

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!

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 3 & 4 & 5 & 6 & 9 & 8 & 7 & 1 & 2 \end{pmatrix}$$
$$= \underbrace{(1 \ 10 \ 2 \ 3 \ 4 \ 5 \ 6 \ 9)}_{\text{Länge 8}} \circ \underbrace{(7 \ 8)}_{\text{Länge 2}}$$

$$\text{sgn}(\alpha) = (-1)^{8-1} \cdot (-1)^{2-1} = 1$$

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

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

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

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

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

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

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

$$\text{sgn}(\gamma) = \begin{cases} (-1)^{\frac{n}{2}} & \text{falls } n \text{ gerade} \\ (-1)^{\frac{n-1}{2}} & \text{falls } n \text{ ungerade} \end{cases}$$

$$\gamma^{-1} = \gamma$$

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)?

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

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

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

$$[2] + [1] = [3]$$

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

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

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.

Für jedes $y \in G$ ist die Abb.

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & y * x \end{array}$$

bijektiv mit Umkehrabb.

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & y^{-1} * x \end{array}$$

Für jedes $y \in G$ ist die Abb.

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x * y \end{array}$$

bijektiv mit Umkehrabb.

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x * y^{-1} \end{array}$$

Also tritt in jeder Spalte und jeder Zeile der Verknüpfungstabelle jedes Element genau einmal auf.

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

Sei $G = (\{a, b\}, *)$ mit $a \neq b$ eine Gruppe. Ein Element muss neutral sein, sagen wir a . Dann gibt es nur eine mögliche Verknüpfungstabelle:

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

*	a	b
a	a	b
b	b	a

Definiere $f: (\mathbb{Z}/2\mathbb{Z}, +) \longrightarrow (\{a, b\}, *)$

$$[0] \mapsto a$$

$$[1] \mapsto b$$

Offenbar ist f bijektiv. Tabelle zeigt: f ist Gruppenhomo.

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

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

Sei wieder o.B.d.A. a neutral.

Wieder gibt es nur eine mögliche Verknüpfungstabelle:

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

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

Definiere $f: (\mathbb{Z}/3\mathbb{Z}, +) \longrightarrow (\{a, b, c\}, *)$

$$[0] \mapsto a$$

$$[1] \mapsto b$$

$$[2] \mapsto c$$

und argumentiere wie oben.

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

Nein: In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gilt für jedes Element

$$x + x = 0 \quad (*)$$

Angenommen, es gäbe einen Gruppenisomorphismus $f: \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dann würde folgen: f Homo.

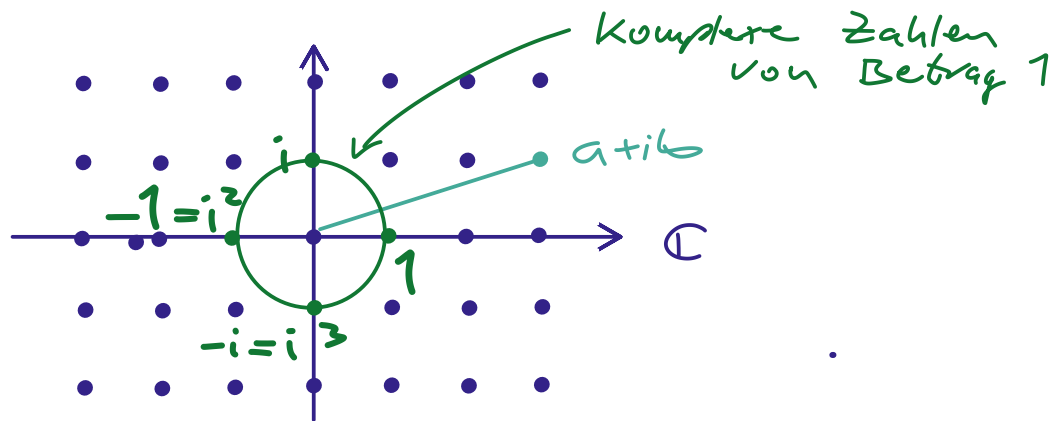
$$\begin{aligned} \underline{f([2])} &= f([1] + [1]) \begin{pmatrix} \downarrow \\ \stackrel{(*)}{=} 0 \\ \downarrow \\ = \underline{f([0])} \end{pmatrix} = f([1]) + f([1]) \\ &= \underline{f([0])} \end{aligned}$$

Aber $[2] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$.

