Gruppen

Werkzeuge

Einführung in die Algebra
31.10.2005

Grundlegende Definitionen und Beispiele

Definition 1.2

Es seien **G** eine nichtleere Menge,
eine Abbildung **T** : G x G → G
und e ∈G ein Element.
Man nennt (G, **T**,e) eine **Gruppe**, wenn gilt

G1) ist **assoziativ**,

$$\forall\ a,b,c \in G: (aTb)\,Tc = aT\,(bTc)$$

G2) e ist ein **neutrales Element**:

$$\forall\ a \in G: eTa = aTe = a$$

G3 Alle Elemente haben ein **Inverses**,

$$\forall\ a \in G\ \exists\ a^{-1} \in G : aT\,a^{-1} = a^{-1}Ta = e$$

Grundlegende Definitionen und Beispiele

G ist die *Trägermenge* der Gruppe,

*** die *Gruppenoperation*.**

Ist die Gruppenoperation kommutativ,

so spricht man von einer

kommutativen oder *Abelschen* Gruppe**.**

Grundlegende Definitionen und Beispiele

Beispiele für Gruppen sind

- die ganzen Zahlen mit der Addition, $(\mathbb{Z}, +, 0)$
- rationalen Zahlen ohne Null mit der Multiplikation $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$
- Für jede nichtleere Menge M ist die Menge

$$S(M) := \{f : M \to M \mid f \text{ bijektiv}\}$$

aller bijektiven Selbstabbildungen mit der Abbildungskomposition eine Gruppe. S(M) heißt die **symmetrische Gruppe** auf M,

ihre Elemente heißen ***Permutationen* von M**.

Gruppen

$\forall \exists \{ \} | \in$

Definition **(S_n):**

S_n bezeichne die Menge aller Permutationen der Menge $N_n = \{1, 2, \ldots, n\}$, d.h. die Menge der bijektiven Abbildungen von N_n.

S_n heißt symmetrische Gruppe.

$\pi \in S_n$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \pi[1] & \pi[2] & \pi[3] & \ldots & \pi[n-1] & \pi[n] \end{pmatrix}$$

Symmetrische Gruppe

Für $N_2 = \{1, 2\}$ erhält man S_2 mit

$S_2 = \{ id, \pi \}$ mit

$$Id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \pi = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Gruppen

Für einen Vektorraum wird die Menge

$$GL(V) := \{f : V \rightarrow V \mid f \text{ Isomorphismus}\}$$

aller bijektiven linearen Abbildungen von V in V mit der Abbildungskomposition zu einer Gruppe , der ***allgemeinen linearen Gruppe*** von V .

Notation

Seien $x, y \in G$ zwei Gruppenelemente und $1 \leq k \in \mathbb{N}$, dann definieren wir

$$\begin{aligned} x^k &:= x\,x \ldots x \quad (k-\text{mal}) \\ x^0 &:= e \\ x^{-k} &:= x^{-1}x^{-1} \ldots x^{-1} \quad (k-\text{mal}) \\ x^y &:= y\,x\,y^{-1} \\ [x,y] &:= xy\,(yx)^{-1} \end{aligned}$$

Und damit gelten dann für beliebige $x, y, z \in G$ und $k \in \mathbb{Z}$ die Rechenregeln

$$\begin{aligned} (x^{-1})^{-1} &= x \\ (xy)^{-1} &= y^{-1}x^{-1} \\ (x^y)^z &= x^{zy} \\ y^x &= [x,y]\,y \\ xy &= [x,y]\,yx \\ [x,y]^{-1} &= [y,x] \\ [x,y]^z &= [x^z, y^z] \\ xy = yx &\iff [x,y] = e \\ xy = yx &\implies (xy)^k = x^k y^k \end{aligned}$$

Kürzen in einer Gruppe

Lemma 1.2.4 (Kürzen in einer Gruppe).

In einer Gruppe folgt aus

a*x = a*y schon x = y und ebenso folgt aus

x*b = y*b schon x = y.

Beweis.

Wir multiplizieren (oder, allgemeiner, verknüpfen) unsere erste Gleichung von links mit dem Inversen von a, und die zweite von rechts mit dem Inversen von b.

Gruppenhomomorphismus $\forall \exists \{ \} | \in$

Definition

Seien G und G´ zwei Gruppen, wobei die jeweiligen neutralen Elemente mit e $\in$ G bzw. mit f $\in$G bezeichnet seien.

