Mathematik I

Vorlesung 6 - Algebraische Strukturen

Prof. Dr. Sandra Eisenreich

09. November 2023

Hochschule Landshut

Motivation Gruppen und Ringe

Wir haben schon viele Zahlenräume kennen gelernt, und viele von diesen haben ähnliche Strukturen:

- $\mathbb{Z}$:
  - addieren (**Verknüpfung**),
  - 0 addieren lässt jede Zahl unverändert (**neutrales Element**),
  - für jede ganze Zahl gibt es eine Negative,so dass die Summe 0 ergibt (**inverses Element**)
  - Es gilt das Assoziativgesetz.

  Eine Menge mit solchen Eigenschaften nennt man **Gruppe**. (ist $\mathbb{N}$ mit der Addition eine Gruppe? - Nein! Kein Inverses.) Da $a + b = b + a$ nennt man $\mathbb{Z}$ **kommutative Gruppe**.
- $\mathbb{Z}$: Man kann ganze Zahlen aber zusätzlich zu obigem auch multiplizieren und bekommt wieder eine ganze Zahl. Eine solche Gruppe nennt man **Ring**.
- $\mathbb{Q}$ ist offensichtlich wie $\mathbb{Z}$ mit der Verknüpfung + eine kommutative Gruppe, und man kann in $\mathbb{Q}$ multiplizieren $\Rightarrow$ Ring.

Motivation Körper

- zusätzliche Struktur auf $\mathbb{Q}\backslash\{0\}$:
  - multiplizieren
  - 1 multiplizieren lässt jede Zahl unverändert (neutrales Element)
  - für jede rationale Zahl außer 0 gibt es einen Kehrbruch, so dass das Produkt 1 ergibt (**inverses Element**)
  - Es gilt das Assoziativgesetz.

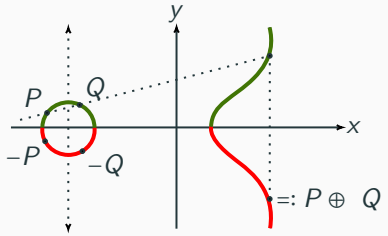
  $\mathbb{Q}\backslash\{0\}$ mit der Mulitplikation ist eine Gruppe, und kommutativ ($a \cdot b = b \cdot a$).
- $\mathbb{Q}$:
  - $\mathbb{Q}$ mit Addition ist eine kommutative Gruppe
  - $\mathbb{Q}\backslash\{0\}$ mit Multiplikation auch.
  - $+$ und $\cdot$ erfüllen das Distributivgesetz.

  Eine solche Struktur nennt man **Körper**.
- $\mathbb{R}$ ist ein Körper. (Überlegen Sie sich das selbst!)

Mengen mit solchen Eigenschaften wie oben beschrieben, also Gruppen, Ringe, Körper, heißen **algebraische Strukturen**. Warum interessiert man sich für so etwas?

Anwendungen in der Informatik

- **Verschlüsselungsverfahren** (Kryptographie) mit sogenannten **elliptischen Kurven**: dies sind Kurven im zweidimensionalen Raum mit einer Gruppen-Struktur (darauf basiert das Verfahren), das heißt man kann ihre Punkte addieren und subtrahieren wie in $\mathbb{Z}$. Sie sehen so aus:



- **Restklassen** haben Gruppen-/Ring- und manchmal sogar Körper-Struktur (Anwendungen in der Informatik: siehe Restklassen)
- die sogenannten **komplexen Zahlen** (siehe nächstes Kapitel) sind ein Körper. Man braucht sie z.B. für Spiele-3D-Engines (und überall in der Physik).

6.1 Gruppen

Verknüpfungen

Definition

Sei M eine Menge. Eine **Verknüpfung auf** M ist eine Abbildung

$$v : M \times M \longrightarrow M, (m_1, m_2) \longmapsto v(m_1, m_2) = m_1 v\ m_2$$

Bezeichnung für v ist meist $+, \cdot, *, \oplus, \cdot, \odot$.

