2 Gruppen

Rechenstrukturen sind uns aus Schule und täglichem Leben bekannt: Wir lernen dort bzw. benötigen die Addition, Subtraktion, Multiplikation und Division von von ganzen, rationalen und reellen Zahlen (mit der Rechenstruktur $\mathbb{Z}$ der ganzen Zahlen haben wir uns schon Kapitel 1 ausführlich beschäftigt). Bei diesen Strukturen werden Elemente von unendlichen Mengen miteinander verknüpft. In der Informatik sind in der Regel Rechenstrukturen mit nur endlich vielen Elementen von Interesse. So rechnen wird dort mit zwei Bits, d.h. mit den Zahlen 0 und 1. Abbildung 7 zeigt die Additions- und die Multiplikationstafel für Bits. Hier wird modulo 2 gerechnet, d.h. alle Zahlen werden durch 2 dividiert und der dabei verbleibende Rest ist das Ergebnis. Deshalb ist $1 + 1 = 0$, weil 2 bei Divison durch 2 den Rest 0 ergibt. In der Informatik wird nicht nur mit kleinen Moduln wie 2, sondern auch mit sehr großen Modulen $m \in \mathbb{N}$ gerechnet, wie z.B. in der Kryptografie mit m in der Größenordnung von $2^{2^{12}}$; wir werden in späteren Kapiteln noch darauf zurückkommen.

$+$	0	1
0	0	1
1	1	0

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

Abb. 7: Addition und Multiplikation von Bits

Als ein weiteres Beispiel für das Modulo-Rechnen zeigt Abbildung 8 die Additions- und die Multiplikationstafel für das Rechnen modulo 5 (siehe auch Satz 1.3). Dabei lassen wir bei der Multiplikation die 0 weg, weil das Ergebnis immer gleich 0 ist (im weiteren Verlauf werden wir noch weitere – mathematische – Gründe dafür kennen lernen).

Aber Rechnen umfasst nicht nur das Addieren und Multiplizieren von Zahlen in endlichen und unendlichen Strukturen, Rechnen kann auch andere Verknüpfungen von Zahlen bedeuten, wie z.B. das Minimum und das Maximum oder der größte gemeinsamer Teiler oder das kleinste gemeinsame Vielfache von Zahlen. Aber nicht nur Zahlen können miteinander verknüpft werden. Ein Datenbanksystem muss z.B. Mengen vereinigen und schneiden können oder die Differenz von zwei Mengen bilden können, um Benutzeranfragen beantworten zu können. Abildung 9 zeigt als einfache Beispiele die Tafeln für die Vereinigung und den Durchschnitt der Teilmengen der Menge $M = \{a, b\}$. Dabei lassen wir bei der Vereinigung die Menge $M = \{a, b\}$ und beim Durchschnitt die leere Menge weg, weil die Vereinigung mit M immer M bzw. der Durchschnitt mit $\emptyset$ immer

K.-U. Witt, *Algebraische und zahlentheoretische Grundlagen für die Informatik*,
DOI 10.1007/978-3-658-04075-8_2, © Springer Fachmedien Wiesbaden 2014

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Abb. 8: Addition und Multiplikation modulo 5

$\emptyset$ ergibt.

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$

$\cap$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{\ a\}$
$\{b\}$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\{a\}$	$\{b\}$	$\{a,b\}$

Abb. 9: Vereinigung und Durschnitt der Teilmengen von $\{a,b\}$

Weitere Beispiele für Verknüpfungen sind die Konjunktion und Disjunktion von Wahrheitswerten und die Komposition von Funktionen.

Lernziele

Nach dem Durcharbeiten dieses Kapitels sollten Sie

- die Definitionen für Halbgruppen, Monoide und Gruppen kennen und für diese jeweils mehrere Beispiele angeben und für kleinere Strukturen die Verknüpfungstafeln aufstellen können,
- überprüfen können, ob gegebene Rechenstrukturen bestimmte Eigenschaften besitzen,
- die Begriffe Gruppen- und Elementordnung definieren, ihre elemntaren Eigenschaften erklären und für (kleinere) endliche Gruppen die Ordnungen ihrer Elemente bestimmen können,
- die von Elementen erzeugten Untergruppen bestimmen können,
- nachweisen könen, ob eine Untermenge einer Gruppe eine Untergruppe bildet,

- den Satz von Lagrange erläutern können,
- die Begriffe Homomorphismus und Isomorphismus erläutern können und nachweisen können, ob eine gegebene Abbildung zwischen Gruppen ein Homomorphismus oder ein Isomorphismus ist,
- den Begriff Kern eines Homomorphismus und seine Bedeutung erläutern und für einfache Beispiele bestimmen können,
- den Homomorphiesatz für Gruppen erläutern und an Beispielen veranschaulichen können.

2.1 Grundlegende Eigenschaften von Rechenstrukturen

Wenn wir uns die obigen Beispiele etwas näher ansehen und die Eigenschaften der verwendeten Verknüpfungen ansehen, dann entdecken wir, dass es Eigenschaften gibt, die alle Beispiele besitzen, und dass es ebenso Eigenschaften gibt, die nicht von allen Beispielen erfüllt werden. So sind z.B. alle betrachteten Verknüpfungen assoziativ, d.h. werden mehr als zwei Elemente miteinander verknüpft, spielt die Reihenfolge des Auswertung keine Rolle. Wenn wir das Symbol $*$ als einen Platzhalter für die verwendeten Verknüpfungen Addition, Multiplikation, Vereinigung, Durchschnitt, Komposition, Konjunktion und Disjunktion benutzen, dann gilt für diese alle die Eigenschaft $(a*b)*c = a*(b*c)$. Da es sich um zweistellige Verknüpfungen handelt, denn es werden immer zwei Elemente der zugrundeliegenden Menge verknüpft, müssen wir zunächst Klammern verwenden, weil sonst nicht klar ist, welche beiden Elemente zunächst miteinander verknüpft werden sollen. Die Assoziativität besagt nun, dass die Reihenfolge bei der Auswertung keine Rolle spielt. Man kann also bei einer assoziativen Rechenstruktur sogar die Klammern weglassen. Das Ergebnis der Auswertung eines Ausdrucks $a_1 * a_2 * \ldots a_n$, $n \geq 3$, ist unabhängig von der Reihenfolge, in der die Operanden und die entstehenden Zwischenergebnisse verknüpft werden.

Assoziativität

Übungsaufgaben

2.1 Überüfen Sie anhand von Beispielen, dass alle oben erwähnten Rechenstrukturen assoziativ sind! □

Eine Eigenschaft, die alle bis auf eine der oben erwähnten Strukturen erfüllen, ist die Kommutativität. Eine Operation $*$ ist kommutativ, wenn für alle Elemente a

Kommutativität

und b der Struktur $a * b = b * a$ gilt, d.h. die Vertauschung der Operanden a und b lässt das Ergebnis ihrer Verknüpfung invariant. Addition und Multiplikation von Zahlen, Vereinigung und Durchschnitt von Mengen, Disjunktion und Konjunktion von aussagenlogischen Ausdrücken sind Beispiele für kommutative Operationen. Die Komposition von Funktionen ist im Allgemeinen nicht kommutativ. Betrachten wir z.B. die beiden Funktionen $f(x) = x + 1$ und $g(x) = x^2$, dann gilt $f \circ g(x) = f(g(x)) = f(x^2) = x^2 + 1 \neq (x + 1)^2 = g(x + 1) = g(f(x)) = g \circ f(x)$. Die Multiplikation von Matrizen ist ein weiteres Beispiel für eine im Allgemeinen nicht kommutative Operation.

Einselement
Neutrales Element

Eine weitere gemeinsame Eigenschaft der obigen Beispiele ist die Existenz eines so genannten Einselements, auch neutrales Element genannt. Die Verknüpfung irgendeines Elementes mit diesem speziellen Element ändert das Element nicht. Wenn wir das Einselement im Allgemeinen mit e bezeichnen, dann gilt also $a * e = a$ für alle Elemente a der Struktur. So ist die Null das Einselement bei der Addition ganzer Zahlen, und die Eins ist das Einselement bei der Multilikation; das Einselement bei der Komposition von Funktionen ist die Identität $id(x) = x$.

Übungsaufgaben

2.2 Stellen Sie fest, ob die in den Abbildungen 7 – 9 dargestellten Strukturen Einselemente besitzen und geben Sie diese gegebenenfalls an! □

Aufgrund dieser Beobachtungen von Gemeinsamkeiten verschiedener Rechenstrukturen werden wir im Folgenden von konkreten Rechenstrukturen abstrahieren und mithilfe von genannten und weiteren Eigenschaften abstrakte Rechenstrukturen definieren und untersuchen. Die Erkenntnisse, die wir so abstrakt gewinnen, gelten dann jeweils für alle konkreten Rechenstrukturen der entsprechenden Art.

Trägermenge
Abgeschlossenheit

Wir betrachten zunächst Rechenstrukturen, bei denen die Elemente einer Menge M mit einer zweistelligen Operation $*$ miteinander verknüpft werden, später kommt noch eine weitere zweistellige Verknüpfung hinzu. Die Menge M wird auch *Trägermenge* der Struktur genannt. Dabei gehen wir grundsätzlich davon aus, dass eine solche Struktur *abgeschlossen* ist. Das bedeutet, dass für alle $a, b \in M$ gilt: $a * b \in M$. Das Ergebnis der Verknüpfung von Elementen der Trägermenge ist also immer ein Element der Trägermenge. Wir können die Verknüpfung $*$ als Abbildung $* : M \times M \rightarrow M$ auffassen; Abgeschlossenheit bedeutet, dass $*$ total definiert ist.

Übungsaufgaben

2.3 (1) Überlegen Sie, dass für alle oben erwähnten Beispiele die Abgeschlossenheit gegeben ist!

(2) Ist die Menge der geraden ganzen Zahlen abgeschlossen gegenüber Addition?

(3) Ist die Menge der ungeraden ganzen Zahlen abgeschlossen gegenüber Addition? □

2.2 Definitionen und Beispiele

Mithilfe der oben bei den Beispielen betrachteten Eigenschaften führen wir nun die ersten Bezeichnungen für algebraische Strukturen ein.

Definition 2.1 Es sei $\mathcal{A} = (M, *)$ eine abgeschlossene algebraische Struktur mit Trägemenge M und der total auf M definierten zweistelligen Verknüpfung $*$. Wir schreiben im Folgenden für Elemente a einer solchen Struktur $a \in \mathcal{A}$ anstelle von $a \in M$, was formal korrekt wäre, d.h. wir unterscheiden nicht zwischen dem Namen einer algebraischen Struktur und ihrer Trägermenge.

a) $\mathcal{A}$ heißt *assoziativ* genau dann, wenn $(a*b)*c = a*(b*c)$ für alle $a, b, c \in \mathcal{A}$ gilt. **Assoziativität**

b) Ein Element $e \in \mathcal{A}$ heißt *Einselement* oder auch *neutrales Element* von $\mathcal{A}$ genau dann, wenn $a * e = a$ und $e * a = a$ für alle $a \in \mathcal{A}$ gilt. **Einselement** **Neutrales Element**

c) Besitzt $\mathcal{A}$ ein Einselement e und existiert zu dem Element $a \in \mathcal{A}$ ein Element $b \in \mathcal{A}$ mit der Eigenschaft $a * b = b * a = e$, dann heißt b *invers* oder *Inverses* zu a. In der Regel notieren wir das Inverse von a mit a^{-1}. Gilt $a^{-1} = a$, dann heißt a *selbstinvers* oder *Involution* **Inverses** **Inverses Element** **Selbstinverses Element** **Involution**

d) $\mathcal{A}$ heißt *kommutativ* genau dann, wenn $a * b = b * a$ für alle $a, b \in \mathcal{A}$ gilt. □ **Kommutativität**

Übungsaufgaben

2.4 Untersuchen Sie, welche der in der Definition 2.1 festgelegten Eigenschaften von den in den Abbildungen 7 – 9 dargestellten Strukturen erfüllt werden! □

Für die wiederholge Verknüpfung eines Elementes a mit sich selber verwenden wir die Potenzschreibweise

$$\underbrace{a * a * \ldots * a}_{n\text{-mal}} = a^n$$

die wir wie folgt auch formal rekursiv definieren können:

$$a^0 = e$$
$$a^{n+1} = a^n * a$$

Des Weiteren setzen wir

$$a^{-n} = \left(a^{-1}\right)^n$$

Es gilt dann für alle $m, n \in \mathbb{Z}$ das bekannte Potenzrechengesetz

$$a^{m+n} = a^m * a^n \tag{2.1}$$

Die Potenzschreibweise kennen wir von der Multiplikation von Zahlen, während wir die wiederholte Addition nicht mit einem Exponenten, sondern mit einem Wiederholungsfaktor ausdrücken. Wir schreiben z.B. für $3+3+3+3+3$ nicht 3^5, sondern $5 \cdot 3$. Entsprechend notieren wir das additive Inverse einer Zahl a nicht mit a^{-1}, sondern mit $-a = -1 \cdot a$. Das Potenzrechengesetz (2.1) lautet dann für die Addition

$$(m+n) \cdot a = m \cdot a + n \cdot a$$

Halbgruppe **Monoid** **Gruppe**

Definition 2.2 **a)** Eine einsortige algebraische Struktur $\mathcal{G} = (M, *)$, die assoziativ ist, heißt *Halbgruppe*. Besitzt eine Halbgruppe ein Einselement, dann heißt $\mathcal{G}$ *Monoid*. Besitzen alle Elemente eines Monoids ein Inverses, dann heißt $\mathcal{G}$ *Gruppe*. Ist die Verknüpfung $*$ kommutativ, dann heißt $\mathcal{G}$ *kommutativ* oder *abelsch*.[4]

Unter- -halbgruppe -monoid -gruppe

b) Bildet eine Untermenge $U \subseteq M$ von $\mathcal{G}$ eine Halbgruppe, ein Monoid oder eine Gruppe, dann heißt $\mathcal{G}_U = (U, *)$ *Unterhalbgruppe*, *Untermonoid* bzw. *Untergruppe* von $\mathcal{G}$. Ist $\mathcal{G}_1$ eine Untergruppe von $\mathcal{G}_2$, so schreiben wir auch $\mathcal{G}_1 \trianglelefteq \mathcal{G}_2$. Ist $\mathcal{G}_1$ eine *echte Untergruppe* von $\mathcal{G}_2$, d.h. ist $\mathcal{G}_1 \trianglelefteq \mathcal{G}_2$ und $\mathcal{G}_1 \neq \mathcal{G}_2$, dann schreiben wir auch $\mathcal{G}_1 \triangleleft \mathcal{G}_2$.

