Abschnitt 27 Erzeugende Systeme

fort.

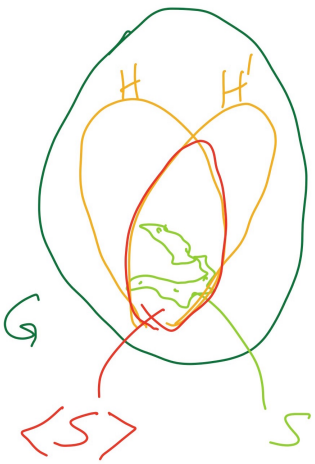
Erinnerung: G eine Gruppe

S = erzeugendes System

= Teilmenge von G

$\langle S \rangle :=$ kleinste Untergruppe von G die S enthält

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



Bsp $D_3 = \{I, A, B, 1, 2, 3\}$
ist durch die Teilmenge

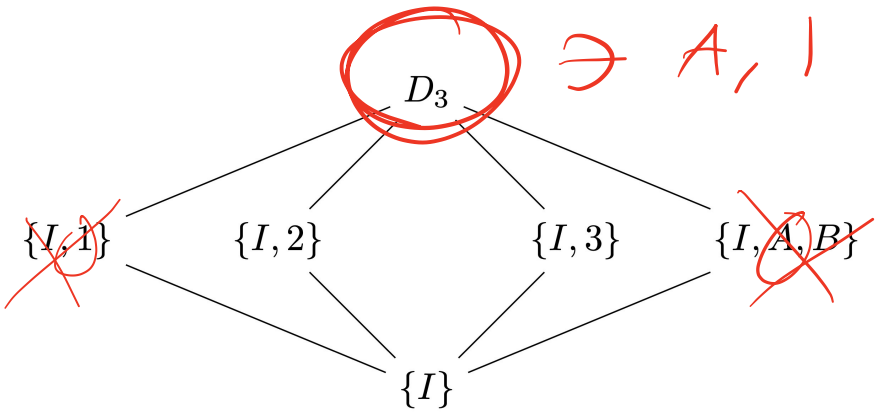
$$S = \{A, 1\}$$

erzeugt, weil $\langle S \rangle = \langle \{A, 1\} \rangle$
ist gezwungen,

$$B = A^2$$
$$2 = 1A$$
$$3 = A1$$
$$I = AA^{-1}$$

zu enthalten.

Oder betrachte:



$\ni A, 1$

Alternative Konstruktion von $\langle S \rangle$

Man kann $\langle S \rangle$ "von innen" aufbauen. $\langle S \rangle$ ist die Menge aller Produkten von positiven und negativen Elementen von S:

Potenzen von

$$S = \{ g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} \mid k \geq 0, \quad g_1, \ldots, g_k \in S, \quad \varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\} \}$$

RHS

Das Produkt ist I, falls $k = 0$ (per Konvention).

Beweis: 1) Die RHS ist nicht leer und abgeschlossen bez. Gruppenoperationen. Also sie ist eine Untergruppe. 2) Sie enthält S. 3) Alle Elemente von ihr sind

notwendig. Also ist sie (die RHS) in jeder Gruppe enthalten, die S enthält. QED

Notation Man schreibt

$$\langle x_1, \dots, x_n \rangle$$

für

$$\langle \{x_1, \dots, x_n\} \rangle.$$

Man nennt $x_1, \dots, x_n$ **Erzeuger** von $H = \langle x_1, \dots, x_n \rangle$.

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

$$\langle A, 1 \rangle = \{I, A, A^{-1}, 1, 1^{-1}, AA, AA^{-1}, A1, A1^{-1}, A^{-1}A, A^{-1}A^{-1}, A^{-1}1, A^{-1}1^{-1}, \dots\}$$

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

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

$$= D_3. \;//$$

Bsp S_5 ist durch die 4 Vertauschungen

$(12), (23), (34), (45)$

erzeugt.

$$(12)(23) = (312)$$

usw.

