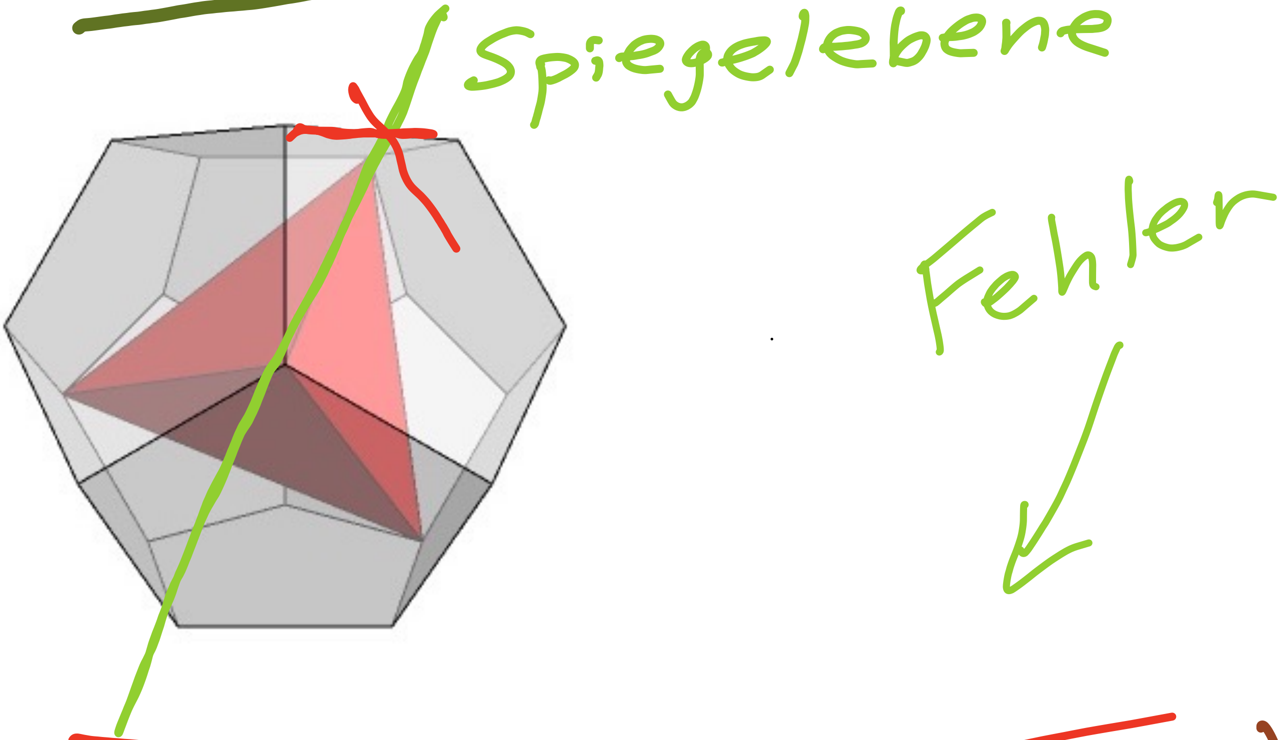
KORREKTUR



$$\cancel{\mathrm{Sym}(T) \subseteq \mathrm{Sym}(D)}$$

Nicht alle Symmetrien des Tetraeders erhalten das Dodekaeder. Oops!

Frage: Welche Symmetrien von T erhalten D?

Die optimale Antwort bekommen wir im Abschnitt 37.

Abschnitt 23

Zyklische Gruppen

Eine Gruppe G heisst **Zyklisch**, falls es ein $a \in G$ gibt, s.d. jedes Element von G die Form

$$a^j$$

hat, für ein $j \in \mathbb{Z}$.

a heisst **Erzeuger** oder **Generator** von G.

Sei $m \geq 1$.

1) Die Menge

$$\mathbb{Z}_m := \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$$

mit der Additionsregel

$$\overline{i} + \overline{j} = \begin{cases} \overline{i+j} & 0 \leq i+j < m \\ \overline{i+j-m} & m \leq i+j < 2m \end{cases}$$

ist eine endliche zyklische Gruppe. (Addition modulo m)

2) Eine zweite Darstellung ist

$$\mathbb{Z}_m' := \{1, \sigma, \sigma^2, \ldots, \sigma^{m-1}\}$$

mit der Regel $\sigma^m = 1$.

