... Teilmenge $R \subseteq X$ mit der Eigenschaft, dass jede Äquivalenz-klasse genau ein Element aus R enthält.

Diedergruppen als Untergruppen der symmetrischen Gruppen S_n

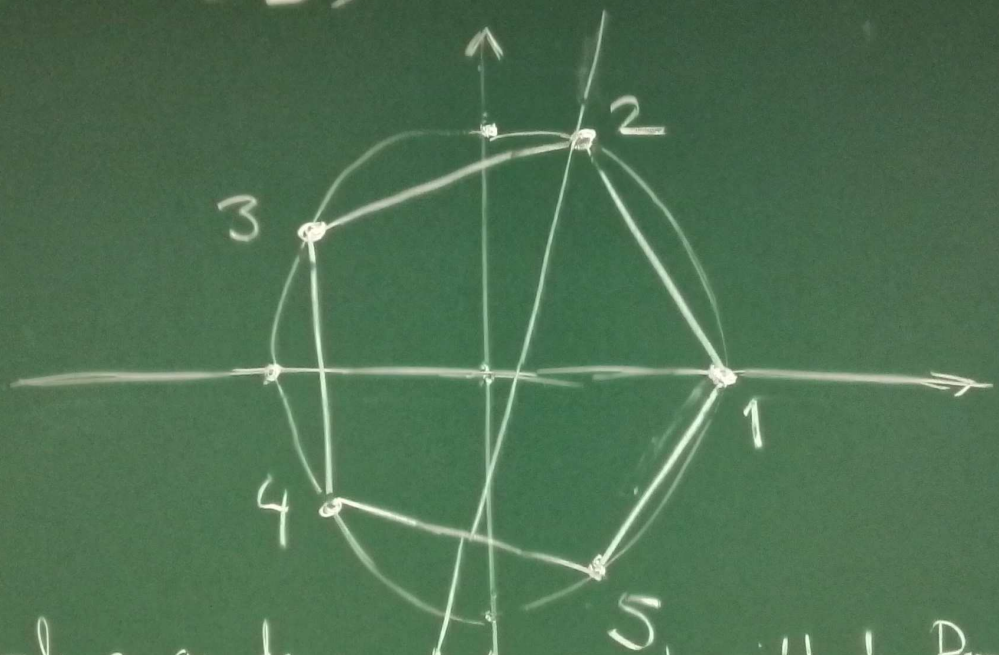
Tatsache. Jede Symmetrieoperation des regelm. n-Ecks ist eindeutig festgelegt durch die Permutation der Eckpunkte. Nummeriert man die Ecken mit den Zahlen von 1 bis n, dann kann auf diese Weise jeder Symmetrieoperation ein Element aus S_n zugeordnet werden.

- Die 72°-Drehung in positive Richtung (gegen den Uhrzeigersinn entspricht der Permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\,2\,3\,4\,5)$

weil die Ecken gemäß $1 \mapsto 2, 2 \mapsto 3, \ldots, 5 \mapsto 1$

abgebildet werden.

- Die 72°-Drehung in negativer Richtung entspricht $\sigma^{-1} = (1\ 5\ 4\ 3\ 2)$



- Die Spiegelung an der x-Achse entspricht der Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} = (2\ 5) \circ (3\ 4)$$

Elemente von D_5 insgesamt, aufgefasst als Elemente der symm. Gruppe S_5:

id , (1 2 3 4 5) , (1 3 5 2 4) , (1 4 2 5 3)

