4. Script zur Vorlesung: Lineare Algebra I

Prof. Dr. Salma Kuhlmann, Dr. Merlin Carl

WS 2011/2012: 28. Oktober 2011

(WS 2015/2016: Korrekturen vom 3. November 2015)

Korollar 2 $n = p$ ist eine Primzahl $\Rightarrow$ $(\mathbb{Z}_p, +_p, \cdot_p)$ ist ein Körper.

Bezeichnung $\mathbb{F}_p$

Beweis $(\mathbb{Z}_p, +_p, \cdot_p)$ ist ein kommutativer Ring mit Eins. Sei nun $x \in \mathbb{Z}_p,\ x \neq 0$.
Wir wollen zeigen: $\exists y \in \mathbb{Z}_p$ mit $\overline{xy} = x \cdot_p y = 1$.
Nun $x \in \{1, \ldots, p-1\}$ und p prim $\Rightarrow ggT(x,p) = 1$. Also $\exists \alpha, \beta \in \mathbb{Z}$ mit $\alpha \neq 0$.
$\alpha x + \beta p = 1. \qquad (*)$

Also $\alpha x = (-\beta)p + 1$. A priori $\alpha \in \mathbb{Z}$, nehme $\overline{\alpha} \in \{1, \ldots, p-1\}$.
(Bemerke, dass $\overline{\alpha} \neq 0$, sonst $p \,|\alpha$. Aber dann im $(*)$ $p \mid 1$; Unsinn).

Also $\alpha = qp + \overline{\alpha} \qquad (**)$
$(**)$ in $(*)$ ergibt: $(qp + \overline{\alpha})x + \beta p = 1$.

Also $\overline{\alpha}x + qxp + \beta p = 1$.

Also $\overline{\alpha}x + (qx + \beta)p = 1 \quad \Rightarrow \overline{\alpha}x = -(qx + \beta)_y p + 1 \qquad (***)$
mit $\overline{\alpha} \in \mathbb{Z}_p$.

Setze $\overline{\alpha} := y$.
Berechne $x \cdot_p y = \overline{xy} = 1$ aus $(***)$ und Eindeutigkeit von Rest in DA. $\square$

ÜA für ÜB: Zeige folgende
Proposition Sei p eine Primzahl, $a, b \in \mathbb{N}$. Wenn $p \mid ab$, dann $p \mid a$ oder $p \mid b$.

Frage Gibt es andere endliche Körper?

Definition (Charakteristik)
Sei K ein Körper, definiere

$$\text{Char}\,(K) := \begin{cases} \text{die kleinste natürliche Zahl } (n \geq 2) \text{ wofür} \\ \underbrace{1 + 1 + \ldots + 1 = 0}_{n\text{-mal}} \qquad \text{falls existiert} \\ 0 \text{ sonst} \end{cases}$$

(Bezeichnung: $\underbrace{1 + \ldots + 1}_{n}$-mal $:= n.1$.)

I.e Char $(K) = 0$ falls $\underbrace{1 + 1 + \ldots + 1}_{n\text{-mal}} \neq 0$ für alle $n \in \mathbb{N}$.

Lemma 1 Char $(K) \neq 0 \ \Rightarrow$ Char $(K) = p$ eine Primzahl.

Beweis Sei $n \neq 0 \quad n = \text{Char}\ (K)$.
n nicht prim $\Rightarrow n = n_1 n_2$ mit $1 < n_i < n$ für $i = 1, 2$.

$$\text{Also } 0 = \underbrace{1 + 1 + \ldots + 1}_{n_1 n_2 \text{mal}} = \underbrace{(1 + \ldots + 1)}_{n_1\text{-mal}} \underbrace{(1 + \ldots + 1)}_{n_2\text{-mal}} = 0.$$

$$\text{Also } \underbrace{1 + \ldots + 1}_{n_1\text{-mal}} = 0 \text{ oder } \underbrace{1 + \ldots + 1}_{n_2\text{-mal}} = 0 \text{ - Widerspruch.} \qquad \square$$