Beispiel:

- Addition auf $\mathbb{Z}$: $a + b$, bzw. formal: $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \longmapsto a + b$
- Multiplikation auf $\mathbb{Z}$: $a \cdot b$, bzw. formal: $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \longmapsto a \cdot b$
- Addition auf $\mathbb{Z}/7\mathbb{Z}$: $\overline{a} \oplus \overline{b}$, bzw. formal: $\oplus : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}, (\overline{a}, \overline{b}) \longmapsto \overline{a + b}$
- Verknüpfung von Abbildungen: $g \circ f$

Gruppen

Definition (Gruppe)

Eine **Gruppe** $(G, *)$ besteht aus einer Menge G und einer Verknüpfung $*$ mit den Eigenschaften:

(G1) **neutrales Element**: Es gibt ein $e \in G$ mit $a * e = e * a = a$ für alle $a \in G$ (e = neutrales Element)

(G2) **inverses Element**: für alle $a \in G$ existiert ein eindeutiges Element $b \in G$ mit $a * b = b * a = e$ (b = inverses Element). Man schreibt auch a^{-1} für dieses b.

(G3) **Assoziativgesetz:** für alle $a, b, c \in G$ gilt: $(a * b) * c = a * (b * c)$.

Die Gruppe $(G, *)$ heißt **kommutativ**, wenn zusätzlich gilt:

(G4) **inverses Element**: für alle $a, b \in G$ gilt: $a * b = b * a$

Bemerkung: Verwendet man für die Verknüpfung das Symbol $+$ oder $\oplus$ (wie in $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$), dann wird häufig e mit 0 bezeichnet, und a^{-1} mit $-a$. In diesen Fall spricht man von einer **additiven Gruppe**. Andernfalls spricht man von einer **multiplikativen Gruppe**.

Beispiele

- $(\mathbb{Z}, +)$ ist eine kommutative additive Gruppe:
  - $+$ ist eine Verknüpfung.
  - (G1) neutrales Element: $e = 0 \in \mathbb{Z}$, da $0 + a = a \forall a \in \mathbb{Z}$.
  - (G2) inverses Element: $a^{-1} = -a \in \mathbb{Z}$, da $-a + a = 0 \forall a \in \mathbb{Z}$.
  - (G3) Assoziativgesetz: klar (Schule)
  - (G4) $\forall a, b \in \mathbb{Z} : a + b = b + a$.
- $(\mathbb{R}\backslash\{0\}, \cdot)$ ist eine kommutative multiplikative Gruppe:
  - $\cdot$ ist eine Verknüpfung.
  - (G1) neutrales Element: $e = 1 \in \mathbb{R}\backslash\{0\}$, da
  - (G2) inverses Element: $a^{-1} = \frac{1}{a} \in \mathbb{R}\backslash\{0\}$, da $a \cdot \frac{1}{a} = 1$
  - (G3) Assoziativgesetz: klar (Schule)
  - (G4) $\forall a, b \in \mathbb{Z} : a \cdot b = b \cdot a$.

- $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ ist eine kommutative additive Gruppe:
  - $\oplus$ ist eine Verknüpfung.
  - (G1) neutrales Element: $e = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$
  - (G2) inverses Element: $\overline{a}^{-1} = \overline{-a} = \overline{b-a} \in \mathbb{Z}/n\mathbb{Z}$ (z.B. in $\mathbb{Z}/7 : \overline{2} \oplus \overline{7-2} = 0$)
  - (G3) Assoziativgesetz: $(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{a+b} \oplus \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} \oplus (\overline{b} \oplus \overline{c})$
  - (G4) $\forall a, b \in \mathbb{Z}/n\mathbb{Z} : \overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a}$.
- $(\mathbb{Z}\backslash\{0\}, \cdot)$ ist keine Gruppe, da für alle $m \in \mathbb{Z}\backslash\{0, 1, -1\}$ kein Inverses existiert. (G2 nicht erfüllt).
- $(\mathbb{N}, +)$ ist keine Gruppe, da für kein $m \in \mathbb{N}$ ein Inverses bezüglich Addition existiert (G2 nicht erfüllt): z.B. wäre das Inverse zu 2 bezüglich Addition -2, aber $-2 \notin \mathbb{N}$.

