Nachtrag zum Thema symmetrische Gruppen bzw. Diedergruppen

Erinnerung: Sei $n \in \mathbb{N}$, $n \geq 3$. Dann ist die Diedergruppe D_n eine Untergruppe der Bewegungsgruppe B_2 bestehend aus $2n$ Elementen (n Drehungen, n Spiegelungen)

genauer: $D_n = \{ \sigma_n^k \mid 0 \leq k < n \} \cup \{ \sigma_n^k \circ \tau \mid 0 \leq k < n \}$

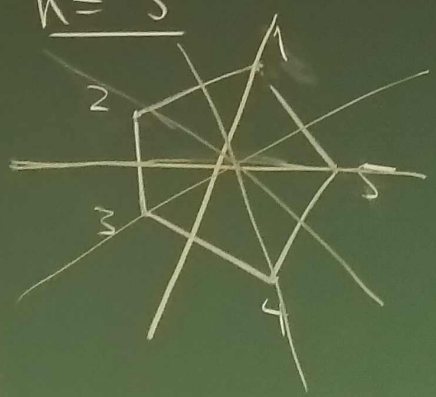
wobei $\sigma_n = D_{2\pi/n}$ = Drehung um $\frac{2\pi}{n}$ (Bogenmaß)

τ = Spiegelung an der x-Achse.

wobei $\sigma_n = D_{2\pi/n}$ = Drehung um $\frac{2\pi}{n}$ (Bogenmaß)

Bem.: Man kann zeigen, dass D_n isomorph zu einer $2n$-elementigen Untergruppe $\tilde{D}_n$ von S_n ist.

n = 5



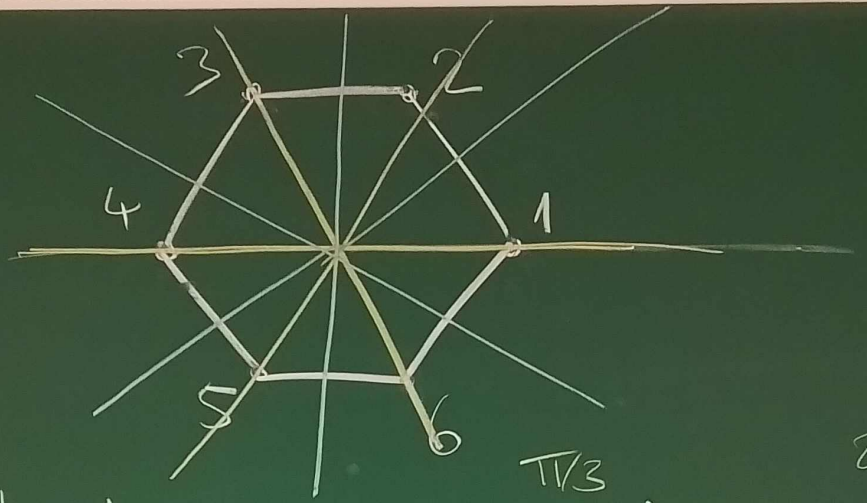
$(1\,2\,3\,4\,5) =: \tilde{\sigma}_5$ entspricht der Drehung um $\frac{2\pi}{5}$

$(1\,4)(2\,3)$ entspricht der Spiegelung an der x-Achse $=: \tilde{\tau}$

$(2\,5)(3\,4)$ entspricht der Spiegelung an der gelben Achse

insgesamt: $\tilde{D}_5 = \{ \underset{0}{\mathrm{id}}, \underset{2\pi/5}{(1\,2\,3\,4\,5)}, \underset{4\pi/5}{(1\,3\,5\,2\,4)}, \underset{6\pi/5}{(1\,4\,2\,5\,3)}, \underset{8\pi/5}{(1\,5\,4\,3\,2)}, (1\,4)(2\,3), (2\,5)(3\,4), (1\,3)(4\,5), (2\,4)(1\,5), (1\,2)(3\,5) \}$

$n = 6$



$\tilde{D}_6 = \{ \mathrm{id}, (123456), (135)(246), (14)(25)(36), (153)(264), (165432), (26)(35), (13)(46), (24)(15), (16)(25)(34), (12)(36)(45), (14)(23)(56) \}$

($\pi/3$, $2\pi/3$, π, $4\pi/3$, $5\pi/3$)

überprüfe: „Spiegelt man das Fünfeck an der x-Achse, dreht um $\frac{2\pi}{5}$ gegen den

Uhrzeigersinn und spiegelt nochmals an der x-Achse. dann entspricht dies insgesamt der Drehung um $\frac{2\pi}{5}$ mit dem Uhrzeigersinn.