Ist φ : G → G´ eine Abbildung, dann nennen wir φ einen **Gruppenhomomorphismus**, falls sie die folgende Bedingung erfüllt

$$\forall \, x; y \in G \text{ gilt } \varphi(xy) = \varphi(x)\,\varphi(y)$$

und in diesem Fall erfüllllt φ sogar die beiden weiteren Eigenschaften

$$\varphi(e) = f \text{ und } \varphi(x^{-1}) = \varphi(x)^{-1}$$

Gruppenhomomorphismen

Definition

Seien G,G` Gruppen.

1. Ist φ : G → G´ eine Abbildung, dann nennen wir φ einen **Gruppenhomomorphismus**, falls sie die folgende Bedingung erfüllt

$$\forall\ \mathbf{x; y} \in \mathbf{G\ gilt\ } \varphi(xy) = \varphi(x)\,\varphi(y)$$

2. Ein injektiver Gruppenhomomorphismus heißt auch **Monomorphismus**.

(Cf. griechisch **μονος einzig**, z.B. der Monarch als Alleinherrscher.)

3. Ein surjektiver Gruppenhomomorphismus heißt auch **Epimorphismus**.

(Cf. griechisch **επι darauf**, z.B. das Epizentrum eines Erdbebens, das auf der Erdoberfläche ¨uber dem Zentrum im Erdinneren liegt.)

Gruppenhomomorphismen

4. *Ein bijektiver Gruppenhomomorphismus heißt auch Isomorphismus. (Cf. griechisch ίσος derselbe, z.B. das Iso-top als Element am selben Platz im Periodensystem.)*

5. *Zwei Gruppen heißen isomorph genau dann, wenn es zwischen ihnen einen Isomorphismus gibt.*

6. *Ein Gruppenhomomorphismus einer Gruppe in sich selbst heißt auch Endomorphismus. (Cf. griechisch ενδο in hinein, z.B. die Endo-skopie, bei der man in den Körper hinein schaut.)*

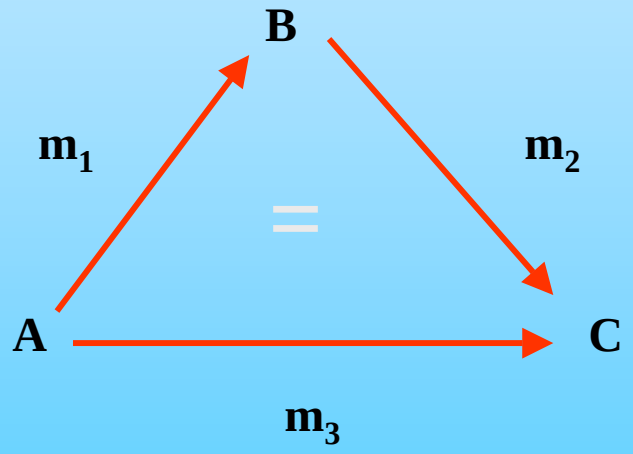
Kategorientheorie

Die Kategorientheorie**, oder kategorielle Algebra, ist ein Zweig der Mathematik, der sich Anfang der 1940er Jahre zuerst im Rahmen der Topologie entwickelte.** MacLane **nennt seine 1945 gemeinsam mit Eilenberg entstandene »**General Theory of Natural Equivalences**« (in** *Trans. Amer. Math. Soc.*, 58**, 1945) die erste explizit kategorientheoretische Arbeit. Die Grundbegriffe dieser Arbeit sind** Kategorie**,** Funktor **und** natürliche Transformation**. Um den letzteren Begriff zu präzisieren, wurden die anderen eingeführt.**

Die Kategorientheorie kann verstanden werden als ein "Jargon" zum Ausdrücken verschiedener mathematischer Theorien. Viele Theorien betrachten Mengen mit einer zusätzlichen Struktur, z.B. eine Topologie, eine Ordnung oder eine oder mehrere Verknüpfungen (Gruppe, Ring, Algebra). Dazu werden häufig Abbildungen zwischen solchen Objekten untersucht, die diese Struktur "respektieren": z.B. stetige, monotone oder lineare Funktionen. Die Kategorientheorie betrachtet nun nur die Begriffe "Objekt" und "Abbildung", sie abstrahiert also von der konkreten Struktur. Dadurch ermöglicht sie es, Beweistechniken, Konzepte und Ergebnisse unterschiedlicher Teildisziplinen der Mathematik zusammen zu führen. Zudem erleichtern die übergeordneten Begriffe das Erlernen neuer Theorien.

