17. Vorlesung 18.11.2020

Notiztitel 18.11.2020

Heute (18.11.) 12:00 Uhr bis morgen (19.11.) 18:00 Uhr 1. edX-Test !

$b, m \in \mathbb{Z} \Rightarrow \underbrace{b = k \cdot m + r \text{ mit } 0 \leq r < |m|}_{\text{Division mit Rest}}$

speziell mit $m \in \mathbb{N}$ (also $m \geq 1$): $b = k \cdot m + r$ mit $0 \leq r < m$

r ist der Rest, der beim ganzzahligen Teilen von b durch m entsteht

Bezeichnung: Gauß: r heißt Modul von b bezüglich m und schreibt dafür $r = b \bmod m$ ← Rest, der beim Teilen von b durch m bleibt

also $r = b \bmod m \iff b = k \cdot m + r$ mit $0 \leq r < m$

als Rest r kommen nur die Zahlen $0, 1, 2, \dots, m-1$ in Frage (denn falls $r = m + l$ für ein $l \in \mathbb{N}_0$ gilt: $b = k \cdot m + r = k \cdot m + (m + l) = (k+1) \cdot m + l \Rightarrow l = b \bmod m$) ← $r \in \mathbb{N}_0$

Die möglichen Reste $0, 1, 2, \dots, m-1$ beim ganzzahligen Teilen durch m liefern uns folgende Mengen:

$$\overline{0} = \{ b \in \mathbb{Z} \mid b = k \cdot m \} = \{ b \in \mathbb{Z} \mid b = k \cdot m + 0 \}$$
$$\overline{1} = \{ b \in \mathbb{Z} \mid b = k \cdot m + 1 \}$$
$$\vdots$$
$$\overline{m-1} = \{ b \in \mathbb{Z} \mid b = k \cdot m + (m-1) \}$$

Beispiel: $m = 3 \Rightarrow$

$$\overline{0} = \{ b \in \mathbb{Z} \mid b = k \cdot 3 \} = \{ \dots, -9, -6, -3, 0, 3, 6, 9, 12, \dots \}$$
$$\overline{1} = \{ b \in \mathbb{Z} \mid b = k \cdot 3 + 1 \} = \{ \dots, -8, -5, -2, 1, 4, 7, 10, \dots \}$$
↳ $-2 = (-1) \cdot 3 + 1$
$$\overline{2} = \{ b \in \mathbb{Z} \mid b = k \cdot 3 + 2 \} = \{ \dots, -7, -4, -1, 2, 5, 8, 11, \dots \}$$

$\overline{0} \cup \overline{1} \cup \overline{2} = \mathbb{Z}$

$\overline{0} \cap \overline{1} = \emptyset$

$\overline{1} \cap \overline{2} = \emptyset$

$\overline{2} \cap \overline{0} = \emptyset$

Teilen durch m ($m \in \mathbb{N}$) und Äquivalenzrelationen

Die zweistellige Relation $R_m \subseteq \mathbb{Z} \times \mathbb{Z}$ über $\mathbb{Z}$ ist definiert durch:

$$(a,b) \in R_m \Leftrightarrow m \mid b-a \Leftrightarrow b-a = k \cdot m \text{ für ein } k \in \mathbb{Z}$$

Behauptung:

1) R_m ist eine Äquivalenzrelation
2) Für $m \in \mathbb{N}$ sind die Äquivalenzklassen gerade die Mengen $\overline{0}, \overline{1}, \ldots, \overline{m-1}$

Beweis:

$\Rightarrow (a,b) \in R_m \wedge (b,c) \in R_m \Rightarrow (a,c) \in R_m$

1) reflexiv, symmetrisch, transitiv
   - $\hookrightarrow (a,a) \in R_m$
   - $\hookrightarrow (a,b) \in R_m \Rightarrow (b,a) \in R_m$

a) reflexiv: $(a,a) \in R_m \ \forall a \in \mathbb{Z}$; denn $a-a = 0 = 0 \cdot m$
$\Rightarrow m \mid a-a$

b) symmetrisch: $(a,b) \in R_m \Rightarrow b-a = k \cdot m$
$\Rightarrow a-b = (-k) \cdot m$
$\Rightarrow m \mid a-b \Rightarrow (b,a) \in R_m$

c) transitiv: $(a,b) \in R_m \wedge (b,c) \in R_m \Rightarrow$
$b-a = k \cdot m \wedge c-b = \tilde{k} \cdot m \Rightarrow$
$c-a = (c-b)+(b-a)$
$= \tilde{k} \cdot m + k \cdot m = (\tilde{k}+k) \cdot m$
$\Rightarrow m \mid c-a \Rightarrow (a,c) \in R_m$

