2 Algebraische Strukturen

Nachträgliche Änderungen sind gelb markiert

Welche Eigenschaften von Zahlen werden benötigt, damit Abschnitt 1.1 funktioniert?

- Brauche $+, -, \cdot, /$.
- Brauche: $a+b = b+a$
  $(a+b)+c = a+(b+c)$ } analog für $\cdot$
  $a - a = 0$
  $a\cdot(b+c) = a\cdot b + a\cdot c$

$\rightsquigarrow$ „Körper"

2.1 Gruppen, Ringe, Körper

Def 2.1.1: (a) Eine Gruppe ist ein Tripel $(G, \circ, e)$, wobei:

- G ist eine Menge
- $\circ : G \times G \to G$ ist eine Verknüpfung
- $e \in G$

Verknüpfung: Abbildung, die zwei Argumente hat, wo das Symbol dazwischen geschrieben wird, also „$a \circ b$" statt „$\circ(a,b)$"

$G \times G$: das, was man in eine Fkt einsetzt

so dass gilt:

Gruppenaxiome:

(i) Assoziativität:
$$\forall a,b,c \in G: (a\circ b)\circ c = a \circ (b \circ c)$$

(ii) e ist neutrales Element:
$$\forall a \in G: (e \circ a = a \wedge a \circ e = a)$$

(iii) Existenz von inversen Elementen:
$$\forall a \in G: \exists b \in G: (a \circ b = e \wedge b \circ a = e)$$

(b) Die Gruppe $(G, \circ, e)$ heißt kommutativ (oder abelsch), wenn außerdem gilt:

(iv) Kommutativität:
$$\forall a,b \in G: a \circ b = b \circ a$$

Man sagt auch: „$(G, \circ)$ ist eine Gruppe" bzw „G ist eine Gruppe", wenn klar ist, was e (und $\circ$) sein soll.

Man nennt $(\circ, e)$ eine Gruppenstruktur auf G.

Konv. 0.5: Statt „eine Gruppe ist ein Tripel $(G, \circ, e)$" sage oft: „eine Grp. ist eine Menge G zusammen mit einer Verknüpfung $\circ$ und einem $e \in G$ ..."

Bsp. 2.1.2: (a) $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe. Wenn $\mathbb{Z}$ als Gruppe bezeichnet wird, ist $(\mathbb{Z}, +, 0)$ gemeint. Analog für $\mathbb{Q}, \mathbb{R}$.

(b) $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ ist eine abelsche Gruppe, die mit $\mathbb{Q}^\times$ bezeichnet wird. Analog: $\mathbb{R}^\times$

$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

Lemma 2.1.3: Sei G eine Gruppe und $a, a', b \in G$. Dann gilt:

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

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

Bsp: $x + 5 = y + 5 \Downarrow x = y$. Das funktioniert in beliebigen Gruppen.

Bew: (a) Wähle $b' \in G$ mit $b \circ b' = e$ (ex. nach (iii)) $(*)$

$$
\begin{array}{ccc}
a \circ b = a' \circ b \Rightarrow & (a \circ b) \circ b' & = (a' \circ b) \circ b' \\
& \| \ (i) & \| \ (i) \\
& a \circ (b \circ b') & a' \circ (b \circ b') \\
& \| \ (*) & \| \ (*) \\
& a \circ e & a' \circ e \\
& \| \ (ii) & \| \ (ii) \\
& a & a'
\end{array}
$$

Also $a = a'$.

(b) Analog. $\square$

Lemma 2.1.4: Sei G eine Gruppe. (a) $\forall a \in G \ \exists^{=1} b \in G: a \circ b = e$.

(b) $\forall a, b \in G: (a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Bew: (a) • Existenz von b: (iii)

• Eindeutigkeit: • Sei $b \in G$ ein Inverses von a.

• Annahme: $b' \in G$ mit $a \circ b' = e$. z.z: $b = b'$.