↪ Injektivität von f .

3 | Gaußsche Zahlen ★

- (a) Zeigen Sie, dass die Teilmenge $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ einen Unterring der komplexen Zahlen $\mathbb{C}$ definiert. Das heißt im Einzelnen: $\mathbb{Z}[i]$ definiert eine Untergruppe von $(\mathbb{C}, +)$, die Multiplikation von $\mathbb{C}$ lässt sich auf $\mathbb{Z}[i]$ einschränken, und $\mathbb{Z}[i]$ enthält das neutrale Element 1 der Multiplikation.



$\mathbb{Z}[i] \subseteq \mathbb{C}$ Untergruppe:

$$(u_1): 0 = 0 + i \cdot 0 \in \mathbb{Z}[i]$$

$$(u_2): \text{Für } a+ib, a'+ib' \in \mathbb{Z}[i] \text{ ist auch}$$

$$(a+ib) + (a'+ib') = \underbrace{(a+a')}_{\in \mathbb{Z}} + i \underbrace{(b+b')}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

$$(u_3): \text{Für } a+ib \in \mathbb{Z}[i] \text{ ist auch}$$

$$-(a+ib) = -a + i(-b) \in \mathbb{Z}[i]$$

Auch bezüglich $\cdot$ ist $\mathbb{Z}[i]$ abgeschlossen:

Für $a+ib, a'+ib' \in \mathbb{Z}[i]$ ist

$$(a+ib) \cdot (a'+ib') = \underbrace{(aa' - bb')}_{\in \mathbb{Z}} + i \underbrace{(ab' + ba')}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

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

- (b) Zeigen Sie, dass eine Zahl $z \in \mathbb{Z}[i]$ genau dann in $\mathbb{Z}[i]$ eine Einheit, also invertierbar bezüglich der Multiplikation, ist, wenn $\|z\| = 1$ ist.

($\Rightarrow$) Sei $z \in \mathbb{Z}[i]$ eine Einheit in $\mathbb{Z}[i]$.

Dann existiert also

$$z' \in \mathbb{Z}[i],$$

$$\text{sodass } z \cdot z' = 1$$

Nehmen wir hier den Betrag, erhalten

$$\text{wir } \underbrace{\|z\|^2}_{\substack{\in \mathbb{Z} \\ \geq 0}} \cdot \underbrace{\|z'\|^2}_{\substack{\in \mathbb{Z} \\ \geq 0}} = \underbrace{\|1\|^2}_1$$

$$\text{Es ist } \|1\| = 1. \quad \text{Da } \|z\|^2 \in \mathbb{Z}, \geq 0$$

$$\text{und } \|z'\|^2 \in \mathbb{Z}, \geq 0$$

$$\text{folgt: } \|z\|^2 = 1, \text{ also } \|z\| = 1.$$

($\Leftarrow$) Ist $\|z\| = 1$, so ist $z \cdot \bar{z} = 1$.

Für $z \in \mathbb{Z}[i]$ ist auch $\bar{z} \in \mathbb{Z}[i]$,

also ist in diesem Fall $z \in \mathbb{Z}[i]^\times$.

- (c) Wie viele Einheiten gibt es in $\mathbb{Z}[i]$? Zu welcher aus der Vorlesung bekannten Gruppe ist die Einheitengruppe $(\mathbb{Z}[i])^\times$ isomorph?