$\tilde{\tau} \circ \rho_5 \circ \tilde{\tau} = (14)(23) \circ (12345) \circ (14)(23)$

$= (15432) = \hat{\rho}_5^{-1}$

Restklassen und Kongruenzen

Erinnerung: $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

„a und b sind kongruent modulo n"

(Notation: $a \equiv_n b$ oder $a \equiv b \bmod n$ oder $a \equiv b\ (n)$) bedeutet: $b - a$ ist teilbar

durch $n \iff \exists k \in \mathbb{Z} : b - a = kn$

Notation: $a \equiv b \equiv c \equiv d \bmod n$ ist eine verkürzte Schreibweise für $(a \equiv b \bmod n) \wedge (b \equiv c \bmod n) \wedge (c \equiv d \bmod n)$

Beispiel: (i) $\ldots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv \ldots \bmod 3$

(ii) $\equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv \ldots \bmod 4$

Erinnerung: $\equiv_n$ ist eine Äquivalenzrelation (d.h. reflexiv, symmetrisch und transitiv)

Jede Äquivalenzrelation $\sim$ auf einer Menge X liefert eine Zerlegung der Menge X gegeben durch die Äquivalenzklassen bzgl. der

(23)

Relation $\sim$ Dabei ist die Äquivalenzklasse eines Elements $x \in X$ gegeben durch

$$[x]_\sim = \{ y \in X \mid x \sim y \}$$

Die Äquivalenzklassen bzgl. $\equiv_n$ sind die Kongruenzklassen (oder Restklassen) modulo n, d.h. die Teilmengen von $\mathbb{Z}$ der Form

$$[a]_{\equiv_n} = \{ b \in \mathbb{Z} \mid a \equiv_n b \} =$$

$$\{ b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b = a + nk \} = a + n\mathbb{Z}$$

Kurzschreibweise: $\bar{a}$ statt $[a]_{\equiv_n}$

Die Menge aller Kongruenzklassen modulo n haben wir mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.

und $3+4\mathbb{Z}$, und $-4 \in 0+4\mathbb{Z}$, $5 \in 1+4\mathbb{Z}$, $10 \in 2+4\mathbb{Z}$, $11 \in 3+4$

bekannt: Für jedes $n \in \mathbb{N}$ besteht $\mathbb{Z}/n\mathbb{Z}$ aus genau n verschiedenen Elementen, nämlich $k+n\mathbb{Z}$ mit $0 \leq k < n$.

Bsp: $\mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

wichtig: Für $n \in \mathbb{N}$ und beliebige $a, b \in \mathbb{Z}$ gilt die Äquivalenz

$$a+n\mathbb{Z} = b+n\mathbb{Z} \iff a \equiv_n b \iff n \mid (b-a)$$

Bsp In $\mathbb{Z}/7\mathbb{Z}$ gilt $\bar{1} = \overline{15}$ und $\overline{-2} = \overline{19}$.

Def. Sei X eine Menge, $\sim$ eine Äquivalenzrelation auf X. Eine Teilmenge $R \subseteq X$ nennt man ein

Repräsentantensystem der Äquivalenzklassen bzgl. $\sim$, wenn jede Äquivalenzklasse bzgl $\sim$ genau ein Element aus R enthält.

Bsp: (i) $R = \{0, 1, 2, \ldots, n-1\}$ ist ein Repr.-system der Äquivalenzklassen bzgl. $\equiv_n$.

denn: Die Äquivalenzklassen sind die Mengen der Form $k + n\mathbb{Z}$ mit $0 \leq k < n$, und jede solche Klasse enthält genau ein Element aus R, nämlich k.