• Habe $b \circ a = e$ (nach Wahl von b)

Betrachte

$$
\begin{array}{ccc}
b \circ (a \circ b') & \overset{(i)}{=} & (b \circ a) \circ b' \\
\| & & \| \\
b \circ e & & e \circ b' \\
\| \ (ii) & & \| \ (ii) \\
b & & b'
\end{array}
$$

$\square$

(b) z.z: $\underbrace{(a \circ b) \circ (b^{-1} \circ a^{-1})}_{= a \circ b \circ b^{-1} \circ a \ = a \circ e \circ a^{-1} \ = a \circ a^{-1} \ = e} \overset{?}{=} e$ $\square$

Notn 2.1.5: Typische Notationen für Gruppen

Verknüpfung	neutr. Elem	Inverses von $a \in G$	Weitere Notation für $a,b \in G, n \in \mathbb{N}$
$\circ$	e	a^{-1}	$a^n := \underbrace{a \cdots a}_{n \text{ mal}}$
$+$	0	$-a$	$a-b := a+(-b)$
$\cdot$	1	a^{-1}	$\frac{a}{b} := a \cdot b^{-1}$ $a^n := \underbrace{a \cdots a}_{n \text{ mal}}$

Satz 2.1.6: (a) Sind $(G_1, \circ, e_1), \dots, (G_n, \circ, e_n)$ Gruppen, so ist auch $G_1 \times \dots \times G_n$ eine Gruppe mit der komponentenweisen Verknüpfung

$$(a_1, \dots, a_n) \circ (b_1, \dots, b_n) = (a_1 \circ b_1, a_2 \circ b_2, \dots, a_n \circ b_n)$$

und mit neutralem Elmt. $(e_1, \dots, e_n)$.

(b) Sind $G_1, \dots, G_n$ abelsch, so ist auch $G_1 \times \dots \times G_n$ abelsch.

Bsp: $\mathbb{R}^n$ vom Anfang der Vorlesung.

Bew: Zeige, dass $G_1 \times \dots \times G_n =: G$ die Gruppenaxiome erfüllt.

(i) z.z.: Für $\underline{a} = (a_1, \dots, a_n), \underline{b} = (b_1, \dots, b_n), \underline{c} = (c_1, \dots, c_n) \in G$:

$$(\underline{a} \circ \underline{b}) \circ \underline{c} \overset{?}{=} \underline{a} \circ (\underline{b} \circ \underline{c})$$

$$(\underline{a} \circ \underline{b}) \circ \underline{c} = (a_1 \circ b_1, \dots) \circ \underline{c} = ((a_1 \circ b_1) \circ c_1, \dots) = (a_1 \circ (b_1 \circ c_1), \dots) = \underline{a} \circ (b_1 \circ c_1, \dots) = \underline{a} \circ (\underline{b} \circ \underline{c})$$

Nach Assoziativität in $G_1, \dots G_n$.

(ii), (iii), abelsch: selbes Prinzip. $\square$

Notn 2.1.7: Ist G eine Gruppe so wird G^n als Gruppe mit der komponentenweisen Verknüpfung; diese wird mit dem gleichen Symbol wie die Verknüpfung von G geschrieben.

Bsp: $(\mathbb{R}, +)$ ist Gruppe $\rightsquigarrow$ $(\mathbb{R}^n, +)$ ist Gruppe

Def 2.1.8: Ein Ring ist eine Menge R mit zwei Verknüpfungen

$$+ : R \times R \longrightarrow R, \quad \cdot : R \times R \longrightarrow R$$

und Elemente $0, 1 \in R$ so dass gilt:

Ring-Axiome:

(a) $(R, +, 0)$ ist eine abelsche Gruppe

(b) $\cdot$ ist assoziativ und 1 ist neutrales Element für $\cdot$

(c) Distributivität: $\forall a,b,c \in R: \big(a\cdot c + b\cdot c = (a+b)\cdot c \;\wedge$
$a\cdot b + a\cdot c = a\cdot(b+c) \big)$

- R heißt kommutativ, wenn $\cdot$ kommutativ ist.
- R heißt körper, wenn $(R\setminus\{0\}, \cdot, 1)$ eine abelsche Gruppe ist (*)
- Man nennt 0 das Null-Element von R und 1 das Eins-Element.

