Formale Grundlagen der Informatik

Herbstsemester 2020

Prof. Dr. Matthias Krause
Dr. Matthias Hamann

Algebraische Strukturen

(Stand: Oktober 2020)

Lehrstuhl für Theoretische Informatik
Universität Mannheim

Algebraische Strukturen

Algebraische Strukturen

Halbgruppen, Monoide, Gruppen

Operationen auf Mengen, Halbgruppen

Definition 10.1

- Eine Abbildung $\circ : M \times M \to M$ heißt **Operation** auf M. Schreibweise: $x \circ y$ für $\circ(x, y)$.
- Die Operation $\circ$ heißt **kommutativ**, falls $x \circ y = y \circ x$ für alle $x, y \in M$.
- Die Operation $\circ$ heißt **assoziativ**, falls $(x \circ y) \circ z = x \circ (y \circ z)$ (Schreibweise: $= x \circ y \circ z$) für alle $x, y, z \in M$.
- Ist $\circ : M \times M \to M$ assoziativ, so heißt $(M, \circ)$ **Halbgruppe**.

Beispiele:

- kommutative, assoziative Operation auf $\mathbb{N}$: $a \circ b := a + b$
- nicht kommutative, nicht assoziative Operation auf $\mathbb{N}$: $a \circ b := a^b$, $(2^2)^3 \neq 2^{(2^3)}$
- kommutative, nicht assoziative Operation auf $\mathbb{Q}$: $a \circ b := (a + b)/2$
- nicht kommutative, assoziative Operation auf $\mathcal{S}_3$: Komposition $\circ$
  Beispiel: $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$, $\pi'(1) = 3$, $\pi'(2) = 2$, $\pi'(3) = 1$,
  $\pi(\pi'(1)) = 3 \neq \pi'(\pi(1)) = 2$.

Neutrale Elemente, Monoide

Definition 10.2

Sei $(M, \circ)$ Halbgruppe. Ein Element $e \in M$ heißt **neutrales Element in** M, falls

$$e \circ m = m \circ e = m$$

für alle $m \in M$.

Halbgruppen, die ein neutrales Element besitzen, heißen **Monoide**.

Lemma 10.3

Seien e, e' neutrale Elemente im Monoid $(M, \circ)$. Dann gilt $e = e'$.

Beweis: Nach Definition gilt $e = e \circ e' = e'$. $\square$

Beispiel: Die ganzen Zahlen mit der Multiplikation bilden einen Monoid mit $e = 1$.

Die geraden ganzen Zahlen mit der Multiplikation bilden eine Halbgruppe, die kein Monoid ist.

Inverse Elemente, Gruppen

Definition 10.4

Es sei $(M, \circ)$ ein Monoid mit neutralem Element e, und es sei $m \in M$. Ein Element $m' \in M$ heißt **inverses Element** (oder **Inverses**) **zu** m, falls

$$m \circ m' = m' \circ m = e.$$

$(M, \circ)$ heißt **Gruppe**, falls alle Elemente in M ein Inverses haben.

Lemma 10.5

Sind $m_1, m_2 \in M$ Inverse zu $m \in M$, dann gilt $m_1 = m_2$.

Beweis: Es gilt $m_1 = m_1 \circ (m \circ m_2) = (m_1 \circ m) \circ m_2 = m_2$. $\square$

Beispiel: Das Inverse von 2 in $(\mathbb{Q}, \cdot)$ ist 0.5.

Die Gruppe M^*

Definition 10.6

Für jeden Monoid $(M, \circ)$ bezeichne $M^* \subseteq M$ die Menge aller Elemente in M, die ein Inverses haben.

Lemma 10.7

Für jeden Monoid $(M, \circ)$ gilt, dass $(M^*, \circ)$ eine Gruppe ist.

Übliche Schreibweise: $(M, \circ)^*$ für $(M^*, \circ)$.

Beweis: Zunächst gilt, dass das neutrale Element e von M in M^* liegt, da $e^{-1} = e$.

Außerdem folgt aus $m, m' \in M^*$, dass auch $m \circ m' \in M^*$, da $(m \circ m')^{-1} = (m')^{-1} \circ m^{-1} \in M$, d. h., M^* abgeschlossen gegenüber $\circ$.

Zudem gilt, dass für alle $m \in M^*$ auch m^{-1} in M^* liegt, da $(m^{-1})^{-1} = m$. $\square$

Beispiele Monoide, Gruppen

- $(\mathbb{N}, +)$: Neutrales Element 0 und $(\mathbb{N}, +)^* = (\{0\}, +)$,
  d. h., Monoid, aber keine Gruppe.
- $(\mathbb{N}, \cdot)$: Neutrales Element 1 und $(\mathbb{N}, \cdot)^* = (\{1\}, \cdot)$,
  d. h., Monoid, aber keine Gruppe.
- $(\mathbb{Z}, +)$: Neutrales Element 0 und $(\mathbb{Z}, +)^* = (\mathbb{Z}, +)$,
  d. h., Gruppe (und damit auch Monoid).
- $(\mathbb{Z}, \cdot)$: Neutrales Element 1 und $(\mathbb{Z}, \cdot)^* = (\{1, -1\}, \cdot)$,
  d. h., Monoid, aber keine Gruppe.
- $(\mathbb{Q}, \cdot)$: Neutrales Element 1 und $(\mathbb{Q}, \cdot)^* = (\mathbb{Q} \setminus \{0\}, \cdot)$,
  d. h., Monoid, aber keine Gruppe.
- $(\mathcal{P}(M), \cap)$: Neutrales Element M, $(\mathcal{P}(M), \cap)^* = (\{M\}, \cap)$,
  d. h., Monoid, aber keine Gruppe.
- $(\mathcal{P}(M), \cup)$: Neutrales Element $\emptyset$, $(\mathcal{P}(M), \cup)^* = (\{\emptyset\}, \cup)$,
  d. h., Monoid, aber keine Gruppe.

