Teil I: Gruppen

A 1: Gruppen: Definitionen und Beispiele

1.1. Einleitung: Gruppe = Menge mit Verknüpfung und neutr. El. / Beispiele

1.2. Def.: G **Gruppe** $:\Leftrightarrow$ G Menge, $\exists$ Verknüpfung/Abb. $\underset{\ast,\,\circ,\,\boxtimes}{\cdot} : G\times G \to G$,
$\exists e \in G$: (1) $\forall a,b,c \in G: (ab)c = a(bc)$

$(G,\cdot,e)$

(2) $\forall a \in G: \; ea = a$ — e linksneutral

(3) $\forall a \in G \; \exists b \in G: \; ba = e$ — linksinv.

e heißt Neutralel., b Links-Inverse von a.

Keine Komm.!

1.3 Lemma: $(G,\cdot,e)$ Gruppe, dann:

(i) $\forall a \in G: ae = a$

(ii) $\forall e' \in G: (\forall a: e'a = a \Rightarrow e' = e)$

(iii) $\forall a,b \in G: (\underset{\sim}{ba = e} \Rightarrow ab = e)$ — rechts-invers

(iv) $\forall a, b_1, b_2 \in G: (b_1 a = b_2 a = e \Rightarrow b_1 = b_2)$

Bew.: (iii): $\underbrace{ba = e \overset{(3)}{\Rightarrow} \exists c \in C: cb = e}$

$\Rightarrow ab \overset{(2)}{=} e(ab) = (cb)(ab) \underset{(1)}{=} c(ba)b = ceb \overset{(1),(2)}{=} cb = e.$

(i): Wähle b mit $ba = e$ (3).

$\Rightarrow ae = a(ba) \overset{(1)}{=} (ab)a \overset{(iii)}{=} ea \overset{(2)}{=} a.$

(ii): Sei $e' = G: \; \forall a: e'a = a \Rightarrow e = e'e \overset{(i)}{=} e'.$

(iv): Sei $b_1 a = b_2 a = e \Rightarrow b_1 = e b_1 = (b_2 a) b_1 = b_2 (a b_1) = b_2 e = b_2.$

$\square$

1.4. Bez.: $b \in G$ mit $ba = e$ heißt <u>Inverses von a</u>, Not.: $b = a^{-1}$.

1.5. Lemma: $\forall a_1,\dots,a_n \in G: (a_1 \cdot a_2 \cdot\ldots\cdot a_n)^{-1} = \underbrace{a_n^{-1} \cdot a_{n-1}^{-1} \cdot\ldots\cdot a_2^{-1} \cdot a_1^{-1}}.$

Bew.: VI nach n: $\underset{\sim}{n=1}$: $a_1^{-1} = a_1^{-1}$ ✓

$\underset{\sim}{n \to n+1}$: $(a_1 \cdot\ldots\cdot a_n \cdot a_{n+1}) \cdot (a_{n+1}^{-1} \cdot a_n^{-1} \cdot\ldots\cdot a_2^{-1} \cdot a_1^{-1})$

$\underset{(1)}{=} (a_1 \cdot\ldots\cdot a_n)\underbrace{(a_{n+1} \cdot a_{n+1}^{-1})}_{e}(a_n^{-1} \cdots a_1^{-1}) \underset{IV}{=} e.$ ✓

$\square$

1.6. Def.: Gruppe G <u>abelsch</u> $:\iff \forall a,b \in G: \ ab = ba$ ⌜komm. Gr.⌟

1.7. Bem.: Bei ab. Gr.: schreibe oft $+$ statt $\cdot$, 0 statt e sowie $-a$ statt a^{-1}
(additive Schreibweise)

1.8. Bsp.: $(\mathbb{Z}, +, 0)$ ab. Gr. ✓

1.9. Bsp.: Sei K ein Körper. Dann $(K, +, 0)$ add. Gr. von K
$(K^* := K \setminus \{0\}, \cdot, 1)$ mult. Gr. von K

1.10. Bsp.: V ein K-VR. Dann: $(V, +, 0)$ Gr.
Ferner: $(\underbrace{Aut(V)}_{= \{f: V \to V \text{ bij. lin. Abb.}\}}, \circ, id_V)$ i.a. nichtabelsche Gruppe

1.11. Bsp.: K Körper, $n \geq 1 \rightsquigarrow GL(n,K) := \{A \in K^{n \times n};\ \det A \neq 0\}$ i.a. nichtab. Gr.

Gruppeniso: $\left.\begin{array}{l} Aut(V) \to GL(n,K) \\ f \mapsto M^{\mathcal{B}}_{\mathcal{B}}(f) \end{array}\right\}$

⌞Basis in V: $\mathcal{B} = (v_1, \ldots, v_n)$

1.12. Bsp.: Sei X bel. Menge $\neq \emptyset$, $Perm(X) := \{f : X \to X \text{ bij.}\}$.
Dann $(Perm(X), \underset{\text{Kompos.}}{\circ}, id_X)$ Gr., die sog. <u>Permutationsgruppe von X</u>