Bsp: • $\mathbb{Z}$ ist ein Ring.
• $\mathbb{Q}, \mathbb{R}$ sind Körper.

Bem (zu Gruppen): Wegen Assoziativität können wir $a\circ b\circ c$ schreiben (ohne Klammern).

Bem 2.1.9: Ist K ein Körper, so gilt für alle $a,b\in K$:

(a) $a\cdot b = 0 \iff (a=0 \vee b=0)$

(b) $a\cdot(-b) = -(a\cdot b)$

Bew: (a) „$\Rightarrow$" Wenn sowohl $a\neq 0$ als auch $b\neq 0$ wäre, also $a,b\in K\setminus\{0\}$, dann müsste laut (*) auch $a\cdot b\in K\setminus\{0\}$.

„$\Leftarrow$" O.E. Ohne Einschränkung $a=0$.

$$0 + 0\cdot b \overset{0\text{ neutr.}}{=} 0\cdot b \overset{0\text{ neutr.}}{=} (0+0)\cdot b \overset{\text{Distrib}}{=} 0\cdot b + 0\cdot b$$

$$\overset{2.1.3}{\Rightarrow} \quad 0 = 0\cdot b \qquad \square$$

(b) z.z. $a\cdot(-b)$ ist das additive Inverse von $a\cdot b$.

d.h. $a\cdot(-b) + a\cdot b \overset{?}{=} 0$

$$\overset{\text{distrib}}{\parallel}$$

$$a\cdot((-b)+b) = a\cdot 0 \overset{(a)}{=} 0 \qquad \square$$

Def 2.1.10: (a) Sei $(G,\circ,e)$ eine Gruppe. Ist $H\subseteq G$ so dass $(H, \circ|_{H\times H}, e)$ auch eine Gruppe ist, so nennt man H eine Untergruppe von G und G eine Obergruppe von H.

(b) Analog für Ringe und Körper.

Bsp: • $\mathbb{Q}$ ist Unterkörper von $\mathbb{R}$,
• $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$
• $\mathbb{Q}^\times$ ist Untergruppe von $\mathbb{R}^\times$

• $(\mathbb{Q}^\times, \cdot)$ ist keine Untergruppe von $(\mathbb{Q}, +)$

Bem 2.1.11: Wähle einen beliebigen Körper K.

Der gesamte Abschnitt 1.1. funktioniert immer noch, wenn man überall „reelle Zahl" durch „Element von K" ersetzt.

- Bzgl. 1.1.1: sage „lineare Gleichung über K^n"
  Lösungen: Elemente von K^n
- Bzgl. 1.1.2: „LGS über K^n"
- Bzgl. 1.1.3: Mit 0 ist das 0-Element von K gemeint.
- Bzgl. 1.1.4 (b): $\underline{x}, \underline{x}' \in K^n$ Lsg einer Gleichung,
  d.h. $\sum_{i=1}^n a_i x_i = 0$ und $\sum_{i=1}^n a_i x_i' = 0$.

$a_1x_1 + \ldots + a_nx_n$

$$\sum_{i=1}^n \underbrace{a_i(x_i + x_i')}_{\substack{\| \text{ Distrib.} \\ a_ix_i + a_ix_i'}} \overset{?}{=} 0$$