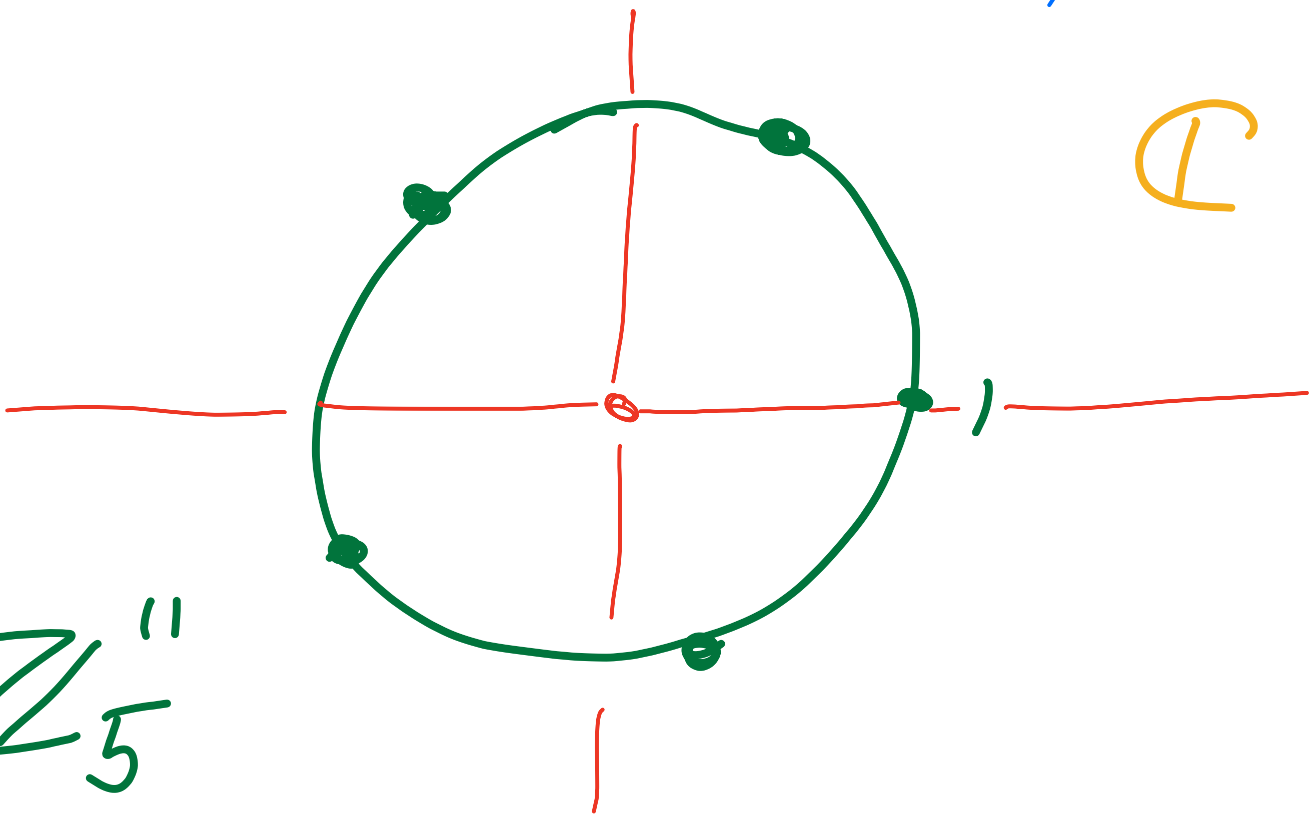
σ = Erzeuger

3) Eine dritte Realisierung ist

$$\mathbb{Z}_m'' := \{ z \in \mathbb{C} \mid z^m = 1 \}$$

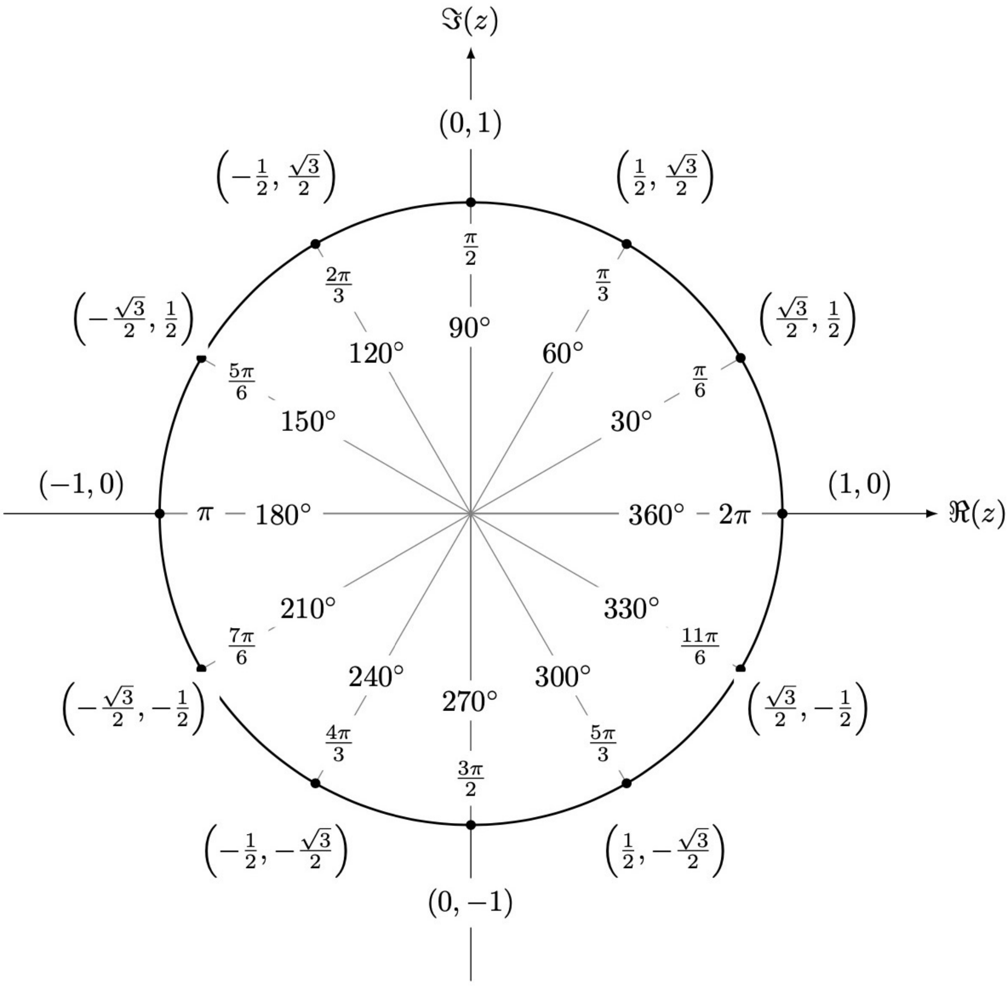
$$= \{ e^{2\pi i k/m} \mid k = 0, 1, 2, \ldots, m-1 \},$$

die m^{te} Würzeln von 1, mit komplexer Multiplikation.



$\mathbb{Z}_5''$

Eine zyklische Gruppe ist wie eine Uhr:



$$\mathbb{Z}_{12}'' \subseteq \mathbb{C}$$

Offensichtlich

$$\mathbb{Z}_m \cong \mathbb{Z}_m' \cong \mathbb{Z}_m''$$

endlich

$$\bar{k} \sim \sigma^k \sim e^{2\pi i k/m}$$

Die Gruppe

$$(\mathbb{Z}, +)$$

ist eine unendliche zyklische Gruppe.

Es gibt genau eine zyklische Gruppe von jeder Ordnung, bis auf Isomorphismus.

Man kann $\mathbb{Z}_m$ als Drehungen

$$C_m = \left\{ I, D_{\frac{2\pi}{m}}, D^2_{\frac{2\pi}{m}}, \dots, D^{m-1}_{\frac{2\pi}{m}} \right\}$$

$\mathbb{R}^2$ oder $\mathbb{R}^3$

realizieren. In dem Fall nennt man $\mathbb{Z}_m$ C_m.

Übung! Man findet eine Figur in $\mathbb{R}^3$, deren Symmetriegruppe C_m ist.

Übung 2

(a) Man findet zyklische Gruppen mit genau 1, 2 oder 4 Erzeuger

(b) Man zeigt, dass es keine zyklische Gruppe gibt mit genau 3 Erzeuger.

($\mathbb{Z}_3 = \{1, \sigma, \sigma^2\}$
hat Erzeuger σ, σ^2
genau 2 Erzeuger.)

Übung 3

$f: G \xrightarrow{\cong} G$

(a) Wieviel Automorphismen hat $\mathbb{Z}_4$? $\mathbb{Z}_5$? $\mathbb{Z}_{28}$?