Identität — 72°-Drehung (pos.) — 144°-Drehung — 216°-Drehung = (−144°)-Drehung

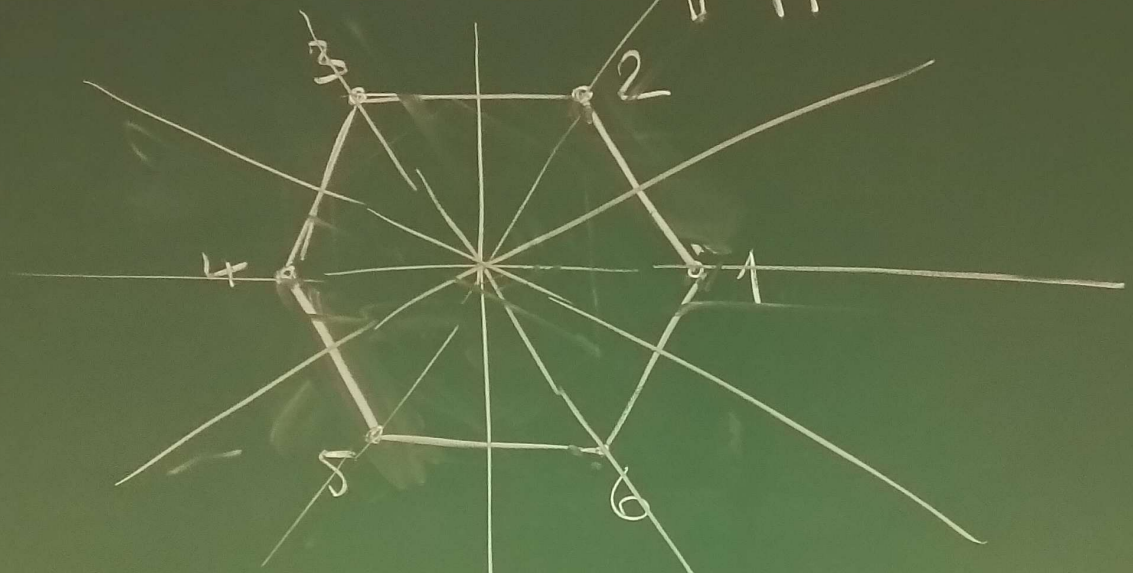
(1 5 4 3 2) , (2 5)(3 4) , (1 3)(4 5) , (2 4)(1 5)

288°-Drehung (= −72°-Drehung) — Spiegelung x-Achse — Achse durch 2 — Achse d. 3

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

Achse durch 4 — Achse durch 5.

Elemente der Diedergruppe D_6



Drehungen: id, (1 2 3 4 5 6),
(1 3 5)(2 4 6), (1 4)(2 5)(3 6),
(1 5 3)(2 6 4), (1 6 5 4 3 2)

Spiegelungen: (2 6)(3 5), (1 3)(4 6),
(1 5)(2 4), (1 2)(3 6)(4 5), (2 3)(1 4)(5 6), (1 6)(2 5)(3 4)

Geometrische Aussagen können rechnerisch überprüft werden, z.B. „Dreht man die 2 auf die 1, spiegelt man an der x-Achse und dreht anschließend zurück, dann hat man im Endeffekt an der Achse durch 2 gespiegelt."

$\underbrace{(12345)}_{\text{„zurückdrehen"}} \circ \underbrace{(25)\circ(34)}_{\text{Spiegelung an der x-Achse}} \circ \underbrace{(21543)}_{\text{„drehe die 2 auf die 1"}} =$

$(13)\circ(2)\circ(45) = (13)\circ(45)$

Wiederholung: Kongruenzen und Restklassenringe

Erinnerung: Definition der Kongruenzrelation $\equiv_n$ modulo n (für ein $n \in \mathbb{N}$)

$\equiv_n$ ist eine Relation auf $\mathbb{Z}$ definiert durch

$$a \equiv_n b \iff n \text{ teilt } b-a, \text{ d.h. } \forall a, b \in \mathbb{Z}$$
$$b - a = k \cdot n \text{ für ein } k \in \mathbb{Z}$$

Bsp.: $1 \equiv_3 4$, da 3 Teiler von $4-1$ ist

weitere Schreibweisen für $a \equiv_n b$:

$a \equiv b \bmod n$ oder $a \equiv b \,(n)$

Kongruenzen können (wie Gleichungen) verkettet

werden, d.h. $a \equiv b \equiv c \equiv \dots \equiv z \bmod n$ ist gleichbedeutend mit $a \equiv b \bmod n \wedge b \equiv c \bmod n \wedge c \equiv d \bmod n \wedge \dots \wedge y \equiv z \bmod n$

Erinnerung: $\equiv_n$ ist eine Äquivalenzrelation, d.h. sie hat die Eigenschaften (1) Reflexivität: $\forall a \in \mathbb{Z} : a \equiv_n a$

(2) Symmetrie: $\forall a, b \in \mathbb{Z} : a \equiv_n b \Rightarrow b \equiv_n a$

(3) Transitivität: $\forall a, b, c \in \mathbb{Z} : a \equiv_n b \wedge b \equiv_n c \Rightarrow a \equiv_n c$

(Bew: $a \equiv_n b \Rightarrow \exists k \in \mathbb{Z}$ mit $b - a = kn$

$b \equiv_n c \Rightarrow \exists l \in \mathbb{Z}$ mit $c - b = ln$

$c - a = (c - b) + (b - a) = ln - kn = (l - k)n \Rightarrow a \equiv_n c$)

Erinnerung: **Zerlegung** einer Menge X = System $\mathcal{Z} \subseteq \mathcal{P}(X)$ von Teilmengen von X mit den Eigenschaften (1) $\emptyset \notin \mathcal{Z}$

(2) $\bigcup_{A \in \mathcal{Z}} A = X$ (3) $\forall A, B \in \mathcal{Z}, A \neq B \Rightarrow A \cap B = \emptyset$

Bsp: $X = \{1, 2, \dots, 6\} \Rightarrow \mathcal{Z} = \{\{3,5\}, \{2,4,6\}, \{1\}\}$ ist eine Zerlegung von X

Def: Sei X eine Menge, $\equiv$ eine Äquivalenzrelation auf X und $x \in X$. Dann wird $[x] = \{y \in X \mid x \equiv y\}$ die Äquivalenzklasse von x genannt.

