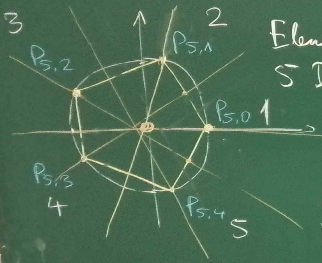
Diedergruppen und Permutationsgruppen



Elemente der Diedergruppe D_5:
5 Drehungen und 5 Spiegelungen

werden später sehen: Die Diedergr. D_5 „operiert" auf der Menge der Ecken $\{P_{5,0}, \dots, P_{5,4}\} =: E_5$

Das liefert einen Gruppenhom. $D_5 \xrightarrow{\Phi} \mathrm{Per}(E_5)$, der in dieser Situation sogar injektiv ist. → können D_5 mit einer Untergruppe von $\mathrm{Per}(E_5)$ „identifizieren", auf Grund der Bijektion $M_5 = \{1, \dots, 5\} \to E_5$, $k \mapsto P_{5,k-1}$

D_5 mit einer Untergruppe von $\mathrm{Per}(E_5)$ identifizieren;
auf Grund der Bijektion $M_5 = \{1, \dots, 5\} \to E_5$, $k \mapsto P_{5,k-1}$

darüber hinaus mit einer Untergr. von $\mathrm{Per}(M_5) = S_5$.

Idee dabei: Das Element in S_5 vertauscht die Zahlen $1, 2, \dots, 5$ „genau so", wie das Element in D_5 die Ecken vertauscht. Die Elemente des Bildes von D_5 in S_5 ist dann geg. durch

$$\tilde{D}_5 = \{ \mathrm{id}, \underset{72^\circ\text{-Drehung}}{(1\,2\,3\,4\,5)}, \underset{144^\circ\text{-Drehung}}{(1\,3\,5\,2\,4)}, \underset{216^\circ\text{-Drehung}}{(1\,4\,2\,5\,3)},$$
$$\underset{288^\circ\text{-Drehung}}{(1\,5\,4\,3\,2)}, \underset{\text{Spiegelung } x\text{-Achse}}{(2\,5)(3\,4)}, (1\,2)(3\,5), (1\,3)(4\,5),$$
$$(2\,3)(1\,4), (1\,5)(2\,4) \}$$

Überprüfe die folgende Aussage:

„Dreht man die Spiegelungsachse durch den Punkt 4 auf die x-Achse, spiegelt an der x-Achse und dreht zurück, dann hat man im Endeffekt an der Achse durch 4 gespiegelt."

Spiegelung an der Achse durch 4 (bzw. $P_{5,3}$):

$$(12)(35)$$

Drehung der Achse durch 4 auf die x-Achse:

Drehung um 144°, also (13524)

Spiegelung an der x-Achse: $(25)(34)$

Zurückdrehen: $(13524)^{-1} = (14253)$

nan

egelt".

$(14253)\circ(25)(34)\circ(13524)$

$= (12)(35)(4) = (12)(35)$

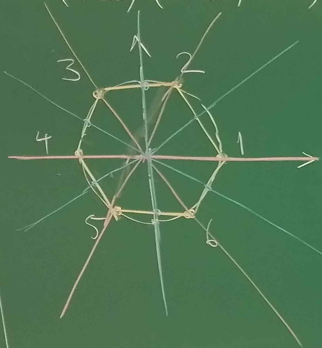


Bild von D_6 in S_6:

$\tilde{D}_6 = \{ id, \underbrace{(123456)}_{60^\circ\text{-Drehung}},$
$(135)(246), (14)(25)(36),$
$(153)(264), (165432)$
$(26)(35), (13)(46), (15)(24),$
$(14)(23)(56), (16)(25)(34),$
$(12)(36)(45) \}$

3)

Kongruenzen und Äquivalenzrelationen

Def. Sei $n \in \mathbb{N}$. Definiere die Relation $\equiv_n$ („Kongruenz modulo n") auf $\mathbb{Z}$ durch

$$a \equiv_n b \iff \underbrace{n \mid (b-a)}_{\uparrow\ \text{„teilt"}} \iff \exists k \in \mathbb{Z}: \ b - a = kn$$

ebenso übliche Notationen:

$$a \equiv_n b \iff a \equiv b \bmod n \iff a \equiv b \ (n)$$

Konvention: $a \equiv b \equiv c \equiv d \bmod n$ ist eine Kurzschreibweise für $a \equiv b \bmod n \wedge b \equiv c \bmod n \wedge c \equiv d \bmod n$

„$\cancel{7 \bmod 4 = 3}$" in der mathematischen Literatur unüblich h

ken

(n)

od n ∧

Literatur
üblich

bekannt: Die Relation $\equiv_n$ ist eine Äquivalenzrelation, d.h. sie ist reflexiv, symmetrisch und transitiv.

