Mi 10.3.2021 VORMITTAG

$\mathbb{K}$ Körper, z.B. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

Ein POLYNOM mit Koeffizienten in $\mathbb{K}$ und in der Variable x ist $f = a_0 + a_1 x + a_2 x^2 + \dots + a_d x^d$ $\quad a_0, a_1, \dots, a_d \in \mathbb{K}$

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

$\mathbb{K}[x]$ ist ein Ring

Beispiel $\mathbb{Q}[x]$ $\quad (1+x)(1-x) = 1 - x^2$

Beispiel $\mathbb{F}_3[x]$ $\quad (x^2 + x + 2)(x+2) =$

$$x^3 + \underline{2x^2} + \underline{x^2} + \underline{\underline{2x}} + \underline{\underline{2x}} + 4$$

$$= x^3 + x + 1$$

Wenn $f = a_d x^d + \dots + a_1 x + a_0$ mit $a_d \neq 0$

$d =: \deg(f)$ GRAD

$a_d =:$ LEITKOEFFIZIENT

$a_d x^d =:$ LEITTERM

$\deg(0) = -\infty$

Eigenschaften vom Grade:

- $\deg(f+g) \leq \max\{\deg f, \deg g\}$
- $\deg f \neq \deg g \Rightarrow \deg(f+g) = \max\{\deg f, \deg g\}$
- $\deg(f \cdot g) = \deg(f) + \deg(g)$
- $\deg f = -\infty \iff f = 0$
- $\deg f = 0 \iff f \in \mathbb{K} - \{0\}$
- $\deg f > 0 \iff f$ nicht konstant

f heißt MONISCH wenn sein Leitkoeffizient gleich 1 ist.

Singular

```
ring r = 0, x, dp;          // es führt Q[x] ein
poly f = 3*x^7 + 9;         // Deklaration einer Variable
                            // Ihr Typ = poly, Element von Q[x]
```

$3x^7 + 9$

```
lead(f);                    // Leitterm
deg(f);                     // Grad
coeffs(f,x)[i+1,1];         // Der Koeffizient von x^i in f
```

$\mathbb{F}_p[x]$

```
ring r = p, x, dp;
```

$\mathbb{K}[x]$ und $\mathbb{Z}$ sind sehr ähnlich

Satz $\mathbb{K}$ Körper, $f, g \in \mathbb{K}[x]$, $g \neq 0$
$\Rightarrow \exists!\ q, r \in \mathbb{K}[x]$ mit $f = qg + r$ und $\deg r < \deg g$

Beispiel $\mathbb{Q}[x]$ $f = x^5 - 2x^3 + 3x + 7$, $g = x^2 - 1$

Teilen f durch g:

$$\begin{array}{rl|l}
x^5 + 0x^4 - 2x^3 + 0x^2 + 3x + 7 & & x^2 - 1 \\
\hline
-x^5 \quad\quad + x^3 & & x^3 - x \\
\hline
// \quad // \quad -x^3 + 0x^2 + 3x + 7 & & \\
\quad + x^3 \quad\quad - x & & \\
\hline
// \quad // \quad 2x + 7 & &
\end{array}$$

In $\mathbb{K}[x]$: f teilt g

$$f \mid g \iff \exists\, h \in \mathbb{K}[x] : g = fh.$$

Def $f \in \mathbb{K}[x]$ heißt IRREDUZIBEL wenn:

- f ist nicht konstant
- $f = gh$ mit $g, h \in \mathbb{K}[x] \Rightarrow \deg g = 0$ oder $\deg h = 0$

Beispiel

- $f \in \mathbb{K}[x]$ $\deg f = 1 \Rightarrow f$ irreduzibel
- $x^2 - 1 = (x+1)(x-1)$ ist reduzibel
- $x^2 - 2$ ist irreduzibel in $\mathbb{Q}[x]$, aber reduzibel in $\mathbb{R}[x]$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Primfaktorzerlegung:

Satz $\mathbb{K}$ Körper, $f \in \mathbb{K}[x]$, $f \neq 0$.

$\Rightarrow \exists!$ $f_1, \dots, f_r$ monische, irreduzible Polynome (paarweise verschiedene)

$\alpha_1, \dots, \alpha_r \in \mathbb{N}^+$

$c \in \mathbb{K} \setminus \{0\}$

sodass $f = c f_1^{\alpha_1} \cdots f_r^{\alpha_r}$

Goal of this week: explain an algorithm to find the Primfaktorzerlegung of polynomials in $\mathbb{F}_p[x]$.