Bsp: Äquivalenzklasse von 2 bzgl $\equiv_7$

$[2]_7 = \{2 + 7k \mid k \in \mathbb{Z}\} = \{\dots, -19, -12, -5, 2, 9, 16, 23, \dots\}$

Satz: Ist X eine Menge, $\equiv$ eine Äquivalenzrelation und $Z = \{[x] \mid x \in X\}$, dann ist Z eine Zerlegung von X.

Beweis: durch Überprüfung der Bed. (1) bis (3) für die Zerlegung

zu (1) Für jedes $x \in X$ gilt $x \equiv x$ und somit $x \in [x]$.
$\rightarrow$ kein Element aus Z ist die leere Menge

zu (2) z.zg. $X = \bigcup_{A \in Z} A$ „$\supseteq$" klar, da $A \subseteq X \; \forall A \in Z$

„$\subseteq$" Sei $x \in X$. $\Rightarrow x \in [x] \Rightarrow$ Es gibt ein $A \in Z$ mit $x \in A$ (nämlich $A = [x]$).

zu (3) Es reicht zu zeigen:

$\forall A, B \in Z : A \cap B \neq \emptyset \Rightarrow A = B$

Seien $A, B \in Z$ mit $A \cap B \neq \emptyset$. $\Rightarrow \exists z \in A \cap B$

$A, B \in Z \Rightarrow \exists x, y \in X$ mit $A = [x]$ und $B = [y]$

Beh.: Es gilt $[x] = [z]$

$z \in A \Rightarrow z \in [x] \Rightarrow x \equiv z$

„$\supseteq$" Sei $u \in [z] \Rightarrow z \equiv u$

$x \equiv z, z \equiv u, \equiv$ transitiv $\Rightarrow x \equiv u$

$\Rightarrow u \in [x]$

„$\subseteq$" Sei $u \in [x]$. $\Rightarrow x \equiv u$ $x \equiv z \xrightarrow{\text{Symm.}} z \equiv x$

$z \equiv x, x \equiv u \xrightarrow{\text{Trans.}} z \equiv u \Rightarrow u \in [z]$

Ebenso folgt aus $z \in B$, dass $[z] = [y] = B$ gilt.

insgesamt also: $A = [x] = [z] = B$ □

Der Beweis zeigt, dass aus $z \in [x]$ jeweils die Übereinstimmung $[x] = [z]$ der Äquivalenzklassen folgt.

Angewendet auf die Relation $\equiv_7$ bedeutet das z. B.

$$[2]_7 = [9]_7 = [16]_7 = [-5]_7 = \dots$$

Def.: Sei X eine Menge, $\equiv$ eine Äquivalenzrelation auf X.
Ein Repräsentantensystem der Äquivalenzklassen von $\equiv$ ist eine Teilmenge $R \subseteq X$ mit der Eigenschaft, dass jede Äquivalenzklasse genau ein Element aus R enthält.

Teilmenge $R \subseteq X$ mit der Eigenschaft, dass jede Äquivalenzklasse genau ein Element aus R enthält.

bekannt: Für jedes $n \in \mathbb{N}$ ist $R_n = \{0, 1, \dots, n-1\}$ ein Repräsentantensystem der Äquivalenzklassen von $\equiv_n$.

Notation $\mathbb{Z}/n\mathbb{Z}$ = Menge der Äquivalenzklassen von $\equiv_n$

$$= \{[a]_n \mid a \in \mathbb{Z}\} = \{[a]_n \mid a \in M_n\}$$

$$= \{[a]_n \mid 0 \leq a < n\}$$

$$\mathbb{Z}/7\mathbb{Z} = \{[0]_7, [1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

Addition auf $\mathbb{Z}/n\mathbb{Z}$: $[a]_n + [b]_n = [a+b]_n \quad \forall a, b \in \mathbb{Z}$

Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$: $[a]_n \cdot [b]_n = [ab]_n \quad \forall a, b \in \mathbb{Z}$

$[4]_7 \cdot [5]_7 = [4 \cdot 5]_7 = [20]_7 = [6]_7$