Also: $(a_1x_1 + a_1x_1') + \ldots + (a_nx_n + a_nx_n') \overset{?}{=} 0$

$$\| \text{ assoz., kommut.}$$

$$(a_1x_1 + \ldots + a_nx_n) + (a_1x_1' + \ldots + a_nx_n')$$

$$\| \qquad \qquad \leftarrow \text{0 neutr.}$$

$$0 + 0 = 0$$

- Bzgl. 1.1.7 (b): $\lambda \in K \setminus \{0\}$
  ($\lambda \neq 0 \Rightarrow$ hat multiplikatives Inverses)
- Bzgl. 1.1.10: 0 ist 0-Element von K
  1 ist 1-Element von K
- Bzgl. 1.1.13: Da $0 \neq 1$ (in K) hat K mehrere Elemente, also stimmt „mehrere Lösungen"

Satz 2.1.12 (a) Sei $n \in \mathbb{N} \setminus \{0\}$ und für $a, b \in \mathbb{Z}$: $a \sim b :\Leftrightarrow a \equiv b \mod n$

$\Leftrightarrow n \mid a - b$

- Bezeichne die Äquiv-Klasse von $a \in \mathbb{Z}$ mit $\bar{a}$.

Dann definiert das folgende eine Ringstruktur auf $\mathbb{Z}/\sim$:

- $\bar{a} + \bar{b} := \overline{a+b}$
- $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

  für $a, b \in \mathbb{Z}$
- 0-Element: $\bar{0}$

  1-Element: $\bar{1}$

Bsp. $n = 10$:

$\bar{3} = \{\ldots, -7, 3, 13, 23, \ldots\}$

$\mathbb{Z}/\sim = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{9}\}$, $\bar{0} = \overline{10}$, $\bar{1} = \overline{11}$

$\bar{4} + \bar{7} = \overline{11} = \bar{1}$

$\bar{4} \cdot \bar{7} = \overline{28} = \bar{8}$

$\overline{14} + \overline{27} = \overline{41} = \bar{1}$

(b) Ist n eine Primzahl, so ist $\mathbb{Z}/\sim$ sogar ein Körper.

(Konvention: 1 ist keine Primzahl)

Bew: (a) • Wohldefiniertheit von $+$:

- zu zeigen ist: Ist $\bar{a} = \bar{a'}$ und $\bar{b} = \bar{b'}$ für $a, a', b, b' \in \mathbb{Z}$, so ist auch $\overline{a+b} = \overline{a'+b'}$

Habe also: $\bar{a} = \bar{a'} \Leftrightarrow a \sim a' \Leftrightarrow n \mid a - a'$

$\bar{b} = \bar{b'} \Leftrightarrow n \mid b - b'$

$$a+b \sim a'+b' \Leftarrow n \mid \underbrace{(a-a') + (b-b')}_{= a+b-(a'+b')}$$

$\Downarrow$

$\overline{a+b} = \overline{a'+b'}$

- Wohldef von $\cdot$: Sei also $\bar{a} = \bar{a'}$ und $\bar{b} = \bar{b'}$, also $n \mid a - a'$, $n \mid b - b'$

  - z.z: $\overline{a \cdot b} = \overline{a' b'}$
  - $n \overset{?}{\mid} \underbrace{a \cdot b - a' b'}$

$$= \underbrace{\underbrace{a \cdot b - a' \cdot b}_{=(a-a') \cdot b}}_{\text{durch } n \text{ teilbar}} + \underbrace{\underbrace{a' \cdot b - a' \cdot b'}_{a' \cdot (b-b')}}_{\text{durch } n \text{ teilbar}}$$

$\Rightarrow$ Summe durch n teilbar

- Prüfe die Ring-Axiome:
  - Assoz. von $+$: $\bar a + (\bar b + \bar c) \overset{?}{=} (\bar a + \bar b) + \bar c \qquad (a,b,c \in \mathbb{Z})$

$$\begin{array}{ccc} \bar a + (\bar b + \bar c) & \overset{?}{=} & (\bar a + \bar b) + \bar c \\ \| & & \| \\ \bar a + \overline{b+c} & & \overline{a+b} + \bar c \\ \| & & \| \\ \overline{a+(b+c)} & = & \overline{(a+b)+c} \end{array}$$