(b) Man zeigt: Jeder Automorphismus von $\mathbb{Z}_m$ ist Multiplikation mit einer Ganzzahl.

Bsp $2: \mathbb{Z}_5 \to \mathbb{Z}_5$

$$\left.\begin{array}{l} \overline{0} \mapsto \overline{0} \\ \overline{1} \mapsto \overline{2} \\ \overline{2} \mapsto \overline{4} \\ \overline{3} \mapsto \overline{6} = \overline{1} \\ \overline{4} \mapsto \overline{8} = \overline{3} \end{array}\right\} \text{Selbstisomorphismus}$$

Abschnitt 24 Permutationen

X : eine Menge

Def Eine *Permutation* von X ist eine Bijektion

$$f : X \to X .$$

Die Menge aller Permutationen von X heisst

$$\mathrm{Perm}(X) := \{ f : X \to X \mid f \text{ bijektiv} \}$$

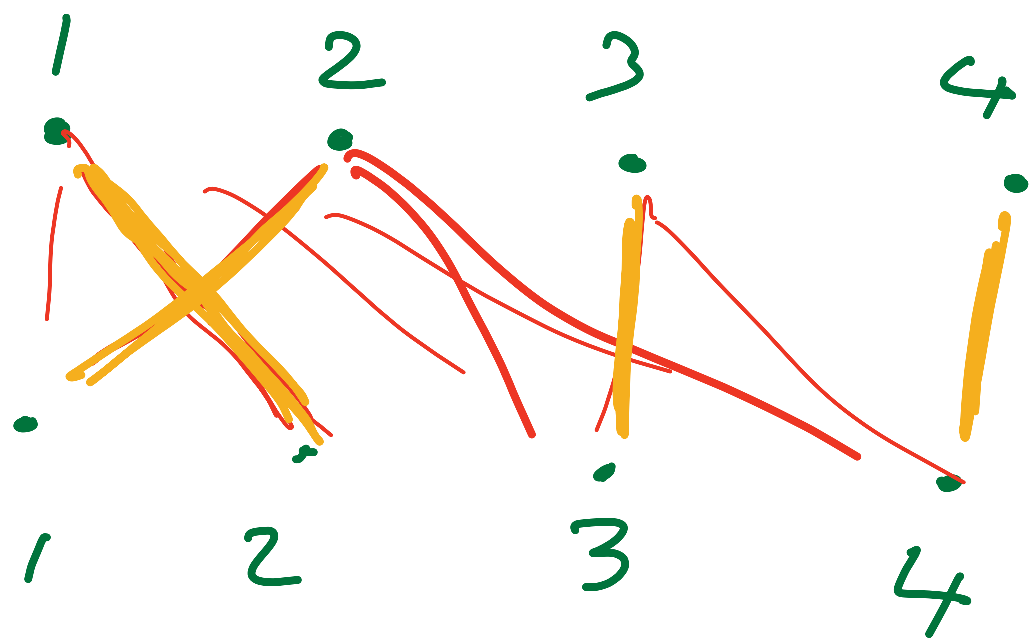
$\mathrm{Perm}(X)$ ist eine Gruppe mit $\circ$ (Hintereinanderschaltung).

Def Die symmetrische Gruppe von n Buchstaben ist

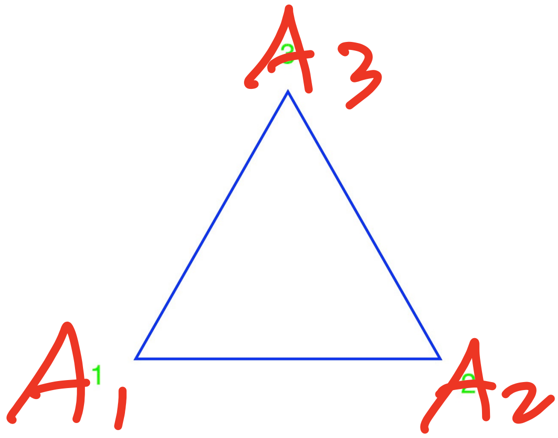
$$S_n := \mathrm{Perm}(\{1, 2, \dots, n\})$$

Die Ordnung von S_n ist

$$n! = \underline{n}\,\underline{(n-1)}\,\underline{(n-2)} \cdots \underline{2} \cdot \underline{1}$$

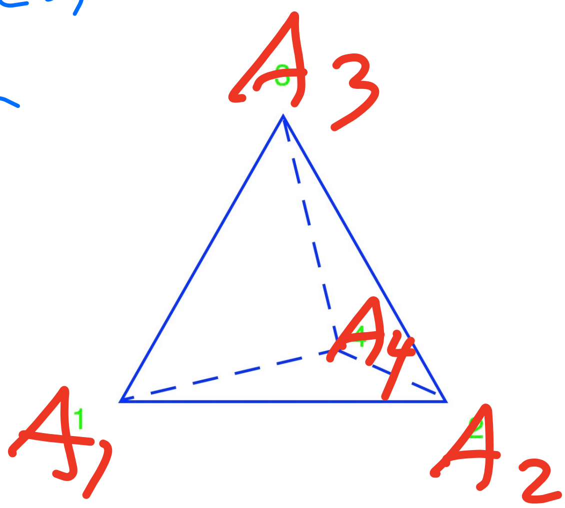


Wir haben schon gesehen, dass



$$\mathrm{Sym}(\Delta) \cong \mathrm{Perm}(\{A_1, A_2, A_3\}) \cong S_3$$

Mit einem ähnlichen Beweis, haben wir



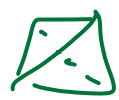
Aussage

$$\mathrm{Sym}(T) \cong S_4.$$

$\# S_3 = 3! = 6$

$\# S_4 = 4! = 24$

Die Verallgemeinerung von Δ und T ist der <u>n-Simplex</u> ($n+1$ Eckpunkte) Δ^n: Δ^n liegt in $\mathbb{R}^n$.
Jede Kante von Δ^n hat Lange 1. Man hat

$$\Delta^3 = T =$$ 

$$\Delta^2 = \Delta$$

$$\Delta^1 =$$  (Intervall)

$$\Delta^0 = \bullet$$

Δ^n in $\mathbb{R}^{n+1}$

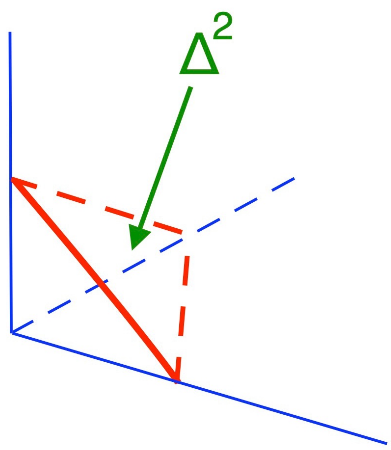
Man kann auch Δ^n in $\mathbb{R}^{n+1}$ realisieren. Man nimmt die Figur

$$\Delta^n := \{ (x_1, \dots, x_{n+1}) \in \mathbb{R}^{n+1} :$$

Ebene $x_1 + \dots + x_{n+1} = 1$

octant $x_1, \dots, x_{n+1} \geq 0 \}$

in $\mathbb{R}^{n+1}$.



