gilt: $x^{-1} = x \Rightarrow a^{-1}xa \neq x$. □

Satz 10 *Sei $h \circ g$ ein Anti-Automorphismus der Gruppe G der Ordnung n, $h, g \in S_n$ mit den Eigenschaften: $ord(g) = 2$, $ord(h)$ ungerade und $g \circ h = h \circ g$. Genau dann ist $h \circ g$ fixpunktfrei, wenn g und h keinen gemeinsamen Fixpunkt $x \neq 0$ besitzen.*

Beweis Sei $h \circ g$ nicht fixpunktfrei, d.h. es existiert ein $x \neq 0$ mit $h(g(x)) = x$. Es folgt $h(g(h(g(x)))) = h(h(g(g(x)))) = h(h(x)) = x$. Da die Ordnung von h ungerade, sprich $2k + 1$ ist, haben wir $x = h^{2k+1}(x) = h(h^{2k}(x)) = h(x)$. Damit gilt $h(g(x)) = g(h(x)) = g(x) = x$ und $x \neq 0$ ist ein gemeinsamer Fixpunkt von g und h. Haben andererseits g und h den gemeinsamen Fixpunkt $x \neq 0$, dann ist $h(g(x)) = h(x) = x$ und $h \circ g$ ist nicht fixpunktfrei. □

Bemerkung Jede Permutation p kann in zwei Permutationen h und g zerlegt werden, so daß die Bedingungen des Satzes erfüllt sind. Dazu schreibt man p als

Produkt disjunkter Zykel. Die Transpositionen werden dann zu g zusammengefaßt, der Rest zu h.

Wir geben nun notwendige und hinreichende Konditionen für die Erkennung der anderen Fehlertypen an, wenn wir ein Prüfziffersystem $\tau^n(x_n)\cdot\ldots\cdot\tau(x_1)\cdot x_0 = c$ mit einem (Anti-)Automorphismus τ benutzen. Dazu sei φ ein Automorphismus und ψ ein Anti-Automorphismus.

Nachbarvertauschungen

a.) Für alle $x \neq 0$: $\psi(x) \neq x$ (d.h. ψ ist fixpunktfrei)

b.) Für alle $x \neq 0$ und alle $y \in G$ gilt: $y^{-1}\varphi(x)y \neq x$ (d.h. $y^{-1}\varphi(x)y$ ist ein fixpunktfreier Automorphismus)

Sprungtranspositionen

a.) Für alle $x \neq 0$ und alle $z \in G$ gilt: $z^{-1}\psi^2(x)z \neq x$ (d.h. ψ^2 ist ein antisymmetrischer Automorphismus)

b.) wie a. für φ

Zwillingsfehler

a.) Für alle $x \neq 0$: $\psi(x^{-1}) \neq x$ (d.h. $\psi \circ inv$ ist ein fixpunktfreier Automorphismus)

b.) Für alle $x \neq 0$ und alle $z \in G$ gilt: $z^{-1}\varphi(x^{-1})z \neq x$ (d.h. $z^{-1}\varphi(x^{-1})z$ ist ein fixpunktfreier Anti-Automorphismus)

Sprungzwillingsfehler

a.) Für alle $x \neq 0$ und alle $z \in G$ gilt: $z^{-1}\psi^2(x^{-1})z \neq x$ (d.h. $z^{-1}\psi^2(x^{-1})z$ ist ein fixpunktfreier Anti-Automorphismus)

b.) wie a. für φ

phonetische Fehler

a.) Für $a = 2, \ldots, n-1$ gilt: $\psi(a)a^{-1} \neq \psi(1) \neq a^{-1}\psi(a)$

b.) Für $a = 2, \ldots, n-1$ gilt: $\varphi(a)a^{-1} \neq \varphi(1)$

Beweis Die Aussagen werden analog zu Satz 7 und 8 gezeigt. Die phonetischen Fehler werden erkannt, falls für $a = 2, \ldots, n-1$ gilt $\psi^{i+1}(a)\psi^i(0) \neq \psi^{i+1}(1)\psi^i(a)$. Da $\psi(0) = 0$ ist haben wir $\psi^{i+1}(a)\psi^i(a^{-1}) \neq \psi^{i+1}(1)$. Je nachdem ob i gerade oder ungerade ist, ist dies äquivalent zu $\psi^i(\psi(a)a^{-1}) \neq \psi^{i+1}(1)$ oder $\psi^i(a^{-1}\psi(a)) \neq \psi^{i+1}(1)$. Wir können ψ^i kürzen und erhalten damit die angegebene Bedingung.

2.5 Eine Abschätzung von $|Ant(G)|$

Die folgenden Sätze zeigen, daß eine große Anzahl Permutationen nicht anti-symmetrisch sein kann.

Lemma 10 *Sei $(G, \cdot)$ eine Gruppe, $G \neq \{e\}$. Die Permutationen $g(x) = a \cdot x \cdot b$ mit $a, b \in G$ sind nicht anti-symmetrisch.*

Beweis Es gilt für beliebige $y \in G$ $g(b^{-1}) \cdot y = a \cdot b^{-1} \cdot b \cdot y = a \cdot y = a \cdot y \cdot b \cdot b^{-1} = g(y) \cdot b^{-1}$. Da in G ein Element $y \neq b^{-1}$ existiert, ist g nicht anti-symmetrisch. □

Lemma 11 *Wenn $g(x) = g(0) \cdot x$ für ein $x \neq 0$ ist, dann ist g nicht anti-symmetrisch.*

Beweis $g(x) \cdot 0 = g(x) = g(0) \cdot x$. □

Mit diesem Lemma findet man eine untere Grenze für die Anzahl der Permutationen, die nicht anti-symmetrisch sein können. Man kann nämlich die Anzahl der Permutationen mit $g(x) = g(0) \cdot x$, für ein $x \neq 0$, berechnen.

Wir bestimmen die Anzahl $a(n)$ der Permutationen die an der ersten ($y = 0$) und einer weiteren Stelle $y \in \{1, \ldots, n\}$ mit einer vorgegebenen Permutation $g \in S_{n+1}$ übereinstimmen. $a(n)$ ist nicht von g abhängig, daher wählen wir o.B.d.A. $g(x) = x$. Da die erste Stelle einer weiteren Permutation p gleich 0 sein muß, reicht es, die letzten n Stellen zu betrachten. Die letzten n Stellen sind aber Permutationen aus S_n, d.h.

$$\begin{aligned} a(n) &= |\{p \in S_{n+1} : p(0) = 0 \text{ und } |\{1 \leq y \leq n : p(y) = y\}| \geq 1\}| \\ &= |\{p \in S_n : |\{0 \leq y \leq n-1 : p(y) = y\}| \geq 1\}|. \end{aligned}$$

(Mit $|M|$ bezeichnen wir die Anzahl der Elemente in der Menge M.)

Dieses Problem ist in der Literatur bekannt als „Mausefallenspiel mit n Karten":

> *Gegeben seien n Ziffern und n numerierte Umschläge. Wieviele Möglichkeiten gibt es, die Ziffern in die Umschläge einzulegen, so daß mindestens eine Zahl in den richtigen Umschlag kommt.*

Die gesuchte Lösung $a(n)$ kann wie folgt berechnet werden (siehe [25], Zahlenreihe: A002467):

1. $a(0) = 0$, $a(1) = 1$ und $a(n) = (n-1)(a(n-1) + a(n-2))$, oder
2. $a(0) = 0$, $a(1) = 1$, $a(n) = n \cdot a(n-1) - (-1)^n$, oder

3. $a(0) = 0$, $a(n) = [n!\frac{e-1}{e}]$, wobei $e = 2,71828...$ die Eulersche Zahl ist und $[\ ]$ die (verschobene) Gaußklammer (auf die nächste ganze Zahl runden).

Nun betrachten wir alle Permutationen aus S_n, die mit $a \cdot x$ an der Stelle 0 und einer weiteren Stelle übereinstimmen. Die Anzahl dieser Permutationen ist gleich $a(n-1)$. Da für $a \neq b$ auch $a \cdot 0 \neq b \cdot 0$ ist, sind die Permutationen, die mit $a \cdot x$ an der ersten Stelle übereinstimmen und die, die mit $b \cdot x$ an der ersten Stelle übereinstimmen, alle verschieden. Es gibt daher mindestens $n \cdot a(n-1)$ Permutationen in S_n, die nicht anti-symmetrisch sind.

Satz 11 *Die Anzahl der nicht anti-symmetrischen Permutationen ist größer oder gleich* $n \cdot a(n-1) = n \cdot [(n-1)!\frac{e-1}{e}]$, *also*

$$n! - |Ant(G)| \geq n \cdot [(n-1)!\frac{e-1}{e}].$$

Durch einfaches Umformen erhalten wir nun ein Abschätzung für $|Ant(G)|$.

Theorem 9 *Sei G eine Gruppe der Ordnung n, dann gilt*

$$|Ant(G)| \leq n! - n \cdot [(n-1)!\frac{e-1}{e}] \leq \frac{n!}{e} + \frac{n}{2}.$$

Beweis Wir können die verschobene Gaußklammer wie folgt abschätzen:

$$[(n-1)!\frac{e-1}{e}] \geq (n-1)!\frac{e-1}{e} - \frac{1}{2}.$$

Damit folgt

$$\begin{aligned} |Ant(G)| &\leq n! - n \cdot [(n-1)!\frac{e-1}{e}] \leq n! - n!\frac{e-1}{e} + \frac{n}{2} \\ &\leq \frac{n!}{e} + \frac{n}{2}. \end{aligned}$$

□

Für Gruppen der Ordnungen 2 bis 12 geben wir eine Abschätzung von $|Ant(G)|$ an:

n	$a(n-1)$	$n!$	$n! - n \cdot a(n-1)$
2	1	2	0
3	1	6	3
4	4	24	8
5	15	120	45
6	76	720	264
7	455	5.040	1.855
8	3.186	40.320	14.832
9	25.487	362.880	133.497
10	229.384	3.628.800	1.334.960
11	2.293.839	39.916.800	14.684.571
12	25.232.230	479.001.600	176.214.840

Für $n = 2, 3, 4$ sind die Abschätzungen sogar bestmöglich. Die Gruppe $\mathbb{Z}_2$ besitzt keine, die Gruppe $\mathbb{Z}_3$ genau 3 und die Kleinsche-Vierergruppe genau 8 anti-symmetrische Abbildungen.

Für größere n gilt $\frac{|Ant(G)|}{n!} \approx \frac{1}{e}$. Demnach können höchstens 36,8% der Permutationen einer beliebigen Gruppe anti-symmetrisch sein.

2.6 Konstruktion anti-symmetrischer Abbildungen

Die anti-symmetrischen Abbildungen einer Gruppe $(G, *, ^{-1}, 0)$ können, ähnlich wie die Primzahlen, durch eine Siebmethode bestimmt werden. Man beginnt dabei mit einer Matrix $M = (m_{ij})$ mit $n \times n$ Elementen ($n = |G|$), wobei in jeder Zeile die Zahlen $0, 1, \ldots, n-1$ stehen, d.h. $m_{ij} = j$ für $i, j = 0, \ldots, n-1$.

Der folgende Algorithmus erzeugt anti-symmetrische Abbildungen oder er zeigt, daß bestimmte Abbildungen nicht anti-symmetrisch sein können.

1) Für i von 0 bis $n-1$ tue 2-6

    2) Sind alle Elemente der i-ten Zeile von M gestrichen, dann Abbruch

    3) Wähle ein Element m_{ij} der Zeile i aus, das noch nicht gestrichen ist, und setze $\varphi(i) := j$

    4) Falls $i = n-1$, dann Ende

    5) Für k von $i+1$ bis $n-1$ tue

        6) Streiche die Elemente $m_{k,j}$ und $m_{k,j*k*i^{-1}}$ aus der k-ten Zeile

Beispiel Im folgenden wird mit diesem Algorithmus eine anti-symmetrische Abbildung der Gruppe $\mathbb{Z}_5$ bestimmt. Dazu sei $M := \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}$.

Das Element m_{00} ist nicht gestrichen, wir können also $\varphi(0) := 0$ setzen. Die Elemente $m_{1,0}$, $m_{1,0+1-0}$, $m_{2,0}$, $m_{2,0+2-0}$, $m_{3,0}$, $m_{3,0+3-0}$, $m_{4,0}$, $m_{4,0+4-0}$ werden gestrichen.

$$\begin{bmatrix} \mathbf{0} & 1 & 2 & 3 & 4 \\ \not{0} & \not{1} & 2 & 3 & 4 \\ \not{0} & 1 & \not{2} & 3 & 4 \\ \not{0} & 1 & 2 & \not{3} & 4 \\ \not{0} & 1 & 2 & 3 & \not{4} \end{bmatrix}$$

Nun können wir $\varphi(1) := 2$ wählen die Elemente $m_{2,2}$, $m_{2,2+2-1}$, $m_{3,2}$, $m_{3,2+3-1}$, $m_{4,2}$, $m_{4,2+4-1}$ werden gestrichen.

$$\begin{bmatrix} \mathbf{0} & 1 & 2 & 3 & 4 \\ \not{0} & \not{1} & \mathbf{2} & 3 & 4 \\ \not{0} & 1 & \not{2} & \not{3} & 4 \\ \not{0} & 1 & \not{2} & \not{3} & \not{4} \\ \not{0} & 1 & \not{2} & 3 & \not{4} \end{bmatrix}$$

Als nächstes muß $\varphi(2) := 4$ gewählt werden, da sonst in der vorletzten Zeile alle Elemente gestrichen wären und der Algorithmus im nächsten Durchlauf abbrechen würde. $m_{3,4}$, $m_{3,4+3-2}$, $m_{4,4}$, $m_{4,4+4-2}$ werden gestrichen.

$$\begin{bmatrix} \mathbf{0} & 1 & 2 & 3 & 4 \\ \not{0} & \not{1} & \mathbf{2} & 3 & 4 \\ \not{0} & 1 & \not{2} & \not{3} & \mathbf{4} \\ \not{0} & 1 & \not{2} & \not{3} & \not{4} \\ \not{0} & \not{1} & \not{2} & 3 & \not{4} \end{bmatrix}$$

Es bleibt $\varphi(3) := 1$, wodurch die Elemente $m_{4,1}$ und $m_{4,1+4-3}$ gestrichen werden. Im letzten Durchlauf ist damit die Wahl $\varphi(4) := 3$ möglich.

$$\begin{bmatrix} \mathbf{0} & 1 & 2 & 3 & 4 \\ \not{0} & \not{1} & \mathbf{2} & 3 & 4 \\ \not{0} & 1 & \not{2} & \not{3} & \mathbf{4} \\ \not{0} & \mathbf{1} & \not{2} & \not{3} & \not{4} \\ \not{0} & \not{1} & \not{2} & \mathbf{3} & \not{4} \end{bmatrix}$$

Der Algorithmus endet mit dem Ergebnis, daß $\varphi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}$ eine anti-symmetrische Abbildung von $\mathbb{Z}_5$ ist. Der folgende Satz zeigt, daß der Algorithmus wie gewünscht arbeitet:

Satz 12 *Es gilt:*

1. *Jede vorgegebene anti-symmetrische Abbildung kann mit dem obengenannten Algorithmus konstruiert werden.*
2. *Endet der Algorithmus im Schritt 4), dann ist die konstruierte Abbildung φ anti-symmetrisch.*
3. *Bricht der Algorithmus im Schritt 2) ab, dann existiert keine anti-symmetrische Abbildung, welche mit dem bis dahin definierten φ übereinstimmt.*

Beweis zu 1: Sei $\psi \in Ant(G)$. Es ist zu zeigen, daß für $k = 0, \ldots, n-1$ das Element $m_{k,\psi(k)}$ nicht gestrichen ist und damit die Wahl $\varphi(k) = \psi(k)$ möglich ist. Dies wird durch Induktion nach k gezeigt.
1) In der Zeile $k = 0$ ist kein Element gestrichen, man kann also $\varphi(0) := \psi(0)$ setzen.
2) Es gelte $\varphi(j) = \psi(j)$ für $j = 0, \ldots, k-1 < n-1$. Nimmt man an, daß das Element $m_{k,\psi(k)}$ in Schritt 6 gestrichen wurde, dann gibt es ein $i < k$ mit $\varphi(i) = \psi(k)$

oder mit $\varphi(i) * k * i^{-1} = \psi(k)$. Im ersten Fall folgt $\psi(i) = \psi(k)$ und ψ wäre keine Permutation. Im zweiten Fall wäre $\psi(i) * k = \psi(k) * i$. Beides steht im Widerspruch zur Voraussetzung $\psi \in Ant(G)$. Also ist das Element $m_{k,\psi(k)}$ nicht gestrichen und die Wahl $\varphi(k) := \psi(k)$ in Schritt 3 ist möglich.
Der Algorithmus bricht auch nicht ab, da das Elemente $m_{k,\psi(k)}$ nicht gestrichen ist.
Dies zeigt, daß jede anti-symmetrische Abbildung mit dem Algorithmus konstruiert werden kann.
zu 2: Es gelte $\varphi(k)*i = \varphi(i)*k$ für $i \leq k$ (o.B.d.A.) und damit $\varphi(k) = \varphi(i)*k*i^{-1}$. Da für $k > i$ das Element $\varphi(i) * k * i^{-1}$ gestrichen wird und die Wahl $\varphi(k) = \varphi(i) * k * i^{-1}$ nicht möglich ist, muß $k \leq i$ gelten, also ist $k = i$ und φ ist eine anti-symmetrische Abbildung.
zu 3: Dies ist eine direkte Folgerung aus 1. □

Um alle anti-symmetrischen Abbildungen einer Gruppe zu bestimmen, muß man offensichtlich in Schritt 3 nacheinander alle nicht gestrichenen Elemente auswählen. Der folgende rekursive Algorithmus verwirklicht dieses Vorgehen.

Erzeuge alle anti-symmetrischen Abbildungen, die mit der Permutation φ bis zur Stelle $i-1$ übereinstimmen und benutze dabei die Matrix $M = (m_{ij})$:

```
Prozedur AntiSymm(i);

  1) Ist i = n, dann gib die anti-symmetrische Abbildung φ aus,
     sonst:

       2) Für alle Elemente m_ij der Zeile i, die nicht
          gestrichen sind, tue 3-7

            3) Setze φ(i) := j

            4) Für k von i+1 bis n-1 tue (falls i < n-1)

                 5) Streiche die Elemente m_{k,j} und m_{k,j*k*i^-1} aus der
                    k-ten Zeile von M

            6) AntiSymm(i+1),
               d.h.  erzeuge alle anti-symmetrischen Abbildungen,
               die mit der Permutation φ bis zur Stelle i überein-
               stimmen.

            7) Widerrufe die Änderungen der Schritte 4+5 (Elemente die
               bereits vorher gestrichen waren, bleiben gestrichen!)
```

Der Algorithmus wird mit dem Aufruf `AntiSymm(0)` gestartet. Wobei $m_{ij} := j$ für $i, j = 0, \ldots, n-1$.

Das folgende Pascal-Programm implementiert diesen Algorithmus. In der Matrix M wird dabei aber nicht das Element $m_{ij} = j$ gespeichert, sondern vielmehr wie oft dieses Element gestrichen wurde. Das Streichen eines Elements entspricht dann dem Erhöhen dieses Elements um 1. Die Schritte 4+5 werden dann durch Erniedrigen der veränderten Elemente um 1 rückgängig gemacht.

```
program antsymm;
const Basis = 10;
type TDigit  = 0..Basis-1;
     TAbb    = array[TDigit] of TDigit;
     TMatrix = array[TDigit,TDigit] of TDigit;
var  phi : TAbb;
     M   : TMatrix;

procedure AntiSymm(i : TDigit);
var j,k : Integer;
begin
  if i=Basis then {phi ausgeben}
  else begin
    for j:=0 to Basis-1 do          {Für jedes Element der i-ten Zeile}
      if M[i,j]=0 then begin        {Wenn M[i,j] nicht gestrichen ist,}
        phi[i]:=j;                  {dann setze phi(i):=j}
        for k:=i+1 to Basis-1 do begin
          Inc(M[k,j]);              {Streiche die Elemente M[k,j]}
          Inc(M[k,j*k*i^(-1)]);     {und M[k,j*k*i^(-1)]}
        end;
        AntiSymm(i+1);              {Rekursiver Aufruf}
        for k:=i+1 to Basis-1 do begin
          Dec(M[k,j]);              {Streichungen rückgängig machen}
          Dec(M[k,j*k*i^(-1)]);
        end;
      end;
  end;
end;

var j,k : TDigit;
begin
  for j:=0 to Basis-1 do
    for k:=0 to Basis-1 do M[k,j]:=0;
  AntiSymm(0);
end.
```

Damit das Programm lauffähig ist, muß noch die Verknüpfung $*$ und das Inverse i^{-1} eines Elements definiert werden. Für die Diedergruppe lautet eine entsprechende Implementierung (vgl. H.P. GUMM [13]):

```
const Basis_2 = Basis div 2;  {Basis muß gerade sein!}

function inv(x : TDigit) : TDigit;
begin
  if x<Basis_2 then inv:=(Basis_2-x) mod Basis_2
               else inv:=x;
end;

function add(x,y : TDigit) : TDigit;
begin
  if x<Basis_2 then begin
    if y<Basis_2 then add:= (x+y) mod Basis_2
                 else add:=((x+y) mod Basis_2)+Basis_2
  end
  else begin
    if y<Basis_2 then add:=((x-y) mod Basis_2)+Basis_2
                 else add:=(x-y+Basis_2) mod Basis_2
  end;
end;
```

Damit ist `j*k*i^(-1)=add(add(j,k),inv(i))`. Für die Gruppe $\mathbb{Z}_n$ kann man die Operationen $+$,$-$ und **mod** benutzen, d.h.

```
j*k*i^(-1)=(Basis+j+k-i) mod Basis.
```

Bei der Konstruktion aller anti-symmetrischen Abbildungen einer Gruppe können wir noch folgende Eigenschaft ausnutzen:

Lemma 12 *Sei $g \in Ant(G)$, dann existiert eine eindeutig bestimmte anti-symmetrische Abbildung $g_0 \in Ant(G)$, mit $g_0(0) = 0$, und ein eindeutig bestimmtes $b \in G$ mit $g = l_b \circ g_0$.*

Beweis Sei $g_0 = l_{g(0)^{-1}} \circ g$, dann ist $g_0 \in Ant(G)$ und es gilt $g_0(0) = g(0)^{-1} \cdot g(0) = 0$. Wenn $l_{b_1} \circ g_0 = l_{b_2} \circ h_0$ gilt, mit $g_0(0) = 0 = h_0(0)$, dann folgt $b_1 = b_1 \cdot g_0(0) = b_2 \cdot h_0(0) = b_2$ und damit $g_0 = h_0$. □

Wir müssen also lediglich die anti-symmetrischen Abbildungen g_0 konstruieren, für die $g_0(0) = 0$ ist. Alle anderen erhalten wir dann durch die Links-Multiplikation

mit einem Element aus der Gruppe. Für den Algorithmus bedeutet dies, daß $\varphi(0) = 0$ gesetzt wird und in der Matrix M die Elemente $m_{k,0}$ und $m_{k,k}$, $k = 1, \ldots, n-1$, gestrichen werden. Der Aufruf erfolgt dann mit `AntiSymm(1)`.

Aus diesem Lemma folgt auch, daß die Anzahl der anti-symmetrischen Abbildungen durch die Anzahl der Elemente der Gruppe teilbar ist.

Mit diesem Programm haben wir die Anzahl der anti-symmetrischen Abbildungen der Diedergruppen D_3 bis D_8 und der zyklischen Gruppen $\mathbb{Z}_3$ bis $\mathbb{Z}_{15}$ bestimmt:

Ordnung $2 \cdot s$	$\lvert Ant(D_s)\rvert$	Rechenzeit	$\lvert Ant(D_s)\rvert/(2s)!$
$2 \cdot 3$	120	nicht meßbar	16,667%
$2 \cdot 4$	1.472	nicht meßbar	3,651%
$2 \cdot 5$	34.040	ca. 50ms	0,938%
$2 \cdot 6$	1.412.928	2,5s	0,295%
$2 \cdot 7$	100.229.976	1m 36s	0,114%
$2 \cdot 8$	6.744.202.240	1h 48m 40s	0,032%

Ordnung n	$\lvert Ant(\mathbb{Z}_n)\rvert$	Rechenzeit	$\lvert Ant(\mathbb{Z}_n)\rvert/n!$
3	3	nicht meßbar	50,000%
5	15	nicht meßbar	12,500%
7	133	nicht meßbar	2,639%
9	2.025	nicht meßbar	0,558%
11	37.851	ca. 110ms	0,095%
13	1.030.367	4s	0,017%
15	36.362.925	2m 3s	0,003%

Bemerkung Für n gerade haben wir bereits gezeigt, daß $|Ant(\mathbb{Z}_n)| = 0$ gilt.

Kapitel 3

Gruppen mit Vorzeichen und ihre anti-symmetrischen Abbildungen

Bei der Untersuchung der Diedergruppen stießen wir unabhängig von J. Širáň, M. Škoviera [24] auf den Begriff des Vorzeichens eines Gruppenelements. Im ersten Abschnitt beweisen wir zunächst einige, von J. Širáň, M. Škoviera erwähnte, grundlegende Eigenschaften. Danach zeigen wir, daß Gruppen der Ordnung $4k+2$ eine nicht-triviale Vorzeichenfunktion besitzen. Damit können wir einen sehr kurzen Beweis von Theorem 2 (Siemon, Seite 19) ableiten. Einen wichtigen Spezialfall untersuchen wir im Abschnitt „Anti-symmetrische Abbildungen der Diedergruppe". Wie bereits gezeigt, ist die Diedergruppe D_5 die einzige Gruppe der Ordnung 10, über der ein Prüfziffersystem existiert.