Gruppenordnung

c) Ist $\mathcal{G}$ endlich, dann heißt $ord_{\mathcal{G}} = |\mathcal{G}|$ die *Ordnung* von $\mathcal{G}$.

Elementordnung

d) Sei $a \in \mathcal{G}$ und e das Einselement von $\mathcal{G}$. Dann heißt

$$ord_{\mathcal{G}}(a) = \min\left\{k \in \mathbb{N} \mid a^k = e\right\}$$

die *Ordnung von a in $\mathcal{G}$*. Falls a keine Ordnung in $\mathcal{G}$ besitzt, dann sagen wir, dass a von *unendlicher Ordnung in $\mathcal{G}$* ist. □

4 Benannt nach *Niels Hendrik Abel* (1802 - 1829), einem norwegischen Mathematiker, der sich unter anderem mit der Auflösbarkeit algebraischer Gleichungen beschäftigte und eine Theorie über Integrale algebraischer Funktionen begründete.

Beispiel 2.1 **a)** $(\mathbb{N}, +)$ ist eine kommutative Halbgruppe, $(\mathbb{N}_0, +)$ ist ein kommutatives Monoid mit dem Einselement 0.

b) Sei Σ ein Alphabet, dann bildet $(\Sigma^*, \circ)$ ein Monoid mit dem leeren Wort ε als Einselement (siehe auch Anhang A.2). Ist $\left|\Sigma^*\right| \geq 2$, dann ist dieses Monoid nicht kommutativ.

c) $(\mathbb{Z}, +)$ bildet eine additive abelsche Gruppe mit dem Einselement 0. Das Inverse von $a \in \mathbb{Z}$ ist $-a$.

d) Die Menge der bijektiven Funktionen einer Menge in sich selbst bildet eine im Allgemeinen nicht kommutative Gruppe mit der Identität als Einselement.

e) $(\mathbb{G}, +)$ ist eine echte Untergruppe von $(\mathbb{Z}, +)$.

f) Die beiden Rechenstrukturen in Abbildung 8 bilden abelsche Gruppen. Die Menge $\{1, 4\}$ bildet eine Untergruppe der multiplikativen Gruppe modulo 5.

g) Einselemente haben immer die Ordnung 1, denn es gilt $e^1 = e$. In der additiven Gruppe modulo 5 in Abbildung 8 hat 2 die Ordnung 5, denn 5 ist die kleinste Zahl, für die $5 \cdot 2 = 0$ modulo 5 ist. Auch alle anderen Elemente außer dem Einselement 0 haben die Ordnung 5. □

Übungsaufgaben

2.5 Geben Sie an, von welcher Art die Rechenstrukturen in den Abbildungen 7 – 9 sind. Im Falle von Gruppen geben Sie deren Ordnung und die Ordnungen ihrer Elemente an!

2.6 Stellen Sie die Multiplikationstafel modulo 7 für die Menge $\{1, 2, \ldots, 6\}$ auf. Überlegen Sie, dass die so entstehende Rechenstruktur eine abelsche Gruppe bildet! Geben Sie zu jedem Element das Inverse an! Welche Ordnung hat die Gruppe? Gegeben Sie die Ordnungen aller Elemente an! Geben Sie eine Untergruppe mit zwei Elementen, eine mit drei Elementen an!

2.7 Die Funktionen $id, nid, rez, nrez : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\}$ seien definiert durch: $id(x) = x$, $nid(x) = -x$, $rez(x) = \frac{1}{x}$ sowie $nrez(x) = -\frac{1}{x}$. Geben Sie die Verknüpfungstafel für die Operation $\circ$ (Komposition von Funktionen) auf dieser Menge von Funktionen an, d.h. geben Sie die Verknüpfungstafel für die Struktur

$$(\{\, id, nid, rez, nrez \,\}, \circ)$$

an. Begründen Sie, dass diese Struktur eine abelsche Gruppe bildet! Geben Sie die Ordnungen ihrer Elemente an!

2.8 Zeigen Sie, dass die algebraische Struktur $(\mathbb{R}, *)$ definiert durch

$$a * b = \sqrt[3]{a^3 + b^3}$$

eine abelsche Gruppe bildet!

2.9 Es sei $\mathcal{SL}_2(\mathbb{Z}) = (\mathbb{Z}^{4,1}, *)$ definiert durch

$$\mathbb{Z}^{4,1} = \left\{(a,b,c,d) \in \mathbb{Z}^4 \mid ad - bc = 1\right\}$$

sowie

$$(a,b,c,d) * (e,f,g,h) = (ae + bg, af + bh, ce + dg, cf + dh)$$

(1) Zeigen Sie, dass $\mathcal{SL}_2(\mathbb{Z})$ eine Gruppe bildet, die im Allgemeinen nicht abelsch ist!

(2) Geben Sie die Ordnungen der Elemente

$$\mathbf{a} = (1,1,0,1), \quad \mathbf{b} = (0,1,-1,0), \quad \text{und } \mathbf{c} = (0,-1,1,1)$$

an! □

Wenn wir die bisherigen Definitionen, Beispiele und Übungen etwas genauer betrachten, stellen wir fest, dass alle Strukturen, die ein Einselement besitzen, auch nur dieses eine besitzen. Ebenso gilt, wenn ein Element invertierbar ist, dann existiert genau ein Inverses. Weiterhin stellen wir fest, dass, wenn b Inverses von a ist, dann ist a auch Inverses von b, d.h. es gilt immer $(a^{-1})^{-1} = a$ für invertierbare Elemente a. Im folgenden Satz zeigen wir, dass diese und weitere Eigenschaften nicht nur für die bisherigen Beispiele zutreffen, sondern generell auf alle Gruppen.

Satz 2.1 Sei $\mathcal{G} = (M, *)$ eine Gruppe mit Einselement e, dann gilt für alle $a, b, c \in \mathcal{G}$:

a) e ist eindeutig;

b) zu a ist a^{-1} eindeutig;

c) $(a^{-1})^{-1} = a$;

Kürzungsregel

d) die *Kürzungsregel*: aus $a * c = b * c$ folgt $a = b$ bzw. aus $c * a = c * b$ folgt $a = b$;

e) $(a * b)^{-1} = b^{-1} * a^{-1}$;

f) die Gleichungen $a * x = b$ bzw. $x * a = b$ mit der Unbekannten x sind eindeutig lösbar;

g) a ist selbstinvers genau dann, wenn a die Ordnung 2 hat.

Beweis **a)** Wir nehmen an, es gebe zwei Einselemente e und e'. Dann gilt einerseits $e * a = a$ für alle $a \in \mathcal{G}$, also auch für $a = e'$, d.h. es gilt $e * e' = e'$. Andererseits gilt $a * e' = a$ für alle $a \in \mathcal{G}$, also auch für $a = e$, d.h. es gilt $e * e' = e$. Insgesamt folgt $e = e * e' = e'$, womit die Behauptung gezeigt ist.

b) Wir nehmen an, zu a gebe es zwei Inverse a_1^{-1} und a_2^{-1}, d.h. es ist $a * a_2^{-1} = e$ und $a_1^{-1} * a = e$, dann gilt mithilfe der Assoziativität:

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * \left(a * a_2^{-1}\right) = \left(a_1^{-1} * a\right) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}$$

c) Es gilt mithilfe der Assoziativität:

$$(a^{-1})^{-1} = (a^{-1})^{-1} * e = (a^{-1})^{-1} * (a^{-1} * a) = ((a^{-1})^{-1} * a^{-1}) * a = e * a = a$$

d) Aus $a * c = b * c$ folgt $(a * c) * c^{-1} = (b * c) * c^{-1}$, daraus mithilfe der Assoziativität $a * (c * c^{-1}) = b * (c * c^{-1})$, daraus $a * e = b * e$, daraus $a = b$. Die zweite Kürzunsregel folgt analog.

e) Es gilt einerseits

$$e = (a * b) * (a * b)^{-1} \tag{2.2}$$

und andererseits

$$e = a * a^{-1} = a * e * a^{-1} = a * (b * b^{-1}) * a^{-1} = (a * b) * (b^{-1} * a^{-1}) \tag{2.3}$$

Aus (2.2) und (2.3) folgt

$$(a * b) * (a * b)^{-1} = (a * b) * (b^{-1} * a^{-1})$$

woraus mit der Kürzungsregel die Behauptung folgt.

f) Die Lösung für $a * x = b$ ist $x = a^{-1} * b$, denn es gilt

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$$

Wir nehmen an, es gebe zwei Lösungen x_1 und x_2, d.h. es gilt $a * x_1 = b$ und $a * x_2 = b$ und damit $a * x_1 = a * x_2$, woraus mit der Kürzungsregel $x_1 = x_2$ folgt.

Die eindeutige Lösung von $x * a = b$ ist $x = b * a^{-1}$, der Beweis ist analog.

g) Die Gültigkeit dieser Aussage ist offensichtlich. □

Übungsaufgaben

2.10 a) Zeigen Sie, dass in den beiden Monoiden in Abbildung 9 die Kürzungsregel nicht gilt!

b) Überlegen Sie, dass für die Verknüpfungstafeln von endlichen Gruppen gilt, dass in jeder Zeile und in jeder Spalte jedes Gruppenelement vorkommen muss und dass alle Elemente innerhalb jeder Spalte und alle Elemente innerhalb jeder Zeile von einander verschieden sein müssen!

c) Zeigen Sie: Sind in einer Gruppe alle Elemente selbstinvers, dann ist die Gruppe abelsch! □

Direktes Produkt von Gruppen

Definition 2.3 Seien $\mathcal{G}_i = (M_i, *_i)$, $1 \leq i \leq n$, Gruppen. Dann bildet

$$\mathcal{G} = \mathcal{G}_1 \times \ldots \times \mathcal{G}_n = (M_1 \times \ldots \times M_n, *)$$

mit

$$x * y = (x_1 *_1 y_1, \ldots, x_n *_n y_n)$$

für $x = (x_1, \ldots, x_n) \in \mathcal{G}$ und $y = (y_1, \ldots, y_n) \in \mathcal{G}$ das *direkte Produkt* von $\mathcal{G}_1, \ldots, \mathcal{G}_n$. □

Beispiel 2.2 Das direkte Produkt der additiven Gruppe der ganzen Zahlen $(\mathbb{Z}, +)$ ist $(\mathbb{Z} \times \mathbb{Z}, +_2)$ definiert durch $(a, b) +_2 (c, d) = (a + c, b + d)$. Die Abgeschlossenheit ist offensichtlich, ebenso die Kommutativität.

Wir rechnen

$$\begin{aligned}(a, b) +_2 ((c, d) +_2 (e, f)) &= (a, b) +_2 (c + e, d + f) \\ &= (a + (c + e), b + (d + f)) \\ &= ((a + c) + e, (b + d) + f) \\ &= ((a + c, b + d) +_2 (e, f) \\ &= ((a, b) +_2 (c, d)) +_2 (e, f)\end{aligned}$$

und stellen die Assoziativität von $+_2$ fest.

$(0, 0)$ ist das Einselement, denn es gilt

$$(a, b) +_2 (0, 0) = (a + 0, b + 0) = (a, b)$$

Zu (a, b) ist $-_2(a, b) = (-a, -b)$ invers, denn es gilt

$$(a, b) +_2 -_2(a, b) = (a, b) + (-a, -b) = (a - a, b - b) = (0, 0)$$

Das direkte Produkt der abelschen Gruppe der ganzen Zahlen bildet also wieder eine additive abelsche Gruppe. □

Übungsaufgaben

2.11 Bilden Sie die Verknüpfungstafel des direkten Produktes der additiven Gruppe modulo 2 (Abbildung 7) und der multiplikativen Gruppe modulo 5 (Abbildung 8); geben Sie das Einselement und die Inversen an! □

Überlegen Sie die Gültigkeit der folgenden Aussage!

Korollar 2.1 Das direkte Produkt $\mathcal{G} = \mathcal{G}_1 \times \ldots \times \mathcal{G}_n = (M_1 \times \ldots \times M_n, *)$ der Gruppen $\mathcal{G}_I = (M_i, *_i)$ mit den Einselementen e_i, $1 \leq i \leq n$, bildet selbst wieder eine Gruppe. Insbesondere ist $e = (e_1, \ldots, e_n)$ das Einselement von $\mathcal{G}$, und das Inverse von $x = (x_1, \ldots, x_n)$ ist $x^{-1} = (x_1^{-1}, \ldots, x_n^{-1})$. □

2.3 Elementordnungen

Wir haben in den bisherigen Beispielen und Übungen auch immer die Gruppenordnung und Elementordnungen betrachtet. Wenn man die Ergebnisse etwas genauer analysiert, kann man Vermutungen aussprechen wie z.B., dass die Ordnung eines Elementes immer die Gruppenordnung teilt sowie dass, wenn $a^r = e$ gilt, r ein Vielfaches der Elementordnung ist. Die folgenden Sätze bestätigen diese Vermutungen und machen weitere wichtige Aussagen über diese Begriffe und deren Zusammenhänge. Dazu erinnern wir uns daran, dass gemäß Definition 2.2 d)

$$a^{ord_{\mathcal{G}}(a)} = e \tag{2.4}$$

für alle $a \in \mathcal{G}$ ist.

Satz 2.2 Sei $\mathcal{G}$ eine Gruppe mit Einselement e und $a \in \mathcal{G}$, dann gilt

a) $a^{ord_{\mathcal{G}}(a)+s} = a^s$ für alle $s \in \mathbb{Z}$;

b) $a^r = e$ genau dann, wenn $ord_{\mathcal{G}}(a) | \, r$ für alle $r \in \mathbb{Z}$;

c) $a^r = a^s$ genau dann, wenn $ord_{\mathcal{G}}(a) | \, r - s$ für alle $r, s \in \mathbb{Z}$.

