3 Script zur Vorlesung: Lineare Algebra I

Prof. Dr. Salma Kuhlmann

In Script 2 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 3.4 siehe unten) ist.

"$\Rightarrow$":

Lemma 3.1.
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 3.2.
Hier haben wir benutzt:
$\forall z(z.0) = 0$. (Übungsaufgabe).

Sei nun $n > 1$. Wir zeigen:

Korollar 3.3.
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 multiplikativen Inversen berechnen:
Der Euklidische Algorithmus.

Definition 3.4. (Erinnerung)

(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) $p \in \mathbb{N}$ $(p > 1)$ 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.

Äquivalent:
$\forall d' : d' \in \mathbb{N}$ und d' gemeinsamer Teiler von a und b gilt: $d' \mid d$.

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.

Der Euklidische Algorithmus (zum Berechnen von $ggT(a,b)$):
$a, b \in \mathbb{Z};\ b > 0;\ b|a \Rightarrow ggT(a,b) = b$
sonst:

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

Rekursion (ρ)

$$\begin{array}{llllll} r_{j-1} & = & r_j\ q_{j+1} & + & r_{j+1} & 0 < r_{j+1} < r_j \\ \vdots & & & & & \\ r_{n-3} & = & r_{n-2}\ q_{n-1} & + & r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} & = & r_{n-1}\ q_n & + & r_n & 0 < r_n < r_{n-1} \\ n \text{ maximal} & & \text{mit} & & r_n \neq 0 & \end{array}$$

Absteigende Folge von natürlichen Zahlen *muss* anhalten nach
$0 < r_n < r_{n-1} < \ldots < r_2 < r_1 < b$ endlich vielen Schritten.

Behauptung 3.5.
$r_n = ggT(a,b)$

Die Behauptung folgt aus:

Lemma 3.6.
$a = bq + r \ \Rightarrow\ ggT(a,b) = ggT(b,r)$

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 3.7.
$r_n = ggT(r_{n-1}, r_{n-2})$ weil

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

und $d' \mid r_{n-1}$, $\quad d' \mid r_{n-2} \;\Rightarrow\; d' \mid (r_{n-2} - r_{n-1}q_n)$, i.e. $d' \mid r_n$

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

Definition 3.8.
Eine (ganze) 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 3.9.

(1) Wir haben ständig die folgende Tatsache benutzt:
$d' \mid a$ und $d' \mid b \;\Rightarrow\; d'$ teilt jede lineare Kombination von a und b, weil
$\gamma = \alpha d'a' + \beta d'b' = d'(\alpha a' + \beta b')$

(2) **Rückwärts EA:**
$ggT(a,b) = r_n$ ist eine lineare Kombination (über $\mathbb{Z}$) von a und b:
Rekursion (ρ):
$r_n = \boxed{r_{n-2}} - \boxed{r_{n-1}}\, q_n$. Aber hier werden nur r_{n-1}, r_{n-2} benötigt.

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

Also $\quad r_n = r_{n-2} - [r_{n-3} - r_{n-2}\; q_{n-1}]q_n$.

Hier werden nur r_{n-2}, r_{n-3} benötigt.
Verfahre so weiter.
Für numerische Beispiele und Berechnungen siehe Übungsblatt.

(3) $ggT(a,b) = ggT(b,a)$ $(a,b > 0)$.