

4 Script zur Vorlesung: Lineare Algebra I

Prof. Dr. Salma Kuhlmann

Korollar 4.1.

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

Bezeichnung 4.2.

$\mathbb{F}_p, |\mathbb{F}_p| = p$

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 $x \in \{1, \dots, p-1\}$ und p prim $\Rightarrow \text{ggT}(x, p) = 1$. Also $\exists \alpha, \beta \in \mathbb{Z}$ mit $\alpha \neq 0$ und $\alpha x + \beta p = 1$. (*)

Also $\alpha x = (-\beta)p + 1$. A priori $\alpha \in \mathbb{Z}$, nehme $\bar{\alpha} \in \{1, \dots, p-1\}$.

(Bemerke, dass $\bar{\alpha} \neq 0$, sonst $p \mid \alpha$. Aber dann im (*) $p \mid 1$; Unsinn).

Also $\alpha = qp + \bar{\alpha}$ (**)

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

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

Also $\bar{\alpha}x + (qx + \beta)p = 1 \Rightarrow \bar{\alpha}x = -(qx + \beta)p + 1$ (***)

mit $\bar{\alpha} \in \mathbb{Z}_p$.

Setze $\bar{\alpha} := y$.

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

ÜA für ÜB: Zeige folgende:

Proposition 4.3.

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 4.4. (Charakteristik)

Sei K ein Körper, definiere

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

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

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

Lemma 4.5.

$\text{Char}(K) \neq 0 \Rightarrow \text{Char}(K) = p$ eine Primzahl.

Beweis

Setze $n = \text{Char}(K)$.

n nicht prim $\Rightarrow n = n_1 n_2$ mit $1 < n_i < n$ für $i = 1, 2$.

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

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

Beispiel 4.6.

$$\text{Char}(\mathbb{F}_p) = p$$

$$\text{Char}(\mathbb{Q}) = \text{Char}(\mathbb{R}) = 0$$

[weil $1 > 0$

$$\text{also } 1 + 1 > 0 + 1 = 1 > 0$$

\vdots

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

Definition 4.7. und Bemerkung

$k \subseteq K$ ist ein *Teilkörper*, falls $0, 1 \in k$,

k abgeschlossen unter $x + y, xy, -x, x^{-1}$ für $x \neq 0$.

Bemerke: $\text{Char}(k) = \text{Char}(K)$.

Lemma 4.8.

$$K \text{ endlich} \Rightarrow \begin{cases} (1) & \text{Char}(K) = p \neq 0, \quad p \text{ Primzahl} & \text{und} \\ (2) & |K| = p^l & \text{für geeignete } l \in \mathbb{N} \end{cases}$$

Beweis

(1) Wir zeigen die Kontraposition: $\text{Char}(K) = 0 \Rightarrow K$ unendlich.

Wir behaupten: $n_1, n_2 \in \mathbb{N}, n_1 \neq n_2 \Rightarrow$

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

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

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

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

Beispiel 4.9.

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

Bemerkung 4.10.

Also K unendlich $\not\Rightarrow \text{Char}(K) = 0$.

Kapitel 1: § 2 Lineare Gleichungssysteme

Definition 4.11.

- (i) Sei $n \in \mathbb{N}$, und K ein Körper. Eine *lineare Gleichung über K* in den Variablen x_1, \dots, x_n und Koeffizienten in K ist eine Gleichung der Form:

$$a_1x_1 + \dots + a_nx_n = b \quad (*)$$

wobei $a_1, \dots, a_n, b \in K$.

Terminologie

a_i ist der Koeffizient der Variablen x_i .

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

Beispiel 4.12.

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 .