Bsp (Zyklische Gruppen)

1) $\mathbb{Z}_n = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ $\sigma^n = 1$

ist durch σ erzeugt:

$$\mathbb{Z}_n = \langle \sigma \rangle$$

2) $\mathbb{Z} = \langle 1 \rangle$ $(\mathbb{Z}, +)$

3) G eine Gruppe, $g \in G$

$\Rightarrow \langle g \rangle$ ist stets zyklisch

4) $\underline{\text{ord}(g)} = \underline{\text{ordnung}(\langle g \rangle)}$

Übung / Welche Elemente von $\mathbb{Z}_n$ erzeugen $\mathbb{Z}_n$?

Bsp $\mathbb{Z}_3$ ist erzeugt von σ, σ^2
$= \{1, \sigma, \sigma^2\}$, $\sigma^3 = 1$

$\mathbb{Z}_4$ ist nicht von τ^2 erzeugt
$\{1, \tau, \tau^2, \tau^3\}$

Übung 2 Zeige:

1) D_n kann nicht von einem Elementen erzeugt werden

2) D_n kann von 2 Spiegelungen erzeugt werden

3) D_n kann von 1 Spiegelung und 1 Drehung erzeugt werden.

$$D_3 = \langle A, I \rangle$$

Drehung, Spiegelung

Übung 3 Mit wie wenig Elementen kann man Sym(W) erzeugen? Sym(I)?

2 ??

Poll: Braucht man mehr als ~~fünf~~ zwei Elemente, um Sym(I) zu erzeugen?

Abschnitt 28 Nebenklassen

G : Gruppe

H : Untergruppe von G

Def 1) Die Mengen

$$gH = \{gh \mid h \in H\}, \quad g \in G,$$

heissen Linksklassen von H in G.

2) Die Mengen

$$Hg = \{hg \mid h \in H\}, \quad g \in G,$$

heissen Rechtsklassen von H in G.

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

$H = \{I, 1\}$

Linksklassen:

$IH, AH, BH, 1H, 2H, 3H$

Man erinnert sich:

$A^2 = B, \; B^2 = A, \; A^3 = B^3 = I$

$1^2 = 2^2 = 3^2 = I$

$12 = 23 = 31 = A, \; 21 = 32 = 13 = B,$

$1A = B1 = 2, \; 2A = B2 = 3, \; 3A = B3 = 1$

$A1 = 1B = 3, \; A2 = 2B = 1, \; A3 = 3B = 2$

Man bekommt (von oben)

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

oder

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

Rechtsklassen:

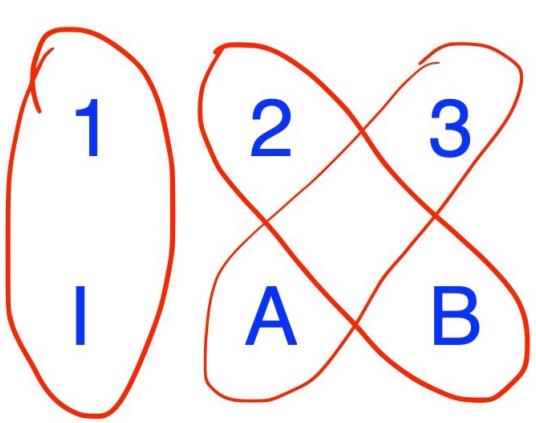
$HI, HA, HB, H1, H2, H3$

oder

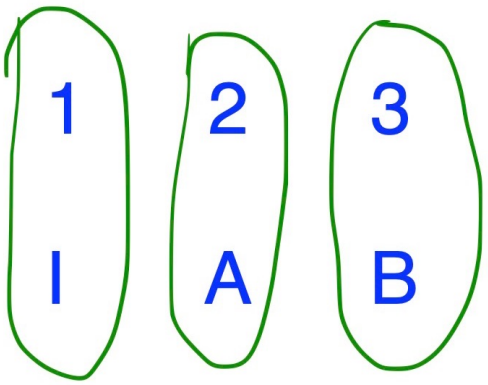
$\{I, 1\}, \{A, 2\}, \{B, 3\}, \{1, I\}, \{2, A\}, \{3, B\}$

oder

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



Links



Rechts

Man merkt in diesem Beispiel:

1) 6 Ausdrücke
   → 3 Linksklassen
   3 Rechtsklassen
   Anzahl gleich

2) Die Nebenklassen sind disjunkt und decken G
   Zerlegung oder Partition von G

3) $gH \neq Hg$ (meistens)

4) Die Menge aller Linksklassen und die Menge aller Rechtsklassen unterscheiden sich.