2) zugehörige Äquivalenzklassen
$\overline{a}$ ist Äquivalenzklasse zu a in $R_m \Rightarrow$

$$\overline{a} = \{ b \in \mathbb{Z} \mid (a,b) \in R_m \}$$
$$= \{ b \in \mathbb{Z} \mid b-a = k \cdot m \}$$
$$= \{ b \in \mathbb{Z} \mid b = k \cdot m + a \}$$

← Menge aller ganzer Zahlen, die beim Teilen durch m den Rest a lassen

Beim Teilen durch m gibt es die Reste $0, 1, 2, \ldots, m-1$

mit den Mengen $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1} \Rightarrow \overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$

Definition: Für $m \in \mathbb{N}$, $m \geq 2$ ist definiert

$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ die Menge der Äquivalenzklassen der Relation R_m. Für $\overline{k} \in \mathbb{Z}_m$ gilt also: Jede Zahl in $\overline{k}$ lässt beim Teilen durch m den Rest k ($0 \leq k \leq m-1$).

Rechenoperationen in $\mathbb{Z}_m$:

Beispiel: $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$\overline{1} \leftarrow b = k \cdot 5 + 1$
$\overline{2} \leftarrow \tilde{b} = \tilde{k} \cdot 5 + 2$

$b + \tilde{b} = (k+\tilde{k}) \cdot 5 + 1 + 2 = \overbrace{(k+\tilde{k})}^{\ell} \cdot 5 + 3 = \ell \cdot 5 + 3$

$\Rightarrow b + \tilde{b} \in \overline{3}$

↑ Repräsentanten von $\overline{1}, \overline{2}$

$\overline{1} + \overline{2} = \overline{3}$

$\overline{2} \leftarrow \tilde{b} = \tilde{k} \cdot 5 + 2$
$\overline{4} \leftarrow b = k \cdot 5 + 4$

$b + \tilde{b} = \overbrace{(k+\tilde{k})}^{\ell} \cdot 5 + 2 + 4 = \ell \cdot 5 + 6 = \ell \cdot 5 + (5+1)$
$= (\ell+1) \cdot 5 + 1$

↑ Repräsentanten von $\overline{2}, \overline{4}$ $\Rightarrow b + \tilde{b} \in \overline{1}$

$\overline{2} + \overline{4} (= \overline{6}) = \overline{1}$

↳ $6 = 1 \cdot 5 + 1 \Rightarrow \overline{6} = \overline{1}$

Addition in $\mathbb{Z}_m$ ist definiert durch

$\overline{\ell}, \overline{k} \in \mathbb{Z}_m \Rightarrow \overline{\ell} + \overline{k} = \overline{\underbrace{(\ell+k) \bmod m}} = \overline{\ell+k}$

Rest, der beim Teilen von $\ell+k$ durch m bleibt

Strich über ℓ heißt: Bestimme den Rest von ℓ beim Teilen durch m

$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ ist eine endliche Menge, die Addition kann man dann in einer Verknüpfungstabelle darstellen

Beispiel: $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\bar{0}$ ist das neutrale Element der Addition in $\mathbb{Z}_5$, das inverse Element zu $\bar{1}$ bez. der Addition in $\mathbb{Z}_5$ ist $\bar{4}$, denn $\bar{1}+\bar{4}=\bar{0}$,
ebenso: $\bar{2}+\bar{3}=\bar{0}$, $\bar{3}+\bar{2}=\bar{0}$, $\bar{4}+\bar{1}=\bar{0}$

Verknüpfungstafel spiegelsymmetrisch zur Diagonalen $\Rightarrow \bar{k}+\bar{l}=\bar{l}+\bar{k}$

diese Verknüpfung (Addition) ist Kommutativ

$$\bar{3}+(\bar{4}+\bar{2}) = \overline{3+(4+2)} = \overline{(3+4)+2} = (\bar{3}+\bar{4})+\bar{2}$$

(Assoziativgesetz in $\mathbb{Z}$)

Für die Addition in $\mathbb{Z}_5$ gilt auch das Assoziativgesetz!

insgesamt: $(\mathbb{Z}_5, +)$ ist eine abelsche (kommutative) Gruppe

allgemein: $(\mathbb{Z}_m, +)$ ist eine abelsche (kommutative) Gruppe
für $m \in \mathbb{N}$, $m \geq 2$

Assoziativgesetz gilt (s.o. Rechnen in $\mathbb{Z}$)

Multiplikation in $\mathbb{Z}_m$ ist definiert durch: $\bar{k} \cdot \bar{l} = \overline{k \cdot l}$