Untergruppe

Satz

Sei $(G, *)$ eine Gruppe und $U \subset G$ eine Teilmenge von G, so dass folgende Bedingungen erfüllt sind:

- **Abgeschlossenheit bzg. $*$:** *$a * b \in U$ für alle $a, b \in U$, und*
- **Abgeschlossenheit bzgl. Inversenbildung**: *$a^{-1} \in U$ für alle $a \in U$.*

Dann ist $(U, *)$ auch eine Gruppe. U heißt **Untergruppe** *von G.*

Beispiel

Wir definieren $m\mathbb{Z} := \{m \cdot z | z \in \mathbb{Z}\}$ für festes m. z.B. $7 \cdot \mathbb{Z} = \{0, 7, -7, 14, -14, \ldots\}$

Behauptung: $(m\mathbb{Z}, +)$ ist eine Gruppe.

Beweis. Es gilt $U := m\mathbb{Z} \subset \mathbb{Z}$ und somit ist $(m\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$, falls:

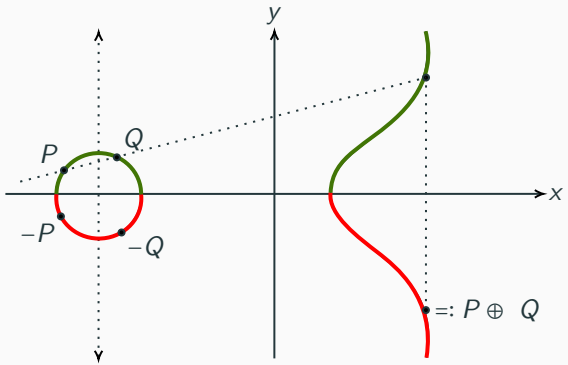
- Abgeschlossenheit bzgl. $+$, also zu zeigen: $a, b \in m\mathbb{Z} \Rightarrow a + b \in m\mathbb{Z}$. Hierzu:
  $a = m \cdot z_1$ und $b = m \cdot z_2 \Rightarrow a + b = m \cdot (z_1 + z_2) \in m\mathbb{Z}$ ✓
- Abgeschlossenheit bzgl. Inversenbildung, also zu zeigen: $a^{-1} \in m\mathbb{Z}$ für alle $a \in m\mathbb{Z}$. Hierzu:
  $a^{-1} = -a = -z \cdot m$ falls $a = z \cdot m$ ✓ ■

Elliptische Kurve

Definition

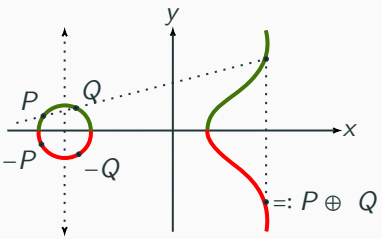
Seien $a, b \in \mathbb{R}$. Dann ist eine Elliptische Kurve definiert als der Punkt ∞ bei $y = \pm\infty$, zusammen mit allen Punkten x, y, die die Gleichung $y^2 = x^3 + ax + b$ erfüllen:

$$E := \{(x,y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\} = \left\{(x,y) \in \mathbb{R}^2 : \begin{array}{l} y = \sqrt{x^3 + ax + b} \\ y = -\sqrt{x^3 + ax + b} \end{array}\right\} \cup \{\infty\}$$



Wir machen die elliptische Kurve E zu einer Gruppe:

1. Das **neutrale Element** 0 sei der Punkt ∞.
2. Für $P, Q \in E$ sei die **Verknüpfung** $P \oplus Q$ wie folgt definiert:



- 1. Fall: $P \neq Q$: Verbinde P und Q mit einer Geraden und schneide diese mit E (falls P und Q übereinander liegen, schneidet sie E bei ∞). Man erhält einen Punkt R. Der Spiegelpunkt von R an der x–Achse wird definiert als $P \oplus Q$. Sind P und Q senkrecht übereinander, ist $P \oplus Q = \infty = 0$.
- 2. Fall $P = Q$: In diesen Fall ist die Gerade durch P und Q die Tangente ("lasse einfach Q nahe an P sein"). Die Tangente schneidet E in einem weiteren Punkt. Das Spiegelbild dieses Punktes an der x-Achse ist dann $P \oplus P = 2P$.