  - Existenz von $+$-Inversen: Für $\bar a \in \mathbb{Z}/\sim$ setze $-\bar a := \overline{-a}$

Z.z.: $\bar a + (-\bar a) \overset{?}{=} \bar 0$

$$\underbrace{\bar a + \overset{\overline{-a}}{\overbrace{(-\bar a)}}}_{\overline{a+(-a)}} \overset{?}{=} \bar 0, \qquad \overline{a+(-a)} = \bar 0$$

  - Alle anderen Axiome: Analog: Jedes Ring-Axiom für $\mathbb{Z}$ impliziert das entsprechende Ring-Axiom für $\mathbb{Z}/\sim$

(b) Kommutativität von $\cdot$ vererbt sich von $\mathbb{Z}$. Bleibt z.z.: Jedes $\bar a \in \mathbb{Z}/\sim \setminus \{\bar 0\}$ hat ein multiplikatives Inverses.

Bsp: $n = 5$

Für $\bar 1, \bar 2, \bar 3, \bar 4$ sind mult. Inverse gesucht.

$\bar 1 \cdot \bar 1 = \bar 1$

$\bar 2 \cdot ? = \bar 1$

$\bar 2 \cdot \bar 3 = \bar 6 = \bar 1$

Also $\bar 2^{-1} = \bar 3$

Analog: $\bar 3^{-1} = \bar 2$, $\bar 4^{-1} = \bar 4$

(da $\bar 4 \cdot \bar 4 = \overline{16} = \bar 1$)

- Sei $\bar a \in \mathbb{Z}/\sim \setminus \{\bar 0\}$ gegeben
- Betrachte $f: \mathbb{Z}/\sim \longrightarrow \mathbb{Z}/\sim$, $\bar b \longmapsto \bar b \cdot \bar a$
- Behauptung: f ist injektiv, d.h. ist $f(\bar b) = f(\bar b')$, so ist bereits $\bar b = \bar b'$ (für $b, b' \in \mathbb{Z}$)

Bew. der Beh: $f(\bar b) = f(\bar b')$, $f(\bar b) = \bar a \cdot \bar b$, $f(\bar b') = \bar a \cdot \bar b'$

Notn: Für $a, b \in G$ ($(G,+)$ Gruppe) setze $a - b := a + (-b)$

$$\Rightarrow \bar a \cdot \bar b - \bar a \cdot \bar b' = \bar 0$$

$$\bar a \cdot \bar b - \bar a \cdot \bar b' = \bar a(\bar b - \bar b') = \overline{a(b-b')}$$

d.h. $a(b-b') \sim 0$

$\Rightarrow n \mid a \cdot (b - b')$

Da $\bar a \neq \bar 0$: $n \nmid a$. Da n Primzahl folgt $n \mid b - b'$

$\Rightarrow \bar b = \bar b'$

$\square$ (Beh)

- Es folgt: f ist surjektiv. (sonst: $\#(\mathbb{Z}/\sim) > \#(f(\mathbb{Z}/\sim))$; kann nicht sein bei endl. Mengen, wenn f injektiv ist)
- Insbes. ex. ein $\bar{b} \in \mathbb{Z}/\sim$ mit $\underset{\bar{a}\cdot\bar{b}}{\overset{\shortparallel}{f(\bar{b})}} = \bar{1}$

Dieses $\bar{b}$ ist ein Inverses von $\bar{a}$. $\square$

„$\mathbb{Z}$ modulo $n\mathbb{Z}$"

<u>Def 2.1.13</u>: Der Ring $\mathbb{Z}/\sim$ aus 2.1.12 wird mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.
Ist p eine Primzahl, so wird der Körper $\mathbb{Z}/\sim$ aus Satz 2.1.12 für $n=p$ mit $\mathbb{F}_p$ bezeichnet.
Die Elemente von $\mathbb{Z}/n\mathbb{Z}$ werden $0, 1, \ldots, n-1$ geschrieben (statt $\bar{0}, \ldots, \overline{n-1}$).