~~(folgt aus (3))~~

Ganz anders:

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

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

Linksklassen

$IK, AK, BK, 1K, 2K, 3K$

oder

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

$\{1, 2, 3\}, \{1, 2, 3\}, \{1, 2, 3\}$

oder

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

Rechtskassen:

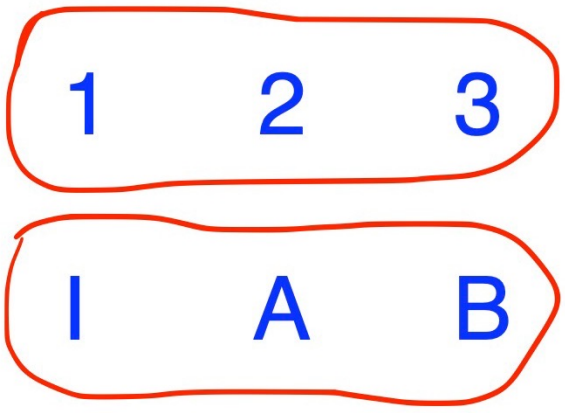
$K_I, K_A, K_B, K_1, K_2, K_3$

oder

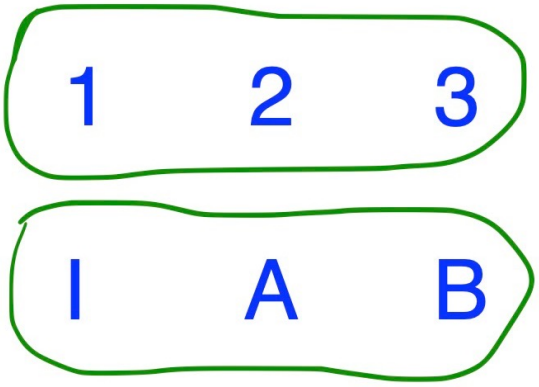
$\{I, A, B\}, \{I, A, B\}, \{I, A, B\},$
$\{1, 2, 3\}, \{1, 2, 3\}, \{1, 2, 3\}$

oder

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



Links



Rechts

Man merkt bei diesem Beispiel:

1) 6 Ausdrücke

→ 2 Linksklassen (gleiche Anzahl)
2 Rechtsklassen

2) Die Nebenklassen sind disjunkt und decken G

3) $\boxed{gk = kg}$ (immer) $\forall g \in G$

4) Die Menge aller Linksklassen ist gleich der Menge aller Rechtsklassen. (Folgt aus (3))

Eine Untergruppe mit Eigenschaft 3) heisst normal. Mehr dazu später.

Abschnitt 29 Teilbarkeit der Ordnung

G : Gruppe

H : Untergruppe

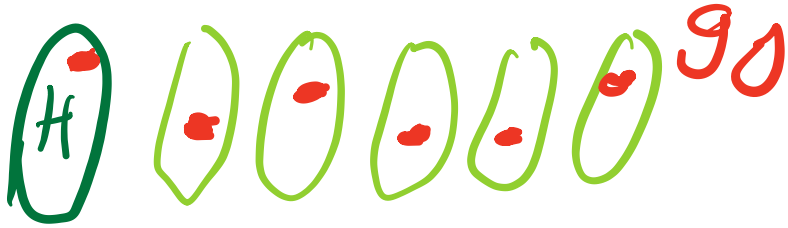
$\#H \mid \#G$ falls G endlich

später

Def Eine Menge

$g_1, g_2, \ldots \in G$

heisst Vertretersystem von den Linksklassen von H, falls jede Linksklasse genau ein g_j enthält.



Satz (Nebenklassensatz)

G Gruppe, H Untergruppe

a) Die Linksklassen von H in G haben alle die gleiche Grösse ✓

b) Die Linksklassen von H in G bilden eine Zerlegung von G (mit Wiederholungen).

D.h. die decken G, und die sind entweder disjunkt oder identisch.