3. Für $P \in E$ ist das **Inverse** $-P$ der Punkt, wenn man P an der x-Achse spiegelt.

Beachte: Obige Definition funktioniert nur, wenn eine Gerade durch zwei Punkte von E genau durch einen weiteren Punkt von E geht. (kann man zeigen). Man kann sogar zeigen:

Satz

Für eine elliptische Kurve und die Verknüpfung $\oplus$ wie oben definiert ist $(E, \oplus)$ eine kommutative Gruppe.

Verschlüsselung mit elliptischen Kurven

Methode: Man kann Vielfache von P über die definierte Addition berechnen:

- Methode 1: $2P = P + P$, $3P = 2P + P$, $4P = 3P + P$. Dauert lange ($N - 1$ Schritte)
- Methode 2 (Abkürzung!): schreibe N als Summe von 2-er Potenzen (in Binärzahl umwandeln) - und berechne NP als Summe der Terme: $2 \cdot P = P + P$, $4 \cdot P = 2 \cdot P + 2 \cdot P$, $8 \cdot P = 4 \cdot P + 4 \cdot P$, ... (viel schneller!)

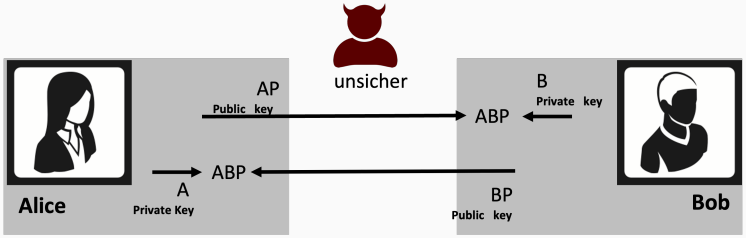
Beispiel: Berechnen von $135 \cdot P$ ...

- Methode 1: 134 Additionen.
- Methode 2: Schreibe $134 = 128 + 4 + 2 + 1 = 2^6 + 2^2 + 2^1 + 2^0$, berechne $2 \cdot P = P \cdot P$ (1 Addition), $4 \cdot P = 2 \cdot P + 2 \cdot P$ (1 Addition), $8 \cdot P = 4 \cdot P + 4 \cdot P$ (1 Addition), $16 \cdot P, 32 \cdot P, 64 \cdot P, 128 \cdot P$ (4 Additionen) und damit: $135 \cdot P = 128 \cdot P + 4 \cdot P + 2 \cdot P + P$ (3 Additionen) $\Rightarrow$ insgesamt 10 Additionen.

Der Unterschied zwischen Methode 1 und 2 wird größer, je größer die Zahl N ist!

Alice und Bob wollen geheime Nachrichten übermitteln.

- Alice und Bob tauschen aus: eine Elliptische Kurve, einen Punkt $P \in E$.
- Jeder überlegt sich einen geheimen Schlüssel $A \in \mathbb{N}$ bzw. $B \in \mathbb{N}$
- jeder berechnet seinen öffentlichen Schlüssel $A \cdot P$ bzw. $B \cdot P$ mit Methode 2 (schnell). Diese werden ausgetauscht.
- Alice hat: A und $B \cdot P$, berechnet $A \cdot B \cdot P$ (mit Methode 2, schnell);
- Bob hat: B und $A \cdot P$, berechnet auch $B \cdot A \cdot P = A \cdot B \cdot P$ (mit Methode 2, schnell);
- Die x-Koordinate von ABP ist der Schlüssel in einem symmetrischen Verfahren.



Was wenn jemand den Code knacken will?

