II Vektorräume

§1 Gruppen

Seien A, B Mengen. Eine Abbildung f ist eine Vorschrift, welche jedem Element $a \in A$ genau ein Element $f(a) \in B$ zuordnet.
Schreibe $f: A \to B$.
A heißt Definitionsbereich (Urbildbereich) von f.
$f(A) = \{f(a);\ a \in A\} \subset B$ heißt Bildbereich.
Wichtige Begriffe: injektiv $(\forall a, a' \in A: f(a) = f(a') \Rightarrow a = a')$
surjektiv $(f(A) = B)$
bijektiv (inj + surj)

Def: Sei M eine Menge. Eine innere Verknüpfung „$\circ$" von M, ist eine Vorschrift $\circ$, welche je zwei Elementen $a, b \in M$ in eindeutiger Weise ein Weiteres zuordnet.
(d.h. eine Abbildung $\circ: M \times M \to M$.)
$(a, b) \mapsto a \circ b$

Def: Eine Gruppe ist ein Paar $(G, \circ)$, bestehend aus einer Menge G und einer inneren Verknüpfung $\circ: G \times G \to G$, $(a, b) \mapsto a \circ b$, mit den Eigenschaften

G1 Assoziativgesetz: $(a \circ b) \circ c = a \circ (b \circ c)$ $\forall a, b, c \in G$

G2 Neutrales Element:
Es gibt ein $e \in G$ so daß gilt:
$$e \circ a = a \quad \forall a \in G$$

G3 Für alle $a \in G$ ex. $a' \in G$ (inverses El. zu a) mit $a' \circ a = e$.

Falls zusätzlich gilt
$$a \circ b = b \circ a \quad \forall a, b \in G$$ (Kommutativgesetz)
so heißt die Gruppe abelsch.

Bem 1 Sei $(G, \circ)$ Gruppe.
i) Sei $e \in G$ neutr. Element. Dann gilt
$$a \circ e = a \quad \forall a \in G$$
ii) Es gibt genau ein neutr. El. $e \in G$.
iii) Ist a' invers zu $a \in G$, dann gilt
$$a \circ a' = e$$
iv) Zu jedem $a \in G$ ex genau ein Inverses El. a', das man auch mit a^{-1} bez.

Bew: iii) Zu $a' \in G$ ex nach G3. ein $a'' \in G$ mit $a'' \circ a' = e$.
$$\Rightarrow \quad a \circ a' = e \circ (a \circ a') = (a'' \circ a') \circ (a \circ a')$$
$$\overset{G1}{=} a'' \circ ((a' \circ a) \circ a')$$
$$\overset{G3}{=} a'' \circ (e \circ a')$$
$$\overset{G2}{=} a'' \circ a'$$
$$= e.$$

i) $a \circ e = a \circ (a' \circ a)$

$= (a \circ a') \circ a$

$\overset{(iii)}{=} e \circ a$

$\overset{G2}{=} a$.

ii) Sei e' weiteres neutr. El.

G2) $(\forall a\ e) \Rightarrow e \circ e' = e'$

" $(\forall a\ e') \overset{i)}{\Rightarrow} e \circ e' = e$ $\Big\} \Rightarrow e = e'$

iii) Sei a' und a'' inverse zu a.

$a'' \overset{i)}{=} a'' \circ e \overset{(iii)}{=} a'' \circ (a \circ a') \overset{G1}{=} (a'' \circ a) \circ a'$

$\overset{G3}{=} e \circ a' \overset{G2}{=} a'$. □

Satz 2: Sei $(G, \circ)$ Gruppe und $a, b \in G$.

i) $(a^{-1})^{-1} = a$

ii) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Beweis: i) Satz 1 iv) $\Rightarrow$ Zu a^{-1} ist genau ein inv. El.

$a \circ a^{-1} = e \Rightarrow a$ ist inv zu a^{-1}

$\Rightarrow (a^{-1})^{-1} = a$

ii) ZZ: $b^{-1} \circ a^{-1}$ ist inv. zu $a \circ b$.

$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b$

$= b^{-1} \circ e \circ b = b^{-1} \circ b = e$. □

Beispiele für Gruppen:

1.) $(\mathbb{Z}, +)$ die Menge der ganzen Zahlen mit der Addition.
Neutrales El: 0
Inverses zu n ist $-n$.
Genauso: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

2.) $(\mathbb{R}^\times, \cdot)$, wobei $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
Neutr. El: 1
Inverses zu $a \in \mathbb{R}^\times$ ist $1/a$.
Genauso: $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$

3.) $(\{\pm 1\}, \cdot)$ ist Gruppe mit 2 Elementen
Gruppentafel:

$\cdot$	1	-1
1	1	-1
-1	-1	1

4) Sei M Menge,
$S(M) = \{ f: M \to M, \ f \text{ bijektiv} \}$
= Menge der bij Abb $M \to M$
$S(M) \times S(M) \to S(M)$, $(f, g) \mapsto f \circ g$
Komposition von Abbildungen
$(S(M), \circ)$ ist Gruppe.
Neutrales Element: $\mathrm{id}_M : M \to M$, $m \mapsto m$
Inverses El zu f ist f^{-1} (Umkehrabb).

Die Gruppen in 1-3 sind kommutativ.
4) im allg. nicht. (Bew: Übung)

§2 Permutationen

Typ 4 von oben ist insbesondere interessant, wenn

$$M = M_n := \{1, \dots, n\}, \quad (n \in \mathbb{N}).$$

Def: $S_n := S(M_n)$, die Menge der bijektiven Selbstabbildungen von M_n (Permutationen von M_n), mit der Komp als Verknüpfung, heißt Symmetrische Gruppe n-ten Grades.

