§1 Elementare Gruppentheorie

<u>Erinnerung:</u> eine <u>Verknüpfung</u> auf einer (nicht leeren) Menge X ist eine Abbildung

$$m: X \times X \to X, \quad (a,b) \mapsto m(a,b)$$

Man schreibt oft $m(a,b) = a\cdot b$ oder $a * b$ oder ab oder $a+b$, je nach Kontext.

1. <u>Def</u> Eine <u>Gruppe</u> $(G, \cdot)$ besteht aus einer (nicht leeren) Menge G mit einer Verknüpfung $\cdot$ mit folgenden Eigenschaften.

(G1) Die Verknüpfung ist <u>assoziativ</u>, für alle $a,b,c \in G$ gilt $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

(G2) Es gibt ein <u>Neutralelement</u> $e \in G$, also $a\cdot e = e\cdot a$ für alle $a \in G$

(G3) Jedes $a \in G$ hat ein Inverses $b \in G$, also $a\cdot b = b\cdot a = e$

Aus (G1) folgt, dass man Klammern weglassen darf, $a\cdot b\cdot c = (a\cdot b)\cdot c = a\cdot(b\cdot c)$ etc.

Falls die Verknüpfung zusätzlich kommutativ ist, also $a \circ b = b \circ a$ für alle $a, b \in G$, so heißt die Gruppe <u>abelsch</u> [N. Abel, norweg. Math., 1802–1829] oder <u>kommutativ</u>. Dann schreibt man auch "+" für die Verknüpfung.

Falls die Verknüpfung nur (G1) und (G2) erfüllt, so spricht man von einem <u>Monoid</u>.

2. <u>Bsp</u>

$$\left.\begin{array}{l} (\mathbb{Z}, +) \\ (\mathbb{Q}, +) \end{array}\right\} \text{Gruppen}$$

$$\left.\begin{array}{l} (\mathbb{Z}, \cdot) \\ (\mathbb{N}, +) \\ (\mathbb{N}, \cdot) \end{array}\right\} \text{Monoide, \underline{keine} Gruppen}$$

3. <u>Beobachtungen</u>

(a) Das Neutralelement e einer Gruppe ist <u>eindeutig</u>.

<u>Denn</u>: $e, \tilde{e} \in G$ Neutralelemente

$$\Rightarrow \underset{\substack{\| \\ e}}{e \circ \tilde{e}} = \tilde{e} \quad \Rightarrow e = \tilde{e}$$

(dies gilt auch in Monoiden)

(b) Inverse sind auch eindeutig.

Denn $a \circ b = e = a \circ c \Rightarrow c \circ a \Rightarrow$

$$c = c \circ e = c \circ a \circ b = e \circ b = b$$

Wir schreiben daher $a^{-1} = b$ für die Inverse von a. ⊛

4. Bsp Sei X eine nicht leere Menge, sei

$M(X) = X^X = \{f : X \to X\}$ die Menge aller Abbildungen von X nach X. Als Verknüpfung auf $M(X)$ nehmen wir die Verkettung von Abbildungen, also

$(f \circ h)(a) = f(h(a))$. Dann gilt (G1) und (G2) mit Neutralelement id_X.

Folglich ist $M(X)$ ein Monoid.

Sei $Sym(X) = \{ f \in M(X) \mid f \text{ ist bijektiv} \}$

Für $f, h \in Sym(X)$ gilt $f \circ h, f^{-1} \in Sym(X)$ (!)

Damit ist $Sym(X)$ eine Gruppe, die symmetrische Gruppe.

Ist $|X| = n$ endlich, so hat $Sym(X)$

$n! = n(n-1)(n-2)\cdots$ Elemente.

Für $X = \{1, 2, \ldots, n\}$ schreibt man auch

$Sym(X) = Sym(n) = S_n$

Folgerungen:

(a) Man kann kürzen:

$$ac = bc \Rightarrow a = b$$

Denn: $ac = bc \Rightarrow acc^{-1} = bcc^{-1}$.

(b) Es gilt $(a^{-1})^{-1} = a$, denn $a^{-1}a = a^{-1}a = e$

(c) Es gilt $(ab)^{-1} = b^{-1}a^{-1}$, denn $(ab)(b^{-1}a^{-1}) = e$

—

Die <u>Ordnung</u> einer (endlichen) Gruppe ist

$|G|$

5. <u>Bsp</u> Sei K ein Körper, sei $GL_n(K)$ $= \{ g \in K^{n\times n} \mid \det(g) \neq 0 \} = \{ g \in K^{n\times n} \mid g \text{ invertibar} \}$

Dann ist $K^{n\times n}$ bzgl. Matrizenmultiplikation ein Monoid (mit Neutralelement $\mathbb{1}_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$)

und $GL_n(K) \subseteq K^{n\times n}$ ist eine Gruppe, die <u>allgemeine lineare Gruppe</u>.

<u>Denn</u>: $g, h \in GL_n(K) \rightsquigarrow \det(gh) = \underbrace{\det(g)}_{\neq 0} \underbrace{\det(h)}_{\neq 0} \neq 0$

$\Rightarrow gh \in GL_n(K)$, $\mathbb{1}_n \in GL_n(K)$, $\det(g) \neq 0 \Rightarrow$ g hat Inverse g^{-1}.

<u>Etwa</u>:

$$\left.\begin{array}{l} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \end{array}\right\} GL_2(K) \text{ ist nicht abelsch}$$

genauso ist $GL_n(K)$ <u>nicht abelsch</u> für alle $n \geq 2$.

$Sym(X)$ ist ebenfalls <u>nicht abelsch</u> für alle X mit $|X| \geq 3$: $u, v, w \in X$ paarweise verschieden

α	β
$u \mapsto v$	$v \mapsto w$
$v \mapsto u$	$w \mapsto v$
$x \mapsto x$ sonst	$x \mapsto x$ sonst

$\alpha \circ \beta$	$\beta \circ \alpha$	$\alpha \circ \beta \neq \beta \circ \alpha$
$v \mapsto w$	$v \mapsto u$	
$w \mapsto u$	$u \mapsto v$	
$u \mapsto v$	$u \mapsto w$	

#