Aufgabe H16T3A2 (4+4+4 Punkte)

Sei $p \geq 3$ eine ungerade Primzahl und $\mathbb{F}_{p^2}$ der Körper mit p^2 Elementen. Beweisen Sie:

(a) Die Abbildung $f : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$, die durch $f(a) = a^p$ gegeben ist, ist ein Isomorphismus von Ringen.

(b) Durch die Vorschrift $g(a) = a + a^p$ ist eine Abbildung $g : \mathbb{F}_{p^2} \to \mathbb{F}_p$ gegeben, und diese ist ein surjektiver Gruppenhomomorphismus.

(c) Durch die Vorschrift $h(a) = a^{p+1}$ ist eine Abbildung $h : \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$ gegeben, und diese ist ein surjektiver Gruppenhomomorphismus.

Lösung:

zu (a) Da $\mathbb{F}_{p^2}$ ein Körper der Charakteristik p ist, gilt $(a+b)^p = a^p + b^p$ für alle $a, b \in \mathbb{F}_{p^2}$. Daraus folgt $f(a+b) = f(a) + f(p)$ für alle $a, b \in \mathbb{F}_{p^2}$. Außerdem gilt offenbar $f(\bar{1}) = \bar{1}^p = \bar{1}$ und $f(ab) = (ab)^p = a^p b^p = f(a)f(b)$ für alle $a, b \in\in \mathbb{F}_{p^2}$. Damit ist gezeigt, dass es sich bei f um einen Ringhomomorphismus handelt. Alle Elemente a des Körpers $\mathbb{F}_{p^2}$ sind bekanntlich Nullstellen des Polynoms $x^{p^2} - x \in \mathbb{F}_p[x]$, es gilt also $a^{p^2} = a$ für alle $a \in \mathbb{F}_{p^2}$. Daraus folgt $f(f(a)) = f(a^p) = (a^p)^p = a^{p^2} = a$ für alle $a \in \mathbb{F}_{p^2}$. Die Abbildung f ist also ihre eigene Umkehrabbildung und somit bijektiv.

zu (b) Die Elemente des Körpers $\mathbb{F}_p$ sind genau die Nullstellen des Polynoms $x^p - x \in \mathbb{F}_p[x]$. Ein Element $c \in \mathbb{F}_{p^2}$ ist also genau dann in $\mathbb{F}_p$ enthalten, wenn $c^p = c$ gilt. Nun gilt für alle $a \in \mathbb{F}_{p^2}$ die Gleichung $g(a)^p = (a + a^p)^p = a^p + (a^p)^p = a^p + a^{p^2} = a^p + a = g(a)$. Dies zeigt, dass durch g tatsächlich eine Abbildung von $\mathbb{F}_{p^2}$ nach $\mathbb{F}_p$ definiert ist. Für jedes $a \in \mathbb{F}_p$ gilt $g(a) = a + a^p = a + a = \bar{2}a$. Da p eine ungerade Primzahl ist, handelt es sich bei $\bar{2} \in \mathbb{F}_p$ um ein invertierbares Element. Mit a durchläuft somit auch $\bar{2}a$ alle Elemente von $\mathbb{F}_p$. Damit ist die Surjektivität von h nachgewiesen. Schließlich gilt für alle $a, b \in \mathbb{F}_{p^2}$ noch

$$g(a+b) \quad = \quad (a+b) + (a+b)^p \quad = \quad a + b + a^p + b^p \quad = \quad (a + a^p) + (b + b^p) \quad = \quad g(a) + g(b).$$

Dies zeigt, dass g ein Gruppenhomomorphismus zwischen $(\mathbb{F}_{p^2}, +)$ und $(\mathbb{F}_p, +)$ ist.

zu (c) Offenbar ist h ein Gruppenhomomorphismus, denn für alle $a, b \in \mathbb{F}_{p^2}^\times$ gilt $h(ab) = (ab)^{p+1} = a^{p+1}b^{p+1} = h(a)h(b)$. Für jedes $a \in \mathbb{F}_{p^2}$ liegt $h(a)$ wegen $h(a)^p = (a^{p+1})^p = a^{p^2+p} = a^{p^2} \cdot a^p = a \cdot a^p = a^{p+1} = h(a)$ in $\mathbb{F}_p^\times$, also ist h eine Abbildung von $\mathbb{F}_{p^2}^\times$ nach $\mathbb{F}_p^\times$. Es bleibt zu zeigen, dass h surjektiv ist.

Als multiplikative Gruppe eines endlichen Körpers in $\mathbb{F}_{p^2}^\times$ zyklisch, es gibt also ein Element c in dieser Gruppe mit $\mathrm{ord}(c) = |\mathbb{F}_{p^2}^\times| = p^2 - 1$. Es ist dann $h(c) = c^{p+1}$ ein Element in $\mathbb{F}_p^\times$ der Ordnung $\frac{p^2-1}{p+1} = p-1$. Wegen $|\mathbb{F}_p^\times| = p-1$ ist $h(c)$ also ein Erzeuger von $\mathbb{F}_p^\times$. Da das Bild von h einen Erzeuger von $\mathbb{F}_p^\times$ enthält und zugleich eine Untergruppe von $\mathbb{F}_p^\times$ ist, muss es mit $\mathbb{F}_p^\times$ übereinstimmen. Dies zeigt, dass h surjektiv ist.