Beweis **a)** Es gilt: $a^{ord_{\mathcal{G}}(a)+s} = a^{ord_{\mathcal{G}}(a)} * a^s = e * a^s = a^s$.

b) „⇒“: Gemäß Satz 1.1 gibt es zu r und $ord_{\mathcal{G}}(a)$ eindeutig einen Quotient q und einen Rest s mit $r = ord_{\mathcal{G}}(a) \cdot q + s$ und $0 \leq s < ord_{\mathcal{G}}(a)$. Damit folgt

$$e = a^r = a^{q \cdot ord_{\mathcal{G}}(a)+s} = \left(a^{ord_{\mathcal{G}}(a)}\right)^q * a^s = e^q * a^s = a^s$$

Falls $s = 0$ ist, ist die Behauptung gezeigt. Falls $s \geq 1$ ist, dann ist $a^s = e$ und $s < ord_{\mathcal{G}}(a)$, was ein Widerspruch dazu ist, dass die Ordnung von a der kleinste Exponent $k \geq 1$ mit $a^k = e$ ist. Für $s \geq 1$ erhalten wir also einen Widerspruch, also kann nur $s = 0$ sein, d.h. es ist $r = q \cdot ord_{\mathcal{G}}(a)$, womit die Behauptung gezeigt ist.

„⇐“: Aus $ord_{\mathcal{G}}(a) | \, r$ folgt, dass es ein q gibt mit $r = ord_{\mathcal{G}} \cdot q$. Damit gilt

$$a^r = \left(a^{ord_{\mathcal{G}}(a)}\right)^q = e^q = e$$

was zu zeigen war. □

Übungsaufgaben

2.12 Beweisen sie die Aussage c)! □

Nun, c) folgt unmittelbar aus b), denn wir können die Gleichung $a^r = a^s$ äquivalent durch die Gleichung $a^{r-s} = e$ ersetzen.

Der folgende Satz macht Aussagen über die Ordnung von Potenzen von Gruppenelementen.

Satz 2.3 Sei $\mathcal{G}$ eine Gruppe. Dann gilt für alle $a \in \mathcal{G}$ und $n \in \mathbb{N}_0$:

a)

$$ord_{\mathcal{G}}(a^n) = \frac{ord_{\mathcal{G}}(a)}{(ord_{\mathcal{G}}(a), n)}$$

b) $ord_{\mathcal{G}}(a^n) | ord_{\mathcal{G}}(a)$,

c) $ord_{\mathcal{G}}(a^n) = ord_{\mathcal{G}}(a)$ genau dann, wenn $(ord_{\mathcal{G}}(a), n) = 1$.

Beweis **a)** Aus schreibtechnischen Gründen setzen wir $k = ord_{\mathcal{G}}(a)$. Wir zeigen

$$ord_{\mathcal{G}}(a^n) \left| \frac{k}{(k,n)} \quad \text{und} \quad \frac{k}{(k,n)} \right| ord_{\mathcal{G}}(a^n) \tag{2.5}$$

dann folgt mit Korollar 1.2 j) die Behauptung.

Es ist

$$(a^n)^{\frac{k}{(k,n)}} = (a^k)^{\frac{n}{(k,n)}} = e^{\frac{n}{(k,n)}} = e \tag{2.6}$$

Mit Satz 2.2 b) folgt hieraus

$$ord_{\mathcal{G}}(a^n) \left| \frac{k}{(k,n)} \right. \tag{2.7}$$

womit die erste Behauptung in (2.5) gezeigt ist.

Wegen (2.4) gilt

$$e = (a^n)^{ord_{\mathcal{G}}(a^n)}$$

Hieraus und aus (2.6) folgt

$$a^{n \cdot ord_G(a^n)} = a^{\frac{nk}{(k,n)}}$$

woraus mit Satz 2.2 c) gilt

$$k | n \cdot ord_{\mathcal{G}}(a^n) - \frac{nk}{(k,n)}$$

und hieraus folgt mit Korollar 1.2 h)

$$k | n \cdot ord_{\mathcal{G}}(a^n)$$

und hieraus

$$\frac{k}{(k,n)} \left| \frac{n}{(k,n)} \cdot ord_{\mathcal{G}}(a^n) \right.$$

Da

$$\left(\frac{k}{(k,n)}, \frac{n}{(k,n)}\right) = 1$$

ist (siehe Satz 1.4), folgt

$$\frac{k}{(k,n)} \Big| \mathit{ord}_{\mathcal{G}}(a^n)$$

womit auch die zweite Behauptung von (2.5) gezeigt ist.

b) folgt unmittelbar aus a).

c) folgt unmittelbar aus a). □

Der folgende Satz macht Aussagen über die Ordnung von Elementverknüpfungen.

Satz 2.4 Sei $\mathcal{G}$ eine Gruppe mit den Elementen a und b, die kommutieren, d.h. es gilt $a * b = b * a$, und die endliche Ordnung haben, dann gilt

a) $\mathit{ord}_{\mathcal{G}}(a * b) | \big[\mathit{ord}_{\mathcal{G}}(a), \mathit{ord}_{\mathcal{G}}(b)\big]$,

b) $\mathit{ord}_{\mathcal{G}}(a * b) = \mathit{ord}_{\mathcal{G}}(a) \cdot \mathit{ord}_{\mathcal{G}}(b)$ genau dann, wenn $(\mathit{ord}_{\mathcal{G}}(a), \mathit{ord}_{\mathcal{G}}(b)) = 1$ ist.

Beweis Wir setzen aus schreibtechnischen Gründen

$$\begin{aligned} r &= \mathit{ord}_{\mathcal{G}}(a) \\ s &= \mathit{ord}_{\mathcal{G}}(b) \\ k &= [\,r, s\,] \qquad (2.8) \\ \ell &= (r, s) \qquad (2.9) \end{aligned}$$

a) Aus (2.8) folgt $r|k$ und $s|k$ und daraus mit Satz 2.2 b) $a^{\,k} = e$ und $b^{\,k} = e$. Hieraus und mit der Voraussetzung, dass a und b kommutieren, folgt

$$e = a^{\,k} * b^{\,k} = (a * b)^{\,k}$$

und daraus wiederum mit Satz 2.2 b) $\mathit{ord}_{\mathcal{G}}(a * b)|k$, was zu zeigen war.

b) „⇒“: Es gilt mit Satz 1.16: $\mathit{ord}_{\mathcal{G}}(a * b) = r \cdot s = (r, s) \cdot [\,r, s\,]$. Hieraus folgt, da wegen a) $r \cdot s | [\,r, s\,]$ ist, $(r, s) = 1$ und damit die Behauptung.

„⇐“: Sei $(r, s) = 1$. Dann existieren gemäß Korollar 1.14 b) ganze Zahlen x und y mit $rx + sy = 1$. Hiermit und, da a und b kommutieren, gilt

$$(a * b)^{\,rx} = a^{\,rx} * b^{\,rx} = a^{\,rx} * b^{\,1-sy} = (a^{\,r})^{\,x} * (b^{\,s})^{\,-y} * b = b \qquad (2.10)$$

Hieraus folgt

$$e = e^{\,rx} = \Big((a * b)^{\,\mathit{ord}_{\mathcal{G}}(a*b)}\Big)^{\,rx} = \big((a * b)^{\,rx}\big)^{\,\mathit{ord}_{\mathcal{G}}(a*b)} = b^{\,\mathit{ord}_{\mathcal{G}}(a*b)} \qquad (2.11)$$

Hieraus folgt wegen Satz 2.2 b)

$$s | ord_{\mathcal{G}}(a * b) \tag{2.12}$$

Analog zu (2.10) und (2.11) erhalten wir

$$(a * b)^{sy} = a^{sy} * b^{sy} = a^{1-rx} * b^{sy} = a * (a^{r})^{-x} * (b^{s})^{y} = a$$

Hieraus folgt

$$e = e^{sy} = \left((a * b)^{ord_{\mathcal{G}}(a*b)}\right)^{sy} = \left((a * b)^{sy}\right)^{ord_{\mathcal{G}}(a*b)} = a^{ord_{\mathcal{G}}(a*b)}$$

und damit ebenfalls wegen Satz 2.2 b)

$$r | ord_{\mathcal{G}}(a * b) \tag{2.13}$$

Aus (2.12) und (2.13) folgt, dass $ord_{\mathcal{G}}(a * b)$ ein gemeinsames Vielfaches von r und s ist. Aus Korollar 1.18 b) folgt $[\, r, s \,] \,|\, ord_{\mathcal{G}}(a * b)$. Wegen a) folgt hieraus mit Korollar 1.2 j)

$$ord_{\mathcal{G}}(a * b) = [\, r, s \,] \tag{2.14}$$

Laut Satz Satz 1.16 gilt $r \cdot s = (r, s) \cdot [\, r, s \,]$. Laut Voraussetzung ist $(r, s) = 1$ und damit ist $r \cdot s = [\, r, s \,]$. Hieraus folgt mit (2.14) $ord_{\mathcal{G}}(a * b) = r \cdot s$, also $ord_{\mathcal{G}}(a * b) = ord_{\mathcal{G}}(a) \cdot ord_{\mathcal{G}}(b)$, was zu zeigen war. □

Bemerkung 2.1 In Satz 2.4 ist die Voraussetzung, dass die Elemente kommutieren wesentlich. Betrachten wir z.B. die Elemente $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{SL}_2(\mathbb{Z})$ in Übung 2.9 (2), dann stellen wir fest, dass $\mathbf{b}$ und $\mathbf{c}$ nicht kommutieren, und es gilt $\mathbf{a} = \mathbf{b} * \mathbf{c}$. Es ist aber $ord_{\mathcal{SL}_2(\mathbb{Z})}(\mathbf{a}) = \infty$, während $ord_{\mathcal{SL}_2(\mathbb{Z})}(\mathbf{b}) \cdot ord_{\mathcal{SL}_2(\mathbb{Z})}(\mathbf{c}) = 4 \cdot 6 = 24$ ist. □

2.4 Untergruppen

Bevor wir im nächsten Abschnitt weitere wichtige Zusammenhänge von Gruppen- und Elementordnungen betrachten, beschäftigen wir uns mit Untergruppen und deren Eigenschaften, die für diese Betrachtugen von Bedeutung sind.

2.4.1 Elementare Eigenschaften

Triviale Untergruppen

Korollar 2.2 Sei $\mathcal{G} = (M, *)$ eine Gruppe, dann sind $\mathcal{G}_{\{e\}}$ und $\mathcal{G}$ Untergruppen, die so genannten *trivialen Untergruppen* von $\mathcal{G}$. □

Satz 2.5 Sei $\mathcal{G} = (M, *)$ eine Gruppe. Dann gilt:

a) Sei $U \subseteq M$. $\mathcal{G}_U$ ist eine Untergruppe von $\mathcal{G}$ genau dann, wenn gilt: Ist $a, b \in \mathcal{G}_U$, dann ist auch $a^{-1} * b \in \mathcal{G}_U$.

b) Sei $U \subseteq M$. $\mathcal{G}_U$ ist eine Untergruppe von $\mathcal{G}$ genau dann, wenn gilt: Ist $a, b \in \mathcal{G}_U$, dann ist auch $a * b^{-1} \in \mathcal{G}_U$.

c) Sei $a \in \mathcal{G}$ und $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$, dann ist $\mathcal{G}_{\langle a \rangle}$ eine Untergruppe von $\mathcal{G}$.

d) Sei $a \in \mathcal{G}$, dann ist $ord_{\mathcal{G}}(a) = ord_{\mathcal{G}_{\langle a \rangle}}$.

Beweis **a)** "⇒": Diese Richtung ist offensichtlich.

„⇐ ": $\mathcal{G}_U$ muss assoziativ sein, sonst wäre $\mathcal{G}$ nicht assoziativ. Wir setzen $b = a$, dann ist $a^{-1} * a \in \mathcal{G}_U$, also $e \in \mathcal{G}_U$, $\mathcal{G}_U$ enthält also das Einselement. Wir setzen jetzt $b = e$, dann ist $a^{-1} * e \in \mathcal{G}_U$, also $a^{-1} \in \mathcal{G}_U$, zu a enthält $\mathcal{G}_U$ also das Inverse a^{-1}. Wir zeigen noch die Abgeschlossenheit von $\mathcal{G}_U$, d.h. ist $x, y \in \mathcal{G}_U$, dann ist auch $x * y \in \mathcal{G}_U$: Setze $a = x^{-1}$ sowie $b = y$, dann ist $a, b \in \mathcal{G}_U$ und damit $a^{-1} * b \in \mathcal{G}_U$, also $x * y \in \mathcal{G}_U$.

b) anaolog zu a).

c) Wir wenden b) an und zeigen, dass aus $x, y \in \langle a \rangle$ folgt: $x * y^{-1} \in \langle a \rangle$. Sei also $x, y \in \langle a \rangle$. Dann gibt es $r, s \in \mathbb{Z}$ mit $x = a^r$ sowie $y = a^s$. Dann ist $x * y^{-1} = a^r * a^{-s} = a^{r-s} \in \langle a \rangle$, da $r - s \in \mathbb{Z}$ ist.

d) Ist die Ordnung von a unendlich, dann ist $a^r \neq a^s$ für $r \neq s$. Daraus folgt, dass $\langle a \rangle$ unendliche viele Elemente besitzt, also unendliche Ordnung hat. Ist die Ordnung von a endlich, dann folgt aus Satz 2.2 a) $a^{ord_{\mathcal{G}}(a) \cdot q + s} = a^s$ für alle $q \in \mathbb{Z}$ und $s \in \mathbb{N}_0$ mit $0 \leq s < ord_{\mathcal{G}}(a)$. Das bedeutet, dass es nur $ord_{\mathcal{G}}(a)$ verschiedene Elemente in $\langle a \rangle$ geben kann:

$$\langle a \rangle = \left\{ a^0, a^1, a^2, a^3, \ldots, a^{ord_{\mathcal{G}}(a)-1} \right\}$$

womit die Behauptung gezeigt ist. □

Übungsaufgaben

2.13 Sei $\mathcal{G} = (M, *)$ eine Gruppe mit $U_1, U_2 \subseteq \mathcal{G}$. Zeigen Sie: Sind $\mathcal{G}_{U_1} = (U_1, *)$ und $\mathcal{G}_{U_2} = (U_2, *)$ Untergruppen von $\mathcal{G}$, dann ist auch $\mathcal{G}_{U_1 \cap U_2} = (U_1 \cap U_2, *)$ Untergruppe von $\mathcal{G}$, d.h. der Durchschnitt von zwei Untergruppen von $\mathcal{G}$ bildet stets wieder eine Untergruppe von $\mathcal{G}$.