Gruppentafeln: Allgemeiner Aufbau

Gruppentafel von $(M, \circ)$ **mit** $M := \{a, b, c, d\}$

$(M, \circ)$	a	b	c	d
a	$a \circ a$	$a \circ b$	$a \circ c$	$a \circ d$
b	$b \circ a$	$b \circ b$	$b \circ c$	$b \circ d$
c	$c \circ a$	$c \circ b$	$c \circ c$	$c \circ d$
d	$d \circ a$	$d \circ b$	$d \circ c$	$d \circ d$

Gruppentafeln: Beispiel $(\mathbb{Z}, \cdot)^*$

Gruppentafel von $(\mathbb{Z}, \cdot)^*$

$(\mathbb{Z}, \cdot)^*$	-1	1
-1	1	-1
1	-1	1

Beachte: Die Gruppentafel von $(\mathbb{Z}, \cdot)^*$ ist symmetrisch bezüglich der Hauptdiagonale, da die Gruppe *abelsch* (d. h. die Verknüpfung der Gruppe kommutativ) ist.

Die Permutationsgruppe $\mathcal{S}(M)$

Definition 10.8

Es sei M eine nichtleere Menge. Dann bezeichnet $\mathcal{S}(M)$ die Menge der Permutationen über M, d. h. der bijektiven Abbildungen von M nach M. Für $n \in \mathbb{N}^+$ und $M = \{1, \ldots, n\}$ wird $\mathcal{S}(M)$ auch mit $\mathcal{S}_n$ bezeichnet.

Erinnerung: $|\mathcal{S}_n| = n!$.

Lemma 10.9

Sei M eine nichtleere Menge und bezeichne $\circ$ die Operation Komposition auf $\mathcal{S}(M)$. Dann ist $(\mathcal{S}(M), \circ)$ eine (i.A. nicht kommutative) Gruppe mit neutralem Element $id_M : M \to M$.

Beweis: Die Hintereinanderausführung $\circ$ von Abbildungen ist offenbar assoziativ. Man sieht auch leicht, dass die Identität id_M hier die Eigenschaft des neutralen Elements erfüllt, und dass für alle $f : M \to M$ bijektiv die Umkehrabbildung f^{-1} das Inverse von f ist. □

Schreibweisen von Monoiden und Gruppen

- Für Monoide unterscheidet man die **multiplikative** Schreibweise (z. B. $(M, \circ)$) und die **additive** Schreibweise (z. B. $(M, +)$).
- Bei der multiplikativen Schreibweise wird das neutrale Element auch als 'Eins' bezeichnet und Inverse werden als m^{-1} geschrieben.
- Bei der additiven Schreibweise wird das neutrale Element auch als 'Null' bezeichnet und Inverse werden als $-m$ geschrieben.
- Bei der multiplikativen Schreibweise wird $m \circ m \circ \cdots \circ m$ mit k Faktoren auch als m^k geschrieben.
- Bei der additiven Schreibweise wird $m + m + \cdots + m$ mit k Summanden auch als $k \cdot m$ geschrieben.

Algebraische Strukturen

Faktorstrukturen und die Monoide $(\mathbb{Z}_m, +)$ und $(\mathbb{Z}_m, \cdot)$

Verträglichkeit von Operationen mit Äquivalenzrelationen

Definition 10.10

Es sei $(M, \circ)$ eine Halbgruppe und R eine Äquivalenzrelation auf M. Die Operation $\circ$ heißt **verträglich mit** R, falls für alle $x, y, x', y' \in M$ gilt: Aus $x \sim_R x'$ und $y \sim_R y'$ folgt $x \circ y \sim_R x' \circ y'$.

Beispiel: $5 \equiv 15 \mod 5$, $12 \equiv 7 \mod 5$, $5 + 12 = 17 \equiv 15 + 7 = 22 \mod 5$.

Lemma 10.11

Es sei $(M, \circ)$ eine Halbgruppe und R eine Äquivalenzrelation, so dass $\circ$ verträglich mit R ist.

Dann definiert $\circ$ folgende Halbgruppenstruktur $(M/R, \circ)$ auf der Menge der Äquivalenzklassen M/R:

Für alle $x, y \in M$ sei $[x]_R \circ [y]_R := [x \circ y]_R$.

Ist $(M, \circ)$ ein Monoid mit neutralem Element e, so ist auch $(M/R, \circ)$ ein Monoid mit neutralem Element $[e]_R$.

Ist $x \in (M, \circ)^*$ und x^{-1} das Inverse zu x, dann gilt $[x]_R \in (M/R, \circ)^*$ und $[x^{-1}]_R$ ist das Inverse von $[x]_R$.

Zum Beweis von Lemma 10.11, Beispiel

Es ist zu zeigen, dass die Definition $[x]_R \circ [y]_R := [x \circ y]_R$ der Operation $\circ$ auf M/R überhaupt sinnvoll ist, d. h., dass für alle $x' \in [x]_R$ und $y' \in [y]_R$ gilt, dass $x' \circ y' \in [x \circ y]_R$. Dies folgt jedoch direkt aus der Definition 10.10 der Verträglichkeit von $\circ$ mit R.

Die Operation $\circ$ auf M/R ist assoziativ, da

$$\begin{aligned}([x]_R \circ [y]_R) \circ [z]_R &= [x \circ y]_R \circ [z]_R = [(x \circ y) \circ z]_R \\ &= [x \circ (y \circ z)]_R = [x]_R \circ [y \circ z]_R = [x]_R \circ ([y]_R \circ [z]_R)\end{aligned}$$

Die Aussagen bezüglich des neutralen Elements und möglicher Inverse folgen direkt aus den Definitionen. □

Wichtiges Beispiel:

Lemma 10.12

Die Operationen $+$ und $\cdot$ auf $\mathbb{Z}$ sind für alle $m \geq 2$ verträglich mit der MOD_m*-Relation.*

Beweis von Lemma 10.12

Wir bezeichnen $\mathbb{Z}/R_{\text{MOD}_m}$ durch $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$.

Wir fixieren beliebige ganze Zahlen $x, y, x', y' \in \mathbb{Z}$ mit $x \equiv x' \mod m$ und $y \equiv y' \mod m$.