Ist X eine Menge, dann gibt es eine 1:1-Korrespondenz zwischen

(1) Äquivalenzrelationen auf X

(2) Zerlegungen der Menge X

Potenzmenge

(Def. Zerlegung von X = Teilmenge $Z \subseteq \mathcal{P}(X)$ wobei $\emptyset \notin Z$, $\bigcup_{A \in Z} A = X$, $\forall A, B \in Z$: $A \cap B \neq \emptyset \Rightarrow A = B$)

Beispiel für eine Zerlegung von $\{1,2,3,4,5,6\}$:

$$Z = \{\{1\},\{5\},\{2,3,4\},\{6\}\}$$

Erinnerung: (1) $\rightarrow$ (2) Def.: Ist $\equiv$ eine Äquivalenzrelation und $x \in X$, dann wird $[x] = \{y \in X \mid x \equiv y\}$ die Äquivalenzklasse von X genannt. Es ist dann $Z = \{[x] \mid x \in X\}$ eine Zerlegung der Menge X. überprüfe: $\forall A, B \in Z$:

$A \cap B \neq \emptyset \Rightarrow A = B$ Seien $A, B \in Z$. $\exists x, y \in X$ mit $A = [x]$, $B = [y]$. $A \cap B \neq \emptyset \Rightarrow \exists z \in X$ mit $z \in [x]$ und $z \in [y]$. Beh: $[x] = [z]$ „$\subseteq$" Sei $u \in [x]$.

$\Rightarrow x \equiv u$, $z \in [x] \Rightarrow x \equiv z$ Symmetrie $\Rightarrow z \equiv x$

$z \in [x]$ und $z \in [y]$. Beh: $[x] = [z]$ „$\subseteq$" Sei $u \in [x]$.

$\Rightarrow x \equiv u$, $z \in [x] \Rightarrow x \equiv z$ Symmetrie $\Rightarrow z \equiv x$

$z \equiv x,\ x \equiv u \xRightarrow{\text{Transitivität}} z \equiv u \Rightarrow u \in [z]$

„$\supseteq$" Sei $v \in [z] \Rightarrow z \equiv v$ $\quad x \equiv z,\ z \equiv v \Rightarrow x \equiv v \Rightarrow v \in [x]$

($\Rightarrow$ Beh.) Zeige genauso, dass aus $z \in [y]$ die Gleichung $[y] = [z]$ folgt. Insgesamt: $A = [x] = [z] = [y] = B$. $\square$

<u>Beispiel</u>: Die Relation $\equiv_3$ zerlegt die Menge $\mathbb{Z}$ in die drei Teilmengen $[0]_3 = 0 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$,

$[1]_3 = 1 + 3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$ und

$[2]_3 = 2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$

Menge der Äquivalenzklassen:

$$\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$$

ems

n von

n

$n=4$

$= 2+4\mathbb{Z}$

$-6 \equiv_4 2$

(2) $\Rightarrow$ (1): Ist Z eine Zerlegung von X, dann erhält man eine Äquivalenzrelation $\equiv_Z$ auf X durch $x \equiv_Z y \Leftrightarrow \exists A \in Z$ mit $x, y \in A$.

<u>bekannt</u>: Auf der Menge $\mathbb{Z}/n\mathbb{Z} = \{[x]_n \mid x \in \mathbb{Z}\}$ gibt es Verknüpfungen $+$ und $\cdot$ mit der Eigenschaft: $\forall a, b \in \mathbb{Z}$:

$$[a]_n + [b]_n = [a+b]_n, \quad [a]_n \cdot [b]_n = [ab]_n$$

<u>Erinnerung</u>: Ist X eine Menge und $\equiv$ eine Äquivalenzrelation, dann wird eine Teilmenge $R \subseteq X$ Repräsentantensystem der Äquivalenz-

D_5 mit einer Untergruppe von $\mathrm{Per}(E_5)$ identifizieren;
auf Grund der Bijektion $M_5 = \{1, \ldots, 5\} \to E_5,\ k \mapsto P_{5,k-1}$

klassen genannt, wenn jede Äquivalenzklasse genau ein Element aus R enthält.

Bsp.: $R_n = \{0, 1, \ldots, n-1\}$ ist ein Repräsentantensystem der Äquivalenzklassen von $\equiv_n$.

weiteres Beispiel: Betrachte auf $X = \mathbb{N} \times \mathbb{N}$ die Äquivalenzrelation $\sim$ geg. durch $(a, m) \sim (b, n) \iff a - m = b - n \iff a + n = b + m$. Ein Repräsentantensystem der Äquivalenzklassen ist geg. durch

$$R = \{(1,1)\} \cup \{(n+1, 1) \mid n \in \mathbb{N}\} \cup \{(1, n+1) \mid n \in \mathbb{N}\}$$

Bem: Mit Hilfe des Repräsentantensystems R_n können die Verknüpfungstafeln von $+$ und $\cdot$ auf $\mathbb{Z}/n\mathbb{Z}$ angeg. werden

$n=4$

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

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

$$\bar{2}\cdot\bar{3} = (2+4\mathbb{Z})\cdot(3+4\mathbb{Z}) = 6+4\mathbb{Z} \underset{6\equiv_4 2}{=} 2+4\mathbb{Z}$$

$$= \bar{2}$$