Beispiele 2 Char $(\mathbb{F}_p) = p$
Char $(\mathbb{Q})$ = Char $(\mathbb{R}) = 0$
[weil $1 > 0$
also $1 + 1 > 0 + 1 = 1 > 0$
$\vdots$

$$\underbrace{1 + 1 + \ldots + 1}_{n+1\text{mal}} = \underbrace{(1 + \ldots + 1)}_{n\text{mal}} + 1 > \underbrace{(1 + \ldots + 1)}_{n\text{mal}} > 0]$$

Bemerkung und Definition $k \subset K$ ist ein *Teilkörper*, falls $0, 1 \in k$,
k abgeschlossen unter $x + y, xy, -x, x^{-1}$ für $x \neq 0$.
Bemerke: Char (k) = Char (K).

Lemma 3

$$K \text{ endlich} \Rightarrow \begin{cases} (1) & \text{Char}\ (K) = p > 0 \quad \text{und} \\ (2) & \mid K \mid = p^l \qquad\qquad l \in \mathbb{N} \end{cases}$$

Beweis

(1) Wir zeigen die Kontraposition: Char $(K) = 0 \ \Rightarrow \ K$ unendlich.
Wir behaupten: $n_1, n_2 \in \mathbb{N},\ n_1 \neq n_2 \ \Rightarrow$

$$\underbrace{1 + \ldots + 1}_{n_1} \neq \underbrace{1 + \ldots + 1}_{n_2}.$$

Ohne Einschränkung (OE) $n_1 > n_2; (n_1 - n_2) > 0$

$$\underbrace{(1 + \ldots + 1)}_{n_1} - \underbrace{(1 + \ldots + 1)}_{n_2} = \underbrace{(1 + \ldots + 1)}_{n_1 - n_2} = 0 \text{ - Widerspruch.}$$

(2) Dafür brauchen wir lineare Algebra! Also später! (Basis und Dimension)

Beispiel 4 $K = \mathbb{F}_p(t)$ ist der Körper der rationalen Funktionen über dem endlichen Körper $\mathbb{F}_p$.
K unendlich; aber Char $(K) = p > 0$. Dafür brauchen wir Polynomringe. Später!

Bemerkung Also K unendlich $\not\Rightarrow$ Char $(K) = 0$.

Kapitel 1: § 2 Lineare Gleichungssysteme

Definition 1

(i) Sei $n \in \mathbb{N}$, und K ein Körper. Eine *lineare Gleichung über* K in den Variablen $x_1, \ldots, x_n$ und Koeffizienten in K ist eine Gleichung der Form:
$a_1x_1 + \ldots, +a_nx_n = b \qquad (*)$
wobei $a_1, \ldots, a_n, b \in K$.

Terminologie a_i ist der Koeffizient der Variablen x_i.

(ii) Ein n-Tupel $c := (c_1, \ldots, c_n) \in K^n$ ist *eine Lösung* der Gleichung $(*)$, falls die Identität
$a_1c_1 + \ldots + a_nc_n = b$ gilt in K.

Beispiele

a) $\sqrt{2}x_1, +\pi x_2 = e$ ist eine l. G. über $\mathbb{R}$.

b) $2\sqrt{x_1} + \pi x_2^2 = e$ ist keine l.G. über $\mathbb{R}$.

c) Linie: $y = ax + b$ ist die Gleichung ($a, b \in \mathbb{R}, a :=$ Steigung; $b := y$ - intersect) einer Geraden (in der Ebene $\mathbb{R}^2$) : l.

Umschreiben: $x_2 - ax_1 = b$.
Lösung: $\underline{P}$: Punkt in $\mathbb{R}^2$; $\underline{P} = \underline{P}(c_1, c_2)$ mit Koordinaten c_1 und c_2 ist eine Lösung gdw $\underline{P} \in l$, d.h. $\underline{P}$ liegt auf l.