7

Vorlesung 7

F.105 **Bsp.:**

① $(8,12) \in \equiv_4 \iff 8 \equiv_4 12$,

da $4 \mid 4 = 12 - 8$

② $(8,12) \notin \equiv_3 \iff 8 \not\equiv_3 12$,

da $3 \nmid 4 = 12 - 8$

③ $(100, 12) \notin \equiv_3$,

da $3 \nmid -88 = 12 - 100$

F.106 **Bew. Satz:**

[z.z.: $\equiv_m$ ist reflexiv, d.h.: $\forall x \in \mathbb{Z} : x \equiv_m x$]

Sei $x \in \mathbb{Z}$. Es gilt:

$m \mid 0 = x - x$. Also gilt: $x \equiv_m x$.

$\boxed{m \cdot 0 = 0}$

[z.z.: $\equiv_m$ ist symmetrisch,

d.h.: $\forall x,y \in \mathbb{Z}: x \equiv_m y \Rightarrow y \equiv_m x$]

Seien $x,y \in \mathbb{Z}$. Es gelte: $x \equiv_m y$.

[z.z.: $y \equiv_m x$, d.h.: $m \mid x-y$,

d.h.: $\exists c \in \mathbb{Z}: m \cdot c = x - y$]

Nach Vor. gilt: $m \mid y-x$. Also ex.

ein $c' \in \mathbb{Z}$ mit (I) $m \cdot c' = y-x$.

Multiplizieren der Gl. (I) mit -1 ergibt:

(II) $m \cdot (-c') = -m \cdot c' = -(y-x) = -y+x = x-y$.

Setze $c := -c' \in \mathbb{Z}$. Es gilt mit (II):

$$m \cdot c = m(-c') \underset{(II)}{=} x-y.$$

[z.z.: $\equiv_m$ ist transitiv,

d.h.: $\forall x,y,z \in \mathbb{Z}: x \equiv_m y \wedge y \equiv_m z \Rightarrow x \equiv_m z$]

Seien $x,y,z \in \mathbb{Z}$. Es gelte: $x \equiv_m y$ und $y \equiv_m z$.

[z.z.: $x \equiv_m z$, d.h.: $m \mid z-x$,

d.h. $\exists c \in \mathbb{Z}: m \cdot c = z-x$]

Nach Vor. gilt: $m \mid y-x$ und $m \mid z-y$. (3)

Also ex. $c', c'' \in \mathbb{Z}$ mit

$$(I)\ m \cdot c' = y-x \quad \text{und} \quad (II)\ m \cdot c'' = z-y.$$

Addition der Gl. (I) und (II) liefert:

$$(III)\ m\cdot(c'+c'') = m\cdot c' + m\cdot c'' = \cancel{y} - x + z - \cancel{y} = z-x.$$

Setze $c := c'+c'' \in \mathbb{Z}$. Es gilt mit (III):

$$m \cdot c = m\cdot(c'+c'') \underset{(III)}{=} z-x. \quad //$$

F.107

$$[0]_2 = \{a \in \mathbb{Z} \mid \underbrace{a \equiv_2 0}\}$$

$$\Leftrightarrow 0 \equiv_2 a$$

$$\Leftrightarrow 2 \mid a-0 = a$$

$$|\mathbb{Z}_m| = m$$

$$\mathbb{Z}_m = \{[0]_m, \dots, [m-1]_m\}$$

$$= \{[1]_m, \dots, [m]_m\}$$

F.109 Bew. Satz:

Der Beweis wurde in DM1 Teil 1 durchgeführt, aber nur für $b \in \mathbb{N}$ und $a \in \mathbb{N}_0$. //

Idee:

$$12 : 5 = \overset{q}{2}\, R\, \overset{r}{2}$$

Darstellungen

$$\underset{a}{12} = \underset{q}{2} \cdot \underset{b}{5} + \underset{r}{2}$$

$$\boxed{0 \leq r < |b|}$$

Forderung für Eindeutigkeit

$$= \underset{q}{3} \cdot 5 \underbrace{- 3}_{r}$$

$$= \underset{q}{1} \cdot 5 + \underset{r}{7} = 1 \cdot 5 + 1 \cdot 5 + 2 = 2 \cdot 5 + 2$$

Zur Beobachtung:

$$[12]_5 \xrightarrow{-5} [7]_5 \xrightarrow{-5} [2]_5$$

$$[12]_5 = [7]_5 = [2]_5$$

F. 110

[z.z.: $\left(\exists x \in \mathbb{Z} : a,b \in [x]_m\right) \iff r_a = r_b$]

Zunächst beweisen wir ein Hilfsbeh.:

$$\forall c \in \mathbb{Z} : [c]_m = [r_c]_m$$

Sei $c \in \mathbb{Z}$. Nach dem Satz von F. 108 ex. $q, r_c \in \mathbb{Z}$ mit $c = q \cdot m + r_c$ und $0 \leq r_c < m$.

