1 Grundlagen

1.1 Abbildungen

Die Gesamtheit aller Abbildungen einer Menge M in eine Menge N ist wieder eine Menge und wird mit $Abb(M,N)$ bezeichnet.

Definition 1. Seien M, N, K Mengen und $f: M \to N$, $g: N \to K$. Die Abb $g \circ f: M \to K, m \mapsto g(f(m))$ heißt die Komposition von f und g. Die Komposition kann man auch als Mengenabbildung auffassen:

$$\circ : Abb(M,N) \times Abb(N,K) \to Abb(M,K)$$
$$(f,g) \mapsto g \circ f.$$

Lemma 1. Seien I und M Mengen und es sei: $(M_i)_{i\in I}$ die Familie von (immergleichen) Mengen $M_i = M$ indiziert über $i \in I$. Dann existiert eine natürliche Bijektion

$$\Phi : Abb(I,M) \to^{\sim} \prod (M_i)_{i\in I} (= M^I).$$

Beweis. rechts: Tupel $(m_i)_{i\in I}, m_i \in M_i = M$ links: Abbildung $f: I \to M$. Eine solche Abbildung ist dadurch gegeben, dass man jedem $i \in I$ ein $m_i = f(i) \in M$ zuordnet. Wir definieren Φ durch die Zuordnung:

$$\Phi : f \in Abb(I,M) \mapsto (f(i))_{i\in I} \in \prod (M_i)_{i\in I}.$$

Da die Abb. f durch ihre Werte $f(i) \in M, i \in I$, gegeben ist, ist Φ injektiv.

Ist umgekehrt $(m_i) \in \prod M_i$ gegeben, so ist die Abbildung $f: I \to M, i \mapsto m_i \in M$ ein Urbild unter Φ. Daher ist Φ surjektiv. □

2 Gruppen, Ringe, Körper

2.1 Gruppen

Definition 2 (Verknüpfung)**.** Eine (binäre) Verknüpfung auf einer Menge M ist eine Abbildung:

$$* : M \times M \to M.$$

Definition 3 (Gruppe)**.** Eine Gruppe $(G, *, e)$ ist eine Menge G mit einer Verknüfung $*$ und einem (ausgezeichneten) Element $e \in G$, so dass:

1. $g * (h * k) = (g * h*) * k \ \forall g,h,k \in G$ (Assoziativität)
2. $e * g = g \ \forall g \in G$ ((Links)neutrales Element)
3. $\forall g \in G$: $\exists h \in G$: $h * g = e$ (Linksinverses)

Eine Gruppe heißt kommutativ oder abelsch wenn zusätzlich gilt:

1. $g * h = h * g \ \forall g,h \in G$

Beispiel 1.
1. $(\mathbb{Z}, +, 0)$ ist abelsche Gruppe
2. $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ sind abelsche Gruppen.
3. $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ ist eine abelsche Gruppe

4. $(\mathbb{R}_{>0}, \cdot, 1)$ ist abelsche Gruppe

Bemerkung 1. Menge der Restklassen:

$$\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \mathbb{Z}/n\mathbb{Z}.$$

$(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ ist eine abelsche Gruppe. Wie ist die Summe von Restklassen definiert?

Seien $A, B \in \mathbb{Z}/n\mathbb{Z}$. Vorschrift für „+".

1. Wähle „Vertreter" $a, b \in \mathbb{Z}$ von A, B, d.h. $a \in A$, $b \in B$.
2. bilde $a + b$ in $\mathbb{Z}$
3. $A + B =^{def} \overline{a+b}$, d.h. die Restklasse zu der $a + b$ gehört.

Damit diese Definition widerspruchsfrei ist (Sprich: „+" ist *wohldefiniert*) muss man nachweisen, dass das Ergebnis nicht von der Auswahl im ersten Schritt abhängt.

