$\mathbb{K}[x] = \{$Polynome mit Koeff. in $\mathbb{K}$, mit Variable $x\}$

Teilung, ggT, eukl. Algorithmus, Primfaktorzerlegung
Lemma von Bézout — $\mathbb{Z}$ und $\mathbb{K}[x]$
Primzahl — irreduzibles Polynom

- $\deg f = 1 \Rightarrow f$ irreduzibel
- $\deg f \geq 2$, f hat eine Nullstelle $\Rightarrow f$ reduzibel
- (char $\mathbb{K}=0$ oder $\mathbb{K}=\mathbb{F}_p$) $\Rightarrow$ (f quadratfrei $\Leftrightarrow$ ggT$(f,f')=1$)
- f irreduzible $\Rightarrow f$ quadratfrei
- $2 \leq \deg f \leq 3 \Rightarrow$ (f hat eine Nullstelle $\Leftrightarrow f$ reduzibel)

$m \in \mathbb{Z}$, $m \geq 1$

$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$

$f = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$

monisches Polynom in $\mathbb{K}[x]$

$\mathbb{K}[x] \longrightarrow \mathbb{K}[x]/(f)$

Beispiel $f = x^3 - x + 1 \in \mathbb{Q}[x]$

$1, x, x^2$ Monome mit Grade $< \deg(f) = 3$

$\mathbb{Q}[x]/(f)$ = der $\mathbb{Q}$-Vektorraum mit Basis $\{1, x, x^2\}$

Er hat eine Summe und eine Skalarmultiplikation.

$$x \cdot x^2 = x^3 = \underbrace{1}\cdot f + \underbrace{x - 1} = x - 1$$

$$x^2 \cdot (x^2 + 1) = x^4 + x^2 = x \cdot f + \underbrace{2x^2 - x} = 2x^2 - x$$

x: Quotient, $2x^2 - x$: Rest

$\mathbb{Z}/3\mathbb{Z}$:

$2 \cdot 2 = 4 = 1$

$f = x^3 - x + 1 \in \mathbb{Q}[x]$

$x^3 = x - 1$ in $\mathbb{Q}[x]/(f)$ "fundamentale Gleichung"

In $\mathbb{Q}[x]/(f)$ gilt $x^4 + x^2 = x \cdot x^3 + x^2 = x(x-1) + x^2$

$= x^2 - x + x^2 = 2x^2 - x$

In $\mathbb{Q}[x]/(f)$ gilt: $x^6 = (x^3)^2 = (x-1)^2 = x^2 - 2x + 1$

$\mathbb{K}$ Körper, $f = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_d$, $d \geq 1$

$\mathbb{K}[x]/(f)$ $\mathbb{K}$-Vektorraum mit Basis $\{1, x, \ldots, x^{d-1}\}$

$a \cdot_{\mathbb{K}[x]/(f)} b = a \cdot_{\mathbb{K}[x]} b$ der Rest der Teilung von b durch f

"Fundamentale Gleichung": $x^d = -a_{d-1}x^{d-1} - \cdots - a_1 x - a_d$

$\mathbb{K}[x] \longrightarrow \mathbb{K}[x]/(f)$ surjektiver Ringhomomorphismus

Satz $m \in \mathbb{Z}$, $m \geq 1$.

$\mathbb{Z}/m\mathbb{Z}$ Körper $\Leftrightarrow$ m prim.

Satz $f \in \mathbb{K}[x]$ monisches Polynom

$\mathbb{K}[x]/(f)$ Körper $\Leftrightarrow$ f irreduzibel

Beispiel $f = x^4 + 6x + 1 \in \mathbb{F}_7[x]$

$A = \mathbb{F}_7[x]/(f)$

Die monomielle Basis von A ist $\{1, x, x^2, x^3\}$

Wie drückt man x^7 als Linearkombination der Elementen der monomiellen Basis aus?

- 1te Möglichkeit: teilen x^7 durch f und nehmen den Rest
- 2te Möglichkeit: benutzen die fundamentale Gleichung:

$$x^4 = -(6x+1) = x - 1$$

$$x^7 = x^4 \cdot x^3 = (x-1)x^3 = x^4 - x^3 = (x-1) - x^3 = -1 + x - x^3$$

Lesen Beispiele 3.35, 3.36, 3.37

Machen Aufgabe 3.4.1