2.14 (1) Es sei $\mathcal{Z} = (\mathbb{Z}, +)$ die additive Gruppe der ganzen Zahlen. Zeigen Sie: Für jedes $m \in \mathbb{N}$ ist $\mathcal{Z}_m = (m\mathbb{Z}, +)$ mit $m\mathbb{Z} = \{m \cdot x \mid x \in \mathbb{Z}\}$ eine Untergruppe von $\mathcal{Z}$.

(2) Sei $\mathcal{G} = (M, *)$ eine abelsche Gruppe. $U \subseteq M$ sei definiert durch

$$U = \left\{ a \in \mathcal{G} \mid ord_{\mathcal{G}}(a) \in \mathbb{U}_+ \right\}$$

Beweisen Sie, dass $\mathcal{G}_U \trianglelefteq \mathcal{G}$ gilt!

Involution

2.15 Sei $\mathcal{G}$ eine Gruppe sowie $\mathcal{I}(\mathcal{G}) = \left\{ x \in \mathcal{G} \mid x^2 = e \right\}$ die Menge der *Involutionen* von $\mathcal{G}$.

(1) Begründen Sie, dass $\mathcal{I}(\mathcal{G}) \neq \emptyset$ für alle Gruppen $\mathcal{G}$ gilt!

(2) Bestimmen Sie $\mathcal{I}(\mathcal{Z}_m)$ für alle $m \geq 2$ (zur Definition von $\mathcal{Z}_m$ siehe Übung 2.14)!

(3) Begründen Sie, dass $\left|\mathcal{I}(\mathbb{Z}_m^*\right|) \geq 2$ für alle $m \geq 3$ gilt!

(4) Zeigen Sie: Ist $\mathcal{G}$ abelsch, dann gilt $\mathcal{I}(\mathcal{G}) \trianglelefteq \mathcal{G}$.

Zentrum einer Gruppe

2.16 Sei $\mathcal{G}$ eine Gruppe. Dann heißt $\mathcal{C}(\mathcal{G}) = \{a \in \mathcal{G} \mid x * a = a * x,\ x \in \mathcal{G}\}$ das *Zentrum* von $\mathcal{G}$. $\mathcal{C}(\mathcal{G})$ enthält alle Elemente von $\mathcal{G}$, die mit allen Elementen von $\mathcal{G}$ kommutieren. Zeigen Sie:

(1) Ist $\mathcal{G}$ abelsch, dann ist $\mathcal{C}(\mathcal{G}) = \mathcal{G}$.

(2) Für alle Gruppen $\mathcal{G}$ ist $|\mathcal{C}(\mathcal{G})| \geq 1$, d.h. das Zentrum einer Gruppe ist niemals leer.

(3) Es gilt $\mathcal{C}(\mathcal{G}) \trianglelefteq \mathcal{G}$ für alle Gruppen $\mathcal{G}$.

2.17 Für eine Gruppe $\mathcal{G} = (M, *)$ und zwei Untergruppen $\mathcal{G}_1 \trianglelefteq \mathcal{G}$ und $\mathcal{G}_2 \trianglelefteq \mathcal{G}$ sei $\mathcal{G}_1 * \mathcal{G}_2 = \{a * b \mid a \in \mathcal{G}_1,\ b \in \mathcal{G}_2\}$.

Sei nun $U \subseteq M$ mit $\mathcal{G}_U \trianglelefteq \mathcal{G}$.

(1) Beweisen Sie, dass $\mathcal{G}_U * \mathcal{G}_U = \mathcal{G}_U$ gilt!

(2) Beweisen Sie, dass $\mathcal{G}_U = \mathcal{G}_U^{-1}$ ist! Dabei Ist $\mathcal{G}_U^{-1} = \left\{ a^{-1} \mid a \in \mathcal{G}_U \right\}$

(3) Beweisen Sie, dass $\mathcal{G}_U * \mathcal{G}_U^{-1} = \mathcal{G}_U$ ist!

(4) Beweisen Sie, dass Folgendes gilt: Ist $a * \mathcal{G}_U = b * \mathcal{G}_U$ für $a, b \in \mathcal{G}$, dann folgt $a * \mathcal{G}_U * a^{-1} = b * \mathcal{G}_U * b^{-1}$! □

2.4.2 Zyklische Gruppen

Wir knüpfen nun an Satz 2.5 c) anund betrachten in diesem Abschnitt zyklische Gruppen etwas näher.

Definition 2.4 **a)** Sei $\mathcal{G}$ eine Gruppe und $a \in \mathcal{G}$, dann heißt $\langle a \rangle$ die von a *erzeugte zyklische Untergruppe von* $\mathcal{G}$.

Generator Primitives Element

b) Sei $\mathcal{G}$ eine Gruppe. Gibt es ein $g \in \mathcal{G}$ mit $\langle g \rangle = \mathcal{G}$, dann heißt $\mathcal{G}$ *zyklisch*, und g ist ein *Generator* (auch *primitves Element*) von $\mathcal{G}$. □

Beispiel 2.3 Es sei $\mathbb{Z}_5^* = (\{1,2,3,4\},\cdot)$ die multiplikative Gruppe modulo 5 aus Abbildung 8. Für diese gilt:

$$\begin{aligned}\langle 1 \rangle &= \{1\}\\ \langle 2 \rangle &= \{1,2,4,3\} = \mathbb{Z}_5^*\\ \langle 3 \rangle &= \{1,3,4,2\} = \mathbb{Z}_5^*\\ \langle 4 \rangle &= \{1,4\}\end{aligned}$$

$\mathbb{Z}_5^*$ ist eine zyklische Gruppe mit den Generatoren 2 und 3. □

Übungsaufgaben

2.18 (1) Berechnen Sie alle zyklischen Untergruppen der multiplikativen Gruppe $\mathbb{Z}_7^*$ modulo 7! Ist diese Gruppe zyklisch?

(2) Zeigen Sie, dass die additiven Produktgruppen $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$, $k \in \mathbb{N}$ nicht zyklisch sind! □

Korollar 2.3 Zyklische Gruppen sind abelsch. □

Übungsaufgaben

2.19 Beweisen Sie Korollar 2.3! □

Sei $x, y \in \langle a \rangle$, d.h. es gibt $r, s \in \mathbb{Z}$ mit $x = a^r$ und $y = a^s$. Es gilt:

$$x * y = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = y * x$$

Wir beweisen jetzt einen Satz über eine Eigenschaft von zyklischen Gruppen, den wir später benötigen, um eine wesentliche Eigenschaft eines Primzahltests zu beweisen.

Satz 2.6 Sei $\mathcal{G}$ eine endliche Gruppe mit Einselement e und $a \in \mathcal{G}$ sowie

$$\langle a \rangle = \left\{e, a, a^2, a^3, \ldots, a^{r-1}\right\} = \left\{a, a^2, a^3, \ldots, a^{r-1}, a^r\right\}$$

die von a erzeugte zyklische Untergruppe mit Ordnung r. Dann gibt es genau $t = (k, r)$ Elemente in $\langle a \rangle$, die die Gleichung $x^k = e$ lösen.

Beweis Ein Element $a^j \in \langle a \rangle$, $1 \leq j \leq r$, erfüllt die Gleichung $x^k = e$ genau dann, wenn $a^{jk} = e$ gilt. Mit Satz 2.2 b) folgt, dass $r|jk$ ist. Hieraus folgt, da $t = (k, r)$ ist, $\frac{r}{t}|j \cdot \frac{k}{t}$. Aus Satz 1.4 folgt $\left(\frac{r}{t}, \frac{k}{t}\right) = 1$. Und damit folgt, dass $\frac{r}{t}|j$ ist, also $j = \frac{r}{t} \cdot q$ für ein geeignetes $q \in \mathbb{N}$ gilt. Da $1 \leq j \leq r$ gilt, folgt $1 \leq \frac{r}{t} \cdot q \leq r$ und daraus $\frac{t}{r} \leq q \leq t$. Da $r \geq t$ gilt, ist $\frac{t}{r} \leq 1$, und, da $q \in \mathbb{N}$ ist, gilt $1 \leq q \leq t$. Das heißt: q kann t Werte annehmen. Da $j = \frac{r}{t} \cdot q$ ist und r und k fest gegeben sind, kann j ebenfalls t Werte annehmen, womit die Behauptung gezeigt ist. □

Beispiel 2.4 Wir betrachten die zyklische Gruppe $\mathbb{Z}_7^*$ aus Übung 2.18. 3 ist ein Generator der Gruppe, $\langle 3 \rangle = \mathbb{Z}_7^*$, mit $ord(3) = 6$. Die Lösungen der Gleichung $x^2 = 1$ sind die Selbstinversen in dieser Gruppe. Es gilt gemäß dem obigen Satz, dass es $t = (2, 6) = 2$ Lösungen dieser Gleichung, also zwei selbstinverse Elemente gibt. Da das Einselement 1 und das additive Inverse davon, in $\mathbb{Z}_7^*$ ist das 6, immer selbstinvers sind, gibt es in $\mathbb{Z}_7^*$ also keine weiteren selbstinversen Elemente (was wir aus Übung 2.18 schon wissen). □

Übungsaufgaben

2.20 Wie viele Lösungen der Gleichung $x^3 = 1$ gibt es in $\mathbb{Z}_7^*$?

Nun, gemäß Satz 2.6 gibt es $t = (3, 6) = 3$ Lösungen. Eine Lösung ist offensichtlich $x = 1$, die beiden anderen sind $x = 2$ und $x = 4$. Wenn wir die Gleichung $x^3 = 1$ wie folgt schreiben: $x^2 \cdot x = 1$ und diese umschreiben zu $x^{-1} = x^2$, dann suchen wir Elemente x mit der Eigenschaft, dass x^2 invers zu x ist. Es folgt unmittelbar, dass 2 und 4 invers zueinander sind.

2.5 Faktorisierung von Gruppen

Wenn man bei den bisherigen Beispielen und Übungen zu endlichen Gruppen jeweils die Gruppenordnungen und die Ordnungen ihrer Untergruppen betrachtet, stellt man fest, dass Untergruppenordnungen immer Teiler der Gruppenordnung sind. Wir werden in diesem Abschnitt sehen, dass diese – auch für viele Anwendungen – wesentliche Eigenschaft von endlichen Gruppen allgemein gilt. Auf dem Weg dorthin verallgemeinern wir – wie bereits am Ende von Abschnitt 1.2.3 angekündigt – das Rechnen mit Äquivalenzklassen.

2.5.1 Nebenklassen

Definition 2.5 Sei $\mathcal{G} = (M, *)$ eine Gruppe, $U \subseteq M$ und $\mathcal{G}_U \trianglelefteq \mathcal{G}$ sowie $a \in \mathcal{G}$.

a) Dann heißt **Linksnebenklasse**

$$a * \mathcal{G}_U = \{\, a * x \mid x \in \mathcal{G}_U \,\}$$

Linksnebenklasse von $\mathcal{G}_U$, und **Rechtsnebenklasse**

$$\mathcal{G}_U * a = \{\, x * a \mid x \in \mathcal{G}_U \,\}$$

Rechtsnebenklasse von $\mathcal{G}_U$. $\mathcal{G}/\mathcal{G}_U = \{\, a * U \mid a \in \mathcal{G} \,\}$ ist die Menge aller Linsknebenklassen von $\mathcal{G}_U$ und $\mathcal{G}_U\backslash\mathcal{G} = \{\, U * a \mid a \in \mathcal{G} \,\}$ die Menge der Rechtsnebenklassen von $\mathcal{G}_U$. Anstelle von $a * \mathcal{G}_U$ und $\mathcal{G}_U * a$ schreiben wir auch $a\mathcal{G}_U$ bzw. $\mathcal{G}_U a$ oder auch aU bzw. Ua sowie $\mathcal{G}/U$ und $U\backslash\mathcal{G}$ anstelle von $\mathcal{G}/\mathcal{G}_U$ bzw. von $\mathcal{G}_U\backslash\mathcal{G}$.

b) a heißt *Repräsentant* der Nebenklasse $a * \mathcal{G}_U$ bzw. der Nebenklasse $\mathcal{G} * a$. **Repräsentant einer Nebenklasse**

c) Gilt $a * \mathcal{G}_U = \mathcal{G}_U * a$ für alle $a \in \mathcal{G}$, dann heißt $\mathcal{G}_U$ ein *Normalteiler* von $\mathcal{G}$. □ **Normalteiler**

Es gilt offensichtlich

Korollar 2.4 Ist $\mathcal{G}$ ein Normalteiler der Gruppe $\mathcal{G}$, dann gilt $a * \mathcal{G}_U = \mathcal{G}_U * a$ für alle $a \in \mathcal{G}$ sowie $\mathcal{G}/\mathcal{G}_U = \mathcal{G}_U\backslash\mathcal{G}$ □

Beispiel 2.5 Aus Beispiel 2.3 wissen wir, dass $\langle\, 4 \,\rangle = \{1, 4\}$ eine Untergruppe von $\mathbb{Z}_5^*$ ist. Wir bestimmen alle Linksnebenklassen dieser Untergruppe:

$$\begin{aligned} 1 \cdot \langle\, 4 \,\rangle &= \{1, 4\} = \langle\, 4 \,\rangle \\ 2 \cdot \langle\, 4 \,\rangle &= \{2, 3\} \\ 3 \cdot \langle\, 4 \,\rangle &= \{3, 2\} \\ 4 \cdot \langle\, 4 \,\rangle &= \{4, 1\} = \langle\, 4 \,\rangle \end{aligned}$$

Da $\mathbb{Z}_5^*$ abelsch ist, gilt $a \cdot \langle\, 4 \,\rangle = \langle\, 4 \,\rangle \cdot a$ für alle $a \in \mathbb{Z}_5^*$, d.h. $\langle\, 4 \,\rangle$ ist ein Normalteiler von $\mathbb{Z}_5^*$.