Sogar wenn Außenstehende E und P kennen und die öffentlichen Schlüssel $A \cdot P$, $B \cdot P$, müssten sie auf A, B und P kommen. Dazu müssten sie $P, 2 \cdot P, 3 \cdot P$ usw berechnen bis sie z.B. zu $A \cdot P$ oder $B \cdot P$ kommen (was lange dauert mit Methode 1!), um auf A, B zu kommen und damit dann auf $A \cdot B \cdot P$.

Satz

Sei M eine Menge, F sei die Menge aller bijektiven Abbildung von M nach M. $(F, \circ)$ ist eine (i.a. nicht kommutative) Gruppe, wobei $\circ$ die Komposition von Abbildungen ist.

Beweis.

- $\circ$ **ist eine Verknüpfung** $F \times F \to F$**, denn:** Seien $f : M \longrightarrow M$ und $g : M \longrightarrow M$ Elemente aus F. Dann ist auch die Komposition $g \circ f : M \longrightarrow M$ bijektiv und somit in F. ✓
- (G1) neutrales Element: die identische Abbildung id: $M \longrightarrow M$ ist in F und es gilt für alle $f \in F$: $f \circ \mathrm{id} = \mathrm{id} \circ f = f$.
- (G2) Inverses Element: Ist $f \in F$, dann ist auch die Umkehrabbildung $f^{-1} \in M$. ✓
- (G3) Assoziativgesetz: $(F, \circ)$ ist assoziativ. ✓
- (G4) gilt im Allgemeinen nicht! Im Allgemeinen ist $\circ$ **nicht kommutativ,** d.h. $f \circ g \neq g \circ f$.

Permutationen

Sei nun $M = \{1, \ldots, n\}$ dann gibt es $n!$ viele bijektive Abbildungen von M nach M. Wir schreiben jede solche Abbildung σ als

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \ldots & \sigma(n) \end{pmatrix}$$

z.B. ist $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ die Abbildung von $\{1, 2, 3\}$ nach $\{1, 2, 3\}$, die 1 auf 3,2 auf 1, und 3 auf 2 abbildet.

Definition

Die Menge aller bijektiven Abbildungen $\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ nennen wir **Permutationsgruppe** S_n.

Beispiele

- Permutationen von drei Elementen: (wie wenn man drei Kugeln in drei durchnummerierten Fächern (1-3) tauscht). Zur Verbildlichung: rot, grün, blau.

  $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$: hier wird die Kugel von Fach 1 in Fach 2 gelegt, die Kugel von Fach 2 in Fach 3 und die Kugel von Fach 3 in Fach 1. Als Abbildung:

  $$f: \{1,2,3\} \longrightarrow \{1,2,3\};\ 1 \longmapsto 2,\ 2 \longmapsto 3,\ 3 \longmapsto 1$$

  $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$: hier wird die rote Kugel von Fach 1 in Fach 3, die blaue Kugel von Fach 2 in Fach 1, und die grüne Kugel von Fach 3 in Fach 2 gelegt. Als Abbildung:

  $$f: \{1,2,3\} \longrightarrow \{1,2,3\};\ 1 \longmapsto 3;\ 2 \longmapsto 1;\ 3 \longmapsto 2$$

  Die Komposition der beiden Abbildungen $g \circ f$ (zuerst f anwenden, und dann g) ist gegeben durch:

  $$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id,$$

  denn: f legt die Kugel von 1 auf 2, und g danach die Kugel von 2 zurück auf 1. f schickt 2 auf 3, und g danach wieder 3 auf 2...

- $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ und $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

  $f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ $\quad g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

  $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ $\quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

  Also gilt $g \circ f \neq f \circ g \Rightarrow (S_n, 0)$ ist eine **nicht kommutative** Gruppe.

