

1 | Zykelzerlegung

Zerlegen Sie folgende Permutationen in Zykel und berechnen Sie jeweils das Signum! Geben Sie außerdem die inversen Permutationen α^{-1} , β^{-1} und γ^{-1} an!

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 3 & 4 & 5 & 6 & 9 & 8 & 7 & 1 & 2 \end{pmatrix}$$

$$= (1 \ 10 \ 2 \ 3 \ 4 \ 5 \ 6 \ 9) \circ (7 \ 8) \quad \frac{1}{2}$$

$$\operatorname{sgn}(\alpha) = (-1)^7 \cdot (-1)^1 = 1 \quad \frac{1}{2}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 10 & 2 & 3 & 4 & 5 & 8 & 7 & 6 & 1 \end{pmatrix} \quad \frac{1}{2}$$

1,5

$$\beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 3 & 1 & 2 & 10 & 9 & 5 & 7 & 8 & 6 & 4 \end{pmatrix}$$

$$= (1 \ 11 \ 4 \ 2 \ 3) \circ (5 \ 10 \ 6 \ 9 \ 8 \ 7)$$

$$\operatorname{sgn}(\beta) = (-1)^4 \cdot (-1)^5 = -1$$

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 2 & 11 & 7 & 10 & 8 & 9 & 6 & 5 & 1 \end{pmatrix}$$

1,5

$$\gamma := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ n & n-1 & n-2 & \dots & 1 \end{pmatrix}$$

$\frac{n}{2}$ Transpositionen



$$= \begin{cases} ((1 \ n) \circ (2 \ n-1) \circ (3 \ n-2) \circ \dots \circ (\frac{n}{2} \ \frac{n}{2}+1)) & \text{falls } n \text{ gerade} \\ ((1 \ n) \circ (2 \ n-1) \circ \dots \circ (\frac{n+1}{2}-1, \frac{n+1}{2}+1)) & \text{falls } n \text{ ungerade} \end{cases}$$

3/4

$$\frac{n+1}{2}-1 = \frac{n-1}{2}$$

Transpositionen

$$\operatorname{sgn}(j) = \begin{cases} (-1)^{\frac{n}{2}} & \text{falls } n \text{ gerade} \\ (-1)^{\frac{n-1}{2}} & \text{falls } n \text{ ungerade} \end{cases} \quad \text{3/4}$$

$$j^{-1} = j^{\frac{1}{2}}$$

$$\text{für } j = \textcircled{2}$$

2 | Kleingruppen

Die **Verknüpfungstabelle** einer Gruppe $(G, *)$ hat eine Zeile für jedes Element $x \in G$ und eine Spalte für jedes Element $y \in G$. Sei w in Zeile x und Spalte y den Wert von $x * y$ aus.

- (a) Wie sehen die Verknüpfungstabellen von $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ aus (siehe Blatt 4, Aufgabe 2)?

② ($\frac{1}{2}$ Punkt pro vollständig richtiger Tabelle)

$$\mathbb{Z}/2\mathbb{Z}: \begin{array}{c|cc} + & [0] & [1] \\ \hline [0] & [0] & [1] \\ [1] & [1] & [0] \end{array}$$

$$\mathbb{Z}/3\mathbb{Z}: \begin{array}{c|ccc} + & [0] & [1] & [2] \\ \hline [0] & [0] & [1] & [2] \\ [1] & [1] & [2] & [0] \\ [2] & [2] & [0] & [1] \end{array}$$

$$\mathbb{Z}/4\mathbb{Z}: \begin{array}{c|cccc} + & [0] & [1] & [2] & [3] \\ \hline [0] & [0] & [1] & [2] & [3] \\ [1] & [1] & [2] & [3] & [0] \\ [2] & [2] & [3] & [0] & [1] \\ [3] & [3] & [0] & [1] & [2] \end{array}$$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$$\begin{array}{c|cccc} + & ([0],[0]) & ([0],[1]) & ([1],[0]) & ([1],[1]) \\ \hline ([0],[0]) & ([0],[0]) & ([0],[1]) & ([1],[0]) & ([1],[1]) \\ ([0],[1]) & ([0],[1]) & ([0],[0]) & ([1],[1]) & ([1],[0]) \\ ([1],[0]) & ([1],[0]) & ([1],[1]) & ([0],[0]) & ([0],[1]) \\ ([1],[1]) & ([1],[1]) & ([1],[0]) & ([0],[1]) & ([0],[0]) \end{array}$$

Tipp für (b-d): Zeigen Sie zunächst, dass für jedes Element y einer Gruppe $(G, *)$ die durch $x \mapsto x * y$ und $x \mapsto y * x$ definierten Abbildungen $G \rightarrow G$ Bijektionen sind. Dann folgt, dass in der Verknüpfungstabelle in jeder Zeile jedes Element von G genau einmal auftritt, und dass auch in jeder Spalte jedes Element von G genau einmal auftritt.