$\subseteq \mathbb{R}^3$

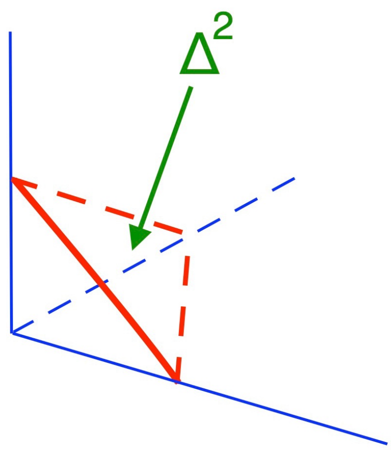
positive octant

Bei dieser Darstellung ist Δ^n der Schnitt der Hyperebene ← gleich $\mathbb{R}^n$

$$x_1 + \cdots + x_{n+1} = 1$$

in $\mathbb{R}^{n+1}$ mit dem positiven Orthant

$$x_1, \ldots, x_{n+1} \geq 0.$$



Übung Zeige

$$\mathrm{Sym}(\underbrace{\Delta^n}_{n\text{-Simplex}}) \cong S_{n+1}$$

Übung a) Wieviel Elemente hat

$$D_n = \mathrm{Sym}(\underbrace{P_n}_{\text{reguläres } n\text{-Eck in } \mathbb{R}^2}) \;?$$

b) Wieviel Permutation der Ecken von P_n gibt es?

c) Man schliesst, dass nicht jeder Permutation der Ecken von P_n durch eine Isometrie realisiert werden kann.

Abschnitt 25

Notation für Permutationen

Wir erklären mindestens 4 Notationen für Permutationen.

Betrachte das folgende Beispiel für $n=5$:

$$\sigma(1) = 2, \qquad \sigma(2) = 3, \qquad \sigma(3) = 1, \qquad \sigma(4) = 5, \qquad \sigma(5) = 4.$$

wobei $\sigma : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$

Man kann σ auf verschiedene Weisen darstellen.

$$\sigma(1) = 2, \qquad \sigma(2) = 3, \qquad \sigma(3) = 1, \qquad \sigma(4) = 5, \qquad \sigma(5) = 4.$$

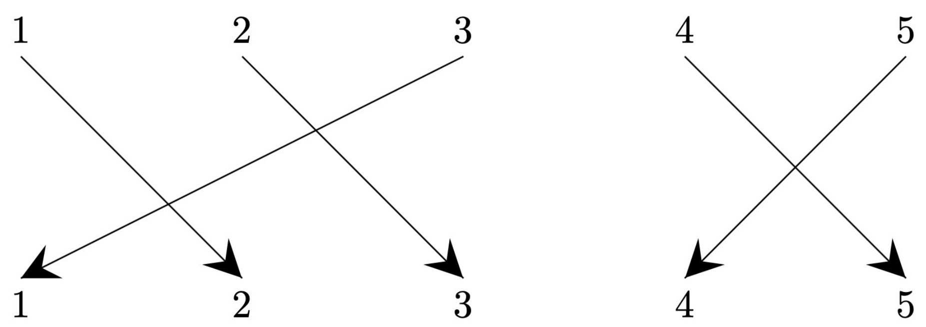
Zuerst eine Abbildungstafel:

k	1	2	3	4	5
$\sigma(k)$	2	3	1	5	4

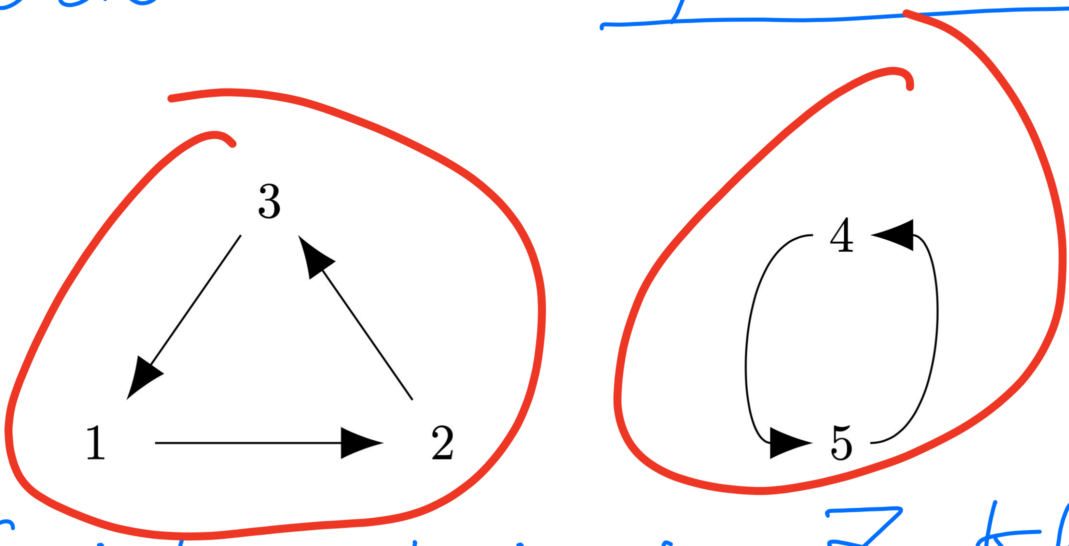
die man auch so schreiben kann:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Man kann σ kodieren durch ein Pfeilendiagramm:



oder ein Zyklendiagramm:



Schliesslich in Zyklen-Notation:

$$\sigma = (123)(45)$$

Def Sei $k \geq 0$.

