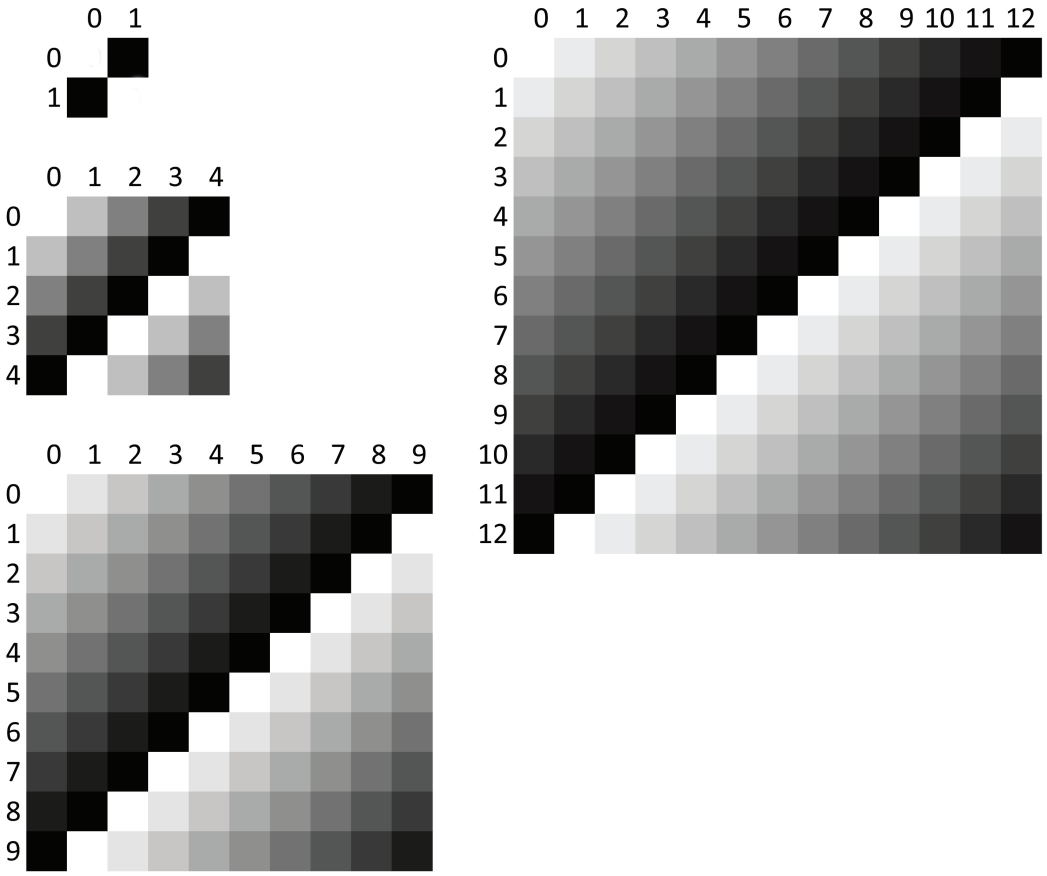
Algebra
Gruppentheorie
Skript zur Vorlesung

Michael Gieding
Pädagogische Hochschule Heidelberg
Institut für Mathematik und Informatik

Sommersemester 2020

1 Was sind algebraische Gruppen?

Kopie.jpg



Mathematik ist ist das Erkennen von Mustern und Strukturen

1.1 Beispiele und Gegenbeispiele für Gruppen

1.1.1 Gruppe?

Eine nichtleere Menge (z.B. die Menge der ganzen Zahlen) zusammen mit einer Operation (z.B. der Addition) heißt algebraische Struktur. Gruppe darf sich eine algebraische Struktur nennen, wenn bezüglich der verwendeten Operation bestimmte Eigenschaften gelten. Welche Eigenschaften das sind werden Sie mittels der folgenden algebraischen Strukturen untersuchen.

1.1.2 Restklassengruppen

Restklassen

Es sei $\mathbb{Z}$ die Menge der ganzen Zahlen. Die Zahlen $-6, -3, 0, 3, 6, 9, 12$ haben eine gemeinsame Eigenschaft: sie sind alle durch 3 teilbar. Wählen wir nun die Zahlen $-5, -2, 1, 4, 7, 10, 13$, so haben auch diese Zahlen eine gemeinsame Eigenschaft: sie lassen alle bei Division durch 3 den Rest 1. Die gemeinsame Eigenschaft der Zahlen $-4, -1, 2, 5, 8, 11, 13$ besteht darin, bei Division durch 3 den Rest 2 zu lassen. Andere Reste können bei Division durch 3 nicht auftreten. Die Relation „*lässt bei Division durch* 3 *denselben Rest*“ ist eine Äquivalenzrelation. Wir geben eine allgemeine Definition für den Begriff an:

Definition 1.1.1

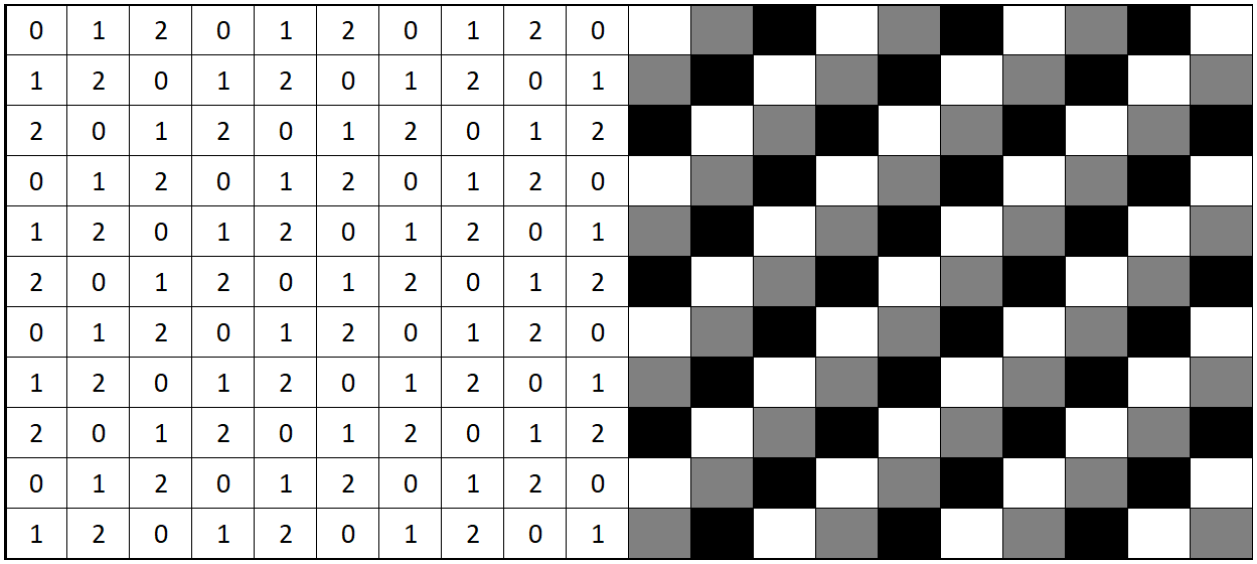
$a \equiv b \ mod \ m$

Es seien a, b, m ganze Zahlen. Die Zahl a ist kongruent b modulo m, wenn a und b bei Division durch m denselben Rest r lassen.

Mathematik ist vor allem die Untersuchung von Mustern und Strukturen. Wir veranschaulichen uns die Idee der Relation a ist kongruent b modulo 3 indem wir uns zunächst die ersten natürlichen Zahlen aufzählen:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99
100	101	102	103	104	105	106	107	108	109

Jetzt ersetzen wir die aufgezählten Zahlen durch die Reste, die die jeweilige Zahl bei Division durch 3 lässt.



Obige Abbildung enstand aus einer Exceltabelle. Rechts wurden die linken Zellwerte bedingt formatiert.

Fall 1: Zellinhalt lässt bei Division durch 3 den Rest 0: weiße Zellfüllung,

Fall 2: Zellinhalt lässt bei Division durch 3 den Rest 1: graue Zellfüllung,

Fall 3: Zellinhalt lässt bei Division durch 3 den Rest 2: schwarze Zellfüllung.