$\frac{1}{2}$ Punkt falls keine Punkte für (b) & (c)

$G \xrightarrow{x \mapsto x * y}$ ist bijektiv mit

Umkehrabbildung $G \xrightarrow{x \mapsto x * y^{-1}}$

$G \xrightarrow{x \mapsto y * x}$ ist bijektiv mit

Umkehrabbildung $G \xrightarrow{x \mapsto y^{-1} * x}$

(b) Jede Gruppe mit zwei Elementen ist isomorph zu $\mathbb{Z}/2\mathbb{Z}$.

①

Sei $G = (\{a, b\}, *)$ mit $a \neq b$.

Ein Element muss neutral sein, sagen wir a . Dann gibt es nur eine mögliche Verknüpfungstabelle:

$*$	a	b
a	a	b
b	b	a

$\frac{3}{4}$ bis hier

Definiere $\mathbb{Z}/2\mathbb{Z} \xrightarrow{f} \{a, b\}$

$\begin{bmatrix} 0 \end{bmatrix} \mapsto a$
 $\begin{bmatrix} 1 \end{bmatrix} \mapsto b$

$+\frac{1}{4}$

Offenbar f bijektiv. Anhand der Tabellen sieht man: f Homomorphismus.

(c) Jede Gruppe mit drei Elementen ist isomorph zu $\mathbb{Z}/3\mathbb{Z}$.

①

Sei $G = (\{a, b, c\}, *)$ mit $|\{a, b, c\}| = 3$.

Sei wieder a neutral.

Wieder gibt es nur eine mögliche Verknüpfungstabelle:

$*$	a	b	c
a	a	b	c
b	b	a	$?$
c	c	c	$?$

geht nicht

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\frac{3}{4}$ bis hier

Definiere $\mathbb{Z}/3\mathbb{Z} \xrightarrow{f} \{a, b, c\}$

$[0] \mapsto a$
 $[1] \mapsto b$
 $[2] \mapsto c$

$+\frac{1}{4}$

und argumentiere wie oben.

(d) Ist die Gruppe $\mathbb{Z}/4\mathbb{Z}$ isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

⑦

Nein:

Für jedes Element $y \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
gilt: $y + y = 0$.

Angenommen, $f: \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
wäre ein Gruppenisomorphismus. Dann
würde insbesondere folgen:

$$f([2]) = f([1] + [1]) = f([1]) + f([1])$$

$\stackrel{\text{Homomorphismus}}{=} 0 = f([0])$

Also $f([2]) = f([0])$, obwohl
 $[2] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$

↯ Injektivität von f .

Aufgabe 3

(a)

Wir zeigen zunächst, dass $\mathbb{Z}[i]$ eine Untergruppe von $\mathbb{C}$ ist:

- offenbar gilt $0 = 0 + i \cdot 0 \in \mathbb{Z}[i]$
- Sind $a+ib, a'+ib' \in \mathbb{Z}[i]$, also $a, a', b, b' \in \mathbb{Z}$,
so auch $(a+ib) + (a'+ib') = \underbrace{a+a'}_{\in \mathbb{Z}} + i \underbrace{(b+b')}_{\in \mathbb{Z}}$

- Ist $a+ib \in \mathbb{Z}[i]$, also $a, b \in \mathbb{Z}$, so sind auch $-a, -b \in \mathbb{Z}$ und somit $-(a+ib) = -a + i(-b) \in \mathbb{Z}[i]$

0,5 Pkt

Auch bezüglich der Multiplikation ist $\mathbb{Z}[i]$ in $\mathbb{C}$ abgeschlossen:

Sind $a+ib, a'+ib' \in \mathbb{Z}[i]$, also $a, a', b, b' \in \mathbb{Z}$, so ist
auch $(a+ib) \cdot (a'+ib') = \underbrace{aa' - bb'}_{\in \mathbb{Z}} + i \underbrace{(ab' + a'b)}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$

Ferner ist $1 = 1 + i \cdot 0 \in \mathbb{Z}[i]$

0,5

(b) Beh.: $z \in \mathbb{Z}[i]^* \Leftrightarrow \|z\|=1$

($\Rightarrow$)
1P

Ist $a+ib \in \mathbb{Z}[i]^*$, so ex. ein $\overline{z} \in \mathbb{Z}[i]$ mit
 $(a+ib)z = 1 = z(a+ib)$.

Somit erhalten wir

$$\begin{aligned} \|(a+ib)z\| &= \|1\| = 1 \\ &= \|a+ib\| \cdot \|z\| \end{aligned}$$

$$= \sqrt{a^2+b^2} \cdot \sqrt{a'^2+b'^2}$$

und daher

$$\underbrace{(a^2+b^2)}_{\in \mathbb{Z}_{\geq 0}} \underbrace{(a'^2+b'^2)}_{\in \mathbb{Z}_{\geq 0}} = 1.$$

$$\text{Also } a^2+b^2 = 1 = (a'^2+b'^2) \quad \text{und somit } \|a+ib\| = \sqrt{a^2+b^2} = 1.$$

($\Leftarrow$) Ist $\|z\|=1$, so ist $\overline{z} \in \mathbb{Z}[i]$ ein Inverses
1P von z , denn $z \cdot \overline{z} = \|z\|^2 = 1$.

