Mathematik I – Lineare Algebra

Vorlesung 9

Wolfgang Globke

6. November 2019

Definition

Es sei G eine Menge. Wir nennen G eine **Gruppe**, wenn folgendes gilt:

1. Es gibt eine **Verknüpfung** $\circ : G \times G \to G$ von Elementen aus G.
2. Die Verknüpfung $\circ$ ist **assoziativ**, d.h. es gilt
$$a \circ (b \circ c) = (a \circ b) \circ c$$
für alle $a, b, c \in G$.
3. Es existiert ein **neutrales Element** $e \in G$ mit
$$g \circ e = g = e \circ g$$
für alle $g \in G$.
4. Für jedes $g \in G$ existiert ein **Inverses** $g^{-1} \in G$ mit
$$g^{-1} \circ g = e = g \circ g^{-1}.$$

Zusatz

Ist G mit $\circ$ eine Gruppe, so heißt G **abelsch** (oder **kommutativ**), falls außerdem
$$g \circ h = h \circ g$$
gilt für alle $g, h \in G$.

Definition
Eine Menge R mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ wird Ring genannt, wenn folgendes gilt:

1. R bildet zusammen mit $+$ eine abelsche Gruppe.
2. Die Verknüpfung $\cdot$ auf R ist assoziativ.
3. Es gelten die Distributivgesetze

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

   für alle $x, y, z \in R$.

Zusatz

- Gilt $x \cdot y = y \cdot x$ für alle $x, y \in R$, so heißt R kommutativ.
- Das neutrale Element für $+$ wird üblicherweise mit 0 bezeichnet.
- Existiert außerdem ein neutrales Element 1 für $\cdot$, so heißt R ein Ring mit Eins.

Es sei R ein Ring.
Ein Polynom f in der Variablen x mit Koeffizienten in R ist ein Ausdruck der Form

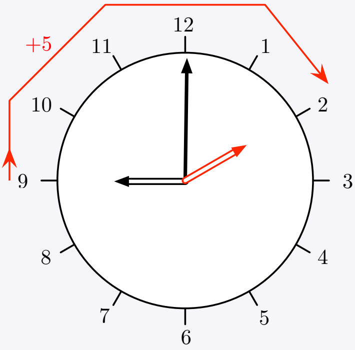
$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

mit $a_n, \ldots, a_0 \in R$ und $a_n \neq 0$. Dabei ist n der Grad von f, geschrieben $\deg(f)$.
Für das Nullpolynom 0 legen wir $\deg(0) = -\infty$ fest.

Satz 4.2
Es sei R ein kommutativer Ring mit Eins.
Dann ist $R[x]$ ein kommutativer Ring mit Eins für die eben definierten Addition $+$ und Multiplikation $\cdot$ von Polynomen.

Modulare Arithmetik

Wenn wir über Uhrzeiten sprechen, rechnen wir immer modular.



$$9 + 5 = 2 \bmod 12$$

Beispiel: Schriftliches Addieren

Beim schriftlichen Addieren rechnen wir spaltenweise modular. (Merken uns jedoch den Übertrag für die nächste Zeile.)

$$\begin{array}{cccc} & 1 & 2 & 8 \\ + & & 7 & 7 \\ \hline \end{array}$$

Beim schriftlichen Addieren rechnen wir spaltenweise modular. (Merken uns jedoch den Übertrag für die nächste Zeile.)

$$\begin{array}{cccc} & 1 & 2 & 8 \\ + & & 7 & 7 \\ & & 1 & \\ \hline & & & 5 \end{array}$$

Beim schriftlichen Addieren rechnen wir spaltenweise modular. (Merken uns jedoch den Übertrag für die nächste Zeile.)

$$
\begin{array}{cccc}
 & 1 & 2 & 8 \\
+ & & 7 & 7 \\
 & {\color{red}1} & 1 & \\
\hline
 & & {\color{blue}0} & 5
\end{array}
$$

Beispiel: Schriftliches Addieren

Beim schriftlichen Addieren rechnen wir spaltenweise modular. (Merken uns jedoch den Übertrag für die nächste Zeile.)

$$\begin{array}{cccc} & 1 & 2 & 8 \\ + & & 7 & 7 \\ & 1 & 1 & \\ \hline & 2 & 0 & 5 \end{array}$$

Beispiel: Schriftliches Addieren

Beim schriftlichen Addieren rechnen wir spaltenweise modular. (Merken uns jedoch den Übertrag für die nächste Zeile.)

$$\begin{array}{cccc} & 1 & 2 & 8 \\ + & & 7 & 7 \\ & 1 & 1 & \\ \hline & 2 & 0 & 5 \end{array}$$

Rechnerarithmetik

Ersetze Basis 10 durch Basis 2, 256,…, `sizeof(int)`.

