F15-T2-A5

Sei p eine Primzahl und $q = p^n$, $n > 0$. Weiter sei K ein Körper der Charakteristik p. Zeigen Sie, dass die Nullstellen des Polynomes $f(X) = X^q - X$ einen Unterkörper von K bilden.

Lösungsvorschlag. Sei $N \subset K$ die Menge der Nullstellen von $X^q - X$ in K. Offensichtlich ist $0, 1 \in N$. Es bleibt also nur zu zeigen, dass gilt[1]:

1. $a + b \in N$ für $a, b \in N$,
2. $ab \in N$ für $a, b \in N$,
3. $-a \in N$ für $a \in N$,
4. $a^{-1} \in N$ für $0 \neq a \in N$.

Setzten wir als bekannt voraus, dass $(\bullet)^p$ und damit auch $(\bullet)^q \colon K \to K$, ein Körperautomorphismus ist, so wären 1. - 4. offensichtlich – wir wollen die einzelnen Punkte hier aber noch einmal explizit nachrechnen: Aufgrund vom $(-a)^q = -a^q$ ist 3. klar (beachte, dass im Fall von $q = 2$ ja $-a = a$ gilt). Der Punkt 2. folgt wegen

$$(ab)^q = a^q b^q = ab.$$

Für den Punkt 1. beobachten wir

$$(a+b)^q = \sum_{i=0}^{q} \binom{q}{i} a^i b^{q-i} \equiv a^q + b^q \mod p.$$

Also $(a + b)^q = a^q + b^q = a + b$ in K wegen $\mathrm{char}(K) = p$. Für den letzten Punkt 4. erhalten wir

$$(a^{-1})^q = (a^q)^{-1} = a^{-1}.$$

[1] Wenn man wollte, könnte man die genannten Bedingungen ersetzen durch $a - b \in N$ für $a, b \in N$ und $ab^{-1} \in N$ für $a, b \in N$ mit $b \neq 0$.