Wichtige Sätze und Definitionen zu
§6: Endliche Körper
aus der Vorlesung:

LV-NR	150 239
Veranstaltung	Diskrete Mathematik II, 4.0 std
Dozent	Holtkamp, R.

6.1
K sei Körper, $1_K \neq 0_K$. Sei $\mathrm{ord}_+(1_K) \in \mathbb{N} \cup \{\infty\}$ die Ordnung von 1_K in der additiven Gruppe $(K,+)$. Dann nennt man

$$\mathrm{char}(K) := \begin{cases} 0 & : \mathrm{ord}_+(1_K) = \infty \\ \mathrm{ord}_+(1_K) & : \textit{sonst} \end{cases}$$

die **Charakteristik** *von K.*

Beispiele
$\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = 0$, $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

Satz 1 (Charakteristik)
Ist $n = \mathrm{char}(K) \neq 0$, so ist n Primzahl in $\mathbb{N}$.

6.2

*a) Eine bijektive Abbildung $\varphi: K \to K'$ von Körpern heißt (Körper-)***Isomorphismus** *genau dann, wenn $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ $\forall\, a, b \in K$*

b) $K \cong K' \iff \exists$ Isomorphismus $\varphi: K \to K'$

c) $F \subseteq K$ heißt **Teilkörper** *von $K \iff \forall\, a, b \in F$ ist $a+b$, $a-b$, $a \cdot b$ und a^{-1} auch in F*

Satz 2 (Primkörper)
K sei Körper.

(i) Wenn $\mathrm{char}(K) = 0$, so gibt es einen zu $\mathbb{Q}$ isomorphen Teilkörper von K und K ist ein $\mathbb{Q}$-Vektorraum.

(ii) Wenn $\mathrm{char}(K) = p$, p Primzahl, so gibt es einen zu $\mathbb{Z}/p\mathbb{Z}$ isomorphen Teilkörper P von K und K ist ein $(\mathbb{Z}/p\mathbb{Z})$-Vektorraum. P heißt auch **Primkörper** von K.

(iii) Ist K endlicher Körper, so ist $\mathrm{char}(K) = p$ prim und $\exists\, n$ mit $\#K = p^n$ (genauer $n = \dim_{\mathbb{Z}/p\mathbb{Z}} K$).

Beispiel
Gibt es Körper mit $4, 6, 8, 9, 10, 12, 14$ oder 15 Elementen? Nein für $6, 10, 12, 14$ und 15!

Übung 1
Es sei V ein K-VR, $E = \{v_1, \ldots, v_r\} \subseteq V$ und $U = \{\sum_{r=1}^{r} \lambda_i v_i\}$. Ist E K-linear unabhängig, so ist E K-VR Basis von U mit $\dim U = r$ (Spezialfall $\dim V = r$: E ist Basis von V).
Ist E K-linear unabhängig und $r < \dim(V) =: n < \infty$, so existiert K-Basis B von V mit $E \subseteq B$.
Für jedes endliche Erzeugendensystem E von V kann man eine Teilmenge $B \subseteq E$ finden, die Basis ist (Auswahlsatz).

Beispiele

a) *$K = \mathbb{Z}/2\mathbb{Z}$, $V = K^3 = (\mathbb{Z}/2\mathbb{Z})^3$, $E = \{v_1, v_2\}$ mit $v_= (1,1,1)$, $v_2 = (1,0,1)$. E ist K-linear unabhängig.*
$U = \{0, v_1, v_2, v_1 + v_2 = (0,1,0)\}$ ist K-UVR von V mit $\dim U = 2$.
Sei $v_3 \in V$, $v_3 \notin U$ etwa $v_3 = (1,1,0)$ $\implies$ $B := \{v_1, v_2, v_3\}$ ist K-Basis von V. Weil B linear unabhängig ist, ist der UVR U' der von B erzeugt wird 3-dimensional, $\#U' = 2^3 = \#V$, also $U' = V$.

b) *$K = \mathbb{Z}/3\mathbb{Z}$, $V = K^3$, $E = \{v_1, v_2\}$, $v_1 = (1,1,1)$, $v_2 = (1,0,1)$, K-linear unabhängig. Ergänze zu Basis von V mit*

$$v_3 \notin Kv_1 + Kv_2 = \{0, v_1, v_2, (0,1,0), (0,-1,0), (-1,-1,-1), (-1,0,-1), (-1,1,-1), (1,-1,1)\}.$$

Übung 2
Es sei $K = \mathbb{Z}/3\mathbb{Z}$. Sei $U := \{f \in K[x] : \operatorname{grad}(f) \leq 4,\ f(1) = f'(1) = 0\}$.
Dann ist $U = \left\{(x-1)^2 \cdot h \mid \operatorname{grad}(h(x)) \leq 2\right\}$.

Satz 3 (Minimalpolynom)
Es sei K endlicher Körper, $\operatorname{char} K = p \neq 0$, $P = \{n \cdot 1_K \mid 0 \leq n < p\}$ der Primkörper von K und es sei $a \in K$. Dann gibt es genau ein normiertes Polynom $g_a \in P[x]$ mit

$$g_a \cdot P[x] = \{f \in P[x] \mid f(a) = 0\}.$$

Weiter gilt: g_a ist irreduzibel in $P[x]$.
Ist U der von $\left\{a^i \mid i \in \mathbb{N}_0\right\}$ erzeugte P-UVR von K, so gilt:
U ist Teilkörper von K, $\dim_P(U) = \operatorname{grad}(g_a)$, $U \cong P[x]/g_a \cdot P[x]$.

6.3
Man nennt g_a das **Minimalpolynom** *von a über P.*

Beispiel
Ist $a \in P \cong \mathbb{Z}/p\mathbb{Z}$, so ist das Minimalpolynom von a über P gegeben durch $g_a(x) = x - a \in P[x]$.

