# Vorlesung 13



F.203 Bew. Satz

Seien $a,b \in \mathbb{Z}$ nicht beide gleich 0.

Setze $M := a\mathbb{Z} + b\mathbb{Z} = \{a \cdot k + b \cdot l \mid k, l \in \mathbb{Z}\}$.

Die Menge $M \cap \mathbb{N} \subseteq \mathbb{N}$ ist nicht leer, denn:

Falls $a \neq 0$ ist, ist $\begin{cases} a = a \cdot 1 + b \cdot 0 \in M \cap \mathbb{N}, & a > 0 \\ -a = a \cdot (-1) + b \cdot 0 \in M \cap \mathbb{N}, & a < 0 \end{cases}$.

Falls $b \neq 0$ ist, ist $|b| \in M \cap \mathbb{N}$.

Nach DM91 besitzt $M \cap \mathbb{N}$ ein kleinstes El. $g \in M \cap \mathbb{N}$. Da insbesondere $g \in M$ ist, ex. $s, t \in \mathbb{Z}$ mit (I) $g = a \cdot s + b \cdot t$.

[z.z.: $g = ggT(a,b)$, d.h.,

① $g \mid a \wedge g \mid b$

② $\forall c \in \mathbb{Z}: c \mid a \wedge c \mid b \Rightarrow c \mid g$ ]

① Nach dem Satz „Teilen mit Rest" ex. $q, r \in \mathbb{Z}$ mit

(II) $a = q \cdot g + r$ und (III) $0 \leq r < g$.

Es gilt:

$$r \underset{(II)}{=} a - q \cdot g \underset{(I)}{=} a - q \cdot (a \cdot s + b \cdot t)$$

$$= a - q \cdot a \cdot s - q \cdot b \cdot t$$

$$= a \cdot \underbrace{(1 - q \cdot s)}_{\in \mathbb{Z}} + b \cdot \underbrace{(-q) \cdot t}_{\in \mathbb{Z}} \in M$$

Ann.: $r > 0$. Dann ist $r \in M \cap \mathbb{N}$.

Nach (III) gilt: $r < g$ Wid.

zu $g$ ist kl. El. von $M \cap \mathbb{N}$.

Also $r = 0$, Damit gilt nach (II): $a = q \cdot g$,

d.h.: $g | a$

Analog folgt: $g | b$.

(2) Sei $c \in \mathbb{Z}$. Es gelte: $c | a$ und $c | b$

[z.z.: $c | g$, d.h.: $\exists\, c' \in \mathbb{Z}: c \cdot c' = g$]

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

(IV) $c \cdot c'' = a$ und (V) $c \cdot c''' = b$.

Es gilt:

$$(\mathrm{VI})\quad g \underset{(\mathrm{I})}{=} a\cdot s+b\cdot t \underset{(\mathrm{IV}),(\mathrm{V})}{=} c\cdot c''\cdot s + c\cdot c'''\cdot t$$

$$= c\cdot (c''\cdot s + c'''\cdot t).$$

Setze $c' := c''\cdot s + c'''\cdot t \in \mathbb{Z}$. Es gilt mit (VI):

$c\cdot c' = c\cdot (c''\cdot s + c'''\cdot t) = g$. //

F.196 Bew Satz

[z.z.: $a,b$ besitzt genau einen ggT]

- Eindeutigkeit wurde auf F.196 bewiesen.
- Existenz ergibt sich aus dem Satz von Bézout. Seien $a,b \in \mathbb{Z}$.

denn ex. nach dem Satz von Bézout

$s,t \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = s\cdot a + t\cdot b$. //

F.204/205 $s_n = t_a$, $t_n = s_a - q_a\cdot t_a$

| a | b | q | s | t |
|---|---|---|---|---|
| 130 | 35 | 3 | 3 | −11 |
| 35 | 25 | 1 | −2 | 3 |
| 25 | 10 | 2 | 1 | −2 |
| 10 | 5 | 2 | 0 | 1 |
| 5 | 0 | | 1 | 0 |

$t = -2 - 3\cdot 3 = -11$

$t = 1 - 1\cdot(-2) = 3$

$t = 0 - 2\cdot 1 = -2$

$t = 1 - 2\cdot 0 = 1$

gesucht

$\boxed{\mathrm{ggT}(130,35) = 3\cdot 130 - 11\cdot 35 = 5}$

$\mathrm{ggT}(35,25) = -2\cdot 35 + 3\cdot 25 = 5$

$\mathrm{ggT}(25,10) = 1\cdot 25 - 2\cdot 10 = 5$

$\mathrm{ggT}(10,5) = 0\cdot 10 + 1\cdot 5 = 5$

$\mathrm{ggT}(5,0) = 1\cdot 5 + 0\cdot 0 = 5$

F. 207 Bew. Satz

Zunächst betrachten wir eine Hilfsbeh. (*):