Also $gH = g'H \overset{\circ}{\underset{r}{g}} gH \cap g'H = \emptyset$

$$G = \coprod_{i \in J} g_i H$$

ist eine echte Zerlegung,

wobei $\dot\cup$ heisst eine disjunkte Vereinigung und $(g_i)_{i\in J}$ ein Vertretersystem für die Linksklassen von H in G ist. Beweis später

---

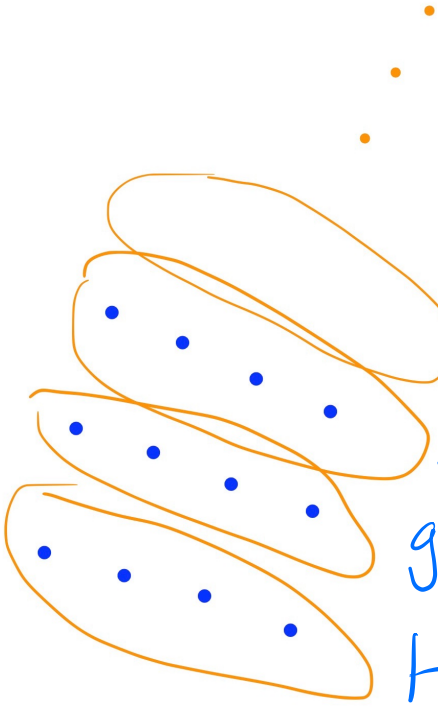
Folgen:

Folge1 (Lagrangscher Satz)

Sei G endlich. Dann

$$\#H \mid \#G.$$

Beweis Die Nebenklassen sind all der gleichen Grösse und zerlegen G. QED



$g'H = g_3H$
$gH = g_2H$
$H = g_1H$

All der gleichen Grösse

Folge 2 Die Anzahl Linksklassen und die Anzahl Rechtsklassen sind gleich.

Beweis Falls G endlich ist, haben wir

$$\#LK = \frac{\#G}{\#H} = \#RH$$

Für alle Fälle (auch unendlich):

$\boxed{X \subseteq G}$

Die Funktion

$$X \longmapsto X^{-1} := \{g^{-1} \mid g \in X\}$$

nimmt Linksklassen zu Rechtsklassen und umgekehrt:

$$gH \mapsto (gH)^{-1} = H^{-1}g^{-1}$$
$$= Hg^{-1}$$

$$Hg \mapsto (Hg)^{-1} = g^{-1}H^{-1}$$
$$= g^{-1}H$$

Diese Funktion ist bijektiv. QED.

Def Der **Index** von H in G ist die Anzahl Linksklassen (oder Rechtsklassen) von H in G.

Man schreibt

$$[G:H]$$

dafür. Falls G endlich ist, hat man

$$[G:H] = \frac{\#G}{\#H}$$

Bsp

- $\{I, A, B\}$ hat Index 2 in D_3.

$$2 = 6/3.$$

- $\{I, 1\}$ hat Index 3 in D_3

$$3 = 6/2.$$

- $n \in \mathbb{Z} \quad n \neq 0$

$\langle n \rangle \leq \mathbb{Z}$, $\langle n \rangle = n\mathbb{Z}$

$\langle n \rangle = \{\ldots, -n, 0, n, 2n, \ldots\}$

$\langle n \rangle$ hat Index n in $\mathbb{Z}$

Nebenklassen:

$\langle n \rangle$, $1+\langle n \rangle$, ..., $n-1+\langle n \rangle$

$\|$ $\|$ $\|$

$n\mathbb{Z}$ $1+n\mathbb{Z}$ $n-1+n\mathbb{Z}$

- $H = \langle 0 \rangle = \{0\} \leq \mathbb{Z}$

  $G = \mathbb{Z}$

Der Index von $\{0\}$ in $\mathbb{Z}$ ist ∞.

Nebenklassen sind

..., $\{-1\}$, $\{0\}$, $\{1\}$, $\{2\}$, ...

Folge 3 Die Ordnung eines Elementen von G teilt die Ordnung von G.:

$$ord(g) \mid \#G.$$

(falls G endlich ist)

Beweis

$$ord(g) = ordnung(\langle g \rangle)$$

$$\mid \#G$$

Frage: Ist die Umkehraussage gültig? D.h., falls $m \mid \#G$, gibt es ein Element von G der Ordnung m?

Abschnitt 30 Beweis des Nebenklassensatzes

Def 1) Sei G eine Gruppe, $g \in G$. Man definiert eine Operation

$$L_g : G \to G, \quad h \mapsto gh$$

Das heisst Linksmultiplikation durch g.