3.1 Gruppen mit Vorzeichen

Definition 8 *Eine Gruppe $(G,\cdot)$ besitzt das Vorzeichen sgn_G, falls $sgn_G : G \to \{-1,+1\}$ ein Homomorhpismus ist, d.h. $sgn_G(x\cdot y) = sgn_G(x)\cdot sgn_G(y)$. Ein Vorzeichen sgn_G heißt nicht-trivial, wenn sgn_G surjektiv ist. Das Vorzeichen eines Gruppenelements $x \in G$ ist $sgn_G(x)$. Die Elemente mit Vorzeichen $+1$ heißen positiv und die mit Vorzeichen -1 negativ. Die Menge aller positiven Elemente von G werde mit G^+, die der negativen Elemente mit G^- bezeichnet.*

Jede Gruppe G der Ordnung n besitzt das triviale Vorzeichen $x \mapsto 1$. Eine weitere Möglichkeit ein Vorzeichen auf G zu definieren erhalten wir, wenn wir G in die symmetrische Gruppe einbetten: Mit $l_a = (x \mapsto a\cdot x)$, der Linksmultiplikation mit a, ist $\alpha = (a \mapsto l_a)$ ein Isomorphismus von G auf $\bar{G} = \{l_a | a \in G\} \subseteq S_n$. Auf S_n können wir die Signatur eines Elements als Vorzeichen benutzen (vgl. Meyberg [17]):

$$sgn_G(a) := sgn_{\bar{G}}(l_a) \tag{3.1}$$

wobei $sgn_{\bar{G}}(l_a) = 1$, falls l_a als Produkt von einer geraden Anzahl Transpositionen dargestellt werden kann und $sgn_{\bar{G}}(l_a) = -1$ sonst. Ist $\bar{G}$ keine Untergruppe von A_n, so ist dieses Vorzeichen nicht-trivial.

Für das Vorzeichen gilt:

1. $sgn_G(e) = 1$.
2. $sgn_G(x^{-1}) = sgn_G(x)^{-1} = sgn_G(x)$.
3. $G = G^+ \cup G^-$.

Lemma 13 *G^+ ist ein Normalteiler mit Index ≤ 2.*

Beweis Als Kern des Homomorphismus sgn_G ist G^+ ein Normalteiler in G und alle Nebenklassen eines Normalteilers sind gleichmächtig. □

Korollar 12 *Gruppen mit ungerader Ordnung und einfache Gruppen (außer $\mathbb{Z}_2$) besitzen nur die triviale Vorzeichenfunktion $sgn_G : x \mapsto 1$.*

Elemente mit ungerader Ordnung haben das Vorzeichen 1, denn aus $ord(x) = 2k + 1$ folgt

$$sgn(x) = sgn(x^{2k+2}) = sgn(x)^{2k+2} = sgn(x)^{k+1} sgn(x)^{k+1} = 1.$$

Einfache Gruppen (außer $\mathbb{Z}_2$) haben keine Normalteiler mit Index 2.

Lemma 14 *Ist U eine Untergruppe mit Index 2 in G, dann wird durch*

$$sgn(x) = \begin{cases} 1 & \text{falls } x \in U \\ -1 & \text{sonst} \end{cases}$$

ein Vorzeichen auf G definiert.

Beweis U ist ein Normalteiler in G und es gilt

$$x \cdot y \in U \qquad \Leftrightarrow \qquad x, y \in U \text{ oder } x, y \notin U$$

und

$$x \cdot y \notin U \qquad \Leftrightarrow \qquad x \in U, y \notin U \text{ oder } x \notin U, y \in U.$$

Folglich ist $sgn : G \to \{-1, 1\}$ ein Homomorphismus. □

Die letzten beiden Lemmata fassen wir wie folgt zusammen

Satz 13 *Eine Gruppe besitzt eine nicht-triviale Vorzeichenfunktion genau dann, wenn sie eine Untergruppe mit Index 2 besitzt.*

Bemerkung Falls G ein nicht-triviales Vorzeichen besitzt, so gilt $G/G^+ \cong \mathbb{Z}_2$, d.h. man kann die Gruppe G als Erweiterung von G^+ durch $\mathbb{Z}_2$ ansehen.
Beispiel Die zyklische Gruppe $\mathbb{Z}_n$ besitzt ein nicht-triviales Vorzeichen genau dann, wenn n gerade ist. Ist n ungerade, dann hat $\mathbb{Z}_n$ kein Vorzeichen. Ist n gerade dann wird durch

$$sgn(x) = \begin{cases} 1 & \text{falls } x \text{ gerade} \\ -1 & \text{falls } x \text{ ungerade} \end{cases}$$

ein Vorzeichen auf $\mathbb{Z}_n$ definiert.

Beispiel Auf der Gruppe der Anti-Automorphismen vereinigt mit den Automorphismen einer Gruppe G wird durch $sgn(\varphi) = 1$, falls φ ein Automorphismus ist und $sgn(\varphi) = -1$, falls φ ein Anti-Automorphismus ist, ein Vorzeichen definiert. Dieses Vorzeichen ist genau dann nicht trivial, wenn G nicht abelsch ist (vgl. Abschnitt „Automorphismen und Anti-Automorphismen").

Satz 14 *Eine Gruppe G der Ordnung $n = 2(2k+1)$, $k \geq 1$, besitzt ein nicht-triviales Vorzeichen.*

Beweis Wir zeigen, daß das in 3.1 definierte Vorzeichen nicht-trivial ist, d.h. es existiert ein $a \in G$ mit $sgn_G(a) = sgn_{\bar{G}}(l_a) = -1$. Da die Ordnung von G gerade ist, existiert ein $a \in G$ der Ordnung 2. Daher ist $l_a \circ l_a = Id$ und l_a besteht aus $2k+1$ Transpositionen ($x_i \in G$ geeignet)

$$l_a = (e \;\; l_a(e))(x_2 \;\; l_a(x_2)) \ldots (x_{2k+1} \;\; l_a(x_{2k+1})).$$

Da $2k+1$ ungerade ist, folgt $sgn_G(a) = sgn_{\bar{G}}(l_a) = -1$. □

Korollar 13 *Jede Gruppe der Ordnung $n = 2(2k+1)$, $k \geq 1$, besitzt einen Normalteiler der Ordnung $2k+1$.*

Beweis Da eine solche Gruppe ein nicht-triviales Vorzeichen besitzt, hat die zugehörige Menge der positiven Elemente G^+ die Ordnung $2k+1$ und ist daher ein Normalteiler mit der gesuchten Eigenschaft. □

Wir geben nun den noch fehlenden Beweis von Theorem 2 an. Wir müssen zeigen, daß eine Gruppe G der Ordnung $2(2k+1)$, $k \geq 1$, keine vollständige Abbildung besitzt. G besitzt ein nicht-triviales Vorzeichen sgn (Satz 14) und G^+

ist ein Normalteiler der Ordnung $2k+1$ (Korollar 13).
Wenn G eine vollständige Abbildung f besitzt, dann folgt:

$$\begin{aligned}\prod_{x\in G} sgn(x) &= \prod_{x\in G^+} sgn(x) \prod_{x\in G^-} sgn(x) \\ &= 1\cdot(-1)^{|G^-|} = (-1)^{|G^+|} = (-1)^{2k+1} = -1\end{aligned}$$

und

$$\begin{aligned}\prod_{x\in G} sgn(x) &= \prod_{x\in G} sgn(xf(x)) = \prod_{x\in G} sgn(x) \prod_{x\in G} sgn(f(x)) \\ &= \prod_{x\in G} sgn(x) \prod_{x\in G} sgn(x) = (-1)\cdot(-1) = 1,\end{aligned}$$

also ein Widerspruch. Demnach kann G keine vollständige Abbildung besitzen. □

3.2 Anti-symmetrische Abbildungen

In diesem Abschnitt zeigen wir weitere Möglichkeiten, wie wir aus einer anti-symmetrischen Abbildung neue konstruieren können.

Wir nennen zwei Permutationen p, q elementfremd, wenn für alle x gilt:

$$p(x) = x \qquad \text{oder} \qquad q(x) = x.$$

Satz 15 *Sei $(G,\cdot)$ eine Gruppe mit Vorzeichen sgn, $g, g\circ r \in Ant(G)$, und es gelte für alle $x \in G$: $sgn(g(x)) = c\cdot sgn(x)$ und $sgn(r(x)) \neq sgn(x)$ mit $c \in \{-1,1\}$, dann ist für jede Zerlegung von r in elementfremde Faktoren, $r = p\circ q$, auch $g\circ p \in Ant(G)$.*

Beweis Annahme: $g\circ p$ ist nicht anti-symmetrisch, d.h. es existieren $a, b \in G$, $a \neq b$ mit

$$g\circ p(a)\cdot b = g\circ p(b)\cdot a.$$

Offensichtlich gilt dann $p(a) \neq a$ oder $p(b) \neq b$, sonst wäre g nicht anti-symmetrisch:

$$g\circ p(a)\cdot b = g(a)\cdot b = g(b)\cdot a = g\circ p(b)\cdot a.$$

Wenn dagegen $p(a) \neq a$ und $p(b) \neq b$ gilt, dann kommen a und b nicht in q vor

und es folgt $q(a) = a$, $q(b) = b$ und damit

$$\begin{aligned} g \circ r(a) \cdot b &= g \circ p \circ q(a) \cdot b \\ &= g \circ p(a) \cdot b \\ &= g \circ p(b) \cdot a \\ &= g \circ p \circ q(b) \cdot a \\ &= g \circ r(b) \cdot a \end{aligned}$$

im Widerspruch zur Voraussetzung $q \circ r \in Ant(G)$. Es bleibt daher nur die Möglichkeit $p(a) \neq a, p(b) = b$. (Die Annahme ist in a und b symmetrisch, es ist also auch $p(a) = a, p(b) \neq b$ abgedeckt.) Auch in diesem Fall kommt a in p vor und damit nicht in q, d.h. $q(a) = a$. Aus der Annahme folgt somit die Gleichung

$$g \circ r(a) \cdot b = g \circ p \circ q(a) \cdot b = g \circ p(a) \cdot b = g \circ p(b) \cdot a = g(b) \cdot a.$$

Ein Vergleich der Vorzeichen zeigt aber

$$sgn(g \circ r(a) \cdot b) = c \cdot sgn(r(a))sgn(b) \neq c \cdot sgn(a)sgn(b) = sgn(g(b) \cdot a).$$

Damit ist die Annahme widerlegt, d.h. es gilt für alle $a, b \in G$, $a \neq b$, $g \circ p(a) \cdot b \neq g \circ p(b) \cdot a$, folglich ist $g \circ p$ eine anti-symmetrische Abbildung. □

Ein ähnlicher Satz gilt für eine nachgeschaltete Permutation.

Satz 16 *Sei $(G, \cdot)$ eine Gruppe mit Vorzeichen sgn, $g, r \circ g \in Ant(G)$ und es gelte für alle $x \in G$: $sgn(g(x)) = c \cdot sgn(x)$ und $sgn(r(x)) \neq sgn(x)$, mit $c \in \{-1, 1\}$, dann ist für jede Zerlegung von r in elementfremde Faktoren, $r = p \circ q$, auch $p \circ g \in Ant(G)$.*

Beweis Seien $\tilde{r} := g^{-1} \circ r \circ g$, $\tilde{p} := g^{-1} \circ p \circ g$ und $\tilde{q} := g^{-1} \circ q \circ g$, dann ist $g \circ \tilde{r} = r \circ g$ anti-symmetrisch und $\tilde{r} = \tilde{p} \circ \tilde{q}$. Die Permutationen $\tilde{p}$ und $\tilde{q}$ sind elementfremd, denn wenn $\tilde{p}(a) \neq a$ gilt, dann folgt $p(g(a)) \neq g(a)$ und, da p und q elementfremd sind, $q(g(a)) = g(a)$. Also gilt $\tilde{q}(a) = g^{-1}(q(g(a))) = g^{-1}(g(a)) = a$ und a kommt in q nicht vor. Außerdem gilt

$$\begin{aligned} sgn(\tilde{r}(x)) &= sgn(g^{-1} \circ r \circ g(x)) = c \cdot sgn(g \circ g^{-1} \circ r \circ g(x)) \\ &= c \cdot sgn(r \circ g(x)) \\ &\neq c \cdot sgn(g(x)) = sgn(x). \end{aligned}$$

Nun sind die Voraussetzungen des vorherigen Satzes für $\tilde{r}$,$\tilde{p}$ und $\tilde{q}$ erfüllt und es folgt $g \circ \tilde{p} = g \circ g^{-1} \circ p \circ g = p \circ g \in Ant(G)$. □

Wie der Beweis zeigt, besitzt jede anti-symmetrische Abbildung $\tilde{p} \circ g$ ($\tilde{p}, g$ gemäß Satz 16) ein weitere Darstellung $g \circ p$ (p gemäß Satz 15).

Am Beweis von Satz 15 sehen wir außerdem, daß wir das nicht-trivale Vorzeichen der Gruppe nur an einer Stelle benutzen. Für beliebige Gruppen gilt daher:

Satz 17 *Sei $(G, \cdot)$ eine Gruppe, $g, g \circ r \in Ant(G)$ und es gelte für alle $x, y \in G$*

$$g \circ r(x) \cdot y = g(y) \cdot x \Rightarrow x = y,$$

dann ist für jede Zerlegung von r in elementfremde Faktoren, $r = p \circ q$, auch $g \circ p \in Ant(G)$.

Bemerkung Aus $g, g \circ r \in Ant(G)$ folgt nicht $g \circ r(x) \cdot y = g(y) \cdot x \Rightarrow x = y$ wie folgendes Gegenbeispiel der Diedergruppe D_5 (Gruppentafel auf Seite 52) zeigt: Sei $g(x) = x^{-1} \cdot 2$ und $r(x) = x \cdot 1$, dann gilt $g, g \circ r \in Ant(D_5)$ (Satz 20, Seite 52), aber

$$g \circ r(0) \cdot 3 = g(1) \cdot 3 = 1 \cdot 3 = 4 = 2 \cdot 2 = g(3) \cdot 0.$$

Für die speziellen anti-symmetrischen Abbildungen $g(x) = b \cdot x^{-1}a$ können wir konkret angeben, für welche p die Voraussetzungen von Satz 15 erfüllt sind.

Satz 18 *Sei $(G, \cdot)$ eine Gruppe mit Vorzeichen sgn, und $g(x) = b \cdot x^{-1}a$ sei eine anti-symmetrische Abbildung. Zudem erfülle die Permutation*

$$p = (k_1 \ l_1)(k_2 \ l_2) \ldots (k_n \ l_n),$$

wobei $(k_i \ l_i)$ eine Transposition ist ($k_i, l_i \in G$), die Bedingungen:

1. *$l_1^{-1} \cdot k_1 = l_j^{-1} \cdot k_j$, für $j = 2, \ldots, n$*
2. *$ord(l_1^{-1} \cdot k_1) = 2$, $sgn(l_1^{-1} \cdot k_1) = -1$*

dann ist auch $g \circ p(x)$ anti-symmetrisch.

Beweis Es sei $p = (k_1 \ l_1)(k_2 \ l_2) \ldots (k_n \ l_n)$ eine Permutation mit den genannten Eigenschaften. Aus den Voraussetzungen folgt, daß die Transpositionen $(k_i \ l_i)$ und $(k_j \ l_j)$ entweder gleich oder elementfremd sind. Wir nehmen daher o.B.d.A. an, daß sie paarweise elementfremd sind. Sei $c := l_1^{-1} \cdot k_1$ und $r(x) := x \cdot c$, dann ist $g \circ r \in Ant(G)$ und man sieht leicht, daß für die Zerlegung von r in elementfremde Faktoren

$$r = (k_1 \ l_1)(k_2 \ l_2) \ldots (k_n \ l_n) \circ q = p \circ q$$

gilt, denn $r(l_i) = l_i \cdot l_1^{-1} \cdot k_1 = l_i \cdot l_i^{-1} \cdot k_i = k_i$ und $r \circ r = id$. Außerdem ist $sgn(g(x)) = sgn(b \cdot x^{-1} \cdot a) = sgn(a \cdot b)sgn(x)$ und $sgn(r(x)) = sgn(x \cdot l_1^{-1} \cdot k_1) = sgn(x)sgn(l_1^{-1} \cdot k_1) = -sgn(x) \neq sgn(x)$. Damit sind die Voraussetzungen von Satz 15 für g und $r = p \circ q$ erfüllt und es folgt $g \circ p \in Ant(G)$. □

Ganz analog zeigt man den folgenden Satz, der ein Spezialfall von Satz 16 ist.

Satz 19 *Sei $(G, \cdot)$ eine Gruppe mit Vorzeichen sgn, und $g(x) = b \cdot x^{-1} \cdot a \in Ant(G)$. Zudem erfülle die Permutation*

$$p = (k_1 \ \ l_1)(k_2 \ \ l_2) \ldots (k_n \ \ l_n)$$

die folgenden Bedingungen:

1. $l_1 \cdot k_1^{-1} = l_j \cdot k_j^{-1}$, *für* $j = 2, \ldots, n$
2. $ord(l_1 \cdot k_1^{-1}) = 2$, $sgn(l_1 \cdot k_1^{-1}) = -1$

dann ist auch $p \circ g(x)$ anti-symmetrisch.

3.3 Anti-symmetrische Abbildungen der Diedergruppe

Die Diedergruppe D_5 spielt eine wichtige Rolle bei der Suche nach einem Prüfziffersystem, denn sie ist die einzige Gruppe der Ordnung 10 die eine anti-symmetrische Abbildung besitzt. In diesem Abschnitt zeigen wir daher einige Eigenschaften der anti-symmetrischen Abbildungen der Diedergruppe. Dazu benutzen wir die Matrixschreibweise der Diedergruppe (H.P. Gumm [12]) ($s > 2$)

$$D_s = \{(e, x) | e \in \{-1, 1\} \text{ und } x \in \mathbb{Z}_s\}$$

mit der Verknüpfung

$$(e, x) \cdot (f, y) := (e \cdot f, e \cdot y + x).$$

In der ersten Komponente wird in der multiplikativ geschriebenen Gruppe $\mathbb{Z}_2$ gerechnet, in der zweiten im Ring $\mathbb{Z}_s$. Den Paaren (e, x) ordnen wir die Ziffern $\{0, \ldots, 2s-1\}$ auf folgende Weise zu:

$$(1, x) \mapsto x \qquad (-1, x) \mapsto s + x$$

Für D_5 haben wir damit die Gruppentafel:

$\cdot$	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

Durch die Matrixschreibweise können wir eine anti-symmetrische Abbildung $g \in Ant(D_s)$ in der Form

$$g(e,x) = (g_1(e,x), g_2(e,x))$$

schreiben, wobei $g_1 : D_s \to \{-1,1\}$ und $g_2 : D_s \to \{0,\ldots,s-1\}$ surjektive Abbildungen sind.

Als Folgerung von Theorem 4 (Seite 24) und Satz 3 (Seite 30) erhalten wir

Satz 20 *Die Abbildungen $b \cdot x^{-1} \cdot a$ mit $b \in D_s$, ($s > 2$ ungerade) und $a \in \{1,...,s-1\}$ sind anti-symmetrisch.*

Beweis Die Abbildung $x^{-1} \cdot a$, $a \in \{1,...,s-1\}$ ist anti-symmetrisch, da a mit keinem Element der Ordnung 2 kommutiert: Weil s ungerade ist, haben nur die Elemente $(-1,c)$ die Ordnung 2, denn aus $(1,x) \cdot (1,x) = (1,2x) = (1,0)$ folgt $x = 0$. Angenommen $a = (1,a)$ kommutiert mit dem Element $(-1,c)$, d.h.

$$(1,a) \cdot (-1,c) = (-1,c+a) = (-1,c-a) = (-1,c) \cdot (1,a).$$

Es folgt $c + a = c - a$ bzw. $2a = 0$ und damit $a = 0$, im Widerspruch zu $a \in \{1,...,s-1\}$. Also ist $x^{-1}a$ und somit auch $bx^{-1}a$ anti-symmetrisch. □

Bei einem Vergleich dieses Satzes mit dem vorherigen Abschnitt, stellt sich die Frage, ob Satz 18 anwendbar ist. Dies ist möglich, wie der folgende Satz zeigt. Zunächst führen wir allerdings das Vorzeichen eines Elements der Diedergruppe ein. Auf der Diedergruppe wird durch die Funktion $sgn : D_s \to \{-1,1\}$,

$$sgn(e,x) := e$$

ein nicht-triviales Vorzeichen definiert, denn es gilt

$$sgn((e,x) \cdot (f,y)) = sgn(ef, ey + x) = ef = sgn(e,x)sgn(f,y).$$

Wenn wir die Darstellung der Diedergruppe mit den Ziffern $\{0, \ldots, 2s-1\}$ benutzen, dann ist $sgn(x) = sgn(1,x) = 1$, $0 \leq x \leq s-1$ und $sgn(s+x) = sgn(-1,x) = -1$, $s \leq s+x \leq 2s-1$.

Satz 21 *Sei* $g(x) := b \cdot x^{-1} \cdot a \in Ant(D_s)$ *und* $p := (k_1\ l_1)(k_2\ l_2)\ldots(k_n\ l_n)$ *mit den Eigenschaften* $s \leq k_i \leq 2s-1$, $0 \leq l_i \leq s-1$, $k_i \neq k_j$ *und* $l_1^{-1} \cdot k_1 = l_j^{-1} \cdot k_j$, *bzw.* $l_1 \cdot k_1^{-1} = l_j \cdot k_j^{-1}$, $j = 2, \ldots, n$, *dann ist auch* $g \circ p$ *bzw.* $p \circ g \in Ant(D_s)$.

Beweis Es ist $sgn(k_1) = -1 \neq 1 = sgn(l_1)$ und $(l_1^{-1} \cdot k_1) \cdot (l_1^{-1} \cdot k_1) = (1,y) \cdot (-1,x) \cdot (1,y) \cdot (-1,x) = (-1, x+y) \cdot (-1, x+y) = (1, -x-y+x+y) = (1,0)$ also $ord(l_1^{-1} \cdot k_1) = ord(l_1 \cdot k_1^{-1}) = 2$. Mit Satz 18 bzw. Satz 19 folgt die Behauptung. □

Mit diesem Satz können wir 3040 anti-symmetrische Abbildungen der Diedergruppe D_5 aus den Permutationen $b \cdot x^{-1} \cdot a$ konstruieren (bislang waren nur 40 bekannt).

Beispiel Wir wählen $b = 0, a = 1$, dann ist $g(x) = x^{-1} \cdot 1 = (10)(42)(98765) \in Ant(D_5)$. Aus Satz 21 folgt, daß z.B. auch $g \circ (50) \circ (61) \in Ant(D_5)$ oder $g \circ (61) \cdot (83) \cdot (94) = (50) \circ (73) \circ (82) \circ g \in Ant(D_5)$.

3.3.1 Fehlererkennung

Für die Komponentenfunktionen g_1, g_2 der Diedergruppe können wir weitere Eigenschaften zeigen. Außerdem beweisen wir am Ende dieses Abschnitts, daß über den Diedergruppen D_s, $s > 2$ ungerade, kein Prüfziffersystem existiert, welches alle Sprungtranspositionen erkennt.

