Korollar 2: $n = p$ 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 $x \in \{1, \dots, p-1\}$ 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 $\overline{\alpha} \in \{1, \dots, p-1\}$

(bemerke daß $\overline{\alpha} \neq 0$ sonst $p \mid \alpha$ aber dann in $(*)$ $p \mid 1$, Unsinn) also

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

(**) in (*) ergibt:

$$(qp + \bar{\alpha})\, x + \beta p = 1$$

also

$$\bar{\alpha} x + q x p + \beta p = 1$$

also

$$\bar{\alpha} x + (q x + \beta) p = 1$$

$$\Rightarrow \quad \bar{\alpha} x = -(q x + \beta)\, p + 1 \qquad (***)$$

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 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?

— 28.10.2011

Definition (Charakteristik)

Sei K ein Körper

definiere

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

Bezeichnung:

$$\underbrace{1+\dots+1}_{n \text{ mal}} := n.1$$

i.e. $\mathrm{Char}(K) = 0$ falls

$$\underbrace{1+1+\dots+1}_{n \text{ mal}} \neq 0 \quad \text{für alle } n \in \mathbb{N}$$

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

Beweis: Sei $n \neq 0$ $n = \mathrm{Char}(K)$

n nicht prim $\Rightarrow n = n_1 n_2$ mit

$1 < n_i < n$ für $i = 1, 2$

Also

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

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

∎

__Beispiele 2__ $\mathrm{Char}(\mathbb{F}_p) = p$

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

[weil $1 > 0$

also $1+1 > 0+1 = 1 > 0$

⋮

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

__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:__ $\mathrm{Char}(k) = \mathrm{Char}(K)$.

∎

Lemma 3:

K endlich $\Rightarrow$

$$\begin{cases} ① \ \mathrm{Char}(K) = p > 0 \quad \text{und} \\ ② \ |K| = p^{l} \quad l \in \mathbb{N}. \end{cases}$$

Beweis: ① wir zeigen die Kontraposition:

$\mathrm{Char}(K) = 0 \Rightarrow K$ unendlich

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

$$\underbrace{1 + \cdots + 1}_{n_1 \text{ mal}} \neq \underbrace{1 + \cdots + 1}_{n_2}$$

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

$$\underbrace{(1 + \cdots + 1)}_{n_1} - \underbrace{(1 + \cdots + 1)}_{n_2} = \underbrace{(1 + \cdots + 1)}_{n_1 - n_2} = 0 \ \lightning.$$

Die Umkehrung gilt i.a. nicht!

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

Example 4: $K = \mathbb{F}_p(t)$ the field of rational functions over the finite field $\mathbb{F}_p$.

K unendlich; aber $\mathrm{char}(K) = p > 0$!

• Dafür brauchen wir Polynomringe. Später!

Kapitel I: §1 Körper. Beendet!

Kapitel I: §2 Lineare Gleichungssysteme.

Definition 1: (i) Sei $n \in \mathbb{N}$, ~~und~~ K ein Körper. Eine lineare Gleichung über K in den Variablen $x_1, \dots, x_n$ und Koeffizienten in K ist eine Gleichung der Form:

$$a_1 x_1 + \dots + a_n x_n = b \qquad (*)$$

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

Terminologie: a_i ist der Koeffizient der Variab. x_i.

(ii) Ein n-Tuple $c := (c_1, \dots, c_n) \in K^n$ ist eine Lösung der Gleichung $(*)$ falls die Identität:

$$a_1 c_1 + \dots + a_n c_n = b$$

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 Gerade (in der Ebene $\mathbb{R}^2$): l.

Umschreiben: $x_2 - a x_1 = b$.

Lösung: P : Punkt in $\mathbb{R}^2$ $\quad P = P(c_1, c_2)$
mit Koordinaten c_1 und c_2
ist eine Lösung gdw $P \in l$
d.h P liegt auf l.