$[a]_m$ besitzt ein Inverses in $(\mathbb{Z}_m \setminus \{[0]_m\}, \otimes)$

$\Longleftrightarrow \exists t \in \mathbb{Z}: [1]_m = [a]_m \otimes [t]_m = [a \cdot t]_m$

$\Longleftrightarrow \exists t \in \mathbb{Z}: a \cdot t \equiv_m 1$

$\Longleftrightarrow \exists t \in \mathbb{Z}: m \mid 1 - a \cdot t$

$\Longleftrightarrow \exists s, t \in \mathbb{Z}: \underbrace{m \cdot s = 1 - a \cdot t}_{\Longleftrightarrow \; 1 = m \cdot s + a \cdot t}$

[z.z.: $[a]_m$ besitzt ein Inverses in $(\mathbb{Z}_m \setminus \{[0]_m\}, \otimes)$
$\Longleftrightarrow ggT(a,m) = 1$]

„$\Rightarrow$": Es gelte: $[a]_m$ besitzt ein Inverses in $(\mathbb{Z}_m \setminus \{[0]_m\}, \otimes)$. Nach (*) ex. $s, t \in \mathbb{Z}$ mit $m \cdot s + a \cdot t = 1$. Da $ggT(a,m) \mid a$ und $ggT(a,m) \mid m$, folgt mit A 5.1 (2) in moodle: $\quad ggT(a,m) \mid m \cdot s + a t = 1$. (5)

Da $ggT(a,m) \in \mathbb{N}$ ist, ist $ggT(a,m) = 1$.

„$\Leftarrow$": Es gelte: $ggT(a,m) = 1$. Nach dem Satz von Bézout ex. $s,t \in \mathbb{Z}$ mit $s \cdot a + t \cdot m = ggT(a,m) = 1$.

Nach $(*)$ besitzt $[a]_m$ ein Inverses in $(\mathbb{Z}_m \setminus \{[0]_m\}, \otimes)$. //

Bew Satz 2

(G1) Produkt von kanonisch Repräsentanten in $\mathbb{Z}_p$ sind kein Vielfache von $p$, d.h. das Produkt ist $\neq [0]_p$.

(G2) ✓

(G3) $[1]_p$

(G4) Satz 1 von F. 207. //

Bew. Satz 3

Folgt aus A 9.3 (1) in moodle. //

<u>Bsp.:</u> $(\mathbb{Z}_6^\times, \otimes) = \{[1]_6, [5]_6\}$

$(\mathbb{Z}_p^\times, \otimes) = \mathbb{Z}_p \setminus \{[0]_p\}$

F. 208 <u>Bew. Satz</u>

[Ziel: $\exists!\, x \in \mathbb{Z}_m : [a]_m \otimes x = [b]_m$]

Da $ggT(m,a) = 1$ ist, ist $[a]_m \in (\mathbb{Z}_m^\times, \otimes)$.

Da $(\mathbb{Z}_m^\times, \otimes)$ eine Gruppe ist, ex. genau ein inv. El. zu $[a]_m$ in $(\mathbb{Z}_m^\times, \otimes)$, nämlich $[a]_m^{-1}$. Dann ist $[a]_m^{-1}$ auch eindeutig in $(\mathbb{Z}_m, \otimes)$, denn:

Gäbe es ein $[a']_m \in (\mathbb{Z}_m, \otimes)$ mit $[a']_m \neq [a]_m^{-1}$ und $[a']$ ist invers zu $[a]_m$. Dann ist $[a']_m \in (\mathbb{Z}_m^\times, \otimes)$ ↯ zur Eindeutigkeit von $[a]_m^{-1}$. Setze $x := [a]_m^{-1} \otimes [b]_m \in \mathbb{Z}_m$.

Da $\otimes$ eine Abb. ist, ist $x$ eindeutig.

Es gilt:

$$
\begin{aligned}
[a]_m \otimes x &= [a]_m \otimes \left( [a]_m^{-1} \otimes [b]_m \right) \\
&= \left( [a]_m \otimes [a]_m^{-1} \right) \otimes [b]_m \\
&= [1]_m \otimes [b]_m \\
&= [b]_m .
\end{aligned}
$$