- $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$ und $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$

  $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ $\quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$

  $f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$ $\quad g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$

6.2 Ringe

Definition

Ein **kommutativer Ring** $(R, \oplus, \odot)$ besteht aus einer Menge R mit 2 Verknüpfungen $\oplus$ und $\odot$, so dass

- $(R1)$ $(R, \oplus)$ ist eine kommutative Gruppe
- $(R2)$ Assoziativgesetz: $(a \odot b) \odot c = a \odot (b \odot c)$ fur alle $a, b, c \in R$
- $(R3)$ Distributivgesetz: $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
- $(R4)$ Kommutativität von $\odot$: $a \odot b = b \odot a$

Satz

Sei S eine Teilmenge von R, und $(R, \oplus, \odot)$ ein Ring. Dann ist $(S, \oplus, \odot)$ ein Ring (genannt: **Unterring** *von $(R, \oplus, \odot)$), falls*

a) $(S, \oplus)$ *ist Untergruppe von* $(R, \oplus)$

b) *Abgeschlossenheit bzgl.* $\odot$*:* $a, b \in S \Rightarrow a \odot b \in S$

Beispiel:

1. $(\mathbb{Z}, +, \cdot)$ ist ein Ring (hier sieht man: $(\mathbb{Z}, \cdot)$ muss keine Gruppe sein! kein Inverses...)
2. für alle $m \in \mathbb{Z}$ ist $(m\mathbb{Z}, +, \cdot)$ ist ein Unterring von $(\mathbb{Z}, +, \cdot)$. Beachte: $m\mathbb{Z}$ hat keine 1 (kein neutrales Element) bzgl $\cdot$.
3. $(\mathbb{Z}/m, \oplus, \odot)$ ist ein Ring. Dies folgt im Wesentlichen aus der Tatsache, dass $(\mathbb{Z}, +, \cdot)$ ein Ring ist, und dass beim Rechnen modulo m Restebildung und Rechenoperationen vertauscht werden dürfen. ($\longrightarrow$ freiwillige übungsaufgabe) $\mathbb{Z}/m$ ist kein Unterrring von $\mathbb{Z}$ da $\oplus \neq +$ und $\odot \neq \cdot$.
4. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sind Ringe.

Beispiel: Polynomringe

Beispiel von Polynomen:

$f(x) = x^5 - x + 1,\ g(x) = \frac{1}{2}x^2,\ h(x) = 7$

Obige Polynome haben reelle Koeffizienten, bzw Koeffizienten in $\mathbb{Q}$. Man kann nun zwei solche Polynome addieren bzw. multiplizieren. Der Typ der Koeffizienten ändert sich dabei nicht.

Definition

Sei R ein Ring. Dann definieren wir

$$\begin{aligned} R[x] &= \text{Menge aller Polynome mit Koeffizienten aus } R \\ &= \{a_0 + a_1 x + \ldots + a_n \cdot x^n \mid n \in \mathbb{N}_0 \text{ und } a_0, \ldots, a_n \in R\} \end{aligned}$$

Satz

Ist R ein Ring, so ist auch $R[x]$ ein Ring.

Kein Beweis. Hier nur ein Beispiel für $R = \mathbb{Z}/5$ (bzw. $R = \mathbb{Z}$):

$$\begin{aligned} f(x) &= 1 + 2x + x^3 \in \mathbb{Z}/5[x] \\ g(x) &= 4 + 3x \in \mathbb{Z}/5[x] \end{aligned}$$

- Abgeschlossenheit bzgl. Multiplikation:

$$\begin{aligned} f(x) \cdot g(x) &= (1 + 2x + x^3) \cdot (4 + 3x) \\ &= (1 \cdot 4) + (1 \cdot 3 + 2 \cdot 4)x + 2 \cdot 3x^2 + 4 \cdot x^3 + 3x^4 \\ &= 4 + 1 \cdot x + 1 \cdot x^2 + 4x^3 + 3x^4. \end{aligned}$$

  (Fasst man f und g als Polynome in $\mathbb{Z}[x]$ auf, dann gilt $f \cdot g = 4 + 11x + 6x^2 + 4x^3 + 3x^4$)

- Abgeschlossenheit bzgl. Addition: Analog
  in $\mathbb{Z}/5$: $f + g = 0 + 0 \cdot x + x^3 = x^3$
  in $\mathbb{Z}$: $f + g = 5 + 5x + x^3$

Gruppen-Homomorphismen

Definition

- Seien $(G, *)$ und $(H, \cdot)$ Gruppen. Eine Abbildung $f : G \longrightarrow H$ mit

$$f(a * b) = f(a) \cdot f(b)$$

  für alle $a, b \in G$ heißt f **(Gruppen-)Homomorphismus**.