Satz 22 *Sei* $g \in Ant(D_s)$ $(s > 2)$, $g(e,x) = (g_1(e,x), g_2(e,x))$, *dann hängt* g_2 *von* e *und von* x *ab.*

Beweis Fall 1: g_2 hänge nur von e ab, d.h. $g_2(e,x) = g_2(e)$. In diesem Fall besitzt $g_2(D_s)$ höchstens zwei Elemente (nämlich $g_2(1,0)$ und $g_2(-1,0)$) und $g(D_s)$ besitzt höchstens vier Elemente $(\pm 1, g_2(\pm 1, 0))$. Damit kann g keine Permutation sein, da D_s für $s > 2$ mindestens sechs Elemente hat. Also ist $g \notin Ant(D_s)$.
Fall 2: g_2 hänge nur von x ab, d.h. $g_2(e,x) = g_2(x)$. Auch hier folgt, daß g nicht anti-symmetrisch ist, denn es gilt entweder $g_1(1,0) = g_1(-1,0)$ und g wäre nicht injektiv, $g(1,0) = (g_1(1,0), g_2(0)) = (g_1(-1,0), g_2(0)) = g(-1,0)$, oder $g_1(1,0) = -g_1(-1,0)$ und damit

$$\begin{aligned} g(1,0) \cdot (-1,0) &= (g_1(1,0), g_2(0)) \cdot (-1,0) = (-g_1(1,0), g_2(0)) \\ &= (g_1(-1,0), g_2(0)) \\ &= g(-1,0) \cdot (1,0). \end{aligned}$$

Folglich ist g nur anti-symmetrisch wenn g_2 von e und von x abhängt. □

Satz 23 *Sei $g \in Ant(D_s)$ ($s > 2$ ungerade), $g(e,x) = (g_1(e,x), g_2(e,x))$, dann hängt g_1 entweder nur von e oder von e und x ab.*

Beweis Wenn g_1 nur von x abhängt, dann gilt für alle $x \in \{0,\ldots,s-1\}$ $g_1(1,x) = g_1(-1,x)$. Die Anzahl $a_1 := |\{(e,x) \in D_s | g_1(e,x) = 1\}|$ und $a_{-1} := |\{(e,x) \in D_s | g_1(e,x) = -1\}|$ der Elemente, für die $g_1(e,x)$ gleich 1 bzw. -1 ist, muß daher gerade sein, $a_i = 2k_i$. Weiterhin gilt $a_1 + a_{-1} = 2k_1 + 2k_{-1} = |D_s| = 2s$, woraus $k_1 + k_{-1} = s$ folgt. Da s ungerade ist, muß $k_1 \neq k_{-1}$ und deshalb $a_1 \neq a_{-1}$ gelten. Damit kann g nicht injektiv sein, denn es gilt $|\{(e,x) \in D_s | e = 1\}| = s = |\{(e,x) \in D_s | e = -1\}|$. Also ist g im Fall, daß g_1 nur von x abhängt, nicht anti-symmetrisch. □

Satz 24 *Sei $g \in Ant(D_s)$, $s > 2$, $g(e,x) = (e, g_2(e,x))$, dann sind $g_2(1,x)$ und $g_2(-1,-x)$ anti-symmetrische Abbildungen von $\mathbb{Z}_s$.*

Beweis Sei $c \in \{-1,1\}$, wir zeigen $g_2(c,cx) \in Ant(\mathbb{Z}_s)$. Dazu sei $g_2(c,cx) + y = g_2(c,cy) + x$. Es folgt $g(c,cx) \cdot (c,cy) = (1, y + g_2(c,cx)) = (1, x + g_2(c,cy)) = g(c,cy) \cdot (c,cx)$ und damit $(c,cx) = (c,cy)$ bzw. $x = y$. □

Satz 25 *Sei $g \in Ant(D_s)$ ($s > 2$ gerade), $g(e,x) = (g_1(e,x), g_2(e,x))$, dann hängt g_1 entweder nur von x oder von e und x ab.*

Beweis Wenn g_1 nur von e abhängt, dann wäre $g_2(1,x)$ eine anti-symmetrische Abbildung von $\mathbb{Z}_s$. Wir haben aber bereits gezeigt, daß $\mathbb{Z}_s$ für gerades s keine anti-symmetrische Abbildung besitzt. □

Abschließend zeigen wir eine wichtige Eigenschaft der anti-symmetrischen Abbildungen der Diedergruppe.

Satz 26 *Sei $g \in Ant(D_s)$, $s > 2$ ungerade, dann existiert ein $c \in D_s$, so daß $g(x) \cdot c \notin Ant(D_s)$ ist.*

Korollar 14 *Über der Diedergruppe D_s, $s > 2$ ungerade, existiert kein Prüfziffersystem das alle Sprungtranspositionen erkennt.*

Beweis Es existiert ein Element $(-1,x) \in D_s$, so daß $-g_1(1,0) = g_1(-1,x)$ gilt, denn sonst hätten wir mindestens $s+1$ Elemente mit dem gleichen Vorzeichen und g wäre keine Permutation. In $\mathbb{Z}_s$ existiert ein multiplikativ Inverses von 2, nämlich $1/2 = k+1$, wenn $s = 2k+1$ ist. Wir setzen

$$c := \big(1, 1/2 \cdot g_1(-1,x)\big(g_1(1,0)x + g_2(1,0) - g_2(-1,x)\big)\big)$$

und es folgt

$$\begin{aligned}
g(1,0)\cdot c\cdot(-1,x) &= \big(g_1(1,0),g_2(1,0)\big)\cdot\big(1,1/2\cdot g_1(-1,x)\cdot\\
&\quad \big(g_1(1,0)x+g_2(1,0)-g_2(-1,x)\big)\big)\cdot\big(-1,x\big)\\
&= \big(g_1(1,0),g_1(1,0)\cdot 1/2\cdot g_1(-1,x)\cdot\\
&\quad \big(g_1(1,0)x+g_2(1,0)-g_2(-1,x)\big)+g_2(1,0)\big)\cdot\big(-1,x\big)\\
&= \big(-g_1(1,0),g_1(1,0)x+g_1(1,0)\cdot 1/2\cdot g_1(-1,x)\cdot\\
&\quad \big(g_1(1,0)x+g_2(1,0)-g_2(-1,x)\big)+g_2(1,0)\big)\\
&= \big(-g_1(1,0),1/2\big(g_1(1,0)x+g_2(1,0)+g_2(-1,x)\big)\big)\\
g(-1,x)\cdot c\cdot(1,0) &= g(-1,x)\cdot c\\
&= \big(g_1(-1,x),g_2(-1,x)\big)\cdot\big(1,1/2\cdot g_1(-1,x)\cdot\\
&\quad \big(g_1(1,0)x+g_2(1,0)-g_2(-1,x)\big)\big)\\
&= \big(g_1(-1,x),g_1(-1,x)\cdot 1/2\cdot g_1(-1,x)\cdot\\
&\quad \big(g_1(1,0)x+g_2(1,0)-g_2(-1,x)\big)+g_2(-1,x)\big)\\
&= \big(-g_1(1,0),1/2\big(g_1(1,0)x+g_2(1,0)+g_2(-1,x)\big)\big)
\end{aligned}$$

also $g(1,0)\cdot c\cdot(-1,x) = g(-1,x)\cdot c\cdot(1,0)$ und $g(x)\cdot c$ ist nicht anti-symmetrisch. Außerdem erkennt g nicht alle Sprungtranspositionen (vgl. Seite 14). □

Zusammen mit Korollar 4 (Seite 19) haben wir damit gezeigt:

Theorem 10 *Sei $s > 2$ ungerade. Über der Gruppe D_s existiert kein Prüfziffersystem, das alle Sprungtranspositionen oder alle Zwillings- oder alle Sprungzwillingsfehler erkennt.*

3.3.2 Automorphismen und Anti-Automorphismen der Diedergruppe

Die Automorphismen und die Anti-Automorphismen sind bei der Bestimmung der Äquivalenzklassen bzw. bei der Suche nach anti-symmetrischen Abbildungen sehr wichtig. Für die Diedergruppe D_s, $s > 2$, kann man diese recht einfach bestimmen. Dazu nutzt man aus, daß die Diedergruppe von den Elementen $(1,1)$ und $(-1,0)$ erzeugt wird. Das Element $(1,1)$ hat in D_s die Ordnung s und $(-1,x)$ hat für alle x die Ordnung 2. Da für jeden Automorphismus oder Anti-Automorphismus φ die Elemente $\varphi(x)$ und x die gleiche Ordnung haben, muß $\varphi(1,1) = (1,d)$ für ein $d \in \mathbb{Z}_s$ gelten. d muß dabei eine Einheit des Ringes $\mathbb{Z}_s$ sein, d.h. $ggT(d,s) = 1$, sonst hätte $(1,d)$ nicht die Ordnung s. Ebenso folgt, daß $\varphi(-1,0) = (-1,c)$ ist mit $c \in \mathbb{Z}_s$, denn andernfalls würde φ alle Elemente auf die Untergruppe

$\{(1,x)|x \in \mathbb{Z}_s\}$ abbilden und φ wäre demnach nicht surjektiv. Wie wir bereits gezeigt haben, reicht es, die Automorphismen einer Gruppe zu bestimmen, denn die Anti-Automorphismen lassen sich durch $inv \circ \varphi$ darstellen, wobei φ ein Automorphismus ist. Mit der Verknüpfung $(e,x)\cdot(f,y) = (ef, ey+x)$ der Diedergruppe erhalten wir die folgenden Eigenschaften des Automorphismus φ:

1. $\varphi(1,x) = \varphi(1,1)^x = (1,d)^x = (1,dx)$, für alle $x \in \mathbb{Z}_s$.
2. $\varphi(-1,x) = \varphi((1,x)\cdot(-1,0)) = \varphi(1,x)\cdot\varphi(-1,0) = (1,dx)\cdot(-1,c) = (-1,c+dx)$, für alle $x \in \mathbb{Z}_s$.

Die Eigenschaften 1 und 2 sind also notwendig dafür, daß φ ein Automorphismus ist. Sie sind aber auch hinreichend. Dazu seien d eine Einheit von $\mathbb{Z}_s$, c ein Element von $\mathbb{Z}_s$ und $\varphi : D_s \to D_s$ eine Abbildung mit $\varphi(1,x) = (1,dx)$, $\varphi(-1,x) = (-1,c+dx)$. Mit dieser Definition ist φ bijektiv, denn aus $\varphi(e,x) = \varphi(f,y)$ folgt $e = f$ und $dx = dy$ bzw. $c+dx = c+dy$ und damit, weil d eine Einheit ist, $x = y$. Also ist φ injektiv und damit auch surjektiv (D_s ist endlich). φ ist außerdem ein Homomorphismus, denn es gilt für alle $x, y \in \mathbb{Z}_s$:

- $\varphi((1,x)\cdot(1,y)) = \varphi(1,x+y) = (1,dx+dy) = (1,dx)\cdot(1,dy) = \varphi(1,x)\cdot\varphi(1,y)$
- $\varphi((1,x)\cdot(-1,y)) = \varphi(-1,y+x) = (-1,c+dy+dx) = (1,dx)\cdot(-1,c+dy) = \varphi(1,x)\cdot\varphi(-1,y)$
- $\varphi((-1,x)\cdot(1,y)) = \varphi(-1,-y+x) = (-1,c-dy+dx) = (-1,c+dx)\cdot(1,dy) = \varphi(-1,x)\cdot\varphi(1,y)$
- $\varphi((-1,x)\cdot(-1,y)) = \varphi(1,-y+x) = (1,-dy+dx) = (-1,c+dx)\cdot(-1,c+dy) = \varphi(-1,x)\cdot\varphi(-1,y)$

Also ist φ ein Automorphismus.

Damit haben wir für die Anti-Automorphismen der Diedergruppe die Darstellung

$$\begin{aligned} inv \circ \varphi(1,x) &= (1,dx)^{-1} = (1,-dx) \\ inv \circ \varphi(-1,x) &= (-1,c+dx)^{-1} = (-1,c+dx). \end{aligned}$$

Der folgende Satz faßt dieses Ergebnis zusammen:

Satz 27 *Seien $\varphi, \psi : D_s \to D_s$ Abbildungen der Diedergruppe D_s,$s > 2$, dann gilt:*

1. *Genau dann ist φ ein Automorphismus, wenn eine Einheit d und ein Element c von $\mathbb{Z}_s$ existieren mit $\varphi(1,x) = (1,dx)$ und $\varphi(-1,x) = (-1,c+dx)$.*

2. *Genau dann ist ψ ein Anti-Automorphismus, wenn eine Einheit d und ein Element c von $\mathbb{Z}_s$ existieren mit $\psi(1,x) = (1,-dx)$ und $\psi(-1,x) = (-1, c + dx)$.*

Wenn s ungerade ist, d.h. $s = 2k+1$, dann besitzt 2 ein multiplikativ Inverses, nämlich $1/2 = k+1$. Die Funktion $(1-e)/2$ ist dann gleich 0, wenn $e = 1$ ist und gleich 1, wenn $e = -1$ ist. Die Automorphismen der Diedergruppe D_s haben daher für $s > 2$ ungerade alle die Form $\varphi(e,x) = (e, (1-e)/2 \cdot c + dx) = (e, (1-e)\tilde{c} + dx) = (e, \tilde{c} - e\tilde{c} + dx)$ und die Anti-Automorphismen haben die Form $\psi(e,x) = (e, \tilde{c} - e\tilde{c} - edx)$ mit $d \in \mathbb{Z}_s^*$ und $\tilde{c} \in \mathbb{Z}_s$.

Damit können wir die folgenden Sätze zeigen:

Satz 28 *Die Diedergruppe D_s $s > 2$ besitzt keinen anti-symmetrischen Automorphismus und sie besitzt einen fixpunktfreien, d.h. anti-symmetrischen, Anti-Automorphismus genau dann, wenn s ungerade ist.*

Beweis Ist s gerade, dann ist $s/2$ das einzige Element der Ordnung 2 in $\mathbb{Z}_s$. Da jeder (Anti-)Automorphismus ψ die Ordnung und das Vorzeichen $e = sgn(e,x)$ erhält, gilt $\psi(1, s/2) = (1, s/2)$ und ψ ist nicht anti-symmetrisch.

Ist s ungerade, dann kommutiert $(1,1)$ mit keinem Element der Ordnung 2, $(1,1) \cdot (-1,x) = (-1, x+1) \neq (-1, x-1) = (-1,x) \cdot (1,1)$, und damit ist $\psi(x) = (1,-1) \cdot x^{-1} \cdot (1,1)$ ein fixpunktfreier Anti-Automorphismus. Ist φ ein Automorphismus mit $\varphi(-1,0) = (-1,c)$, dann definieren wir $z := (-1, 1/2 \cdot c)$ und es folgt

$$\begin{aligned} \varphi(-1,0) &= (-1,c) = (-1, 1/2 \cdot c + 1/2 \cdot c) \\ &= (-1, 1/2 \cdot c)(-1,0)(-1, 1/2 \cdot c) \\ &= z^{-1}(-1,0)z. \end{aligned}$$

Also ist φ nicht anti-symmetrisch (Satz 8, Seite 35). □

Satz 29 *Sei ψ ein Anti-Automorphismus der Diedergruppe D_s, d.h. $\psi(1,x) = (1,dx)$ und $\psi(-1,x) = (-1, c-dx)$ mit $c \in \mathbb{Z}_s$, $d \in \mathbb{Z}_s^*$, dann ist ψ genau dann fixpunktfrei, wenn $d-1$ eine Einheit und $d+1$ kein Teiler von c (in $\mathbb{Z}_s$) ist.*

Beweis Wenn ψ einen Fixpunkt $(1,x) \neq (1,0)$ oder $(-1,x)$ besitzt, dann gilt $\psi(1,x) = (1,dx) = (1,x)$ oder $\psi(-1,x) = (-1, c-dx) = (-1,x)$. Im ersten Fall folgt $dx = x$ bzw. $(d-1)x = 0$ und $d-1$ ist keine Einheit. Im zweiten Fall ist $c - dx = x$ also $c = (d+1)x$ und $d+1$ teilt c. Da nur Äquivalenzumformungen benutzt wurden, folgt damit auch die Rückrichtung. □

Beispiel Für die Diedergruppe D_5 können wir $c = 1,2,3,4$ und $d = 4$ wählen.

3.3.3 Beispiele

In diesem Abschnitt geben wir verschiedene Literatur-Beispiele von anti-symmetrischen Abbildungen der Diedergruppe an und zeigen, daß diese Spezialfälle der bisher erarbeiteten Sätze darstellen. Mit diesen Sätzen gelingt uns jeweils ein deutlich kürzerer Beweis der Behauptungen.

Beispiel (VERHOEFF [27]) Definiere φ durch $\varphi(a^k) = a^{-k}$ und $\varphi(a^j b) = a^{j-d}b$, $d \neq 0$, dann ist $\varphi \in Ant(D_s)$, s ungerade.
Beweis Wir schreiben φ zunächst in der Matrixschreibweise: $\varphi(1,k) = (1,-k)$ und $\varphi(-1,j) = (-1, j-d)$. Es folgt, daß $\varphi(e,x) = (1,-1/2\cdot d)\cdot(e,x)^{-1}\cdot(1,1/2\cdot d)$ ist, denn

$$\begin{aligned}(1,-1/2\cdot d)\cdot(e,x)^{-1}\cdot(1,1/2\cdot d) &= (1,-1/2\cdot d)\cdot(e,-ex)\cdot(1,1/2\cdot d)\\ &= (e,-ex-1/2\cdot d+1/2\cdot ed)\\ &= \begin{cases}(1,-x) & \text{falls } e=1\\ (-1,x-d) & \text{falls } e=-1.\end{cases}\end{aligned}$$

Nach Satz 20 (Seite 52) ist damit φ eine anti-symmetrische Abbildung von D_5.

Beispiel (H.P. GUMM [12]) Für $a,b \in \mathbb{Z}_s$, s ungerade, $a \neq 0$ ist $\varphi(e,x) := (e, e(a-x)+b) \in Ant(D_s)$.
Beweis Es ist $\varphi(e,x) = (1,b)(e,x)^{-1}(1,a) = (1,b)(e,-ex)(1,a) = (e,-ex+b+ea) = (e,e(a-x)+b)$ und wir können wieder Satz 20 anwenden.

Beispiel (GALLIAN/MULLIN [10]) Die im Beweis von Theorem 3 (Seite 22) definierte Abbildung der Diedergruppe D_n, n ungerade, in Matrixschreibweise lautet $\varphi(1,x) = (1,2-x)$, $\varphi(-1,x) = (-1,x)$. Mit $a=b=1$ ist dies ein Spezialfall des vorherigen Beispiels.

Beispiel (STEVEN J. WINTERS [28]) Für jede ungerade Zahl $s > 2$ definiere die Permutation (Zyklenschreibweise)

$$\varphi = (0)(1,s-1)(2,s-2)\ldots(\frac{s-1}{2},\frac{s+1}{2})(s,s+1,\ldots,2s-1).$$

Dann ist φ eine anti-symmetrische Abbildung von D_s.

Beweis Die Matrixschreibweise dieser Permutation lautet

$$\varphi(e,x) = \begin{cases}(1,-x) & \text{falls } e=1\\ (-1,x+1) & \text{falls } e=-1.\end{cases}$$

Für $d = -1$ stimmt diese Permutation mit der von VERHOEFF gefundenen überein.

Beispiel Die elfstelligen Seriennummern der deutschen Banknoten werden mit der Permutation $\varphi = [1576283094] = [7046913258]^{-1}$ (vgl. Seite 100) gesichert [21]. Die Nummern enthalten an den Positionen 1,2 und 10 statt Ziffern Buchstaben. Diese werden vor der Prüfung gemäß folgender Tabelle umgesetzt:

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

Die Prüfgleichung lautet

$$\varphi(x_{10}) \cdot \varphi^2(x_9) \cdot \ldots \cdot \varphi^{10}(x_1) \cdot x_0 = 0.$$

Wäre die vorletzte Stelle der Seriennummer kein Buchstabe, sondern eine Ziffer, dann würde das Verfahren nicht alle Vertauschungen von x_0 mit x_1 erkennen. Aber durch den Buchstaben besteht keine Verwechslungsgefahr. Bei der benutzten Prüfgleichung ist nicht φ, sondern φ^{-1} eine anti-symmetrische Abbildung, da die Potenzen von φ aufsteigend gewählt wurden.

Für die Seriennummer DG2661778N1 eines 10-DM Scheines ergibt sich beispielsweise

Seriennummer	DG2661778N1
codierte Zahl	1226617785 1
$\varphi(x_{10}), \ldots, \varphi^{10}(x_1), x_0$	5016372799 1

Die Diedermultiplikation liefert $5 \cdot 0 \cdot 1 \cdot 6 \cdot 3 \cdot 7 \cdot 2 \cdot 7 \cdot 9 \cdot 9 \cdot 1 = 0$, d.h. die Seriennummer ist gültig.

Kapitel 4

Prüfziffersysteme über Quasigruppen

In diesem Kapitel verallgemeinern wir den Begriff des Prüfziffersystems auf Quasigruppen. Wir untersuchen verschiedene Ansätze und geben am Ende Prüfziffersysteme zu den Basen 6, 8 und 10 an, die eine bessere oder zumindest gleich gute Fehlererkennung bieten, wie Prüfziffersysteme basierend auf Gruppen. Außerdem zeigen wir, daß eine Reihe von Quasigruppen keine bessere Fehlererkennung bieten können als Prüfziffersysteme über Gruppen.

4.1 Allgemeine Ergebnisse

Wir stellen zuerst zwei Möglichkeiten vor, wie der Begriff „Prüfziffersystem" verallgemeinert werden kann.

Definition 9 *Sei* $D = \{0, \ldots, m-1\}$ *eine Menge von Ziffern,* $c \in D$ *und* $g : D^{n+1} \to D$ *eine Abbildung. Die Menge* $P_{g,c} := \{(d_n, \ldots, d_0) \in D^{n+1} | g(d_n, \ldots, d_0) = c\}$ *heißt* implizites Prüfziffersystem zur Basis m, *wenn gilt:*

1. $g(d_n, \ldots, d_i, \ldots, d_0) = g(d_n, \ldots, d'_i, \ldots, d_0) = c$ *impliziert* $d_i = d'_i$
2. $g(d_n, \ldots, d_i, d_{i-1}, \ldots, d_0) = g(d_n, \ldots, d_{i-1}, d_i, \ldots, d_0) = c$ *impliziert* $d_i = d_{i-1}$
3. *für alle* $d_n, \ldots, d_1 \in D$ *existiert ein* $d_0 \in D$ *s.d.* $g(d_n, \ldots, d_1, d_0) = c$

oder, vgl. H.P. Gumm [12]

Definition 10 *Sei* $D = \{0, \ldots, m-1\}$ *eine Menge von Ziffern und* $f : D^n \to D$ *eine Abbildung. Die Menge* $P'_f := \{(d_n, \ldots, d_0) \in D^{n+1} | f(d_n, \ldots, d_1) = d_0\}$ *heißt* explizites Prüfziffersystem zur Basis m, *wenn gilt:*

1. $f(d_n, \ldots, d_i, \ldots, d_1) = f(d_n, \ldots, d'_i, \ldots, d_1)$ *impliziert* $d_i = d'_i$

2. $f(d_n, \ldots, d_i, d_{i-1}, \ldots, d_1) = f(d_n, \ldots, d_{i-1}, d_i, \ldots, d_1)$ *impliziert* $d_i = d_{i-1}$

3. $f(d_n, \ldots, d_2, d_0) = d_1$, *wobei* $f(d_n, \ldots, d_1) = d_0$, *impliziert* $d_0 = d_1$

Bei den impliziten Prüfziffersystemen ist die Prüfziffer d_0 einer vorgegebenen Zahl $d_n d_{n-1} \ldots d_1$ die eindeutig bestimmte Lösung der Gleichung $g(d_n, \ldots, d_1, d_0) = c$. Dabei garantiert uns die dritte Eigenschaft, daß überhaupt eine Lösung existiert, mit der ersten Eigenschaft folgt deren Eindeutigkeit. Die zweite Eigenschaft sorgt für die Erkennung aller Nachbarvertauschungen.
Die expliziten Prüfziffersysteme haben den Vorteil, daß sich die Prüfziffer nicht als Lösung einer Gleichung ergibt, sondern daß diese direkt durch $f(d_n, \ldots, d_1)$ ausgerechnet werden kann. Die dritte Eigenschaft dient hier dazu, die Vertauschung der letzten Ziffer mit der Prüfziffer zu erkennen.
Beide Definitionen lassen es auch zu, eine Prüfziffer zu bestimmen, die in die ursprüngliche Zahl an einer Position i eingebaut wird. Dazu bestimmt man die eindeutige Lösung p der Gleichung

$$g(d_n, \ldots, d_{i+1}, p, d_i, \ldots, d_1) = c$$

bzw.

$$f(d_n, \ldots, d_{i+1}, p, d_i, \ldots, d_2) = d_1.$$

Die gesicherte Zahl lautet in beiden Fällen $d_n d_{n-1} \ldots d_{i+1} p d_i \ldots d_2 d_1$.

Die Definitionen sind im folgenden Sinne äquivalent: Zu jedem expliziten Prüfziffersystem P'_f erhält man ein implizites Prüfziffersystem $P_{g,c}$ mit der Eigenschaft $f(d_n, \ldots, d_1) = d_0 \Leftrightarrow g(d_n, \ldots, d_0) = c$ (und damit $P'_f = P_{g,c}$) durch die Definitionen $c := 0$ und

$$g(d_n, \ldots, d_0) := \begin{cases} 0 & \text{falls } f(d_n, \ldots, d_1) = d_0 \\ 1 & \text{sonst} \end{cases}$$

Und umgekehrt erhält man zu jedem impliziten Prüfziffersystem $P_{g,c}$ ein explizites Prüfziffersystem P'_f indem man $f(d_n, \ldots, d_1)$ durch die eindeutig bestimmte Lösung x der Gleichung $g(d_n, \ldots, d_1, x) = c$ definiert, also

$$f(d_n, \ldots, d_1) := x \Leftrightarrow g(d_n, \ldots, d_1, x) = c.$$

Schwieriger ist die Lösung des folgenden Problems: Wenn f eine bestimmte Darstellung (z.B. mit Quasigruppen) besitzt, gibt es dann auch ein g, das eine analoge Darstellung mit der Eigenschaft

$$f(d_n, \ldots, d_1) = d_0 \Leftrightarrow g(d_n, \ldots, d_0) = c \tag{4.1}$$

besitzt? Für das genannte Beispiel kann man die Fragestellung positiv beantworten, wie der folgende Satz zeigt:

Satz 30 *1. Zu jedem expliziten Prüfziffersystem P'_f, wobei f eine Darstellung mit $n-1$ Quasigruppen $*_i$ besitzt, $f(d_n,\ldots,d_1) = (\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-1} \ldots) *_2 d_1$, existiert eine Quasigruppe $*_1$ und ein $c \in D$, so daß 4.1 für $g(d_n,\ldots,d_0) := f(d_n,\ldots,d_1) *_1 d_0 = (\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-1} \ldots) *_1 d_0$ gilt.*

2. Zu jedem impliziten Prüfziffersystem $P_{g,c}$, wobei g eine Darstellung mit n Quasigruppen $*_i$ besitzt, $g(d_n,\ldots,d_0) = (\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-1} \ldots) *_1 d_0$, existiert eine Quasigruppe $*'_2$, so daß 4.1 für $f(d_n,\ldots,d_1) := ((\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-1} \ldots) *_3 d_2) *'_2 d_1$ gilt.

