Die Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ zusammen mit den entsprechenden Verknüpfungen "+" & "·" unterscheiden sich deutlich in ihrer algebraischen Struktur. 02.05.18

Kurzer Exkurs zu algebraischen Strukturen

Def. 2.16

Sei G eine nichtleere Menge und „$\circ$" eine Verknüpfung auf G, d.h.

$$\circ : G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 \circ g_2$$

mit folgenden Eigenschaften:

(A1) Es gibt ein neutrales Element $e_G \in G$ bzgl. $\circ$, d.h. $\forall g \in G$ gilt $g \circ e_G = e_G \circ g = g$

(A2) Es gibt ein inverses Element bzgl. $\circ$, d.h. $\forall g \in G \; \exists \tilde{g} \in G$ mit $g \circ \tilde{g} = e_G = \tilde{g} \circ g$

(A3) Es gilt das Assoziativgesetz, d.h. $\forall g_1, g_2, g_3 \in G$ gilt: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

In diesem Fall nennen wir $(G, \circ)$ eine Gruppe. Ist die Wahl der Verknüpfung klar, so sagen wir auch, dass G eine Gruppe ist.

Gilt zu dem

(A4) (Kommutativgesetz) $\forall g_1, g_2 \in G$ gilt $g_1 \circ g_2 = g_2 \circ g_1$

So nennt man G eine Abelsche Gruppe (Nils Hendrik Abel, 1802 - 1829)

Beispiele 2.17

- $(\mathbb{N}, +)$ bzw. $(\mathbb{N}, \cdot)$ sind keine Gruppen, da Existenz eines Inversen fehlschlägt.

- $(\mathbb{Z}, +)$ ist eine Abelsche Gruppe. $(\mathbb{Z}, \cdot)$ ist keine Gruppe
- Ist $G = GL(n, \mathbb{Q})$ die Menge der invertierbaren $n \times n$ Matrizen mit Einträgen in $\mathbb{Q}$. So ist G bzgl. der Matrixmultiplikation eine Gruppe, jedoch keine Abelsche Gruppe.
  Bzgl. der Matrizenaddition ist G keine Gruppe, da die Addition keine wohldefinierte Verknüpfung auf G sein.
  (z.B. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin GL(2, \mathbb{Q})$)
- $S_n = \{ \varphi : \{1, \dots, n\} \to \{1, \dots, n\} \}$ die Menge der bijektiven Abbildungen von $\{1, \dots, n\}$ nach $\{1, \dots, n\}$
  (Ein Element $\varphi \in S_n$ wird auch Permutation genannt)
  S_n wird bzgl. der „Hintereinanderausführung" zu einer Gruppe

Def. 2.18

Sei $M \neq \emptyset$ eine Menge mit zwei Verknüpfungen

$\oplus : M \times M \to M$ $\qquad$ $\odot : M \times M \to M$

$(m_1, m_2) \to m_1 \oplus m_2$ $\qquad$ $(m_1, m_2) \to m_1 \odot m_2$

sodass folgende Eigenschaften erfüllt sind.

(A) $(M, \oplus)$ erfüllt (A1)-(A4), ist also eine Abelsche Gruppe mit neutralem Element e_M $(= 0_M)$

(M1) Es gibt ein neutrales Element bzgl. $\odot$, d.h.
$\exists\, 1_M$ s.d. $1_M \odot m = m \odot 1_M = m \quad \forall m \in M$

(M2) Für alle $m \in M$ mit $m = e_M$ gibt es ein inverses Element bzgl. $\odot$, d.h. $\forall m \in M \setminus \{e_M\} \; \exists \tilde{m}$ mit $m \odot \tilde{m} = \tilde{m} \odot m = 1_M$

(M3) Es gilt das Assoziativgesetz bzgl. $\odot$, d.h.
$\forall m_1, m_2, m_3 \in M$ gilt $m_1 \odot (m_2 \odot m_3) = (m_1 \odot m_2) \cdot m_3$

(M4) Es gilt das Kommutativgesetz bzgl. $\odot$.
Also $\forall m_1, m_2 \in M$ gilt: $m_1 \odot m_2 = m_2 \odot m_1$

(D) Die beiden Verknüpfungen erfüllen das Distributivgesetz, d.h. $\forall m_1, m_2, m_3 \in M$ gilt
$m_1 \odot (m_2 \oplus m_3) = (m_1 \odot m_2) \oplus (m_1 \odot m_3)$

In diesem Fall nennt man $(M, \oplus, \odot)$ einen Körper
Ein Körper ist also eine Menge M mit zwei Verknüpfungen, sodass die Menge bzgl. einer Verknüpfung eine Abelsche Gruppe ist & $M \setminus \{e_\oplus\}$ bzgl. der anderen Verknüpfung auch eine Abelsche Gruppe ist.