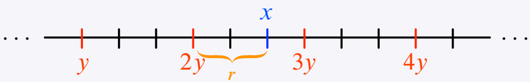
Division mit Rest

Erinnerung:

- Die einzigen Elemente im Ring $\mathbb{Z}$, die ein Inverses für $\cdot$ haben, sind ± 1.
- Für die übrigen Elemente $x \neq \pm 1$ dürfen wir in $\mathbb{Z}$ keine Inversen $\frac{1}{x}$ nehmen.
- Wir können aber Division mit Rest durchführen:
  Für $x, y \in \mathbb{Z}$ gibt es eindeutige $a, r \in \mathbb{Z}$ mit
  $$x = ay + r,$$
  wobei $0 \leq r < |y|$.
- Der Rest r ist 0 genau dann, wenn y ein Teiler von x ist.

Beispiele

- Für $x = 8$ und $y = 2$ ist der Divisionsrest $r = 0$, denn $8 = 4 \cdot 2$.
- Für $x = 8$ und $y = 3$ ergibt Division mit Rest $8 = 2 \cdot 3 + 2$, also $a = 2$ und $r = 2$.



- Für $x = -8$ und $y = 3$ erhalten wir $a = -3$ und $r = 1$, denn $-8 = (-3) \cdot 3 + 1$.

Kongruenz modulo n

Wir führen die folgende Schreib- und Sprechweise ein:
Sind $x, y, n \in \mathbb{Z}$ und haben x und y bei Division durch n den gleichen Rest r, also

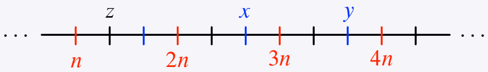
$$x = an + r, \quad y = bn + r$$

für gewisse Zahlen $a, b \in \mathbb{Z}$ und $0 \leq r < |n|$, so schreiben wir

$$x \equiv y \mod n$$

und sagen, x und y sind kongruent modulo n.

Beispiel
Hier ist $n = 3$. Die Zahlen x und y sind kongruent modulo 3.



Die Zahl z ist nicht kongruent zu x oder y modulo 3.
Beachte, dass der Abstand zwischen x und y genau $n = 3$ ist.

Untersuche die Beobachtung im letzten Beispiel:

- Sind $x = an + r$ und $y = bn + r$, so gilt

$$x - y = (an + r) - (bn + r) = (a - b)n,$$

  d.h. die Differenz ist ein Vielfaches von n.

- Gilt umgekehrt für zwei beliebige Zahlen $x, y \in \mathbb{Z}$, dass $x - y = kn$ ist, dann folgt nach Division mit Rest

$$kn = x - y = (an + r) - (bn + r') = (a - b)n + (r - r')$$

  oder äquivalent

$$(k - a + b)n = r - r'.$$

  Da $0 \leq r, r' < n$, ist auch $|r - r'| < |n|$. Auf der linken Seite steht aber ein Vielfaches von n, somit muss auf der rechten Seite $r - r' = 0 \cdot n$ stehen.

Wir haben somit bewiesen:

Hilfssatz 4.3
Es seien $x, y, n \in \mathbb{Z}$. Dann gilt $x \equiv y \mod n$ genau dann, wenn $x - y \in n\mathbb{Z}$ ist.

Sei $n \in \mathbb{Z}$. Die Menge der möglichen Reste modulo n ist

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

(Die Schreibweise $\mathbb{Z}/n\mathbb{Z}$ ist ebenfalls verbreitet.)

- Mit den Zahlen aus $\mathbb{Z}_n$ können wir wie in $\mathbb{Z}$ Additionen und Multiplikationen durchführen.
- Nun führen wir eine zusätzliche Rechenregel auf $\mathbb{Z}$ ein, die die Menge $\mathbb{Z}_n$ zu einem kommutativen Ring mit Eins macht.
- Diese Rechenregel lautet:

$$n = 0.$$

Was passiert, wenn wir die Rechenregel $n = 0$ einführen?

- Für alle Vielfachen von n gilt: $an = a \cdot 0 = 0$.
- Für beliebige $x \in \mathbb{Z}$ mit $x = an + r$ gilt: $x = an + r = a \cdot 0 + r = r$.
- Folge: *Jedes $x \in \mathbb{Z}$ wird durch die neue Regel identisch mit seinem Divisionsrest r bei Division durch n.*
- Es gilt also "$x = y$" für $x - y = an$ (äquivalent: $x \equiv y \bmod n$).

