Noch zu A2: G Gruppe

Hatten: • $H \leq G \Leftrightarrow H \neq \emptyset \wedge (\forall a, b \in H: ab^{-1} \in H)$

(H ist UG von G)

• UG von $\mathbb{Z}$: $n\mathbb{Z}$, $n \in \mathbb{N}_0$

• $Z(G) = \{a;\ \forall b \in G: \underbrace{ab = ba}_{\text{"a komm. mit b"}}\}$ Zentrum von G

• $S \subseteq G \rightsquigarrow \langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H = \{ s_1^{\varepsilon_1} \cdot \ldots \cdot s_n^{\varepsilon_n};\ n \in \mathbb{N}_0,\ \varepsilon_i \in \{\pm 1\}\}$ die von S erz. UG in G

• $a \in G \rightsquigarrow \langle a \rangle = \langle \{a\} \rangle = \{a^0 = e, a^1 = a, a^2, a^3, \ldots\}$

• G zyklisch $:\Leftrightarrow \exists a \in G: \langle a \rangle = G$

a heißt Erzeuger

• Situation: Gr. G, $H \leq G$

$a \underset{l}{\sim} b :\Leftrightarrow b \in aH \Leftrightarrow a^{-1}b \in H$

Ä-Kl. bzgl. $\underset{l}{\sim}$, heißen Linksnebenklasse

$aH = \{a \cdot b;\ b \in H\}$

⌈Bsp.: $\mathbb{Z}$, $H = n\mathbb{Z} \rightsquigarrow \underbrace{100}_{a=100} \cdot H = 100 \cdot n\mathbb{Z} = \{100nm;\ m \in \mathbb{Z}\}$ ⌋

2.16. Def.: $G/H := \{aH;\ a \in G\}$ Faktormenge

$[G:H] := \# G/H$ Index von H in G

2.17. Satz: $\#G$ endl. $\Rightarrow \#G = \#H \cdot [G:H]$. (Satz von Lagrange)

$\#G = q \cdot \#H$ $\qquad [G:H] = \dfrac{\#G}{\#H}$

Bew.: Nach 2.15: Ä-Klassen bzgl. $\underset{l}{\sim}$ sind genau die Linksnebenklassen.

Sei $a_1, \ldots, a_q$ ein Repräsentantensystem für die die Linksnebenkl., $eH = H$

also $G = a_1 H \,\dot\cup\, a_2 H \,\dot\cup \ldots \dot\cup\, a_q H$

a_1H | a_2H | ... | a_iH e | ... | a_qH G

Bet. $\varphi: H \twoheadrightarrow aH$, $h \mapsto a \cdot h$: ist inj., denn $ah_1 = ah_2$ (surj.)

$\Rightarrow h_1 = h_2$. Also φ bij. Daher haben alle Linksn.kl. gleichviele El. $= \#H$. □

2.18. **Kor.:** G endl. Gr. $\Rightarrow \operatorname{ord}(a) \mid \# G$ (bel. $a \in G$) [Ordn. eines El. a teilt die Gr.ordnung]

Bew.: $\operatorname{ord}(a) = \# \langle a \rangle \mid \# G$ nach 2.17. $\square$

2.19. **Kor.:** G endl. Gr., $\# G = p$ prim $\Rightarrow G = \langle a \rangle$ mit bel. $a \neq e$, d.h. zyklisch.

Bew.: $e \subsetneq \langle a \rangle \subseteq G$

$\Rightarrow 1 \neq \# \langle a \rangle \mid \# G = \underset{\text{prim}}{p} \Rightarrow \langle a \rangle = G$ $\square$

2.20. **Def.:** $N \subseteq G$ UG von G heißt **Normalteiler** (NT), falls
$$\forall a \in G: \underline{aNa^{-1}} = N \quad (\Leftrightarrow \underline{aN = Na})$$

2.21. **Bem.:** • $ab = ba$ muss nicht notw. gelten!

• $H \subseteq G \Rightarrow aHa^{-1}$ ist UG $\left((ah_1a^{-1}) \cdot (ah_2a^{-1})^{-1} = ah_1 a^{-1} a h_2^{-1} a^{-1} = a \underbrace{h_1 h_2^{-1}}_{\in H} a^{-1} \in aHa^{-1} \checkmark \right)$

2.22. Bsp.: In G sind e, G stets NT.

2.23. Bsp.: G abelsch, H UG $\Rightarrow H$ NT

Bew.: $\forall a \in G \ \forall b \in H: aba^{-1} = b \Rightarrow aHa^{-1} = H$. $\square$

2.24. Bsp.: In G ist $Z(G)$ NT.

Bew.: $Z(G) = \{ a \in G;\ \forall b \in G: \underset{\Leftrightarrow\, bab^{-1} = a}{ab = ba} \} \Rightarrow b Z(G) b^{-1} = Z(G)$ für alle $b \in Z(G)$. $\square$

2.25. **Satz:** Sei G Gruppe, $\underline{N \subseteq G \text{ NT}}$, $\cdot : G/N \times G/N \to G/N$, $(aN, bN) \mapsto (ab)N$.