Def + Bemerkung 2.19
Sei M wieder eine Menge mit zwei Verknüpfungen $\oplus$ & $\odot$ sodass $(M, \oplus)$ eine Abelsche Gruppe ist und $\odot$ (M1), (M3), (M4) & (D) erfüllt.
So nennen wir $(M, \oplus, \odot)$ einen kommutativen Ring mit Einselement (oder einfach nur Ring)
Im Gegensatz zu Körpern sind Ringe nicht immer nullteilerfrei. Die Nullteilerfreiheit von Körpern folgt aus der Existenz eines Inversen bzgl. $\odot$

Γ Ist $a \odot b = \underbrace{0}_{e_\odot}$ mit $a = \underbrace{0}_{e_\odot} \Rightarrow \exists \underbrace{\tilde{a}}_{\tilde{a}}$ mit $\underbrace{\tilde{a} \odot \overbrace{a \odot b}^{0}}_{b} = \tilde{a} \odot 0 = 0 \rightsquigarrow b = 0$ $\lrcorner$

Nullteilerfreie Ringe nennt man auch Integritätsring
Für die Konstruktion von $\mathbb{Q}$ und $\mathbb{Z}$ ist die Nullteilerfreiheit von $\mathbb{Z}$ entscheidend.

Beispiele 2.20

- $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsring
- $(\mathbb{Q}, +, \cdot)$ ist ein Körper
- Sei $M = Mat(n, n, \mathbb{Q})$ die Menge aller $n \times n$-Matrizen, dann ist $(M, +, \cdot)$ ein Ring aber kein Integritätsring

  (z.B. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$)
- Die Menge $\mathcal{C}(0,1)$ der stetigen Funktionen auf dem Intervall $(0,1)$ ist ein Ring bzgl. punktweiser Addition & Multiplikation

  $(f+g)(x) := f(x) + g(x)$

  $(f \cdot g)(x) := f(x) \cdot g(x)$

  Aber $\mathcal{C}(0,1)$ ist kein Integritätsring
- Additive & Multiplikative Inverse sind eindeutig in Gruppen / Ringen / Körpern.

Bemerkung 2.21

Schreibt man eine Gruppe additiv mit „+" so schreibt man in der Regel 0 für das neutrale Element & $2 \cdot g$ für $g+g$ usw.

Schreibt man G multiplikativ, so schreibt man 1 für das neutrale Element und $g^2 = g \cdot g$ usw.

Def. 2.22

Ist G eine Gruppe und $U \subset G$ eine Teilmenge mit der Eigenschaft, dass $(U, \circ|_U)$ wieder eine Gruppe ist, so heißt U eine Untergruppe von G.

Analog für Ringe & Körper.

Um Gruppen / Ringe / Körper zu studieren betrachtet man häufig strukturerhaltende Abbildungen zwischen Gruppen /... /...

Def. 2.23

Seien $(G, \circ_G)$ und $(H, \circ_H)$ zwei Gruppen mit neutralen Elementen e_G und e_H.

Eine Abbildung $\varphi: G \to H$ heißt Gruppenhomomorphismus, falls $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$.

Lemma 2.24

Seien $(G, \circ_G)$ und $(H, \circ_H)$ zwei Gruppen und $\varphi: G \to H$ ein Gruppenhomomorphismus dann ist

1) $\varphi(e_G) = e_H$.
2) $\varphi(g^{-1}) = \varphi(g)^{-1}$

Beweis:

1) $\forall g \in G$ gilt $\varphi(g) \circ_H e_H = \varphi(g) = \varphi(g \circ_G e_G)$
$= \varphi(g) \circ_H \varphi(e_G)$

$\Rightarrow e_H = \varphi(e_G)$

2) $e_H = \varphi(e_G) = \varphi(g \circ_G g^{-1}) = \varphi(g) \circ_H \varphi(g^{-1})$

$\Rightarrow \varphi(g^{-1}) \in H$ ist das Inverse zu $\varphi(g) \in H$. ▨

Def. 2.25

Seien $(R, +, \cdot)$ & $(S, \oplus, \odot)$ kommutative Ringe mit Eins.