Ein **k-Zyklus** ist eine Permutation

$$\sigma : X \to X,$$

die nur endlich viel Elemente

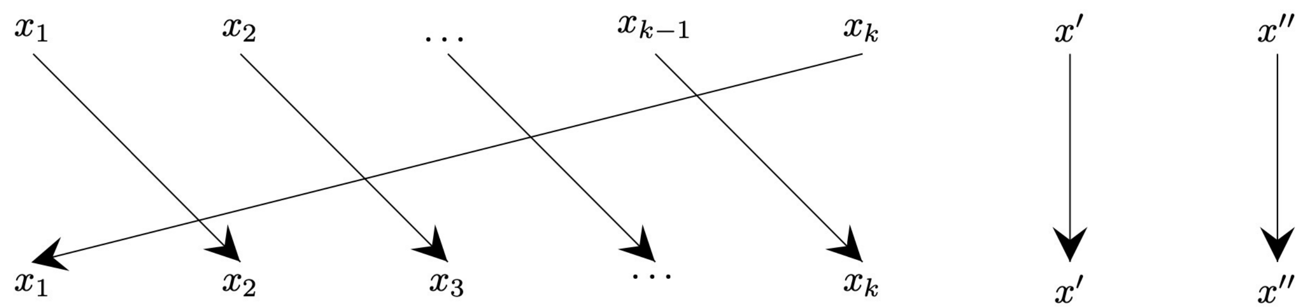
$$x_1, x_2, \dots, x_k$$

von X bewegt (wobei alle x_i verschieden sind), und diese **zyklisch permutiert**; d. h.

$$\sigma(x_i) = x_{i+1} \qquad i = 1, \dots, k-1$$

$$\sigma(x_k) = x_1$$

$$\sigma(x) = x \qquad x \notin \{x_1, \dots, x_k\}$$



Ein k-Zyklus

Ein 2-Zyklus nennt man eine <u>Vertauschung</u> oder <u>Transposition</u>.

1-Zyklen und 0-Zyklen sind einfach die Identitätspermutation.

---

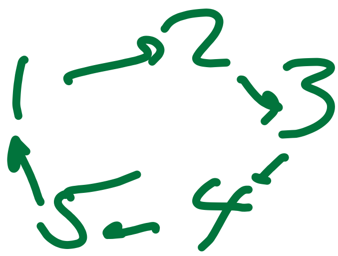
k-Zyklen bewegen k Elemente, mit Ausnahme 1-Zyklen, die 0 Elemente bewegen.

Man schreibt

$$\sigma = (x_1 x_2 \cdots x_k)$$

für ein k-Zyklus.

Die Einträge einer zyklischen Permutation können "zyklisch" permutiert werden, ohne die Permutation zu ändern:



$$(12345) = (23451)$$

$$\neq (12354)$$

Wenn man Zyklen verknüpft, man wendet die Permutationen von rechts nach links an, wie üblich bei Abbildungen.

Zum Beispiel

$$\sigma_3 = (1\,2\,3)$$

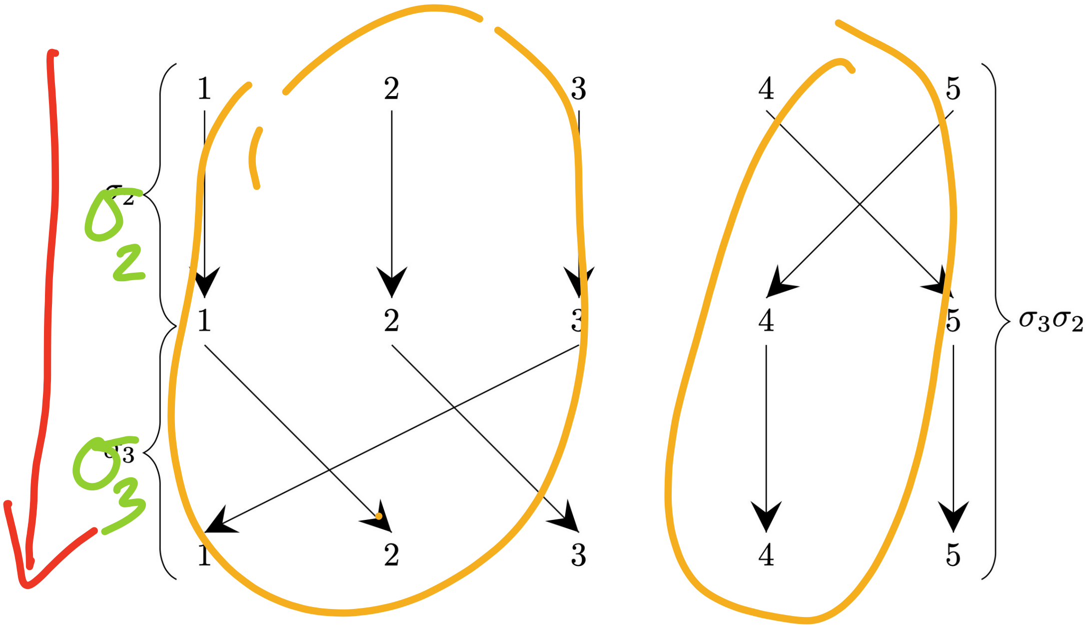
$$\sigma_2 = (4\,5)$$

$$\sigma_3 \sigma_2 = (1\,2\,3)(4\,5)$$

Zuerst σ_2

Dann σ_3

$\sigma_3 \sigma_2$



(45)

(123)

Def

(1) Seien $k, \ell \geq 2$. Die Zyklen

$$(x_1 \cdots x_k) \qquad (y_1 \cdots y_\ell)$$

heissen disjunkt, falls

$$\{x_1, \dots, x_k\} \cap \{y_1, \dots, y_\ell\} = \emptyset$$

(2) ~~1-Zyklen~~ und 0-Zyklen sind automatisch per Definition disjunkt von allen Zyklen.

Dann:

$$\boxed{\text{Disjunkte Zyklen kommutieren}}$$

z.B.

$$(123)(45) = (45)(123).$$

Das ist im Diagramm klar: Die Fäden gleiten aneinander vorbei.