D. h., es existieren ganze Zahlen $a, b \in \mathbb{Z}$ mit $x' = x + a \cdot m$ und $y' = y + b \cdot m$.

Wir müssen zeigen, dass $x + y \equiv x' + y' \mod m$ und $x \cdot y \equiv x' \cdot y' \mod m$.

Das folgt aus

$$x' + y' = (x + a \cdot m) + (y + b \cdot m) = x + y + (a + b) \cdot m$$

und

$$\begin{aligned} x' \cdot y' &= (x + a \cdot m) \cdot (y + b \cdot m) \\ &= x \cdot y + x \cdot b \cdot m + a \cdot m \cdot y + a \cdot m \cdot b \cdot m. \\ &= x \cdot y + (x \cdot b + y \cdot a + a \cdot b \cdot m) \cdot m. \ \square \end{aligned}$$

Monoidstruktur auf $\mathbb{Z}_m$

Als Folgerung aus Lemma 10.11 und Lemma 10.12 erhalten wir die Monoide $(\mathbb{Z}_m, +)$ und $(\mathbb{Z}_m, \cdot)$ mit

$$[i] + [j] = [i + j] \text{ und } [i] \cdot [j] = [i \cdot j]$$

für alle $[i], [j] \in \mathbb{Z}_m$.

Da $(\mathbb{Z}, +)$ eine Gruppe ist, ist auch $(\mathbb{Z}_m, +)$ eine Gruppe mit

$$-[i] = [m - i]$$

für alle $[i] \in \mathbb{Z}_m$.

Die Monoide $(\mathbb{Z}_m, \cdot)$ sind im Allgemeinen keine Gruppen.

Im Folgenden analysieren wir die Struktur von Gruppen vom Typ $(\mathbb{Z}_m, \cdot)^*$.

Gruppentafel von $(\mathbb{Z}_6, +)$

$(\mathbb{Z}_6, +)$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Beachte: Die Gruppentafel von $(\mathbb{Z}_6, +)$ ist symmetrisch bezüglich der Hauptdiagonale, da die Gruppe *abelsch* (d. h. die Verknüpfung der Gruppe kommutativ) ist.

Multiplikationstafel von $(\mathbb{Z}_6, \cdot)$

$(\mathbb{Z}_6, \cdot)$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Beachte: $(\mathbb{Z}_6, \cdot)^* = \{1, 5\}$.

Theorem 10.13

Für alle $m \in \mathbb{N}^+$, $m \geq 2$, gilt $(\mathbb{Z}_m, \cdot)^* = \{[b] \mid ggT(m, b) = 1\}$.

Beweis: Für alle $[b], [y] \in \mathbb{Z}_m$ gilt genau dann $[y] \cdot [b] = [1]$, wenn ein $x \in \mathbb{Z}$ existiert, so dass

$$y \cdot b - 1 = x \cdot m.$$

Also $[b] \in (\mathbb{Z}_m, \cdot)^* \iff \exists x, y \in \mathbb{Z} : \; x \cdot m + y \cdot b = 1$.

Das Theorem ergibt sich aus dem folgenden Lemma 10.14 und dem Fakt, dass 1 ein Teiler von m und b ist.

Lemma 10.14

*Der größte gemeinsame Teiler $ggT(m,b)$ ist der **einzige Teiler** d von m und b, für den ganze Zahlen x, y existieren, so dass $x \cdot m + y \cdot b = d$.*

Beweis: Es sei d ein Teiler von m und b, für den ganze Zahlen x, y existieren, so dass $x \cdot m + y \cdot b = d$.

Es gilt $d \leq ggT(m,b)$.

Andererseits teilt $ggT(m,b)$ die Zahl $x \cdot m + y \cdot b = d$, da $ggT(m,b)$ ein Teiler von m und b ist, also $ggT(m,b) \leq d$.

Das ergibt $d = ggT(m,b)$. $\square$

Beispiele:

- $(\mathbb{Z}_2, \cdot)^* = \{[1]\}$,
- $(\mathbb{Z}_{12}, \cdot)^* = \{[1], [5], [7], [11]\}$,
- $(\mathbb{Z}_p, \cdot)^* = \{[1], [2], [3], \cdots, [p-2], [p-1]\}$, für p Primzahl.

Gruppentafel von $(\mathbb{Z}_{14}, \cdot)^*$

$(\mathbb{Z}_{14}, \cdot)^*$	[1]	[3]	[5]	[9]	[11]	[13]
[1]	[1]	[3]	[5]	[9]	[11]	[13]
[3]	[3]	[9]	[1]	[13]	[5]	[11]
[5]	[5]	[1]	[11]	[3]	[13]	[9]
[9]	[9]	[13]	[3]	[11]	[1]	[5]
[11]	[11]	[5]	[13]	[1]	[9]	[3]
[13]	[13]	[11]	[9]	[5]	[3]	[1]

Beachte: Die Gruppentafel von $(\mathbb{Z}_{14}, \cdot)^*$ ist symmetrisch bezüglich der Hauptdiagonale, da die Gruppe *abelsch* (d. h. die Verknüpfung der Gruppe kommutativ) ist.

Die Schulmethode zur ggT-Berechnung

- **Eingabe:** n-bit Zahlen m, b
- **Berechne** die **Primfaktorenzerlegungen**

$$m = p_1^{x_1} \cdot p_2^{x_2} \cdots p_s^{x_s}$$

$$b = p_1^{y_1} \cdot p_2^{y_2} \cdots p_s^{y_s}$$

  wobei $p_1 < p_2 < \cdots$ die Folge aller Primzahlen bezeichnet, und p_s die größte Primzahl ist, die m oder b teilt.
- **Ausgabe:** $ggT(m, b) = p_1^{z_1} \cdot p_2^{z_2} \cdots p_s^{z_s}$ mit $z_i = \min\{x_i, y_i\}$.
- **Beispiel:** $b = 4410 = 2 \cdot 3^2 \cdot 5 \cdot 7^2$ und $m = 10500 = 2^2 \cdot 3 \cdot 5^3 \cdot 7$
- **Ausgabe:** $ggT(m, b) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.
- **Problem:** Die Laufzeit aller bekannten Algorithmen zur Berechnung der Primfaktorenzerlegung von n-Bit Zahlen ist exponentiell in n.

