Beweis von Satz 16.2.2 (Klass. von endlichen Körpern)

Ein Element von $Gal(K/\mathbb{F}_p)$ ist die Frobenius, $F: K \to K$. Wissen: $Gal(K/\mathbb{F}_p)$ ist endl. also existiert $m \in \mathbb{N}$: $\underbrace{F \circ \dots \circ F}_{m\text{ x}} = Id$. Sei m minimal mit dieser Eigenschaft, dann ist $G = \{ Id_K, F, F \cdot F, \dots, \underbrace{F \circ \dots \circ F}_{(m-1)\text{ x}} \} \subset Gal(K/\mathbb{F}_p)$ eine Untergruppe von Größe m.

Wissen: Nach Bsp. 15.1.7 ist $Fix(G) = \mathbb{F}_p$. Artin: $K/\mathbb{F}_p$ ist Galois mit Gruppe G, also

$$m = \#Gal = [K : \mathbb{F}_p] = \dim_{\mathbb{F}_p} K$$

und K hat p^m viele Elemente.

Weiter gilt: $\underbrace{F \circ \dots \circ F}_{m\text{ x}}(a) = a$ für alle $a \in K$

$\Leftrightarrow$ $a^{(p^m)} = a$ — " —

$\Leftrightarrow$ a ist Nullstelle von $x^{(p^m)} - x = 0$, für all. $a \in K$.

$\Rightarrow$ $K/\mathbb{F}_p$ ist die Zerfällungskörper des Polynoms $x^{(p^m)} - x \in \mathbb{F}_p[x]$.

□