Betrachtet man dass Muster linear, so lässt es sich wie folgt beschreiben: weiß, grau, schwarz, weiß, grau, schwarz, weiß, ... Wir haben es bezüglich des Moduls 3 mit genau drei Typen

von Zahlen zu tun: weiße Zahlen, graue Zahlen und schwarze Zahlen. Weiße Zahlen lassen bei Division durch 3 den Rest 0, graue Zahlen lassen bei Division durch 3 den Rest 1 und schwarze Zahlen lassen bei Division durch 3 den Rest 2. Andere Reste kann es bei Division durch 3 nicht geben. Interessant ist nun, die Regelmäßigkeit in der Aufzählung: Zahl die den Rest 0 lässt, Zahl, die den Rest 1 lässt, Zahl die den Rest 2 lässt. Die nun folgende Zahl, die wiederum durch 3 teilbar ist, hat zur davor genannten durch 3 teilbaren Zahl den Abstand 3 . Generell gilt: Zwei aufeinander folgende Zahlen, die bei Division durch 3 denselben Rest lassen, haben immer den Abstand 3 zueinander. Das legt den folgenden allgemeinen Satz nahe:

Satz 1.1.1

Wenn $a \equiv b \bmod m$, dann ist m ein Teiler der Differenz $a - b$.

Aufgabe 1.1.1

Beweisen Sie Satz 1.1

Sicher haben Sie die Relation „a kongruent b modulo m“ bereits gegoogelt und festgestellt, dass es Definitionen gibt, die die Behauptung von Satz 1.1 als definierende Eigenschaft verwenden. Das bedeutet, dass auch der folgende Satz gelten muss:

Satz 1.1.2

Es seien a, b, m drei ganze Zahlen. Wenn m die Diferenz $a - b$ teilt, dann lassen a und b bei Division durch m denselben Rest.

Aufgabe 1.1.2

Beweisen Sie Satz 1.2.

Hinweis: Falls Ihnen der allgemeine Beweis zunächst zu schwer fällt, versuchen Sie es zunächst für das konkrete Modul 3. Und wenn einem überhaupt nichts einfällt, kann man es ja mal indirekt versuchen.

Nach den beiden Sätzen 1.1 und 1.2 formulieren wir die Definition der Relation $a \equiv b \bmod m$ noch einmal:

Definition 1.1.2

$a \equiv b \bmod m$ reloaded

Es seien a, b, m ganze Zahlen. $a \equiv b \bmod m :\Leftrightarrow m|(a - b)$

Wir schauen uns noch einmal das Modul 3 an. Dieses Modul zerlegt die Menge der ganzen Zahlen in genau drei Typen: weiß, grau, schwarz, bzw. lässt bei Division durch 3 den Rest 0 oder 1 oder 2. Das verwendete „oder“ ist eigentlich ein „entweder oder“, denn jede Zahl lässt jeweils genau den jeweiligen Rest. $\mathbb{Z}$ wird in drei TeilMengen eingeteilt:

T1 $\overline{0} := \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$ bzw. $\overline{0} := \{a | a \in \mathbb{Z} \wedge \exists t \in \mathbb{Z} : t \cdot 3 + 0 = a\}$

T2 $\overline{1} := \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$ bzw. $\overline{1} := \{a | a \in \mathbb{Z} \wedge \exists t \in \mathbb{Z} : t \cdot 3 + 1 = a\}$

T3 $\overline{2} := \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$ bzw. $\overline{2} := \{a | a \in \mathbb{Z} \wedge \exists t \in \mathbb{Z} : t \cdot 3 + 2 = a\}$

Diese drei TeilMengen der ganzen Zahlen bilden eine sogenannte Klasseneinteilung der Menge der ganzen Zahlen:

1. Keine der drei Mengen $\overline{0}, \overline{1}, \overline{2}$ ist leer. (Die leere Menge ist bei Klasseneinteilungen nicht zugelassen.)

2. Je zwei der drei Mengen $\overline{0}, \overline{1}, \overline{2}$ sind disjunkt zueinander. D.h. jede ganze Zahl findet sich höchsten in einer der drei Klassen wieder.

3. $\overline{0} \cup \overline{1} \cup \overline{2} = \mathbb{Z}$, d.h. alle drei TeilMengen zusammen ergeben wieder die ganzen Zahlen.

Die Punkte 2. und 3. kann man auch so zusammenfassen: Jede ganze Zahl gehört zu genau einer der drei Mengen $\overline{0}, \overline{1}, \overline{2}$.
Genügt eine Einteilung einer Menge in gewisse TeilMengen, den drei Punkten 1., 2. und 3. , dann heißt eine solche Einteilung in TeilMengen eine Klasseneinteilung und die TeilMengen dürfen sich stolz Klassen nennen.
Die Zugehörigkeit einer ganzen Zahl zur entsprechenden Klasse richtet sich nach dem Rest, den diese Zahl bei Division durch 3 lässt. Wir wollen die Klassen $\overline{0}, \overline{1}, \overline{2}$ deshalb Restklassen modulo 3 nennen. Alle drei Klassen zusammen bilden eine Menge die aus drei Elementen besteht, die Menge der Restklassen modulo 3. Wir bezeichnen diese Menge mit $\mathbb{Z}_3$:

$$\mathbb{Z}_3 := \{\overline{0}, \overline{1}, \overline{2}\}$$

Aufgabe 1.1.3

Schreiben Sie alle Elemente der Menge $\mathbb{Z}_5$ auf und erläutern Sie diese Elemente.

Restklassengruppen

Zahlen sind dazu da, um mit ihnen zu rechnen. Letztlich sind Zahlen auch nichts anderes als Mengen:

- Eine gebrochene Zahl ist eine Menge von Brüchen, die durch Kürzen oder Erweitern auseinander hervorgehen.

- Brüche bestehen aus natürlichen Zahlen. Jede natürliche Zahl ist eine Menge von Mengen, die jeweils gleichmächtig zueinander sind. Die Zahl *Drei* vereinigt in sich zum Beispiel alle Mengen, die etwa zu der Menge $\{\diamond, \nabla, \Delta\}$ gleichmächtig sind.

- Eine ganze Zahl ist eine Menge von geordneten Paaren natürlicher Zahlen, die alle auf dem Zahlenstrahl jeweils denselben gerichteten Abstand haben.z.B. wäre

  $$-2 = \{(0,2), (1,3), (2,4), (3,5), (4,6), \ldots, (10001, 10003), \ldots\}$$

  (Sie vermuten richtig, jede ganze Zahl ist eine Äquivalenzklasse differenzengleicher Paare natürlicher Zahlen.)

Mit $\overline{0}, \overline{1}, \overline{2}$ haben wir wieder sowas wie besondere Zahlen. Wir sollten schauen, ob wir nicht ein paar vernünftige Regeln zum Rechnen mit diesen Zahlen finden. Letztlich bestehen unsere neuen Zahlen aus alten Zahlen. Es erscheint sinnvoll, sich das Rechnen mit den alten Zahlen noch einmal anzuschauen. Vieleicht entdecken wir gewisse Gesetzmäßigkeiten, die uns auf vernünftige Rechenregeln mit den neuen Zahlen, den Restklassen führen:

- $4 + 5 = 9$
  4 lässt bei Division durch 3 den Rest 1, 5 lässt bei Division durch 3 den Rest 2, die Summe 9 lässt bei Division durch 3 den Rest 0.

- $10 + 5 = 15$
  10 lässt bei Division durch 3 den Rest 1, 5 lässt bei Division durch 3 den Rest 2, die Summe 15 lässt bei Division durch 3 den Rest 0.

- $16 + 11 = 27$
  16 lässt bei Division durch 3 den Rest 1, 11 lässt bei Division durch 3 den Rest 2, die Summe 27 lässt bei Division durch 3 den Rest 0.

- $1 + 2 = 3$
  1 lässt bei Division durch 3 den Rest 1, 2 lässt bei Division durch 3 den Rest 2, die Summe 3 lässt bei Division durch 3 den Rest 0.

