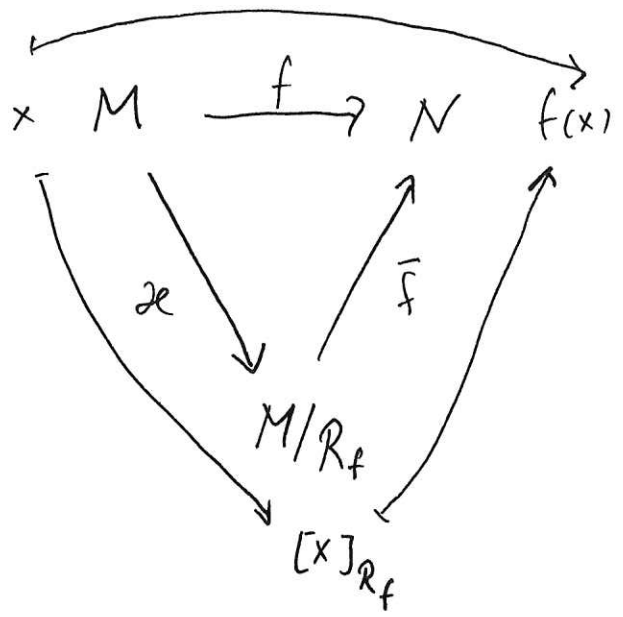
Wiederholung

- Äquivalenzrelationen, ÄR R, S, T
  - M Menge, $\sim$ ÄR $\Rightarrow$ $M/\sim \; = \{ [x]_\sim \mid x \in M \}$
    $M/\sim$ Partition von M
  - $\{ \sim$ ÄR auf $M \}$ $\xrightarrow{\text{bijektiv}}$ $\{P$ Partion von $M\}$
    $\sim \longmapsto M/\sim$



$R_f : \quad x \, R_f \, x' \iff f(x) = f(x')$

$\bar{f}([x]_{R_f}) := f(x)$

$\bar{f}$ ist injektiv

$f = \bar{f} \circ \pi$

M Glasperlen, N Farben

$f(x)$:= Farbe von x

M/R_f Menge der Farbklassen

- Ordnungen RAT

  Präordnung R T

  Totalordnung: RAT mit: für alle $x, y \in M$: $x \leq y$ oder $y \leq x$

  Präordnung $\leq$: $x \sim y :\Leftrightarrow x \leq y$ und $y \leq x$

  z.B. $\mathbb{Z}$, $|$ teilbarkeit

- - x <u>minimal</u> (maximal): ($\leq$ Ordnung auf M)

  $y \leq x \Rightarrow y = x$ ($x \leq y \Rightarrow x = y$)

  - x <u>kleinster</u> Element (größter)

  $x \leq y$ für alle $y \in M$ ($y \leq x$ für alle $y \in M$)

  - x kleinster & größter $\Rightarrow$ x minimal (maximal)
  - <u>Falls</u> kleinster (größter) Element ex.: min M, (max M)

Algebraische Strukturen

Verknüpfungen

Motivation

Rechenregeln in $\mathbb{N}_0$

Für alle $x, y, z \in \mathbb{N}_0$ gilt:

- $x + (y + z) = (x + y) + z$
- $0 + x = x$
- $x + y = y + x$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $1 \cdot x = x$
- $x \cdot y = y \cdot x$

Die Operationen $+$ und $\cdot$ sind Beispiele für *Verknüpfungnen*.

Verknüpfungen (Forts.)

Definition

M Menge

Verknüpfung auf M: Abbildung $\bullet\colon M \times M \to M$

Notation:

- für $x, y \in M$: $\quad x \bullet y := \bullet(x, y)$

Verknüpfungen (Forts.)

Beispiele

- auf $\mathbb{N}_0$: $+ : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0, \ (x,y) \longmapsto x+y$,
- auf $\mathbb{Z}$: $+, \cdot, - : (x,y) \longmapsto x-y$
- auf $\mathbb{Q}$: $+, \cdot, -$
- auf $\mathbb{Q} \setminus \{0\}$: : geteilt durch $(x,y) \longmapsto x:y = \frac{x}{y}$

Verknüpfungen (Forts.)

Definition

M Menge, $\bullet$ Verknüpfung auf M

- $\bullet$ *assoziativ*: für alle $x, y, z \in M$:

$$x \bullet (y \bullet z) = (x \bullet y) \bullet z$$

- $\bullet$ *kommutativ*: für alle $x, y \in M$:

$$x \bullet y = y \bullet x$$

Verknüpfungen (Forts.)

Definition

M Menge, $\bullet$ Verknüpfung auf M

neutrales Element bzgl. $\bullet$: $e \in M$ so, dass für $x \in M$:

$$e \bullet x = x \bullet e = x$$

Bemerkung

M Menge, $\bullet$ Verknüpfung auf M

es gibt höchstens ein neutrales Element bzgl. $\bullet$

Beweis: Seien e, e' neutrale Elemente bzgl. $\bullet$

$\Rightarrow \quad e = e \bullet e' = e'$.

