

## 2 Script zur Vorlesung: Lineare Algebra I

Prof. Dr. Salma Kuhlmann

Aus Divisionsalgorithmus: Sei  $n \in \mathbb{N}$ .  $\mathbb{Z}_n := \{0, \dots, n-1\}$  ist die Menge der "Reste" für die Division durch  $n$ .

### Bezeichnung 2.1.

$a \in \mathbb{Z}$ ;  $\bar{a} :=$  Rest der Division von  $a$  durch  $n$ .

i.e.  $a = qn + \bar{a} \quad 0 \leq \bar{a} < n$

i.e. mit  $\bar{a} \in \{0, \dots, n-1\}$ .

Wir definieren eine Verknüpfung:

Für  $x, y \in \mathbb{Z}_n$  definiere  $x +_n y := \overline{x + y}$ .

### Behauptung 2.2.

$(\mathbb{Z}_n, +_n)$  ist eine abelsche Gruppe.

**Fall 1**  $n = 1$   $\mathbb{Z}_n = \{0\}$  die *triviale* Gruppe.

**Fall 2** Sei  $n \geq 2$ .

• Kommutativ? Seien  $x, y \in \mathbb{Z}_n$ .  $x +_n y = y +_n x$  ?

L.S. berechnen:

$$x +_n y \quad = \quad \overline{x + y} \quad = \quad \overline{y + x} \quad = \quad y +_n x$$

Def. von  $+_n$  weil  $(\mathbb{Z}, +)$  Def. von  $+_n$   
abelsche Gruppe

• Assoziativ? Seien  $x, y, z \in \mathbb{Z}_n$ .

$$(x +_n y) +_n z \quad = \quad x +_n (y +_n z)$$

?

Berechne L.S.:

Setze  $\overline{x + y} = r_1$  und  $\overline{r_1 + z} := r_2$ .

Also  $x + y = q_1n + r_1$ , und  $r_1 + z = q_2n + r_2$ .

Also  $(x + y) + z = (q_1 + q_2)n + r_2$ . (\*)

Berechnung der R.S.:

Setze  $\overline{y + z} := r_3$  und  $\overline{x + r_3} := r_4$ .

Also  $y + z = q_3n + r_3$  und  $x + r_3 = q_4n + r_4$ .

Also  $x + (y + z) - q_3n = q_4n + r_4$ .

Also  $x + (y + z) = (q_3 + q_4)n + r_4$ . (\*\*)

Nun vergleiche (\*) und (\*\*) und beachte, dass  $(x + y) + z = x + (y + z)$  in  $\mathbb{Z}$ .

$$\begin{aligned} \text{Also } (x + y) + z &= (q_1 + q_2)n + r_2 = \\ x + (y + z) &= (q_3 + q_4)n + r_4 \end{aligned}$$

Eindeutigkeit von Rest im Divisionsalgorithmus  $\Rightarrow r_2 = r_4$

i.e.  $\overline{x + y + z} = \overline{x + \overline{y + z}}$

i.e.  $(x +_n y) +_n z = x +_n (y +_n z)$  wie erwünscht.

- Ex. von neutralem Element  $0 \in \mathbb{Z}_n$ . Sei  $x \in \mathbb{Z}_n$ .

$$x +_n 0 \stackrel{?}{=} x$$

$$x +_n 0 = \overline{x + 0} = \bar{x}.$$

Aber für  $x \in \mathbb{Z}_n$  gilt  $\bar{x} = x$ . Also  $x +_n 0 = x$ .

- Ex. von additiven Inversen.

Sei  $x \in \{0, 1, \dots, n-1\}$ . Falls  $x = 0$ , setze  $-x = 0$ .

Sei nun  $x \neq 0$  und setze  $-x := (n - x) \in \mathbb{Z}_n$ .

Es gilt  $x +_n (-x) = \overline{x + (-x)} = \bar{n} = 0$  wie erwünscht.

### Definition 2.3.

Ein Tripel  $(R, +, \cdot)$  ist ein *Ring mit Eins*, falls:

- $R$  ist eine nichtleere Menge und
- $+, \cdot$  sind Verknüpfungen auf  $R$  und
- $(R, +)$  ist eine abelsche Gruppe mit neutralem Element  $0 \in R$  und  $(R, \cdot)$  ist ein *Monoid*, d.h.
- $\cdot$  ist assoziativ und es existiert  $1 \in R$  mit  $x \cdot 1 = 1 \cdot x = x \forall x \in R$  und
- $1 \neq 0$  und
- die Distributivitätsgesetze gelten:

Links:  $x \cdot (y + z) = (x \cdot y) + (x \cdot z) \forall x, y, z \in R$  und

Rechts:  $(y + z) \cdot x = (y \cdot x) + (z \cdot x) \forall x, y, z \in R$

### Definition 2.4.

Ein Ring  $(R, +, \cdot)$  ist *kommutativ* falls  $x \cdot y = y \cdot x \forall x, y \in R$ .

**Beispiel 2.5.** $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot).$ 

Gibt es endliche Beispiele?

Auf  $\mathbb{Z}_n$  definieren wir:  $x \cdot_n y := \overline{xy}$ .

Übungsaufgabe: Prüfe, dass für  $n > 1$   $(\mathbb{Z}_n, +_n, \cdot_n)$  ein kommutativer Ring mit Eins ist.

**Bezeichnung 2.6.** $F^\times := F \setminus \{0\}.$ **Definition 2.7.**

$(F, +, \cdot)$  ist ein *Körper*, falls  $F \neq \emptyset$ ,  $(F, +)$  und  $(F^\times, \cdot)$  abelsche Gruppen sind mit 0 bzw. 1 als neutrale Elemente,  $1 \neq 0$  und die Distributivitätsgesetze gelten.

**Bemerkung 2.8.**

Also  $(F, +, \cdot)$  ist ein Körper, falls  $(F, +, \cdot)$  ein kommutativer Ring mit Eins ist und alle  $x \in F^\times$  sind *multiplikativ invertierbar*, d.h.  $\exists x^{-1} \in F^\times$  mit  $x \cdot x^{-1} = 1$ .

**Beispiel 2.9.**

$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$  und später  $(\mathbb{C}, +, \cdot)$  sind Körper.

**Frage**

Gibt es endliche Körper? Insbesondere betrachten wir nun die Frage:

Ist der Ring  $(\mathbb{Z}_n, +, \cdot)$  ein Körper?

Wir werden zeigen:  $(\mathbb{Z}_n, +, \cdot)$  ist ein Körper, genau dann, wenn  $n = p$  Primzahl.