Kategorientheorie

Die Kategorientheorie versucht, Strukturen und Konzepte einzelner mathematischer Teildisziplinen nur mit Objekten und Morphismen auszudrücken. Die dabei entstehenden verallgemeinerten Begriffe sind **universal**, d.h. für eine Vielzahl von Kategorien verfügbar.



$$m_3 = m_2 \circ m_1$$

Ein Hauptwerkzeug für die Definition universaler Konstrukte sind **Limiten**, **Colimiten und adjungierte Funktoren.**

A1 Mengentheoretische Beschreibung (Peano):
Die natürlichen Zahlen bilden eine Menge N mit folgenden Eigenschaften

1. $\exists\, \mathsf{zero} \in \mathbb{N}$
2. $\forall\, n \in \mathbb{N},\ \exists\, \mathsf{succ}\, n \in \mathbb{N}$
3. $\forall\, n \in \mathbb{N},\ \mathsf{succ}\, n \neq \mathsf{zero} \in \mathbb{N}$
4. $\forall\, n, m \in \mathbb{N},\ \mathsf{succ}\, n = \mathsf{succ}\, m \Longrightarrow n = m\ (injectivity)$
5. $\forall\, A \subseteq \mathbb{N}\ (\mathsf{zero} \in A \wedge a \in A \Longrightarrow \mathsf{succ}\, a \in A) \Longrightarrow A = \mathbb{N}$

Kategorielle Beschreibung der natürlichen Zahlen*

Eine Menge N zusammen mit 2 Abbildungen

$$1 \xrightarrow{0} N \xrightarrow{s} N$$

heißt **Menge der natürlichen Zahlen**, wenn zu jeder anderen Menge X mit 2 Abbildungen

$$1 \xrightarrow[e]{} X \xrightarrow[g]{} X$$

es genau eine Abbildung f: N → X gibt, so dass folgende Diagramme kommutativ sind:

$$\begin{array}{ccccc} 1 & \xrightarrow{0} & N & \xrightarrow{s} & N \\ {\scriptstyle id_1}\downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ 1 & \xrightarrow[e]{} & X & \xrightarrow[g]{} & X \end{array}$$

1 = einelementige Menge

* Lawvere 1960

Kategorie

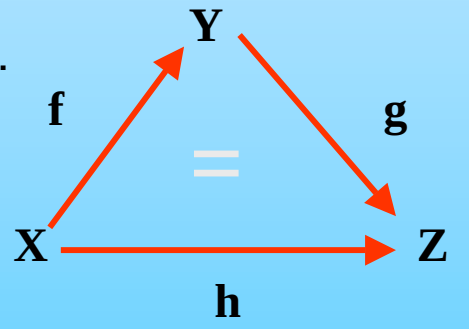
Eine Kategorie C **ist durch folgende Daten gegeben:**

Kat 1) Eine Klasse O(C) (= Objekte der Kategorie).

Kat 2) Zu jedem Paar X,Y von Objekten eine Menge Mor(X,Y),
(= Morphismen von X nach Y)

Schreibweise: $f \in Mor(X,Y) = f: X \rightarrow Y$.

Statt Mor(X,Y) schreibt man auch MorC(X,Y) oder auch C(X,Y).



h = g o f

Kat 3) Komposition von Morphismen

$Mor(X,Y) \times Mor(Y,Z) \rightarrow Mor(X,Z)$;

(f,g) → gf (oder g o f) notiert.

Kat 4) Dabei müssen folgende Axiome erfüllt sein:

4.1(Assoziativität) Sind Morphismen $f: X \rightarrow Y$, $g: Y \rightarrow Z$, $h: Z \rightarrow A$ gegeben, so gilt
$(hg)f = h(gf)$.

4.2 (Identitäten) Zu jedem Objekt X gibt es einen Morphismus idX in Mor(X,X) mit
fo idX = f und id o Xg für und alle Morphismen $f: X \rightarrow Y$ und $g: W \rightarrow X$.