Verknüpfungen (Forts.)

Definition

M Menge, $\bullet$ Verknüpfung auf M, e neutrales Element bzgl. $\bullet$
$x \in M$

- *linksinverses Element* zu x bzgl. $\bullet$: $y \in M$ mit

$$y \bullet x = e$$

- *rechtsinverses Element* zu x bzgl. $\bullet$: $y \in M$ mit

$$x \bullet y = e$$

- *inverses Element* zu x bzgl. $\bullet$: $y \in M$ mit

$$y \bullet x = e = x \bullet y$$

Verknüpfungen (Forts.)

Bemerkung

M Menge

• assoziative Verknüpfung auf M, e neutrales Element bzgl. •
$x \in M$

es gibt höchstens ein inverses Element zu x bzgl. •

Seien x', x'' inverse Elemente zu x.

$$\Rightarrow x' = x' \bullet e = x' \bullet (x \bullet x'') = (x' \bullet x) \bullet x'' = e \bullet x'' = x''.$$

Monoide

Definition

- *Monoid*: besteht aus $(M, \bullet)$
  - M Menge
  - $\bullet$ assoziative Verknüpfung auf M
  - e, neutrales Element bezgl. $\bullet$

Missbrauch von Notation: notiere Monoid wieder als M

Terminologie und Notationen:

- *Multiplikation* von M: $\bullet$
  Notation: $\cdot$ (Verknüpfungszeichen weggelassen)

$x \cdot y \quad xy$

- M Monoid

M heißt *abelsch* (oder *kommutativ*): $\cdot$ ist kommutativ

Monoide (Forts.)

Axiome in Standardnotation

- Monoid M:
  - für $x, y, z \in M$: $x(yz) = (xy)z$ AG
  - es ex. $e \in M$ so, dass für $x \in M$: ~~$ex = e = xe$~~
    $ex = x = xe$ NE
    $1x = x = x1$ NE
- Abelsches Monoid M:

  Zusätzlich:
  - für $x, y \in M$: $xy = yx$ KG

Wir sagen auch: M ist *multiplikativ geschrieben*.

Bei multiplikativer Schreibweise benutzt man oft das Zeichen 1 für das neutrale Element e. Für $x \in M$ und $n \in \mathbb{N}$ schreibt man auch $x^n := x \cdot x \cdot \cdots \cdot x$ (n Faktoren).

Monoide (Forts.)

Bei einem abelschen Monoid M benutzt man oft das Zeichen $+$ für die Verknüpfung.

Wir sagen auch: M ist *additiv geschrieben*.

In diesem Fall schreibt man meistens 0 für das neutrale Element. Für $x \in M$ und $n \in \mathbb{N}$ schreibt man auch $nx := x + x + \cdots + x$ (n Summanden).

Axiome in Standardnotation

- für $x, y, z \in M$: $x + (y + z) = (x + y) + z$ AG
- es ex. $0 \in M$ so, dass für $x \in M$: $0 + x = x = x + 0$ NE
- für $x, y \in M$: $x + y = y + x$ KG

Monoide (Forts.)

Beispiele

- $\mathbb{N}$ mit üblicher Addition: [Halbgruppe] Kein Monoid, da kein NE bzgl. +
- $\mathbb{N}$ mit üblicher Multiplikation: Monoid
- $\mathbb{N}_0$ mit üblicher Addition: Monoid
- $\mathbb{N}_0$ mit üblicher Multiplikation: Monoid

alle abelsch

- $\mathbb{Z}$ mit üblicher Addition: "

Monoide (Forts.)

Beispiel

nicht-kommutatives Monoid mit genau drei Elementen:

$M = \{1, c_1, c_2\}$

$\cdot$	1	c_1	c_2
1	1	c_1	c_2
c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2

Multiplikationstafel $\quad x \cdot y$ Zeile zu x, Spalte zu y

Für AG: Beweise $c_1 \cdot x = c_1 \;\forall x \in M$, $c_2 \cdot y = c_2 \;\forall y \in M$.

Wortmonoid

Definition
A Menge

Alphabet z.B. $\{a, b, \ldots, z\}$

- Für $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ nennen wir

$$a_1 a_2 \cdots a_n \qquad \text{emil}$$

ein *Wort der Länge n über A*. Länge 0: ε leeren Wort

- $A^* := \{w \mid w \text{ ist Wort der Länge } n \text{ über } A, n \in \mathbb{N}_0\}$.
  A^* enthält das Wort ϵ der Länge 0.
- Für zwei Wörter $v := a_1 \cdots a_n$ und $w := b_1 \cdots b_m$ über A sei

$$v * w := a_1 \cdots a_n b_1 \cdots b_m$$

die *Verkettung* oder *Konkatenation* von v und w.