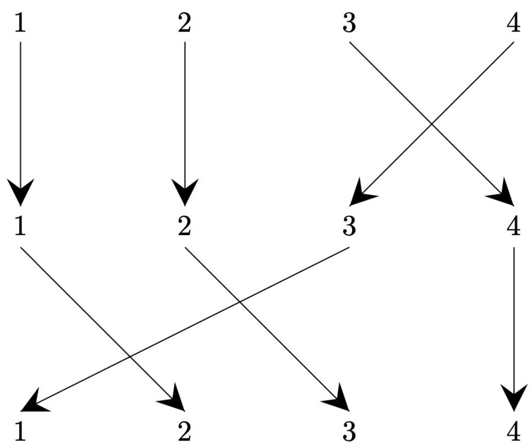
Aber nicht alle Permutationen kommutieren:

nicht disjunkt

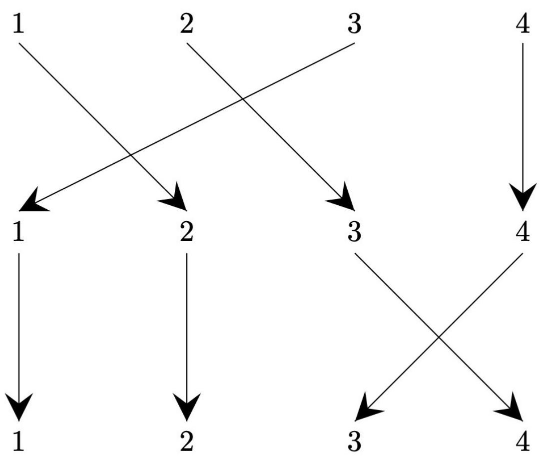
$$(123)(34) = (1234)$$

$$(34)(123) = (1243)$$

$$(123)(34) \neq (34)(123)$$



$= (123)(34) = (1234)$



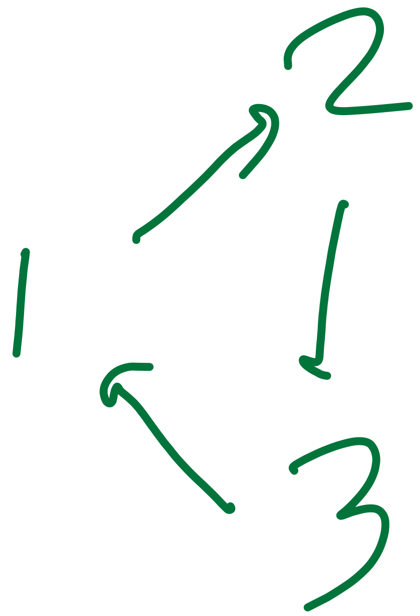
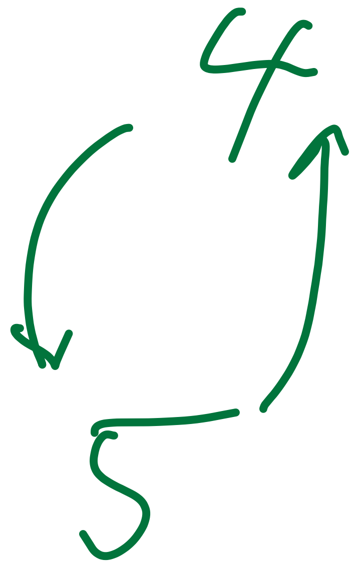
$= (34)(123) = (1243) \neq (1234)$

Satz Jede Permutation einer endlichen Menge kann als Produkt disjunkter Zyklen dargestellt werden.

Die Faktorisierung ist eindeutig bis auf die Reihenfolge der Faktoren, (solange keine 0-Zyklen und 1-Zyklen erscheinen).

Beweis: Man betrachtet das Zyklendiagramm und liest die disjunkten Zyklen ab.

QED


1
2
3

4
5

Konvention

Die 0- und 1-Zyklen sind sowieso die Identität und man lässt sie üblicherweise weg.

$$(123)(45)\cancel{(6)}\cancel{(7)}$$

$$= (123)(45)$$

Beispiel Die disjunkte Zyklen-Darstellung von

$$(123)(34) \quad ✗$$

ist

$$(1234) \quad ✓$$

(oben)

Abschnitt 26 Untergruppen

Def Sei G eine Gruppe.
Eine <u>Untergruppe</u> von G ist eine Teilmenge H von G, die mit den geerbten Operationen eine Gruppe ist.

Man schreibt

$$H \leq G$$

für eine Untergruppe.

Bsp $\{e_G\}$ und G sind stets Untergruppen von G.

Bsp Betrachte

$$D_3 = \{I, A, B, 1, 2, 3\}.$$

Man erkennt $\{I, A, B\}$ als Untergruppe, weil sie eine abgeschlossene 3×3 Untertafel von D_3 ist:

$\circ$	I	A	B	1	2	3
I	I	A	B	1	2	3
A	A	B	I	$\boxed{3}$	1	2
B	B	I	A	2	3	1
1	1	$\boxed{2}$	3	I	A	B
2	2	3	1	B	I	A
3	3	1	2	A	B	I

Hier sind all die Untergruppen von D_3:

$\{I\}$

$\{I, A, B, 1, 2, 3\}$

$\{I, A, B\}$

$\{I, 1\}$

$\{I, 2\}$

$\{I, 3\}$

Untergruppenverband:

heisst "$\subseteq$"

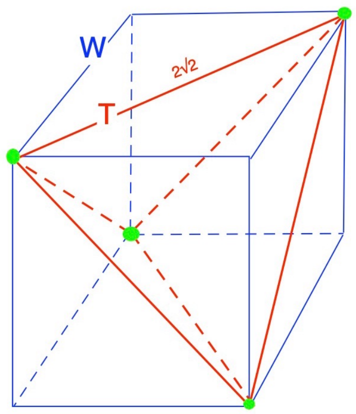
$$
\begin{tikzcd}
 & & D_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\{I,1\} \arrow[drr, dash] & \{I,2\} \arrow[dr, dash] & & \{I,3\} \arrow[dl, dash] & \{I,A,B\} \arrow[dll, dash] \\
 & & \{I\} & &
\end{tikzcd}
$$

Bsp

- $\mathbb{Q} \leq \mathbb{R}$ mit $+$
- $\mathbb{R}_+ \leq \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ mit $\cdot$
- $Sym_{\mathbb{R}^n}(F) \leq Isom(\mathbb{R}^n)$

Bsp Wir sehen, dass

$$Sym(T) \leq Sym(W)$$



Kriterium für eine Untergruppe

Wie kann man erkennen, das eine Teilmenge einer Gruppe eine Untergruppe ist?

<u>Def</u> Falls

$$a, b \in H \implies \begin{array}{l} ab \in H \\ a^{-1} \in H \end{array}$$

dann sagt man, H ist <u>abgeschlossen</u> <u>bezüglich</u> <u>Gruppenoperationen</u>.

oder einfach "abgeschlossen"

Bsp In D_3 ist die Teilmenge

$$\{I, A, B, 1\} \not\ni 3$$

nicht abgeschlossen bez. Gruppenoperationen, weil

$$A \circ 1 = 3.$$

Offensichtlich ist die Abgeschlossenheit eine notwendige Bedingung, um eine Untergruppe zu sein.

Nach der folgenden Aussage ist sie auch hinreichend.