Wir definieren Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}_n$, indem wir $x, y \in \mathbb{Z}_n$ wie üblich in $\mathbb{Z}$ addieren (bzw. multiplizieren) und dann von $x + y$ (bzw. xy) den Rest modulo n nehmen.

Die Schreibweisen

$$x + y \bmod n,$$
$$xy \bmod n$$

sollen verdeutlichen, dass wir in $\mathbb{Z}_n$ und nicht in $\mathbb{Z}$ rechnen.

Satz 4.4
Es sei $n > 1$. Mit den eben definierten Verknüpfungen $+$ und $\cdot$ ist $\mathbb{Z}_n$ ein kommutativer Ring mit Eins.

Beweis

- Assoziativität und Kommutativität von $+$ und $\cdot$ sowie die Distributivgesetze für $\mathbb{Z}_n$ folgen sofort aus denen von $\mathbb{Z}$, sobald wir gezeigt haben, dass „Restbildung" mit den Operationen $+$ und $\cdot$ in $\mathbb{Z}$ verträglich ist.
  Genauer: Seien $x, x', y, y' \in \mathbb{Z}$. Falls $x \equiv x' \mod n$ und $y \equiv y' \mod n$, so gilt
  $$x + y = x' + y' \mod n,$$
  $$xy = x'y' \mod n.$$
  (Siehe Übungsblatt.)
- Die neutralen Elemente für $+$ und $\cdot$ sind natürlich $0 \in \mathbb{Z}_n$ und $1 \in \mathbb{Z}_n$.
- Das inverse Element für $+$ von $x \in \mathbb{Z}_n$ ist $n - x \in \mathbb{Z}_n$, denn
  $$x + (n - x) = n = 0 \mod n. \quad \square$$

Beispiele: $\mathbb{Z}_2$ und $\mathbb{Z}_5$

$\mathbb{Z}_2$

$+$	0	1
0	0	1
1	1	0

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

$\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

4.3 Körper

Erinnerung:

- $\mathbb{Z}$ mit $+$ und $\cdot$ ist ein kommutativer Ring mit Eins.
- Aber ± 1 sind die einzigen Elemente von $\mathbb{Z}$, die ein Inverses für die Multiplikation haben.
- $\mathbb{Q}$ und $\mathbb{R}$ sind mit $+$ und $\cdot$ ebenfalls kommutative Ringe mit Eins.
- Allerdings hat in $\mathbb{Q}$ oder $\mathbb{R}$ jedes Element $x \neq 0$ ein Inverses $x^{-1} = \frac{1}{x}$.

Definition

Es sei R ein Ring mit Eins. Die Menge

$$R^{\times} = \{x \in R \mid \text{ es gibt } x^{-1} \in R \text{ mit } xx^{-1} = 1 = x^{-1}x\}$$

wird die Einheitengruppe von R genannt.

Aufgabe (5 Minuten)

Zeige: $R^{\times}$ ist eine Gruppe (mit der Multiplikation als Verknüpfung).

Definition (kurz)

Ein kommutativer Ring mit Eins $\mathbb{K}$ wird Körper genannt, wenn gilt:

$$\mathbb{K}^{\times} = \mathbb{K} \backslash \{0\}.$$

Definition (etwas länger)

Eine Menge $\mathbb{K}$ mit zwei Verknüpfungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ wird Körper genannt, wenn folgendes gilt:

1. $\mathbb{K}$ bildet zusammen mit $+$ eine abelsche Gruppe.
2. $\mathbb{K} \backslash \{0\}$ bildet zusammen mit $\cdot$ eine abelsche Gruppe.
3. Es gelten die Distributivgesetze

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

   für alle $x, y, z \in \mathbb{K}$.

Wir wissen bereits, dass $\mathbb{Q}$ und $\mathbb{R}$ kommutative Ringe mit Eins sind.

- Für alle $\frac{p}{q} \in \mathbb{Q}\backslash\{0\}$ ist $\frac{q}{p} \in \mathbb{Q}\backslash\{0\}$.
- Für alle $x \in \mathbb{R}\backslash\{0\}$ ist $x^{-1} = \frac{1}{x} \in \mathbb{R}\backslash\{0\}$.

Somit sind sowohl $\mathbb{Q}$ als auch $\mathbb{R}$ Körper.