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

$$\|z\| = 1 \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow (a = \pm 1 \wedge b = 0) \vee (a = 0 \wedge b = \pm 1)$$

Also folgt: $\mathbb{Z}[i]^\times = \{ \pm 1, \pm i \}$

$$|\mathbb{Z}[i]^\times| = 4$$

Verknüpfungstabelle:

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

Die Gruppe ist isomorph zu $\mathbb{Z}/4\mathbb{Z}$
via

$$(\mathbb{Z}/4\mathbb{Z}, +) \longrightarrow (\mathbb{Z}[i]^+, \cdot)$$

$$[0] \mapsto 1$$

$$[1] \mapsto i$$

$$[2] \mapsto -1$$

$$[3] \mapsto -i$$

bzw. $[4] \mapsto i^4$

4 | Millimeterarbeit ★

Zu je zwei teilerfremden Zahlen $n, m \in \mathbb{Z} \setminus \{0\}$ existieren Koeffizienten $x, y \in \mathbb{Z}$, für die gilt:

$$xm + yn = 1$$

Schritt 1: Es gibt eine Abbildung $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/(nm)\mathbb{Z}$, die $([x], [y])$ auf $[xm + yn]$ abbildet.

Wohldefiniertheit:

Angenommen, $[x'] = [x]$ in $\mathbb{Z}/n\mathbb{Z}$
und $[y'] = [y]$ in $\mathbb{Z}/m\mathbb{Z}$

Dann ist $x' = x + k \cdot n$ für ein $k \in \mathbb{Z}$,
 $y' = y + l \cdot m$ für ein $l \in \mathbb{Z}$

und somit

$$\begin{aligned} (x'm + y'n) &= (x + kn)m + (y + lm)n \\ &= (xm + yn) + (k+l) \cdot \textcircled{mn} \end{aligned}$$

Daraus folgt:

$$[x'm + y'n] = [xm + yn] \quad \text{in } \mathbb{Z}/nm\mathbb{Z}$$

Schritt 2: Diese Abbildung ist ein Gruppenhomomorphismus.

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

Schritt 3: Sie ist für teilerfremde m, n injektiv.

Seien m, n teilerfremd.

Wir benutzen Injektivitätskriterium: Es reicht, z.z.: $f([x], [y]) = [0]$ $\Rightarrow$ $([x], [y]) = ([0], [0])$

Sei also $f([x], [y]) = [0]$,

also $[xm + yn] = [0]$ in $\mathbb{Z}/mn\mathbb{Z}$,

also $xm + yn = k \cdot mn$ für ein $k \in \mathbb{Z}$.

Inbesondere:

$$x \cdot m = (km - y) \cdot n, \text{ also } n \mid x \cdot m$$

$$y \cdot n = (kn - x) \cdot m, \text{ also } m \mid y \cdot n$$

Da m, n teilerfremd sind, folgt: $n \mid x$
 $m \mid y$

Also ist $[x] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$
 $[y] = [0]$ in $\mathbb{Z}/m\mathbb{Z}$.

Schritt 4: Sie definiert für teilerfremde m, n sogar einen Gruppenisomorphismus.

Es reicht noch z.z.: f bijektiv.

Es ist

$$|\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z}| \cdot |\mathbb{Z}/m\mathbb{Z}| = m \cdot n = |\mathbb{Z}/mn\mathbb{Z}|$$

Also folgt Bijektivität nach Satz 1.26
aus Injektivität.

Wieso folgt nun die Behauptung?

Seien m, n teilerfremd, f wie oben.

Da f surjektiv ist, $\exists x, y \in \mathbb{Z}$ mit

$$f([x], [y]) = [1],$$

also $[xm + yn] = [1].$

Das bedeutet:

$$xm + yn = 1 + k \cdot mn \quad \text{für ein } k \in \mathbb{Z}$$

bzw. $(x - kn) \cdot m + yn = 1.$

Beispiel: $n = 13, \quad m = 17$

$$-3 \cdot 17 + 4 \cdot 13 = -51 + 52 = 1$$