2) Auf ähnlicher Weise, haben wir Rechtsmultiplikation

$$R_g : G \to G, \quad h \mapsto hg.$$

Beobachtung:

$L_g : G \to G$

$R_g : G \to G$

sind beide **bijektiv** & Exist. der Inversen

(durch die Kürzungsregel)

$$L_g h = L_g h'$$

$$gh = gh'$$

$$h = h'$$

injektiv

$$L_g h = k$$

surjektiv $gh = k$

$h = g^{-1}k \overset{L_g}{\mapsto} k$

Beweis des Nebenklassensatzes

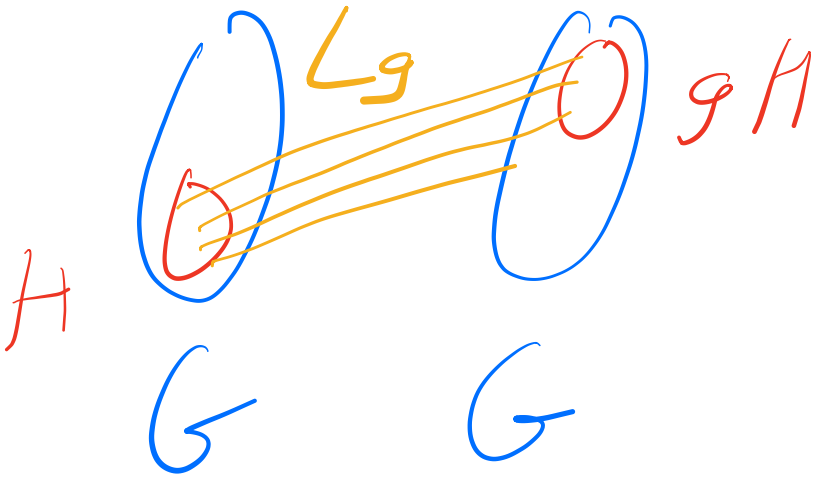
1. Sei G Gruppe, $H \leq G$.

Dann ist

$$gH = L_g(H)$$

ein bijektives Bild von H

weil L_g bijektiv ist.



L_g hat inverse $L_{g^{-1}}$

$$L_{g^{-1}} \circ L_g = L_{g^{-1}g}$$
$$= L_{;d} = id$$

Also

$$\#H = \#(gH)$$

Alle Linksklassen von H in G haben die gleiche Grösse.

---

2. Zu zeigen:
Linksklassen von H entweder disjunkt sind oder übereinstimmen.

Seien sH und tH Linksklassen.

Nehme an, dass sH und tH nicht disjunkt sind. Wir wollen zeigen, dass $sH = tH$.

Sei $k \in sH \cap tH$.

Dann

$$k = sh_1 = th_2$$

für ein $h_1 \in H$

$h_2 \in H$.

$$sh_1 = th_2$$

$$t^{-1}s = h_2 h_1^{-1} \in H$$

$$t^{-1}sH \subseteq H$$

$$\epsilon\epsilon^{-1}sH \subseteq \epsilon H$$

$$sH \subseteq \epsilon H$$

Auf gleicher Weise

$$\epsilon H \subseteq sH$$

d.h.

$$sH = \epsilon H$$

wie versprochen!

3. Wir müssen zeigen:

$$G = \bigcup_{g \in G} gH$$

(die gH'en decken G).

Sei $g \in G$ $\quad 1 \in H$

$$g = g \cdot 1 \in gH$$

d.h.

$$g \in \bigcup_{g' \in G} g'H$$

d.h.

$$G \subseteq \bigcup_{g' \in G} g'H \subseteq G$$

$$G = \bigcup_{g' \in G} g'H.$$

QED Satz

Bemerkung

Der Beweis zeigt

$$sH = tH$$

$$\Longleftrightarrow$$

$$t^{-1}s \in H$$

Man schreibt

$$s \underset{L}{\sim} t$$

(links-äquivalent mod H)

für diese Relation.

Es ist nicht schwierig zu sehen, dass

$\sim_L$

eine Äquivalenzrelation ist, und die Äquivalenzklassen davon sind genau die Linksklassen von H in G.