Euklidischer Algorithmus zur ggT-Berechnung

Eingabe: $m > b > 0$ **Ausgabe:** $ggT(m, b)$

Informal: Wir erzeugen eine Folge von Zahlen $a_0 = m, a_1 = b, a_2, a_3, \cdots$ nach der Regel $a_{i+1} \leftarrow a_{i-1} \bmod a_i$ solange bis Runde s mit $a_s = 0$ erreicht ist.

Dann ergibt sich $ggT(m, b)$ als das vorletzte Element a_{s-1}.

1 $a_0 \leftarrow m$
2 $a_1 \leftarrow b$
3 $i \leftarrow 1$
4 **repeat**
5 $\quad a_{i+1} \leftarrow a_{i-1} \bmod a_i$
6 $\quad i \leftarrow i + 1$
7 **until** $a_i = 0$
8 **output** a_{i-1}

Euklidischer Algorithmus (Bsp.: Berechnung des ggT von 123 und 45)

Eingabe: $m > b > 0$

1 $a_0 \leftarrow m$
2 $a_1 \leftarrow b$
3 $i \leftarrow 1$
4 **repeat**
5 $\quad a_{i+1} \leftarrow a_{i-1} \bmod a_i$
6 $\quad i \leftarrow i + 1$
7 **until** $a_i = 0$
8 **output** a_{i-1}

i	0	1	2	3	4	5	6
a_i	123	45	33	12	9	3	0

Euklidischer Algorithmus, Korrektheit I

Beobachtung: Eingabe $a_0 > a_1$ liefert Folge

$$a_0 > a_1 > \cdots > a_{s-1} > a_s = 0,$$

wobei für alle i, $1 \leq i \leq s-1$, $a_{i+1} = a_{i-1} \bmod a_i$, d. h.,

$$a_{i-1} = d_i \cdot a_i + a_{i+1} \quad \text{mit} \quad d_i = \left\lfloor \frac{a_{i-1}}{a_i} \right\rfloor. \tag{1}$$

Behauptung: $a_{s-1} = ggT(a_0, a_1)$.

Lemma 10.15

a_{s-1} teilt a_i für alle $i \leq s-1$.

Beweis: a_{s-1} teilt a_{s-1} und (wegen $a_s = 0$) auch a_{s-2}.

Wegen Relation (1) teilt a_{s-1} auch a_{s-3} und a_{s-4} usw., also auch a_1 und a_0. □

Lemma 10.16

Für alle $i \geq 0$ existieren ganze Zahlen $x_i, y_i \in \mathbb{Z}$ mit $a_i = x_i \cdot a_0 + y_i \cdot a_1$.

Beweis: Offensichtlich gilt $x_0 = 1$, $y_0 = 0$ und $x_1 = 0$, $y_1 = 1$.

Für $i \geq 1$ setzen wir $d_i = \lfloor \frac{a_{i-1}}{a_i} \rfloor$.

Nach Definition gilt für $i \geq 1$, dass

$$a_{i+1} = a_{i-1} - d_i \cdot a_i.$$

Also folgt für alle $i \geq 1$, dass

$$x_{i+1} = x_{i-1} - d_i \cdot x_i \quad \text{und} \quad y_{i+1} = y_{i-1} - d_i \cdot y_i. \; \square$$

Lemmata 10.15 und 10.16 (zusammen mit Lemma 10.14) beweisen die Behauptung, dass $a_{s-1} = ggT(a_0, a_1)$.

Erweiterter Euklidischer Algorithmus

Eingabe: $m > b > 0$,

Ausgabe: $ggT(m, b)$ und y mit $y \cdot b \equiv ggT(m, b) \mod m$.

1 $y_0 \leftarrow 0$
2 $y_1 \leftarrow 1$
3 $a_0 \leftarrow m$
4 $a_1 \leftarrow b$
5 $i \leftarrow 1$
6 **repeat**
7 $\quad a_{i+1} \leftarrow a_{i-1} \bmod a_i$
8 $\quad d_i \leftarrow \lfloor a_{i-1}/a_i \rfloor$
9 $\quad y_{i+1} \leftarrow y_{i-1} - d_i \cdot y_i$
10 $\quad i \leftarrow i + 1$
11 **until** $a_i = 0$
12 **output** $a_{i-1},\ y_{i-1}$

Beispiel Erweiterter Euklidischer Algorithmus

Eingabe: $m = 147, b = 32$

i	0	1	2	3	4	5	6
a_i	147	32	19	13	6	1	0
d_i		4	1	1	2		
y_i	0	1	-4	5	-9	23	

Ausgabe: $ggT(m, b) = 1, y = 23$

(**Probe:** $-5 \cdot 147 + 23 \cdot 32 = -735 + 736 = 1$; hier wäre $x = -5$.)

Anmerkung zur Laufzeit

Lemma 10.17

Für alle $a_0 > a_1$ gilt, dass falls $a_0 > a_1 > \cdots a_{s-1} > a_s = 0$ die vom Euklidischen Algorithmus erzeugte Zahlenfolge ist, so gilt $s \leq 2 \cdot \log_2(a_0)$.

Beweis: Es genügt zu zeigen, dass sich die Größe der Zahlen a_i alle 2 Runden mindestens halbiert, d.h., dass für alle i, $2 \leq i \leq s$, gilt $a_i < \frac{1}{2} \cdot a_{i-2}$.

Das liegt daran, dass $a_{i-2} = d \cdot a_{i-1} + a_i$ für ein $d \geq 1$, und $a_i < a_{i-1}$.

Also $a_{i-2} \geq a_{i-1} + a_i > 2 \cdot a_i$. □

Folgerung: Damit ist die Laufzeit des Euklidischen Algorithmus auf Eingabezahlen der Bitlänge n (also $a_0 \leq 2^n - 1$) proportional zu $2 \cdot n$, und damit effizient.

Algebraische Strukturen

Untergruppen, zyklische Gruppen und Ordnungen von Gruppenelementen

Untergruppen

Definition 10.18

Sei $G = (G, \circ)$ Gruppe mit neutralem Element e. Eine Teilmenge $H \subseteq G$ heißt **Untergruppe von** G, falls $e \in H$ und $(H, \circ)$ eine Gruppe mit neutralem Element e ist.