(ii) $R = \{-4, 5, 10, 11\}$ ist ein Repräsentantensystem der Äquivalenzkl. bzgl. $\equiv_4$ (d.h. $\mathbb{Z}/4\mathbb{Z}$)

denn: Die Äquivalenzklassen sind $0+4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, und $3+4\mathbb{Z}$, und $-4 \in 0+4\mathbb{Z}$, $5 \in 1+4\mathbb{Z}$, $10 \in 2+4\mathbb{Z}$, $11 \in 3+4\mathbb{Z}$.

Bem: Jedes Repräsentantensystem von $\mathbb{Z}/n\mathbb{Z}$, und nicht nur $\{0, 1, \ldots, n-1\}$ kann benutzt werden, um die Verknüpfungstafeln von $+$ und $\cdot$ auf $\mathbb{Z}/4\mathbb{Z}$ anzugeben.

Bsp:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$+$	$\overline{-4}$	$\overline{5}$	$\overline{10}$	$\overline{11}$
$\overline{-4}$	$\overline{-4}$	$\overline{5}$	$\overline{10}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{10}$	$\overline{11}$	$\overline{-4}$
$\overline{10}$	$\overline{10}$	$\overline{11}$	$\overline{-4}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{-4}$	$\overline{5}$	$\overline{10}$

$\bar{0} = \overline{-4}$, $\bar{1} = \overline{5}$, $\bar{2} = \overline{10}$, $\bar{3} = \overline{11}$

$\overline{5} + \overline{10} = \overline{15} = \overline{3} = \overline{11}$

$\cdot$	$\overline{-4}$	$\overline{5}$	$\overline{10}$	$\overline{11}$
$\overline{-4}$	$\overline{-4}$	$\overline{-4}$	$\overline{-4}$	$\overline{-4}$
$\overline{5}$	$\overline{-4}$	$\overline{5}$	$\overline{10}$	$\overline{11}$
$\overline{10}$	$\overline{-4}$	$\overline{10}$	$\overline{-4}$	$\overline{10}$
$\overline{11}$	$\overline{-4}$	$\overline{11}$	$\overline{10}$	$\overline{5}$

$\overline{5} \cdot \overline{10} = \overline{50} = \overline{2} = \overline{10}$

Algebraische Strukturen

Sei $n \in \mathbb{N}$. Aus der Vorlesung ist bekannt:

- $(\mathbb{Z}/n\mathbb{Z}, +)$ ist eine Gruppe
  (Neutralelement ist $\overline{0}$, das Inverse von $\overline{a}$ ist jeweils $-\overline{a} = \overline{-a}$)

- $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ ist ein Monoid (Neutralelement $\bar{1}$)

(Das Assoziativgesetz gilt, denn: Seien $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$, zzg: $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$. Seien $a, b, c \in \mathbb{Z}$ so gewählt, dass $\bar{a} = a + n\mathbb{Z}$, $\bar{b} = b + n\mathbb{Z}$, $\bar{c} = c + n\mathbb{Z}$.

$\Rightarrow (\bar{a} \cdot \bar{b}) \cdot \bar{c} = ((a+n\mathbb{Z}) \cdot (b+n\mathbb{Z})) \cdot (c+n\mathbb{Z})$

$= (ab+n\mathbb{Z}) \cdot (c+n\mathbb{Z}) = (ab) \cdot c + n\mathbb{Z} =$

$a \cdot (bc) + n\mathbb{Z} = (a+n\mathbb{Z}) \cdot (bc+n\mathbb{Z}) =$

$(a+n\mathbb{Z}) \cdot ((b+n\mathbb{Z}) \cdot (c+n\mathbb{Z})) = \bar{a} \cdot (\bar{b} \cdot \bar{c})$.)

- $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ ist für $n > 1$ keine Gruppe (da $\bar{0}$ kein Inverses bzgl. $\cdot$ besitzt), aber:

Die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z}$ der invertierbaren Elemente ist mit der (eingeschränkten) Multiplikation eine Gruppe.

Bsp: $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$