- Sind $(R, +, \cdot)$ und $(S, \oplus, \odot)$ Ringe und gilt für eine Abbildung $f : R \longrightarrow S$, dass

$$\begin{aligned} f(a + b) &= f(a) \oplus f(b) \text{ und} \\ f(a \cdot b) &= f(a) \odot f(b) \end{aligned}$$

  für alle $a, b \in R$, dann heißt f **(Ring-) Homomorphismus**.

- Ein bijektiver Homomorphismus heißt **Isomorphismus**. Gibt es einen Isomorphismus $f \cdot R \longrightarrow S$, dann nennt man R und S **isomorph**.

Beispiel:

- $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad a \longmapsto \overline{a},$ ist ein Ringhomomorphismus, da

$$\begin{aligned} f(a) \oplus f(b) = \overline{a} \oplus \overline{b} &= \overline{(a+b)} = f(a+b) \\ f(a) \odot f(b) = \overline{a} \odot \overline{b} &= \overline{a \cdot b} = f(a \odot b). \end{aligned}$$

- $f : (\mathbb{Z}, +) \longrightarrow (n\mathbb{Z}, +), \quad a \longmapsto n \cdot a$ ist ein Gruppenhomomorphismus:

$$f(a+b) = n \cdot (a+b) = n \cdot a + n \cdot b = f(a) + f(b),$$

aber die Abbildung $f \cdot (\mathbb{Z}, +, \cdot) \longrightarrow (n\mathbb{Z}, +, \cdot)$ ist kein Ringhomomorphismus für $n \neq 1$, da

$$f(a \cdot b) = n \cdot a \cdot b, \text{ aber } f(a) \cdot f(b) = (n \cdot a) \cdot (n \cdot b) = n^2 \cdot a \cdot b$$

- Sei $f : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x], \quad p \longmapsto p'$, die Abbildung, die eine Funktion p auf ihre Ableitung abbildet (z.B. $x^3 + 2x + 1 \longmapsto 3x^2 + 2$)
  - f ist ein Gruppenhomomorphismus zwischen $(\mathbb{Z}[x], +)$ und $(\mathbb{Z}[x], +)$, da:

$$f(p+q) = (p+q)' = p' + q' = f(p) + f(q).$$

  - f ist aber kein Ringhomomorphismus, da beispielsweise für $p = 1 + x$ und $q = 1 - x$ gilt:

$$\begin{aligned} f((1+x)(1-x)) &= f(1+x^2) = -2x, \text{ aber} \\ f(1+x) \cdot f(1-x) &= 1 \cdot (-1) = -1 \\ \Rightarrow f((1+x)(1-x)) &\neq f(1+x) \cdot f(1-x) \end{aligned}$$

6.3 Körper

Definition

Sei K eine Menge mit zwei Verknüpfungen $\oplus, \odot$, so dass gilt:

(K1) $(K, \oplus, \odot)$ ist ein kommutativer Ring.

(K2) $(K \backslash \{0\}, \oplus)$ ist eine Gruppe.

Dann nennt man K mit diesen zwei Verknüpfungen einen **Körper.** In einem Körper schreibt man auch

$$a \odot b^{-1} =: \frac{a}{b}$$

Beispiele

- $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.
- "Der kleinste Körper" $= (\mathbb{Z}/2\mathbb{Z}, \oplus, \odot)$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

  Wir wissen bereits, dass $\mathbb{Z}/m\mathbb{Z}$ für alle m ein Ring ist, also ist $\mathbb{Z}/2\mathbb{Z}$ ein Ring. Damit es auch ein Körper ist, muss $(\mathbb{Z}/2\mathbb{Z}\{\overline{0}\} = \{\overline{1}\}, \odot)$ eine Gruppe sein. $\overline{1}$ ist neutrales Element und gleichzeitig sein eigenes Inverses $\overline{1}^{-1} = \overline{1}$, also eine Gruppe.