Lemma 10.19

Sei $G = (G, \circ)$ Gruppe mit neutralem Element e. Eine Teilmenge $H \subseteq G$ ist genau dann Untergruppe von G, wenn für alle $x, y \in H$ gilt, dass $x \circ y^{-1} \in H$. (Beweis auf Übungsblatt) $\square$

- Triviale Untergruppe $\{e\} \subseteq G$.
- $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +)$.
- $\{1, -1\} \subseteq (\mathbb{Q} \setminus \{0\}, \cdot) \subseteq (\mathbb{R} \setminus \{0\}, \cdot)$.
- Sei $a \in \mathbb{R} \setminus \{0\}$. $\{a^i \mid i \in \mathbb{Z}\} \subseteq (\mathbb{R} \setminus \{0\}, \cdot)$.

Lemma 10.20

Sei G Gruppe und H, H' Untergruppen von G. Dann ist auch $H \cap H'$ Untergruppe von G. (Beweis auf Übungsblatt) $\square$

Das rechtfertigt (hinsichtlich Eindeutigkeit):

Definition 10.21

Sei $G = (G, \circ)$ Gruppe mit neutralem Element e. Für alle $g \in G$ bezeichne $\langle g \rangle$ die von g erzeugte Untergruppe, d. h. die kleinste Untergruppe in G, die g enthält.

Definition 10.22

Die Ordnung $ord_G(g)$ eines Elementes $g \in G$ bezeichnet die kleinste natürliche Zahl $k > 0$, so dass $g^k = e$.

Falls $g^k \neq e$ für alle $k \in \mathbb{N}^+$, so sei $ord_G(g) = \infty$.

Illustration und Beispiele

Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e, und es sei $g \in G$.

Wir betrachten die Folge $e = g^0, g, g^2, g^3, \cdots$

Fall 1: Es existieren $s < t$ mit $g^s = g^t$.

Dann gilt $e = (g^t) \circ (g^s)^{-1} = (g^t) \circ (g^{-1})^s = g^{t-s}$, d.h., $ord_G(g)$ endlich.

Folgerung: Jedes Element einer endlichen Gruppe hat endliche Ordnung.

Fall 2: Es existieren keine $s < t \in \mathbb{N}^+$ mit $g^s = g^t$. Dann gilt $ord_G(g) = \infty$.

Beispiel 1 $G = (\mathbb{Q} \setminus \{0\}, \cdot)$, $g = 2$:

$2^s \neq 2^t$ für alle $s < t \in \mathbb{N}$ (Fall 2).

Beispiel 2 $G = (\mathbb{Z}_{11}, \cdot)^*$, $g = 2$:

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$.

$ord_G(2) = 10$

Die Struktur der von g erzeugten Untergruppe

Lemma 10.23

Für alle Gruppen G und $g \in G$ gilt :

(a) *Falls $ord_G(g)$ unendlich ist, gilt* $\langle g \rangle = \{g^k \mid k \in \mathbb{N}\} \cup \left\{ \left(g^{-1}\right)^k \mid k \in \mathbb{N} \right\}$,

(b) *Falls $ord_G(g)$ endlich ist, gilt* $\langle g \rangle = \left\{ e, g, g^2, \ldots, g^{ord_G(g)-1} \right\}$,

Also gilt stets $|\langle g \rangle| = ord_G(g)$.

Beweis: Relation (a) ergibt sich direkt daraus, dass $\langle g \rangle$ (da Untergruppe) alle Potenzen g^k von g und deren Inverse $(g^{-1})^k$ für alle natürlichen Zahlen k enthalten muss.

Man beachte, dass $e = g^0$ und $(g^{-1})^k = g^{-k}$.

Andererseits ist $\{g^k \mid k \in \mathbb{N}\} \cup \left\{ \left(g^{-1}\right)^k \mid k \in \mathbb{N} \right\}$ bereits einen Untergruppe.

Also ist $\{g^k \mid k \in \mathbb{N}\} \cup \left\{ \left(g^{-1}\right)^k \mid k \in \mathbb{N} \right\}$ die kleinste Untergruppe, die g enthält.

Der Beweis von Lemma 10.23

Beweis von (b): Sei nun $n = ord_G(g)$ endlich.

Ist $n = 1$, so gilt $g = e$ und $\langle g \rangle = \{e\}$.

Ist $n > 1$, so haben alle $k \in \mathbb{Z}$ eine eindeutig bestimmte Darstellung $k = d \cdot n + k'$ und $k' = k \bmod n$.

Also gilt $g^k = g^{d \cdot n + k'} = (g^n)^d \circ g^{k'} = e^d \circ g^{k'} = g^{k'}$.

Das heißt $g^k = g^{k \bmod n}$ für alle $k \in \mathbb{Z}$ und damit $\{e, g, g^2, \ldots, g^{n-1}\} \subseteq \langle g \rangle$.

Die Menge $\{e, g, g^2, \ldots, g^{n-1}\}$ ist aber bereits eine Untergruppe, da für alle $s \in \{0, \ldots, n-1\}$ gilt $(g^s)^{-1} = g^{n-s}$. $\square$

Beispiel $G = (\mathbb{Z}_{11}, \cdot)^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $ord_G(2) = 10$

$\langle 2 \rangle = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$

$(5)^{-1} = (2^4)^{-1} = 2^{10-4} = 2^6 = 9.$

Zyklische Gruppen

Definition 10.24

Eine Gruppe G heißt **zyklisch**, falls ein Element $g \in G$ existiert, so dass $G = \langle g \rangle$. In diesem Fall heißt g **Erzeugendes von** G.

