Aufgabe H19T1A5 (12 Punkte)

Es sei die Gleichung $x^2 + ux + v = 0$ mit $u, v \in \mathbb{F}_q$ betrachtet, wobei $\mathbb{F}_q$ der endliche Körper mit q Elementen ist.

(a) Zeigen Sie für ungerades q: Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$, wenn $u^2 - 4v$ ein Quadrat in $\mathbb{F}_q$ ist.

(b) Zeigen Sie für gerades q und $u \neq 0$: Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$, wenn v/u^2 von der Form $z^2 + z$ für ein $z \in \mathbb{F}_q$ ist.

Lösung:

zu (a) Für jedes $\alpha \in \mathbb{F}_q$ gilt die Äquivalenz

$$\alpha^2 + u\alpha + v = \bar{0} \quad \Leftrightarrow \quad \alpha^2 + u\alpha + (\bar{2}^{-1}u)^2 = \bar{4}^{-1}u^2 - v \quad \Leftrightarrow \quad (\alpha + \bar{2}^{-1}u)^2 = \bar{4}^{-1}u^2 - v$$
$$\Leftrightarrow \quad (\bar{2}\alpha + u)^2 = u^2 - \bar{4}v.$$

Dabei ist zu beachten, dass mit q auch $\mathrm{char}(\mathbb{F}_q)$ ungerade ist und die Elemente $\bar{2}$ und $\bar{4}$ in $\mathbb{F}_q$ in $\mathbb{F}_q$ somit ein multiplikatives Inverses besitzen. Die Rechnung zeigt, dass $u^2 - \bar{4}v$ ein Quadrat in $\mathbb{F}_q$ ist, wenn die Gleichung $x^2 + ux + v = \bar{0}$ in $\mathbb{F}_q$ eine Lösung α besitzt. Setzt man umgekehrt voraus, dass $u^2 - \bar{4}v$ in $\mathbb{F}_q$ ein Quadrat ist, also $\beta^2 = u^2 - \bar{4}v$ für ein $\beta \in \mathbb{F}_q$ gilt, dann erhält man durch Auflösung der Gleichung $\bar{2}\alpha + u = \beta$ nach $\alpha = \bar{2}^{-1}(\beta - u)$ eine Lösung der Gleichung $x^2 + ux + v = \bar{0}$, denn es gilt

$$\begin{aligned}\alpha^2 + u\alpha + v &= (\bar{2}^{-1}(\beta - u))^2 + u(\bar{2}^{-1}(\beta - u)) + v = \bar{4}^{-1}(\beta^2 - \bar{2}u\beta + u^2) + \bar{2}^{-1}u\beta - \bar{2}^{-1}u^2 + v \\ &= \bar{4}^{-1}\beta^2 - \bar{2}^{-1}u\beta + \bar{4}^{-1}u^2 + \bar{2}^{-1}u\beta - \bar{2}^{-1}u^2 + v = \bar{4}^{-1}\beta^2 - \bar{4}^{-1}u^2 + v \\ &= \bar{4}^{-1}(u^2 - \bar{4}v) - \bar{4}^{-1}u^2 + v = \bar{0}.\end{aligned}$$

zu (b) Hier gilt für jedes $\alpha \in \mathbb{F}_q$ die Äquivalenz

$$\alpha^2 + u\alpha + v = \bar{0} \quad \Leftrightarrow \quad u^{-2}\alpha^2 + u^{-1}\alpha + u^{-2}v = \bar{0} \quad \Leftrightarrow \quad u^{-2}v = -(u^{-1}\alpha)^2 - u^{-1}\alpha$$
$$\Leftrightarrow \quad u^{-2}v = (u^{-1}\alpha)^2 + u^{-1}\alpha$$

wobei im letzten Schritt verwendet wurde, dass auf Grund der Voraussetzung, dass q gerade ist, $\mathrm{char}(\mathbb{F}_q) = 2$ und somit $-\bar{1} = \bar{1}$ gilt. Ist α also eine Lösung der Gleichung $x^2 + u + v = \bar{0}$ und setzt man $z = u^{-1}\alpha$, dann gilt $u^{-2}v = z^2 + z$. Ist umgekehrt $z \in \mathbb{F}_q$ ein Element mit $u^{-2}v = z^2 + z$, dann ist $\alpha = uz$ eine Lösung der Gleichung $\alpha^2 + u\alpha + v = \bar{0}$, denn dann gilt

$$\begin{aligned}\alpha^2 + u\alpha + v &= u^2z^2 + u^2z + v = u^2(z^2 + z) + v = u^2 \cdot u^{-2}v + v \\ &= v + v = \bar{2}v = \bar{0}.\end{aligned}$$