Dann: • ist wohldef., $(G/N, \cdot, N = eN)$ ist Gruppe.

Bew.: Wohldef.: Sei $a_1 N = a_2 N$, $b_1 N = b_2 N$

$\Rightarrow a_1^{-1} a_2 \in N$, $b_1^{-1} b_2 \in N$

$\Rightarrow (a_1 b_1)^{-1}(a_2 b_2) = \underbrace{b_1^{-1} \underbrace{a_1^{-1} a_2}_{\in N} b_1}_{\in N,\ \text{da } N \text{ NT}} \cdot \underbrace{\overset{e}{b_1^{-1}} \cdot b_2}_{\in N} \in N$

$\Rightarrow (a_1 b_1) N = (a_2 b_2) N$.

Gruppenaxiome … $\square$

2.26. Def.: $(G/N, \cdot, \underbrace{N}_{=eN})$ heißt Faktorgruppe von G nach N
(auch: Quotientengruppe, G mod N)

2.27. Bsp.: Die Faktorgruppen von $\mathbb{Z}$

Die UG von $\mathbb{Z}$ sind genau die $n\mathbb{Z}$, $n \in \mathbb{N}_0$
abelsch → diese sind NT nach Bsp. 2.23

→ Die Faktorgr. von $\mathbb{Z}$ sind genau die Restklassengruppen

$\mathbb{Z}/n\mathbb{Z} \overset{!}{=} \{\underline{0}, \underline{1}, \underline{2}, \ldots, \underline{n-1}\}$ die $a + n\mathbb{Z} =: \underline{a}$

↑ „Div. mit Rest bei „⊆""

$\underline{a} + \underline{b} = \underline{a+b}$
„(⇒) $(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b) + n\mathbb{Z}$"

→ $\mathbb{Z}/n\mathbb{Z}$ hat n El. und ist zykl. der Ordnung n,
denn $\mathbb{Z}/n\mathbb{Z} = \langle \underline{1} \rangle$
$= \{0 \cdot \underline{1}, 1 \cdot \underline{1}, 2 \cdot \underline{1}, \ldots, (n-1) \cdot \underline{1}\}$
↪ $\underbrace{\underline{1} + \underline{1} + \ldots + \underline{1}}_{n \text{ mal}} = \underline{0}$.

□

2.28. Bsp.: Def.: G Gruppe, $K(G) := \langle \{\underbrace{aba^{-1}b^{-1}}_{\text{Kommutator}};\ a, b \in G\} \rangle$
heißt Kommutator UG.
Lemma: $K(G)$ ist NT in G. „…"
↪ $G/K(G)$ ist abelsche Gruppe.

A3: Gruppenoperationen

≠ Gruppenverknüpfungen („·")
$G \times G \to G$
$(a, b) \mapsto a \cdot b$

3.1. Einleitung: Gr.op., Bahnen, Klassenglg.

$A \in GL(n, K)$: $Av = w$
$v, w \in K^n$

3.2. Def.: Sei G Gruppe, X Menge. Eine (Gruppen-) Operation von G auf X (Gruppenwirkung) ist eine Abb. $T : G \times X \to X$

$$(a, x) \mapsto T_a(x) \quad \text{mit}$$

(i) $\forall x \in X : T_e(x) = x$, d.h. $T_e = id_X$,

(ii) $\forall a, b \in G \ \forall x \in X : T_{ab}(x) = T_a(T_b(x)) = T_a \circ T_b(x)$.

„G op. auf X (vermöge T)", „G wirkt auf X"

Schreiben oft: ax statt $T_a(x)$. Damit:

(i') $\forall x \in X : ex = x$,

(ii') $\forall a, b \in G \ \forall x \in X : (ab)x = a(bx)$.

3.3. Bem.: $T_{a^{-1}} \circ T_a \overset{(ii)}{=} T_{a^{-1}a} = T_e \overset{(i)}{=} id_X$, $\quad T_a \circ T_{a^{-1}} = id_X$.

Alle T_a sind daher Bijektionen (von X auf sich), $(T_a)^{-1} = T_{a^{-1}}$.

3.4. Bsp.: $S_n = \{X \to X \text{ bij}\}$, $X = \{1, \dots, n\}$.

S_n op. auf X vermöge $S_n \times X \to X$

$$(\sigma, i) \mapsto \sigma(i) =: \sigma i$$

Denn: $ei = e(i) = id_X(i) = i$, $(\sigma\tau)(i) = (\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(\tau i)$.