Beispiel 2. Die symmetrische Gruppe O_n

$$O_n := \text{die Menge aller bijektiven Abb.} \pi : \{1, \ldots, n\} \to \{1, \ldots, n\}.$$

(sogennante Permutationen)

$* = \circ$ Komposition von Abbildungen
$e = id_{\{1,\ldots,n\}}$
Wir schreiben Permutationen in der Form:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}.$$

Elementare Kombinationen: n Möglichkeiten für $\pi(1)$, $(n-1)$ Möglichkeiten, für $\pi(2)\ldots$, 1 Möglichkeit für $\pi(n)$.

$$\#O_n = n! \text{ (Fakultät)}.$$

Verifikation der Gruppenaxiome

1. $g * (h * k) = g \circ (h \circ k) = (g \circ h) \circ k = (g * h) * k$
2. $e * g = id * g = g$
3. Sei g eine Permutation und $h = g^{-1}$ die Umkehrabbildung. Dann gilt $h * g = g^{-1} \circ g = id = e$.

Für $n \geq 3$ ist σ_n nicht kommutativ.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 2 & 1 & 3 & 4 & \ldots \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 1 & 3 & 2 & 4 & \ldots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 2 & 3 & 1 & 4 & \ldots \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 1 & 3 & 2 & 4 & \ldots \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 2 & 1 & 3 & 4 & \ldots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 3 & 1 & 2 & 4 & \ldots \end{pmatrix}.$$

Satz 1. Sei $G = (G, *, e)$ eine Gruppe. Dann gilt für alle $g, h, k \in G$.

1. $g * h = g * k \implies h = k$ (Linkskürzung)
2. $g * h = k * h \implies g = k$ (Rechtskürzung)
3. $g * e = g$ (das (links)neutrale Element ist auch rechtsneutral)
4. aus $g * h = g$ oder $h * g = g$ für ein einziges $g \in G$, so folgt $h = e$
5. $\forall g \in G$: existiert ein eindeutig bestimmtes Element $g^{-1} \in G$ mit $g^{-1} * g = e = g * g^{-1}$.
6. Aus $h * g = e$ oder $g * h = e$ folgt $h = g^{-1}$.
7. $\left(g^{-1}\right)^{-1} = g \; \forall g \in G$

Beweis 1. Sei $g * h = g * k$.

Nach (G3) $\exists s \in G$, sodass $s * g = e$. Daher gilt $s * (g * h) = (s * g) * h = e * h = k$.
Analog: $s * (g * k) = (s * g) * k = e * k = k$ Daraus folgt: $h = k$. □

Beweis 3. Nach (G3) existiert $h \in G$ und $h * g = e$.

Es folgt $h * (g * e) = (h * g) * e = e * e = e = h * g$
Nach (1) folgt $g * e = g$ □

Beweis 5, Existenz. Sei $h \in G$ mit $h * g = e$ (ex. nach G3)

$h * (g * h) = (h * g) * h = e * h = h = h * e$
Durch Linkskürzung erhalten wir $g * h = e$. □

Beweis 2. Sei $g * k = h * k$. Sei $s \in G$ so dass $k * s = e$ (existenz nach 5).

$\implies (g * k) * s = g * (k * s) = g * e = g$, analog
$\implies (h * k) * s = h * (k * s) = h * e = h$
Daraus folgt $g = h$. □

Beweis 4. $g * h = g = g * e \implies h = e$, analog
$h * g = g = e * g \implies h = e$ □

Beweis 5 Eindeutigkeit und 6. Seien $h, h' \in G$ mit $h * g = e = h' * g$ Nach Rechtskürzung folgt $h = h'$.
Daher ist g^{-1}*eindeutig*. Sei $h \in G$ mit $g * h = e$. Wegen $g^{-1} * g = e$ folgt mit Linkskürzung, dass $h = g^{-1}$. □

Beweis 7. aus $g * g^{-1} = e$ folgt $\left(g^{-1}\right)^{-1} = g$ □

Bemerkung 2. $g, h \in G$, so gilt $(g * h)^{-1} = h^{-1} * g^{-1}$
Grund: $(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g * g^{-1} * h = h^{-1} * e * h = h * h^{-1} = e$.