Komplexe Zahlen

Wir wissen, dass die negativen Zahlen in $\mathbb{R}$ keine Quadratwurzeln haben, d.h. es gibt keine Zahl $x \in \mathbb{R}$ mit

$$x^2 + 1 = 0.$$

Wir erweitern nun die reellen Zahlen um eine sogenannte imaginäre Einheit i mit der Eigenschaft

$$\mathrm{i}^2 = -1.$$

Dies führt zu:

Definition

Die Menge der komplexen Zahlen ist

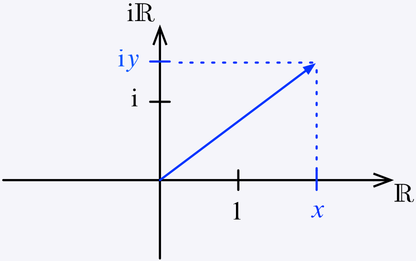
$$\mathbb{C} = \{x + \mathrm{i}y \mid x, y \in \mathbb{R}\}.$$

Für $z = x + \mathrm{i}y$ nennen wir $x = \mathrm{Re}(z)$ den Realteil von z und $y = \mathrm{Im}(z)$ den Imaginärteil von z (beachte: dies sind beides *reelle* Zahlen).

Die Menge der komplexen Zahlen ist

$$\mathbb{C} = \{x + \mathrm{i}y \mid x, y \in \mathbb{R}\}.$$

Wir können diese Menge geometrisch mit der Ebene identifizieren, wobei die Achsen die reellen Zahlen $\mathbb{R}$ und die imaginäre Achse $\mathrm{i}\mathbb{R}$ sind.



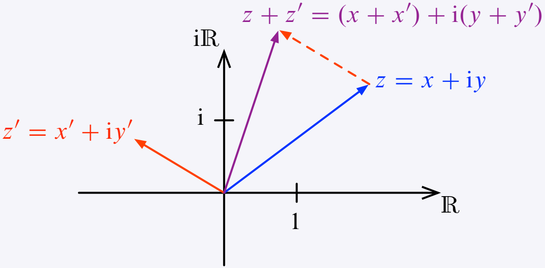
Diese Darstellung wird oft als Gaußsche Zahlenebene bezeichnet.

Die geometrische Sichtweise macht die Definition des Betrags $|z|$ einer komplexen Zahl $z = x + \mathrm{i}y$ klar:

$$|z| = \sqrt{x^2 + y^2}.$$

Wir können auf $\mathbb{C}$ eine Addition definieren. Sei $z = x + \mathrm{i}y$ und $z' = x' + \mathrm{i}y'$. Dann ist ihre Summe

$$z + z' = (x + x') + \mathrm{i}(y + y').$$



(Würden wir die Punkte der Ebene durch $\binom{x}{y}$ darstellen, entspräche dies der üblichen Vektoraddition.)

Multiplikation

Wir können auch eine Multiplikation auf $\mathbb{C}$ definieren, indem wir die Regel $i^2 = -1$ berücksichtigen: Für $z, z' \in \mathbb{C}$ ist

$$\begin{aligned} zz' &= (x + iy)(x' + iy') = xx' + iyx' + xiy' + i^2 yy' \\ &= (xx' - yy') + i(xy' + x'y). \end{aligned}$$

In anderen Worten,

$$\operatorname{Re}(zz') = xx' - yy', \qquad \operatorname{Im}(zz') = xy' + x'y.$$

Beobachtung

Diese Multiplikation ist kommutativ, weil die Multiplikation der reellen Zahlen es ist.

Beobachtung

Ist α der Winkel, den $z \in \mathbb{C}$ mit der reellen Achse $\mathbb{R}$ einschließt, so ist

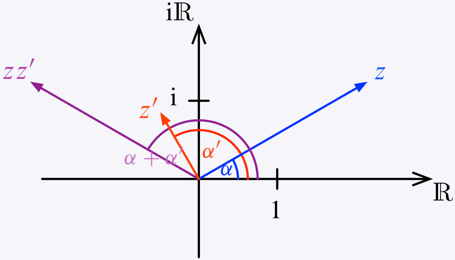
$$x = \cos(\alpha)|z|, \quad y = \sin(\alpha)|z|.$$

Wir können die Multiplikation anschaulicher machen, wenn wir $z = x + \mathrm{i}y$ schreiben als

$$z = |z|\big(\cos(\alpha) + \mathrm{i}\sin(\alpha)\big).$$

Dann ist

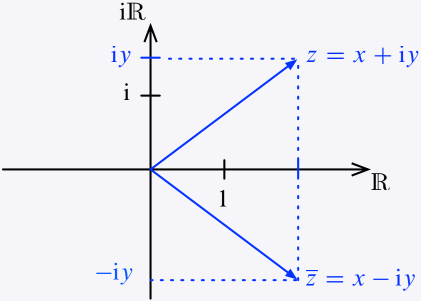
$$zz' = |z||z'|\big(\cos(\alpha + \alpha') + \mathrm{i}\sin(\alpha + \alpha')\big).$$



Eine weitere Operation auf den komplexen Zahlen ist die komplexe Konjugation. Sie entspricht der Spiegelung an der reellen Achse. Für $z = x + \mathrm{i}y$ ist

$$\overline{z} = x - \mathrm{i}y$$

die komplex konjugierte Zahl.