3.5. Bsp.: K Körper, $G := GL(n, K)$ operiert auf K^n vermöge

$$G \times K^n \to K^n, \ (A, x) \mapsto Ax.$$

Denn: $Ix = x$, $(AB)x = A(Bx)$.

3.6. Bsp.: G Gruppe, G op. auf $X := G$ vermöge der Linkstranslation $G \times G \to G$, $(a, x) \mapsto l_a(x) := ax$.

Denn: $ex = x$, $(ab)x = a(bx)$. ✓

3.7. Bsp.: G Gruppe, G op. auf $X := G$ vermöge der (Gruppen-) Konjugation : $G \times G \to G$

($\neq$ Komplex-Konjugation) $\quad (a, x) \mapsto \underbrace{axa^{-1}}_{\text{Konj. von } x \text{ mit } a}$

Denn: $exe^{-1} = x$, $(ab)x(ab)^{-1} = a(bxb^{-1})a^{-1}$. ✓

3.8. Def.: G operiere auf X. Dann: $x \sim y :\Leftrightarrow \exists a \in G: ax = y$.

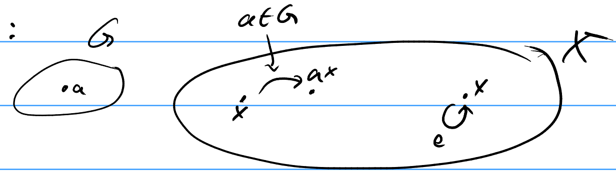
3.9. Lemma: $\sim$ def. eine Ä-Rel. auf X. ⌜.....⌟

3.10. Def.: Die $\sim$-Ä-Klassen heißen Bahnen ⌜orbits⌟:
Für $x \in G$ sei $Gx := \{ax;\ a \in G\} \subseteq X$
Gx heißt Bahn von $x \in X$.

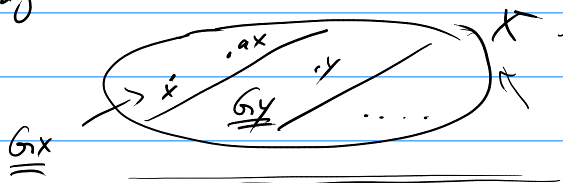
G operiert transitiv auf X, falls X aus nur einer Bahn besteht.

3.11. Satz: Die Einschränkung einer Gruppenop. auf eine Bahn ist transitiv. ✓

Situation:



→ Bahnenzerlegung:



$\to X = Gx_1 \dot\cup \ldots \dot\cup Gx_q$ falls X endlich

$\# X = \sum \# Gx_i$? → Bahnengl., s.u.

3.12. Def.: Sei $x \in X$. $Iso(x) := \{a \in G;\ ax = x\}$ heißt Isotropiegruppe von x, bzw. Stabilisator von x.

⌜die $a \in G$, die x festlassen⌟

3.13 Lemma: $Iso(x)$ ist UG G.

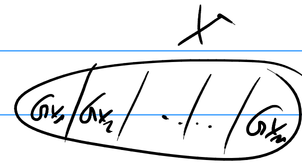
Bew.: $e \in Iso(x)$ ✓, $a, b \in Iso(x)$

$$\Rightarrow (ab^{-1})x = a(b^{-1}x) \underset{\substack{\uparrow \\ bx = x}}{=} ax = x \Rightarrow ab^{-1} \in Iso(x)$$

□

3.14. <u>Satz (Bahnengleichung):</u>

G endliche Gr., G op. auf endl. Menge X,
$x_1, \dots, x_m$ vollst. Repr.system für Bahnen,
d.h. $X = Gx_1 \,\dot\cup\, Gx_2 \,\dot\cup \dots \dot\cup\, Gx_m$.



Dann: $\#X = \sum_{i=1}^{m} \#Gx_i = \sum_{i=1}^{m} [G : Iso(x_i)]$.

<u>Bew.:</u> Betr. Bahn Gx. Für $a, b \in G$ gilt:

$ax = bx \iff b^{-1}(ax) = b^{-1}(bx) = x \iff b^{-1}a \in Iso(x)$
$\iff a\,Iso(x) = b\,Iso(x)$,

d.h. $\varphi : \overbrace{G/Iso(x)}^{\text{Faktormenge}} \to Gx$
$a\,Iso(x) \mapsto ax$,

ist Bijektion.

Da G endl., folgt $\#\underbrace{Gx}_{\{bx;\, b \in G\}} = \#\underbrace{G/Iso(x)}_{\{a\,Iso(x);\, a \in G\}} = [G : Iso(x)]$,

insg.: $\#X = \sum_{i=1}^{m} \#Gx_i = \sum_{i=1}^{m} [G : Iso(x_i)]$.

$\square$