Speziell: $X = \{1, 2, \ldots, n\} \rightsquigarrow$ <u>Def.</u>: $\underline{\underline{S_n}} := Perm(\{1, \ldots, n\})$ <u>symmetrische</u>
<u>Gruppe der Größe n</u>

1.13. Bsp.: Seien $G_1, \dots, G_m$ Gruppe, $G := G_1 \times \dots \times G_m = \{(a_1,\dots,a_m);\ \forall i \leq m : a_i \in G_i\}$

G ist Gruppe bzgl. $(a_1,\dots,a_m)\cdot(b_1,\dots,b_m) = (a_1 b_1, \dots, a_m b_m)$

$e := (e_1, \dots, e_m)$

Ferner: G ab. $\Leftrightarrow \forall i \in \{1,\dots,m\}: G_i$ ab.

1.14. Def.: Sei $a_0, \dots, a_{n-1}$ endl. Folge aus G. $\qquad a_1 \cdots a_n = \prod_{i=1}^{n} a_i$

Dann: $\prod_{i=0}^{0-1} \emptyset := e$, $\prod_{i=0}^{n} a_i := \left(\prod_{i=0}^{n-1} a_i\right)\cdot a_n$, $\qquad a_1 + \dots + a_n = \sum_{i=1}^{n} a_i$

Additiv: $\sum_{i=0}^{n-1} a_i$ für $\prod_{i=0}^{n-1} a_i$, sowie na für a^n $\qquad \begin{cases} a^n = \underbrace{a \cdots a}_{n \text{ mal}} \\ na = a + \dots + a \end{cases}$

$a^{-n} := (a^{-1})^n$ für $n \geq 1 \Rightarrow a^{-n} \underset{1.5}{=} (a^n)^{-1}$.

1.15. Lemma: $\forall a_i, b_j \in G$: $\left(\prod_{i=0}^{m-1} a_i\right)\cdot\left(\prod_{j=0}^{n-1} b_j\right) = \prod_{k=0}^{m+n-1} c_k$ } Assoziativität!

mit $c_k = a_k$, für $k < m$

$c_k = b_{k-m}$, für $m \leq k < m+n$

Bew.: VI nach: $n=0$: ✓ $\left(\prod_{i=0}^{m-1} a_i\right) e = \prod_{i=0}^{m-1} a_i$ ✓

$n \to n+1$ .... $\square$

1.16. Lemma: $\forall a \in G\ \forall m, n \in \mathbb{Z}$: (i) $a^m \cdot a^n = a^{m+n}$

(ii) $(a^m)^n = a^{m \cdot n}$

Bew.: VI nach n, Fallunterscheidung, ob Expon. neg.! ...

(bzw. wende 1.15 an) $\qquad$ 2 i.a. $a^n b^n \neq (ab)^n$

$\qquad a \cdots a \quad b \cdots b \neq abab\dots$

1.17. Def.: G sei Gruppe. $\operatorname{ord} G := \# G \in \mathbb{N} \cup \{\infty\}$ heißt Ordnung von G.

Sei $a \in G$. $\operatorname{ord}(a) := \min\{n \in \mathbb{N};\ a^n = e\} \geq 1$ falls existent,

sonst $\operatorname{ord}(a) := \infty$ heißt Ordnung von a.

$\operatorname{ord}(a) \in \mathbb{N} \rightsquigarrow a$ heißt ein El. endl. Ordnung.

sonst $\rightsquigarrow$ " " unendl. "

1.18 Bsp.: $G = \mathbb{Z}$, Alle El. $\neq 0$ haben unendl. Ordn.

1.19 Bsp.: $K = \mathbb{R}$, $V = \mathbb{R}^2$, $f_\varphi \hat{=}$ Drehung um $\measuredangle \varphi$, Drehzentrum 0

Sei $\varphi := \frac{2\pi}{m}$, dann $\operatorname{ord}(f_\varphi) = m$.

1.20 Bsp.: Sei G endl., dann hat jedes El. $a \in G$ endl. Ordnung.

Bew.: die Potenzen $a^0, a^1, a^2, \ldots$ können nicht pwv., wenn G endl.

$\Rightarrow \exists\ 0 < i < j: \quad a^i = a^j \Rightarrow e = (a^{-i}) a^i = (a^{-i}) a^j \underset{1.16}{=} a^{j-i}$

d.h. $\operatorname{ord}(a) \leq j - i \in \mathbb{N}$. $\square$

1.21 Lemma: $a \in G$, $\operatorname{ord}(a) = n \in \mathbb{N}$: Dann: $\forall i, j \in \mathbb{N}: \quad a^i = a^j \Leftrightarrow n \mid i - j$

$(\Rightarrow$ Speziell: $\forall i \in \mathbb{N}: a^i = e \Leftrightarrow n \mid i$.