Beispiele von Kategorien

Die Kategorie Men der Mengen
OBJEKTE: Mengen MORPHISMEN: Abbildungen

Die Kategorie Grp der Gruppen
OBJEKTE: Gruppen MORPHISMEN: Gruppen-Homorphismen

Die Kategorie Ab der abelschen Gruppen
OBJEKTE: Abelsche Gruppen MORPHISMEN: Gruppen-Homorphismen

Die Kategorie k-Vekt der Vektorräume **(über einem festen Körper k)**
OBJEKTE: k-Vektorräume MORPHISMEN: k-lineare Abbildungen

Die Kategorie Ring der Ringe
OBJEKTE: Ringe MORPHISMEN: Ring-Homorphismen

Die Kategorie Top der topologischen Räume
OBJEKTE: topologische Räume MORPHISMEN: stetige Abbildungen

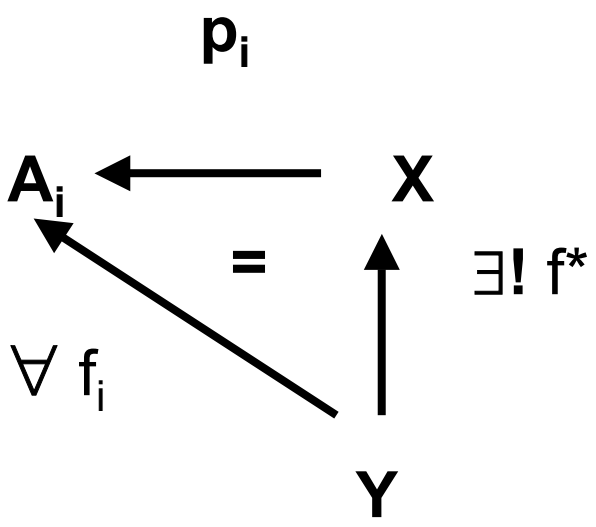
Produkte in Kategorien

Sei $(A_i, i \in \mathbf{I})$ **eine Familie von Objekten in einer Kategorie C.**

Ein Objekt X zusammen mit einer Familie von Morphismen p_i: X → A_i heißt Produkt der $(A_i, i \in \mathbf{I})$, wenn folgendes gilt:

Zu jedem Objekt Y und jeder Familie von Morphismen $f_i : Y \rightarrow A_i$ existiert genau ein Morphismus $f^*: Y \rightarrow X$ mit

$$p_i^* \, f^* = f_i$$



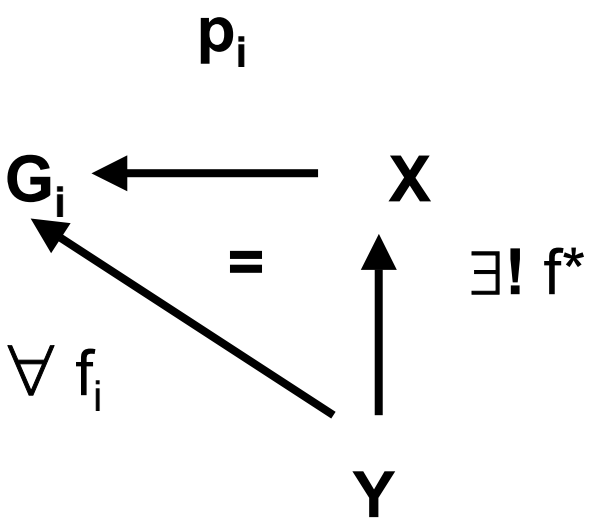
Beispiel
Produkt von Gruppen

Sei $(G_i, i \in I)$ **eine Familie von Gruppen.**

Eine Gruppe X zusammen mit einer Familie von Gruppenhomomorphismen p_i: X → G_i heißt **Produkt** der $(G_i, i \in I)$, **wenn folgendes gilt:**

Zu jeder Gruppe Y und jeder Familie von Gruppenhomomorphismen $f_i : Y \rightarrow G_i$ existiert genau ein **Gruppenhomomorphismus** $f^*: Y \rightarrow X$ mit

$$p_i^* \, f^* = f_i$$



Produkte in Gruppen

Seien $(G_i, i \in I)$ **eine Familie von Gruppen.**

Dann ist $\prod G_i$ **:=** $\{ (g_i ; i \in I) \mid g_i \in G_i$ für alle $i \in I\}$ **=: mit der komponentenweisen Verknüpfung**

g := $(g_i ; i \in I)$ **und h:=** $(h_i ; i \in I) \in \prod G_i$

g*h := $(g_i * h_i ; i \in I)$ **eine Gruppe.**

Es gelten:

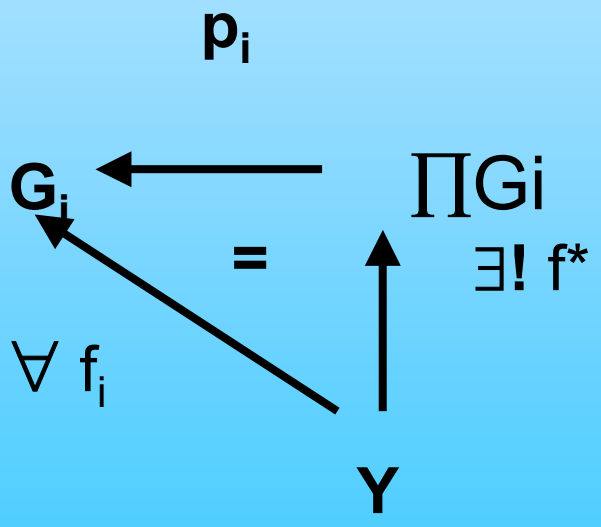
1) **Inverse:**
   g := $(g_i ; i \in I) \in \prod G_i \rightarrow$ **g^{-1}:=** $(g_i^{-1} ; i \in I) \in \prod G_i$
2) **Einselement:**
   e:= $(e_i ; i \in I)$ **;** $e_i \in G_i$ Einselement **in** G_i
3) $p_j: \prod G_i \rightarrow G_j$ $(g_i ; i \in I) \rightarrow g_j$ heißt j-te Projektion

Universelle Eigenschaft von Produkten

Zu jeder Gruppe Y und jeder Familie von Gruppenhomorphismen

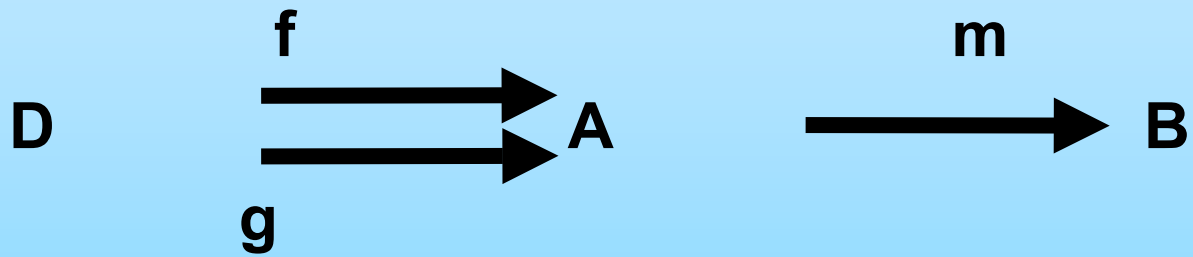
$f_i : Y \rightarrow G_i$ existiert genau ein Morphismus $f^*: Y \rightarrow \prod G_i$ mit

$$\mathbf{p_i}^* f^* = f_i$$



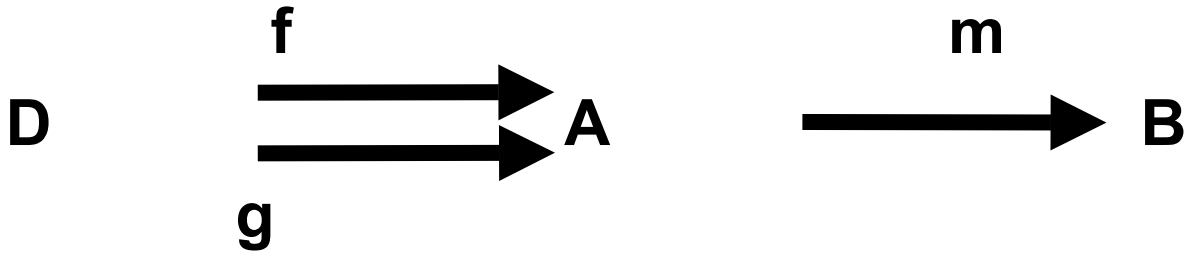
$$\forall\, y \in Y;\ f^*(y) := (f_i(y)\ ;\ i \in \mathbf{I})$$

Typen von Morphismen
- Monomorhpismus -



Def. **m ist ein** Monomorphismus **wenn gilt**

m o f = m o g impliziert f=g,.



