ALG Ü12

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

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

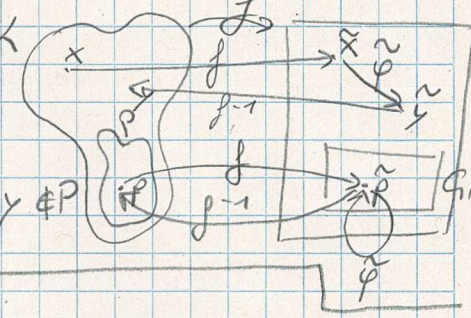
Da K endlich $\exists p \in \mathbb{P}\ \exists n \in \mathbb{N}: |K| = p^n \Rightarrow K \cong GF(p^n) \wedge P \cong GF(p)$.

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

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

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



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

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 $a \in GF(p)$.

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

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