Des Weiteren gilt $\mathbb{Z}_5^*/\langle\, 4 \,\rangle = \{\{1, 4\}, \{2, 3\}\} = \langle\, 4 \,\rangle\backslash\mathbb{Z}_5^*$. □

Übungsaufgaben

2.21 Berechnen Sie alle Nebenklassen der Untergruppe $\langle\, 2 \,\rangle$ in $\mathbb{Z}_7^*$!

2.22 Sei $\mathcal{G} = (M, *)$ eine endliche Gruppe mit $U \subseteq M$ und $\mathcal{G}_U \trianglelefteq \mathcal{G}$. Für jedes $a \in \mathcal{G}$ sei die Abbildung $\varphi_a : U \to aU$ definiert durch $\varphi_a(x) = a * x$. Zeigen Sie, dass φ_a bijektiv, d.h. dass $|U| = |aU|$ für alle $a \in \mathcal{G}$ ist! □

Korollar 2.5 Sei $\mathcal{G}$ eine Gruppe und $\mathcal{G}_U \trianglelefteq \mathcal{G}$. Dann gilt

a) $a \in a * \mathcal{G}_U$ für alle $a \in \mathcal{G}$;

b) $a * \mathcal{G}_U = b * \mathcal{G}_U$ für alle $b \in a * \mathcal{G}_U$, d.h. eine Nebenklasse ist unabhängig von ihrem Repräsentanten, sprich: Jedes Element einer Nebenklasse kann als ihr Repräsentant dienen;

c) $a * \mathcal{G}_U = a^{-1} * \mathcal{G}_U$;

d) $a^{-1} \in a * \mathcal{G}_U$.

Beweis **a)** gilt, weil $e \in \mathcal{G}_U$ ist.

b) Da $b \in a * \mathcal{G}_U$ ist, gibt es ein $x_b \in \mathcal{G}_U$ mit $b = a * x_b$, d.h. mit $a = b * x_b^{-1}$. Dies verwenden wir, um (1) $a * \mathcal{G}_U \subseteq b * \mathcal{G}_U$ und (2) $b * \mathcal{G}_U \subseteq a * \mathcal{G}_U$ zu zeigen, womit die Behauptung gezeigt ist.

Zu (1): Sei $c \in a * \mathcal{G}_U$. Dann gibt es $x_c \in \mathcal{G}_U$ mit $c = a * x_c$. Es folgt $c = b * x_b^{-1} * x_c$ und damit $c \in b * \mathcal{G}_U$, da $x_b^{-1} * x_c \in \mathcal{G}_U$ ist.

Zu (2): Sei $c \in b * \mathcal{G}_U$. Dann gibt es $y_c \in \mathcal{G}_U$ mit $c = b * y_c$. Es folgt $c = a * x_b * y_c$ und damit $c \in a * \mathcal{G}_U$, da $x_b * y_c \in \mathcal{G}_U$ ist.

c) Mithilfe von Satz 2.1 c) und e) sowie Übung 2.17 (2) rechnen wir:

$$a * \mathcal{G}_U = \left((a * \mathcal{G}_U)^{-1}\right)^{-1} = \left(\mathcal{G}_U^{-1} * a^{-1}\right)^{-1} = \left(\mathcal{G}_U * a^{-1}\right)^{-1} = a^{-1} * \mathcal{G}_U^{-1} = a^{-1} * \mathcal{G}_U$$

d) folgt unmittelbar aus a) und c). □

2.5.2 Faktorgruppen

Wir führen nun eine Verknüpfung für die Nebenklassen von Normalteilern ein und werden feststellen, dass dadurch eine neue Gruppenstruktur entsteht.

Definition 2.6 Sei $\mathcal{G} = (M, *)$ eine Gruppe, $U \subseteq M$ und $\mathcal{G}_U \trianglelefteq \mathcal{G}$ ein Normalteiler von $\mathcal{G}$. Dann ist die Verknüpfung $*_U : \mathcal{G}/\mathcal{G}_U \times \mathcal{G}/\mathcal{G}_U \to \mathcal{G}/\mathcal{G}_U$ definiert durch

$$(a * \mathcal{G}_U) *_U (b * \mathcal{G}_U) = (a * b) * \mathcal{G}_U \tag{2.15}$$

Korollar 2.6 Für die in dieser Definition festgelegte Verknüpfung von Nebenklassen gilt für $a' \in a * \mathcal{G}_U$ und $b' \in b * \mathcal{G}_U$

$$(a * b) * \mathcal{G}_U = (a' * b') * \mathcal{G}_U \tag{2.16}$$

Die in (2.15) festgelegt Verknüpfung von Nebenklassen ist als unabhängig vom gewählten Repräsentanten; man sagt deshalb auch, dass diese Verknüpfung *wohldefiniert* ist.

Beweis Zu $a' \in a * \mathcal{G}_U$ gibt es $x_{a'} \in \mathcal{G}_U$ mit $a' = a * x_{a'}$ und zu $b' \in b * \mathcal{G}_U$ gibt es $x_{b'} \in \mathcal{G}_U$ mit $b' = b * x_{b'}$. Damit überlegen wir

$$
\begin{aligned}
c \in (a' * b') * \mathcal{G}_U \quad & \text{gdw. es } x_c \in \mathcal{G}_U \text{ gibt mit} \\
& \quad c = (a' * b') * x_c \\
& \text{gdw. } \; c = (a * x_{a'}) * (b * x_{b'}) * x_c \\
& \text{gdw. } \; c = a * (x_{a'} * b) * x_{b'} * x_c \\
& \text{gdw. } \; c \in a * (\mathcal{G}_U * b) * \mathcal{G}_U && \text{da } x_{a'}, x_{b'}, x_c \in \mathcal{G}_U \\
& \text{gdw. } \; c \in a * (b * \mathcal{G}_U) * \mathcal{G}_U && \text{da } \mathcal{G}_U \text{ Normalteiler} \\
& \text{gdw. } \; c \in (a * b) * (\mathcal{G}_U * \mathcal{G}_U) \\
& \text{gdw. } \; c \in (a * b) * \mathcal{G}_U && \text{wegen Übung 2.17 (1)}
\end{aligned}
$$

womit die Behauptung gezeigt ist. □

Satz 2.7 Sei $\mathcal{G} = (M, *)$ eine Gruppe, $U \subseteq M$ und $\mathcal{G}_U \trianglelefteq \mathcal{G}$ ein Normalteiler von $\mathcal{G}$. Dann bildet $(\mathcal{G}/\mathcal{G}_U, *_U)$ mit $(a * \mathcal{G}_U) *_U (b * \mathcal{G}_U) = (a * b) * \mathcal{G}_U$ eine Gruppe, die so genannte *Faktorgruppe von* $\mathcal{G}$ nach $\mathcal{G}_U$. **Faktorgruppe**

Beweis Die Verknüpfung $*_U$ ist offensichtlich abgeschlossen.

Die Verknüpfung ist assoziativ, denn es gilt:

$$
\begin{aligned}
((a * \mathcal{G}_U) *_U (b * \mathcal{G}_U)) *_U (c * \mathcal{G}_U) &= ((a * b) * \mathcal{G}_U) *_U (c * \mathcal{G}_U) \\
&= ((a * b) * c) * \mathcal{G}_U \\
&= (a * (b * c)) * \mathcal{G}_U \\
&= (a * \mathcal{G}_U) *_U ((b * c) * \mathcal{G}_U) \\
&= (a * \mathcal{G}_U) *_U ((b * \mathcal{G}_U) *_U (c * \mathcal{G}_U))
\end{aligned}
$$

$e * \mathcal{G}_U = \mathcal{G}_U$ ist das Einselement, denn es ist

$$\mathcal{G}_U *_U (a * \mathcal{G}_U) = (e * \mathcal{G}_U) *_U (a * \mathcal{G}_U) = (e * a) * \mathcal{G}_U = a * \mathcal{G}_U$$

Zu $a * \mathcal{G}_U$ ist $a^{-1} * \mathcal{G}_U$ das Inverse, denn es gilt

$$(a * \mathcal{G}_U) *_U (a^{-1} * \mathcal{G}_U) = (a * a^{-1}) * \mathcal{G}_U = e * \mathcal{G}_U = \mathcal{G}_U$$

Beispiel 2.6 Wir greifen nun die Überlegungen zum Rechnen mit Restklassen vom Ende von Abschnitt 1.2.3 auf. Wir wissen, dass $(\mathbb{Z}, +)$, die Menge der ganzen Zahlen mit Addition, eine abelsche Gruppe bildet. Wir betrachten nun für $m \in \mathbb{N}$ die Menge $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$ (siehe Definiton 1.6). $m\mathbb{Z}$ bildet eine Untergruppe von $\mathbb{Z}$ (siehe Übung 2.14). $m\mathbb{Z}$ ist zudem Normalteiler in $\mathbb{Z}$, denn wegen der Kommutativität der Addition gilt $a + m\mathbb{Z} = m\mathbb{Z} + a$ für alle $a \in \mathbb{Z}$.

Die Nebenklassen von $m\mathbb{Z}$ in $\mathbb{Z}$ sind (siehe auch Definition 1.4, Korollare 1.8 und 1.9 sowie Satz 1.3)

$$r + m\mathbb{Z} = \{mx + r \mid x \in Z\}\,,\ 0 \leq r < m \tag{2.17}$$

$m\mathbb{Z}$ besitzt genau diese m Nebenklassen, denn zu $a \in \mathbb{Z}$ existiert wegen Satz 1.1 genau ein $x \in \mathbb{Z}$ und ein $r \in \mathbb{N}_0$ mit $a = mx + r$ und $0 \leq r < m$, d.h. zu $a \in \mathbb{Z}$ gibt es ganau ein r, $0 \leq r < m$ mit $a \in r + m\mathbb{Z}$.

Gemäß Definition 2.6 ergibt sich die Rechenstruktur $(\mathbb{Z}/m\mathbb{Z}, +_{m\mathbb{Z}})$ definiert durch

$$(a + m\mathbb{Z}) +_{m\mathbb{Z}} (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z} \tag{2.18}$$

Additive Restklassengruppe modulo m

Diese Addition der Nebenklassen ist gemäß Korollar 2.6 unabhängig vom gewählten Repräsentanten, und wegen Satz 2.7 bildet $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe, die additive Faktorgruppe von $\mathbb{Z}$ nach $m\mathbb{Z}$, auch *additive Restklassengruppe modulo* m genannt. □

Übungsaufgaben

2.23 Stellen Sie die Gruppentafel für die Faktorgruppe $\mathbb{Z}_7^*/\langle 2 \rangle$ auf! □

Quotientengruppe

Eine Untergruppe U teilt („faktorisiert“) die Elemente der Gruppe $\mathcal{G} = (M, *)$ in Teilmengen ein. Durch eine entsprechende Verallgemeinerung der Elementverknüpfung $*$ auf die Mengenverknüpfung $*_U$ erhält man eine Gruppenstruktur, die sogenannte Faktorgruppe (auch *Quotientengruppe*) $\mathcal{G}/\mathcal{G}_U$ von $\mathcal{G}$ nach $\mathcal{G}_U$. Wir werden im Folgenden zumeist nicht mehr zwischen den beiden Verknüpfungen unterscheiden und beide mit $*$ notieren, und wir werden, wie in Definition 2.5 schon erklärt, in der Regel die Nebenklasse $a * U$ durch aU bzw. $a * \mathcal{G}_U$ durch $a\mathcal{G}_U$ notieren.

2.5.3 Satz von Lagrange

Wenn wir die bisherigen Beispiele von Faktorgruppen betrachten, dann können wir folgende Beobachtungen machen: Nebenklassen sind entweder identisch oder disjunkt; die Nebenklassen einer Faktorgruppe haben die gleiche Anzahl von Elementen, nämlich genau so viele wie die Untergruppe, die die Faktorgruppe bestimmt, die ja das Einselement der Faktorgruppe darstellt. Außerdem greifen wir die schon füher aufgestellte Vermutung auf, dass die Ordnung von Untergruppen immer ein Teiler der Gruppenordnung ist. Diese Beobachtungen und Vermutungen bestätigt der folgende *Satz von Lagrange*.

Satz von Lagrange

Satz 2.8 Sei $\mathcal{G} = (M, *)$ eine endliche Gruppe, $U \subseteq M$ und $\mathcal{G}_U \trianglelefteq \mathcal{G}$.

(1) Für $a, b \in \mathcal{G}$ gilt entweder $aU = bU$ oder $aU \cap bU = \emptyset$. Analoges gilt für die Rechtsnebenklassen.

(2) Die Nebenklassen legen eine Äquivalenzrelation und damit eine Partition auf $\mathcal{G}$ fest.

(3) Es gilt $|aU| = |bU| = |U|$ für alle $a, b \in \mathcal{G}$. Analoges gilt für die Rechtsnebenklassen.

(4) Es gibt eine Zahl $r \in \mathbb{N}$ mit $|\mathcal{G}| = r \cdot |U|$, d.h. mit $ord_{\mathcal{G}} = r \cdot ord_{\mathcal{G}_U}$. Die Ordnungen von Untergruppen sind also immer Teiler der Gruppenordnung.

(5) Es ist $r = |\mathcal{G}/U| = |U\backslash\mathcal{G}|$, und r heißt *Index* von U in $\mathcal{G}$. Schreibweise: $[\mathcal{G} : U] = r$. Es gilt also $|\mathcal{G}| = [\mathcal{G} : U] \cdot |U|$, anders formuliert $ord_{\mathcal{G}} = [\mathcal{G} : U] \cdot ord_{\mathcal{G}_U}$. **Index**

(6) Für die trivialen Untergruppen $U = \{e\}$ und $U = \mathcal{G}$ gilt

$$[\mathcal{G} : \{e\}] = |\mathcal{G}| \text{ bzw. } [\mathcal{G} : \mathcal{G}] = 1$$

(7) Ist $\mathcal{G}_U$ keine triviale Untergruppe von $\mathcal{G}$, dann gilt

$$|\mathcal{G}| \geq 2 \cdot |U|, \text{ d.h. } \frac{ord_{\mathcal{G}}}{2} = \frac{|\mathcal{G}|}{2} \geq |U| = ord_{\mathcal{G}_U}$$

Beweis (1) Wenn $a = b$ ist, folgt $aU = bU$. Es sei also $a \neq b$. Des Weiteren sei $aU \cap bU \neq \emptyset$, d.h. es gibt mindestens ein $c \in aU \cap bU$. Wir betrachten zwei Fälle:

(i) Es gibt $x \in U$ mit $c = ax$ und $c = bx$.

(ii) Es gibt $x, y \in U$, $x \neq y$, mit $c = ax$ und $c = by$.