- $a + b = c$
  a lässt bei Division durch 3 den Rest 1, b lässt bei Division durch 3 den Rest 2, die Summe c lässt bei Division durch 3 den Rest 0.

Der letzte Aufzählungspunkt ist natürlich nur eine Vermutung und bedarf eines Beweises und das vorliegende wäre ein schlechtes mathematisches Script, wenn jetzt bemerkt werden würde: Der Leser überzeuge sich davon (Übungsaufgabe).

Aufgabe 1.1.4

Beweisen Sie: Wenn man zu einer ganzen Zahl, die bei Division durch 3 *den Rest* 1 *lässt, eine ganze Zahl addiert, die bei Division durch* 3 *den Rest* 2 *lässt, dann erhält man eine durch* 3 *teilbare ganze Zahl.*

Aufgabe 1.1.5

Entwerfen Sie eine zur obigen Aufzählung analoge Aufzählung zum Rechnen mit Restklassen, nur die Reste sollten andere sein.

Allgemein scheint die folgende Rechenregel sinnvoll zu sein: Man addiert zwei Restklassen, indem man jeweils einen beliebigen Vertreter aus jeder Restklasse nimmt, diese beiden addiert und dann die Restklasse bestimmt, in der die eben errechnete Summe liegt:

Definition 1.1.3

Restklassenaddition
$\overline{a} \oplus \overline{b} := \overline{a + b}$

Aufgabe 1.1.6

Erläutern Sie, warum in Definition 1.3 zwei verschiedene Zeichen für die Addition ver-

wendet werden und was diese beiden Zeichen im Speziellen bedeuten.

Aufgabe 1.4 war ein Spezialfall zur sogenannten Wohldefiniertheit der Addition von Restklassen. Anders ausgedrückt: Mit Aufgabe 1.4 haben Sie für einen Spezialfall die sogenannte Repäsentantenunabhängigkeit der Restklassenaddition bewiesen. Die nächste Übungsaufgabe zielt auf einen analogen allgemeinen Beweis der Wohldefiniertheit der Restklassenaddition ab.

Aufgabe 1.1.7

Beweisen Sie: Definition 1.3 ist für Restklassen (ein und desselben Moduls) repräsentantenunabhängig.

Zusammenfassend haben wir jetzt eine Menge ($\mathbb{Z}_3$), die aus drei Restklassen ($\overline{0}, \overline{1}, \overline{2}$) besteht und eine Addition ($\oplus$) dieser Restklassen. Eine Menge zusammen mit einer auf ihr definierten Operation nennt man eine algebraische Struktur. Unsere Untersuchungen werden zeigen, dass die Struktur $[\mathbb{Z}_3, \oplus]$ eine sogenannte Gruppe ist.
Hierzu werden wir zunächst die sogenannte Verknüpfungstafel der Struktur $[\mathbb{Z}_3, \oplus]$ untersuchen. In effizienter Art und Weise werden hier alle möglichen Additionen der drei Restklassen aufgeschrieben.

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Natürlich kann man auch eine Restklassenmultiplikation definieren.

Definition 1.1.4

Restklassenmultiplikation
$\overline{a} \odot \overline{b} := \overline{a \cdot b}$

Aufgabe 1.1.8

Stellen Sie die Verknüpfungstafeln für folgende Strukturen auf:

a) $[\mathbb{Z}_4, \oplus]$

b) $[\mathbb{Z}_4, \odot]$

c) $[\mathbb{Z}_5, \oplus]$

d) $[\mathbb{Z}_5, \odot]$

e) $[\mathbb{Z}_6, \oplus]$

f) $[\mathbb{Z}_6, \odot]$

g) $[\mathbb{Z}_7, \oplus]$

h) $[\mathbb{Z}_7, \odot]$

i) $[\mathbb{Z}_{256}, \oplus]$

Hinweis: Bei den multiplikativen Strukturen wird die Restklasse $\overline{0}$ nicht für die Verknüpfungstafel verwendet. (So wie man bei der Multiplikation natürlicher Zahlen, die 0 gern außen vor lässt.)

Aufgabe 1.1.9

Was hat Aufgabe 1.8.i) mit Photoshop zu tun?

Aufgabe 1.1.10

Generieren Sie eine Verknüpfungstafel für $[\mathbb{Z}_{256}, \oplus]$ *als Graustufengrafik mit Excel.*

1.2 Definition des Begriffs Gruppe und weitere Beispiele

1.2.1 Gruppendefinition

Definition 1.2.1

Algebraische Gruppe:
Es sei G *eine nichtleere Menge auf der eine zweistellige Operation* $\circ$ *definiert ist.* $[G, \circ]$ *heißt Gruppe, wenn die folgenden Eigenschaften erfüllt sind:*

1. *Abgeschlossenheit von* $\circ$ *auf* G
   $\forall a, b \in G : a \circ b \in G$

2. *Assoziativität von* $\circ$ *aug* G
   $\forall a, b, c \in G : (a \circ b\ ) \circ c = a \circ (b \circ c)$

3. *Existenz des Neutral bzw. Einselementes in* G *bzgl.* $\circ$
   $\exists e \in G \forall a \in G : a \circ e = e \circ a = a$

4. *Existenz der inversen Elemente zu jedem Element auss* G
   $\forall a \in G \exists a^{-1} : a \circ a^{-1} = a^{-1} \circ a = e$

Sollte ferner $\forall a, b \in G\ a \circ b = b \circ a$ *gelten, so heißt* $[G, \circ]$ *kommutative bzw. abelsche* [1] *Gruppe.*

1.2.2 Die symmetrische Gruppe S_4

Definition 1.2.2

Bijektion
Eine eineindeutige Abbildung von einer Menge A *auf eine Menge* B *heißt Bijektion.*

Definition 1.2.3

Permutation
Eine Bijektion einer Menge auf sich selbst heißt Permutation.

Satz 1.2.1

Anzahl von Permutationen einer n-elementigen Menge
Es sei M eine Menge mit $|M| = n$. Die Anzahl der verschiedenen Permutationen von M auf sich selbst beträgt $n!$.

Aufgabe 1.2.1

Beweis von Satz 2.1
Beweisen Sie Satz 2.1.

Es sei $M = \{A, B, C, D\}$ eine vierelementige Menge. Wir generieren systematisch alle Permutationen von M auf sich selbst. Das Schema erkennen Sie sicher selbst und haben damit die Grundlage für den Beweis von Satz 2.1.

1	A	B	C	D
2	A	B	D	C
3	A	C	B	D
4	A	C	D	B
5	A	D	B	C
6	A	D	C	B
7	B	A	C	D
8	B	A	D	C
9	B	C	A	D
10	B	C	D	A
11	B	D	A	C
12	B	D	C	A
13	C	B	A	D
14	C	B	D	A
15	C	A	B	D
16	C	A	D	B
17	C	D	B	A
18	C	D	A	B
19	D	B	C	A
20	D	B	A	C
21	D	C	B	A
22	D	C	A	B
23	D	A	B	C
24	D	A	C	B

Wir führen je zwei Permutationen nacheinander aus und erhalten die folgende Verknüfungstafel:

Die symmetrische Gruppe S4

∘	ABCD	ABDC	ACBD	ACDB	ADBC	ADCB	BACD	BADC	BCAD	BCDA	BDAC	BDCA	CABD	CADB	CBAD	CBDA	CDAB	CDBA	DABC	DACB	DBAC	DBCA	DCAB	DCBA
ABCD	ABCD	ABDC	ACBD	ACDB	ADBC	ADCB	BACD	BADC	BCAD	BCDA	BDAC	BDCA	CABD	CADB	CBAD	CBDA	CDAB	CDBA	DABC	DACB	DBAC	DBCA	DCAB	DCBA
ABDC	ABDC	ABCD	ACDB	ACBD	ADCB	ADBC	BADC	BACD	BDCA	BDAC	BCDA	BCAD	CADB	CABD	CBDA	CBAD	CDBA	CDAB	DACB	DABC	DBCA	DBAC	DCBA	DCAB
ACBD	ACBD	ADBC	ABCD	ADCB	ACDB	ABDC	BCAD	BCDA	BACD	BADC	BDCA	BDAC	CBAD	CBDA	CABD	CADB	CDBA	CDAB	DBAC	DBCA	DABC	DACB	DCBA	DCAB
ACDB	ACDB	ADCB	ABDC	ABCD	ADBC	ACBD	BCDA	BCAD	BADC	BACD	BDCA	BDAC	CBDA	CBAD	CADB	CABD	CDBA	CDAB	DBCA	DBAC	DACB	DABC	DCBA	DCAB
ADBC	ADBC	ABDC	ADCB	ABCD	ACDB	ACBD	BDAC	BDCA	BCAD	BCDA	BACD	BADC	CBAD	CBDA	CADB	CABD	CDAB	CDBA	DBAC	DBCA	DACB	DABC	DCAB	DCBA
ADCB	ADCB	ACDB	ACBD	ABCD	ABDC	ADBC	BDCA	BDAC	BCDA	BCAD	BADC	BACD	CBDA	CBAD	CDBA	CDAB	CADB	CABD	DBCA	DBAC	DCBA	DCAB	DACB	DABC
BACD	BACD	BADC	CABD	CADB	DACB	DABC	ABDC	ABCD	BDAC	BDCA	BCAD	BCDA	CADB	CABD	CDAB	CDBA	DABC	DACB	DBAC	DBCA	DCAB	DCBA	DABC	DACB
BADC	BADC	BACD	CADB	CABD	DABC	DACB	ABCD	ABDC	BDCA	BDAC	BCDA	BCAD	CABD	CADB	CDBA	CDAB	DACB	DABC	DBCA	DBAC	DCBA	DCAB	DABC	DACB
BCAD	BCAD	BDAC	CBAD	CDAB	DBAC	DCAB	ADBC	ADCB	ABDC	ABCD	BDCA	BDAC	CBDA	CBAD	CADB	CABD	CDBA	CDAB	DBCA	DBAC	DCBA	DCAB	DACB	DABC
BCDA	BCDA	BDCA	CBDA	CDBA	DBCA	DCBA	ADCB	ADBC	ABCD	ABDC	BDAC	BDCA	CBAD	CBDA	CADB	CABD	CDAB	CDBA	DBAC	DBCA	DCAB	DCBA	DACB	DABC
BDAC	BDAC	BDCA	CBAD	CDAB	DBAC	DCAB	ACDB	ACBD	ABCD	ABDC	BCAD	BCDA	CABD	CADB	CBAD	CBDA	CDAB	CDBA	DABC	DACB	DBAC	DBCA	DCAB	DCBA
BDCA	BDCA	BDAC	CBDA	CDBA	DBCA	DCBA	ACDB	ACBD	ABDC	ABCD	BCDA	BCAD	CBDA	CBAD	CADB	CABD	CDBA	CDAB	DBCA	DBAC	DCBA	DCAB	DACB	DABC
CABD	CABD	CADB	DABC	DACB	BADC	BACD	CBAD	CBDA	CABD	CADB	DBAC	DBCA	BADC	BACD	BCAD	BCDA	DBAC	DBCA	CABD	CADB	CBAD	CBDA	DBAC	DBCA
CADB	CADB	CABD	DACB	DABC	BACD	BADC	CBDA	CBAD	CADB	CABD	DBCA	DBAC	BACD	BADC	BCDA	BCAD	DBCA	DBAC	CADB	CABD	CBDA	CBAD	DBCA	DBAC
CBAD	CBAD	CBDA	DBAC	DBCA	BCAD	BCDA	CABD	CADB	CBAD	CBDA	DABC	DACB	BCAD	BCDA	BADC	BACD	DABC	DACB	CBAD	CBDA	CABD	CADB	DABC	DACB
CBDA	CBDA	CBAD	DBCA	DBAC	BCDA	BCAD	CADB	CABD	CBDA	CBAD	DACB	DABC	BCDA	BCAD	BACD	BADC	DACB	DABC	CBDA	CBAD	CADB	CABD	DACB	DABC
CDAB	CDAB	CDBA	DCAB	DCBA	BDAC	BDCA	DABC	DACB	CABD	CADB	DBAC	DBCA	BADC	BACD	BCAD	BCDA	DBAC	DBCA	CABD	CADB	CBAD	CBDA	DBAC	DBCA
CDBA	CDBA	CDAB	DCBA	DCAB	BDCA	BDAC	DACB	DABC	CADB	CABD	DBCA	DBAC	BACD	BADC	BCDA	BCAD	DBCA	DBAC	CADB	CABD	CBDA	CBAD	DBCA	DBAC
DABC	DABC	DACB	CABD	CADB	BADC	BACD	CBAD	CBDA	DABC	DACB	ABDC	ABCD	CBAD	CBDA	CABD	CADB	CDAB	CDBA	ABDC	ABCD	CBAD	CBDA	CABD	CADB
DACB	DACB	DABC	CADB	CABD	BACD	BADC	CBDA	CBAD	DACB	DABC	ABCD	ABDC	CBDA	CBAD	CADB	CABD	CDBA	CDAB	ABCD	ABDC	CBDA	CBAD	CADB	CABD
DBAC	DBAC	DBCA	DABC	DACB	BADC	BACD	CBAD	CBDA	DABC	DACB	ABDC	ABCD	CBAD	CBDA	CABD	CADB	CDAB	CDBA	ABDC	ABCD	CBAD	CBDA	CABD	CADB
DBCA	DBCA	DBAC	DACB	DABC	BACD	BADC	CBDA	CBAD	DACB	DABC	ABCD	ABDC	CBDA	CBAD	CADB	CABD	CDBA	CDAB	ABCD	ABDC	CBDA	CBAD	CADB	CABD
DCAB	DCAB	DCBA	DBAC	DBCA	BCAD	BCDA	CABD	CADB	CBAD	CBDA	DABC	DACB	BCAD	BCDA	BADC	BACD	DABC	DACB	CBAD	CBDA	CABD	CADB	DABC	DACB
DCBA	DCBA	DCAB	DBCA	DBAC	BCDA	BCAD	CADB	CABD	CBDA	CBAD	DACB	DABC	BCDA	BCAD	BACD	BADC	DACB	DABC	CBDA	CBAD	CADB	CABD	DACB	DABC

Aufgabe 1.2.2

Deckabbildungen des Quadrates
Eine Teilmenge der S_4 lässt sich als Deckabbildungen des Quadrates kennzeichnen. Benennen Sie alle Permutationen der S_4, die als Deckabbildungen des Quadrates interpretiert werden können und stellen. Die Menge der Permutationen, die als Deckabbildungen des Quadrates interpretiert werden können ist bezüglich der NAF von Abbildungen selbst eine Gruppe. Stellen Sie die Gruppentafel auf.

Zur Lösung hier eine leere Tabelle:

$\circ$								

Die Darstellung der S_4 ist in der angegebenen Form recht unübersichtlich. Wir kodieren wie folgt:

ABCD	1	CBAD	13
ABDC	2	CBDA	14
ACBD	3	CABD	15
ACDB	4	CADB	16
ADBC	5	CDBA	17
ADCB	6	CDAB	18
BACD	7	DBCA	19
BADC	8	DBAC	20
BCAD	9	DCBA	21
BCDA	10	DCAB	22
BDAC	11	DABC	23
BDCA	12	DACB	24

Mit dieser Kodierung stellt sich die S_4 wie folgt dar:

$\circ$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15	18	17	20	19	22	21	24	23
3	3	5	1	6	2	4	9	11	7	12	8	10	15	17	13	18	14	16	21	23	19	24	20	22
4	4	6	2	5	1	3	10	12	8	11	7	9	16	18	14	17	13	15	22	24	20	23	19	21
5	5	3	6	1	4	2	11	9	12	7	10	8	17	15	18	13	16	14	23	21	24	19	22	20
6	6	4	5	2	3	1	12	10	11	8	9	7	18	16	17	14	15	13	24	22	23	20	21	19
7	7	8	15	16	23	24	1	2	13	14	20	19	9	10	3	4	21	22	12	11	17	18	5	6
8	8	7	16	15	24	23	2	1	14	13	19	20	10	9	4	3	22	21	11	12	18	17	6	5
9	9	11	13	18	20	22	3	5	15	17	23	21	7	12	1	6	19	24	10	8	14	16	2	4
10	10	12	14	17	19	21	4	6	16	18	24	22	8	11	2	5	20	23	9	7	13	15	1	3
11	11	9	18	13	22	20	5	3	17	15	21	23	12	7	6	1	24	19	8	10	16	14	4	2
12	12	10	17	14	21	19	6	4	18	16	22	24	11	8	5	2	23	20	7	9	15	13	3	1
13	13	20	9	22	11	18	15	23	3	21	5	17	1	19	7	24	12	6	14	2	10	4	8	16
14	14	19	10	21	12	17	16	24	4	22	6	18	2	20	8	23	11	5	13	1	9	3	7	15
15	15	23	7	24	8	16	13	20	1	19	2	14	3	21	9	22	10	4	17	5	12	6	11	18
16	16	24	8	23	7	15	14	19	2	20	1	13	4	22	10	21	9	3	18	6	11	5	12	17
17	17	21	12	19	10	14	18	22	6	24	4	16	5	23	11	20	8	2	15	3	7	1	9	13
18	18	22	11	20	9	13	17	21	5	23	3	15	6	24	12	19	7	1	16	4	8	2	10	14
19	19	14	21	10	17	12	24	16	22	4	18	6	20	2	23	8	5	11	1	13	3	9	15	7
20	20	13	22	9	18	11	23	15	21	3	17	5	19	1	24	7	6	12	2	14	4	10	16	8
21	21	17	19	12	14	10	22	18	24	6	16	4	23	5	20	11	2	8	3	15	1	7	13	9
22	22	18	20	11	13	9	21	17	23	5	15	3	24	6	19	12	1	7	4	16	2	8	14	10
23	23	15	24	7	16	8	20	13	19	1	14	2	21	3	22	9	4	10	5	17	6	12	18	11
24	24	16	23	8	15	7	19	14	20	2	13	1	22	4	21	10	3	9	6	18	5	11	17	12

Aufgabe 1.2.3

Eindeutige Lösbarkeit von $a \circ x = y$ in der S_4
Untersuchen Sie, wie oft jedes Element der S_4 in jeder Zeile und jeder Spalte der Verknüpfungstafel auftaucht. Was hat Ihr Untersuchungsergebnis mit der Aufgabenüberschrift zu tun?

Aufgabe 1.2.4

Vierergruppen
Es sei $G = \{e, a, b, c\}$ eine vierelementige Menge und $\odot$ eine Verknüpfung auf G. Generieren Sie alle möglichen Gruppentafeln für $[G, \odot]$.

Hinweis: Ihr Untersuchungsergebnis aus Aufgabe 2.3 gilt für jede Gruppe.
Leere Tabellen zur Hilfe:

$\odot$	e	a	b	c
e				
a				
b				
c				

$\odot$	e	a	b	c
e				
a				
b				
c				

$\odot$	e	a	b	c
e				
a				
b				
c				

$\odot$	e	a	b	c
e				
a				
b				
c				

1.3 Eigenschaften von Gruppen und weitere Gruppendefinitionen

1.3.1 Sinn und Zweck dieses Abschnitts

Bei der Generierung von Verknüpfungstabellen ist Ihnen sicherlich aufgefallen, dass in dem Fall, da die jeweilige Verknüpfungstabelle eine Gruppe repräsentiert, in jeder Spalte und in jeder Zeile jedes Gruppenelement jeweils genau einmal auftaucht. Wenn das nicht nur ein Zufall sondern eine Gesetzmäßigkeit wäre, könnte uns dieses Wissen sehr hilfreich bei

der Untersuchung weiterer Gruppen sein. Wir werden an dieser Stelle die Definition des Begriffs Gruppe noch einmal genetisch entstehen lassen um dann die die beits aufgestellte Gruppendefinition genauer aus theoretischer Sicht zu untersuchen und ggf. die Definition des Begriffs algebraische Gruppe neu. bzw anders zu formulieren.

1.3.2 Genetische Entstehung des Begriffs algebraische Gruppe

algebraische Struktur

Definition 1.3.1

Algebraische Struktur
Eine Menge S zusammen mit einer Operation o oder Relation r auf dieser Menge nennt man algebraische Struktur.

Schreibweise:

$[S, o]$ *bzw* $[S, r]$

Halbgruppe

Definition 1.3.2

Halbgruppe
Eine algebraische Struktur $[H, \odot]$ heißt Halbgruppe, wenn $\odot$ auf H abgeschlossen und assoziativ ist.

D.h. es gilt:

- *(Abgeschlossenheit)* $\forall a, b \in H : a \odot b \in H$
- *(Assoziativität)* $\forall a, b, c \in H : (a \odot b) \odot c = a \odot (b \odot c)$.

Monoid

Definition 1.3.3

Monoid
Eine Halbgruppe $[M, \odot]$ heißt Monoid, wenn sie ein Einselement hat:

- *(Einselement)* $\exists e \in M \forall a \in M : e \odot a = a \odot e = a$

Gruppe

Definition 1.3.4

Gruppe

Ein Monoid $[G, \odot]$ heißt Gruppe, wenn jedes Element von G in G ein inverses Element bzgl. $\odot$ hat:

- *(inverse Elemente)* $\forall a \in G a^{-1} \in G : a \odot a^{-1} = a^{-1} \odot a = e$

abelsche Gruppe

Definition 1.3.5

Abelsche Gruppe
Wenn in einer Gruppe $[G, \odot]$ für alle Gruppenelemente a und b $a \odot b = b \odot a$ gilt, dann heißt $[G, \odot]$ kommutative oder abelsche Gruppe.

Bemerkungen zur Schreibweise

Additiv geschriebene Gruppen

Unsere bisherigen Definitionen waren in gewisser Weise "multiplikativ"geschrieben. Bezieht man sich auf eine Struktur mit einer Operation, die eher ädditivßu verstehen ist, spricht man häufig vom neutralen Element n und schreibt die Inversen als $-a$.

Wir geben im Folgenden die Langfassung einer Gruppendefinition, die additiv geschrieben ist und sich nicht auf bereits definierte Strukturen stützt.

Zusammenfassung: Gruppendefinition Langfassung

Definition 1.3.6

Gruppe, Langfassung
Eine nichtleere Menge G zusammen mit einer Verknüpfung $\oplus$ heißt Gruppe, wenn gilt:

- *$\oplus$ ist abgeschlossen auf G:* $\forall a, b \in G : a \oplus b \in G$
- *$\oplus$ ist assoziativ auf G:* $\forall a, b, c \in G : (a \oplus b) \oplus c = a \oplus (b \oplus c)$
- *Es gibt in G bzgl. $\oplus$ ein neutrales Element n:* $\exists n \in G \forall a \in G : a \oplus n = n \oplus a = a$
- *Jedes Element aus G hat in G ein inverses Element bzgl. $\oplus$:* $\forall a \in G \exists -a \in G : a \oplus -a = -a \oplus a = n$.

1.3.3 Links = Rechts

Linksinvers gleich Rechtsinvers

Satz 1.3.1

Linksinvers = Rechtsinvers
Es sei $[G, \odot]$ eine Gruppe.

$\forall a \in G : a \odot b = e \wedge c \odot a = e \Rightarrow b = c$

Beweis:

Es sei b das Linksinverse bzgl. $\odot$ von a. Also $b \odot a = e$ ist unsere Voraussetzung.

Wir multiplizieren b von rechts mit a:

(I)	$a \odot b = e \odot a \odot b$	(Wir haben a mit b von rechts multipliziert.)
(II)	$a \odot b = (b^{-1} \odot b) \odot a \odot b$	(Auch b hat ein Linksinverses b^{-1}.)
(III)	$a \odot b = b^{-1} \odot (b \odot a) \odot b$	(Assoziativität)
(IV)	$a \odot b = b^{-1} \odot e \odot b$	(b ist das Linksinverse von a)
(V)	$a \odot b = b^{-1} \odot b$	(Eigenschaften des Einselements)
(VI)	$a \odot b = e$	(b^{-1} ist das Linksinverse von b.)

