1 Beispiele und Gegenbeispiele für Gruppen

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.

1.2 Restklassengruppen

1.2.1 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

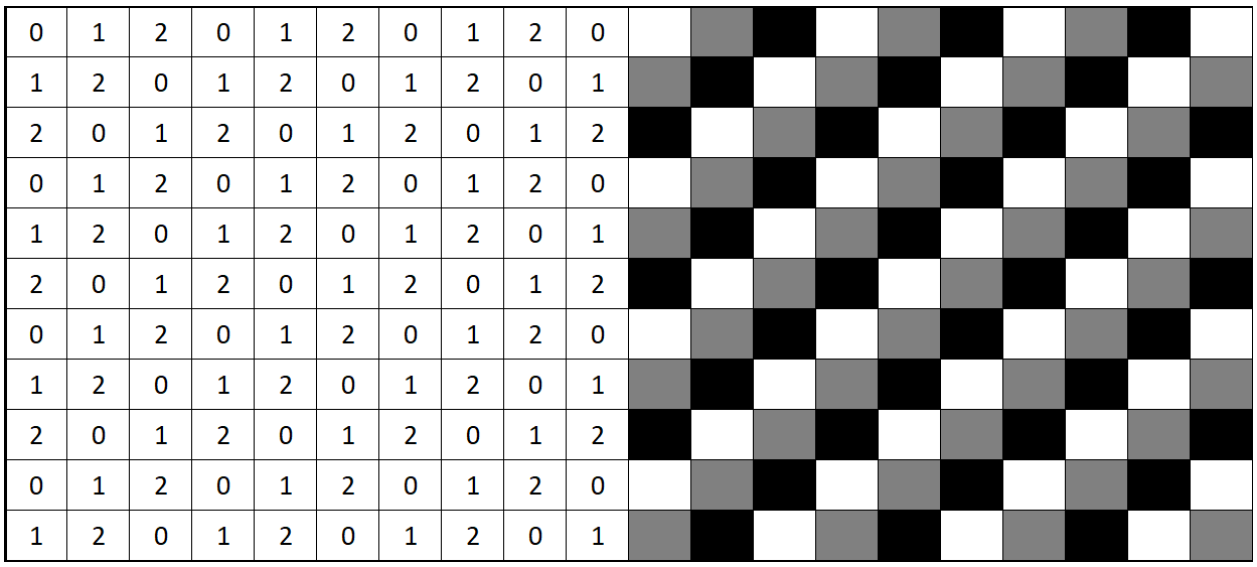
$a \equiv b \ mod \ m$

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

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

Aufgabe 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 1.2

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 1.2

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 1.2

$a \equiv b \ mod \ m$ reloaded

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

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 1.3

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

1.2.2 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 1.4

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 1.5

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 1.3

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

Aufgabe 1.6

Erläutern Sie, warum in Definition 1.3 zwei verschiedene Zeichen für die Addition verwendet 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 1.7

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 1.4

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

Aufgabe 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 1.9

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

Aufgabe 1.10

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