Damit ergibt sich: $q \cdot m = c - r_c$.

Also gilt: $m \mid c - r_c$. Damit gilt: $r_c \equiv_m c$.

Nach Satz von F. 97 gilt: $[c]_m = [r_c]_m$.

„$\Longrightarrow$": Es gelte: $\exists x \in \mathbb{Z}: a,b \in [x]_m$.

Wähle ein $x \in \mathbb{Z}$ mit $a,b \in [x]_m$. $\boxed{0 \leq r_x < m}$

Nach Hilfsbeh. gilt: $a,b \in [x]_m = [r_x]_m$.

Damit gilt: $a \equiv_m r_x$ und $b \equiv_m r_x$

Also gilt: $m \mid r_x - a$ und $m \mid r_x - b$.

Nach Def. „$\mid$" ex. $c', c'' \in \mathbb{Z}$ mit

$m \cdot c' = r_x - a \iff a = m \cdot (-c') + r_x$ und

$m \cdot c'' = r_x - b \iff b = m \cdot (-c'') + r_x$.

Also gilt mit der Eindeutigkeit (Teilen mit Rest):

$r_a = r_x = r_b$.

"$\Leftarrow$": Es gelte: $r_a = r_b$. Mit der Hilfsbeh. ergibt sich: $[a]_m = [r_a]_m = [r_b]_m = [b]_m$

Setze $x := r_a \in \mathbb{Z}$. Dann gilt:

$a, b \in [r_a]_m = [x]_m$.

Bsp.:

$$0 + 5\mathbb{Z} = 5\mathbb{Z} = \{0, 5, 10, \dots, -5, -10, \dots\} = [0]_5$$

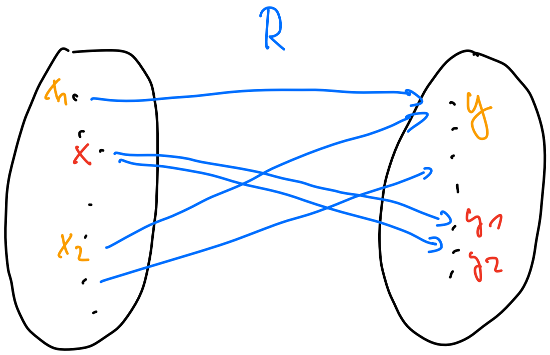
$$1 + 5\mathbb{Z} = \{1, 6, 11, \dots, -4, -9, \dots\} = [1]_5$$

$$\implies a + m\mathbb{Z} = [a]_m$$

Zum Beweis:

$$b - a \in m\mathbb{Z} \iff b - a = mk \iff m \mid b - a \iff b \equiv_m a$$
$$\iff b = a + mk$$

F. 115



$(x_1, y) \in R \wedge (x_2, y) \in R$,

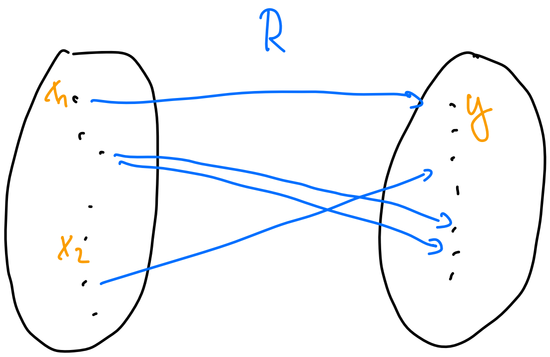
aber $x_1 \neq x_2$

$\Rightarrow$ R nicht l.e.

$(x, y_1) \in R \wedge (x, y_2) \in R$,

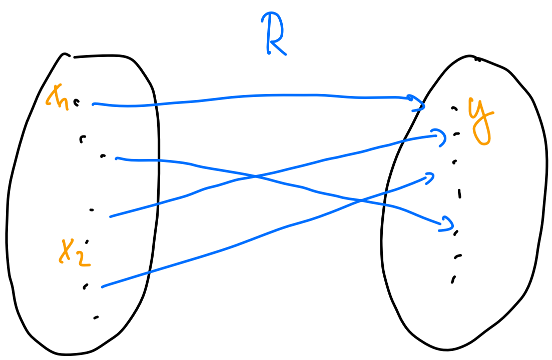
aber $y_1 \neq y_2$

$\Rightarrow$ R nicht r.e



l.e.

nicht r.e.



l.e.

r.e.

F.11P Bew. Satz 1

$R^{-1} \subseteq N \times M$

R l.e

$\Longleftrightarrow$

$\forall x_1, x_2 \in M \ \forall y \in N: \quad (x_1, y) \in R \wedge (x_2, y) \in R \Rightarrow x_1 = x_2$

$\Longleftrightarrow$

$\forall x_1, x_2 \in M \ \forall y \in N: \quad (y, x_1) \in R^{-1} \wedge (y, x_2) \in R^{-1} \Rightarrow x_1 = x_2$

$\Longleftrightarrow$

R^{-1} r.e. //