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:

- $\mathbb{Z}$: 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**.
- $\mathbb{Z}$: 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.

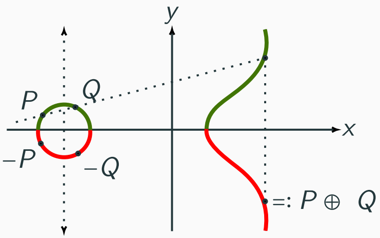
  $\mathbb{Q} \backslash \{0\}$ mit der Mulitplikation ist eine Gruppe, und kommutativ ($a \cdot b = b \cdot a$).
- $\mathbb{Q}$:
  - $\mathbb{Q}$ mit Addition ist eine kommutative Gruppe
  - $\mathbb{Q} \backslash \{0\}$ mit Multiplikation auch.
  - $+$ und $\cdot$ erfüllen das Distributivgesetz.

  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 $+, \cdot, *, \oplus, \cdot, \odot$.

Beispiele: → Mitschrift.

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**.

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 $a \in U$.*

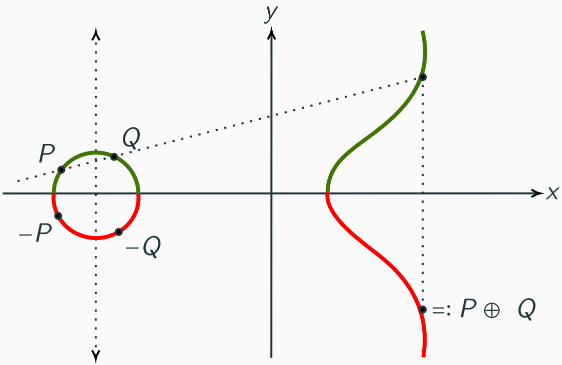
Dann ist $(U, *)$ auch eine Gruppe. U heißt **Untergruppe** *von G.*

Elliptische Kurve

Definition

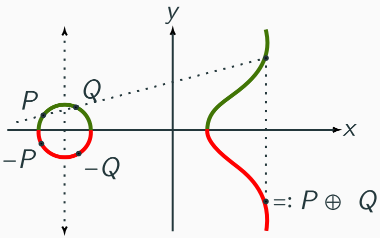
Seien $a, b \in \mathbb{R}$. Dann ist eine Elliptische Kurve definiert als der Punkt ∞ bei $y = \pm\infty$, zusammen mit allen Punkten x, y, die die Gleichung $y^2 = x^3 + ax + b$ erfüllen:

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



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

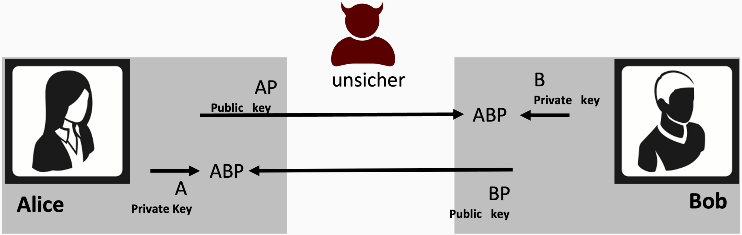
Methode: Man kann Vielfache von P über die definierte Addition berechnen:

- 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 $135 \cdot P$ 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.



Gemeinsamer Schlüssel:
x-Komponente von ABP

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. $\rightarrow$ Mitschrift.

Permutationen

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

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

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 $\sigma : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$ 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:

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

$g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$: 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:

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

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

Beispiele: → Mitschrift

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

Beispiele: → Mitschrift

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.

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**.

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: → Mitschrift.