Beweis Mit $x *_1 y := x - y$ (Rechnung in der Gruppe $\mathbb{Z}_m$) und $c := 0$ folgt Behauptung 1. $*'_2$ wird durch die Bedingung $x *'_2 y = z \Leftrightarrow (x *_2 y) *_1 z = c$ definiert. Damit folgt Behauptung 2. (Das $*'_2$ eine Quasigruppe ist, folgt aus den Kürzungsregeln der Quasigruppen $*_2$ und $*_1$, siehe unten)

Sollen allerdings alle benutzten Quasigruppen gleich sein, so führen die unterschiedlichen Definitionen i.allg. auch zu unterschiedlichen Codewörtern:

Beispiel Seien $D := \{0,\ldots,6\}$, $f(x,y) := x - 2y$, $g(x,y,z) := (x-2y) - 2z$ und $c := 0$. Es gilt $f(5,2) = 1$, aber $g(5,2,1) = -1 \neq 0 = g(5,2,4)$, d.h. im ersten Fall ist 52-1, im zweiten Fall 52-4 die gesicherte Zahl.

4.2 n-Quasigruppen

Zunächst definieren wir einige Grundbegriffe.

Definition 11 *Eine Quasigruppe ist eine Algebra $(Q,*)$ mit der Eigenschaft, daß die Gleichungen $a * x = b$ und $y * a = b$ für jedes Paar a,b eine eindeutige Lösung x, bzw. y besitzen.*

Eine n-Quasigruppe ist eine Algebra (Q,f), $f : Q^n \to Q$, so daß für $i = 1,\ldots,n$ und alle $x_n,\ldots,x_{i+1},x_{i-1},\ldots,x_1,x_0 \in Q$ die Gleichung

$$f(x_n,\ldots,x_{i+1},x,x_{i-1},\ldots,x_1) = x_0$$

eine eindeutig bestimmte Lösung $x \in Q$ besitzt.

Bemerkung Die Quasigruppen sind ein Spezialfall der n-Quasigruppen. Sie werden daher im Zusammenhang mit n-Quasigruppen als binäre Quasigruppen bezeichnet.

Bekanntlich ist ein endlicher Gruppoid genau dann eine Quasigruppe, wenn in ihm die Kürzungsregeln $a * x = a * y \Rightarrow x = y$ und $x * a = y * a \Rightarrow x = y$ gelten.

Definition 12 *Zwei n-Quasigruppen f, g sind isotop, falls Permutationen α, $\beta_n, \ldots, \beta_1$ existieren mit*

$$\alpha(f(x_n, \ldots, x_1)) = g(\beta_n(x_n), \ldots, \beta_1(x_1)),$$

sie heißen isomorph, falls $\alpha = \beta_n = \ldots = \beta_1$ gilt.

Bemerkung Isotopie und Isomorphie definieren eine Äquivalenzrelation auf der Menge der n-Quasigruppen.

Definition 13 *Die* Parastrophie f_α *einer n-Quasigruppe f und der Permutation $\alpha \in S_{n+1}$ wird definiert durch*

$$f(x_n, \ldots, x_1) = x_0 \quad \Leftrightarrow \quad f_\alpha(x_{\alpha(n)}, \ldots, x_{\alpha(n)}) = x_{\alpha(0)}.$$

Sie heißt hauptsächlich *wenn $\alpha(0) = 0$ ist.*

Offensichtlich sind die Parastrophien einer n-Quasigruppe wieder eine n-Quasigruppe. Für eine Quasigruppe $(Q, *)$ definieren wir speziell:

$$\begin{aligned} x *_t y = z \quad &\Leftrightarrow \quad y * x = z \\ x/y = z \quad &\Leftrightarrow \quad y = x * z \\ x\backslash y = z \quad &\Leftrightarrow \quad x = z * y \\ x/_t y = z \quad &\Leftrightarrow \quad x = y * z \\ x\backslash_t y = z \quad &\Leftrightarrow \quad y = z * x \end{aligned}$$

Es gilt $x/(x * y) = y$, $x * (x/y) = y$ und $(x * y)\backslash y = x$, $(x\backslash y) * y = x$.

Definition 14 *Die Quasigruppen $(Q, *)$ und $(Q, \cdot)$ heißen orthogonal, wenn die Paare $(x * y, x \cdot y)$ für alle $x, y \in Q$ paarweise verschieden sind. Eine Quasigruppe $(Q, *)$ heißt selbstorthogonal, wenn sie orthogonal zu $(Q, *_t)$ ist.*

Lemma 15 *Zwei endliche Quasigruppen $(Q, *)$ und $(Q, \cdot)$ der Ordnung m sind genau dann orthogonal, wenn für alle $a, b \in Q$ die Gleichungen $x * y = a$, $x \cdot y = b$ eine eindeutig bestimmte Lösung $x, y \in Q$ besitzen.*

Beweis Seien $(Q, *)$ und $(Q, \cdot)$ orthogonal, und es gelten die Gleichungen $x' * y' = x * y = a$, $x' \cdot y' = x \cdot y = b$. Dies ist äquivalent zur Gleichheit der Paare $(x' * y', x' \cdot y')$ und $(x * y, x \cdot y)$. Die Paare sind aber nach Voraussetzung genau dann gleich, wenn $x = x'$ und $y = y'$ gilt. Also ist die Lösung der Gleichungen eindeutig.

Wir müssen noch zeigen, daß die Gleichungen überhaupt eine Lösung besitzen. Da die Paare $(x * y, x \cdot y)$ alle verschieden sind, haben wir m^2 verschiedene Paare. Folglich muß es für jedes Paar (a, b) Elemente $x, y \in Q$ mit $(x * y, x \cdot y) = (a, b)$ geben. Die Rückrichtung folgt analog. □

Für die Verknüpfungstafel einer Quasigruppe ist der Begriff *lateinisches Quadrat* üblich. Lateinische Quadrate heißen orthogonal, wenn ihre zugehörigen Quasigruppen orthogonal sind. Die orthogonalen lateinischen Quadrate spielen im Zusammenhang mit den endlichen affinen Ebenen eine wichtige Rolle.

Beispiel 1. Die folgenden beiden Quasigruppen sind orthogonal.

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$\cdot$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\longrightarrow$

$(*,\cdot)$	0	1	2
0	(0,0)	(1,1)	(2,2)
1	(2,1)	(0,2)	(1,0)
2	(1,2)	(2,0)	(0,1)

2. Die folgende Quasigruppe ist selbstorthogonal.

$*$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	3	2	1	0
3	1	0	3	2

$*_t$	0	1	2	3
0	0	2	3	1
1	1	3	2	0
2	2	0	1	3
3	3	1	0	2

Orthogonale lateinische Quadrate wurden zuerst von EULER Ende des 18. Jahrhunderts untersucht. Für das Kreuzprodukt zweier orthogonaler lateinischer Quadrate benutzte er den Begriff „Griechisch-Lateinisches-Quadrat", da er für das eine Quadrat griechische und für das andere lateinische Buchstaben verwendete. Griechisch-Lateinische-Quadrate werden aus diesem Grund auch Euler-Quadrate genannt.

Definition 15 *Eine Quasigruppe* $(Q,*)$ *ist* anti-symmetrisch, *wenn* $x*y = y*x \Rightarrow x = y$ *gilt. Analog heißt eine* n*-Quasigruppe* anti-symmetrisch, *wenn*

$$f(x_n,\ldots,x_i,x_{i-1},\ldots,x_1) = f(x_n,\ldots,x_{i-1},x_i,\ldots,x_1) \Rightarrow x_i = x_{i-1}.$$

Definition 16 *Eine Permutation* φ *einer Quasigruppe* $(Q,*)$ *heißt anti-symmetrische bzw. vollständige Abbildung, falls gilt:*

$$\varphi(x) * y = \varphi(y) * x \qquad \Rightarrow \qquad x = y$$

bzw.

$$\varphi^{-1}(x) * x = \varphi^{-1}(y) * y \qquad \Rightarrow \qquad x = y.$$

Die Menge aller anti-symmetrischen bzw. vollständigen Abbildungen einer Quasigruppe werde mit $Ant(Q,*)$ *bzw.* $Com(Q,*)$ *bezeichnet.*

Bemerkung Die zweite Eigenschaft ist äquivalent zu

$$x * \varphi(x) = y * \varphi(y) \qquad \Rightarrow \qquad x = y.$$

Die Definition der vollständigen Abbildungen stimmt also mit der für Gruppen getroffenen Definition überein.

Definition 17 *Sei f eine n-Quasigruppe dann wird die n-Quasigruppe $\hat{f}$ definiert durch*

$$\hat{f}(x_n, \ldots, x_1) = x_0 \Leftrightarrow f(x_0, x_1, \ldots, x_{n-1}) = x_n$$

Wir zeigen nun den Zusammenhang zwischen n-Quasigruppen und Prüfziffersystemen.

Satz 31 *1. Jede n-Quasigruppe erkennt alle Einzelfehler. Wenn g eine anti-symmetrische n-Quasigruppe ist, so definiert $P_{g,c}$ ein implizites Prüfziffersystem für alle $c \in D$.*

2. P'_f ist ein explizites Prüfziffersystem genau dann, wenn $P'_{\hat{f}}$ ein explizites Prüfziffersystem ist.

3. P'_f ist genau dann ein explizites Prüfziffersystem, wenn f und $\hat{f}$ anti-symmetrische n-Quasigruppen sind.

Beweis 1) Folgt direkt aus den Definitionen.
2) Da $(\hat{\hat{f}}) = f$ gilt, reicht es, eine Richtung zu zeigen. Sei P'_f ein Prüfziffersystem. $\hat{f}$ ist eine n-Quasigruppe und erkennt daher alle Einzelfehler. Es gelte nun

$$\hat{f}(d_n, \ldots, d_i, d_{i-1}, \ldots, d_1) = d_0 = \hat{f}(d_n, \ldots, d_{i-1}, d_i, \ldots, d_1)$$

oder

$$\hat{f}(d_n, \ldots, d_1) = d_0, \hat{f}(d_n, \ldots, d_2, d_0) = d_1.$$

Es folgt

$$f(d_0, \ldots, d_{i-1}, d_i, \ldots, d_{n-1}) = d_n = f(d_0, \ldots, d_i, d_{i-1}, \ldots, d_{n-1}), \text{ falls } i < n$$

und

$$f(d_0, \ldots, d_{n-1}) = d_n,\ f(d_0, \ldots, d_{n-2}, d_n) = d_{n-1}, \text{ falls } i = n.$$

Mit den Eigenschaften von f folgt nun, daß $d_i = d_{i-1}$ ist. Also ist $P'_{\hat{f}}$ ein Prüfziffersystem.
3) Sei P'_f ein Prüfziffersystem. Aus 2) folgt, daß auch $P'_{\hat{f}}$ ein Prüfziffersystem ist

und damit f und $\hat{f}$ anti-symmetrische n-Quasigruppen sind. Sind umgekehrt f und $\hat{f}$ anti-symmetrische n-Quasigruppen so sind die Bedingungen 1 und 2 der Definition 10 (Seite 61) für f erfüllt. Bedingung 3 folgt aus der Anti-Symmetrie von $\hat{f}$:

$$\begin{aligned} & f(d_n,\ldots,d_2,d_1)=d_0, f(d_n,\ldots,d_2,d_0)=d_1 \\ \Leftrightarrow\ & \hat{f}(d_0,d_1,\ldots,d_{n-1})=\hat{f}(d_1,d_0,d_2,\ldots,d_{n-1}) \\ \Leftrightarrow\ & d_0=d_1. \end{aligned}$$

□

Lemma 16 *Sei (Q,f) eine anti-symmetrische n-Quasigruppe und φ,ψ Permutationen von Q, dann ist auch $(Q,\bar{f})$ mit*

$$\bar{f}(x_n,\ldots,x_1) := \psi^{-1}(f(\varphi(x_n),\ldots,\varphi(x_1)))$$

anti-symmetrisch.

Beweis Aus $\bar{f}(x_n,\ldots,x_{i-1},x_i,\ldots,x_1)=\bar{f}(x_n,\ldots,x_i,x_{i-1},\ldots,x_1)$ folgt

$$f(\varphi(x_n),\ldots,\varphi(x_i),\varphi(x_{i-1}),\ldots,\varphi(x_1))=f(\varphi(x_n),\ldots,\varphi(x_{i-1}),\varphi(x_i),\ldots,\varphi(x_1)).$$

Da (Q,f) anti-symmetrisch ist, folgt $\varphi(x_i)=\varphi(x_{i-1})$ und damit $x_i=x_{i-1}$. □

Der folgende Satz stellt einen Zusammenhang zwischen anti-symmetrischen Abbildungen und anti-symmetrischen Quasigruppen her:

Satz 32 *Eine Quasigruppe, und insbesondere eine Gruppe, besitzt eine anti-symmetrische Abbildung genau dann, wenn sie isotop zu einer anti-symmetrischen Quasigruppe ist.*

Beweis Die Quasigruppe $(Q,\cdot)$ besitze die anti-symmetrische Abbildung φ, dann ist $(Q,*)$ mit $x*y := \varphi(x)\cdot y$ eine anti-symmetrische Quasigruppe. Sei umgekehrt die anti-symmetrische Quasigruppe $(Q,*)$ isotop zur Quasigruppe $(Q,\cdot)$, also $\gamma(x*y)=\alpha(x)\cdot\beta(y)$ mit den Permutationen α,β,γ. Die Quasigruppe $x\bullet y := \gamma(\beta^{-1}(x)*\beta^{-1}(y))$ ist wieder anti-symmetrisch (Lemma 16 für $n=2$). Es folgt, daß $\alpha\circ\beta^{-1}$ eine anti-symmetrische Abbildung von $(Q,\cdot)$ ist, denn

$$\begin{aligned} x\bullet y &= \gamma(\beta^{-1}(x)*\beta^{-1}(y)) \\ &= \gamma(\gamma^{-1}(\alpha(\beta^{-1}(x))\cdot\beta(\beta^{-1}(y)))) \\ &= \alpha\circ\beta^{-1}(x)\cdot y \\ &= \alpha\circ\beta^{-1}(y)\cdot x \\ &= y\bullet x \end{aligned}$$

ist nur erfüllt wenn $x = y$ ist. □

Satz 33 *In einer Isotopieklasse besitzt entweder jede oder keine Quasigruppe eine anti-symmetrische bzw. vollständige Abbildung.*

Beweis Aus dem vorherigen Satz folgt, daß jede Quasigruppe, die isotop ist zu einer Quasigruppe mit anti-symmetrischer Abbildung, ebenfalls eine anti-symmetrische Abbildung besitzt.

Sei $(Q, *)$ eine Quasigruppe mit vollständiger Abbildung φ^{-1} und $(Q, \cdot)$ mit $x \cdot y = \gamma^{-1}(\alpha(x) * \beta(y))$ sei isotop zu $(Q, *)$, dann ist $\tilde{\varphi}^{-1} := \alpha^{-1} \circ \varphi^{-1} \circ \beta$ eine vollständige Abbildung von $(Q, \cdot)$: Aus

$$\tilde{\varphi}(x) \cdot x = \gamma^{-1}(\alpha(\tilde{\varphi}(x)) * \beta(x)) = \gamma^{-1}(\alpha(\tilde{\varphi}(y)) * \beta(y)) = \tilde{\varphi}(y) \cdot y$$

folgt

$$\varphi^{-1}(\beta(x)) * \beta(x) = \varphi^{-1}(\beta(y)) * \beta(y).$$

φ^{-1} ist eine vollständige Abbildung von $(Q, *)$, also folgt $\beta(x) = \beta(y)$ und damit $x = y$. □

Definition 18 *Eine Quasigruppe besitzt die* Transversale (φ_1, φ_2)*, wenn* φ_1, φ_2 *und* $\varphi_1(x) * \varphi_2(x)$ *Permutationen sind.*

Lemma 17 *Eine Quasigruppe besitzt eine vollständige Abbildung genau dann, wenn sie eine Transversale besitzt.*

Beweis Ist (φ_1, φ_2) eine Transversale, so ist $\varphi_2 \circ \varphi_1^{-1}$ eine vollständige Abbildung. Andererseits erhalten wir durch die vollständige Abbildung φ die Transversale (Id, φ). □

Wenn die Quasigruppe $(Q, *)$ die anti-symmetrische bzw. vollständige Abbildung φ besitzt, dann ist φ^{-1} eine anti-symmetrische bzw. vollständige Abbildung der Parastrophie $(Q, *_t)$. Für vollständige Abbildungen gilt außerdem:

Lemma 18 *(vgl.* Belousov [4]*) Besitzt die Quasigruppe* $(Q, *)$ *eine vollständige Abbildung, dann gilt dies auch für jede Parastrophie von* $(Q, *)$*.*

Beweis Wir zeigen die Behauptung mit Lemma 17. $(Q, *)$ besitze die Transversale (φ_1, φ_2). Wir definieren die Permutation φ_3 durch $\varphi_3(x) := \varphi_1(x) * \varphi_2(x)$. Damit ist (φ_1, φ_3) eine Transversale der Parastrophie $(Q, /)$, denn $\varphi_1(x)/\varphi_3(x) = \varphi_1(x)/(\varphi_1(x) * \varphi_2(x)) = \varphi_2(x)$ ist eine Permutation. Die Behauptung für die anderen Parastrophien folgt analog. □

4.3 Reduzible n-Quasigruppen

In diesem Abschnitt geben wir ein Kriterium an, mit dem wir entscheiden können, ob eine n-Quasigruppe eine Darstellung mit binären Quasigruppen hat.

Definition 19 *(vgl. [6]) Eine n-Quasigruppe (Q, f), $n > 2$ heißt reduzibel wenn eine Permutation $\alpha \in S_n$ und Quasigruppen $g : Q^{n-k+1} \to Q$, $h : Q^k \to Q$ $(1 \leq k < n-1)$ existieren mit*

$$x_0 = f(x_n, \ldots, x_1) = g(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, h(x_{\alpha_k}, \ldots, x_{\alpha_1})).$$

Sie heißt total reduzibel wenn $n-1$ binäre Quasigruppen (Q, g_i), $i = 1, \ldots, n-1$ existieren, so daß f als Komposition der g_i dargestellt werden kann. Eine n-Quasigruppe heißt irreduzibel wenn sie nicht reduzibel ist.

Theorem 11 *(Verhoeff [27]) Es existieren irreduzible n-Quasigruppen.*

Man könnte vermuten, daß die Anti-Symmetrie-Eigenschaft verhindert, daß eine n-Quasigruppe irreduzibel ist. Dies ist allerdings nicht der Fall, wie folgendes Theorem zeigt:

Theorem 12 *Es existieren irreduzible anti-symmetrische n-Quasigruppen.*

Beweis Die folgende 3-Quasigruppe f ist irreduzibel und anti-symmetrisch:

$k =$	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5
j=0	0 1 2 3 4 5	1 2 0 5 3 4	2 0 1 4 5 3	3 4 5 1 2 0	4 5 3 0 1 2	5 3 4 2 0 1
1	2 0 1 4 5 3	0 1 2 3 4 5	1 2 0 5 3 4	5 3 4 2 0 1	3 4 5 1 2 0	4 5 3 0 1 2
2	1 2 0 5 3 4	2 0 1 4 5 3	0 1 2 3 4 5	4 5 3 0 1 2	5 3 4 2 0 1	3 4 5 1 2 0
3	4 5 3 0 1 2	3 4 5 1 2 0	5 3 4 2 0 1	0 1 2 4 5 3	2 0 1 5 3 4	1 2 0 3 4 5
4	5 3 4 2 0 1	4 5 3 0 1 2	3 4 5 1 2 0	1 2 0 3 4 5	0 1 2 4 5 3	2 0 1 5 3 4
5	3 4 5 1 2 0	5 3 4 2 0 1	4 5 3 0 1 2	2 0 1 5 3 4	1 2 0 3 4 5	0 1 2 4 5 3
	i=0	1	2	3	4	5

Wenn $f(i,j,k)$ zerlegbar wäre in $g(i,j)$ und $h(i,j)$, dann würde gelten

1. $f(i,j,k) = g(i, h(j,k))$ oder
2. $f(i,j,k) = g(j, h(i,k))$ oder
3. $f(i,j,k) = g(k, h(i,j))$.

Im ersten Fall folgt aus $f(i,j,k) = f(i,j',k')$, daß $h(j,k) = h(j',k')$ und folglich, daß $f(i',j,k) = f(i',j',k')$. Es gilt aber $f(0,0,0) = f(0,3,3) = 0$ und $f(3,0,0) = 3 \neq 4 = f(3,3,3)$. Analog folgt im zweiten bzw. dritten Fall, daß $f(i,j,k) =$

$f(i',j,k') \Rightarrow f(i,j',k) = f(i',j',k')$ bzw. $f(i,j,k) = f(i',j',k) \Rightarrow f(i,j,k') = f(i',j',k')$. Es gilt aber $f(0,0,0) = f(1,0,2) = 0$, $f(0,3,0) = 4 \neq 5 = f(1,3,2)$ und $f(0,0,0) = f(3,3,0) = 0$, $f(0,0,3) = 3 \neq 4 = f(3,3,3)$.

Daß diese 3-Quasigruppe die Vertauschungen $j \leftrightarrow k$ erkennt, läßt sich leicht an den anti-symmetrischen Quasigruppen $f(0,j,k), \ldots, f(5,j,k)$ ablesen. Wenn wir eine andere Projektionsebene wählen, dann sieht man ebenso, daß auch die Quasigruppen $f(i,j,0), \ldots, f(i,j,5)$ anti-symmetrisch sind.

$i=$	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5
j=0	0 1 2 3 4 5	1 2 0 4 5 3	2 0 1 5 3 4	3 5 4 1 0 2	4 3 5 2 1 0	5 4 3 0 2 1
1	2 0 1 5 3 4	0 1 2 3 4 5	1 2 0 4 5 3	4 3 5 2 1 0	5 4 3 0 2 1	3 5 4 1 0 2
2	1 2 0 4 5 3	2 0 1 5 3 4	0 1 2 3 4 5	5 4 3 0 2 1	3 5 4 1 0 2	4 3 5 2 1 0
3	4 3 5 0 2 1	5 4 3 1 0 2	3 5 4 2 1 0	0 1 2 4 5 3	1 2 0 5 3 4	2 0 1 3 4 5
4	5 4 3 1 0 2	3 5 4 2 1 0	4 3 5 0 2 1	2 0 1 3 4 5	0 1 2 4 5 3	1 2 0 5 3 4
5	3 5 4 2 1 0	4 3 5 0 2 1	5 4 3 1 0 2	1 2 0 5 3 4	2 0 1 3 4 5	0 1 2 4 5 3
	k=0	1	2	3	4	5

Damit ist f eine irreduzible anti-symmetrische 3-Quasigruppe. □

Verhoeff [27] gab ein Beispiel für eine irreduzible 3-Quasigruppen bereits für $m = 4$ an. Diese definiert aber kein Prüfziffersystem, da sie nicht anti-symmetrisch ist.

Eine interessante Anwendungsmöglichkeit der irreduziblen n-Quasigruppen ergibt sich aus der Tatsache, daß man mit einer kleinen Anzahl gesicherter Zahlen nicht auf das verwendete Prüfziffersystem schließen kann. Damit kann man verhindern, daß absichtlich falsche Zahlen (z.B. Kreditkartennummern) mit gültiger Prüfziffer eingegeben werden.

Im folgenden beschäftigen wir uns mit reduziblen n-Quasigruppen.