Beispiele:

- Die Gruppe $(\mathbb{Z}, +) = \{k \cdot 1 \mid k \in \mathbb{Z}\}$ ist zyklisch mit Erzeugendem 1 (additive Schreibweise beachten!).
- Die Gruppe $(\mathbb{Z}_m, +) = \{[0], [1], \ldots, [m-1]\}$ ist für alle natürlichen Zahlen $m \geq 2$ zyklisch mit Erzeugendem [1] (additive Schreibweise beachten!).
- Die Gruppen $(\mathbb{Q}, \cdot)^* = (\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R}, \cdot)^* = (\mathbb{R} \setminus \{0\}, \cdot)$ sind nicht zyklisch.
- Die Gruppe $(\mathbb{Z}_5, \cdot)^* = \{[1], [2], [3], [4]\}$ ist zyklisch mit den Erzeugenden [2] und [3] ($\rightarrow$ Übung).
- Die Gruppe $(\mathbb{Z}_{12}, \cdot)^* = \{[1], [5], [7], [11]\}$ ist nicht zyklisch ($\rightarrow$ Übung).

Satz von Lagrange, Linksnebenklassen

Theorem 10.25 (Satz von Lagrange)

Sei $(G, \circ)$ eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann gilt: $|H|$ teilt $|G|$.

Definition 10.26

Für alle $g, g' \in G$ gelte $g \sim_H g'$ g.d.w. $\exists h \in H : g \circ h = g'$.

Für jedes $g \in G$ heißt die Menge

$$gH = \{g \circ h \mid h \in H\}$$

die **Linksnebenklasse von g bezüglich H**.

Zum **Beweis** von Theorem 10.25 bemerke man zunächst, dass $\sim_H$ eine Äquivalenzrelation auf G ist,

(reflexiv, da $g \circ e = g$, symmetrisch, da $g \circ h = g'$ genau dann, wenn $g' \circ h^{-1} = g$ und transitiv, da aus $g_1 = g \circ h$ und $g_2 = g_1 \circ h'$ folgt, dass $g_2 = g \circ (h \circ h')$).

Die Äquivalenzklassen von $\sim_H$ sind genau die Linksnebenklassen bezüglich H, und jede Linksnebenklassen bezüglich H hat genau $|H|$ Elemente (da für $h \neq h'$ stets $g \circ h \neq g \circ h'$).

Wir erhalten eine Partition von G in disjunkte Teilmengen der Kardinalität $|H|$. □

Ordnung teil Gruppenordnung

Lemma 10.27

Sei $(G, \circ)$ eine endliche Gruppe mit neutralem Element e.

Dann gilt für alle $g \in G$, dass $ord_G(g)$ die Gruppenordnung $|G|$ teilt.

Zudem gilt $g^{|G|} = e$.

Beweis: Die Aussage $ord_G(g)$ teilt $|G|$ folgt direkt aus Theorem 10.25, da $|\langle g \rangle| = ord_G(g)$.

Damit existiert eine natürliche Zahl s mit $|G| = ord_G(g) \cdot s$.

Also gilt $g^{|G|} = g^{ord_G(g) \cdot s} = \left(g^{ord_G(g)}\right)^s = e^s = e$. $\square$

Beispiel $G = (\mathbb{Z}_{11}, \cdot)^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $|G| = 10$, $ord_G(4) = 5$

$\langle 4 \rangle = \{4^1 = 4, 4^2 = 5, 4^3 = 9, 4^4 = 3, 4^5 = 1\}$

Der Kleine Satz von Fermat

Lemma 10.28 (Kleiner Satz von Fermat)

Sei p Primzahl. Dann gilt für alle ganzen, zu p teilerfremden Zahlen a:

$$a^{p-1} \equiv 1 \mod p.$$

Beweis: Aus $ggT(p,a) = 1$ folgt $[a] \in (\mathbb{Z}_p, \cdot)^*$.

Da $|\mathbb{Z}_p^*| = p - 1$, gilt $[a]^{p-1} = [1]$ in $(\mathbb{Z}_p, \cdot)^*$.

Also $a^{p-1} \equiv 1 \mod p$. □

Lemma 10.29

Es sei $n \in \mathbb{N}$, $n \geq 2$. $(\mathbb{Z}_n, +) = \{[0], [1], \ldots, [n-1]\}$ bezeichne die zyklische Gruppe der Ordnung n (in additiver Schreibweise). Dann gilt für alle j, $0 \leq j \leq n-1$, dass

$$ord_G([j]) = \frac{n}{ggT(n,j)}.$$

Beweis: siehe Übungsblatt.

Algebraische Strukturen

Permutationsgruppen

Die Permutationsgruppe $\mathcal{S}_n$

Definition 10.30

Für alle natürlichen Zahlen $n \geq 1$ bezeichne $\mathcal{S}_n$ die Menge aller Permutationen von $\{1, \ldots, n\}$, d. h. die Menge der bijektiven Abbildungen von $\{1, \cdots, n\}$ in sich (vgl. auch Definition 10.8).

Lemma 10.31

$(\mathcal{S}_n, \circ)$ ist bezüglich der Komposition $\circ$ eine Gruppe, die für $n \geq 3$ nicht kommutativ ist.

Beweis: Das neutrale Element in $\mathcal{S}_n$ ist die Identität *id*.

Das Inverse π^{-1} einer Permutation π ist deren Umkehrabbildung.

Außerdem gibt es in $\mathcal{S}_3$ Permutationen π, π', für die $\pi \circ \pi' \neq \pi' \circ \pi$.

Beispiel: $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\pi' = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

$\pi \circ \pi' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\pi' \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. $\square$

Grundlagen der Zyklendarstellung von Permutationen

Die naheliegende Darstellung von Permutationen $\pi \in \mathcal{S}_n$ ist durch ihre Wertetabelle:

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

Alternativ wird oft die **Zyklendarstellung** verwendet, die auf Folgendem basiert.

Lemma 10.32

Für alle i, $1 \leq i \leq n$, existiert eine Zahl q, $1 \leq q \leq n$ mit $\pi^q(i) = i$ und die Zahlen $i, \pi(i), \cdots, \pi^{q-1}(i)$ sind alle untereinander verschieden.

Beweis: Es existieren Zahlen p, q, $0 \leq p < q \leq n$ mit $\pi^p(i) = \pi^q(i)$.

Wir wählen p, q minimal mit dieser Eigenschaft.

