

3. Script zur Vorlesung: Lineare Algebra I

Prof. Dr. Salma Kuhlmann, Dr. Merlin Carl

WS 2011/2012: 25. Oktober 2011

(WS 2015/2016: Korrekturen vom 5. November 2015)

Am Freitag, 21.10.2011, haben wir gesehen, dass für $n > 1$ $(\mathbb{Z}_n, +_n, \cdot_n)$ ein kommutativer Ring mit Eins ist. Wir wollen nun zeigen, dass $(\mathbb{Z}_n, +_n, \cdot_n)$ ein Körper ist, genau dann, wenn $n = p$ eine Primzahl (Definition siehe unten) 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. $(x^{-1}x)y = 1 \cdot y = y = 0$.
 \square

Bemerkung Hier haben wir benutzt:
 $\forall z(z \cdot 0) = 0$. (Übungsaufgabe).

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. \square

“ \Leftarrow ”:

Wir wollen nun zeigen, dass $n = p$ Primzahl $\Rightarrow (\mathbb{Z}_p, +_p, \cdot_p)$ ist ein Körper.

Dafür wollen wir explizit die multiplikativen Inversen berechnen: Der Euklidische Algorithmus.

Definition 1

- (i) (positive) Divisoren
 $a, b \in \mathbb{Z}; b > 0; a = bq + r$. Falls $r = 0$: b teilt a ; Bezeichnung: $b \mid a$.
 b ist ein *Divisor von a* oder a ist ein *Vielfaches von b* .
- (ii) $p \in \mathbb{N}$ (also $p > 1$) ist eine Primzahl, falls 1 und p die einzigen (positiven) Divisoren von p sind.
- (iii) $\mathbb{N} \ni d$ ist ein *gemeinsamer Teiler* von a und b falls $d \mid a$ und $d \mid b$ (schreibe: d ist $gT(a, b)$).
- (iv) $\mathbb{N} \ni d$ ist der größte gemeinsame Teiler von a und b (Bezeichnung: $d = ggT(a, b)$), falls d gemeinsamer Teiler und d die größte natürliche Zahl mit dieser Eigenschaft ist.

Bemerke: Die Menge der gemeinsamen Teiler zweier Zahlen a und b mit $b \neq 0$ enthält stets die 1, ist also nicht leer und außerdem durch das Maximum von a und b nach oben beschränkt. Also existiert zu je zwei solchen Zahlen der größte gemeinsame Teiler.

Äquivalent:

$\forall d' : d' \in \mathbb{N}$ und d' gemeinsamer 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:

$$\begin{array}{rcl} a = b q_1 + r_1 & 0 < r_1 < b \\ b = r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 & 0 < r_3 < r_2 \\ \vdots & & \end{array}$$

$$\begin{array}{l} \text{Rekursion } (\rho) \\ r_{j-1} = r_j q_{j+1} + r_{j+1} \quad 0 < r_{j+1} < r_j \\ \vdots \\ r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \quad 0 < r_{n-1} < r_{n-2} \\ r_{n-2} = r_{n-1} q_n + r_n \quad 0 < r_n < r_{n-1} \\ n \text{ maximal mit } r_n \neq 0 \end{array}$$

Absteigende Folge von natürlichen Zahlen *muss* anhalten nach $0 < r_n < r_{n-1} < \dots < r_2 < r_1 < b$ 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 in (ρ) :

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

$$\left. \begin{array}{l} r_n \mid r_{n-1} \\ \text{und} \\ r_n \mid r_n \end{array} \right\} \Rightarrow r_n \mid r_{n-2}$$

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 (ρ)): $ggT(a, b) = ggT(b, r_1) = ggT(r_1, r_2) = \dots = ggT(r_{n-1}, r_{n-2}) = r_n$.

Definition 2 Eine lineare Kombination von a und b (über \mathbb{Z}) ist eine ganze Zahl γ der Gestalt:
 $\gamma := \alpha a + \beta b$ 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:
 $r_n = \boxed{r_{n-2}} - \boxed{r_{n-1}} q_n$. Aber hier werden nur r_{n-1}, r_{n-2} benötigt.

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

Also $r_n = r_{n-2} - [r_{n-3} - r_{n-2} q_{n-1}] q_n$.
Hier werden nur r_{n-2}, r_{n-3} benötigt.

Verfahre so weiter.

Für numerische Beispiele und Berechnungen siehe Übungsblatt.

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