Satz 34 *Wenn das explizite Prüfziffersystem P'_f auf der (total) reduziblen n-Quasigruppe f beruht, dann existiert ein äquivalentes implizites Prüfziffersystem $P_{g,c}$, bei dem g eine (total) reduzible $n+1$-Quasigruppe ist. Die Umkehrung gilt im allgemeinen nicht.*

Beweis Wir definieren

$$g(d_n, \ldots, d_1, d_0) := f(d_n, \ldots, d_1) - d_0$$

und $c = 0$. Damit folgt der erste Teil der Behauptung. Sei nun P'_f ein explizites Prüfziffersystem und f eine irreduzible n-Quasigruppe. Dann ist g eine, offensichtlich reduzible, $n+1$-Quasigruppe. Wenn eine n-Quasigruppe $\tilde{f}$ mit

$$\tilde{f}(d_n, \ldots, d_1) = d_0 \Leftrightarrow g(d_n, \ldots, d_0) = 0$$

existiert, dann folgt, daß $\tilde{f}(d_n, \ldots, d_1) = d_0 = f(d_n, \ldots, d_1)$ und damit $f = \tilde{f}$ gilt. Also ist $\tilde{f}$ irreduzibel und es existiert kein reduzibles explizites Prüfziffersystem, das äquivalent zu $P_{g,c}$ ist. □

Theorem 13 *Sei f eine n-Quasigruppe über der Menge Q und $c_{n-2}, \ldots, c_1 \in Q$ beliebige, aber fest gewählte Konstanten. Es gibt Quasigruppen $*_i$, $i = 2, \ldots, n$ mit*

$$f(x_n, \ldots, x_1) = (\ldots((x_n *_n x_{n-1}) *_{n-1} x_{n-2}) *_{n-1} \ldots) *_2 x_1,$$

genau dann, wenn für $i = 1, \ldots, n-2$ gilt

$$\begin{aligned} f(x_n, \ldots, x_{i+1}, c_i, c_{i-1}, \ldots, c_1) &= f(x'_n, \ldots, x'_{i+1}, c_i, c_{i-1}, \ldots, c_1) \\ \Rightarrow f(x_n, \ldots, x_{i+1}, x, c_{i-1}, \ldots, c_1) &= f(x'_n, \ldots, x'_{i+1}, x, c_{i-1}, \ldots, c_1) \end{aligned}$$

Beweis Es gelte $f(x_n, \ldots, x_1) = (\ldots((x_n *_n x_{n-1}) *_{n-1} x_{n-2}) *_{n-1} \ldots) *_2 x_1$ für die Quasigruppen $*_i$. Aus

$$f(x_n, \ldots, x_{i+1}, c_i, c_{i-1}, \ldots, c_1) = f(x'_n, \ldots, x'_{i+1}, c_i, c_{i-1}, \ldots, c_1)$$

folgt mit Hilfe der Kürzungsregel für die Quasigruppen $*_j$, $j = 2, \ldots, i+1$

$$(\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_{i+2} x_{i+1} = (\ldots(x'_n *_n x'_{n-1}) *_{n-1} \ldots) *_{i+2} x'_{i+1}$$

und damit

$$\begin{aligned} f(x_n, .., x_{i+1}, x, c_{i-1}, .., c_1) &= (..((..(x_n *_n x_{n-1}) *_{n-1} ..) *_{i+1} x) *_i c_{i-1}..) *_2 c_1 \\ &= (..((..(x'_n *_n x'_{n-1}) *_{n-1} ..) *_{i+1} x) *_i c_{i-1}..) *_2 c_1 \\ &= f(x'_n, .., x'_{i+1}, x, c_{i-1}, .., c_1). \end{aligned}$$

Für die Rückrichtung definieren wir die Quasigruppen $*_i$, $i = 2, \ldots, n-1$ folgendermaßen:

$$x *_i y := f(x_n, \ldots, x_i, y, c_{i-2}, \ldots, c_1), \text{ falls } f(x_n, \ldots, x_i, c_{i-1}, c_{i-2}, \ldots, c_1) = x,$$

und

$$x *_n y := f(x, y, c_{n-2}, \ldots, c_1).$$

Die $*_i$ sind wohldefiniert, weil die Gleichung $f(0, \ldots, 0, y, c_{i-1}, c_{i-2}, \ldots, c_1) = x$ eine Lösung y besitzt und weil aus

$$f(x_n, \ldots, x_i, c_{i-1}, c_{i-2}, \ldots, c_1) = x = f(x'_n, \ldots, x'_i, c_{i-1}, c_{i-2}, \ldots, c_1)$$

folgt, daß $f(x_n, \ldots, x_i, y, c_{i-2}, \ldots, c_1) = f(x'_n, \ldots, x'_i, y, c_{i-2}, \ldots, c_1)$ ist. Außerdem gilt:

$$\begin{aligned} f(x_n, \ldots, x_1) &= f(x_n, \ldots, x_2, c_1) *_2 x_1 \\ &= (f(x_n, \ldots, x_3, c_2, c_1) *_3 x_2) *_2 x_1 \\ &\vdots \\ &= (\ldots(f(x_n, x_{n-1}, c_{n-2}, \ldots, c_1) *_{n-1} x_{n-2}) *_{n-1} \ldots) *_2 x_1 \\ &= (\ldots((x_n *_n x_{n-1}) *_{n-1} x_{n-2}) *_{n-1} \ldots) *_2 x_1 \end{aligned}$$

□

Ist f auf diese Weise zerlegbar, dann gilt sogar für beliebige x_j, x'_j

$$\begin{aligned} f(x_n, \ldots, x_{i+1}, x_i, x_{i-1}, \ldots, x_1) &= f(x'_n, \ldots, x'_{i+1}, x_i, x_{i-1}, \ldots, x_1) \\ \Rightarrow f(x_n, \ldots, x_{i+1}, x'_i, x_{i-1}, \ldots, x_1) &= f(x'_n, \ldots, x'_{i+1}, x'_i, x_{i-1}, \ldots, x_1) \end{aligned}$$

und die Voraussetzungen des Theorems sind für verschiedene Konstanten c_j erfüllt. Für verschiedene $c_1 \neq c'_1$ sind aber die Quasigruppen $x *_n y := f(x, y, c_{n-2}, \ldots, c_1)$ und $x *'_n y := f(x, y, c_{n-2}, \ldots, c'_1)$ verschieden, denn aus $x *_n y = x *'_n y$ folgt, da f eine n-Quasigruppe ist, $c_1 = c'_1$. Wir sehen also, daß für f unterschiedliche Darstellungen existieren.

Theorem 14 *(*Belousov [6]*) Eine n-Quasigruppe f ist reduzibel genau dann, wenn folgende Abschlußbedingung für eine hauptsächliche Parastrophie f_α erfüllt ist ($1 < k < n$):*

$$\begin{aligned} f_\alpha(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, x_{\alpha_k}, \ldots, x_{\alpha_1}) &= f_\alpha(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, y_{\alpha_k}, \ldots, y_{\alpha_1}) \\ \Rightarrow f_\alpha(x'_{\alpha_n}, \ldots, x'_{\alpha_{k+1}}, x_{\alpha_k}, \ldots, x_{\alpha_1}) &= f_\alpha(x'_{\alpha_n}, \ldots, x'_{\alpha_{k+1}}, y_{\alpha_k}, \ldots, y_{\alpha_1}) \end{aligned}$$

Den folgenden Beweis dieser Aussage haben wir unabhängig von Belousov gefunden.

Beweis Sei f reduzibel, also

$$f(x_n, \ldots, x_1) = g(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, h(x_{\alpha_k}, \ldots, x_{\alpha_1})).$$

Aus

$$\begin{aligned} f(x_n, \ldots, x_1) &= f_\alpha(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, x_{\alpha_k}, \ldots, x_{\alpha_1}) \\ &= g(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, h(x_{\alpha_k}, \ldots, x_{\alpha_1})) \\ &= g(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, h(y_{\alpha_k}, \ldots, y_{\alpha_1})) \\ &= f_\alpha(x_{\alpha_n}, \ldots, x_{\alpha_{k+1}}, y_{\alpha_k}, \ldots, y_{\alpha_1}) \end{aligned}$$

folgt $h(x_{\alpha_k},\ldots,x_{\alpha_1}) = h(y_{\alpha_k},\ldots,y_{\alpha_1})$ und damit

$$\begin{aligned} f_\alpha(x'_{\alpha_n},\ldots,x'_{\alpha_{k+1}},x_{\alpha_k},\ldots,x_{\alpha_1}) &= g(x'_{\alpha_n},\ldots,x'_{\alpha_{k+1}},h(x_{\alpha_k},\ldots,x_{\alpha_1})) \\ &= g(x'_{\alpha_n},\ldots,x'_{\alpha_{k+1}},h(y_{\alpha_k},\ldots,y_{\alpha_1})) \\ &= f_\alpha(x'_{\alpha_n},\ldots,x'_{\alpha_{k+1}},y_{\alpha_k},\ldots,y_{\alpha_1}) \end{aligned}$$

Es gelte nun die Abschlußbedingung für die n-Quasigruppe f und die Permutation α, $1 \le k < n$. Wir definieren die beiden Abbildungen g und h durch:

$$\begin{aligned} h(x_{\alpha_k},\ldots,x_{\alpha_1}) &:= f_\alpha(0,\ldots,0,x_{\alpha_k},\ldots,x_{\alpha_1}) \\ \text{und}\quad g(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},y) &:= f_\alpha(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},x_{\alpha_k},\ldots,x_{\alpha_1}), \\ &\quad \text{falls } h(x_{\alpha_k},\ldots,x_{\alpha_1}) = y. \end{aligned}$$

Die $(n-k+1)$-Quasigruppe g ist wohldefiniert, weil die Gleichung $h(0,\ldots,0,x) = y$ für jedes y eine eindeutig bestimmte Lösung x besitzt (h ist eine k-Quasigruppe), und außerdem folgt, falls $h(x_{\alpha_k},\ldots,x_{\alpha_1}) = h(x'_{\alpha_k},\ldots,x'_{\alpha_1}) = y$, d.h.

$$f_\alpha(0,\ldots,0,x_{\alpha_k},\ldots,x_{\alpha_1}) = f_\alpha(0,\ldots,0,x'_{\alpha_k},\ldots,x'_{\alpha_1}),$$

daß

$$\begin{aligned} f_\alpha(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},x_{\alpha_k},\ldots,x_{\alpha_1}) &= g(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},y) \\ &= f_\alpha(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},x'_{\alpha_k},\ldots,x'_{\alpha_1}) \end{aligned}$$

gilt. Aus der Definition von g und h folgt nun

$$\begin{aligned} f(x_n,\ldots,x_1) &= f_\alpha(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},x_{\alpha_k},\ldots,x_{\alpha_1}) \\ &= g(x_{\alpha_n},\ldots,x_{\alpha_{k+1}},h(x_{\alpha_k},\ldots,x_{\alpha_1})). \end{aligned}$$

Also ist f reduzibel. □

Bemerkung Anstatt der $0 \in Q$ können wir, wie im vorhergehenden Theorem, verschiedene Konstanten $c_n,\ldots,c_{k+1} \in Q$ benutzen, um die Abbildungen g und h zu definieren.

4.4 Existenz von Prüfziffersystemen

Die Existenz von Prüfziffersystemen für beliebige Basen größer 2 wurde von H.P. Gumm [12] 1985 bewiesen.

Theorem 15 *(H.P. Gumm) Für jede Basis $m > 2$ und alle $n \ge 2$ existiert eine Abbildung $f : D^n \to D$ bzw. $g : D^{n+1} \to D$, so daß P'_f bzw. $P_{g,0}$ ein Prüfziffersystem definiert.*

Beweis Wir können den Beweis durch die in Kapitel 2 aufgebaute Theorie etwas verkürzen. Ist m ungerade, dann besitzt $\mathbb{Z}_m$ die anti-symmetrische Abbildung $\tau(x) := -x$. Ist $m = 2k$ gerade, dann wissen wir, daß die Diedergruppe D_k (neutrales Element '0') mit m Elementen eine anti-symmetrische Abbildung τ besitzt. In beiden Fällen definiert daher die Gleichung

$$f(x_n, x_{n-1}, \ldots, x_2, x_1) := [\tau^n(x_n)\tau^{n-1}(x_{n-1}) \ldots \tau^2(x_2)\tau(x_1)]^{-1} = x_0$$

bzw.

$$g(x_n, x_{n-1}, \ldots, x_1, x_0) := \tau^n(x_n)\tau^{n-1}(x_{n-1}) \ldots \tau^2(x_2)\tau(x_1)x_0 = 0$$

ein Prüfziffersystem zur Basis m. □

Korollar 15 *Für alle $n \geq 2$ und für alle $m > 2$ existiert eine anti-symmetrische n-Quasigruppe zur Basis m.*

Zur Basis 2 existiert kein Prüfziffersystem (und damit auch keine anti-symmetrische n-Quasigruppe), denn den Zahlen 00, 01 und 10 müßten verschiedene Prüfziffern aus der Menge $\{0, 1\}$ zugeordnet werden, was unmöglich ist.

Eine weitere Möglichkeit ein Prüfziffersystem zur Basis p^m, wobei p eine Primzahl ist, zu definieren, bietet der Galois-Körper mit p^m Elementen. Mit der gewichteten Summe $\sum_{i=0}^{n} a_i x_i = 0$ erhalten wir ein Prüfziffersystem, falls $a_i \neq 0$ und benachbarte Gewichte verschieden sind. Auch hier sehen wir, daß der Fall $p = 2$ ausgeschlossen ist, da wir nur $a_i = 1$ wählen können und damit benachbarte Gewichte gleich sind.

Des weiteren ist erwähnenswert, daß wir aus zwei Prüfziffersystemen zu den Basen m_1 und m_2 auf natürliche Weise ein Prüfziffersystem zur Basis $m_1 \cdot m_2$ erhalten, indem wir jede Zahl der Basis $m_1 \cdot m_2$ als eindeutiges Paar (d_1, d_2) darstellen, wobei d_1 eine Ziffer der Basis m_1 und d_2 eine Ziffer der Basis m_2 ist. Danach berechnen wir die Prüfziffern p_1 und p_2 getrennt für jede Komponente und wandeln das Paar (p_1, p_2) zurück in die zugehörige Zahl der Basis $m_1 \cdot m_2$. Es ist leicht einzusehen, daß die Eigenschaften 1–3 der Definitionen 9 und 10 (Seite 61) sowohl bei den impliziten als auch bei expliziten Prüfziffersystemen erhalten bleiben.

4.5 Prüfziffersysteme über Quasigruppen

In diesem Abschnitt untersuchen wir die total reduziblen Prüfziffersysteme der Form

$$g(x_n, x_{n-1}, \ldots, x_0) = (\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_1 x_0 = d$$

mit den (endlichen) Quasigruppen $(Q, *_i)$, $i = 1, \ldots, n$, und $d \in Q$. Wir benutzen die implizite Form, weil dadurch die Bedingungen für die Fehlererkennung einfacher formuliert werden können. Für die einzelnen Fehlerarten stellen wir die Anforderungen an die benutzten Quasigruppen zusammen. Zunächst zeigen wir, daß durch eine solche Prüfgleichung alle Einzelfehler erkannt werden können. Es gelte

$$(\ldots((\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_{i+1} x_i)\ldots) *_1 x_0 = d$$

und

$$(\ldots((\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_{i+1} x_i')\ldots) *_1 x_0 = d.$$

Wir setzen $c := (\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_{i+2} x_{i+1}$ und kürzen die Elemente $x_{i-1}, \ldots, x_0$ auf der rechten Seite. Es folgt

$$c *_i x_i = c *_i x_i'$$

und durch Kürzen von c erhalten wir $x_i = x_i'$.

Da $d \in Q$ beliebig gewählt werden kann, haben wir damit auch die Injektivität, und weil Q endlich ist, auch die Surjektiviät der Translationen $x \mapsto g(x_n, \ldots, x_{i+1}, x, x_{i-1}, \ldots, x_0)$ für alle i gezeigt. Folglich definiert g eine $(n+1)$-Quasigruppe über der Menge Q.

Die Transposition benachbarter Elemente wird genau dann erkannt, wenn die folgenden Implikationen für alle i und alle $c, x, y \in Q$ gelten:

$$\begin{aligned} x *_n y = y *_n x \quad &\Rightarrow \quad x = y \\ (c *_{i+1} x) *_i y = (c *_{i+1} y) *_i x \quad &\Rightarrow \quad x = y. \end{aligned} \tag{4.2}$$

Diese Aussage wird genauso gezeigt, wie die Aussage zur Erkennung der Einzelfehler. Zunächst werden die gleichen Elemente auf der rechten Seite gekürzt, dann werden die gleichen Elemente auf der linken Seite zu c zusammengefaßt.

Wir haben damit den folgenden Satz bewiesen:

Satz 35 *Mit den Quasigruppen $(Q, *_i)$ wird durch*

$$g(x_n, x_{n-1}, \ldots, x_0) := (\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_1 x_0$$

genau dann eine anti-symmetrische $(n+1)$-Quasigruppe definiert, wenn $*_n$ anti-symmetrisch ist und jede Zeile der Quasigruppe $*_{i+1}$ eine anti-symmetrisch Abbildung der Quasigruppe $*_i$ ist.

Die anderen Fehlerarten benötigen weitere Voraussetzungen, die für alle i und für alle $x, y, z, c \in Q$ erfüllt sein müssen.

Sprungtranspositionen:

$$\begin{aligned}(x *_n z) *_{n-1} y &= (y *_n z) *_{n-1} x \quad \Rightarrow \quad x = y \\ ((c *_{i+1} x) *_i z) *_{i-1} y &= ((c *_{i+1} y) *_i z) *_{i-1} x \quad \Rightarrow \quad x = y.\end{aligned}$$

Zwillingsfehler:

$$\begin{aligned}x *_n x &= y *_n y \quad \Rightarrow \quad x = y \\ (c *_{i+1} x) *_i x &= (c *_{i+1} y) *_i y \quad \Rightarrow \quad x = y.\end{aligned}$$

Sprungzwillingsfehler:

$$\begin{aligned}(x *_n z) *_{n-1} x &= (y *_n z) *_{n-1} y \quad \Rightarrow \quad x = y \\ ((c *_{i+1} x) *_i z) *_{i-1} x &= ((c *_{i+1} y) *_i z) *_{i-1} y \quad \Rightarrow \quad x = y.\end{aligned}$$

Im Vergleich zu den Prüfziffersystemen über Gruppen müssen wir also eine Vielzahl verschiedener Bedingungen überprüfen. Eine Verbesserung dieser Situation wäre erreichbar, wenn wir jeweils bei der zweiten Voraussetzung umklammern könnten. Dann wäre es möglich, das Element c ebenfalls zu kürzen. Diesen Gedanken werden wir im Abschnitt „Verallgemeinerte Assoziativität" ausführen. Zunächst zeigen wir jedoch einige wichtige Eigenschaften einer Quasigruppe in einem Prüfziffersystem.

Satz 36 *Jede Quasigruppe in einem Prüfziffersystem besitzt eine anti-symmetrische Abbildung. Erkennt das Prüfziffersystem alle Zwillingsfehler, dann besitzt jede Quasigruppe eine vollständige Abbildung, erkennt es alle Sprungzwillingsfehler, dann besitzt jede Quasigruppe außer ggf. $*_n$ eine vollständige Abbildung.*

Beweis Sei $*_i$ eine Quasigruppe eines Prüfziffersystems über Quasigruppen, d.h. sie erfüllt die Bedingung 4.2. Ist $i = n$, dann ist $*_n$ anti-symmetrisch und die Identität ist eine anti-symmetrische Abbildung. Für $*_i$, $i < n$, definieren wir $\varphi(x) := c *_{i+1} x$ für eine beliebige Konstante c. Damit ist $\varphi(x) *_i y = \varphi(y) *_i x$ äquivalent zur zweiten Bedingung von 4.2 und φ ist eine anti-symmetrische Abbildung von $*_i$.

Erkennt das Prüfziffersystem alle Zwillingsfehler, dann ist die Identität eine vollständige Abbildung von $*_n$ und φ mit $\varphi^{-1}(x) := c *_{i+1} x$ eine vollständige Abbildung von $*_i$, $i < n$. Falls das Prüfziffersystem alle Sprungzwillingsfehler erkennt, dann ist für fest gewählte $c, z \in Q$ die Permutation φ mit $\varphi^{-1}(x) := x *_n *z$ Element von $Com(Q, *_{n-1})$ und die Permutation φ mit $\varphi^{-1}(x) := (c *_{i+1} x) *_i z$ ist Element von $Com(Q, *_{i-1})$, $i < n$. □

Zusammen mit Satz 33 (Seite 68) sehen wir, daß viele Quasigruppen ungeeignet sind, ein Prüfziffersystem zu definieren, das alle (Sprung-)Zwillingsfehler erkennt.

Insbesondere eignen sich die Isotopien einer Gruppe ohne anti-symmetrische oder vollständige Abbildung nicht. Speziell für den Fall $m = 10$ bedeutet dies, daß wir kein Prüfziffersystem finden werden, das alle (Sprung-)Zwillingsfehler erkennt und in dem Quasigruppen vorkommen, die zu einer Gruppe isotop sind.

Da wir bereits gezeigt haben, daß $\mathbb{Z}_{2k}$ keine anti-symmetrische und jede Gruppe der Ordnung $2k$ für ungerades k keine vollständige Abbildung besitzt, erhalten wir das Korollar:

Korollar 16 *In einem Prüfziffersystem über Quasigruppen der Ordnung $2k$ ist keine Quasigruppe zur Gruppe $\mathbb{Z}_{2k}$ isotop. Erkennt das Prüfziffersystem alle Zwillings- oder alle Sprungzwillingsfehler und ist k ungerade, dann ist keine Quasigruppe isotop zu einer Gruppe der Ordnung $2k$.*

Der im Abschnitt „Quasigruppen isotop zu einer Gruppe" beschriebene Ansatz ist daher hauptsächlich für andere Ordnungen von Interesse.

Wir zeigen nun einen interessanten Zusammenhang zwischen Prüfziffersystemen über Quasigruppen und orthogonalen lateinischen Quadraten.

Satz 37 *Seien $(Q, *_i)$ die Quasigruppen eines Prüfziffersystems, das alle Zwillingsfehler erkennt, dann ist die Quasigruppe $(Q, *_i)$, $i = 1, \ldots, n-1$, orthogonal zu der durch*

$$x *'_i y = z \quad :\Leftrightarrow \quad z *_{i+1} y = x$$

definierten.

Beweis Wir müssen zeigen, daß die Gleichungen $x *_i y = a$ und $x *'_i y = b$ für alle $a, b \in Q$ eine Lösung besitzen. Die zweite Gleichung ist äquivalent zu $b *_{i+1} y = x$. Wir setzen diese in die erste Gleichung ein und erhalten die Bedingung, daß $(b *_{i+1} y) *_i y = a$ für alle $a, b \in Q$ eine Lösung besitzt. Weil das Prüfziffersystem alle Zwillingsfehler erkennt, ist $\varphi_b(y) = (b *_{i+1} y) *_i y$ eine Permutation und die Gleichung besitzt eine Lösung $y = \varphi_b^{-1}(a)$. □

Ganz analog zeigt man den folgenden Satz:

Satz 38 *Seien $(Q, *_i)$ die Quasigruppen eines Prüfziffersystems, das alle Sprungzwillingsfehler erkennt, dann ist die Quasigruppe $(Q, *_i)$, $i = 1, \ldots, n-2$, orthogonal zu den durch*

$$x *'_{c,i} y = z \quad :\Leftrightarrow \quad (c *_{i+2} y) *_{i+1} z = x$$

definierten Quasigruppen mit $c \in Q$, und $*_{n-1}$ ist orthogonal zu

$$x *''_{n-1} y = z \quad :\Leftrightarrow \quad y *_n z = x.$$

Wenn ein Prüfziffersystem über Quasigruppen der Ordnung m alle Zwillings- oder alle Sprungzwillingsfehler erkennt, dann können wir also eine ganze Reihe verschiedener orthogonaler lateinischer Quadrate konstruieren. Hat außerdem die Gleichung $a *_n x = x *_n b$ oder für feste $c_1, c_2 \in Q$ die Gleichung $(c_1 *_{i+2} y) *_{i+1} a = (c_2 *_{i+2} y) *_{i+1} b$ für alle $a, b \in Q$ eine Lösung, dann ist, wie man leicht durch die Definition der Quasigruppen sieht, $*'_{n-1}$ orthogonal zu $*''_{n-1}$ bzw. $*'_{c_1,i}$ orthogonal zu $*'_{c_2,i}$. In diesem Fall hätten wir drei paarweise orthogonale lateinische Quadrate der Ordnung m.

Die Frage, für welche Ordnungen ein Paar orthogonaler lateinischer Quadrate, bzw. ein griechisch-lateinisches Quadrat existiert, blieb lange ungeklärt. EULER wußte (1780), daß es kein griechisch-lateinisches Quadrat der Ordnung 2 gibt und er kannte Konstruktionen für ungerade oder durch 4 teilbare Ordnungen. Basierend auf vielfältigen Untersuchungen vermutete er, daß griechisch-lateinische Quadrate der Ordnung $4k+2$ nicht existieren. G. TARRY bewies 1900 durch Ausschluß aller Möglichkeiten, daß es kein griechisch-lateinisches Quadrat der Ordnung 6 gibt [8], womit er die Vermutung von EULER stützte. Trotzdem gelang es PARKER, BOSE und SHRIKHANDE 1960, also 180 Jahre nach EULERS Vermutung, ein griechisch-lateinisches Quadrat der Ordnung 10 zu konstruieren [8]. Außerdem lieferten sie eine Konstruktion für die fehlenden geraden Ordnungen, die nicht durch vier teilbar sind (außer für 2 und 6).

0A	7E	8B	6H	9C	3J	5I	4D	1G	2F
6I	1B	7F	8C	0H	9D	4J	5E	2A	3G
5J	0I	2C	7G	8D	1H	9E	6F	3B	4A
9F	6J	1I	3D	7A	8E	2H	0G	4C	5B
3H	9G	0J	2I	4E	7B	8F	1A	5D	6C
8G	4H	9A	1J	3I	5F	7C	2B	6E	0D
7D	8A	5H	9B	2J	4I	6G	3C	0F	1E
4B	5C	6D	0E	1F	2G	3A	7H	8I	9J
1C	2D	3E	4F	5G	6A	0B	9I	7J	8H
2E	3F	4G	5A	6B	0C	1D	8J	9H	7I

Grichisch-lateinisches Quadrat der Ordnung 10.

