21. 10. 2011

2. Vorlesung

Aus Divisionsalgorithmus: Sei $n \in \mathbb{N}$; $n > 1$

$\mathbb{Z}_n := \{0, \ldots, n-1\}$ ist die Menge der "Reste" für die Division durch n.

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

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

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

Wir definieren eine Verknüpfung:

$x, y \in \mathbb{Z}_n$

definiere

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

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

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

Fall 2 Sei $n \geq 2$. Die Verknüpfung ist wohldefiniert. ✓

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

$$x +_n y \overset{?}{=} y +_n x$$

l.S berechnen:

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

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

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

$$(x +_n y) +_n z \overset{?}{=} x +_n (y +_n z)$$

Berechne l. S:

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

Also: $x+y = q_1 n + r_1$ und $\overline{r_1+z} = q_2 n + r_2$

Also $(x+y-q_1 n) + z = q_2 n + r_2$

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

Berechnung der R.S.:

Setze $\overline{y+z} := r_2$ und $\overline{x+r_3} := r_4$

Also $y+z = q_3 n + r_3$ und $x+r_3 = q_4 n + r_4$

Also $x + (y+z) - q_3 n = q_4 n + r_4$

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

Nun vergleiche (*) und (**) und beachte

dass $(x+y)+z = x+(y+z)$ in $\mathbb{Z}$.

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

$x+(y+z) = (q_3 + q_4) n + r_4$

Eindeutigkeit vom Rest in DA $\Rightarrow$

$r_2 = r_4$

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

i.e

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

wie erwünscht. ∎

- $\exists^z$ von neutralem Element $0 \in \mathbb{Z}_n$

Sei $x \in \mathbb{Z}_n$

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

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

Aber für $x \in \mathbb{Z}_n$ gelt: $\overline{x} = x$

Also $x +_n 0 = x$. □

- $\exists^z$ 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:

$$x +_n (-x) = \overline{x + (-x)}$$

$$= \overline{n} = 0 \quad \text{wie erwünscht.} \quad \square$$

— 11 21.10.2014

Definition 1: Ein Triple $(R, +, \cdot)$ 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

$$x \cdot 1 = 1 \cdot x = x \quad \forall x \in R$$

und

- $1 \neq 0$

- und die Distributivitätsgesetze gelten:

Links: $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$ und

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

Definition 2 Ein Ring $(R, +, \cdot)$ ist kommutativ falls: $x \cdot y = y \cdot x \quad \forall x, y \in R$.

Beispiele $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.

Gibt es endliche Beispiele?

Auf $\mathbb{Z}_n$ definieren wir:

$$x \cdot_n y := \overline{x\,y}$$

üA: Prüfe daß $(\mathbb{Z}, +_n, \cdot_n)$ ist ein kommutativer Ring mit Eins.

Bezeichnung: $F^\times := F \setminus \{0\}$.

Definition 3 $(F, +, \cdot)$ ist ein Körper falls $F \neq \emptyset$, $(F, +)$ und $(F^\times, \cdot)$ sind abelsche Gruppen mit 0, bzw. 1 als neutrale Elemente, $1 \neq 0$ und die distributivitätsgesetze

gelten.

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

Beispiele: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ 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 $n = p$