Mit Gleichung (VI) haben wir gezeigt, dass das Linksinverse von a auch Rechtsinverses von a ist.

Linkseins gleich Rechtseins

Satz 1.3.2

Linkseins = Rechtseins
Es sei $[G, \otimes]$ eine Gruppe. Wenn $e \in G$ von links multipliziert Einselement von $[G, \otimes]$ ist, dann ist e auch von rechts multipliziert Einselement von G.

Beweis:

Es sei $[G, \otimes]$ Gruppe. Es gelte ferner für das Element $e \in G$ die folgende Eigenschaft: $\forall g \in G : e \otimes g = g$.

Wir haben zu zeigen, dass jetzt auch $g \otimes e = g$ für alle g aus G gilt.

Wir gehen von $(I) e \otimes g = g$ aus.

In Gleichung (I) multiplizieren wir von rechts auf beiden Seiten mit $g^{-1} \otimes g$ und erhalten:.

(II) $e \otimes g \otimes (g^{-1} \otimes g) = g \otimes (g^{-1} \otimes g)$.

Aus (II) folgt:

(III) $e \otimes g = g \otimes e$ q.e.d.

Verkürzte Gruppendefinition

Wegen der Gültigkeit der gerade bewiesenen Sätze können wir unsere Gruppendefinition kürzer schreiben:

Definition 1.3.7

Gruppe (verkürzte Schreibweise)
Eine nichtleere Menge G zusammen mit einer Verknüpfung $\oplus$ heißt Gruppe, wenn gilt:

- *$\oplus$ ist abgeschlossen auf G:*
  $\forall a, b \in G : a \oplus b \in G$
- *$\oplus$ ist assoziativ auf G:*
  $\forall a, b, c \in G : (a \oplus b) \oplus c = a \oplus (b \oplus c)$
- *Es gibt in G bzgl. $\oplus$ ein neutrales Element n:*
  $\exists n \in G \forall a \in G : a \oplus n = a$
- *Jedes Element aus G hat in G ein inverses Element bzgl. $\oplus$:*
  $\forall a \in G \exists - a \in G : a \oplus -a = n.$

Bemerkung:

Natürlich hätte man in obiger Definition alles auch „von links“ schreiben können.

1.3.4 Eindeutigkeiten

Eindeutigkeit des Einslementes

Satz 1.3.3

Eindeutigkeit des Einselementes
Jede Gruppe hat genau ein Einslement.

Beweis:

Es sei $[G, \odot]$ eine Gruppe. Nach der Definition des Begriffs Gruppe hat $[G, \odot]$ eine Einslement e_1. Es bleibt zu zeigen, dass $[G, \odot]$ kein weiteres Einslement e_2 hat. Wir nehmen an es gibt e_2 mit $e_2 \neq e_1$. Nach Satz 2 sind e_1 und e_2 von links und von rechts Einselemente. Wir gehen aus von der Gleichung $e_1 \odot e_2 = e_1 \odot e_2$. Aus dieser Gleichung folgt wegen der Einslement eigenschaft beider Elemente e_1 und e_2 (und das sowohl von rechts, wie auch von links) $e_1 = e_2$.

Eindeutigkeit der inversen Elemente

Satz 1.3.4

Eindeutigkeit der inversen Elemente
In jeder Gruppe $[G, \odot]$ gilt: Jedes Gruppenelement $g \in G$ hat genau ein inverses Element.

Beweis:

Es sei $g \in G$ eine Gruppe mit dem Einslement e. Nach der Definition des Begriffs Gruppe hat g in G ein Inverses g_1^{-1} bezüglich $\odot$. Wir nehmen an, g hat in G ein weiteres Inverses g_2^{-1}, das natürlich von g_1^{-1} verschieden ist. Nach Satz 1 wissen wir, dass g_1^{-1} und g_2^{-1} von links und von rechts invers zu g bzgl. $\odot$ sind.

Die triviale Gleichung $(I) e = e$ "pumpen"wir zu $(II) g \odot g_1^{-1} = g \odot g_2^{-1}$ auf.

(II) multiplizieren wir auf beiden Seiten von links mit g_1^{-1} und erhalten (III) $g_1^{-1} \odot g \odot g_1^{-1} = g_1^{-1} \odot g \odot g_2^{-1}$.

(III) verkürzt sich zu $g_1^{-1} = g_2^{-1}$, was ein Widerspruch zu unserer Annahme $g_1^{-1} \neq g_2^{-1}$ ist.

Kürzbarkeit

Satz 1.3.5

Kürzbarkeit Es sei $[G, \odot]$ eine Gruppe. Für alle Elemente $a, b, c \in G$ gilt:

$a \odot b = a \odot c \Rightarrow b = c$

$b \odot a = c \odot a \Rightarrow b = c$

Beweis:

Jeweils von rechts bzw. links beide Seiten der Gleichung mit a^{-1} multiplizieren.

Lösbarkeit der Gleichungen

Satz 1.3.6

Lösbarkeit der Gleichungen
In jeder Gruppe $[G, \odot]$ sind die Gleichungen

(a) $a \odot x = b$ und

(b) $y \odot a = b$

jeweils eindeutig lösbar.

Beweis:

Wir führen den Beweis nur für die Gleichung $a \odot x = b$, für die Gleichung $y \odot a = b$ wird der Beweis analog geführt.

Existenzbeweis

Zuerst formen wir $a \odot x = b$ um:

$$a \odot x = b \odot a^{-1} \tag{1.1}$$
$$a^{-1} \odot a \odot x = a^{-1} \odot b \tag{1.2}$$
$$e \odot x = a^{-1} \odot b \tag{1.3}$$
$$x = a^{-1} \odot b \tag{1.4}$$
$$\tag{1.5}$$

$x = a^{-1} \odot b$ setzen wir nun in $a \odot x = b$ ein und formen um:

$$a \odot (a^{-1} \odot b) = (a \odot a^{-1}) \odot b = e \odot b = b.$$

Eindeutigkeitsbeweis:

Es seien x_1 und x_2 Lösungen der Gleichung $a \odot x = b$. Damit folgt $a \odot x_1 = a \odot x_2$. Damit gilt $x_1 = x_2$

Ein Monoid in dem die Gleichungen lösbar sind, ist eine Gruppe

Satz 1.3.7

Es sei $[M, \odot]$ ein Monoid. e sei das Einslement dieses Monoids. Wenn die Gleichungen

(a) $a \odot x = b$ und

(b) $y \odot a = b$

in $[M, \odot]$lösbar sind, dann ist das Monoid sogar eine Gruppe.

Beweis:

Wir haben zu zeigen, dass zu jedem Element $a \in M$ ein Inverses in M existiert. Wegen der Lösbarkeit der Gleichungen 1 und 2 sind auch die Gleichungen

(a) $a \odot x = e$ und

(b) $y \odot a = e$

lösbar.
Daraus folgt, dass x, y Inverse von a sind, also $x = y = a^{-1}$.

Weitere Möglichkeit der Gruppendefinition

Die bewiesenen Sätze erlauben, eine Gruppe als ein Monoid zu definieren, in dem die Gleichungen

(a) $a \odot x = b$ und

(b) $y \odot a = b$

lösbar sind.

2 zyklische Gruppen

2.1 Ordnungen und Potenzen

2.1.1 Die Ordnung einer Gruppe

Definition 2.1.1

Gruppenordnung
Es sei $[G, \odot]$ eine Gruppe. Unter der Ordnung $|G|$ von $[G, \odot]$ versteht man die Anzahl der Elemente der Menge G.