Eine Abbildung $\varphi: R \to S$ heißt Ringhomomorphismus, falls $\forall a, b \in R$:

1) $\varphi(a+b) = \varphi(a) \oplus \varphi(b)$
2) $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$
3) $\varphi(1_R) = 1_S$, wobei 1_R das neutrale Element der Multiplikation bezeichnet.

z.B. $\varphi: \mathbb{Z} \to \mathbb{Z}$ $x \mapsto 0$ erfüllt 1) & 2) aber nicht 3)

Bemerkung 2.26 (Konstruktion von $\mathbb{R}$ und $\mathbb{C}$)

Die komplexen Zahlen lassen sich aus $\mathbb{R}$ konstruieren, indem wir entsprechende Verknüpfungen auf $\mathbb{R}\times\mathbb{R} = \mathbb{R}^2$

$+ : \mathbb{R}^2 \to \mathbb{R}^2$

$(a,b),(c,d) \mapsto (a+c, b+d)$

$\cdot : \mathbb{R}^2 \to \mathbb{R}^2$

$(a,b)\cdot(c,d) \mapsto (ac-bd, ad+bc)$

Man rechnet nach, dass $(\mathbb{R}^2, +, \cdot)$ ein Körper ist.

Um hingegen $\mathbb{R}$ zu konstruieren (aus $\mathbb{Q}$) benutzt man Mittel der Analysis:

Man definiert die reellen Zahlen als "Äquivalenzklassen von Cauchy-Folgen (oder Intervallschachtelungen) bzgl. der Äquivalenzrelation $(\overset{\in\mathbb{Q}}{a_n})_{n\in\mathbb{N}} \sim (\overset{\in\mathbb{Q}}{b_n})_{n\in\mathbb{N}} :\Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}}$ ist eine Nullfolge. Die Menge der Äquivalenzklassen bzgl. dieser Äquivalenzrelation heißen die reellen Zahlen. Man kann passende Verknüpfungen auf dieser Menge konstruieren, sodass man den bekannten Körper der reellen Zahlen erhält.

Die reellen Zahlen sind der kleinste Körper in dem jede Cauchy-Folge mit Folgengliedern in $\mathbb{Q}$ konvergiert.

Beispiel

$(a_n)_{n\in\mathbb{N}}$ mit $a_n := \left(1+\frac{1}{n}\right)^n$ $a_n \in \mathbb{Q}$ $\forall n \in \mathbb{N}$

$\lim\limits_{n\to\infty} (a_n)_{n\in\mathbb{N}} = e \in \mathbb{R}\setminus\mathbb{Q}$

§3 Teilbarkeitslehre

In diesem Kapitel möchten wir wichtige Eigenschaften der natürlichen (bzw. ganzen-) Zahlen untersuchen.

Def. 3.1

Eine Zahl $b \in \mathbb{Z}$ (oder $\mathbb{N}$) teilt eine ganze Zahl $a \in \mathbb{Z}$, wenn ein $c \in \mathbb{Z}$ existiert mit $a = b \cdot c$

Wir schreiben hierfür auch $b \mid a$ und sagt, dass b ein Teiler von a ist.

Ein $b \in \mathbb{Z}$ heißt gemeinsamer Teiler von $a_1, a_2 \in \mathbb{Z}$, falls c_1 & c_2 existieren mit $a_1 = c_1 \cdot b$ und $a_2 = c_2 \cdot b$.

Beispiel 3.2

Die Teiler von 12 sind $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

Lemma 3.3.

(i) $a \mid a$ $(a \in \mathbb{Z}, a \neq 0)$

(ii) $a \mid 0$ $(a \in \mathbb{Z}, a \neq 0)$

(iii) $1 \mid a$ $(a \in \mathbb{Z})$

(iv) $b \mid a, c \mid b \Rightarrow c \mid a$ $(a, b, c \in \mathbb{Z}, b, c \neq 0)$

(v) $b \mid a \Rightarrow b \cdot c \mid a \cdot c$ $(a, b, c \in \mathbb{Z}, b, c \neq 0)$

(vi) $b \cdot c \mid a \cdot c \Rightarrow b \mid a$ $(a, b, c \in \mathbb{Z}, b, c \neq 0)$

(vii) $b_1 \mid a_1 \wedge b_2 \mid a_2 \Rightarrow b_1 \cdot b_2 \mid a_1 \cdot a_2$ $(a_i, b_i \in \mathbb{Z}, b_i \neq 0, i = 1, 2)$

(viii) $b \mid a_1 \wedge b \mid a_2 \Rightarrow b \mid (c_1 a_1 + c_2 \cdot a_2)$ $(a_i, c_i \in \mathbb{Z}, b \neq 0)$

(ix) $b \mid a \Rightarrow b \mid a \cdot c$ $(a, b, c \in \mathbb{Z}, b \neq 0)$

(x) $b \mid a \wedge a \mid b \Rightarrow a = b$ $(a, b \in \mathbb{Z}, a, b \neq 0)$