Übung 3
Es sei $P = \mathbb{Z}/2\mathbb{Z}$, $f = x^4 + x + 1 \in K[x]$. Dann ist $K = P[x]/f \cdot P[x]$ Körper, denn $x^4 + x + 1 \in P[x]$ ist irreduzibel.

$$\dim_P(K) = 4 \quad \implies \quad \#K = 2^4 = 16$$

Ist a die Restklasse von x in K, so ist f gerade das Minimalpolynom g_a von a über P. $\left\{1, a, a^2, a^3\right\}$ ist P-VR-Basis von K. Es ist $\operatorname{ord}(a) = 15$, *da $\#(K^*) = 15$ und $a^3 \neq 1 \neq a^5$.*

6.4
Ein Körper E der einen Körper K als Teilkörper enthält, heißt auch **Körpererweiterung** *von K.*

Satz 4 (Zerfällungskörper)
K sei Körper, $f \in K[x]$, f normiert mit $\operatorname{grad}(f) = n \geq 1$ $\implies$ $\exists$ Körpererweiterung E von K mit $f = \prod_{i=1}^{n}(x - \lambda_i)$ und $\lambda_i \in E\ \forall\ i$, d.h. f ist in $E[x]$ ein Produkt von Linearfaktoren.

Beispiel
$K = \mathbb{Z}/2\mathbb{Z}$, $f = x^2 + x + 1 \in K[x]$, $E = K[x]/\left(x^2 + x + 1\right) \cdot K[x]$. Bezeichnet $a \in E$ die Restklasse von x, so ist $f(a) = 0$, $f(a+1) = 0$, $f = (x-a)(x-(a+1))$.

Ist $h(x) = x^4 - x \in K[x]$ *so ist*

$$\begin{aligned} h(x) &= x(x-1)(x-a)(x-(a+1)) \\ &= \left(x^2 - x\right)\left(x^2 + x + 1\right) \end{aligned}$$

h zerfällt also in $E[x]$ *in Linearfaktoren.*

Satz 5 ($\mathbb{F}_{p^n}$)
p sei Primzahl, $n \in \mathbb{N}_{\geq 1}$
$\Longrightarrow$ Es gibt bis auf Isomorphie genau einen Körper K mit p^n Elementen.
Er wird oft mit $\mathbb{F}_{p^n}$ oder $GF(p^n)$ bezeichnet (Galois Field).

Satz 6 (Teilkörper von $\mathbb{F}_{p^n}$)
Sei $n \in \mathbb{N}$, $n \geq 1$.

(i) Ist F Teilkörper von $\mathbb{F}_{p^n}$, so ist $\#F = p^m$ und $m|n$.

(ii) Ist $m \in \mathbb{N}$ gegeben mit $m|n$, so existiert genau ein Teilkörper F von K der p^m Elemente hat ($F \cong \mathbb{F}_{p^m}$).

Beispiel
$\mathbb{F}_{2^6}$ *enthält als (echte) Teilkörper* $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$.
$\mathbb{F}_{2^{10}}$ *enthält als (echte) Teilkörper* $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^5}$.

Bemerkung 6.1
Ist p prim, $n \in \mathbb{N}_{\geq 1}$, $P = \mathbb{Z}/p\mathbb{Z}$, *so existiert ein irreduzibles Polynom f in* $P[x]$ *vom Grad n.*
Sind f, $\tilde{f}$ *irreduzible Polynome in* $P[x]$ *von Grad n, so folgt, dass* $K = P[x]/fP[x]$ *isomorph zu* $\tilde{K} = P[x]/\tilde{f} \cdot P[x]$,
d.h. es existiert $a \in \tilde{K}$ *mit der Eigenschaft: das Minimalpolynom von a über P ist f.*

- $\mathbb{F}_4 = \mathbb{F}_2[x] / \left(x^2 + x + 1\right)\mathbb{F}_2[x]$, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{F}_8 = \mathbb{F}_2[x] / \left(x^3 + x + 1\right)\mathbb{F}_2[x]$
- $\mathbb{F}_{16} = \mathbb{F}_2[x] / \left(x^4 + x + 1\right)\mathbb{F}_2[x]$

Übung 4
$K = \mathbb{Z}/5\mathbb{Z}$, $f = x^2 - 2$, *f ist irreduzibel. Sei a die Restklasse von x in* $A = K[x]/f \cdot K[x]$. *Da* $a^2 = 2$, *ist f das Minimalpolynom* $g_a(x)$ *von a über K.*
Sei $c = 2a - 1$. *Was ist* $g_c(x)$*?*
Man berechnet die (ersten) Potenzen von c:

$$c^0 = 1,\ c^1 = c = 2a - 1,\ c^2 = a - 1$$

Die Potenzen c^0, c^1, c^2 *sind linear abhängig* ($c^2 + \lambda_1 c^1 + \lambda_0 c^0 = 0$)*:*

$$(a-1) + 2 \cdot (2a-1) - 2 = 0$$

d.h. $g_c(c) = 0$ *mit* $g_c(x) = x^2 + 2x - 2$. *Es ist* g_c *das Minimalpolynom von c, da es kein Polynom von Grad* 1 *gibt, das c als Nullstelle hat.*

Satz 7 (Satz vom primitiven Element)
K sei endlicher Körper, $\#K = p^n$. $\implies$ die Einheitengruppe K^* von K ist eine zyklische Gruppe, d.h. $\exists\ a \in K^*$ mit $\operatorname{ord}(a) = p^n - 1$, $K^* = \left\{a^i \mid 0 \leq i < p^n\right\}$.