Es muss $p = 0$ gelten, da ansonsten $\pi(\pi^{p-1}(i)) = \pi(\pi^{q-1}(i))$ gelten würde, was wegen der Bijektivität von π bedeuten würde $\pi^{p-1}(i) = \pi^{q-1}(i)$.

Damit gilt $\pi^q(i) = \pi^0(i) = i$ und die Zahlen $i, \pi(i), \cdots, \pi^{q-1}(i)$ sind alle untereinander verschieden. □

Beispiel: $\pi(1) = 3$, $\pi^2(1) = \pi(3) = 4$, $\pi^3(1) = \pi(4) = 5$, $\pi^4(1) = \pi(5) = 1$, $q = 4$.

Zyklen

Definition 10.33

Eine Permutation $\pi \in \mathcal{S}_n$ heißt **Zyklus der Länge** k, falls eine Folge $(i_1, \ldots, i_k)$ von paarweise verschiedenen Zahlen aus $\{1, \ldots, n\}$ existiert, so dass

- $\pi(i_1) = i_2$, $\pi(i_2) = i_3$, $\cdots$, $\pi(i_{k-1}) = i_k$, und $\pi(i_k) = i_1$.
- $\pi(i) = i$ für alle $i \notin \{i_1, \ldots, i_k\}$.

Schreibweise: $\pi = (i_1, \ldots, i_k)$.

Zyklen $(i_1, \ldots, i_k)$ und $(j_1, \ldots, j_s)$ heißen **disjunkt**, falls $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_s\} = \emptyset$.

Beispiel: $Z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 4 & 5 & 1 & 6 & 7 & 8 & 9 \end{pmatrix}$, entspricht $Z = (1, 3, 4, 5)$.

Lemma 10.34

Für disjunkte Zyklen $Z, Z' \in \mathcal{S}_n$ gilt: $Z \circ Z' = Z' \circ Z$. $\square$

Die Zyklendarstellung von Permutationen

Theorem 10.35

Für jede Permutation $\pi \in \mathcal{S}_n$ existiert eine eindeutig bestimmte Menge paarweise disjunkter Zyklen $Z_1, \ldots, Z_t$, so dass $\pi = Z_1 \circ \cdots \circ Z_t$ und jedes i, $1 \leq i \leq n$, in genau einem dieser t Zyklen vorkommt.

Beweis: Wir erzeugen Z_1 durch die Folge $(1, \pi(1), \pi^2(1), \ldots)$ im Sinne von Lemma 10.32.

Es seien die paarweise disjunkten Zyklen $Z_1, \ldots, Z_s$ bereits erzeugt und es existiere noch ein i, $1 \leq i \leq n$, das in keinem dieser Zyklen vorkommt.

Dann erzeugen wir Z_{s+1} durch die Folge $(i, \pi(i), \pi^2(i), \ldots)$.

Z_{s+1} ist offensichtlich disjunkt zu jedem der bereits erzeugten Zyklen $Z_1, \ldots, Z_s$. $\square$

Beispiel: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 5 & 1 & 9 & 8 & 7 & 2 \end{pmatrix}$, $\pi = (1,3,4,5)(2,6,9)(7,8)$

Die Ordnung von Permutationen

Theorem 10.36

Für alle $n \geq 1$ und Permutationen $\pi \in \mathcal{S}_n$ gilt, dass

$$ord_{\mathcal{S}_n}(\pi) = kgV\left(|Z_1|, |Z_2|, \ldots, |Z_t|\right),$$

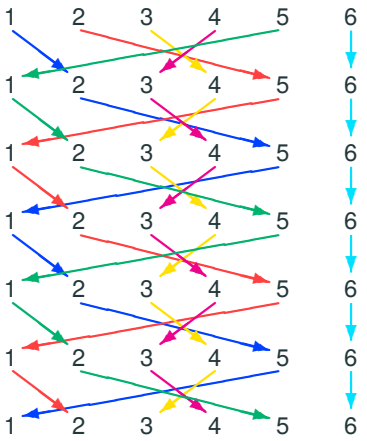
wobei $\pi = Z_1 \circ Z_2 \circ \cdots \circ Z_t$ die eindeutig bestimmte Zyklendarstellung von π ist und $|Z_j|$, $1 \leq j \leq t$, die Länge des Zyklus Z_j bezeichnet.

Beweis: siehe Übungsblatt.

Beispiel: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 5 & 1 & 9 & 8 & 7 & 2 \end{pmatrix}$, $\pi = (1,3,4,5)(2,6,9)(7,8)$,

$ord_{\mathcal{S}_n}(\pi) = 12$.

Die Ordnung von Permutationen - Bsp.: $\mathcal{S}_6$



Gegeben:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}$$

$$= (1,2,5)(3,4)$$

Gesucht: $ord_{\mathcal{S}_6}(\sigma)$

$$\Rightarrow ord_{\mathcal{S}_6}(\sigma) = 6 = kgV(3,2)$$

Algebraische Strukturen

Strukturerhaltende Abbildungen (Homomorphismen)

Definition 10.37

$G = (G, \circ)$ und $G' = (G', \otimes)$ seien Gruppen mit neutralen Elementen e, e'. Eine Abbildung $f : G \to G'$ heißt **Gruppenhomomorphismus**, falls $f(e) = e'$ und für alle $g, h \in G$ gilt:

$$f(g \circ h) = f(g) \otimes f(h).$$

Die Gruppen G, G' heißen **isomorph** (Schreibweise: $G \sim G'$), falls ein bijektiver Gruppenhomomorphismus $f : G \to G'$ (ein sogenannter **Gruppenisomorphismus**) existiert.

Lemma 10.38

Ist $f : G \to G'$ ein Gruppenhomomorphismus, dann gilt $f(g^{-1}) = f(g)^{-1}$ für alle $g \in G$. Ist f bijektiv, so gilt $ord_G(g) = ord_{G'}(f(g))$ für alle $g \in G$. (Beweis auf Übungsblatt) □

Beispiele

- **Trivialbeispiel 1:** Die Abbildung $f : G \to G'$ mit $f(g) = e'$ für alle $g \in G$ ist ein Gruppenhomomorphismus.
- **Trivialbeispiel 2:** $id_G : G \to G$ ist ein Gruppenisomorphismus.
- $f : (\mathbb{Z}, +) \to (\mathbb{Z}_m, +)$ mit $f(a) = [a]$ ist für natürliche $m \geq 2$ ein Gruppenhomomorphismus.

