

## Aufgabe 1

### 1. Einheiten in $\mathbb{Z}/N\mathbb{Z}$ , $\mathbb{K}[x]/(x^2)$

•  $\mathbb{Z}/N\mathbb{Z}$  - Beh:  $[m] \in \mathbb{Z}/N\mathbb{Z}$  ist g.d. Einheit, wenn  $\text{ggT}(m, N) = 1$ .

\* "⇐": Sei  $m \in \mathbb{Z}$  mit  $\text{ggT}(m, N) = 1$ . Nach Euklid ex.

$$k, l \in \mathbb{Z} \text{ mit } 1 = \text{ggT}(m, N) = k \cdot m + l \cdot N$$

⇒  $[1] = [km + lN] = [k][m]$ , d.h.  $[m]$  ist eine Einheit.

\* "⇒": Sei  $[m] \in \mathbb{Z}/N\mathbb{Z}$  eine Einheit. Dann ex.  $[k] \in \mathbb{Z}/N\mathbb{Z}$  mit  $[mk] = [m][k] = [1]$ . ⇒  $mk = 1 + l \cdot N$  für ein  $l \in \mathbb{Z}$ .

⇒  $mk + lN = 1$ . Angenommen  $\text{ggT}(m, N) = d \in \mathbb{N}$ .

⇒  $d \mid km + lN = 1$  ⇒  $d = 1$ , □

Also gelten:  $(\mathbb{Z}/9\mathbb{Z})^* = \{[1], [2], [4], [5], [7], [8]\}$

$$(\mathbb{Z}/10\mathbb{Z})^* = \{[1], [3], [7], [9]\}$$

•  $\mathbb{K}[x]/(x^2)$

Analog kann man für Polynome zeigen, dass

$[p] \in \mathbb{K}[x]/(x^2)$  g.d. Einheit ist, wenn  $\text{ggT}(p(x), x^2) = 1$

gilt. Also gilt  $(\mathbb{K}[x]/(x^2))^* = (\mathbb{K}[x]/(x^2)) \setminus \{[x], [0]\}$

$$2. \mathbb{R} = \mathbb{R}[x]/(x^2) \quad \left\{ \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 + b_1 x \\ a_2 + b_2 x \end{pmatrix} \in \mathbb{R}^2 : x^2 + y^2 = 1 \right\}$$

$$\begin{aligned} 1_{\mathbb{R}} = x^2 + y^2 &= (a_1 + b_1 x)^2 + (a_2 + b_2 x)^2 = a_1^2 + b_1^2 x^2 + 2a_1 b_1 x + a_2^2 + b_2^2 x^2 + 2a_2 b_2 x \\ &= a_1^2 + a_2^2 + 2(a_1 b_2 + a_2 b_1)x = 1 + 0 \cdot x \end{aligned}$$

$$\Leftrightarrow a_1^2 + a_2^2 = 1 \wedge (a_1 b_1 + a_2 b_2 = 0 \Leftrightarrow \langle \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \rangle = 0)$$

Also liegt  $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$  auf  $S^1$  und  $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$  ist senkrecht zu  $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ ,

d.h.  $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} x$  beschreibt tangente Geraden zu  $S^1$ .

## Aufgabe 3

1.  $4x^2+8x+4$ ,  $x^5+5x^3+15$ ,  $x^6+x^3+1$

•  $4x^2+8x+4 = 4(x^2+2x+1) = 4(x+1)^2$

Da 4 keine Einheit in  $\mathbb{Z}[x]$  ist und  $x+1$  primitiv und linear ist ist  $2 \cdot 2 \cdot (x+1)^2$  eine Zerlegung in irreduziblen Faktoren in  $\mathbb{Z}[x]$ .  
Diese ist auch eine Zerlegung in  $\mathbb{Q}[x]$ .

•  $x^5+5x^3+15$  da  $\sqrt[5]{5} \mid a_3 = 5$  aber  $25 \nmid a_0 = 15$  ist

dieses Polynom nach dem Eisensteinkriterium in  $\mathbb{Z}[x]$  und damit auch in  $\mathbb{Q}[x]$  irreduzibel.

•  $x^6+x^3+1 = \frac{x^9-1}{x^3-1} = \Phi_{9/3}(x)$ , nach Aufgabe 3.2. des letzten ÜB also irreduzibel in  $\mathbb{Z}[x]$  und auch in  $\mathbb{Q}[x]$ .

2.  $x^2+y^2+1$ ,  $\mathbb{Q}(x,y)$ ,  $\mathbb{C}(x,y)$ . Angenommen: reduzibel

Da für ein Körper  $K$   $K[x,y]$  und  $(K[y])[x]$  isomorph sind und  $\deg_x(x^2+y^2+1) = 2$  in  $(\mathbb{C}[y])[x]$  können wir es in zwei lineare Faktoren zerlegen:

$$(x^2+y^2+1) = (a_1(y)x + b_1(y))(a_2(y)x + b_2(y)), \quad a_1, a_2, b_1, b_2 \in \mathbb{C}[y]$$

$$\Rightarrow x^2+y^2+1 = (a_1 a_2(y) x^2 + (b_1 b_2(y) + (a_1 b_2 + b_1 a_2)(y) \cdot x)$$

$$\Rightarrow a_1(y) a_2(y) = 1, \quad b_1(y) b_2(y) = y^2+1, \quad a_1(y) b_2(y) + b_1(y) a_2(y) = 0$$

Daher sind  $a_1, a_2$  Einheiten und somit konstante Polynome in  $\mathbb{Q}[y]$ .  $\Rightarrow a_1(y) = c, a_2(y) = \frac{1}{c}, c \in \mathbb{C}^*$ .

$$c \cdot \frac{1}{c} = 1, \quad c b_2(y) + b_1(y) \cdot \frac{1}{c} = 0 \quad (\Rightarrow) \quad b_2(y) = -\frac{c}{c} b_1(y)$$

$$\Rightarrow -\frac{c}{c} b_1(y)^2 = y^2+1 \Rightarrow c^2 b_1(y)^2 = -(y^2+1)$$

Damit so ein  $b_1(y)$  ex. muss  $y^2+1 = (ax+b)^2$ ,  $a, b \in \mathbb{C}$  gelten.

$$y^2+1 = a^2 x^2 + 2abx + b^2 \Rightarrow a^2 = 1, 2ab = 0, b^2 = 1 \rightarrow \leftarrow$$

Also ex. kein solches  $b_1(y) \in \mathbb{C}[y]$ , d.h.  $x^2+y^2+1$  irreduzibel über  $\mathbb{C}(x,y)$  und folglich über  $\mathbb{Q}(x,y)$ .