Schreibweise: $\sigma \in S_n$ stellt man häufig durch ein Schema der Form

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

dar.

Bsp: $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$ ist die Permutation von $\{1,2,3\}$, die 1 auf 3, 2 auf 2 und 3 auf 1 abbildet.

Bsp: $S_1 = \{(id)\}$

$S_2 = \{\begin{pmatrix}1&2\\1&2\end{pmatrix}, \begin{pmatrix}1&2\\2&1\end{pmatrix}\}$

$S_3 = \{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\}$

Bem 1: Die Anzahl der Elemente von S_n ist $n! = n\cdot(n-1)\cdot\ldots\cdot 2\cdot 1$.

Bew: Übung.

Def: Eine Permutation $\tau \in S_n$ heißt Transposition, falls es $i,j \in \{1,\ldots,n\}$ mit $i \neq j$ gibt, so daß

$$\tau(i) = j\,,\quad \tau(j) = i\,,$$
$$\tau(k) = k \quad \forall\, k \neq i,j\,.$$

Bem 2: Es gibt $\binom{n}{2}$ Transpositionen in S_n.

Lemma 3: Sei $n \in \mathbb{N}$, $n \geq 2$. Jede Permutation $\sigma \in S_n$ läßt sich als Produkt von endl. vielen Transpositionen schreiben,

$$\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_m\,.$$

Bew: Induktion nach n.

$n=2$: $S_2 = \{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \}$ Beh. ist klar.

$n>2$: Die Beh. sei bewiesen für n. Wir zeigen, daß sie dann auch für $n+1$ gilt.

Sei $\sigma \in S_{n+1}$.

1. Fall: $\sigma(n+1) = n+1$.

Dann permutiert σ die Ziffern $1, \dots, n$, und definiert damit ein Elt von S_n. ($\sigma' = \sigma|_{M_n}$)
Nach Induktionsvoraussetzung ist σ' ein Produkt von Transp. aus S_n.
Dies liefert Darst von σ als Produkt von Transp.

2. Fall: $\sigma(n+1) \neq n+1$.

Sei $\tau \in S_{n+1}$ die Transposition, die $n+1$ und $\sigma(n+1)$ vertauscht.
Sei $\tilde{\sigma} = \tau \circ \sigma \in S_{n+1}$.
Es gilt $\tilde{\sigma}(n+1) = n+1$.
Nach 1. ist $\tilde{\sigma}$ Produkt von Transp.
$\Rightarrow$ Beh.

□

Die Darst. von σ als Produkt von Transp. ist nicht eindeutig. Bsp: Ist $\tau \in S_n$ Transp, so gilt $\tau^2 = id \Rightarrow \tau^{2n} = id$ usw.
Es gilt aber:

Satz 4: Sei $n \geq 2$, $\sigma \in S_n$. Sei

$$\sigma = \tau_1 \circ \dots \circ \tau_m \qquad (*)$$

eine Darstellung von σ als Produkt von Transpositionen. Setze

$$\operatorname{sgn}(\sigma) := (-1)^m \in \{\pm 1\}.$$

Dann ist $\operatorname{sgn}(\sigma)$ unabhängig von der Wahl der Darst. in $(*)$.

Folg: Es gibt eine eindeutig bestimmte Abb

$$\operatorname{sgn} : S_n \to \{\pm 1\}, \text{ so daß}$$

i) $\operatorname{sgn}(\sigma \circ \sigma') = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma') \quad \forall \sigma, \sigma' \in S_n$

ii) $\operatorname{sgn}(\tau) = -1 \quad \forall$ Transpositionen $\tau \in S_n$.

Bew von Satz 4:

Idee: Finde Formel für $\operatorname{sgn}(\sigma)$, die nicht von der Darst in $(*)$ abhängt.

Definiere dann

$$\Delta : \mathbb{Z}^n \to \mathbb{Z}, \quad \Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

Ist τ Transposition, so gilt

$$\Delta(x_1, \dots, x_n) = -\Delta(x_{\tau(1)}, \dots, x_{\tau(n)})$$

($\binom{n}{2}$ Faktoren)

~~Somit $\sigma, \sigma' \in S_n$, so gilt~~

Es folgt: Ist $\tau = \tau_1 \circ \dots \circ \tau_m$ Produkt

von Transpositionen, so gilt

$$\Delta(x_{\sigma(1)},\dots,x_{\sigma(n)}) = (-1)^m \Delta(x_1,\dots,x_n).$$

Es folgt $\operatorname{sgn}(\sigma) = (-1)^m = \dfrac{\Delta(\sigma(1),\dots,\sigma(n))}{\Delta(1,\dots,n)}$

↑ unabh. von Dart. □

Def: $\sigma \in S_n$ heißt gerade, falls $\operatorname{sgn}(\sigma) = +1$, ungerade, falls $\operatorname{sgn}(\sigma) = -1$.

Bsp:
$$\operatorname{sgn}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \operatorname{sgn}\left(\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right)$$
$$= +1 \quad \Rightarrow \text{gerade}.$$

§4 Körper

Def: Ein Körper ist ein Tupel $(K,+,\cdot)$ bestehend aus einer Menge K und zwei inneren Verknüpfungen $+$ und $\cdot$ (Addition u. Multiplikation), so dass gilt:

K1: $(K,+)$ ist abelsche Gruppe
(Ihr neutr. El. wird mit 0 bez.)

K2: $(K^\times,\cdot)$ ist abelsche Gruppe, wobei $K^\times = K\setminus\{0\}$
(Ihr neutr. El. wird mit 1 bez.)
(Insbes. gilt $\forall a,b \in K^\times$, dass $a\cdot b \in K^\times$.)

K3: Distributivgesetze: $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$
[und $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$] $\forall a,b,c \in K$.