ALG Ü12

405) $K := \mathbb{Z}_2[x] / (f(x))$ $\quad f(x) = x^3 + x + 1$

Begründen Sie warum der Faktorring K ein Körper ist!

Prop 6.2.1.1. Satz von Kronecker

K ... Körper $\quad f \in K[x]$ ... irreduzibel $\Rightarrow K[x]/(f)$ ist ein Körper

angenommen $\exists\, p, q \in \mathbb{Z}_2[x]: p(x) \cdot q(x) = f(x)$

$\text{grad}(p) = 0 \rightarrow p(x) = 1$ .. Einheit $\vee$ $p(x) = 0$ .. geht nicht

$\text{grad}(p) = 1 \Rightarrow p(x) = x$ ... geht nicht $\vee$ $p(x) = x + 1$

$x^3 + x + 1 : x + 1 = x^2 + x \quad \Rightarrow$ .. geht nicht

$-(x^3 + x^2)$

$-x^2 + x + 1 = x^2 + x + 1$

$-(x^2 + x)$

$1 \in \mathbb{R}$

$\text{grad}(p) = 2 \Rightarrow \text{grad}(q) = 1$ ... geht nach oben nicht

$\text{grad}(p) = 3 \Rightarrow \text{grad}(q) = 0$ ... — " — $\Rightarrow f(x)$ ... irreduzibel

$\rightarrow$ K ist Körper

Berechnen Sie das multiplikative Inverse von $x + (x^3 + x + 1) \in K$ mit euklidischen Algorithmus!

$p(x) = x + (x^3 + x + 1) = x^3 + 1$

$f(x) : p(x) = x^3 + x + 1 : x^3 + 1 = 1 \quad p(x) : r_1(x) = x^3 + 1 : x = x^2$

$-x^3 - 1$ $\qquad -x^3$

$x = r_1(x) \qquad 1 = r_2(x)$

$\Rightarrow \text{ggT}(f(x), p(x)) = 1$ und $f(x) = p(x) + r_1(x)$; $p(x) = x^2 r_1(x) + r_2(x)$

$1 = r_2(x) = p(x) - x^2 r_1(x) = p(x) - x^2 (f(x) - p(x)) = p(x) - x^2 f(x) + x^2 p(x)$

$= p(x)(x^2 + 1) - x^2 f(x)$

$\Rightarrow 1 = p(x)(x^2 + 1) \mod f(x) \quad \Rightarrow p^{-1}(x) = x^2 + 1$

Probe: $f(x) = 0 \quad \Rightarrow x^3 = x + 1$

$p(x) \cdot p^{-1}(x) = (x^3 + 1)(x^2 + 1) = (x + 1 + 1)(x^2 + 1) = x(x^2 + 1) = x^3 + x = x + 1 + x = 1$