Beispiel: $\mathbb{Z}_5$; die Multiplikation regelt folgende Verknüpfungstabelle

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{1}$ ist das neutrale Element bezüglich der Multiplikation in $\mathbb{Z}_5$

$\mathbb{Z}_5^* = \mathbb{Z}_5 \setminus \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ ← in jeder Zeile der Teiltabelle steht genau einmal $\bar{1}$, d.h. jedes $\bar{k} \in \mathbb{Z}_5^*$ hat bezügl. der Multiplikation ein inverses Element, z.B. $\bar{3} \cdot \bar{2} = \bar{1}$

Spiegelsymmetrie zur Diagonale

die Multiplikation in $\mathbb{Z}_5$ ist Kommutativ

Distributivgesetz: $\bar{k} \cdot (\bar{l} + \bar{m}) = \overline{k \cdot (l+m)} = \overline{(k \cdot l) + (k \cdot m)} = \overline{(k \cdot l)} + \overline{(k \cdot m)}$
$= \bar{k} \cdot \bar{l} + \bar{k} \cdot \bar{m}$

(Distributivgesetz in $\mathbb{Z}$)

insgesamt $(\mathbb{Z}_5, +, \cdot)$ ist ein Körper (endlicher Körper mit 5 Elementen)

Beispiel: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Es gibt kein $\bar{k} \in \mathbb{Z}_4$ mit $\bar{2} \cdot \bar{k} = \bar{1}$
d.h. zu $\bar{2} \in \mathbb{Z}_4$ gibt es bezgl. der Multiplikation kein inverses Element
$\mathbb{Z}_4^* = \mathbb{Z}_4 \setminus \{\bar{0}\}$ ist keine Gruppe

$\Rightarrow (\mathbb{Z}_4, +, \cdot)$ ist kein Körper sonder (nur) ein Kommutativer Ring mit Eins!

allgemein: $(\mathbb{Z}_m, +, \cdot)$ ist ein Kommutativer Ring mit Eins.

Frage: Wann hat $\bar{k} \in \mathbb{Z}_m$ ein inverses Element bezüglich der Multiplikation in $\mathbb{Z}_m$? Wann ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper?

Satz:
Für $\bar{k} \in \mathbb{Z}_m$ gilt: $\bar{k}$ hat ein inverses Element bezüglich der Multiplikation in $\mathbb{Z}_m$, falls $ggT(k, m) = 1$ ist (d.h. k und m sind teilerfremd).

Beweisidee: Angenommen $ggT(k, m) = 1$, dann gibt es nach dem Lemma von Bézout ganze Zahlen $s, t \in \mathbb{Z}$ mit $1 = s \cdot k + t \cdot m$, damit gilt für die Reste beim Teilen durch m

$$\bar{1} = \overline{s \cdot k + t \cdot m} = \bar{s} \cdot \bar{k} + \bar{t} \cdot \bar{m} \quad \leftarrow \bar{m} = \bar{0} \text{ in } \mathbb{Z}_m$$
$$= \bar{s} \cdot \bar{k} + \bar{t} \cdot \bar{0} \quad \leftarrow \bar{t} \cdot \bar{0} = \bar{0}$$
$$= \bar{s} \cdot \bar{k}$$

Es gilt also $\bar{1} = \bar{s} \cdot \bar{k}$ d.h. $\bar{s}$ ist das inverse Element zu $\bar{k}$ bezüglich der Multiplikation in $\mathbb{Z}_m$.

Beispiel: $\mathbb{Z}_{42}$; gesucht ist die Inverse bezgl. der Multiplikation zu $\overline{5}$ in $\mathbb{Z}_{42}$ (falls es sie gibt).

↳ Inverse existiert, falls $ggT(42,5) = 1$ ist

$$42 = 8 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1 \quad \leftarrow ggT(42,5) = 1$$
$$2 = 2 \cdot 1 + 0$$

Anwendung des Lemmas von Bézout:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (42 - 8 \cdot 5) \\ &= 17 \cdot 5 + (-2) \cdot 42 \end{aligned}$$

Reste beim Teilen durch 42 bilden!

$$\Rightarrow \overline{1} = \overline{17 \cdot 5 + (-2) \cdot 42}$$
$$= \overline{17} \cdot \overline{5} + \overline{(-2)} \cdot \underbrace{\overline{42}}_{=\overline{0}}$$
$$= \overline{17} \cdot \overline{5}$$

$\Rightarrow \overline{17}$ ist die Inverse zu $\overline{5}$ bezgl. der Multiplikation in $\mathbb{Z}_{42}$.

Probe:

$$17 \cdot 5 = 85 = 2 \cdot 42 + 1 \Rightarrow \overline{17} \cdot \overline{5} = \overline{1}$$