Lemma 10.39

Für $(G, \circ)$ Gruppe (multiplikative Schreibweise) und $g \in G$ gilt:

- *Falls $ord_G(g) = k$ so ist $f : (\mathbb{Z}_k, +) \to \langle g \rangle$ mit $f([j]) = g^j$ ein Gruppenisomorphismus.*
- *Falls $ord_G(g) = \infty$, so ist $f : (\mathbb{Z}, +) \to \langle g \rangle$ mit $f(j) = g^j$ ein Gruppenisomorphismus.*

Für $(G, \oplus)$ Gruppe (additive Schreibweise) und $g \in G$ gilt:

- *Falls $ord_G(g) = k$ so ist $f : (\mathbb{Z}_k, +) \to \langle g \rangle$ mit $f([j]) = j \cdot g$ ein Gruppenisomorphismus.*
- *Falls $ord_G(g) = \infty$, so ist $f : (\mathbb{Z}, +) \to \langle g \rangle$ mit $f(j) = j \cdot g$ ein Gruppenisomorphismus.*

(Beweis auf Übungsblatt) $\square$

Karthesisches Produkt von Gruppen

Definition 10.40

Seien $G = (G, \oplus)$ und $G' = (G', \otimes)$ Gruppen mit neutralen Elementen e, e'. Dann bezeichnet $(G, \oplus) \times (G', \otimes)$ das karthesische Produkt, d. h. die Gruppe mit der Gruppenoperation $\circ$, definiert durch

$$(g, g') \circ (h, h') = (g \oplus h, g' \otimes h')$$

für alle $g, h \in G$, $g', h' \in G'$.

Beispiel: Kleinsche Vierergruppe $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$. (vgl. Folie 45)

Wichtiger Satz aus der Algebra:

Theorem 10.41

Jede endliche kommutative Gruppe G ist isomorph zu einer Gruppe der Gestalt $(\mathbb{Z}_{m_1}, +) \times \cdots \times (\mathbb{Z}_{m_s}, +)$ *für natürliche Zahlen* $m_1, \ldots, m_s$. *(ohne Beweis hier)* □

Beispiel: $(\mathbb{Z}_{12}, \cdot)^* \sim (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$

$(\mathbb{Z}_{12}, \cdot)^*$	[1]	[5]	[7]	[11]
[1]	[1]	[5]	[7]	[11]
[5]	[5]	[1]	[11]	[7]
[7]	[7]	[11]	[1]	[5]
[11]	[11]	[7]	[5]	[1]

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([0], [0])	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([0], [1])	([0], [1])	([0], [0])	([1], [1])	([1], [0])
([1], [0])	([1], [0])	([1], [1])	([0], [0])	([0], [1])
([1], [1])	([1], [1])	([1], [0])	([0], [1])	([0], [0])

Die folgende Abbildung $f : (\mathbb{Z}_{12}, \cdot)^* \to (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ ist ein Gruppenisomorphismus:

- $f([1]) = ([0], [0])$,
- $f([5]) = ([0], [1])$,
- $f([7]) = ([1], [0])$,
- $f([11]) = ([1], [1])$,

Es gilt bspw. auch: $(\mathbb{Z}_{15}, \cdot)^* \sim (\mathbb{Z}_2, +) \times (\mathbb{Z}_4, +)$. (**selbst prüfen!**)

Weitere Beispiele isomorphe Gruppen

Weiterer wichtiger Satz aus der Algebra:

Theorem 10.42

Für alle Primzahlen p ist $(\mathbb{Z}_p, \cdot)^*$ *zyklisch, d. h. isomorph zu* $(\mathbb{Z}_{p-1}, +)$. *(ohne Beweis hier)* □

Bemerkung: Für Primzahlen p spielen die Gruppen $(\mathbb{Z}_p, \cdot)^*$ eine entscheidende Rolle im Bereich der asymmetrischen Kryptographie!

Grundidee: Sei p eine große , **öffentlich bekannte** Primzahl (z.B. $p \approx 2^{1024}$), $[g]$ ein **öffentlich bekanntes** Erzeugendes in $(\mathbb{Z}_p, \cdot)^*$ und $x \in \{0, \ldots, p-1\}$ ein **Geheimnis**.

Wer x kennt, kann $y = g^x \bmod p$ effizient berechnen.

Ein Angreifer, der y „beobachtet“, müsste jedoch x aus g, p, y ermitteln, also den entsprechenden **diskreten Logarithmus** ziehen.

Hierfür sind (bei ausreichend großem p) keine effizienten Algorithmen für Nicht-Quantencomputer bekannt.

Theorem 10.43

Für alle natürlichen Zahlen $n \geq 1$ gilt, dass jede n-elementige Gruppe $(G, \otimes)$ mit neutralem Element e isomorph zu einer Untergruppe in $\mathcal{S}_n$ ist.

Beweis: Wir ordnen jedem Gruppenelement $g \in G$ eine Permutation π_g über G zu:

Für alle $h \in G$ sei $\pi_g(h) = g \otimes h$ (ist bijektiv, da aus $g \otimes h = g \otimes h'$ stets $h = h'$ folgt).

Man sieht leicht ein, dass $\pi_e = id_G$.

Außerdem gilt für alle $g, g' \in G$ gilt, dass $\pi_{g' \otimes g} = \pi_{g'} \circ \pi_g$.

Das gilt, da

$$\pi_{g' \otimes g}(h) = (g' \otimes g) \otimes h = g' \otimes (g \otimes h) = \pi_{g'}(g \otimes h) = \pi_{g'}(\pi_g(h)). \square$$

Beispiel $(\mathbb{Z}_3, +)$

Wir betrachten die zyklische Gruppe $(\mathbb{Z}_3 = \{0, 1, 2\}, +)$ der Ordnung drei.

$$\pi_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\pi_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$