∀∃{}|∈

Lemma. Sei Men (Grp,..) die Kategorie der Mengen (Gruppen,..). Sei m: A → B. Dann gilt:

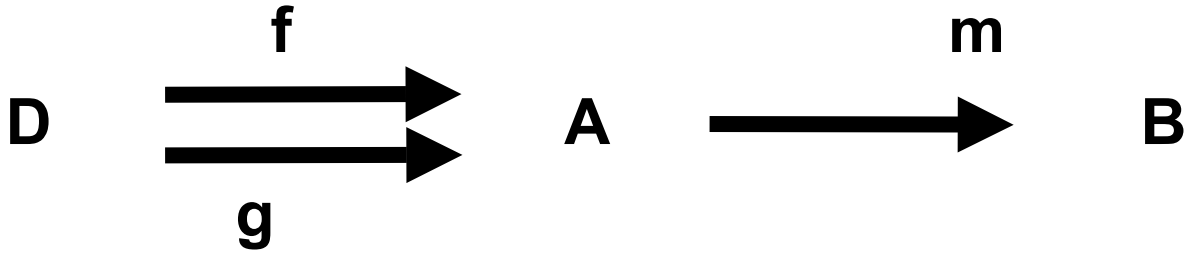
(Für alle Morphismen f,g gilt:

m o f = m o g impliziert f=g) ⟺ m injektiv ist,.

Beweis.

⟸: Sei m injektiv u. $f, g: D \to A$ mit $mf = mg$

$\Rightarrow \forall_{x \in D}\ mf(x) = mg(x) \Rightarrow \forall_{x \in D}\ f(x) = g(x) \Rightarrow f = g$



Lemma. Sei Men (Grp,..) die Kategorie der Mengen (Gruppen,..). Dann gilt:

∀ Morphismen f,g gilt:

m o f = m o g impliziert f=g genau dann wenn m injektiv ist,.

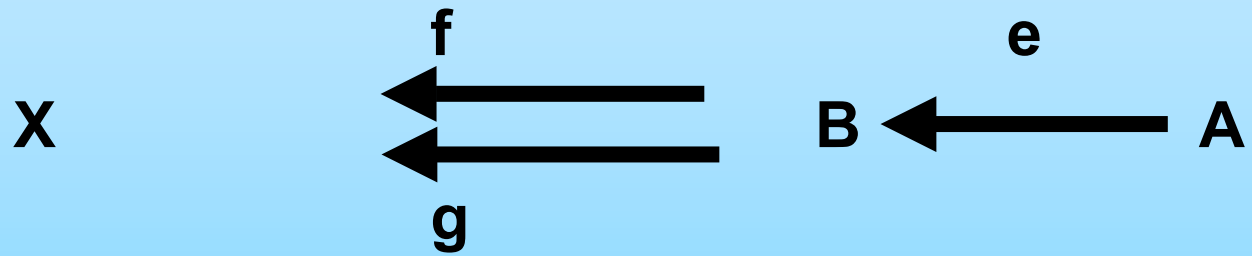
Beweis „⇒"

Seien $a, a' \in A$ m. $m(a) = m(a')$.

Definiere $D := \{1\}$ m. $f, g : D \to A$ durch $f(1) = a, g(1) = a'$

$\Rightarrow m(a) = m \circ f(1) = m g(1) \Rightarrow f = g \Rightarrow a = a'$ ∎

Typen of Morphismen
- Epimorphismus -



Def. **e ist ein Epimorphismus wenn gilt**

f o e = g o e impliziert f=g,.

Gruppen

DEFINITION
Wir nennen H eine **Untergruppe** der Gruppe $(G, \circ)$, falls erfüllt sind

- $\emptyset \neq H \subseteq G$ ist eine nicht-leere Teilmenge
- $\forall\, x, y \in H$ gilt $xy \in H$ multiplikativ abgeschlossen
- $\forall\, x \in H$ gilt $x^{-1} \in H$ invers abgeschlossen

Und eine Untergruppe H von G heisst ein **Normalteiler** von G falls weiterhin eine der folgenden drei äquivalenten Aussagen erfüllt ist

(a) $\forall\, x \in G$ gilt $xH = Hx$

(b) $\forall\, x \in G$ gilt $H^x = H$ mit $H^x := \{xhx^{-1};\, h \in H\} = \{h^x;\, h \in H\}$

(c) $\forall\, x \in G$ gilt $H^x \subseteq H$

Gruppen

Schreibweise

U ist eine Untergruppe von G:

$$U \leq_g G$$

N ist ein Normalteiler von G:

$$N \leq_n G$$