Def Der ggT von $a, b \in \mathbb{K}[x]$ ist das eintige $f \in \mathbb{K}[x]$:

- f ist monisch oder $f = 0$
- $f \mid a$, $f \mid b$
- $g \mid a$, $g \mid b \Rightarrow \underbrace{g \mid f}_{\deg g \leq \deg f}$

$\gcd(a, b)$

Euklidische Algorithmus

Nullstellen

$\mathbb{K}$ Körper, $f = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{K}$

$\alpha \in \mathbb{K}$

$f(\alpha) = a_d \alpha^d + \cdots + a_1 \alpha + a_0$ oder Wert von f an α

Def α ist eine NULLSTELLE von f wenn $f(\alpha) = 0$.

Beispiel $f = x^2 + x + 3 \in \mathbb{F}_5[x]$

$f(0) = 0^2 + 0 + 3 = 3$

$f(1) = 1^2 + 1 + 3 = 5 = 0 \Rightarrow 1$ ist eine Nullstelle von f

$f(2) = \ldots$

$f(3) = 3^2 + 3 + 3 = 15 = 0 \Rightarrow 3$ ist eine Nullstelle von f.

$f = (x-1)(x-3) = x^2 - 4x + 3$

Satz $\mathbb{K}$ Körper, $f \in \mathbb{K}[x]$, $\alpha \in \mathbb{K}$.

$f(\alpha) = 0 \iff x - \alpha \mid f$

Bei dieser Gelegenheit, wenn $\deg f \geq 2$, dann f ist reduzibel

f hat eine Nullstelle in $\mathbb{K}$, $\deg f \geq 2$ $\Rightarrow$ f reduzibel

---

Beispiel $(X^2+1)^2 \in \mathbb{R}[x]$ hat keine Nullstelle in $\mathbb{R}$, aber ist reduzibel in $\mathbb{R}[x]$

Satz $\mathbb{K}$ Körper, $f \in \mathbb{K}[x]$, $\deg f = 2$ oder $\deg f = 3$.

f hat keine Nullstelle in $\mathbb{K}$ $\iff$ f ist irreduzibel in $\mathbb{K}[x]$

Def $f \in K[x]$ heißt QUADRATFREI wenn jeder Primfaktor von f hat Vielfachheit gleich 1 :

$g \in K[x]$ irreduzibel, $g \mid f \implies g^2 \nmid f$

Beispiel . irreduzibel $\implies$ quadratfrei

- $x^2-1 \in \mathbb{Q}[x]$ ist quadratfrei $\quad x^2-1 = (x+1)(x-1)$
- $x^2-1 \in \mathbb{F}_2[x]$ ist nicht quadratfrei $\quad x^2-1 = (x+1)^2$

Def $\mathbb{K}$ Körper, $f = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$

Die ABLEITUNG von f

$$f' = d a_d x^{d-1} + (d-1) a_{d-1} x^{d-2} + \cdots + a_1$$

Beispiel • $f = x^3 + x^2 \in \mathbb{Q}[x] \Rightarrow f' = 3x^2 + 2x$

• $f = x^5 + 2x^3 + x^2 \in \mathbb{F}_3[x]$

$\Rightarrow f' = 5x^4 + 2 \cdot 3x^2 + 2x = 2x^4 + 2x$

• $f = x^{14} + 5x^7 + 3 \in \mathbb{F}_7[x]$

$f' = 14 x^{13} + 5 \cdot 7 x^6 = 0$

$5^7 = 5$, $3^7 = 3$ $\quad f = x^{14} + 5^7 x^7 + 3^7 = (x^2 + 5x + 3)^7$

Satz $\mathbb{K}$ Körper.

$\operatorname{char} \mathbb{K} = 0$ oder $\mathbb{K} = \mathbb{F}_p$

$f \in \mathbb{K}[x]$.

f quadratfrei $\iff$ $\gcd(f, f') = 1$

3.1.1

3.1.2

3.1.3

3.1.4

3.2.1

3.2.2

3.2.3

3.2.4

3.2.5

3.3.1

3.3.2