- $(A^*, *)$ ist ein Monoid mit neutralem Element ϵ, das *Wortmonoid* über A.

$A = \emptyset$ $\qquad A^* = \{\varepsilon\}$

$A = \{a\}$ $\qquad A^* = \{\varepsilon, a, aa, aaa, \dots\}$

$= \{\varepsilon, a^n \mid n \in \mathbb{N}\} = \{a^n \mid n \in \mathbb{N}_0\}$

↑ Konvention $a^0 = \varepsilon$.

Bijektion: $\varphi : \mathbb{N}_0 \longrightarrow A^*, \quad n \mapsto a^n$

Es gilt: $\varphi(n+m) = \varphi(n)\,\varphi(m)$ $\qquad a^{n+m} = a^n a^m$

Abbildungsmonoid

Bemerkung

M Menge

$\mathrm{Abb}(M, M)$ ist Monoid mit Verknüpfung $(g, f) \mapsto g \circ f$

und neutralem Element id_M. Nach früheren Regeln für „$\circ$"

Bemerkung

Sei M Menge und $f \in \mathrm{Abb}(M, M)$.

- f besitzt Rechtsinverses $\Leftrightarrow$ f ist surjektiv.
- f besitzt Linksinverses $\Leftrightarrow$ f ist injektiv.
- f besitzt Inverses $\Leftrightarrow$ f ist bijektiv.

f hat Rechtsinversen $\Rightarrow$ f surjektiv

Bew.: Sei $g \in Abb(M,M)$ mit $f \circ g = id_M$

Sei $y \in M$.

$y = id_M(y) = (f \circ g)(y) = f(g(y))$. $\Rightarrow$ $g(y)$ ist Urbild von y unter f.

f besitzt Linksinversen $\Rightarrow$ f injektiv

Sei $g \in Abb(M,M)$ mit $g \circ f = id_M$.

Seien $x, x' \in M$ mit $f(x) = f(x')$.

Zu zeigen: $x = x'$. Haben:

$x = id_M(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = id_M(x') = x'$.

Invertierbare Elemente

Definition

- M Monoid, $x \in M$
  - x *invertierbar* in M: es gibt ein inverses Element zu x bzgl. $\cdot$
  - x invertierbar

  Inverse zu x in M: das zu x inverse Element y bzgl. $\cdot$
  Notation:
  - *Menge der invertierbaren Elemente* in M:

$$M^\times = \{x \in M \mid x \text{ invertierbar}\}$$

M multiplikativ geschrieben, x invertierbar: x^{-1} das Inverse von x

M additiv — " — , x " : $-x$ — " — von x

Invertierbare Elemente (Forts.)

Beispiel

- $\mathbb{N}_0{}^\times = \{1\}$ $\quad (\mathbb{N}_0, \cdot)^\times = \{1\}$
- 0 einziges invertierbare Element in $\mathbb{N}_0$ $\quad (\mathbb{N}_0, +)^\times = \{0\}$
- A Menge: $(A^*)^\times = \{\epsilon\}$

Proposition

M Monoid

- für $x, y \in M^\times$: $\quad xy \in M^\times$ mit $(xy)^{-1} = y^{-1}x^{-1}$
- $\quad 1 \in M^\times$ mit $1^{-1} = 1$
- für $x \in M^\times$: $\quad x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$

Beweis: - $(xy)\cdot(y^{-1}x^{-1}) = xyy^{-1}x^{-1} = x1x^{-1} = xx^{-1} = 1.$

$(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}1y = yy^{-1} = 1.$

- $x\cdot x^{-1} = x^{-1}x = 1 \Rightarrow$ x^{-1} ist invertierbar und

$(x^{-1})^{-1} = x$

Gruppen

Definition

- *Gruppe*:
  Monoid, in dem jedes Element invertierbar ist.
- *Abelsche Gruppe*:
  abelsches Monoid, in dem jedes Element invertierbar ist.

In einer Gruppe G gilt also: (1 NE)

Zu jedem $x \in G$ ex. $y \in G$ mit $xy = yx = 1$.

Gruppen (Forts.)

Beispiel

- $\mathbb{Z}$ mit üblicher Addition: Abelsche Gruppe
- $\mathbb{Z}$ mit üblicher Multiplikation: Keine Gruppe, z.B. ist 0 nicht invertierbar
- $\mathbb{Q}$ mit üblicher Addition: Abelsche Gruppe
- $\mathbb{Q}$ mit üblicher Multiplikation: Keine Gruppe, da 0 nicht invertierbar
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ Abelsche Gruppe
- $(\mathbb{R}_{>0}, \cdot)$ " "

Gruppen (Forts.)

Definition

A abelsche Gruppe

Subtraktion von A: Verknüpfung $(x, y) \mapsto x + (-y)$ auf A
Notation: $-$

$$x + (-y) =: x - y$$

I. A. nicht assoziativ $\quad 0 - (1 - 1) \neq (0 - 1) - 1$