Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil I: GRUPPEN

A1: Gruppen: Definitionen und Beispiele

Stichworte: Def. Gruppe, neutrale und inverse Elemente, abelsche Gruppe, additiv und multiplikativ geschriebene Gruppe, Bsp. $\mathrm{Aut}(V)$, $GL(n,K)$, $\mathrm{Perm}(X)$, S_n, $G_1 \times \ldots \times G_m$, Gruppenordnung, Ordnung eines Gruppenelements, $\mathrm{ord}(a)$ teilt i mit $a^i = e$

1.1. Einleitung: Eine Gruppe ist durch Angabe einer Gruppenverknüpfung (multiplikativ oder additiv geschrieben) und zugehörigem (links-) neutralen Element e (d.h. 1 oder 0) definiert. Wir untersuchen erste Beispiele.

1.2. Def.: G Gruppe $:\Leftrightarrow$ G Menge, $\exists$ Verknüpfung $\cdot : G \times G \to G$, $\exists e \in G$:

$(G, \cdot, e)$

(1) $\forall a,b,c \in G$: $(ab)c = a(bc)$ assoziativ

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

(3) $\forall a \in G\ \exists b \in G$: $ba = e$ linksinvers

$e \in G$ heißt Neutralelement, b Links-Inverses von a.

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

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

(ii) $\forall e' \in G$: $(\forall a \in G: e'a = a \Rightarrow e' = e)$ Eind. des Neutralel.

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

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

Bew.: (iii): $ba = e \overset{(3)}{\Rightarrow} \exists c \in G: cb = e \Rightarrow ab \overset{(2)}{=} e(ab) = (cb)(ab) \overset{(1)}{=} c(ba)b$
$= ceb \overset{(1),(2)}{=} cb = e$.

(i): Wähle b mit $ba = e$ (3).
$\Rightarrow ae = a(ba) \overset{(1)}{=} (ab)a \overset{(iii)}{=} ea \overset{(2)}{=} a$.

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

(iv): Sei $b_1 a = b_2 a = e$
$\Rightarrow b_1 = eb_1 = (b_2 a)b_1 = b_2(ab_1) = b_2 e = b_2$. $\square$

1.4. **Bez.:** Das eind. best. $b \in G$: $ba = e$ heißt Inverses von a, man bezeichnet es mit a^{-1}.

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

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

$n \rightsquigarrow n+1$: $(a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}) \cdot (a_{n+1}^{-1} \cdot a_n^{-1} \cdot \ldots \cdot a_1^{-1}) = (a_1 \cdots a_n) \cdot \overbrace{(a_{n+1} \cdot a_{n+1}^{-1})}^{=e} \cdot (a_n^{-1} \cdots a_1^{-1})$

$= (a_1 \cdots a_n) \cdot (a_n^{-1} \cdots a_1^{-1}) \underset{IV}{=} e$. ✓ $\square$

1.6. **Def.:** Gruppe G abelsch $:\Leftrightarrow \forall a, b \in G$: $ab = ba$

1.7. **Bem.:** Bei abelschen Gruppen schreibt man oft $+$ statt $\cdot$, 0 statt e sowie $-a$ statt a^{-1} (additive Schreibweise).

1.8. **Bsp.:** $(\mathbb{Z}, +, 0)$ ist abelsche Gruppe.

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

1.10. **Bsp.:** Sei K Körper, V ein K-VR. Dann $(V, +, 0)$ Gruppe.
Ferner: $(\mathrm{Aut}(V), \circ, \mathrm{id}_V)$ i.a. nichtabelsche Gruppe, die Automorphismengruppe von V,
wobei $\circ$ die Komposition, und $\mathrm{Aut}(V) = \{f : V \to V \text{ bij. Hom.}\}$.

1.11. **Bsp.:** Sei K Körper, $n \geq 1$, $GL(n, K) := \{A \in K^{n \times n};\ A \text{ regulär, d.h. } \det(A) \neq 0\}$, ist i.a. nichtabelsche Gruppe.
Betr. K-VR V, Basis $\mathcal{B} = (v_1, \dots, v_n)$ in V. Dann:

$$\left.\begin{aligned} \mathrm{Aut}(V) &\longrightarrow GL(n, K) \\ f &\longmapsto M_{\mathcal{B}}^{\mathcal{B}}(f) \end{aligned}\right\} \text{ Gruppenisomorphismus}$$

Matrixdarst. bzgl. Basis $\mathcal{B}, \mathcal{B}$

1.12. **Bsp.:** Sei X bel. Menge, $\mathrm{Perm}(X) := \{f;\ f : X \to X \text{ bij.}\}$.
Dann $(\mathrm{Perm}(X), \circ, \mathrm{id}_X)$ Gruppe, die sog. Permutationsgruppe von X.
Komposition

Speziell: $X = \{1, 2, \dots, n\}$
Def.: $S_n := \mathrm{Perm}(\{1, \dots, n\})$ symmetrische Gruppe der Größe n.

1.13. **Bsp.:** Seien $G_1, \dots, G_n$ Gruppen, $G := G_1 \times \dots \times G_n$.
G ist Gruppe bzgl. $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) := (a_1 b_1, \dots, a_n b_n)$,
$e := (e_1, \dots, e_n)$.

Ferner gilt: G abelsch $\Leftrightarrow \forall i \in \{1, \dots, n\}: G_i$ abelsch.