Ob dagegen drei paarweise orthogonale lateinische Quadrate der Ordnung 10 existieren, ist bis heute unbekannt. Wir können allerdings zeigen:

Satz 39 *([8]) Die Anzahl der paarweise orthogonalen lateinischen Quadrate der Ordnung n ist nicht größer als $n-1$.*

Beweis Die Elemente der lateinischen Quadrate können umbenannt werden, ohne die Eigenschaft der Orthogonalität zu zerstören. Daher permutieren wir die

Elemente so, daß die erste Zeile jedes lateinischen Quadrates gleich $0, 1, 2, \ldots$ ist. Nun folgt, da die 1 bei jedem Paar lateinischer Quadrate mit sich selbst in der ersten Zeile zusammenfällt, daß die 1 in der ersten Spalte nicht zweimal an der gleichen Position steht. Weil sie auch nicht an der Position $(0, 0)$ steht, gibt es folglich nur $n - 1$ mögliche Positionen für 1. □

4.6 Verallgemeinerte Assoziativität

Definition 20 *(*R. SCHAUFFLER [20]*) Die vier Quasigruppen $(Q, *_1)$, $(Q, *_2)$, $(Q, *_3)$ und $(Q, *_4)$, definiert auf der gleichen Grundmenge Q, erfüllen das verallgemeinerte Assoziativgesetz, wenn für alle $x, y, z \in Q$ die folgende Gleichung gilt:*

$$(x *_1 y) *_2 z = x *_3 (y *_4 z).$$

Eine Menge Ω von Quasigruppen heißt im Ganzen assoziativ (oder Assoziativsystem) wenn zu je zwei Quasigruppen $*_1, *_2 \in \Omega$ zwei weitere Quasigruppen $*_3, *_4 \in \Omega$ existieren, so daß diese das verallgemeinerte Assoziativgesetz erfüllen. $*_3, *_4$ heißen dann rechts assoziiert zu $*_1, *_2$ und $*_1, *_2$ links assoziiert zu $*_3, *_4$.

Die Menge der Quasigruppen mit den Elementen $0, 1, \ldots, n$ werde mit Ω_n bezeichnet. Es wäre sehr nützlich, wenn Ω_n im Ganzen assoziativ wäre, dann könnten wir immer umklammern und die notwendigen Bedingungen zur Fehlererkennung wären deutlich einfacher nachzuprüfen. Leider ist dies i.allg. nicht der Fall, wie das folgende Theorem zeigt.

Theorem 16 *(*R. SCHAUFFLER [20]*) Ω_n ist nur dann im Ganzen assoziativ, wenn $n \leq 3$ ist.*

Beweis Für $n = 1$ ist die Aussage trivial.

Für $n = 2$ haben wir die beiden Quasigruppen

$+$	0	1
0	0	1
1	1	0

und

$*$	0	1
0	1	0
1	0	1

Die erste Quasigruppe ist die zyklische Gruppe $(\mathbb{Z}_2, +)$, die zweite läßt sich darstellen durch $x * y = x + y + 1$ und ist isotop zu $(\mathbb{Z}_2, +)$. Wie man nun leicht sieht, gilt damit das verallgemeinerte Assoziativgesetz für die vier möglichen Paare $++$, $*+$, $+*$ und $**$.

Auch für $n = 3$ sind alle Quasigruppen isotop zu $(\mathbb{Z}_3, +)$, denn es existieren für alle Quasigruppen $(Q, *)$ vier Permutationen p_1, p_2, p_3, p_4, so daß

$$x * y = p_1(x) + p_2(y) = p_3(x + p_4(y))$$

gilt. Für die 12 Quasigruppen der Ordnung 3 geben wir in der folgenden Tabelle jeweils die zugehörigen Permutationen mit der genannten Eigenschaft an:

Q	p_1	p_2	p_3	p_4	Q	p_1	p_2	p_3	p_4
0 1 2 1 2 0 2 0 1	[012]	[012]	[012]	[012]	0 2 1 1 0 2 2 1 0	[012]	[021]	[012]	[021]
0 1 2 2 0 1 1 2 0	[021]	[012]	[021]	[021]	0 2 1 2 1 0 1 0 2	[021]	[021]	[021]	[012]
1 0 2 2 1 0 0 2 1	[012]	[102]	[012]	[102]	1 2 0 2 0 1 0 1 2	[012]	[120]	[012]	[120]
1 0 2 0 2 1 2 1 0	[021]	[102]	[021]	[201]	1 2 0 0 1 2 2 0 1	[021]	[120]	[021]	[210]
2 0 1 0 1 2 1 2 0	[012]	[201]	[012]	[201]	2 1 0 0 2 1 1 0 2	[012]	[210]	[012]	[210]
2 0 1 1 2 0 0 1 2	[021]	[201]	[021]	[102]	2 1 0 1 0 2 0 2 1	[021]	[210]	[021]	[120]

Für zwei beliebige Quasigruppen $*_1$, $*_2$ gilt also $x *_1 y = p_1(x) + p_2(y)$ und $x *_2 y = p_3(x + p_4(y))$. Es folgt

$$\begin{aligned}(x *_1 y) *_2 z &= p_3((p_1(x) + p_2(y)) + p_4(z)) \\ &= p_3(p_1(x) + (p_2(y) + p_4(z))) \\ &= x *_3 (y *_4 z),\end{aligned}$$

wobei wir die Quasigruppen $*_3, *_4$ durch $x *_3 y = p_3(p_1(x) + y)$ und $y *_4 z = p_2(y) + p_4(z)$ definieren.

Wir zeigen nun, daß es für $n \geq 4$ stets Quasigruppen gibt, die keine rechtsassozierten Quasigruppen besitzen. Wenn die Quasigruppen $*_1, *_2, *_3, *_4$ das verallgemeinerte Assoziativgesetz erfüllen, d.h. es gilt für alle $x, y, z \in Q$

$$(x *_1 y) *_2 z = x *_3 (y *_4 z),$$

dann gibt es nur n verschiedene Permutationen

$$\varphi_{y,z}(x) := (x *_1 y) *_2 z = x *_3 (y *_4 z),$$

denn $y *_4 z$ nimmt nur n unterschiedliche Werte an. Im folgenden Beispiel erhalten wir aber mehr als n verschiedene Permutationen. Diese Quasigruppen befinden sich daher nicht in einem Assoziativsystem.

Sei $p = (0\ 1)$ die Transposition, welche die Elemente 0 und 1 vertauscht. Wir definieren die Quasigruppen durch

$$x *_1 y := x + p(y) \pmod n \qquad x *_2 y := p(x) + y \pmod n.$$

Beide Quasigruppen entstehen aus der Gruppe $(\mathbb{Z}_n, +)$, indem die ersten beiden Spalten bzw. Zeilen vertauscht werden. Die Permutationen $\varphi_{0,i}$, $i = 0, \ldots, n-1$, sind paarweise verschieden, denn es gilt

$$\varphi_{0,i}(0) = (0 *_1 0) *_2 i = p(0+1) + i = 0 + i = i.$$

Für die Permutation $\varphi_{1,0}$ erhalten wir $\varphi_{1,0}(0) = p(0 + p(1)) + 0 = 1$ und $\varphi_{1,0}(1) = p(1 + p(1)) + 0 = 0$. Weil $\varphi_{0,1}(1) = p(1 + p(0)) + 1 = p(2) + 1 = 3$ gilt, unterscheidet sich $\varphi_{1,0}$ von den Permutationen $\varphi_{0,i}$ in wenigstens einer Stelle. Damit haben wir aber $n+1$ paarweise verschiedene Permutationen und die Quasigruppen $*_1, *_2$ genügen nicht dem verallgemeinerten Assoziativgesetz. □

Theorem 17 *(*Aczél, Belousov, Hosszú [1]*) Erfüllen die vier Quasigruppen $(Q, *_1)$, $(Q, *_2)$, $(Q, *_3)$ und $(Q, *_4)$ das verallgemeinerte Assoziativgesetz,*

$$(x *_1 y) *_2 z = x *_3 (y *_4 z), \tag{4.3}$$

dann existiert eine Verknüpfung $\circ$, so daß $(Q, \circ)$ eine Gruppe bildet, zu der die $*_i$ isotop sind. Im Detail: Es existieren 5 Permutation $\alpha, \beta, \gamma, \delta, \epsilon$ von Q, so daß

$$\begin{aligned} x *_1 y &= \delta^{-1}(\alpha(x) \circ \beta(y)), \\ x *_2 y &= \delta(x) \circ \gamma(y), \\ x *_3 y &= \alpha(x) \circ \epsilon(y), \\ x *_4 y &= \epsilon^{-1}(\beta(x) \circ \gamma(y)). \end{aligned} \tag{4.4}$$

Die Gruppe, zu der die $*_i$ isotop sind, ist bis auf Isomorphie eindeutig bestimmt. Andererseits erfüllen alle Isotopien einer beliebigen Gruppe mit den genannten Eigenschaften das verallgemeinerte Assoziativgesetz.

Beweis Die letzte Behauptung wird einfach durch Einsetzen von 4.4 in 4.3 gezeigt, wobei wir die Assoziativität der Gruppe $(Q, \circ)$ benutzen.

Um die erste Aussage beweisen zu können, definieren wir zunächst die Permutationen

$$\rho_i(x) := x *_i a, \qquad \lambda_i(x) := a *_i x, \qquad (i = 1, 2, 3, 4),$$

wobei a ein beliebiges, fest gewähltes Element aus Q ist. Wir setzen $x = z = a$ in 4.3 und erhalten

$$\rho_2(\lambda_1(y)) = \lambda_3(\rho_4(y)). \tag{4.5}$$

Wir erhalten nun durch Substitution von $x = a, y = \lambda_1^{-1}(\rho_2^{-1}(u)), z = \lambda_4^{-1}(\lambda_3^{-1}(v))$ und $x = \rho_1^{-1}(\rho_2^{-1}(u)), y = a, z = \lambda_4^{-1}(\lambda_3^{-1}(v))$ und $x = \rho_1^{-1}(\rho_2^{-1}(u)), y = \rho_4^{-1}(\lambda_3^{-1}(v))$, $z = a$ in 4.3 die Gleichungen

$$\rho_2^{-1}(u) *_2 \lambda_4^{-1}(\lambda_3^{-1}(v)) = \lambda_3(\lambda_1^{-1}(\rho_2^{-1}(u)) *_4 \lambda_4^{-1}(\lambda_3^{-1}(v)))$$

und

$$\rho_2^{-1}(u) *_2 \lambda_4^{-1}(\lambda_3^{-1}(v)) = \rho_1^{-1}(\rho_2^{-1}(u)) *_3 \lambda_3^{-1}(v)$$

und

$$\rho_2(\rho_1^{-1}(\rho_2^{-1}(u)) *_1 \rho_4^{-1}(\lambda_3^{-1}(v))) = \rho_1^{-1}(\rho_2^{-1}(u)) *_3 \lambda_3^{-1}(v).$$

Die letzten drei Gleichungen zeigen, daß alle 4 Ausdrücke in ihnen gleich sind. Wir benennen diesen gemeinsamen Wert mit

$$u \circ v.$$

Damit erhalten wir 4.4 wenn wir

$$\alpha := \rho_2\rho_1, \quad \delta := \rho_2, \quad \gamma := \lambda_3\lambda_4, \quad \epsilon := \lambda_3$$

und (vergleiche 4.5)

$$\beta := \lambda_3\rho_4 = \rho_2\lambda_1$$

setzen.

Setzen wir 4.4 in 4.3 ein, dann sehen wir, daß die Operation $x \circ y$ assoziativ ist und, als Isotopie einer Quasigruppe, ebenfalls eine Quasigruppe ist. Bekanntlich sind die Gruppen genau die assoziativen Quasigruppen und so bildet Q eine Gruppe mit der Operation $\circ$. Die Eindeutigkeit, bis auf Isomorphie, der Gruppe $(G, \circ)$ folgt aus dem folgenden Theorem.

Theorem 18 *([1]) Isotope Gruppen sind isomorph, d.h. wenn die Gruppen* $(Q, \circ)$ *und* $(R, \cdot)$ *isotop sind*

$$\varphi(x \circ y) = \psi(x) \cdot \chi(y), \tag{4.6}$$

dann sind sie isomorph

$$\kappa(x \circ y) = \kappa(x) \cdot \kappa(y). \tag{4.7}$$

Beweis Sei e das neutrale Element von $(Q, \circ)$. Wir setzen $y = e$ bzw. $x = e$ in 4.6 und erhalten

$$\psi(x) = \varphi(x) \cdot b^{-1}$$

und

$$\chi(y) = a^{-1} \cdot \varphi(y),$$

wobei $a = \psi(e)$, $b = \chi(e)$ und a^{-1}, b^{-1} die Inversen in $(R, \cdot)$ sind. Setzen wir diese Gleichungen wieder in 4.6 ein, dann erhalten wir

$$\varphi(x \circ y) = \varphi(x) \cdot b^{-1} \cdot a^{-1} \cdot \varphi(y)$$

und wenn wir diese Gleichung von links mit a^{-1} und von rechts mit b^{-1} durchmultiplizieren und

$$\kappa(x) := a^{-1} \cdot \varphi(x) \cdot b^{-1}$$

definieren, so erhalten wir 4.7. □

Korollar 17 *In einem Assoziativsystem sind alle Quasigruppen zur selben Gruppe isotop.*

Wie bereits erwähnt, können wir bei Quasigruppen, die das verallgemeinerte Assoziativgesetz erfüllen, die Voraussetzungen vereinfachen, die für das Erkennen der einzelnen Fehlerarten notwendig sind. Seien $*'_{i+1}, *'_i$ rechtsassozierte Quasigruppen von $*_{i+1}$ und $*_i$. Wir erhalten für die einzelnen Fehlertypen folgende Bedingungen:

Satz 40 *Sei Ω ein Assoziativsystem. Durch die Quasigruppen $*_i \in \Omega$ und die Gleichung*

$$g(x_n, x_{n-1}, \ldots, x_0) = (\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_1 x_0 = d$$

wird genau dann ein Prüfziffersystem definiert, wenn $*_n$ anti-symmetrisch ist und für jedes Paar $*_{i+1}, *_i$ rechtsassoziierte Quasigruppen $*'_{i+1}, *'_i \in \Omega$ existieren, so daß $*'_i$ anti-symmetrisch ist.

Sind die Quasigruppen $*_n, *'_i$ selbstorthogonal, dann erkennt dieses Prüfziffersystem zusätzlich noch alle Zwillingsfehler.

Beweis Die genannte Gleichung erkennt alle Einzehlfehler und sie erkennt alle Nachbarvertauschungen, falls

$$\begin{aligned} x *_n y &= y *_n x \quad \Rightarrow \quad x = y \\ (c *_{i+1} x) *_i y &= (c *_{i+1} y) *_i x \quad \Rightarrow \quad x = y. \end{aligned}$$

gilt. Die erste Bedingung ist nach Voraussetzung erfüllt. Um die zweite Bedingung nachzuweisen, nehmen wir an, daß $(c *_{i+1} x) *_i y = (c *_{i+1} y) *_i x$ gilt. Nach Voraussetzung existieren rechtsassozierte Quasigruppen $*'_{i+1}, *'_i$, wobei $*'_i$ anti-symmetrisch ist, so daß $(s *_{i+1} t) *_i u = s *'_{i+1} (t *'_i u)$ für alle $s, t, u \in Q$ gilt. Damit folgt $c *'_{i+1} (x *'_i y) = c *'_{i+1} (y *'_i x)$. Wir kürzen c auf beiden Seiten der Gleichung und erhalten $x *'_i y = y *'_i x$. Da $*'_i$ anti-symmetrisch ist, folgt $x = y$ und die zweite Bedingung ist erfüllt. Bei der Rückrichtung sieht man leicht, daß falls entweder $*'_i$ oder $*_n$ nicht anti-symmetrisch ist, die Gleichung nicht alle Nachbarvertauschungen erkennen kann.

Für den zweiten Teil der Behauptung müssen wir zeigen, daß aus $x *_n x = y *_n y$ bzw. $x *'_i x = y *'_i y$ die Gleichheit von x und y folgt. Dazu benutzen wir das folgende Lemma:

Lemma 19 *Eine selbstorthogonale Quasigruppe $(Q, *)$ ist anti-symmetrisch und es gilt:*

$$x * x = y * y \qquad \Rightarrow \qquad x = y.$$

Beweis Weil Q selbstorthogonal ist, sind die Paare $(x * y, y * x)$ für alle $x, y \in Q$ paarweise verschieden. Gäbe es $x, y \in Q$ mit $x \neq y$ und $x * y = y * x$, dann wären die Paare $(x * y, y * x)$ und $(y * x, x * y)$ gleich und Q wäre nicht selbstorthogonal. Ebenso folgt aus $x * x = y * y$, daß die Paare $(x * x, x * x)$ und $(y * y, y * y)$ gleich sind, also folgt entweder $x = y$ oder Q ist nicht selbstorthogonal. □

Für $m = 10$ existiert allerdings keine selbstorthogonale Quasigruppe in einem Assoziativsystem. Denn solch eine Quasigruppe wäre isotop zu der Diedergruppe, die dann eine vollständige Abbildung hätte. Aber D_5 besitzt keine vollständige Abbildung, Theorem 2 (Seite 19).

Bemerkung Selbstorthogonale Quasigruppen werden auch *anti-abelsch* genannt (vgl. Dénes, Keedwell [8]). Eine anti-symmetrische Quasigruppe muß aber nicht anti-abelsch sein, wie das folgende Gegenbeispiel zeigt:

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Diese Quasigruppe ist offensichtlich anti-symmetrisch, aber es gilt $0 * 0 = 1 * 1$, also ist sie nicht anti-abelsch.

4.7 Quasigruppen isotop zu einer Gruppe

In diesem Abschnitt untersuchen wir die speziellen Eigenschaften von Prüfziffersystemen über Quasigruppen, die isotop zu einer Gruppe sind. Im vorherigen

Abschnitt haben wir gesehen, daß der dortige Ansatz mit Quasigruppen in einem Assoziativsystem ebenfalls zu diesen Quasigruppen führt.

Im folgenden seien die Quasigruppen $(Q, *_i)$ isotop zu der Gruppe $(Q, \cdot)$, d.h. es existieren Permutationen $\varphi_{i,1}, \varphi_{i,2}, \varphi_{i,3}$, so daß

$$x *_i y = \varphi_{i,3}(\varphi_{i,1}(x) \cdot \varphi_{i,2}(y))$$

gilt.

Die entsprechenden Voraussetzungen an die $\varphi_{i,j}$ für das Erkennen der einzelnen Fehlertypen erhält man nun einfach durch Einsetzen dieser Gleichungen in die Bedingungen 4.2, Seite 75f, für Quasigruppen. Wir zeigen allerdings eine etwas einfacher zu erfüllende Voraussetzung:

Satz 41 *Die Quasigruppen $(G, *_i)$ seien isotop zu $(G, \cdot)$. Sie definieren ein Prüfziffersystem, falls folgende Bedingungen erfüllt sind, $i = 1, \ldots, n-1$,*

$$\varphi_{n,1} \circ \varphi_{n,2}^{-1} \in Ant(G) \tag{4.8}$$

$$\varphi_{i,1} \circ \varphi_{i+1,3} \circ \varphi_{i+1,2} \circ \varphi_{i,2}^{-1} \in Ant(G) \tag{4.9}$$

$$\varphi_{i,1} \circ \varphi_{i+1,3} \in Aut(G). \tag{4.10}$$

Beweis Es ist $x *_n y = y *_n x$ äquivalent zu

$$\varphi_{n,3}(\varphi_{n,1}(x) \cdot \varphi_{n,2}(y)) = \varphi_{n,3}(\varphi_{n,1}(y) \cdot \varphi_{n,2}(x)).$$

Wir kürzen $\varphi_{n,3}$, setzen $\tilde{x} := \varphi_{n,2}(x)$ und $\tilde{y} := \varphi_{n,2}(y)$ womit $\varphi_{n,1}(\varphi_{n,2}^{-1}(\tilde{x})) \cdot \tilde{y} = \varphi_{n,1}(\varphi_{n,2}^{-1}(\tilde{y})) \cdot \tilde{x}$ folgt. Nach Voraussetzung ist $\varphi_{n,1} \circ \varphi_{n,2}^{-1}$ anti-symmetrisch und daher impliziert diese Gleichung $x = y$.

Nun nehmen wir an, daß $(c *_{i+1} x) *_i y = (c *_{i+1} y) *_i x$ bzw.

$$\begin{aligned} &\varphi_{i,3}\big[\varphi_{i,1}\big(\varphi_{i+1,3}(\varphi_{i+1,1}(c) \cdot \varphi_{i+1,2}(x))\big) \cdot \varphi_{i,2}(y)\big] \\ = &\varphi_{i,3}\big[\varphi_{i,1}\big(\varphi_{i+1,3}(\varphi_{i+1,1}(c) \cdot \varphi_{i+1,2}(y))\big) \cdot \varphi_{i,2}(x)\big] \end{aligned}$$

gilt. Wir definieren $\tilde{x} := \varphi_{i,2}(x)$, $\tilde{y} := \varphi_{i,2}(y)$, $\tilde{c} := \varphi_{i+1,1}(c)$ und $\alpha := \varphi_{i,1} \circ \varphi_{i+1,3}$, $\beta := \varphi_{i+1,2} \circ \varphi_{i,2}^{-1}$. Es folgt

$$\alpha(\tilde{c} \cdot \beta(\tilde{x})) \cdot \tilde{y} = \alpha(\tilde{c} \cdot \beta(\tilde{y})) \cdot \tilde{x}$$

und, weil α ist ein Automorphismus ist,

$$\alpha(\tilde{c}) \cdot \alpha \circ \beta(\tilde{x})) \cdot \tilde{y} = \alpha(\tilde{c}) \cdot \alpha \circ \beta(\tilde{y})) \cdot \tilde{x}.$$

Wir können $\alpha(\tilde{c})$ auf beiden Seiten der Gleichung kürzen. Da wir vorausgesetzt haben, daß $\alpha \circ \beta = \varphi_{i,1} \circ \varphi_{i+1,3} \circ \varphi_{i+1,2} \circ \varphi_{i,2}^{-1}$ eine anti-symmetrische Abbildung

ist, folgt aus der resultierenden Gleichung $\tilde{x} = \tilde{y}$ bzw. $x = y$. Damit haben wir gezeigt, daß die Quasigruppen $(G, *_i)$ ein Prüfziffersystem definieren. □

Bemerkung Die ersten beiden Eigenschaften sind auch notwendig für das Erkennen aller Nachbarvertauschungen.

Beispiel Sei φ eine anti-symmetrische Abbildung der Gruppe $(G, \cdot)$. Wir wählen $\varphi_{i,2} := \varphi^{i-1}$, $\varphi_{n,1} := \varphi^n$, $\varphi_{i,1} \circ \varphi_{i+1,3} = Id$ und $\varphi_{1,3}$ beliebig. Damit sind die Voraussetzungen des Satzes für die Quasigruppen $x *_i y := \varphi_{i,3}\big(\varphi_{i,1}(x) \cdot \varphi_{i,2}(y)\big)$ erfüllt. Es folgt, daß

$$(\dots(x_n *_n x_{n-1}) *_{n-1} \dots) *_1 x_0 = c$$

ein Prüfziffersystem definiert.

Konkret wählen wir die anti-symmetrische Abbildung $\varphi := [02413]$ der Gruppe $(\mathbb{Z}_5, +)$ (vgl. Seite 40) und $\varphi_{i,1} := \varphi_{i,3} := [10324]$. Damit erhalten wir für $n = 3$ die folgenden Quasigruppen:

$*_3$	0	1	2	3	4
0	1	4	2	3	0
1	2	3	0	1	4
2	0	1	4	2	3
3	4	2	3	0	1
4	3	0	1	4	2

$*_2$	0	1	2	3	4
0	0	2	1	3	4
1	1	3	4	0	2
2	2	1	3	4	0
3	3	4	0	2	1
4	4	0	2	1	3

$*_1$	0	1	2	3	4
0	0	3	2	4	1
1	1	0	3	2	4
2	2	4	1	0	3
3	3	2	4	1	0
4	4	1	0	3	2

4.7.1 Lineare Quasigruppen

Um die Anforderungen an die Quasigruppen zu verringern, ist es sinnvoll, sogenannte lineare Quasigruppen zu betrachten, da diese eine sehr einfache Darstellung besitzen.