<u>Aussage</u> Sei G eine Gruppe, H eine Teilmenge von G. Falls

- $H \neq \emptyset$
- H ist abgeschlossen bez. Gruppenoperationen,

so ist H eine Untergruppe mit der induzierten Multiplikation $\circ_H$.

Beweis Definiere

$$\circ_H := \circ_G\big|_{H\times H} : H\times H \to G$$

$$\mathrm{inv}_H := \mathrm{inv}_G\big|_H : H \to G$$

$$e_H := e_G .$$

wobei $\mathrm{inv}_G(a) = a^{-1}$ in G. Da H abgeschlossen ist, sind

$$\circ_H : H\times H \to H$$

$$\mathrm{inv}_H : H \to H$$

wohldefiniert.

Da $H \neq \emptyset$, gibt es $a \in H$ und

$$e_H = e_G = a^{-1} \circ a \in H.$$

Die Gruppenaxiome gelten dann automatisch für $(H, \circ_H)$ (verifiziere)

QED $\qquad inv_H, e_H$

Man schreibt

$$\circ = \circ_H$$

$$H = (H, \circ)$$

Aussage Seien H und K Untergruppen von G. Dann ist auch $H \cap K$ eine Untergruppe von G.

Beweis $H \cap K$ enthält e_G, also nicht leer ist. Da H und K abgeschlossen sind, ist auch $H \cap K$ abgeschlossen. Also $H \cap K$ ist eine Untergruppe von G. QED

Eine analoge Aussage gilt auch für beliebige Durchschnitte

$$\bigcap_{\alpha \in A} H_\alpha$$

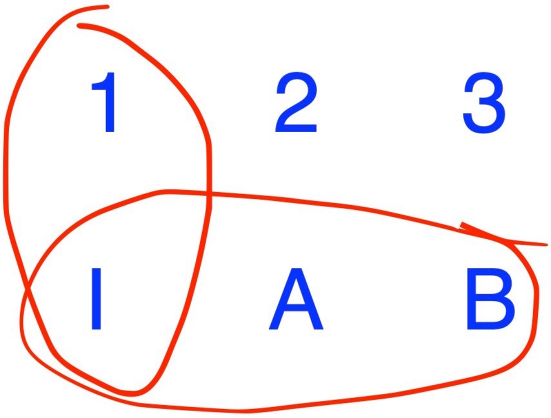
von Untergruppen H_α.

$$H_\alpha, \quad \alpha \in \overbrace{A}^{\text{Indexmenge}}$$

indizierte Familie von Untergruppen von G.

Die Vereinigung von Untergruppen muss nicht eine Untergruppe sein:

D_3:



$H = \{I, A, B\}$

$K = \{I, 1\}$

$H \cup K$ $\Rightarrow$ keine Untergruppe

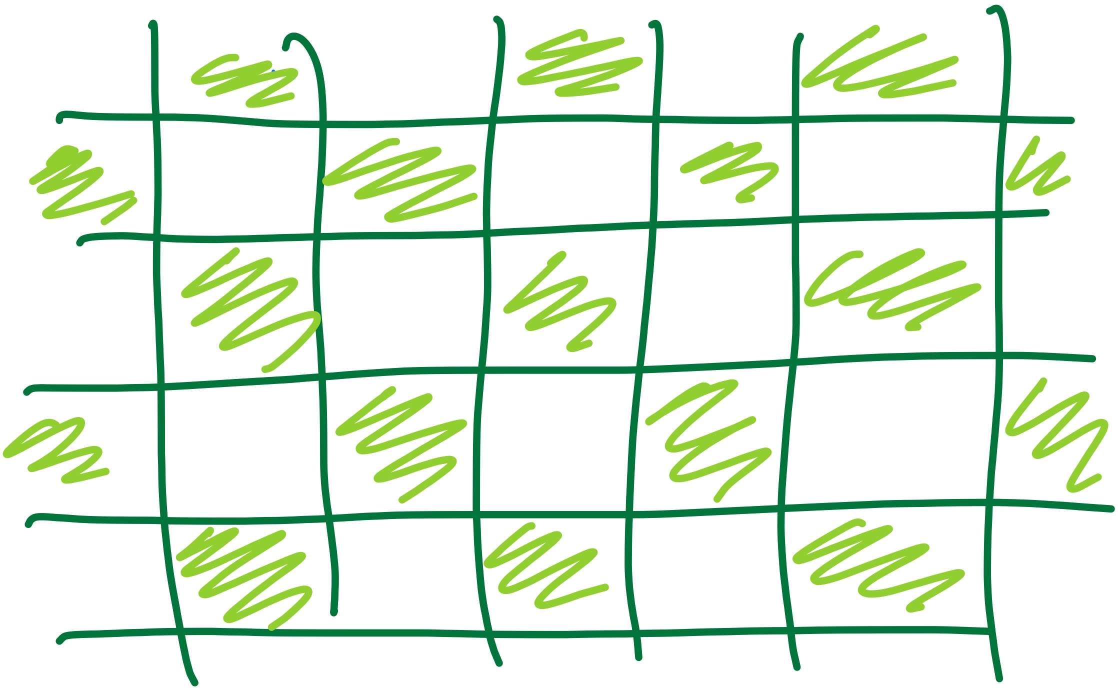
ist nicht abgeschlossen bez. Multiplikation.

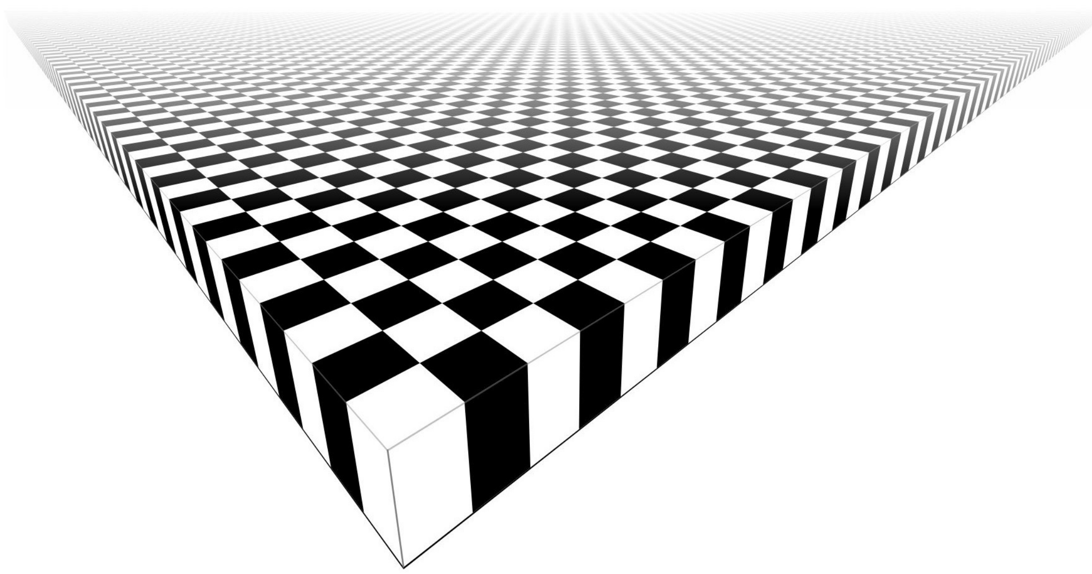
Die kleinste Untergruppe, die $H \cup K$ enthält, ist D_3

Übung Die Vereinigung $H \cup K$ von Untergruppen H und K ist nie eine Untergruppe, ausser $H \subseteq K$ oder $K \subseteq H$.