Beispiele:

1) $[\mathbb{Z}_5, \oplus] : |\mathbb{Z}_5| = 5$

2) $[\mathbb{Z}_5, \odot] : |\mathbb{Z}_5| = 4$

3) $[\mathbb{Q}, +] : |\mathbb{Q}| = \infty$

2.1.2 Die Ordnung eines Gruppenelements

Potenzschreibweisen in Gruppen

Aus der Schule sind uns Potenzen bezüglich der Multiplikation reeller Zahlen bekannt:

- $3^5 := 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 243$
- $5^{-3} := 5^{-1} \cdot 5^{-1} \cdot 5^{-1} = \frac{1}{5} \cdot \frac{1}{5} \cdot \frac{1}{5} = \frac{1}{5^3} = \frac{1}{125} = 0,008$
- $a^n := \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n-mal}, , a \in \mathbb{R}, n \in \mathbb{N}$
- $a^{-n} := \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{n-mal} = \frac{1}{\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n-mal}}, a \in \mathbb{R}, n \in \mathbb{N}$

Verallgemeinerung auf beliebige Gruppen:

Beispiel 1: $[\mathbb{Z}_5, \oplus]$

- $\overline{2}^3 = \overline{2} \oplus \overline{2} \oplus \overline{2} = \overline{2+2+2} = \overline{6} = \overline{1}$
- $\overline{2}^{-3} = \overline{3}^3 = \overline{3} \oplus \overline{3} \oplus \overline{3} = \overline{3+3+3} = \overline{9} = \overline{4}$

Definition 2.1.2

Potenz g^z eines Gruppenelements für $z \in \mathbb{Z}, z \geq 0$
Es sei $[G, \oplus]$ eine Gruppe mit dem Neutralelement n. Für beliebige Elemente $g \in G$ und ganze Zahlen $z \geq 0$ definieren wir:

1) $g^z := n \; falls \; z = 0$

2) $g^z := g^{z-1} \oplus g \; falls \; z > 0$

Definition 2.1.3

Potenz g^z eines Gruppenelements für $z \in \mathbb{Z}, z < 0$
Es sei $[G, \oplus]$ eine Gruppe und $z \in \mathbb{Z}, z < 0$. Ferner sei g eine beliebiges Gruppenelement und g^{-1} sein Inverses in $[G, \oplus]$.

1) $g^z := g^{-1} \; falls \; z = -1$

2) $g^z := g^{z+1} \oplus g^{-1} \; falls \; z < -1$

Die Ordnung eines Gruppenelements

Definition 2.1.4

Ordnung eines Gruppenelements
Es sei $[G, \odot]$ eine Gruppe.

Die Ordnung eines Elements $g \in G$ ist die kleinste natürliche Zahl n für die gilt:

$$g^n = e$$

2.1.3 Übungsaufgaben zu den Ordnungen

Aufgabe 2.1.1

Bestimmen Sie in $[\mathbb{Z}/_7, \oplus]$ die Ordnungen aller Gruppenelemente.

Aufgabe 2.1.2

Bestimmen Sie in $[\mathbb{Z}/_7, \odot]$ die Ordnungen aller Gruppenelemente.

Aufgabe 2.1.3

Bestimmen Sie in der Gruppe der Deckdrehungen des regelmäßigen 6-Ecks alle Ordnungen der Gruppenelemente.

Aufgabe 2.1.4

Warum kann es nur einen einzigen Typ von Gruppen der Ordnung 3 geben?

Aufgabe 2.1.5

Lineare Funktionen werden durch Gleichungen der Form $y(x) = m \cdot x + n$ mit $m, n \in \mathbb{R}$ (beliebig aber fest) beschrieben. Die linearen Funktionen bilden bzgl. der NAF von Funktionen eine Gruppe. Bestimmen sie für $f : y = \frac{1}{2}x+2$ die Potenzen $f^0, f^1, f^2, f^3, f^m, m \in \mathbb{N}$.

2.2 Beispiele für zyklische Gruppen

2.2.1 $[[Z], +]$

Jede ganze Zahl z mit $z > 0$ lässt sich durch sukzessives Aufaddieren der Zahl 1 generieren:

$$z = \underbrace{1 + 1 + \ldots + 1}_{z \ mal}$$

erzeugen.
Jede ganze Zahl z mit $z < 0$ lässt sich durch sukzessives Aufaddieren der Zahl -1 generieren:

$$z = \underbrace{-1 + -1 + \ldots + -1}_{|z| \ mal}$$

erzeugen.
Nach Definition ist bezüglich der Addition $1^0 = 0$
Jede ganze Zahl lässt sich also als Potenz der ganzen Zahl 1 schreiben. Die Zahl 1 ist ein erzeugendes Element der Gruppe der ganzen Zahlen bzgl. der Addition.

2.2.2 Eine spezielle Gruppe von Matrizen

Gegebe sei die Matrix $M_{90} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Wir bilden Potenzen von M_{90}:

$$M_{90}^1 = M_{90} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$M_{90}^2 = M_{90} \cdot M_{90} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$M_{90}^3 = M_{90}^2 \cdot M_{90} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$M_{90}^4 = M_{90}^3 \cdot M_{90} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

M_{90}^4 ergibt die Einheitsmatrix. Mittels der vier Potenzen von M_{90} wurden vier Matrizen generiert, die bezüglich der Matrizenmultiplikation eine zyklische Vierergruppe bilden.

2.2.3 Die multiplikative Restklassengruppe modulo 5

Bei den multiplikativen Restklassengruppen läßt man bekannterweise $\overline{0}$ weg. Bei Primzahleigenschaft des Moduls m bilden auch die Restklassen modulo m bezüglich der Restklassenmultiplikation eine Gruppe. Sie besteht aus den Restklassen $\overline{1}, \overline{2}, \overline{2}, \overline{2}$. Jede dieser Restklassen läßt sich als Potenz der Restklasse $\overline{3}$ schreiben:

$$\overline{3}^1 = \overline{3}, \overline{3}^2 = \overline{4}, \overline{3}^3 = \overline{2}, \overline{3}^4 = \overline{1}.$$

Fazit: Die Gruppe selbst hat die Ordnung 4. In der vierten Potenz von $\overline{3}$ wird das Einselement $\overline{1}$ generiert. In den Potenzen zuvor wurden alle anderen Gruppenelemente generiert.

2.3 Definition zyklische Gruppe

Definition 2.3.1

erzeugendes Element einer Gruppe

Es sei $[G, \times]$ eine Gruppe mit $|G| = n$ unddem Einselement e. Wenn für ein Element $g \in G$ gilt:

$$g^n = e,$$

dann ist g eine erzeugendes Element der Gruppe $[G, \times]$.

Definition 2.3.2

zyklische Gruppe
Wenn eine Gruppe ein erzeugendes Element hat, dann heißt diese Gruppe zyklisch.

Sofort einsichtig ist, dass jede zyklische Gruppe kommutativ ist.

Satz 2.3.1

Jede zyklische Gruupe ist kommutativ.

Aufgabe 2.3.1

Beweisen Sie, dass jede zyklische Gruppe kommutativ ist.

3 Untergruppen

3.1 Beispiele

3.1.1 Beispiel 1

Wir gehen von der additiven Gruppe der Restklassen modulo 6 aus $[\mathbb{Z}_6, \oplus]$.
Die Gruppe besteht aus den folgenden Restklassen: $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

Die Gruppentafel sieht wie folgt aus:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Wir wählen aus $\mathbb{Z}_6$ die folgende Teilmenge $2\mathbb{Z}_6$aus:

$2\mathbb{Z}_6 := \{\overline{0}, \overline{2}, \overline{4}\}$

$[2\mathbb{Z}_6, \oplus]$ ist eine Gruppe und damit eine Untergruppe von $[\mathbb{Z}_6, \oplus]$

$\oplus$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

3.1.2 Beispiel 2

Die Gruppe der Bewegungen

Die Gruppenmitglieder

Unter einer Bewegung β versteht man eine abstandserhaltende Abbildung der Ebene auf sich:
Es sei ε unsere Ebene.

β ist Relation

$\forall P \in \varepsilon \exists P' \in \varepsilon : P' = \beta(P)$
β ist eindeutig und damit Abbildung

$\forall P \in \varepsilon : P' = \beta(P) \wedge P^* = \beta(P) \Rightarrow P' = P^*$
β ist abstandserhaltend

$\forall P, Q \in \varepsilon : |PQ| = |\beta(P)\beta(Q)|$
Die Menge aller Bewegungen wollen wir mit β bezeichnen.

