Aufgabe F17T2A3 (12 Punkte)

Sei K ein endlicher Körper mit seiner multiplikativen Gruppe $(K^\times, \cdot)$, und sei weiter $H = \{a^2 \mid a \in K^\times\}$. Zeigen Sie:

(a) H ist eine Untergruppe von $(K^\times, \cdot)$;

(b) $H = K^\times$, falls $\mathrm{char}(K) = 2$;

(c) H hat Index 2 in $K^\times$, falls $\mathrm{char}(K) > 2$.

Lösung:

zu (a) Wegen $1 = 1^2$ ist jedenfalls das Neutralelement von $K^\times$ in H enthalten. Seien nun $c, d \in H$ vorgegeben. Dann gibt es $a, b \in K^\times$ mit $c = a^2$ und $d = b^2$. Es folgt $cd = a^2b^2 = (ab)^2 \in H$ und $c^{-1} = (a^2)^{-1} = (a^{-1})^2 \in H$.

zu (b) Wegen $\mathrm{char}(K) = 2$ gilt $|K| = 2^n$ für ein $n \in \mathbb{N}$. Außerdem ist $K^\times$ als multiplikative Gruppe eines endlichen Körpers zyklisch, also eine zyklische Gruppe der Ordnung $2^n - 1$. Sei $c \in K^\times$ ein Element mit $K^\times = \langle c \rangle$. Wir beweisen nun die Gleichung $H = K^\times$. Die Inklusion „$\subseteq$“ ist auf Grund der Definition offensichtlich. Sei umgekehrt $a \in K^\times$ vorgegeben. Dann gibt es ein $m \in \mathbb{N}_0$ mit $a = c^m$. Ist m gerade, $m = 2k$ mit $k \in \mathbb{N}_0$, dann gilt $a = c^{2k} = (c^k)^2 \in H$. Ist m ungerade, dann ist $m + 2^n - 1$ gerade, also $m + 2^n - 1 = 2k$. Wegen $c^{2^n-1} = 1$ gilt dann $a = c^m \cdot 1 = c^m \cdot c^{2^n-1} = c^{m+2^n-1} = c^{2k} = (c^k)^2$. Also liegt a auch in diesem Fall in H.

zu (c) Hier verwenden wir den Homomorphiesatz für Gruppen. Sei $\phi : K^\times \to K^\times$ gegeben durch $\phi(a) = a^2$ für alle $a \in H$. Diese Abbildung ist ein Gruppenhomomorphismus, denn es gilt $\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$ für alle $a, b \in K^\times$. Das Bild von ϕ ist offenbar genau die Untergruppe H. Außerdem gilt $\ker(\phi) = \{\pm 1\}$. Denn für alle $a \in K^\times$ gilt die Äquivalenz $a \in \ker(\phi) \Leftrightarrow \phi(a) = 1 \Leftrightarrow a^2 = 1 \Leftrightarrow a^2 - 1 = 0$, die Elemente des Kerns sind also genau die Nullstellen des Polynoms $f = x^2 - 1 \in K[x]$. Offenbar sind ± 1 Nullstellen von f; wegen $\mathrm{char}(K) > 2$ sind diese verschieden, und mehr als zwei Nullstellen kann f als Polynom vom Grad 2 über einem Körper nicht besitzen. Es gilt also $|\ker(\phi)| = |\{\pm 1\}| = 2$. Der Homomorphiesatz liefert einen Isomorphismus $K^\times/\ker(\phi) \cong \mathrm{im}(\phi)$, also

$$\tfrac{1}{2}|K^\times| \quad = \quad \tfrac{|K^\times|}{|\ker(\phi)|} \quad = \quad |K^\times/\ker(\phi)| \quad = \quad |\mathrm{im}(\phi)| \quad = \quad |H|.$$

Es folgt $(K^\times : H) = \frac{|K^\times|}{|H|} = 2$.