Zu (i): Aus $c = ax$ und $c = bx$ folgt $ax = bx$ und daraus $a = b$, ein Widerspruch zur Voraussetzung $a \neq b$. Die Annahme $aU \cap bU \neq \emptyset$ führt also im Fall (i) zu einem Widerspruch, es folgt somit $aU \cap bU = \emptyset$.

Zu (ii): Aus $c = ax$ und $c = by$ folgt $ax = by$ und daraus $a = byx^{-1}$. Sei $d \in aU$, dann gibt es $z \in U$ mit $d = az$. Es folgt $d = byx^{-1}z$. Da U Untergruppe und $x, y, z \in U$ ist, ist $u = yx^{-1}z \in U$ und damit $d = bu \in bU$. Wir haben gezeigt, dass $aU \subseteq bU$ ist. Analog kann gezeigt werden, dass $bU \subseteq aU$ ist. Es folgt also im Fall (ii) die Gleichheit $aU = bU$.

(2) Aus (1) folgt, dass die Nebenklassen entweder identisch oder disjunkt sind. Wir müssen noch zeigen, dass die Vereinigung aller Nebenklassen gleich der Gruppe ist, also

$$\bigcup_{a \in \mathcal{G}} aU = \mathcal{G}$$

gilt. Offensichtlich ist $\bigcup_{a\in\mathcal{G}} aU \subseteq \mathcal{G}$. Wir müssen noch $\mathcal{G} \subseteq \bigcup_{a\in\mathcal{G}} aU$ zeigen: Sei dazu $b \in \mathcal{G}$. Es gilt $b = b * e$ und damit $b \in bU$, da $e \in U$ ist. Also ist $b \in \bigcup_{a\in\mathcal{G}} aU$.

(3) folgt unmittelbar aus Übung 2.22.

(4) folgt unmittelbar aus (2) und (3): $\mathcal{G}$ wird vollständig, disjunkt überdeckt von allen Nebenklassen, und diese besitzen alle dieselbe Anzahl von Elementen, nämlich genau $|U|$ viele. Es folgt, dass r die Anzahl der Nebenklassen, d.h. die Anzahl der Elemente in der Faktorgruppe $\mathcal{G}/\mathcal{G}_{U}$ ist.

(5) folgt unmittelbar aus (4).

(6) ist offensichtlich: In $\mathcal{G}/\mathcal{G}_{\{e\}}$ bildet jedes Element $a \in \mathcal{G}$ eine Nebenklasse $\{a\}$. In $\mathcal{G}/\mathcal{G}$ ist $\mathcal{G}$ die einzige Nebenklasse.

(7) Da $\mathcal{G}_{U}$ nicht trivial ist, muss $2 \leq |U| < |\mathcal{G}|$, also $|\mathcal{G}| \geq 3$ sein. Es sei also $\mathcal{G} = \{ e, a_1, a_2, \ldots, a_{k-1} \}$ mit $k \geq 3$. Es gilt $U = eU \neq a_i U$, $1 \leq i \leq k-1$. Daraus folgt, dass es mindestens zwei Nebenklassen gibt, nämlich U und z.B. $a_1 U$ (von den anderen Nebenklassen $a_i U$, $2 \leq i \leq k-1$, könnten welche verschieden von $a_1 U$ und welche (sogar alle) könnten gleich $a_1 U$ sein). Da es somit aber mindestens zwei Nebenklassen gibt, ist der Index größer gleich 2: $[\mathcal{G} : U] \geq 2$. Mit (5) folgt dann

$$|\mathcal{G}| = [\mathcal{G} : U] \cdot |U| \geq 2 \cdot |U|$$

womit die Behauptung gezeigt ist. □

Bemerkung 2.2 Die Aussagen (4) und (5) bilden die eigentliche Aussage des Satzes von Lagrange: Für eine endliche Gruppe $\mathcal{G}$ und eine Untergruppe $\mathcal{G}_{U} \trianglelefteq \mathcal{G}$ gilt, dass die Untergruppenordnung ein Teiler der Gruppenordnung ist:

$$|\mathcal{G}| = [\, \mathcal{G} : \mathcal{G}_{U} \,] \cdot |\mathcal{G}_{U}| \tag{2.19}$$

Die Aussagen (1) – (3) sind Hilfsaussagen, mit denen der Satz bewiesen werden kann. Die Aussagen (6) und (7) betrachten Spezialfälle. Der Satz von Lagrange ist von immanenter Bedeutung in der Gruppentheorie und in ihren Anwendungen. Das werden wir in späteren Kapitel noch sehen, z.B. bei der Verschlüsselung von Daten sowie bei Primzahltests. □

Korollar 2.7 Sei $\mathcal{G}$ mit $ord_{\mathcal{G}} \in \mathbb{P}$. Dann gilt:

a) $\mathcal{G}$ besitzt außer den trivialen keine weiteren Untergruppen.

b) $\mathcal{G}$ ist zyklisch.

c) $\mathcal{G}$ ist abelsch.

Beweis **a)** folgt unmittelbar aus dem Satz 2.8 (4): Primzahlen besitzen keine echten Teiler, also kann $\mathcal{G}$ keine echten Untergruppen besitzen, da deren Ordnung Teiler der Gruppenordnung sind. Somit besitzt $\mathcal{G}$ nur die trivialen Untergruppen.

b) $\langle a \rangle$ bildet gemäß Satz 2.5 c) eine Untergruppe von $\mathcal{G}$ für jedes $a \in \mathcal{G}$. Da wegen a) $\mathcal{G}$ außer den trivialen Untergruppen keine weiteren Untergruppen besitzt, muss $\langle a \rangle = \mathcal{G}$ für $a \neq e$ ein. Also ist $\mathcal{G}$ gemäß Definition 2.4 b) zyklisch.

c) Folgt aus b) und Korollar 2.3. □

Korollar 2.8 Sei $\mathcal{G} = (M, *)$ eine endliche Gruppe.

a) Sei $a \in \mathcal{G}$, dann ist $ord_{\mathcal{G}}(a) | ord_{\mathcal{G}}$.

b) Sei $a \in \mathcal{G}$, dann ist $a^{ord_{\mathcal{G}}} = e$.

c) Ist $\mathcal{G}$ zyklisch und $g \in \mathcal{G}$ ein Generator von $\mathcal{G}$, dann gilt $g^n = e$ genau dann, wenn $ord_{\mathcal{G}} | n$ gilt.

Beweis **a)** Wegen Satz 2.5 d) gilt $ord_{\mathcal{G}}(a) = ord_{\mathcal{G}_{\langle a \rangle}}$ und aus dem Satz 2.8 (4) folgt $ord_{\mathcal{G}_{\langle a \rangle}} | ord_{\mathcal{G}}$, also gilt auch $ord_{\mathcal{G}}(a) | ord_{\mathcal{G}}$.

b) folgt aus a) und Satz 2.2 b).

c) folgt aus b) und Satz 2.2 b). □

2.6 Gruppenhomomorphismen

Wir haben in den bisherigen Beispielen und Übungen eine Reihe von Gruppen betrachtet, welche dieselbe Anzahl von Elementen und verschiedene Verknüpfungen haben. Es stellt sich die Frage, ob diese Gruppen tatsächlich verschieden sind oder ob in ihnen nicht dasselbe berechnet wird, nur mit anderen Elementen und verschiedenen Bezeichnungen für die Verknüpfungen. In den folgenden Abschnitten führen wir Begriffe für den Vergleich von Gruppen ein.

2.6.1 Beispiele und Definitionen

Wie viele Gruppen mit genau einem Element gibt es? Nun, da jede Gruppe ein Einselement besitzen muss, enthalten Gruppen mit einem Element nur das Einselement. Solche Gruppen haben wir als triviale Untergruppen schon kennen gelernt: Die Untergruppen $(\{0\}, +)$ der additiven Gruppen $(\mathbb{Z}_m, +)$; die Untergruppe $(\{1\}, \cdot)$ der multiplikativen Gruppe $(\mathbb{Z}_7^*, \cdot)$; die Untergruppe $(\{id\}, \circ)$ der Funktionengruppe aus Übung 2.7. Die entsprechenden Gruppentafeln bestehen jeweils nur aus dem Einselement. Das heißt, wenn wir von den verschiedenen Bezeichnungen der Einselemente wie 0, 1 und id absehen, sind alle einelementigen Gruppen identisch; abstrakt betrachtet gibt es nur eine einzige Gruppe mit einem Element: $(\{e\}, *)$ mit der Verknüpfungstafel

$*$	e
e	e

Übungsaufgaben

2.24 Überlegen Sie, wie viele verschiedene Gruppen es mit zwei bzw. mit drei Elementen gibt! □

Nun betrachten wir die additive Verknüpfungstafel von $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$ ist eine additive abelsche Gruppe mit Einselement 0, und $y = 4 - x$ ist das additive Inverse zu $x \in \mathbb{Z}_4$; 0 und 2 sind selbstinvers, 1 und 3 sind invers zueinander.

Des Weiteren betrachten wir die multiplikative Verknüpfungstafel von $\mathbb{Z}_5^*$:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_5^*$ ist bezüglich der Multiplikation eine abelsche Gruppe mit Einselement 1. 1 und 4 sind invers zu sich selbst, 2 und 3 sind invers zueinander.

Die Frage ist, ob es sich hier ebenfalls um ein und dieselbe Gruppe handelt, d.h. gibt es eine eineindeutige Zuordnung der Elemente dieser beiden Gruppen, die verträglich mit den beiden Operationen ist, so dass es sich letztendlich um ein und dieselbe Rechenstruktur handelt. Wenn es sich abgesehen von der Benennung der Elemente und abgesehen von der Benennung der Verknüpfung um dieselbe Gruppe handeln soll, dann ist es einsichtig, dass die Einselemente einander zugeordnet werden sollten. Wir halten also schon einmal die Umbenennung $0 \to 1$ fest. Neben diesen beiden Elementen sind noch 2 in $\mathbb{Z}_4$ bzw. noch 4 in $\mathbb{Z}_5^*$ selbstinvers, also halten wir die Umbenennung $2 \to 4$ fest. Für die verbliebenen Elemente bleiben noch die beiden Zuordnungen $1 \to 2$ und $3 \to 3$ oder $1 \to 3$ und $3 \to 2$. Für die erste Zuordnung

$$\begin{aligned} 0 &\to 1 \\ 1 &\to 2 \\ 2 &\to 4 \\ 3 &\to 3 \end{aligned} \tag{2.20}$$

stellen wir die beiden Verknüpfungstafeln entsprechend nebeneinander:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Übungsaufgaben

2.25 Stellen Sie die andere Zuordnung entsprechend dar! □

Für diese Zuordnung

$$\begin{aligned} 0 &\to 1 \\ 1 &\to 3 \\ 2 &\to 4 \\ 3 &\to 2 \end{aligned} \tag{2.21}$$

erhalten wir

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

Die beiden Rechenstrukturen $(\mathbb{Z}_4, +)$ und $(\mathbb{Z}_5^*, \cdot)$ sind offensichtlich identisch; es gibt sogar zwei eineindeutige Zuordnungen der Elemente beider Strukturen, nämlich (2.20) und (2.21), und diese Umbenennungen sind verträglich mit den beiden Verknüpfungen.

Kleinsche Vierergruppe

Wir betrachten als weiteres Beispiel einer Gruppe mit vier Elementen, die so genannte *Kleinsche Vierergruppe*:[5] $\mathbb{K}_4 = (\{0,1,2,3\}, \diamond)$ definiert durch die Verknüpfungstafel:

$\diamond$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

5 Benannt nach dem deutschen Mathematiker *Felix Klein* (1849 - 1925), der zu vielen Gebieten der Mathematik und zur Didaktik der Mathematik wesentliche Beiträge lieferte. Er legte zum Ende des 19. und am Anfang des 20. Jahrhunderts die Grundsteine dafür, das Göttingen bis zum zweiten Weltkrieg zu *dem* Zentrum der Mathematik weltweit wurde.

$\mathbb{K}_4$ ist eine abelsche Gruppe mit Einselement 0, und jedes Element ist invers zu sich selbst.

Übungsaufgaben

2.26 Überlegen Sie, ob $\mathbb{K}_4$ strukturgleich zu $\mathbb{Z}_4$ (und damit strukturgleich zu $\mathbb{Z}_5^*$) sein kann! □

Da im Gegensatz zu $\mathbb{Z}_4$ alle Elemente von $\mathbb{K}_4$ selbstinvers sind, können die Strukturen nicht strukturgleich sein.

Wir wollen nun den Begriff der Strukturgleichheit von Gruppen formal definieren.

Homomorphismus
Strukturgleichung

Definition 2.7 Seien $\mathcal{G}_1 = (M_1, *_1)$ und $\mathcal{G}_2 = (M_2, *_2)$ zwei Gruppen. Eine totale Abbildung $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ mit

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b) \tag{2.22}$$

heißt *Homomorphismus* von $\mathcal{G}_1$ nach (auch: in) $\mathcal{G}_2$ (siehe Abbildung 10). Die Gleichung (2.22) heißt *Strukturgleichung*.

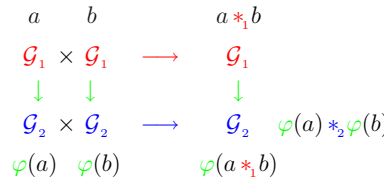

Abb. 10: Homomorphismus

Isomorphismus

Ist ein Homomorphismus φ von $\mathcal{G}_1$ nach $\mathcal{G}_2$ bijektiv, dann heißt φ *Isomorphismus* zwischen $\mathcal{G}_1$ und $\mathcal{G}_2$. Die Gruppen $\mathcal{G}_1$ und $\mathcal{G}_2$ heißen *isomorph* genau dann, wenn es einen Isomorphismus zwischen $\mathcal{G}_1$ und $\mathcal{G}_2$ gibt. Sind $\mathcal{G}_1$ und $\mathcal{G}_2$ isomorph, so schreiben wir $\mathcal{G}_1 \cong \mathcal{G}_2$.

Automorphismus

Ist φ ein Isomorphismus einer Gruppe $\mathcal{G}$ auf sich selbst, so heißt φ ein *Automorphismus* von $\mathcal{G}$. □

Die sinnvollen Eigenschaften, dass ein Homomorphismus das Einselement der Gruppe $\mathcal{G}_1$ dem Einselement der Gruppe $\mathcal{G}_2$ zuordnet und verträglich mit der

Inversenbildung ist, müssen nicht explizit in der Definition gefordert werden, sondern sie folgen mithilfe der Kürzungsregel aus der Strukturgleichung (2.22).