Definition 21 *([5]) Sei $(Q, \cdot)$ eine Gruppe mit den Automorphismen ψ_1, ψ_2 und einem fest gewählten $c \in Q$. Die Quasigruppe $(Q, *)$ heißt* lineare Quasigruppe (der Gruppe $(Q, \cdot)$), *falls die Gleichung $x * y = \psi_1(x) \cdot c \cdot \psi_2(y)$ für alle $x, y \in Q$ erfüllt ist.*

Satz 42 *Die Menge der linearen Quasigruppen einer Gruppe $(Q, \cdot)$ bildet ein Assoziativsystem.*

Beweis Seien $(Q, *_1)$ und $(Q, *_2)$ lineare Quasigruppen der Gruppe $(Q, \cdot)$, d.h. $x *_1 y = \psi_1(x) \cdot c \cdot \psi_2(y)$ und $x *_2 y = \varphi_1(x) \cdot d \cdot \varphi_2(y)$ mit $\psi_1, \psi_2, \varphi_1, \varphi_2 \in Aut(Q, \cdot)$,

$c, d \in Q$. Es gilt:

$$\begin{aligned}(x *_1 y) *_2 z &= \varphi_1(\psi_1(x) \cdot c \cdot \psi_2(y)) \cdot d \cdot \varphi_2(z) \\ &= \varphi_1 \circ \psi_1(x) \cdot \varphi_1(c) \cdot \big(\varphi_1 \circ \psi_2(y) \cdot d \cdot \varphi_2(z)\big) \\ &= x *_3 (y *_4 z)\end{aligned}$$

mit $x *_3 y := \varphi_1 \circ \psi_1(x) \cdot \varphi_1(c) \cdot y$ und $y *_4 z := \varphi_1 \circ \psi_2(y) \cdot d \cdot \varphi_2(z)$ und $*_3$, $*_4$ sind lineare Quasigruppen der Gruppe $(Q, \cdot)$. □

Der folgende Spezialfall der linearen Quasigruppen wurde von ECKER und POCH untersucht. Dabei setzen wir $*_i := *$ für alle i:

Satz 43 *(*ECKER, POCH [9]*) Sei $\mathbb{Z}_n = \{0, \ldots, n-1\}$, $n \geq 2$ und $h, k, l \in \mathbb{Z}_n$ mit h und k teilerfremd zu n. Dann ist $Q_n = (\mathbb{Z}_n, *)$ mit $x * y = (h \cdot x + k \cdot y + l) \bmod n$ eine lineare Quasigruppe. Nachbarvertauschungen werden erkannt, falls $h-1$ und $h-k$ teilerfremd zu n sind, und Sprungtranspositionen werden erkannt, falls $h-1$, $h+1$ und $h^2 - k$ teilerfremd zu n sind.*

Beweis Die Abbildungen $x \mapsto h \cdot x$ und $y \mapsto k \cdot y$ sind Automorphismen der Gruppe $\mathbb{Z}_n$, da h und k teilerfremd zu n sind. Wir zeigen die erste Eigenschaft von 4.2 (Seite 75). Dazu sei $x * y = y * x$, also $hx + ky + l = hy + kx + l$. Es folgt $(h-k)(x-y) = 0$ und mit der Eigenschaft, daß $h-k$ eine Einheit in $\mathbb{Z}_n$ ist, $x - y = 0$ bzw. $x = y$. Nun nehmen wir an, daß $(c * x) * y = (c * y) * x$ gilt, d.h. $h(hc + kx + l) + ky + l = h(hc + ky + l) + kx + l$. Wir kürzen auf beiden Seiten die gleichen Terme und erhalten $hkx + ky = hky + kx$. k ist eine Einheit, daher können wir auch k kürzen. Es folgt $(h-1)(x-y) = 0$ und damit, weil wir $h-1$ als Einheit vorausgesetzt haben, $x = y$. Die entsprechenden Bedingungen für Sprungtranspositionen werden ganz analog gezeigt. □

Korollar 18 *(*ECKER, POCH [9]*) Sei q teilerfremd zu n, $1 \leq q \leq n-2$ ($n \geq 3$). Wenn wir $h = -q$, $k = 1$ und $l = 0$ setzen, dann werden alle Nachbarvertauschungen erkannt, vorausgesetzt, daß $q+1$ teilerfremd zu n ist. Zusätzlich werden alle Sprungtranspositionen erkannt, falls $q-1$ teilerfremd zu n ist.*

Ist n gerade, dann ist entweder h oder $h-1$ gerade und daher nicht teilerfremd zu n. Also gibt es für gerades n keine lineare Quasigruppe, die alle Nachbarvertauschungen erkennt. Dies liegt u.a. auch am folgenden Zusammenhang:

Satz 44 *Ein Prüfziffersystem über linearen Quasigruppen der Gruppe $(G, \cdot)$ ist ein Prüfziffersystem über dieser Gruppe.*

Beweis Seien $(G, *_i)$, $i = 1, \ldots, n$, lineare Quasigruppen der Gruppe $(G, \cdot)$ mit $x *_i y = \psi_i(x) \cdot c_i \cdot \varphi_i(y)$. Wir zeigen die Behauptung durch vollständige Induktion

nach der Anzahl der beteiligten Quasigruppen. Für eine Quasigruppe $*_n$ haben wir

$$x_n *_n x_{n-1} = \psi_n(x_n) \cdot c_n \cdot \varphi_n(x_{n-1}).$$

Wir setzen $\tau_n(x) := \psi_n(x)$ und $\tau_{n-1}(x) := c_n \cdot \varphi_n(x)$ und erhalten den Induktionsanfang

$$x_n *_n x_{n-1} = \tau_n(x_n) \cdot \tau_{n-1}(x_{n-1}).$$

Nun gelte $(\dots(x_n *_n x_{n-1}) *_{n-1} \dots) *_i x_{i-1} = \tau_n(x_n) \cdot \ldots \cdot \tau_{i-1}(x_{i-1})$. Es folgt

$$(\tau_n(x_n) \cdot \ldots \cdot \tau_{i-1}(x_{i-1})) *_{i-1} x_{i-2} = \psi_{i-1}(\tau_n(x_n) \cdot \ldots \cdot \tau_{i-1}(x_{i-1})) \cdot c_{i-1} \cdot \varphi_{i-1}(x_{i-2}).$$

Mit $\tilde{\tau}_j(x) := \psi_{i-1} \circ \tau_j(x)$, $j = n, \dots, i-1$, $\tilde{\tau}_{i-2}(x) := c_{i-1} \cdot \varphi_{i-1}(x)$ und der Eigenschaft, daß ψ_{i-1} ein Automorphismus ist, haben wir $(\dots(x_n *_n x_{n-1}) *_{n-1} \dots) *_i x_{i-2} = \tilde{\tau}_n(x_n) \cdot \ldots \cdot \tilde{\tau}_{i-2}(x_{i-2})$ gezeigt. Damit folgt die Behauptung. □

Bemerkung Wir haben die Eigenschaft, daß ψ_n und die φ_i Automorphismen sind nicht benutzt. Die gleiche Aussage gilt daher auch für Quasigruppen, bei denen ψ_n und die φ_i nur Permutationen sind, aber keine Automorphismen.

Der Ansatz mit linearen Quasigruppen führt also auf die bereits in Kapitel 1 behandelten Prüfziffersysteme über Gruppen. Da wir schon gezeigt haben, daß über der Gruppe $\mathbb{Z}_{2n}$, kein Prüfziffersystem existiert, kann es auch kein Prüfziffersystem über linearen Quasigruppen der Gruppe $\mathbb{Z}_{2n}$ geben.

4.8 Total anti-symmetrische Quasigruppen

Ein naheliegender Ansatz zur Reduktion der Anzahl der Paare orthogonaler lateinischer Quadrate, ist es, anstatt verschiedener Quasigruppen, nur eine einzelne Quasigruppe zu betrachten. Dies hat auch praktische Vorteile, da wir in diesem Fall die Stellenzahl der zu sichernden Zahlen einfach erhöhen können, während bei verschiedenen Quasigruppen nicht klar ist, wie wir eine weitere Quasigruppe hinzu nehmen können, ohne dabei die Fehlererkennung zu zerstören.

Wir betrachten daher die Prüfziffersysteme der Form

$$(\dots((x_n * x_{n-1}) * x_{n-2}) * \dots) * x_0 = c. \tag{4.11}$$

Eine Quasigruppe heißt *total anti-symmetrisch*, falls sie anti-symmetrisch ist und außerdem gilt:

$$(c * x) * y = (c * y) * x \qquad \Rightarrow \qquad x = y. \tag{4.12}$$

Damit definiert die Gleichung 4.11 genau dann ein Prüfziffersystem, wenn $*$ eine total anti-symmetrische Quasigruppe ist.

4.8.1 Konstruktion

In diesem Abschnitt geben wir einen Algorithmus an, mit dessen Hilfe total anti-symmetrische Quasigruppen konstruiert werden können. Die Eigenschaft 4.12 können wir durch die Parastrophie $(Q, /)$ etwas anders formulieren. Wir setzen $\tilde{x} := c * x$, also $c/\tilde{x} = x$ und erhalten die neue Bedingung

$$\tilde{x} * y = (c * y) * (c/\tilde{x}) \quad \Rightarrow \quad c/\tilde{x} = y \quad (\text{für alle } c, \tilde{x}, y \in Q)$$

Nun sei $M = m(i, j, k)$ ein Würfel mit $m(i, j, k) := k$, $(i, j, k = 0, 1, \ldots, n-1)$. Wir konstruieren die Quasigruppe $*$ durch:

1) Für i von 0 bis $n-1$ tue 2-10

   2) Für j von 0 bis $n-1$ tue 3-7

      3) Sind alle Elemente $m(i, j, 0), \ldots, m(i, j, n-1)$ gestrichen, dann Abbruch

      4) Wähle ein Element $m(i, j, k)$ aus, das noch nicht gestrichen ist und setze $i * j := k$

      5) Streiche die Elemente $m(i+1, j, k), \ldots, m(n-1, j, k)$

      6) Streiche die Elemente $m(i, j+1, k), \ldots, m(i, n-1, k)$

      7) Streiche das Element $m(j, i, k)$, falls $j > i$

   8) Streiche die Elemente $m(c * y, c/x, x * y)$, $c = 0, \ldots, i-1,\ x = i,\ y = 0, \ldots, n-1$

   9) Streiche die Elemente $m(c * y, c/x, x * y)$, $c = i,\ x = 0, \ldots, i,\ y = 0, \ldots, n-1$

   10) Gibt es in den Schritten 8 oder 9 $x \neq c * y$ mit $x * y = (c * y) * (c/x)$, $c * y \leq i$, dann Abbruch

Erläuterungen: Die Schritte 5+6 sorgen dafür, daß eine Quasigruppe konstruiert wird. Durch Schritt 7 werden nur anti-symmetrische Quasigruppen erzeugt. Die Schritte 8-10 beschleunigen den Algorithmus erheblich, denn es werden schon während der Konstruktion diejenigen Quasigruppen ausgeschlossen, die nicht total anti-symmetrisch sind. Wir zeigen dies in dem folgenden Satz:

Satz 45 *Eine Quasigruppe $(Q, \cdot)$ kann genau dann mit dem Algorithmus konstruiert werden, wenn sie total anti-symmetrisch ist.*

Beweis Wir zeigen zunächst mit vollständiger Induktion, daß eine total anti-symmetrische Quasigruppe $(Q, \cdot)$ mit dem Algorithmus konstruiert werden kann. Es sei $(i', j') < (i, j)$ falls $i' < i$ oder falls $i' = i$ und $j' < j$ ist. Wir beginnen die

Induktion mit $(i,j) = (0,0)$. Da für $i = j = 0$ noch kein Element gestrichen ist, können wir $0 * 0 := 0 \cdot 0$ setzen. Nun gelte $i' * j' = i' \cdot j'$ für alle $(i',j') < (i,j)$.
Annahme: In Durchlauf (i,j) ist das Element $m(i,j,i \cdot j)$ gestrichen, d.h. es existiert ein $(i',j') < (i,j)$, so daß in Durchlauf (i',j') $m(i,j,i \cdot j)$ gestrichen wurde. Wir unterscheiden die folgenden Fälle:
Fall 1: $m(i,j,i \cdot j)$ wurde in Schritt 5 oder 6 gestrichen. Entweder gilt dann $j = j'$ und $i' \cdot j = i' * j = i \cdot j$ oder $i = i'$ und $i \cdot j' = i * j' = i \cdot j$. In beiden Fällen folgt $(i',j') = (i,j)$ im Widerspruch zu $(i',j') < (i,j)$.
Fall 2: $m(i,j,i \cdot j)$ wurde in Schritt 7 gestrichen, also $i' = j$ und $j' = i$. Es folgt $j \cdot i = j * i = i \cdot j$. Nach Voraussetzung an $(Q,\cdot)$ impliziert dies $i = j$ und damit $(i',j') = (i,j)$, Widerspruch.
Fall 3: $m(i,j,i \cdot j)$ wurde in Schritt 8 gestrichen, d.h. $i' < i$ und es existiert ein $c < i'$, $y \in \{0,\ldots,n-1\}$ mit $c \cdot y = c * y = i$, $c/i' = j$, $i' \cdot y = i' * y = i \cdot j$. Die zweite Gleichung ist äquivalent zu $i' = c * j = c \cdot j$. Wir setzen diese und die erste Gleichung in die dritte ein und erhalten $(c \cdot j) \cdot y = (c \cdot y) \cdot j$. Dies impliziert nach Voraussetzung $j = y$ und wir erhalten aus der dritten Gleichung $i' = i$ im Widerspruch zu $i' < i$.
Fall 4: $m(i,j,i \cdot j)$ wurde in Schritt 9 gestrichen, d.h. $i' < i$ und es existiert ein $x \leq i' < i$, $y \in \{0,\ldots,n-1\}$ mit $i' \cdot y = i' * y = i$, $i'/x = j$ und $x \cdot y = x * y = i \cdot j$. Auch hier folgt durch Einsetzen in die letzte Gleichung $(i' \cdot j) \cdot y = (i' \cdot y) \cdot j$. Demnach ist $j = y$ und $i = x$ im Widerspruch zu $x < i$.

Damit ist die Annahme widerlegt, d.h. das Element $m(i,j,i \cdot j)$ ist nicht gestrichen. Wir setzen daher $i * j := i \cdot j$.

Der Algorithmus bricht nicht in Schritt 3 ab, da wir gezeigt haben, daß mindestens ein Element, nämlich $m(i,j,i \cdot j)$ nicht gestrichen ist. Wenn der Algorithmus in Schritt 10 abbrechen würde, dann gäbe es $c,x \in \{0,\ldots,i\}$, $y \in \{0,\ldots,n-1\}$, $c * y \leq i$, $x \neq c * y = c \cdot y$ mit $x * y = (c * y) * (c/x)$. Wir setzen $z := c/x$ bzw. $x = c * z = c \cdot z$ und es folgt $x \cdot y = (c \cdot y) \cdot z = (c \cdot z) \cdot y$. Wir erhalten $z = y$, woraus $x = c \cdot y$ folgt im Widerspruch zu $x \neq c \cdot y$. Damit haben wir gezeigt, daß die Quasigruppe $(Q,\cdot)$ mit dem Algorithmus konstruiert werden kann.

Sei nun andererseits $(Q,*)$ eine Quasigruppe, die mit dem Algorithmus konstruiert wurde. Wir nehmen an, es gäbe $c,x,y \in \{0,\ldots,n-1\}$, $x \neq c * y$ mit $x * y = (c * y) * (c/x)$. Sei $i := max(c,x)$, also $c,x \leq i$. Wir betrachten nun den Algorithmus in Durchlauf i bei den Schritten 8-10.
Fall 1: $c = i$, $x \leq i$, $c * y \leq i$. In Schritt 9 gibt es demnach $x \neq c * y$ mit $x * y = (c * y) * (c/x)$, $c * y \leq i$ und der Algorithmus bricht ab.
Fall 2: $c < i$, $x = i$, $c * y \leq i$. In Schritt 8 sind damit die Bedingungen von Schritt

10 erfüllt und der Algorithmus bricht ab.
Fall 3: $c = i$, $x \leq i$, $c * y > i$. Es ist $(x, y) < (c * y, c/x)$. In Schritt 9 wurde das Element $m(c * y, c/x, x * y)$ gestrichen, daher ist die Wahl $(c * y) * (c/x) = x * y$ im Durchlauf $(i', j') = (c * y, c/x)$ nicht möglich, im Widerspruch dazu, daß wir $(Q, *)$ mit dem Algorithmus konstruiert haben.
Fall 4: $c < i$, $x = i$, $c * y > i$. Auch hier ist $(x, y) < (c * y, c/x)$ und es folgt analog zu Fall 3, daß in Schritt 8 $m(c * y, c/x, x * y)$ gestrichen wurde und deshalb ist $(c * y) * (c/x) \neq x * y$, Widerspruch.
Nun nehmen wir an, es gäbe $x \neq y$ mit $x * y = y * x$, o.B.d.A. $x < y$. Im Durchlauf (x, y) wird das Element $m(y, x, x * y)$ gestrichen und kann daher im Durchlauf (y, x) nicht ausgewählt werden, also $x * y \neq y * x$, Widerspruch.
Damit ist der Beweis des Satzes abgeschlossen. □

Wie bei den anti-symmetrischen Abbildungen kann man alle total anti-symmetrischen Quasigruppen konstruieren, indem man in Schritt 4) nacheinander alle nicht gestrichenen Elemente auswählt und den Algorithmus rekursiv aufruft.

Mit diesem rekursiven Algorithmus haben wir die Anzahl der total anti-symmetrischen Quasigruppen mit einer Linkseins und derer, die zusätzlich noch alle Sprungtranspositionen erkennen, bestimmt.

Ordnung	Anzahl (Gesamt)	total anti-symmetrisch	Sprungtrans-positionen
3	2	1	0
4	24	2	2
5	1.344	18	12
6	1.128.960	0	0
7	12.198.297.600	2.400	480
8	2.697.818.265.354.240	31.680	1.440

Die Werte für $n = 3, 4, 5, 6$ bestätigen die von ECKER und POCH [9] bestimmte Anzahl. Die Rechenzeit für $n = 7$ betrug ca. 6 Minuten, die für $n = 8$ ca. 12,5 Stunden. Für die Konstruktion der total anti-symmetrischen Quasigruppen haben wir die folgenden Sätze ausgenutzt.

Satz 46 *Ist $(Q, *)$ eine total anti-symmetrische Quasigruppe, φ und ψ Permutationen, dann wird durch $x \cdot y := \psi^{-1}(\psi(x) * \varphi(y))$ ebenfalls eine total anti-symmetrische Quasigruppe definiert, falls $\psi \circ \varphi^{-1} \in Ant(Q, *)$ oder $(Q, \cdot)$ eine Linkseins besitzt.*

Beweis Wir nehmen zunächst an, daß $(c \cdot x) \cdot y = (c \cdot y) \cdot x$ gilt, dann folgt mit der Definition von $(Q, \cdot)$, daß $(\psi(c) * \varphi(x)) * \varphi(y) = (\psi(c) * \varphi(y)) * \varphi(x)$ ist. Da $(Q, *)$ total anti-symmetrisch ist, folgt $\varphi(x) = \varphi(y)$ und demnach $x = y$.

Falls $(Q,\cdot)$ eine Linkseins 0 besitzt, dann folgt aus $x\cdot y=(0\cdot x)\cdot y=(0\cdot y)\cdot x=y\cdot x$ die Gleichung $x=y$. Also ist $(Q,\cdot)$ total anti-symmetrisch.
Gilt $\psi\circ\varphi^{-1}\in Ant(Q,*)$, dann impliziert $x\cdot y=\psi^{-1}(\psi(x)*\varphi(y))=\psi^{-1}(\psi(y)*\varphi(x))=y\cdot x$ die Gleichung $\psi(x)*\varphi(y)=\psi(y)*\varphi(x)$ und damit $\psi(\varphi^{-1}(\varphi(x)))*\varphi(y)=\psi(\varphi^{-1}(\varphi(y)))*\varphi(x)$. Nach Voraussetzung ist $\psi\circ\varphi^{-1}$ eine anti-symmetrische Abbildung der Quasigruppe $(Q,*)$, deshalb folgt $\varphi(x)=\varphi(y)$ und $x=y$. Folglich ist $(Q,\cdot)$ total anti-symmetrisch. □

Korollar 19 *Ist $(Q,*)$ eine total anti-symmetrische Quasigruppe, so ist auch $(Q,\cdot)$ mit $x\cdot y:=\varphi^{-1}(\varphi(x)*\varphi(y))$ total anti-symmetrisch.*

Beweis Setze $\psi:=\varphi$, dann ist $\psi\circ\varphi^{-1}=Id\in Ant(Q,*)$, weil $(Q,*)$ anti-symmetrisch ist.

Satz 47 *Sei $(Q,*)$ eine total anti-symmetrische Quasigruppe, dann existiert eine total anti-symmetrische Quasigruppe mit Linkseins, $(Q,\cdot)$ und eine anti-symmetrische Abbildung $\varphi^{-1}\in Ant(Q,\cdot)$ mit $x*y=x\cdot\varphi(y)$.*

Beweis Sei $\varphi(x):=0*x$ und $x\cdot y:=x*\varphi^{-1}(y)$, dann gilt $y=0*\varphi^{-1}(y)$ und demnach $0\cdot y=0*\varphi^{-1}(y)=y$ für alle $y\in Q$, also besitzt $(Q,\cdot)$ eine Linkseins und ist nach Satz 46 total anti-symmetrisch. Außerdem gilt $\varphi^{-1}\in Ant(Q,\cdot)$, denn aus $\varphi^{-1}(x)\cdot y=\varphi^{-1}(y)\cdot x$ folgt $\varphi^{-1}(x)*\varphi^{-1}(y)=\varphi^{-1}(y)*\varphi^{-1}(x)$. $(Q,*)$ ist anti-symmetrisch daher erhalten wir $\varphi^{-1}(x)=\varphi^{-1}(y)$ bzw. $x=y$. Damit haben wir $x\cdot\varphi(y)=x*\varphi^{-1}(\varphi(y))=x*y$ und die Behauptung ist bewiesen. □

Wir können also alle total anti-symmetrischen Quasigruppen bestimmen, indem wir die total anti-symmetrischen Quasigruppen mit Linkseins und deren anti-symmetrische Abbildungen konstruieren.

Satz 48 *Eine total anti-symmetrische Quasigruppe mit Linkseins ist isomorph zu einer total anti-symmetrischen Quasigruppe mit Linkseins $(Q,\cdot)$, $Q=\{0,\ldots,n-1\}$, für die*

$$1\cdot x\leq x+2,\qquad x=0,\ldots,n-1$$

gilt.

Beweis Sei $(Q,*)$ eine total anti-symmetrische Quasigruppe mit Linkseins 0. Wir beweisen den Satz mit vollständiger Induktion.

Falls $1*0\leq 2$ ist (Bem.: in diesem Fall gilt $1*0=2$) , dann ist nichts zu zeigen. Gilt $1*0>0+2=2$, dann definieren wir $\varphi(1*0):=2$, $\varphi(2):=1*0$ und

$\varphi(x) := x$ sonst. Die Quasigruppe $(Q, \cdot)$ mit $x \cdot y := \varphi(\varphi(x) * \varphi(y))$ ist isomorph zu $(Q, *)$, da $\varphi^{-1} = \varphi$ gilt und es ist $1 \cdot 0 = \varphi(\varphi(1) * \varphi(0)) = \varphi(1 * 0) = 2 \leq 0 + 2$.

Nun sei $(Q, *)$ isomorph zu $(Q, *')$, und es gelte $1 *' x \leq x + 2$ für $0 \leq x \leq k < n - 3$. Ist $1 *' (k + 1) > k + 3$, dann setzen wir $\varphi(1 *' (k + 1)) := k + 3$, $\varphi(k + 3) := 1 *' (k + 1)$ und $\varphi(x) := x$ sonst. Damit erfüllt die Quasigruppe $(Q, \cdot)$ mit $x \cdot y := \varphi(\varphi(x) * \varphi(y))$ die gesuchte Bedingung, denn es gilt

$$1 \cdot x = \varphi(\varphi(1) *' \varphi(x)) = \varphi(1 *' x) = 1 *' x \leq x + 2, \qquad \text{für } 0 \leq x \leq k$$

und

$$1 \cdot (k + 1) = \varphi(\varphi(1) *' \varphi(k + 1)) = \varphi(1 *' (k + 1)) = k + 3 = (k + 1) + 2$$

und $(Q, \cdot)$ ist isomorph zu $(Q, *)$.

Da für $x \geq n - 3$ die Aussage $1 * x \leq x + 2$ trivial ist (denn schließlich ist $1 * x \leq n - 1$ für alle $x \in Q$), haben wir damit den Satz bewiesen. □

Wir brauchen also nur solche Quasigruppen zu konstruieren, welche eine Linkseins besitzen, und für die $1 * x \leq x + 2$ gilt. Die Gesamtanzahl erhalten wir durch das Auszählen der verschiedenen isomorphen Quasigruppen. Damit verkürzt sich die Rechenzeit erheblich, z.B. für $n = 8$ von schätzungsweise einer Woche auf etwa einen halben Tag.

Außerdem haben wir den Algorithmus noch dadurch beschleunigt, daß wir beim Streichen eines Elements gleich überprüfen, ob bereits alle Elemente $m(i, j, k)$, $k = 0, \ldots, n - 1$ gestrichen wurden. Dies erreichen wir, indem wir mitzählen, wieviele Elemente noch nicht gestrichen sind. Sind alle Elemente gestrichen, so können wir den aktuellen Durchlauf abbrechen und in der Rekursion eine Ebene höher gehen.

Für $n = 10$ haben wir auch nach längerer Suche keine total anti-symmetrische Quasigruppe gefunden. Da die Zahl der Quasigruppen mit n stark anwächst (siehe McKay, Rogoyski [16]), konnten wir allerdings nur einen sehr geringen Prozentsatz überprüfen. Ecker und Poch haben sogar die Vermutung ausgesprochen, daß Quasigruppen der Ordnung $4k + 2$ nicht total anti-symmetrisch sein können. Wir stützen diese Vermutung durch den folgenden Satz:

Satz 49 *Es existiert keine zu D_s, $s > 2$ ungerade, isotope Quasigruppe, die total anti-symmetrisch ist. Die Quasigruppen, die zu $\mathbb{Z}_{2k}$ isotop sind, können nicht anti-symmetrisch sein.*

Beweis Nehmen wir an, wir hätten eine total anti-symmetrische Quasigruppe $(Q, *)$, die isotop zu D_s ist, d.h. $x * y = \varphi_3(\varphi_1(x)\varphi_2(y))$. Damit ist $(c * x) * y = \varphi_3(\varphi_1(c * x)\varphi_2(y)) = \varphi_3(\varphi_1(\varphi_3(\varphi_1(c)\varphi_2(x)))\varphi_2(y))$. Mit $\tilde{\varphi} = \varphi_1 \circ \varphi_3$, $\tilde{c} =$

$\varphi_1(c)$, $\tilde{x} = \varphi_2(x)$ und $\tilde{y} = \varphi_2(y)$ folgt $(c * x) * y = \varphi_3(\tilde{\varphi}(\tilde{c}\tilde{x})\tilde{y})$. Da $(Q, *)$ total anti-symmetrisch ist, folgt, daß für alle $\tilde{c} \in D_s$ die Permutation $\tilde{\varphi}(\tilde{c}\tilde{x})$ eine anti-symmtrische Abbildung von D_s ist. Nach Satz 4 (Seite 30) ist damit auch $\tilde{\varphi}(\tilde{c}^{-1}\tilde{c}\tilde{x})\tilde{c}^{-1} = \tilde{\varphi}(\tilde{x})\tilde{c}^{-1} \in Ant(D_s)$ im Widerspruch zu Satz 26 (Seite 54).