1.14. **Def.:** Sei $a_0, \dots, a_{n-1}$ endl. Folge aus G. Dann: $\prod_{i=0}^{0-1} \emptyset := e$, $\prod_{i=0}^{n} a_i := \left(\prod_{i=0}^{n-1} a_i\right) \cdot a_n$.
Falls $\forall i \in \{1, \dots, n\}: a_i = a$, so schreibe a^n.
Additive Schreibweise: $\sum_{i=0}^{n-1} a_i$ für $\prod_{i=0}^{n-1} a_i$, sowie na für a^n.
$a^{-n} := (a^{-1})^n$ für $n \geq 1 \Rightarrow a^{-n} = (a^n)^{-1}$ nach Lemma 1.5.

1.15. **Lemma:** $\forall a_i, b_j \in G: \left(\prod_{i=0}^{m-1} a_i\right)\left(\prod_{j=0}^{n-1} b_j\right) = \prod_{k=0}^{m+n-1} c_k$
mit $\begin{cases} c_k = a_k, & \text{für } k < m, \\ c_k = b_{k-m}, & \text{für } m \leq k < m+n. \end{cases}$

Bew.: VI nach n: $n=0$: ✓ da $\left(\prod_{i=0}^{m-1} a_i\right) e = \prod_{i=0}^{m-1} a_i$.
$n \to n+1$: $\left(\prod_{i=0}^{m-1} a_i\right) \cdot \left(\prod_{j=0}^{n} b_j\right) = \left(\prod_{i=0}^{m-1} a_i\right)\left(\prod_{j=0}^{n-1} b_j\right) b_n \overset{IV}{=} \left(\prod_{k=0}^{m+n-1} c_k\right) \cdot b_n = \prod_{k=0}^{m+n} c_k$. ✓ □

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.: (i) $n \geq 0$: VI nach n: $n=0$: $a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}$ ✓,
(oder 1.15) $n \to n+1$: $a^m \cdot a^{n+1} = a^m \cdot a^n \cdot a = a^{m+n} \cdot a$
$m+n \geq 0$: $a^{m+n} \cdot a = a^{(m+n)+1} = a^{m+(n+1)}$ ✓.
$m+n < 0$: $a^{m+n} \cdot a = (a^{-1})^{-m-n} \cdot a = (a^{-1})^{-m-n-1} = a^{m+(n+1)}$ ✓.
$n < 0$: $a^m \cdot a^n = (a^{-1})^{-m} \cdot (a^{-1})^{-n} = (a^{-1})^{-m-n} = a^{m+n}$. ✓
(ii) $n \geq 0$: VI nach n: $n=0$: $(a^m)^0 = e = a^{m \cdot 0}$ ✓.
$n \to n+1$: $(a^m)^{n+1} = (a^m)^n \cdot a^m \overset{(i)}{=} a^{mn+m} = a^{m(n+1)}$ ✓.
$n < 0$: $(a^m)^n = ((a^m)^{-1})^{-n} = (a^{-m})^{-n} = a^{(-m)(-n)} = a^{mn}$ ✓. □

1.17. **Def.:** G sei Gruppe. $\operatorname{ord} G := \#G \in \mathbb{N} \cup \{\infty\}$ heißt Ordnung von G.
Sei $a \in G$. $\operatorname{ord}(a) := \min\{n \in \mathbb{N};\ a^n = e\}$, falls existent,
sonst $\operatorname{ord}(a) := \infty$ heißt Ordnung von a.
Im ersten Fall heißt a ein El. endlicher Ordnung,
im zweiten Fall heißt a ein El. unendlicher Ordnung.

1.18. **Bsp.:** Sei $G := \mathbb{Z}$. Alle El. $\neq 0$ haben unendliche Ordnung.

1.19. **Bsp.:** Sei $K := \mathbb{R}$, $V := \mathbb{R}^2$, $f_\varphi \hat{=}$ Drehung um $\measuredangle \varphi$.
Sei $\varphi := \frac{2\pi}{n}$, dann $\operatorname{ord}(f_\varphi) = n$.

1.20. **Bsp.:** Sei G endl., dann hat jedes $a \in G$ endl. Ordnung.
Bew.: $\exists\, 0 < i < j$: $a^i = a^j \Rightarrow e = (a^{-i})a^i = (a^{-i})a^j \overset{1.16}{=} a^{j-i}$,
d.h. $\operatorname{ord}(a) \leq j - i \in \mathbb{N}$. $\square$

1.21. **Lemma:** Sei $a \in G$ (G Gruppe), $\operatorname{ord}(a) = n \in \mathbb{N}$.
(Genau) Dann: $\forall i, j \in \mathbb{N}$: $(a^i = a^j \Leftrightarrow n \mid i - j)$.
Speziell $\forall i \in \mathbb{N}$: $(a^i = e \Leftrightarrow n \mid i)$.
Bew.: „$\Leftarrow$": Sei $i - j = m \cdot n$ mit $m \in \mathbb{Z}$.
$\Rightarrow a^{i-j} = a^{mn} = (a^n)^m = e^m = e$
$\Rightarrow a^i = a^{i-j} \cdot a^j = e a^j = a^j$.
„$\Rightarrow$": Division mit Rest: $i - j = mn + r$ mit $r \in \{0, \dots, n-1\}$, $r < n$.
$a^i = a^j \Rightarrow a^i \cdot a^{-j} = a^{i-j} = e$
$\Rightarrow a^r = a^{(i-j)-mn} = a^{i-j} \cdot \underbrace{(a^{mn})^{-1}}_{=e} = a^{i-j} = e \Rightarrow r = 0$,
da $r < n = \operatorname{ord}(a)$. $\square$