Korollar 2.9 Sei $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ ein Homomorphismus von der Gruppe $\mathcal{G}_1 = (M_1, *_1)$ mit dem Einselement e_1 in die Gruppe $\mathcal{G}_2 = (M_2, *_2)$ mit dem Einselement e_2. Dann gilt:

a) $\varphi(e_1) = e_2$ sowie

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

Beweis **a)** Es sei $\varphi(a_1) = a_2$, dann gilt:

$$a_2 *_2 e_2 = a_2 = \varphi(a_1) = \varphi(a_1 *_1 e_1) = \varphi(a_1) *_2 \varphi(e_1) = a_2 *_2 \varphi(e_1)$$

Hieraus folgt mithilfe der Kürzungsregel $e_2 = \varphi(e_1)$.

b) Es gilt einerseits

$$e_2 = \varphi(a) *_2 (\varphi(a))^{-1}$$

und andererseits mit a)

$$e_2 = \varphi(e_1) = \varphi(a *_1 a^{-1}) = \varphi(a) *_2 \varphi(a^{-1})$$

woraus folgt, dass $\varphi(a) *_2 (\varphi(a))^{-1} = \varphi(a) *_2 \varphi(a^{-1})$ ist. Hieraus folgt mithilfe der Kürzungsregel die Behauptung $\varphi(a^{-1}) = (\varphi(a))^{-1}$. □

Beispiel 2.7 Die Zuordnungen (2.20) und (2.21) stellen Isomorphismen zwischen der additiven Gruppe modulo 4 und der multiplikativen Gruppe modulo 5 dar. Es gilt also $\mathbb{Z}_4 \cong \mathbb{Z}_5^*$. Des Weiteren haben wir bereits überlegt, dass die Kleinsche Vierergruppe $\mathbb{K}_4$ nicht isomorph zu $\mathbb{Z}_4$ und damit auch nicht isomorph zu $\mathbb{Z}_5^*$ ist. □

Übungsaufgaben

2.27 (1) Zeigen Sie: $\mathbb{K}_4$ ist isomorph zu den Gruppen
(i) $F = (\{ id, nid, rez, nrez \}, \circ)$ aus Übung 2.7,
(ii) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +_2)$ und
(iii) $\mathbb{Z}_8^*$!

(2) Zeigen Sie: Die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R} - \{0\}, \cdot)$ sind isomorph!

(3) Zeigen Sie: Die Gruppe $(\mathbb{Z}, +)$ ist isomorph zu allen Untergruppen $(m\mathbb{Z}, +)$, $m \in \mathbb{N}$! □

Bemerkung 2.3 Man kann zeigen, dass $(\mathbb{Z}_4, +)$ und $\mathbb{K}_4$ bis auf Isomorphie die einzigen, vierelementigen Gruppen sind. Ist $\mathcal{G}$ eine Gruppe mit $ord_{\mathcal{G}} = 4$, dann gilt entweder $\mathcal{G} \cong \mathbb{Z}_4$ oder $\mathcal{G} \cong \mathbb{K}_4$. Für die grundsätzliche Untersuchung vierelementiger Gruppen reicht es also aus, die Gruppe $\mathbb{Z}_4$ und die Gruppe $\mathbb{K}_4$ zu betrachten. □

Homomorphismen sind deutlich schwächer als Isomorphismen als Kriterien für Strukturvergleiche.

Korollar 2.10 Zwischen zwei Gruppen $\mathcal{G}$ und $\mathcal{G}'$ existiert immer ein Homomorphismus.

Beweis Sei e' das Einselement von $\mathcal{G}'$. Dann ist die Abbildung $\varphi : \mathcal{G} \to \mathcal{G}'$ definiert durch $\varphi(a) = e'$ für alle $a \in \mathcal{G}$ ein Homomorphismus von $\mathcal{G}$ in $\mathcal{G}'$, denn φ erfüllt die Strukturgleichung:

$$\varphi(a * b) = e' = e' *' e' = \varphi(a) *' \varphi(b)$$

Korollar 2.11 **a)** Sei $\mathcal{G}$ eine Gruppe sowie φ und ψ Homomorphismen von $\mathcal{G}$ in sich selbst. Dann ist auch $\psi \circ \varphi$ ein Homomorphismus von $\mathcal{G}$ in sich selbst. Die Komposition von Homomorphismen ist also wieder ein Homomorphismus.

b) Sei φ ein Isomorphismus von der Gruppe $\mathcal{G}_1 = (M_1, *_1)$ auf die Gruppe $\mathcal{G}_2 = (M_2, *_2)$, dann ist φ^{-1} ein Isomorphismus von $\mathcal{G}_2$ auf $\mathcal{G}_1$.

Beweis **a)** Wir zeigen schrittweise, dass $\psi \circ \varphi(x * y) = \psi \circ \varphi(x) * \psi \circ \varphi(y)$ gilt:

$$\begin{aligned} \psi \circ \varphi(x * y) &= \psi(\varphi(x * y)) \\ &= \psi(\varphi(x) * \varphi(y)) \\ &= \psi(\varphi(x)) * \psi(\varphi(y)) \\ &= \psi \circ \varphi(x) * \psi \circ \varphi(y) \end{aligned}$$

b) Nach Voraussetzung ist φ bijektiv, dann ist auch die Umkehrung φ^{-1} bijektiv. Wir müssen noch zeigen, dass

$$\varphi^{-1}(a *_2 b) = \varphi^{-1}(a) *_1 \varphi^{-1}(b) \tag{2.23}$$

gilt. Es seien $x, y \in \mathcal{G}_1$ mit $\varphi(x) = a$ und $\varphi(y) = b$, womit $x = \varphi^{-1}(a)$ bzw. $y = \varphi^{-1}(b)$ gilt. Da φ Homomorphismus ist, gilt

$$\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$$

Mit diesen Voraussetzungen rechnen wir

$$\varphi^{-1}(a *_2 b) = \varphi^{-1}(\varphi(x) *_2 \varphi(y)) = \varphi^{-1}(\varphi(x *_1 y)) = x *_1 y = \varphi^{-1}(a) *_1 \varphi^{-1}(b)$$

womit (2.23) gezeigt ist. □

Übungsaufgaben

2.28 Sei $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ ein Homomorphismus der Gruppe $\mathcal{G}_1$ in die Gruppe $\mathcal{G}_2$. Zeigen Sei, dass $Bild(\varphi)$ eine Untergruppe von $\mathcal{G}_2$ ist!

2.29 a) Sei $\mathcal{G}$ eine Gruppe. Welche Voraussetzung muss gelten, damit die Abbildung $\varphi : \mathcal{G} \to \mathcal{G}$ definiert durch

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

ein Isomorphismus von $\mathcal{G}$ in sich selbst ist?

b) Sei $\mathcal{G} = (M, *)$ eine Gruppe. Für jedes $t \in \mathcal{G}$ sei die Abbildung $\varphi_t : \mathcal{G} \to \mathcal{G}$ definiert durch

$$\varphi_t(x) = t * x * t^{-1}$$

(1) Zeigen Sie, dass φ_t ein Isomorphismus von $\mathcal{G}$ auf sich selbst, also ein Automorphismus ist!

(2) Es sei $\mathcal{AUT} = \{ \varphi_t \mid t \in \mathcal{G} \}$ die Menge dieser Automorphismen. Zeigen Sie, dass $(\mathcal{AUT}, \circ)$ eine Gruppe bildet!

2.30 a) Sei $\mathcal{G} = (M, *)$ eine Gruppe. Zeigen Sie, dass für jedes Element $a \in \mathcal{G}$ die Abbildung $f_a : \mathcal{G} \to \mathcal{G}$ definiert durch $f_a(x) = a * x$ eine bijektive Abbildung ist!

b) Geben Sie für die multiplikative Gruppe $(\mathbb{Z}_5^*, \cdot)$ alle Abbildungen f_a an!

c) Sei $\mathcal{G} = (M, *)$ eine Gruppe. Zeigen Sie, dass dann die Struktur $\mathcal{F}(\mathcal{G}) = (\{f_a \mid a \in \mathcal{G}\}, \circ)$ ebenfalls eine Gruppe bildet. Dabei ist $(f_a \circ f_b)(x) = f_a(f_b(x))$.

d) Geben Sie die Gruppe $\mathcal{F}(\mathbb{Z}_5^*)$ an.

e) Zeigen Sie, dass für jede Gruppe $\mathcal{G}$ gilt: $\mathcal{G} \cong \mathcal{F}(\mathcal{G})$.

f) Verifizieren Sie die allgemeinen Ergebnisse aus c) und e) am Beispiel b) und d). □

2.6.2 Kerne von Homomorphismen

Bei einem Isomorphismus zwischen zwei Gruppen werden genau die Einselemente aufeinander abgebildet (siehe Korollar 2.9 a). Bei nicht injektiven Homomorphismen ist dies nicht der Fall. Wir betrachten im Folgenden die Menge der Elemente, die von einem Homomorphismus auf das Einselement abgebildet werden, und wir werden sehen, dass diese Menge im Wesentlichen den Homomorphismus beschreibt.

Definition 2.8 Sei $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ ein Homomorphismus von Gruppe $\mathcal{G}_1$ nach Gruppe $\mathcal{G}_2$. Dann heißt

$$Kern(\varphi) = \{x \in \mathcal{G}_1 \mid \varphi(x) = e_2\}$$

Kern eines Homomorphismus

der *Kern* von φ. □

Der Kern enthält also alle Elemente von $\mathcal{G}_1$, die auf das Einselement von $\mathcal{G}_2$ abgebildet werden, oder anders dargestellt gilt $\varphi^{-1}(e_2) = Kern(\varphi)$: Der Kern ist das Urbild des Einselementes von $\mathcal{G}_2$ unter φ.

Korollar 2.12 Es sei $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ ein Homomorphismus von der Gruppe $\mathcal{G}_1$ in die Gruppe $\mathcal{G}_2$.

a) Es gilt immer $e_1 \in Kern(\varphi)$.

b) Falls $|Kern(\varphi)| > 1$ ist, dann ist der Homomorphismus φ nicht injektiv und damit kein Isomorphismus.

c) Falls der Homomorphismus φ injektiv ist, dann gilt $Kern(\varphi) = \{e_1\}$.

d) Ist $|Kern(\varphi)| = 1$, d.h. $Kern(\varphi) = \{e_1\}$, dann ist φ injektiv.

e) φ ist injektiv genau dann, wenn $|Kern(\varphi)| = 1$, d.h. $Kern(\varphi) = \{e_1\}$ ist.

Beweis **a)** Folgt unmittelbar aus Korollar 2.9 a).

b) Da $|Kern(\varphi)| > 1$ ist, gibt es neben $e_1 \in Kern(\varphi)$ ein davon verschiedenes $x \in Kern(\varphi)$ mit $\varphi(e_1) = e_2$ und $\varphi(x) = e_2$. Damit ist $\varphi(e_2) = \varphi(x)$ für $e_1 \neq x$, also ist φ nicht injektiv.

c) Folgt unmittelbar durch Umkehrung von b) unter Beachtung von a).

d) Wir nehmen an, φ sei nicht injektiv. Dann existieren $x, y \in \mathcal{G}_1$ mit $x \neq y$ und $\varphi(x) = \varphi(y)$. Daraus folgt $\varphi(x) *_2 (\varphi(y))^{-1} = e_2$ und daraus $\varphi(x) *_2 \varphi(y^{-1}) = e_2$ und daraus $\varphi(x *_1 y^{-1}) = e_2$. Hieraus folgt nun $x *_1 y^{-1} \in Kern(\varphi)$. Da $x \neq y$ ist, ist $x *_1 y^{-1} \neq e_1$. Das bedeutet, dass $Kern(\varphi)$ außer e_1 noch das Element $x *_1 y^{-1}$ enthält, was einen Widerspruch zur Voraussetzung darstellt.

e) folgt unmittelbar aus c) und d). □

Der Kern bildet eine Untergruppe, sogar einen Normalteiler von $\mathcal{G}_1$.

Satz 2.9 Der Kern eines Homomorphismus φ zwischen zwei Gruppen $\mathcal{G}_1$ und $\mathcal{G}_2$ bildet einen Normalteiler in $\mathcal{G}_1$.

Beweis Wir zeigen zunächst mithilfe von Satz 2.5 a), dass $Kern(\varphi)$ eine Untergruppe von $\mathcal{G}_1$ bildet. Sei also $a, b \in Kern(\varphi)$, d.h. es ist $\varphi(a) = e_2$ und $\varphi(b) = e_2$. Dann gilt $\varphi(a^{-1} *_1 b) = \varphi(a)^{-1} *_2 \varphi(b) = e_2 *_2 e_2 = e_2$. Es folgt, dass $a^{-1} *_1 b \in Kern(\varphi)$ ist.