Da $\mathbb{Z}_n$ keine anti-symmetrische Abbildung besitzt, gilt dies auch für alle Isotopien. □

Wenn die Vermutung stimmt, dann existiert kein Prüfziffersystem basierend auf einer einzelnen Quasigruppe der Ordnung 10. Falls es allerdings eine total anti-symmetrische Quasigruppe der Ordnung 10 geben sollte, dann bedeutet dies allerdings noch nicht, daß diese eine bessere Fehlererkennung der anderen Fehler (Zwillingsfehler, Sprungzwillingsfehler) bietet als ein Prüfziffersystem basierend auf der Diedergruppe D_5. Im nächsten Abschnitt werden wir zeigen, daß bestimmte Quasigruppen nicht alle Fehler erkennen können.

Für ungerade n gilt allerdings:

Satz 50 *Es existieren total anti-symmetrische Quasigruppen für alle ungeraden n.*

Beweis In $(\mathbb{Z}_n, +)$ sind die Abbildungen $\varphi(x) = c - x$ anti-symmetrisch für alle $c \in \mathbb{Z}_n$. Wir definieren nun $x * y := -x + y$ und haben damit $(c * x) * y = -(-c + x) + y = c - x + y$ und $*$ ist total anti-symmetrisch. □

4.9 Quasigruppen mit Vorzeichen

Dieser Abschnitt verallgemeinert den Begriff des Vorzeichens auf Quasigruppen.

Definition 22 *Eine (endliche) Quasigruppe $(Q, *)$ mit einem Homomorphismus $sgn : Q \to \{-1, +1\}$ heißt Quasigruppe mit Vorzeichen sgn. Ist sgn surjektiv, dann heißt das Vorzeichen* nicht-trivial. *Die Menge der positiven bzw. negativen Elemente wird mit Q^+ bzw. Q^- bezeichnet.*

Eigenschaften:

1. Besitzt $(Q, *)$ eine Links- oder Rechtseins e, dann ist $sgn(e) = 1$.
2. $Q = Q^+ \cup Q^-$ und $Q^+ \cap Q^- = \emptyset$.
3. Es gilt $|Q^+| = |Q^-|$, falls das Vorzeichen auf Q nicht trivial ist, sonst $Q^+ = Q$ und $Q^- = \emptyset$.

zu 1: $sgn(e) = sgn(e * e) = sgn(e)sgn(e) = 1$.
zu 2: klar.
zu 3: Sei $x \in Q^- \neq \emptyset$, dann ist $x * x \in Q^+$, denn $sgn(x * x) = sgn(x)sgn(x) = 1$, also ist das Vorzeichen sgn nicht trivial. Es ist $x * Q^+ \subseteq Q^-$, und da $x * y_1 \neq x * y_2$ für $y_1 \neq y_2$ gilt, haben wir $|Q^+| \leq |Q^-|$. Ebenso gilt $x * Q^- \subseteq Q^+$ und damit $|Q^-| \leq |Q^+|$. Folglich haben wir $|Q^+| = |Q^-|$. Ist das Vorzeichen trivial, dann gilt $Q^- = \emptyset$ und $Q = Q^+$.

Satz 51 *Quasigruppen mit ungerader Ordnung besitzen nur die triviale Vorzeichenfunktion $sgn(x) = 1$.*
Eine Quasigruppe der Ordnung $2k$ besitzt ein nicht-triviales Vorzeichen genau dann, wenn sie eine Unterquasigruppe der Ordnung k besitzt.

Beweis Falls eine Quasigruppe ein nicht-triviales Vorzeichen besitzt, dann gilt $|Q^+| = |Q^-|$ und die Anzahl der Elemente der Quasigruppe ist gerade, denn $|Q| = |Q^+| + |Q^-| = k + k = 2k$. Q^+ ist in diesem Fall eine Unterquasigruppe der Ordnung k, denn wenn $x, y \in Q^+$ sind, dann gilt $sgn(x * y) = sgn(x)sgn(y) = 1 \cdot 1 = 1$ und es folgt $x * y \in Q^+$.
Andererseits können wir mit einer Unterquasigruppe U der Ordnung k ein Vorzeichen definieren durch

$$sgn(x) = \begin{cases} 1 & \text{falls } x \in U \\ -1 & \text{sonst.} \end{cases}$$

Wir müssen zeigen, daß $sgn(x * y) = sgn(x)sgn(y)$ gilt. Dazu sei $x \in U$. Für $y \in U$ sind auch die Elemente $x * y \in U$. Da $x * y_1 \neq x * y_2$ für $y_1 \neq y_2$ gilt, ist $x * U = U$. Aus diesem Grund ist für $z \notin U$ auch $x * z \notin U$, denn wenn $x * z \in U$ wäre, dann gäbe es ein $y \in U$ mit $x * z = x * y$ und damit ist $y = z$, Widerspruch. Genauso folgt, daß für $z \notin U$ auch $z * x \notin U$ ist. Nun sei $z \in \bar{U} := Q \setminus U$. Wir haben gezeigt, daß für $x \in U$, $z * x$ und $x * z$ Elemente von $\bar{U}$ sind, d.h. $z * U = U * z = \bar{U}$, denn die Elemente $z * x$ bzw. $x * z$ sind für verschiedene x ebenfalls verschieden und $|U| = |\bar{U}|$. Ist $y \in \bar{U}$, dann muß $z * y, y * z \in U$ gelten, denn sonst gäbe es ein $x \in U$ mit $z * y = z * x$ bzw. $y * z = x * z$ und es würde $x = y$ und daher ein Widerspruch folgen. Damit haben wir gezeigt, daß sgn ein Homomorphismus ist. □

Theorem 19 *Sei Q eine Quasigruppe der Ordnung $4k + 2$ mit nicht trivialem Vorzeichen, dann besitzt Q keine vollständige Abbildung.*

Beweis Siehe Beweis auf der Seite 48.

Wir haben bereits gezeigt, daß in einer Isotopieklasse entweder alle oder keine Quasigruppe eine vollständige Abbildung besitzt. Daher wissen wir, daß jede Quasigruppe der Ordnung $4k+2$, die zu einer Quasigruppe mit Vorzeichen isotop ist, keine vollständige Abbildung besitzt. Also gilt:

Korollar 20 *Prüfziffersysteme zur Basis $4k+2$ über Quasigruppen, von denen wenigstens eine isotop zu einer Quasigruppe mit Vorzeichen ist, erkennen nicht alle Zwillings- und auch nicht alle Sprungzwillingsfehler.*

Das Gleiche gilt auch für alle Parastrophien dieser Quasigruppen.

4.9.1 Beispiele

Die Quasigruppe $(\mathbb{Z}_n, *)$, n gerade, mit

$$x * y = \begin{cases} (x+y) \bmod n & \text{falls } x \text{ gerade} \\ (x-y-k) \bmod n & \text{falls } x \text{ ungerade,} \end{cases}$$

$k \in \mathbb{Z}_n$ gerade, besitzt das nicht-triviale Vorzeichen

$$sgn(x) = \begin{cases} 1 & \text{falls } x \text{ gerade} \\ -1 & \text{falls } x \text{ ungerade,} \end{cases}$$

denn die Menge der geraden Zahlen bildet eine Unterquasigruppe von $(\mathbb{Z}_n, *)$. Dies wird besonders deutlich, wenn wir die Zeilen und Spalten so permutieren, daß zuerst die geraden und dann die ungeraden Zahlen kommen. Für $n = 10, k = 0$ haben wir z.B. die Quasigruppe

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

Wir zeigen, daß $(\mathbb{Z}_n, *)$ für alle geraden n, k eine Quasigruppe definiert. Wir setzen $y := a - x$, falls x gerade und $y := x - a - k$, falls x ungerade ist, und haben

so eine eindeutige Lösung der Gleichung $x * y = a$ mit vorgegebenen $x, a \in \mathbb{Z}_n$. Sind $y, b \in \mathbb{Z}_n$ vorgegeben und y und b entweder beide gerade oder beide ungerade, dann ist $x := b - y$ gerade und Lösung der Gleichung $x * y = b$. Falls y und b unterschiedliche Vorzeichen haben, dann ist $x := b + y + k$ ungerade und löst die Gleichung $x * y = b$. Um zu zeigen, daß diese Lösung eindeutig ist, nehmen wir an, daß $x_1 * y = x_2 * y = b$ gilt. Haben x_1 und x_2 das gleiche Vorzeichen, dann können wir y und ggf. k auf beiden Seiten der Gleichung kürzen und erhalten $x_1 = x_2$. Gilt dagegen x_1 ungerade und x_2 gerade, so haben wir die Gleichung $x_1 - y - k = x_2 + y$ bzw. $x_1 = x_2 + 2y + k$. Auf der rechten Seite der Gleichung steht eine gerade, auf der linken eine ungerade Zahl, da n gerade ist haben wir daher einen Widerspruch. Damit folgt, daß $(\mathbb{Z}_n, *)$ eine Quasigruppe ist. □

Weitere Beispiele können wir aus der Arbeit von ECKER und POCH entnehmen. Sie definieren über den folgenden Quasigruppen der Ordnung $2n = 4k + 2$ ein Prüfziffersystem (siehe letzten Abschnitt). Für $x, y \in \mathbb{Z}_n$ sei $x *_1 y$ bzw. $x *_2 y$ definiert durch:

$$\begin{array}{rcl}
0 \le x, y \le n-1 & : & x *_1 y = (y - x) \bmod n \\
0 \le x \le n-1, n \le y \le 2n-1 & : & x *_1 y = n + ((y - x) \bmod n) \\
n \le x \le 2n-1, 0 \le y \le n-1 & : & x *_1 y = n + ((-x - y) \bmod n) \\
n \le x, y \le 2n-1 & : & x *_1 y = (y - x + 1) \bmod n
\end{array}$$

bzw.

$$\begin{array}{rcl}
0 \le x, y \le n-1 & : & x *_2 y = (y - x) \bmod n \\
0 \le x \le n-1, n \le y \le 2n-1 & : & x *_2 y = n + ((y + x) \bmod n) \\
n \le x \le 2n-1, 0 \le y \le n-1 & : & x *_2 y = n + ((y - x + 1) \bmod n) \\
n \le x, y \le 2n-1 & : & x *_2 y = (-y + x + 1) \bmod n
\end{array}$$

Auch diese Quasigruppen besitzen ein nicht triviales Vorzeichen, denn für $0 \le x, y \le n-1$ gilt $0 \le x *_{1,2} y \le n-1$ und damit habe wir eine Unterquasigruppe der Ordnung $2k+1$. Also können wir Korollar 20 (Seite 96) anwenden und es folgt, daß über dieser Quasigruppe kein Prüfziffersystem existiert, welches alle (Sprung-)Zwillingsfehler erkennt.

Im Gegensatz zu den Gruppen, muß eine Quasigruppe der Ordnung $4k + 2$ nicht unbedingt ein nicht-triviales Vorzeichen besitzen, wie das folgende Beispiel zeigt.

$*$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	6	2	9	4	3	7	5	1	0	8
2	5	6	4	8	7	3	1	9	2	0
3	9	5	6	7	0	1	3	8	4	2
4	3	8	5	6	1	2	9	0	7	4
5	8	3	0	5	6	9	4	2	1	7
6	7	0	3	2	5	6	8	4	9	1
7	2	4	7	1	9	8	0	3	6	5
8	4	7	1	9	8	0	2	6	5	3
9	1	9	8	0	2	4	7	5	3	6

Die Identität ist eine vollständige Abbildung dieser Quasigruppe, denn die Elemente $x * x$ auf der Diagonalen sind paarweise verschieden. Nach Theorem 19 kann sie daher nicht isotop zu einer Quasigruppe mit nicht-trivialem Vorzeichen sein, insbesondere besitzt sie selbst nur das triviale Vorzeichen.

4.10 Total anti-symmetrische Abbildungen

Wenn wir den Ansatz im Abschnitt „Total anti-symmetrische Quasigruppen" mit Kapitel 1 vergleichen (insbesondere Satz 1, Seite 15), dann ist der deutlichste Unterschied, daß wir die Prüfziffer nur mit einer Quasigruppe berechnet haben, ohne eine Permutation auf die einzelnen Elemente anzuwenden.

Wir untersuchen nun diese Möglichkeit mit dem Ansatz

$$((\dots((\varphi^n(x_n) * \varphi^{n-1}(x_{n-1})) * \varphi^{n-2}(x_{n-2})) * \dots) * \varphi(x_1)) * x_0 = c \qquad (4.13)$$

wobei $(Q, *)$ eine Quasigruppe und φ eine Permutation ist.

Zunächst zeigen wir, daß dies im wesentlichen dem vom Ecker und Poch vorgeschlagenen Ansatz entspricht. Sie definieren die Prüfziffer durch

$$x_0 := (\dots((x_n * \varphi(x_{n-1})) * \varphi^2(x_{n-2})) * \dots) * \varphi^{n-1}(x_1) \qquad (4.14)$$

und verzichten auf das Erkennen der Vertauschung $x_0 \leftrightarrow x_1$. Dies erscheint aufgrund der Tatsache, daß die Häufigkeit der Fehler mit wachsender Stellenzahl zunimmt, als wenig sinnvoll. Außerdem können wir auf die einzelnen Stellen x_i die Permutation φ^{-n} anwenden, ohne daß die Anti-Symmetrie-Eigenschaft der durch die Gleichung definierten n-Quasigruppe verlorengeht (Satz 16, Seite 67). Wir erhalten somit die Form 4.13, wobei es besser ist, die Prüfziffer implizit durch die genannte Gleichung zu bestimmen.

Für eine Quasigruppe reicht es nicht aus, daß φ eine anti-symmetrische Abbildung ist. Wir benötigen zusätzlich noch die Bedingung

$$(c * \varphi(x)) * y = (c * \varphi(y)) * x \quad \Rightarrow \quad x = y,$$

damit alle Nachbarvertauschungen erkannt werden. Wir nennen eine Permutation die anti-symmetrisch ist und zusätzlich diese Bedingung erfüllt *total anti-symmetrisch*. In einer Gruppe sind anti-symmetrische Abbildungen auch total anti-symmetrisch, für Quasigruppen gilt dies aber i.allg. nicht.

4.10.1 Konstruktion

Total anti-symmetrische Abbildungen einer Quasigruppen $(Q, *)$ können ganz ähnlich wie die anti-symmetrischen Abbildungen einer Gruppe konstruiert werden. In einer Quasigruppe haben wir allerdings im allgemeinen kein inverses Element. Dieses Problem können wir aber leicht lösen, indem wir die Parastrophien $(Q, /)$ und $(Q, \backslash)$ betrachten. Dann sind die Implikationen

$$\begin{aligned} \varphi(x) * y = \varphi(y) * x \quad &\Rightarrow \quad x = y \\ (c * \varphi(x)) * y = (c * \varphi(y)) * x \quad &\Rightarrow \quad x = y \end{aligned}$$

äquivalent zu

$$\begin{aligned} \varphi(x) = (\varphi(y) * x)\backslash y \quad &\Rightarrow \quad x = y \\ \varphi(x) = c/(((c * \varphi(y)) * x)\backslash y) \quad &\Rightarrow \quad x = y. \end{aligned}$$

Damit erhalten wir einen Algorithmus, der die total anti-symmetrischen Abbildungen einer Quasigruppe konstruiert, indem wir statt des Elements $m_{k,j*k*i^{-1}}$ bei Gruppen, das Element $m_{k,(j*k)\backslash i}$ und für alle $c \in Q$ die Elemente $m_{k,c/(((c*j)*k)\backslash i)}$ streichen (vgl. Seite 39). Mit diesem Algorithmus können wir sehr effektiv die total anti-symmetrischen Abbildungen einer vorgegebenen Quasigruppe konstruieren. Wir haben nun für verschiedene Quasigruppen die total anti-symmetrischen Abbildungen bestimmt und deren Erkennungsquote der anderen Fehlerarten untersucht. Dabei fanden wir eine Quasigruppe, die eine bessere Fehlererkennung bietet als die Diedergruppe.

Zum Vergleich geben wir zunächst die Erkennungsquote des von Ecker und Poch definierten „Shift-Code" an. Sie benutzen die im Abschnitt 4.9.1 (Seite 97) definierten Quasigruppen mit der Prüfgleichung 4.14 und der Permutation $\varphi(x) := x + 1$. Damit erzielten sie die folgenden Fehlererkennungsraten für die Quasigruppe $*_1$ der Ordnung 10: Sprungtranspositionen (Spr.): 84,89%, Zwillingsfehler (Zw.): 71,11%, Sprungzwillingsfehler (SprZw.): 87,67% und phonetische Fehler (Ph.): 76,19%.

Bei der zweiten angegebenen Quasigruppe stellten wir fest, daß diese zusammen mit φ nicht alle Nachbarvertauschungen erkennt. Es gilt für $2n = 4k + 2$, $k > 1$:

$$0 *_2 \varphi(3k+2) = 0 *_2 (3k+3) = 2k + 1 + ((3k+3) \bmod 2k+1) = 3k+3$$

und

$$(3k+2) *_2 \varphi(0) = (3k+2) *_2 1 = 2k + 1 + ((1 - 3k - 2 + 1) \bmod 2k+1) = 3k+3.$$

Folglich ist $(3k+2) *_2 \varphi(0) = 0 *_2 \varphi(3k+2)$.

Das Ergebnis von ECKER und POCH [9, Seite 299] ist für diese Quasigruppe daher falsch.

Bei der Diedergruppe fanden wir total anti-symmetrische Permutationen, die eine deutlich höhere Fehlererkennung bieten als der Shift-Code von ECKER und POCH.

Ordnung	Permutation	Spr.	Zw.	SprZw.	Ph.
6	[034152]	82,22%	86,67%	82,22%	80,00%
	[305214]	82,22%	86,67%	82,22%	100,00%
8	[07526431]	89,29%	100,00%	89,29%	91,43%
	[43571602]	92,86%	92,86%	92,86%	97,14%
10	[0458613297]	92,00%	95,56%	92,00%	90,48%
	[0542978136]	92,00%	91,11%	92,00%	100,00%
	[7046913258]	94,22%	95,56%	94,22%	96,83%

Bei der Suche nach anderen Quasigruppen, die eine bessere Fehlererkennung haben als die Diedergruppe, fanden wir die Quasigruppe $(\mathbb{Z}_n, *)$, n gerade, definiert durch

$$x * y = \begin{cases} (x+y) \bmod n & \text{falls } x \text{ gerade} \\ (x-y-2) \bmod n & \text{falls } x \text{ ungerade} \end{cases}$$

(vgl. Abschnitt 4.9.1) und die folgenden total anti-symmetrischen Abbildungen:

Ordnung	Permutation	Spr.	Zw.	SprZw.	Ph.
6	[013425]	82,22%	86,67%	82,22%	100,00%
	[014352]	82,22%	86,67%	82,22%	100,00%
8	[12053467]	92,86%	100,00%	92,86%	94,29%
	[01526374]	92,86%	100,00%	92,86%	100,00%
10	[0137268459]	92,00%	95,56%	92,00%	100,00%
	[0147389625]	92,00%	95,56%	92,00%	100,00%
	[2096813574]	94,22%	95,56%	94,22%	96,83%

Mit der Permutation [2096813574] erreichen wir eine Fehlererkennung von 99,89% aller nicht zufälligen Fehler (einschließlich der Einzelfehler und der Nachbarvertauschungen, die zu 100% erkannt werden). Die Permutation [0147389625] bietet eine Fehlererkennung von 99,87%. Sie hat den Vorteil, daß die 0 fixiert wird, womit führende Nullen die Prüfziffer nicht verändern und Formatfehler erkannt werden können. Im Vergleich zur Permutation [0542978136] der Diedergruppe erkennt dieses Prüfziffersystem mehr Fehler und ist diesem daher vorzuziehen.

Schlußbemerkung

Wir haben gesehen, daß das Problem, ein Prüfziffersystem zur Basis 10 zu bestimmen, welches alle Sprung-/Zwillingsfehler, alle Sprungtranspositionen und alle phonetischen Fehler erkennt, keine naheliegende Lösung besitzt. Die Frage, ob es überhaupt ein solches Prüfziffersystem gibt, bleibt offen. Die Existenz zu widerlegen, erscheint allerdings sehr schwer, da ein entsprechender Beweis auf den speziellen Eigenschaften der Zahl 10 beruhen muß, denn zur Basis 11 existiert ein entsprechendes Prüfziffersystem. Trotzdem können wir mit dem im letzten Abschnitt angegebenen Prüfziffersystem 99,89% aller nicht zufälligen Fehler erkennen und somit eine sehr hohe Fehlererkennung gewährleisten.

Literaturverzeichnis

[1] J. Aczél, V.D. Belousov, M. Hosszú. *Generalized associativity and bisymmetry on quasigroups*. Acta Math. Acad. Sci. Hungar 11 (1960), 127-136.

[2] P. Batemann. *Complete mappings of infinite groups*. Amer. Math. Monthly 57 (1950), 621-622.

[3] J. A. Beachy, W. D. Blair. *Abstract Algebra, Second Edition*. Waveland Press, Illinois 1996.

[4] V.D. Belousov. *Extensions of quasigroups*. Bull. Akad. Stiince RSS Moldoven No. 8 (1967), 3-24. (Russisch)

[5] G.B. Belyavskaya, A.Kh. Tabarov. *Characteristic of linear and alinear quasigroups*. Diskretn. Mat. 4, No.2 (1992), 142-147. (Russisch)

[6] O. Chein, H.O. Pflugfelder, J.D.H. Smith. *Quasigroups and Loops, Theory and Applications*. Sigma Series in Pure Mathematics, Volume 8 (1990), Heldermann Verlag Berlin.

[7] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson. *Atlas of Finit Groups*. Oxford 1985.

[8] J. Dénes, A.D. Keedwell. *Latin Squares and theire Applications*. New York: Academic Press (1974).

[9] A. Ecker, G. Poch. *Check Character Systems*. Computing 37 (1986), 277-301.

[10] J. A. Gallian, M. Mullin. *Groups with Anti-symmetric Mappings*. Archive der Math. 65 (1995), 273-280.

[11] D. Gorenstein. *Classifying the finit simple groups*. Bull. Amer. Math. Soc. 14 (1986), 1-98.

[12] H.P. Gumm. *A New Class of Check-Digit Methods for Arbitrary Number Systems*. IEEE Tran. Inf. Th. 31 (1985), 102-105.

[13] H.P. Gumm. *Encoding of Numbers to Detect Typing Errors.* Inter. J. Applied Eng. Ed. 2 (1986), 61-65.

[14] M. Hall, L.J. Paige. *Complete mappings of finite groups.* Pacific J. Math. 5 (1955), 541-549.

[15] H.B. Mann. *The construction of orthogonal latin squares.* Ann. Math. Statistics 13 (1942), 418-423.

[16] B. D. McKay, E. Rogoyski. *Latin Squares of Order 10.* The Electronic Journal of Combinatorics 2 (1995) #N3.

[17] K. Meyberg. *Algebra, Teil 1.* Carl Hanser Verlag München Wien 1980.

[18] L.J. Paige. *A note on finite abelian groups.* Bull. Amer. Math. Soc. 53 (1947), 590-593.

[19] L.J. Paige. *Complete mappings of finite groups.* Pacific J. Math. 1 (1951), 111-116.

[20] R. Schauffler. *Die Assoziativität im Ganzen, besonders bei Quasigruppen.* Math. Z. 67 (1957), 428-435.

[21] R.-H. Schulz. *Codierungstheorie. Eine Einführung.* Vieweg V. Braunschweig/Wiesbaden 1991.

[22] R.-H. Schulz. *A note on Check character Systems using Latin squares.* Discr. Math. 97 (1991) 371-375.

[23] H. Siemon. *Anwendungen der elementaren Gruppentheorie in Zahlentheorie und Kombinatorik.* Stuttgart: Klett-Verlag 1981.

[24] J. Širáň, M. Škoviera. *Groups with sign structure and theire antiautomorphisms.* Discr. Math. 108 (1992), 189-202.

[25] N. J. A. Sloane, S. Plouffe. *The Encyclopedia of Integer Sequences.* Academic Press, San Diego, 1995.

[26] S. K. Stein. *On the foundations of quasigroups.* Trans. Amer. Math. Soc. 85 (1957), 228-256.

[27] J. Verhoeff. *Error detecting decimal codes.* Math. Centre Tracts 29, Amsterdam 1969.

[28] Steven J. Winters. *Error Detecting Schemes Using Dihedral Groups.* UMAP Journal 11 (1990), 299-308.

Erklärung

Hiermit versichere ich, daß ich diese Arbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Marburg, den 6. März 1998