Beobachtung

$$z\overline{z} = (x + \mathrm{i}y)(x - \mathrm{i}y) = x^2 + y^2 = |z|^2.$$

Folgerung

Jede komplexe Zahl $z \neq 0$ hat ein Inverses:

$$z \frac{\overline{z}}{|z|^2} = \frac{z\overline{z}}{|z|^2} = 1 (= 1 + \mathrm{i} \cdot 0).$$

Also:

$$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{x - \mathrm{i}y}{x^2 + y^2}.$$

Satz 4.3

Die komplexen Zahlen $\mathbb{C}$ mit der oben definierten Addition und Multiplikation bilden einen Körper.

Beweis

- Die Addition ist assoziativ und kommutativ, da sie komponentenweise durch reelle Zahlen erfolgt.
- Das Nullelement ist $\mathbf{0}(= 0 + \mathrm{i} \cdot 0) \in \mathbb{C}$.
  Das additiv Inverse von $z = x + \mathrm{i}y$ ist $-z = -x - \mathrm{i}y$.
- Die Multiplikation ist kommutativ. Assoziativität: Übung.
- Das Einselement ist $\mathbf{1} = (1 + \mathrm{i} \cdot 0) \in \mathbb{C}$.
  Das multiplikativ Inverse von $z \neq \mathbf{0}$ ist $z^{-1} = \frac{\overline{z}}{|z|^2}$. $\square$

Endliche Körper

$\mathbb{Z}_p$ mit Primzahl p

Wir wissen, dass $\mathbb{Z}_n$ für $n \in \mathbb{N}$ ein kommutativer Ring mit Eins ist.
Wann ist $\mathbb{Z}_n$ ein Körper?

- Dazu muss lediglich jedes $x \in \mathbb{Z}_n \backslash \{0\}$ ein Inverses haben.
- Ist x ein Teiler von n, etwa $ax = n$ für $a \in \mathbb{Z} \backslash \{0\}$, so ist $ax = 0 \mod n$.
- Hätte so ein $x \mod n$ ein Inverses x^{-1} in $\mathbb{Z}_n$, so wäre

  $$0 = 0 \cdot x^{-1} = axx^{-1} = a \neq 0 \mod n,$$

  ein Widerspruch.
- Somit darf n keine Teiler haben, muss also eine Primzahl p sein.
- Ist die Existenz eines Inversen x^{-1} für alle $x \in \mathbb{Z}_p$ garantiert, wenn p prim ist?
- Ja! Der erweiterte Euklidische Algorithmus erlaubt es, den ggT zweier Zahlen $x, y \in \mathbb{Z}$ zu bestimmen, und außerdem Zahlen $a, b \in \mathbb{Z}$ mit

  $$ax + by = \mathrm{ggT}(x, y).$$

- Ist p prim und $x \in \mathbb{Z}_p \backslash \{0\}$, so liefert dies $ax + bp = \mathrm{ggT}(x, p) = 1$, also

  $$ax = 1 \mod p.$$

  Also $a = x^{-1} \mod p$.

Satz 4.4
$\mathbb{Z}_p$ ist genau dann ein Körper, wenn p eine Primzahl ist.

$\mathbb{Z}_4$ ist kein endlicher Körper

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$ ist ein endlicher Körper

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Satz 4.5

1. *Jeder endliche Körper $\mathbb{F}$ hat Kardinalität $|\mathbb{F}| = p^k$ für eine Primzahl p und $k \in \mathbb{N}$.*
2. *Für jede Primzahlpotenz p^k gibt es nur einen einzigen Körper $\mathbb{F}$ mit $|\mathbb{F}| = p^k$ (bis auf „Umbenennung" der Elemente).*

(Ohne Beweis.)

Für den eindeutigen Körper mit $|\mathbb{F}| = p^k$ schreiben wir $\mathbb{F}_{p^k}$.
Die Schreibweise $\mathrm{GF}(p^k)$ ist auch verbreitet (für „Galois Field").

Folgerung
$\mathbb{F}_{p^k} = \mathbb{Z}_{p^k}$ *genau dann, wenn* $k = 1$.