Jetzt zeigen wir noch, dass $Kern(\varphi)$ normal in $\mathcal{G}_1$ ist, d.h., dass $a *_1 Kern(\varphi) = Kern(\varphi) *_1 a$ für alle $a \in \mathcal{G}_1$ ist. Sei $x \in a *_1 Kern(\varphi)$, d.h. es gibt ein $k \in Kern(\varphi)$ mit $x = a *_1 k$. Wir müssen zeigen, dass $x \in Kern(\varphi) *_1 a$ ist. Dazu setzen wir

$$x = a *_1 k *_1 a^{-1} *_1 a = \overline{k} *_1 a$$

mit $\overline{k} = a *_1 k *_1 a^{-1}$. Es gilt $\overline{k} \in Kern(\varphi)$, denn es ist:

$$\begin{aligned}\varphi(\overline{k}) &= \varphi(a *_1 k *_1 a^{-1}) \\ &= \varphi(a) *_2 \varphi(k) *_2 \varphi(a^{-1}) \\ &= \varphi(a) *_2 e_2 *_2 \varphi(a^{-1}) \\ &= \varphi(a) *_2 \varphi(a)^{-1} \\ &= e_2\end{aligned}$$

Damit folgt also $x \in Kern(\varphi) *_1 a$ und damit $a *_1 Kern(\varphi) \subseteq Kern(\varphi) *_1 a$. Die Umkehrung kann analog gezeigt werden. □

Übungsaufgaben

2.31 Die Abbildung $\varphi : \mathbb{Z}^2 \to \mathbb{Z}$ (zur Definiton von $\mathbb{Z}^2$ siehe Beispiel 2.2) sei definiert durch

$$\varphi(a, b) = b - a$$

a) Zeigen Sie: φ ist ein Homomorphismus von $(\mathbb{Z}^2, +)$ nach $(\mathbb{Z}, +)$.

b) Bestimmen Sie $Kern(\varphi)$!

c) Ist φ ein Isomorphismus? Beweisen Sie Ihre Antwort!

d) $Kern(\varphi)$ ist ein Normalteiler von $(\mathbb{Z}^2, +)$. Geben Sie die Nebenklasse von $Kern(\varphi)$ an, von der $(3, 7)$ ein Repräsentant ist! Geben Sie die Nebenklasse von $Kern(\varphi)$ an, von der $(a, b) \in \mathbb{Z}^2$ ein Repräsentant ist. □

Aus den Sätzen 2.7 und 2.9 folgt unmittelbar

Korollar 2.13 Sei φ ein Homomorphismus zwischen den Gruppen $\mathcal{G}$ und $\mathcal{G}'$, dann ist $\mathcal{G}/Kern(\varphi)$ eine Gruppe, die Faktorgruppe von $\mathcal{G}$ nach dem Kern von φ. □

Mit Defintion 2.8 und Satz 2.9 wissen wir, dass das Urbild $\varphi^{-1}(e_2)$ von e_2 unter dem Homomorphismus φ der Kern von φ ist und dass dieser ein Normalteiler, also insbesondere eine Nebenklasse ist. Da durch $a *_1 Kern(\varphi)$ für $a \in \mathcal{G}_1$ alle Nebenklassen von $Kern(\varphi)$ bestimmt sind, besagt der folgende Satz, dass die Nebenklassen von $Kern(\varphi)$ gerade alle Urbilder von φ sind.

Satz 2.10 Sei φ ein Homomorphismus der Gruppe $\mathcal{G}_1$ nach der Gruppe $\mathcal{G}_2$ sowie $\varphi(a) = c$. Dann gilt $\varphi^{-1}(c) = a *_1 Kern(\varphi)$.

Beweis Es gilt

$$\begin{aligned} b \in \varphi^{-1}(c) \quad & \text{genau dann, wenn} \quad \varphi(b) = c \\ & \text{genau dann, wenn} \quad \varphi(b) = \varphi(a) \\ & \text{genau dann, wenn} \quad \varphi(a)^{-1} *_2 \varphi(b) = e_2 \\ & \text{genau dann, wenn} \quad \varphi(a^{-1} *_1 b) = e_2 \\ & \text{genau dann, wenn} \quad a^{-1} *_1 b \in Kern(\varphi) \\ & \text{genau dann, wenn} \quad b \in a *_1 Kern(\varphi) \end{aligned}$$

Damit haben wir gezeigt, dass $\varphi^{-1}(c) = a *_1 Kern(\varphi)$ ist. □

Aus Übung 2.28 wissen wir, dass die Bildmenge eines Homomorphismus eine Gruppe bildet. Die nächste Folgerung zeigt Zusammehänge zwischen dem Kern und der Bildgruppe eines Gruppenhomomorphismus auf.

Korollar 2.14 Sei $\varphi : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus von der Gruppe $\mathcal{G}$ in die Gruppe $\mathcal{G}'$ mit $|Bild(\varphi)| < \infty$.

a) Dann gilt

$$[\mathcal{G} : Kern(\varphi)] = |Bild(\varphi)| \tag{2.24}$$

b) sowie

$$|\mathcal{G}| = |Kern(\varphi)| \cdot |Bild(\varphi)| \tag{2.25}$$

Beweis **a)** Aus Satz 2.10 folgt unmittelbar, dass die Anzahl der Nebenklassen von $Kern(\varphi)$, d.h. der Index von $Kern(\varphi)$ in $\mathcal{G}$, gleich der Anzahl der Bilder von φ ist.

b) Unmittelbar aus dem Satz von Lagrange (Satz 2.8), insbesondere in der Form von Gleichung (2.19), folgt für die Untergruppe $Kern(\varphi)$:

$$|\mathcal{G}| = [\mathcal{G} : Kern(\varphi)] \cdot |Kern(\varphi)|$$

Hieraus folgt mit Gleichung (2.24) aus a) unmittelbar die Behauptung (2.25). □

2.6.3 Der Homomorphiesatz für Gruppen

Satz 2.10 und die daraus folgende Gleichung (2.24) lassen vermuten, dass die Faktorgruppe $\mathcal{G}/Kern(\varphi)$ isomorph zur Bildgruppe $Bild(\varphi)$ eines Homomorphismus φ ist. Diese Vermutung wird durch den folgenden Satz, den Homomorphiesatz für Gruppen, bestätigt.

Satz 2.11 Sei $\varphi : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus von der Gruppe $\mathcal{G}$ in die Gruppe $\mathcal{G}'$. Dann ist die Abbildung

$$\phi : \mathcal{G}/Kern(\varphi) \to Bild(\varphi)$$

definiert durch

$$\phi(a * Kern(\varphi)) = \varphi(a) \tag{2.26}$$

ein Isomorphismus zwischen den Gruppen $\mathcal{G}/Kern(\varphi)$ und $Bild(\varphi)$, es gilt also $\mathcal{G}/Kern(\varphi) \cong Bild(\varphi)$.

Beweis Die Abbildung ϕ ist offensichtlich total und surjektiv. Zum Nachweis der Injektivität sei $\phi(a * Kern(\varphi)) = \phi(b * Kern(\varphi))$ für $a, b \in \mathcal{G}$. Wegen Gleichung (2.26) gilt dann $\varphi(a) = \varphi(b)$. Es folgt (siehe Beweis von Satz 2.10) $a \in b * Kern(\varphi)$ und damit (siehe Korollar 2.5 b) $a * Kern(\varphi) = b * Kern(\varphi)$, womit die Injektivität von ϕ gezeigt ist.

Des Weiteren gilt

$$\phi((a * Kern(\varphi)) *_{Kern(\varphi)} (b * Kern(\varphi)))$$

$$\begin{aligned}
&= \phi((a * b) * Kern(\varphi)) && \text{wegen (2.15) und Definition 2.6}\\
&= \varphi(a * b) && \text{wegen (2.26)}\\
&= \varphi(a) *' \varphi(b) && \text{da } \varphi \text{ Homomorphismus}\\
&= \phi(a * Kern(\varphi)) *' \phi(b * Kern(\varphi)) && \text{wegen (2.26)}
\end{aligned}$$

womit die Homomorphieeigenschaft (Definition 2.7) von ϕ gezeigt ist. □

Aus dem Satz 2.11 folgt unmittelbar

Korollar 2.15 Sei $\varphi : \mathcal{G} \to \mathcal{G}'$ ein surjektiver Homomorphismus von der Gruppe $\mathcal{G}$ in die Gruppe $\mathcal{G}'$. Dann ist die Abbildung

$$\phi : \mathcal{G}/Kern(\varphi) \to \mathcal{G}'$$

definiert durch

$$\phi(a * Kern(\varphi)) = \varphi(a)$$

ein Isomorphismus zwischen den Gruppen $\mathcal{G}/Kern(\varphi)$ und $\mathcal{G}'$, es gilt also $\mathcal{G}/Kern(\varphi) \cong \mathcal{G}'$. □

Beispiel 2.8 **a)** In der Lösung zu Übung 2.31 d) haben wir den Kern des Homomorphismus $\varphi : \mathbb{Z}^2 \to \mathbb{Z}$ definiert durch $\varphi(a, b) = b - a$ und seine Nebenklassen $(a, b) + Kern(\varphi)$ betrachtet. Da φ surjektiv ist, gilt gemäß Korollar 2.15: $\mathbb{Z}^2/Kern(\varphi) \cong \mathbb{Z}$. Die Gleichheit (E.24)

$$(a, b) + Kern(\varphi) = \{(x, y) \mid y - x = \varphi(a, b)\}$$

drückt quasi diesen Isomorphismus für unser Beispiel aus:

$$\phi : \mathbb{Z}^2/Kern(\varphi) \to \mathbb{Z}$$

definiert durch

$$\phi((a, b) + Kern(\varphi)) = \varphi(a, b)$$

b) Wir haben verschiedentlich in $\mathbb{Z}_m$, $m \in \mathbb{N}$, gerechnet. Wir betrachten nun allgemein die additive Struktur $(\mathbb{Z}_m, +_m)$ mit der Trägermenge $\mathbb{Z}_m = \{0_m, 1_m, \ldots, (m-1)_m\}$. Die Verknüpfung $+_m$ ist definiert durch

$$a_m +_m b_m = \begin{cases} (a+b)_m, & a+b \leq m-1 \\ (a+b-m)_m, & a+b \geq m \end{cases} \tag{2.27}$$

Es gilt also z.B. $2_8 +_8 5_8 = (2+5)_8 = 7_8$ und $3_8 +_8 7_8 = (3+7-8)_8 = 2_8$.

Die Struktur $\mathbb{Z}_m$ ist offensichtlich abgeschlossen und kommutativ, und sie ist assoziativ (etwas umständlich nachzurechnen, aber machbar). Das Einselement ist 0_m, denn es gilt $a_m +_m 0_m = (a+0)_m = a_m$. Das Inverse $(-a)_m$ zu a_m ist $(m-a)_m$, denn es gilt

$$\begin{aligned} a_m +_m (-a)_m &= a_m +_m (m-a)_m \\ &= (a + (m-a) - m)_m \qquad \text{da } a + (m-a) = m \geq m \text{ ist} \\ &= 0_m \end{aligned}$$

$\mathbb{Z}_m$ ist also eine additive abelsche Gruppe.

Am Ende von Abschnitt 1.2.1 haben wir die Operation mod kennengelernt: $r = mod(a,b)$ ist für $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ der kleinste Rest größer gleich 0, der bei der Division von a durch b bleibt (sieh Satz 1.1). Mithilfe dieser Operation setzen wir nun für $a \in \mathbb{Z}$ und $m \in \mathbb{N}$: $a_m = mod(a,m)$; offensichtlich ist

$$(a_m)_m = a_m \tag{2.28}$$

Es gilt

$$(a+b)_m = a_m +_m b_m \tag{2.29}$$

Dazu rechnen wir: Es gibt $q_a, q_b \in \mathbb{Z}$ mit

$$\begin{aligned} a &= mq_a + a_m,\ 0 \leq a_m \leq m-1 \\ b &= mq_b + b_m,\ 0 \leq b_m \leq m-1 \end{aligned}$$

Damit ist $a_m + b_m \leq 2m-2$, also $a_m + b_m - m \leq m-2 < m-1$.

Es folgt (mithilfe von (2.27) im dritten bzw. (2.28) im vierten Schritt)

$$a + b = m(q_a + q_b) + a_m + b_m$$

$$= \begin{cases} m(q_a+q_b) + (a_m + b_m), & a_m + b_m \leq m-1 \\ m(q_a+q_b+1) + (a_m + b_m - m), & a_m + b_m \geq m \end{cases}$$

$$= \begin{cases} m(q_a+q_b) + ((a_m)_m +_m (b_m)_m), & a_m + b_m \leq m-1 \\ m(q_a+q_b+1) + ((a_m)_m +_m (b_m)_m), & a_m + b_m \geq m \end{cases}$$

$$= \begin{cases} m(q_a+q_b) + (a_m +_m b_m), & a_m + b_m \leq m-1 \\ m(q_a+q_b+1) + (a_m +_m b_m), & a_m + b_m \geq m \end{cases}$$

womit (2.29) gezeigt ist.

Wir definieren nun $\varphi_m : \mathbb{Z} \to \mathbb{Z}_m$ durch

$$\varphi_m(a) = a_m$$

Dann ist φ_m ein Homomorphismus von $\mathbb{Z}$ nach $\mathbb{Z}_m$, denn es ist mithilfe von (2.29)

$$\varphi_m(a+b) = (a+b)_m = a_m +_m b_m = \varphi_m(a) +_m \varphi_m(b)$$

φ_m ist offensichtlich surjektiv.

Wir bestimmen nun den Kern von φ_m (siehe Beispiel 2.6):

$$\begin{aligned} Kern(\varphi_m) &= \{a \in \mathbb{Z} \mid \varphi_m(a) = 0_m\} \\ &= \{a \in \mathbb{Z} \mid a_m = 0_m\} \\ &= \{ma \mid a \in \mathbb{Z}\} \\ &= m\mathbb{Z} \end{aligned}$$

Wir wissen, dass $m\mathbb{Z}$ ein Normalteiler in $\mathbb{Z}$ ist.

Insgesamt folgt mit Korollar 2.15: $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Deswegen werden wir im Folgenden nicht mehr zwischen $\mathbb{Z}/m\mathbb{Z}$ und $\mathbb{Z}_m$ unterscheiden und $\mathbb{Z}_m$ als Bezeichnung für diese Rechenstruktur wählen.

Additive Restklassengruppe modulo m

Wir nennen $(\mathbb{Z}_m, +_m)$ die *additive Restklassengruppe modulo* m. Wenn aus dem Zusammenhang klar ist, dass wir in $\mathbb{Z}_m$ rechnen, lassen wir beim Verknüpfungssymbol das m weg und schreiben einfach nur $+$ anstelle $+_m$. □

Übungsaufgaben

2.32 Sei $\mathcal{G} = (M, *)$ eine endliche zyklische Gruppe und $b \in \mathcal{G}$ ein Generator für $\mathcal{G}$. Des Weiteren sei $(\mathbb{Z}, +)$ die additive Gruppe der ganzen Zahlen.

a) Zeigen Sie, dass die Abbildung $\varphi_b : \mathbb{Z} \to \mathcal{G}$ definiert durch $\varphi_b(k) = b^k$ ein Homomorphismus ist!

b) Bestimmen Sie $Kern(\varphi_b)$!

c) Wie viele Elemente besitzt $\mathbb{Z}/Kern(\varphi_b)$? □

http://www.springer.com/978-3-658-04074-1

Algebraische und zahlentheoretische Grundlagen für die Informatik
Gruppen, Ringe, Körper, Primzahltests, Verschlüsselung

Witt, K.-U.

2014, VIII, 220 S., Softcover
ISBN: 978-3-658-04074-1