Die Verknüpfunghallo
wir wählen als Verknüpfung auf β die NAF von Abbildungen und kennzeichnen diese mit $\circ$.

$[\beta, \circ]$ ist Gruppe

Abgeschlossenheit

Es seien α und β zwei Bewegungen.
Wir haben zu zeigen, dass $\alpha \circ \beta$ eine Bewegung ist.
Da die NAF zweier Abbildungen der Ebene auf sich ist tivialerweise wieder eine Abbildung der Ebene auf sich. Wir müssen nur zeigen dass $\alpha \circ \beta$ abstandserhaltend ist:

(1) $|PQ| = |\alpha(P)\alpha(Q)|$ α ist Bewegung und damit abstandserhaltend

(2) $|\alpha(P)\alpha(Q)| = |\beta(\alpha(P))\beta(\alpha(Q))|$ β ist Bewegung und damit abstandserhaltend Asso-

(3) $|PQ| = |\beta(\alpha(P))\beta(\alpha(Q))|$ (1), (2)

ziativität

Die NAF von Abbildungen ist immer assoziativ.
Einselement

Wir betrachten die Abbildung id, die jeden Punkt die Abbildung der ebene auf sich selbst abbildet:

$\forall P \in \varepsilon : \mathrm{id}(P) = P$
Damit ist id eine Abbildung der Ebene auf sich. Wegen $\mathrm{id}(A) = A \wedge \mathrm{id}(B) = B, \forall A, B \in \varepsilon$ gilt natürlich auch $|AB| = |\,\mathrm{id}(A)\,\mathrm{id}(B)|$.
id erfüllt die Eigenschaften eines Einselementes:
$\forall P \in \varepsilon : \beta \circ \mathrm{id}(P) = \mathrm{id}(\beta(P)) = \beta(P)$ und somit $\mathrm{id} \circ \beta = \beta$.
inverse Elemente

Es genügt zu zeigen, dass jede Bewegung β eineindeutig ist, d.h. dass jeder Punkt $R \in \varepsilon$ bei β ein und nur ein Urbild $Q \in \varepsilon$ hat.
Injektivität von β

Sei P' das Bild von P bei der Bewegung β. Wir haben zu zeigen, dass es keinen Punkt $Q \in \varepsilon, Q \not\equiv P$ gibt, der durch β auch auf P' abgebildet wird. Wir nahemen, an, dass es einen solchen Punkt Q gibt. Dann gilt:
$0 = |P'P'| = |PQ|$ und damit $P \equiv Q$, was ein Widerspruch zur Annahme $P \not\equiv Q$ ist. hallo=Surjektivität von βhallo= Wir haben zu zeigen, dass jeder Punkt $Q \in \varepsilon$ bei der Bewegung β ein Urbild hat.
Annahme: Q hat kein Urbild bei β. Da jeder Punkt der Ebene ε durch β auf genau einen Punkt der Ebene ε abgebildet wird und der Punkt Q kein Urbild hat, müssen wenigstens zwei verschiedene Punkte A und B aus ε durch β auf ein und denselben Punkt C abgebildet werden:
$A \overset{\beta}{\to} C\ B \overset{\beta}{\to} C$ Wegen $|CC| = 0 = |\beta(A)\beta(B)|$ müssen A und B ein und derselbe Punkt, also identisch sein. Das ist ein Widerspruch zu $A \not\equiv B$. Unsere Annahme Q hat kein Urbild ist also zu verwerfen.

Die Untergruppe der Drehungen um ein und denselben Punkt

Drehungen

Eine Bewegung die entweder die Identität ist oder genau einen Fixpunkt Z besitzt, heißt Drehung. Falls die Bewegung genau den Fixpunkt Z hat, sprechen wir von einer Drehung um Z.
Die Gruppe der Drehungen um ein und denselben Fixpunkt

Es sei Z ein beliebiger aber fester Punkt der Ebene. Wir betrachten $\mathbb{D}_Z$ die Menge aller Drehungen um Z. Als Verknüpfung auf $\mathbb{D}_Z$ wählen wir die $\circ$, die NAF von Abbildungen. $[\mathbb{D}_Z, \circ]$ ist eine Gruppe:

- Abgeschlossenheit
  Es seien D_1 und D_2 zwei Drehungen um Z. Wir haben bererits geszeigt, dass die NAF zweier Bewegungen eine Bewegung ist. Da D_1 und D_2 zwei Bewegungen sind, ist $D_3 := D_1 \circ D_2$ ebenfalls eine Bewegung. Weil Z ein Fixpunkt sowohl von D_1 als auch von D_2 ist, muss Z auch ein Fixpunkt von D_3 sein. Es können jetzt genau zwei Fälle auftreten:

- Fall 1
  Z ist der einzige Fixpunkt von D_3. In diesem Fall ist D_3 eine Drehung mit dem Fixpunkt Z.
- Fall 2
  D_3 hat neben Z einen weiteren Fixpunkt F.
  Das bedeutet:

  (I) $Z \overset{D_3}{\to} Z$

  (II) $F \overset{D_3}{\to} F$

  Wegen der Abstandserhaltung von D_3 ist jeder Punkt G der Geraden ZF ein Fixpunkt bei D_3. (Der Leser überzeuge sich davon.) Die Gerade ZF ist damit eine Fixpunktgerade bei D_3.
  Sei $P \notin ZF$. Für das Bild P' mit $P \overset{D_3}{\to} P'$
  gibt es jetzt genau zwei Möglichkeiten:

  a) $P' \in ZF, P^+$

  b) $P' \in ZF, P^-$

  Im Fall a) ist wegen der Abstandserhaltung von D_3 $P' \equiv P$, woraus folgt, dass jeder Punkt der Ebene bei D_3 ein Fixpunkt ist. D_3 wäre damit die Identität und somit eine Drehung.
  Fall b) kann nicht eintreten. (Der Leser überzeuge sich davon.)

- Assoziativität
  Die NAF von Abbildungen (Funktionen) ist generell assoziativ.

- Einselement
  Die Identität leistet das Verlangte.

- Inverse Elemente
  Wir wissen bereist, dass jede Bewegung genau ein inverses Element besitzt. Es bleibt zu zeigen, dass die inverse Bewegung D_Z^{-1} zu einer Bewegung D_Z mit genau dem Fixpunkt Z eine Bewegung mit genau dem Fixpunkt Z ist. Zunächst ist Z ein Fixpunkt von D_Z^{-1}: D_Z^{-1} bildet jeden Punkt der Ebene auf sein Urbild bei D_Z ab. Weil Z das Bild von Z bei D_Z ist, ist Z also auch ein Fixpunkt bei D_Z^{-1} . Sollte D_Z^{-1} enen weiteren von Z verschiedenen Fixpunkt F haben, wäre jener Punkt F nach analogen Überlegungen auch ein Fixpunkt bei D_Z. D_Z hat jedoch nur den einen Fixpunkt Z.

Fazit

Die Drehungen um ein und denselben Punkt Z bilden bzgl. der NAF von Abbildungen eine Gruppe und sind damit eine Untergruppe der Gruppe aller Bewegungen.

3.2 Definitionen und Kriterien für Untergruppen

Definition 3.2.1

Untergruppe
Es sei $[G, \odot]$ eine Gruppe und U eine Teilmenge von G.
Wenn $[U, \odot]$ selbst eine Gruppe ist, dann ist $[U, \odot]$ eine Untergruppe von $[G, \odot]$

Satz 3.2.1

Untergruppenkriterium 1
Es sei $[G, \odot]$ eine Gruppe und $U \subseteq G$ mit $G \neq$.
$[U, \odot]$ ist genau dann Untergruppe von $[G, \odot]$, wenn

(1) $\forall a, b \in U : a \odot b \in U$,

(2) $\forall a \in U : a^{-1} \in U$.

Satz 3.2.2

Untergruppenkriterium 2
Es sei $[G, \odot]$ eine Gruppe und $U \subseteq G$ mit $G \neq$.
$[U, \odot]$ ist genau dann Untergruppe von $[G, \odot]$, wenn

$$\forall a, b \in U : a \odot b^{-1} \in U$$