Schachbrett

Man betrachtet das unendliche Schachbrett





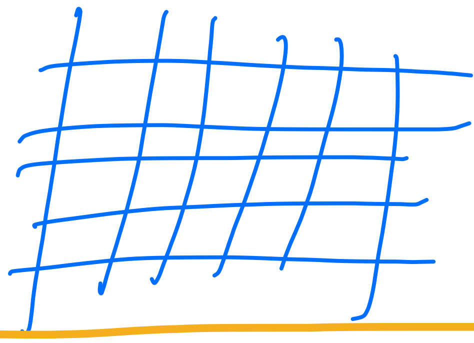
Übung

(a) Man zeigt, dass

Sym(Schachbrett)

eine Untergruppe von

Sym(Gitter) ist.

Gitter:  (ohne Farben)

(b) Sind diese beiden Gruppen isomorph?

Abschnitt 27

Erzeugende Systeme

Def Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Die Untergruppe von G erzeugt von S, geschrieben

$$\langle S \rangle,$$

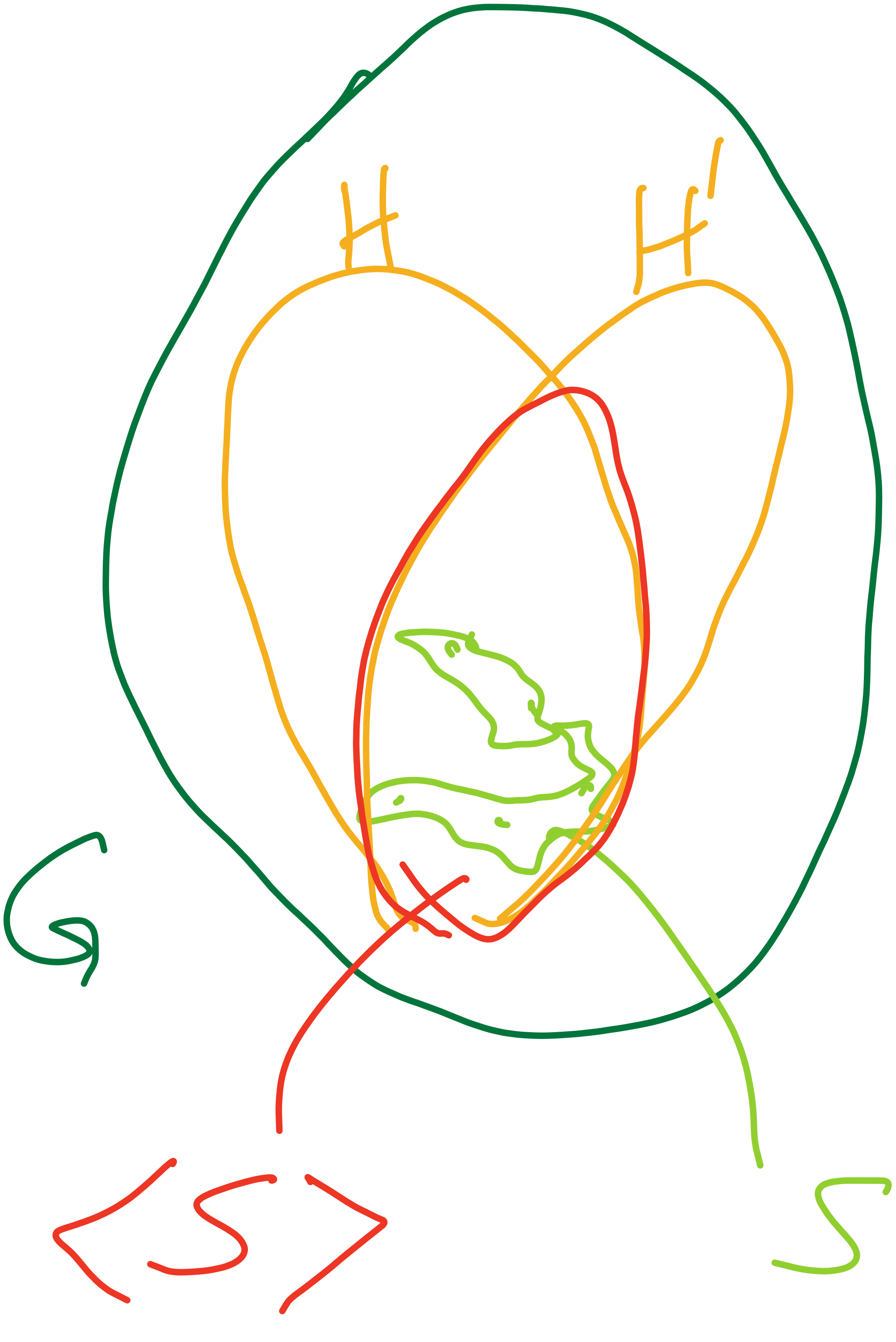
ist die kleinste Untergruppe von G, die S enthält.

Man nennt S ein <u>erzeugendes System</u> <u>von H_0</u> $= \langle S \rangle$

Wie kann man sicher sein, dass so eine "kleinste" Untergruppe existiert?

Man kann $\langle S \rangle$ konstruieren, als

$$S = \bigcap \{ H \mid H \supseteq S, \; H \leq G \}$$


G
H
H'
⟨S⟩
S

$$\langle S \rangle = \bigcap \underbrace{\{H \mid H \supseteq S,\ H \le G\}}$$

1) Das ist eine Untergruppe von G

2) Das enthält S

3) Das ist enthalten in jeder Untergruppe von G, die S enthält.

$\Longrightarrow$ Die RHS ist doch die "kleinste Untergruppe von G, die S enthält".
Das ist $\langle S \rangle$. QED.