Übungsblatt № 14

Aufgabe 14.2: Ein Körper mit genau 4 Elementen

Es sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ und $f = X^2 + X + 1_{\mathbb{F}_2} \in \mathbb{F}_2[X]$. Ferner sei $K = \mathbb{F}_2[X]/\langle f \rangle$.

a) Zeigen Sie, dass f irreduzibel ist und folgern Sie, dass K ein Körper ist
b) Bestimmen Sie alle Elemente in K und stellen Sie die zugehörigen Additions- und Multiplikationstafeln auf
c) Ist $K^\times$ zyklisch? Falls ja, bestimmen Sie *alle* Erzeuger von $K^\times$

Zu a). Wir erinnern uns, dass Polynome mit Grad 2 genau dann irreduzibel sind, wenn sie keine Nullstellen im zugrundeliegenden Körper haben. Da 2 eine Primzahl ist, ist $\mathbb{F}_2$ ein Körper. Durch einfaches einsetzen lässt sich prüfen:

$$f(0_{\mathbb{F}_2}) = 1_{\mathbb{F}_2} \neq 0_{\mathbb{F}_2} \qquad f(1_{\mathbb{F}_2}) = 1_{\mathbb{F}_2} + 1_{\mathbb{F}_2} + 1_{\mathbb{F}_2} = 1_{\mathbb{F}_2} \neq 0_{\mathbb{F}_2}$$

Somit hat f in $\mathbb{F}_2$ keine Nullstellen und ist damit irreduzibel. Da $\mathbb{F}_2$ ein Körper ist, ist $\mathbb{F}_2[X]$ euklidisch und damit insbesondere ein Hauptidealbereich. Das hat zur Folge, dass für irreduzible Ideale $\mathfrak{a}$ gilt, dass $\mathbb{F}_2[X]/\mathfrak{a}$ ein Körper ist. Somit ist K ein Körper.

Zu b). Wir wissen, dass wir Elemente in Faktorringen durch ihre Restklassen beschreiben können. In Polynomringen betrachten wir dazu natürlich die Polynomdivision mit Rest. Da f Grad 2 hat, können also höchstens Polynome von Grad 1 in K auftauchen. Von diesen gibt es in K aber nur die folgenden vier:

$$0 \qquad 1 \qquad X \qquad X+1$$

Für die Multiplikationstafel betrachten wir noch

$$\begin{aligned}
&X^2 \mod X^2 + X + 1 = -X - 1 = X + 1\\
&X(X+1) = X^2 + X = X + 1 + X = 2X + 1 = 1\\
&(X+1)(X+1) = X^2 + 2X + 1 = X + 1 + 1 = X + 2 = X
\end{aligned}$$

Damit ergeben sich:

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Hier sehen wir auch sehr schön, dass K die Kommutativität von $\mathbb{F}_2[X]$ erbt, da die Multiplikationstafel symmetrisch ist.

Zu c). Da K ein endlicher Körper ist, ist $K^\times$ zyklisch. Mit der oben bestimmten Multiplikationstafel sehen wir schnell

$$K^\times = \langle X \rangle = \langle X + 1 \rangle$$