(c) Für $z=a+ib \in \mathbb{Z}[i]$ gilt:

$$\|z\|=1 \Leftrightarrow \|z\|^2=1$$

$$\Leftrightarrow a^2+b^2=1$$

$$\Leftrightarrow (a=\pm 1 \wedge b=0) \vee (a=0 \wedge b=\pm 1).$$

Also folgt aus (b): $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ — 1 P
 $|\mathbb{Z}[i]^*| = 4.$

Die Verknüpfungstabelle von $\mathbb{Z}[i]^*$ ist

•	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	1	-1
-i	-i	i	-1	1

bzw.

	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

1 Pwr

sodass $\mathbb{Z}[i]^*$ nach dem letzten Blatt isomorph
zu $\mathbb{Z}/4\mathbb{Z}$ ist

(Ein Isomorphismus ist durch

$$\begin{aligned} \mathbb{Z}[i]^* &\rightarrow \mathbb{Z}/4\mathbb{Z} \\ i &\mapsto [4] \end{aligned}$$

gegeben.)

Aufgabe 4

Schritt 1:

Die Abbildung

$$f: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/(nm)\mathbb{Z}, ([x], [y]) \mapsto [xm + yn]$$

ist wohldefiniert:

Seien $[x] \in \mathbb{Z}/n\mathbb{Z}$ und $[y] \in \mathbb{Z}/m\mathbb{Z}$ und seien x' bzw. y' andere Repräsentanten von $[x]$ bzw. $[y]$. Es gelten also

$$x - x' = na \quad (\sim x' = x - na)$$

und

$$y - y' = mb \quad (\sim y' = y - mb)$$

für geeignete $a, b \in \mathbb{Z}$. Somit erhalten wir

$$\begin{aligned} f([x'], [y']) &= [x'm + y'n] = [(x - na)m + (y - mb)n] \\ &= [xm - nam + yn - mbn] \\ &= [xm + yn - (nm)(a + b)] \\ &= [xm + yn] - \underbrace{[(nm)(a + b)]}_{= [0]} \\ &= [xm + yn], \end{aligned}$$

sodass f wohldefiniert ist.

1 Pkt.

Schritt 2:

Die Abbildung f ist ein Gruppenhomomorphismus:

Sind $(x), (x') \in \mathbb{Z}/n\mathbb{Z}$ und $(y), (y') \in \mathbb{Z}/n\mathbb{Z}$,
so erhalten wir

$$\begin{aligned} f((x), (y)) + f((x'), (y')) &= f((x+x'), (y+y')) \\ &= [(x+x')m + (y+y')n] \\ &= [xm + yn + x'm + y'n] \\ &= [xm + yn] + [x'm + y'n] \\ &= f((x), (y)) + f((x'), (y')). \end{aligned}$$

1 Pkt

1 Pu

Schritt 3:

für teilerfremde n, m

Die Abbildung f ist $\checkmark$ injektiv:

Sei $([x], [y]) \in \ker(f)$, d.h. es ex. ein

$a \in \mathbb{Z}$ mit

$$xm + yn = nma.$$

Dann erhalten wir

$$xm = n(ma - y) \text{ und } yn = m(na - x),$$

sodass n ein Teiler von xm und m ein Teiler von yn ist. Sind n und m nun teilerfremd, so muss also n ein Teiler von x und m ein Teiler von y sein, sodass

$$([x], [y]) = ([0], [0]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Somit ist f für teilerfremde n und m injektiv.

Schritt U:

für teilerfremde ~~n, m~~ n, m

Die Abbildung f ist ^vsogar ein Gruppenisomorphismus:

Da f ein Gruppenhomomorphismus ist, welcher für teilerfremde ~~n und m~~ n und m injektiv ist, müssen wir nur noch begründen, dass f dann auch surjektiv ist.

Dies ist der Fall, da $\#(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = nm = \#(\mathbb{Z}/nm\mathbb{Z})$, und die Begriffe "injektiv" und "surjektiv" für endliche Mengen gleicher Kardinalität zusammenfallen.

[Satz 1.26]

1 PL

Die Behauptung folgt nun, da $[1] \in \mathbb{Z}/(nm)\mathbb{Z}$ für teilerfremde n und m ein Urbild unter f haben muss. Es ex. also $x', y \in \mathbb{Z}$ mit

$$mx' + ny = 1 + (nm)a$$

für ein geeignetes $a \in \mathbb{Z}$. Somit

$$\underbrace{m(x' - na)}_{=: x} + ny = 1.$$

Im Bsp.:

$$\underbrace{(-3) \cdot 17}_{-51} + \underbrace{4 \cdot 13}_{52} = 1$$

$c = -51$

$s2$

1 PL