3. Vorlesung 1. Teil 25/10/2011

Am Freitag 21/10 haben wir gesehen daß für $n>1$ $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein kommutativer Ring mit Eins. Wir wollen nun zeigen, daß $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper genau dann wenn $n = p$ eine Primzahl ist.

"$\Rightarrow$":

Lemma 1. Jeder Körper ist ein Integritätsbereich, d.h. aus $xy = 0$ folgt $x = 0$ oder $y = 0$ $\forall x, y$.

Beweis Sei $xy = 0$ und $x \neq 0$.

Also $x^{-1}(xy) = x^{-1} 0 = 0$

d.h. $(x^{-1}x)y = 1.y = y = 0$. ∎

Bemerkung: Hier haben wir benutzt:

$\forall z \; (z.0) = 0$. ÜA. ∎

Sei nun $n > 1$, wir zeigen:

Korollar 1. Sei $n > 1$,

$(\mathbb{Z}_n, +_n, \cdot_n)$ Körper $\Rightarrow$

$n = p$ ist eine Primzahl.

Beweis: Annahme: n ist keine Primzahl,

also $n = xy$ mit $1 < x < n$
$1 < y < n$

Also $x, y \in \mathbb{Z}_n$, $x \neq 0$, $y \neq 0$

aber $x \cdot_n y = \overline{xy} = 0$.

Also ist $(\mathbb{Z}_n, +_n, \cdot_n)$ kein Körper. ∎

"$\Leftarrow$" Wir wollen nun zeigen daß

$n = p$ Primzahl $\Rightarrow (\mathbb{Z}_p, +_p, \cdot_p)$

ist ein Körper.

Dafür wollen wir explizit die multiplikative Inversen berechnen; Der Euklidische Algorith

25. 10. 2011

3. Vorlesung · ~~2. Teil~~

Definition 1 (i) (positive) Divisoren:

$a, b \in \mathbb{Z}$; $b > 0$; $a = bq + r$. Falls $r = 0$: b teilt a; $b \mid a$; ← Bezeichnung

b ist ein Divisor ~~von~~ a oder

a ist ein Vielfach von b.

(ii) $p \in \mathbb{N}$ (also $p > 1$) ist eine Primzahl falls die einzigen (positive) Divisoren von p sind 1 und p.

(iii) $\mathbb{N} \ni d$ ist ein gemeinsamer Teiler von a und b falls $d \mid a$ und $d \mid b$. } schreibe: d is $gT(a,b)$

(iv) $\mathbb{N} \ni d$ ist der größte gemeins. Teiler von a und b (Bezeich: $d = ggT(a,b)$) falls d gemeins. Teiler und d ist die größte natürliche

mit dieser Eigenschaft.

Äquivalent:

$\forall\, d'$; $d' \in \mathbb{N}$ und d' gemeins. Teiler von a und b

gilt: $d' \mid d$.

Der Euklidische Algorithmus (Zum berechnen von $ggT(a,b)$).

$a, b \in \mathbb{Z}$; $b > 0$; $b \mid a \Rightarrow ggT(a,b) = b$

(Sonst):

$$a = b\,q_1 + r_1 \qquad 0 < r_1 < b$$

$$b = r_1\,q_2 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = r_2\,q_3 + r_3 \qquad 0 < r_3 < r_2$$

$$\vdots$$

(ρ) Rekursion:

$$r_{j-1} = r_j\,q_{j+1} + r_{j+1} \qquad 0 < r_{j+1} < r_j$$

$$\vdots$$

$$r_{n-3} = r_{n-2}\,q_{n-1} + r_{n-1} \qquad 0 < r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}\,q_n + \boxed{r_n} \qquad 0 < r_n < r_{n-1}$$

↖ letzte $\neq 0$

absteigende Folge von natürlichen Zahlen muss anhalten nach

$$0 < r_n < r_{n-1} < \cdots < r_2 < r_1 < b$$

endlich vielen Schritten.

Behauptung $r_n = ggT(a, b)$.

Die Behauptung folgt aus:

Lemma 1: $a = bq + r \Rightarrow$

$$ggT(a, b) = ggT(b, r)$$

Beweis setze $d := ggT(b, r)$

(1) $d \mid b$ und $d \mid r \Rightarrow d \mid a$

also d ist $gT(a, b)$.

(2) Ferner: $d' \mid a$ und $d' \mid b$

$\Rightarrow d' \mid a - bq$ i.e $d' \mid r$

also $d' \mid d$.

Also: $d = ggT(a, b)$ wie behauptet. ∎

und ferner:

Bemerkung 1 $r_n = ggT(r_{n-1}, r_{n-2})$

weil: $r_n \mid r_{n-1}$ und $r_n \mid r_n$ $\Rightarrow r_n \mid r_{n-2}$

und $d' \mid r_{n-1}$, $d' \mid r_{n-2}$

$\Rightarrow$

$d' \mid (r_{n-2} - r_{n-1} q_n)$

i.e. $d' \mid r_n$. ∎

Also (in (P)): $ggT(a,b) = ggT(b, r_1) = ggT(r_1, r_2) = \dots = ggT(r_{n-1}, r_{n-2}) = r_n$ ∎

Definition 2: eine lineare Kombination von a und b (über $\mathbb{Z}$) ist eine ganze Zahl γ aus der Gestalt

$$\gamma := \alpha a + \beta b \qquad \text{wobei } \alpha, \beta \in \mathbb{Z}.$$

Bemerkung 2 Wir haben ständig die folgende Tatsache benutzt:

$d' \mid a$ und $d' \mid b$ $\Rightarrow$

d' teilt jede lineare Kombination

von a und b.

Beweis: $\gamma = \alpha d'a' + \beta d' b' = d'(\alpha a' + \beta b')$. ∎

Bemerkung 3: Rückwärts EA:

$ggT(a,b) = r_n$ ist eine lineare Kombination (über $\mathbb{Z}$) von a und b:

Rekursion:

$$r_n = r_{n-2} - r_{n-1} q_n$$

aber hier nur r_{n-1}, r_{n-2} werden benötigt

$$r_{n-1} = r_{n-3} - (r_{n-2}) q_{n-1}$$

also

$$r_n = r_{n-2} - \left[r_{n-3} - (r_{n-2}) q_{n-1} \right] q_n$$

hier nur

r_{n-2}, r_{n-3} werden benötigt

Verfahre so weiter. ∎

Für numerische Beispiele und Berechnungen siehe ÜB.

Bemerkung 4: $ggT(a,b) = ggT(b,a)$ $(a, b > 0)$