ALG Ü12

399+400)

400) Geben Sie einen unendlichen Körper K der Charakteristik p an, für den die Abbildung $a \mapsto a^p$ keinen Automorphismus von K definiert.

$K := GF(p)(x)$ hat Charakteristik p $\quad \varphi: K \to K, \; a \mapsto a^p$

Wir wollen zeigen, dass φ nicht surjektiv ist und somit kein Automorphismus sein kann.

$x \in K$ $\quad$ Sei $z = \frac{a}{b} \in K$ bel. mit $\varphi(z) = x$

$\Rightarrow x = \varphi(z) = \varphi\left(\frac{a}{b}\right) = \frac{a^p}{b^p} \iff x b^p = a^p$

$a = \sum_{i=0}^{n} a_i x^i$ $\quad$ grad$(a^p) = np$. $\quad b = \sum_{j=0}^{m} b_j x^j$ $\quad$ grad$(b^p) = mp$

$\Rightarrow$ grad(x) + gra(b^p) = grad(a^p) $\Rightarrow 1 + mp = np \iff 1 = p(n-m)$

Widerspruch zu $p \in \mathbb{P}$ und $n, m \in \mathbb{N} \cup \{0\}$

399) Geben Sie einen unendlichen Körper K der Charakteristik p an, für den die Abbildung $a \mapsto a^p$ einen Automorphismus von K definiert.

Auf jedem Körper K mit char p ist $\varphi: K \to K, \; a \mapsto a^p$ ein Endomorphismus:

$\varphi(0) = 0$, $\varphi(1) = 1$, $\forall a, b \in K: \varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$ klar

$\forall a, b \in K: \varphi(a+b) = (a+b)^p = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} b + \ldots + \binom{p}{p-1} a b^{p-1} + \binom{p}{p} b^p$

$= a^p + \underbrace{p a^{p-1} b + \ldots + p a b^{p-1}}_{\text{enthalten alle den Faktor } p (=0 \text{ da char } p)} + b^p = a^p + b^p = \varphi(a) + \varphi(b)$

$\Rightarrow$ Endomorphismus

(inj) Sei $a \in K$ mit $\varphi(a) = 0$ bel. $\Rightarrow a^p = 0 \Rightarrow a = 0$ da K nullteilerfrei

Def $\tilde{K} := GF(p) \times GF(p^2) \times GF(p^3) \times \ldots$ $\quad (a_i)_{i \in \mathbb{N}} \sim (b_i)_{i \in \mathbb{N}} :\iff a_i = b_i$ für fast alle $i \in \mathbb{N}$

$\sim$ ist eine Kongruenzrelation $\quad$ Dann ist $K := \tilde{K}/\sim$ ein Körper mit char p.

(surj) Sei $[(a_i)_{i \in \mathbb{N}}]_\sim \in K = \tilde{K}/\sim$ bel. In 397 1. haben wir gezeigt, dass $\varphi_i: GF(p^i) \to GF(p^i), \; a \mapsto a^p$ ein Automorphismus ist also surjektiv.

$\Rightarrow \forall i \in \mathbb{N} \; \exists b_i : \varphi_i(b_i) = b_i^p = a_i \quad \Rightarrow \varphi(b_i)_{i \in \mathbb{N}} = (b_i^p)_{i \in \mathbb{N}} = (a_i)_{i \in \mathbb{N}}$

ALG Ü12

401) K ... endlicher Körper   P ... Primkörper von K

zz: $\exists \varphi \in Aut(K): \{x \in K \mid \varphi(x) = x\} = P$

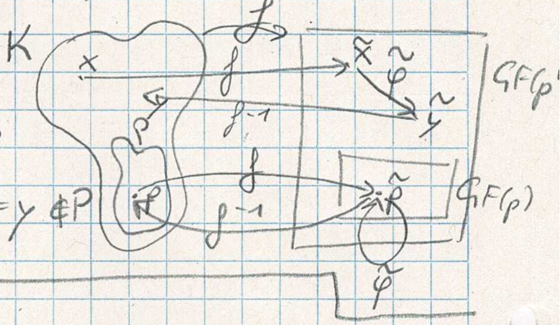
Da K endlich $\exists p \in \mathbb{P}\ \exists n \in \mathbb{N} : |K| = p^n \Rightarrow K \cong GF(p^n) \wedge P \cong GF(p)$.

Also reicht es einen Automorphis $\tilde{\varphi}: GF(p^n) \to GF(p^n)$ zu finden mit

$\{x \in GF(p^n) \mid \tilde{\varphi}(x) = x\} = GF(p)$, da dann

$\forall p \in P: \varphi(p) = f^{-1} \circ \tilde{\varphi} \circ f(p) = f^{-1} \circ \tilde{\varphi}(\tilde{p}) = f^{-1}(\tilde{p}) = p$

$\forall x \in K \setminus P: \varphi(x) = f^{-1} \circ \tilde{\varphi} \circ f(x) = f^{-1} \circ \tilde{\varphi}(\tilde{x}) = f^{-1}(\tilde{y}) = y \notin P$



$\tilde{\varphi}: GF(p^n) \longrightarrow GF(p^n) \qquad x \longmapsto x^p$

Da in GF(p) gilt $\forall x: x^p - x = 0 \Rightarrow \forall x \in GF(p) \subseteq GF(p^n): x^p = x$

$\Rightarrow GF(p) \subseteq \{x \in GF(p^n) \mid \tilde{\varphi}(x) = x\}$

Nun für die andere Richtung: Sei $x \in GF(p^n)$ mit $\tilde{\varphi}(x) = x^p = x$ bel.

$\Rightarrow x^p - x = 0$

In $GF(p)[y]$ gilt $y^p - y = \prod_{\alpha \in GF(p)} (y - \alpha)$. Da $GF(p)[y] \subseteq GF(p^n)[y]$

$\Rightarrow f(y) = y^p - y$ hat genau Nullstellen bei allen $\alpha \in GF(p)$.

Da $f(x) = 0$ folgt also $x \in GF(p)$.

$\Rightarrow \{x \in GF(p^n) \mid \tilde{\varphi}(x) = x\} \subseteq GF(p)$

ALG Ü12

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

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

$grad(p) = 0 \quad \rightarrow p(x) = 1$ … Einheit $\vee\ p(x) = 0$ … geht nicht

$grad(p) = 1 \quad \Rightarrow p(x) = x$ … geht nicht $\vee\ p(x) = x+1$

$$\begin{aligned} &x^3+x+1 : x+1 = x^2+x \quad \Rightarrow \text{… geht nicht}\\ &-(x^3+x^2)\\ &\quad -x^2+x+1 = x^2+x+1\\ &\quad -(x^2+x)\\ &\qquad 1\ R \end{aligned}$$

$grad(p) = 2 \Rightarrow grad(q) = 1$ … geht nach oben nicht

$grad(p) = 3 \Rightarrow grad(q) = 0$ … — " — $\qquad \Rightarrow f(x)$ … irreduzibel

$\Rightarrow$ K ist Körper

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

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

$$f(x) : p(x) = x^3+x+1 : x^3+1 = 1 \qquad p(x) : r_1(x) = x^3+1 : x = x^2$$
$$-x^3-1 \qquad\qquad\qquad -x^3$$
$$x = r_1(x) \qquad\qquad\qquad 1 = r_2(x)$$

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

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

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

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

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

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