Aufgabe F20T2A4

(a) Sei $h : A \to G$ ein surjektiver Gruppenhomomorphismus einer abelschen Gruppe A in eine Gruppe G. Zeigen Sie, dass dann auch G abelsch ist.

(b) Sei p eine Primzahl, $p \neq 2$. Bestimmen Sie die Anzahl der Nullstellen des Polynoms $f(X) = x^2 + 2x + 1$ in $\mathbb{F}_{p^2}$ und in $\mathbb{Z}/p^2\mathbb{Z}$.

(c) Man zeige oder widerlege folgende Aussage: Für alle $a, b, c \in \mathbb{N}$ gilt $\mathrm{ggT}(a, b, c)\mathrm{kgV}(a, b, c) = abc$.

Lösung:

zu (a) Seien $u, v \in G$ vorgegeben. Zu zeigen ist $uv = vu$. Da h surjektiv ist, gibt es $a, b \in A$ mit $h(a) = u$ und $h(b) = v$. Weil A abelsch ist, gilt $ab = ba$. Auf Grund der Homomorphismus-Eigenschaft von h folgt $uv = h(a)h(b) = h(ab) = h(ba) = h(b)h(a) = vu$.

zu (b) Für alle $\alpha \in \mathbb{F}_{p^2}$ gilt die Äquivalenz

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

Dabei wurde im vorletzten Schritt verwendet, dass in jedem Körper K die Äquivalenz $\beta = 0_K \Leftrightarrow \beta^2 = 0_K$ für alle $\beta \in K$ gültig ist. (Im Fall $\beta = 0_K$ ist die Äquivalenz offensichtlich, im Fall $\beta \neq 0_K$ die Implikation „$\Rightarrow$“ ebenfalls, und „$\Leftarrow$“ erhält man durch $\beta = \beta^{-1}\beta^2 = \beta^{-1} \cdot 0_K = 0_K$.) Das Polynom f besitzt in $\mathbb{F}_{p^2}$ also genau eine Nullstelle.

Im Ring $\mathbb{Z}/p^2\mathbb{Z}$ ist diese Äquivalenz aber falsch, weshalb hier anders vorgegangen werden muss. Sei $a \in \mathbb{Z}$ und $\bar{a}$ das Bild von a in $\mathbb{Z}/p^2\mathbb{Z}$. Es gilt die Äquivalenz

$$\begin{aligned} f(\bar{a}) = \bar{0} \quad \Leftrightarrow \quad \bar{a}^2 + 2\bar{a} + \bar{1} = \bar{0} \quad \Leftrightarrow \quad (\bar{a} + \bar{1})^2 = \bar{0} \quad \Leftrightarrow \quad p^2 \mid (a+1)^2 \quad \Leftrightarrow \quad p \mid (a+1) \\ \Leftrightarrow \quad \exists\, k \in \mathbb{Z} : a + 1 = kp \quad \Leftrightarrow \quad a \in -1 + p\mathbb{Z} \quad \Leftrightarrow \quad \bar{a} \in \{-\bar{1} + \bar{p}\bar{k} \mid k \in \mathbb{Z}\} \\ \Leftrightarrow \quad \bar{a} \in \{-\bar{1} + \bar{p}\bar{k} \mid 0 \leq k < p\}. \end{aligned}$$

Im vierten Schritt ist die Implikation „$\Leftarrow$“ erfüllt, denn aus $a+1 = kp$ für ein $k \in \mathbb{Z}$ folgt $(a+1)^2 = k^2p^2$. Ebenso gilt „$\Rightarrow$“, denn wäre $a+1$ teilerfremd zu p, dann würde dies auch für $(a+1)^2$ gelten. Im letzten Schritt haben wir verwendet, dass für $k, \ell \in \mathbb{Z}$ die Elemente $-\bar{1} + \bar{p}\bar{k}$ und $-\bar{1} + \bar{p}\bar{\ell}$ in $\mathbb{Z}/p^2\mathbb{Z}$ genau dann übereinstimmen, wenn $-1 + pk \equiv -1 + p\ell \bmod p^2$ gilt, was zu $pk \equiv p\ell \bmod p^2$ und $k \equiv \ell \bmod p$ äquivalent ist. Damit $-\bar{1} + \bar{p}\bar{k}$ alle Elemente von $\mathbb{Z}/p^2\mathbb{Z}$ durchläuft, genügt es also, für k alle Elemente aus einem Repräsentantensystem von $\mathbb{Z}/p\mathbb{Z}$ einzusetzen, zum Beispiel $\{0, 1, ..., p-1\}$. Zugleich sind diese Elemente dann alle verschieden. Das Polynom f hat also in $\mathbb{Z}/p^2\mathbb{Z}$ genau p Nullstellen.

zu (c) Diese Aussage ist im Allgemeinen falsch. Setzt man zum Beispiel $a = 5$, $b = 5^2$, $c = 5^3$, dann gilt $\mathrm{ggT}(a, b, c) = 5$, $\mathrm{kgV}(a, b, c) = 5^3$ und somit $\mathrm{ggT}(a, b, c)\mathrm{kgV}(a, b, c) = 5^4$, andererseits aber $abc = 5 \cdot 5^2 \cdot 5^3 = 5^6$. (Im Gegensatz dazu ist die Gleichung $\mathrm{ggT}(a, b)\mathrm{kgV}(a, b) = ab$ für beliebige $a, b \in \mathbb{N}$ richtig. Man beweist diese Gleichung leicht, indem man die Primfaktorzerlegung von a und b betrachtet und die Formeln für die Primfaktorzerlegung von ggT und kgV aus der Vorlesung verwendet.)