Bsp für Eindeutigkeit (b.a. Isom.) eines Körpers mit gegebener Anzahl von Elementen; vgl Lemma 2.58

Wir haben konstruiert auf 16.06.20 - 8 ff:

$$\mathbb{F}_8 := \mathbb{F}_2[X] / (X^3 + X + 1)$$

Wir haben geschrieben:

$$\beta := X + (X^3 + X + 1)$$

Das hatte $2 = 0$ und $\beta^3 = \beta + 1$ in $\mathbb{F}_8$ zur Folge. Ferner ist

$$\mathbb{F}_8 = \{ 0, 1, \beta, 1+\beta, \beta^2, 1+\beta^2, \beta+\beta^2, 1+\beta+\beta^2 \}.$$

Aber es gibt auch $X^3 + X^2 + 1$ ein irreduzibles normiertes Polynom in $\mathbb{F}_2[X]$ vom Grad 3.

Alternativ können wir also konstruieren:

$$\widetilde{\mathbb{F}}_8 := \mathbb{F}_2[X] / (X^3 + X^2 + 1),$$

$$\tilde{\beta} := X + (X^3 + X^2 + 1),$$

$$2 = 0, \quad \tilde{\beta}^3 = \tilde{\beta}^2 + 1 \text{ in } \widetilde{\mathbb{F}}_8,$$

$$\widetilde{\mathbb{F}}_8 = \{ 0, 1, \tilde{\beta}, \tilde{\beta}+1, \tilde{\beta}^2, 1+\tilde{\beta}^2, \tilde{\beta}+\tilde{\beta}^2, 1+\tilde{\beta}+\tilde{\beta}^2 \}.$$

In Lemma 258 wird folgende Aussage gezeigt:

Sei $A \mid \mathbb{F}_2$ ein algebraischer Abschluß. Sei

$$K := \{ y \in A : y^8 = y \}.$$

Dann gibt es Isomorphismen

$$\mathbb{F}_8 \xrightarrow[\sim]{\varphi} K \xleftarrow[\sim]{\tilde{\varphi}} \tilde{\mathbb{F}}_8$$

Also gibt es auch den Isomorphismus

$$\tilde{\mathbb{F}}_8 \xrightarrow[\sim]{\varphi^{-1} \circ \tilde{\varphi}} \mathbb{F}_8$$

Einen solchen wollen wir konstruieren.

Es hat $X^3 + X + 1$ in $\mathbb{F}_8$

die Nullstellen β, β^2 und $\beta^4 = \beta^2 + \beta$.

Es hat $X^3 + X^2 + 1$ in $\mathbb{F}_8$

die Nullstelle $\beta + 1$:

$$(\beta+1)^3 + (\beta+1)^2 + 1$$

$$= \beta^3 + 3\beta^2 + 3\beta + 1 + \beta^2 + 1 + 1$$

$$= (\beta+1) + \beta^2 + \beta + 1 + \beta^2$$

$$= 0$$

Also hat $X^3 + X^2 + 1$ in $\mathbb{F}_8$

die Nullstellen $\beta + 1$, $(\beta+1)^2 = \beta^2 + 1$

und $(\beta+1)^4 = \beta^4 + 1 = \beta^2 + \beta + 1$.

Wir erhalten folgende Tabelle für die Minimalpolynome der Elemente von $\mathbb{F}_8$:

ξ	$\mu_{\xi,\mathbb{F}_2}(X)$
0	X
1	$X+1$
β	X^3+X+1
$1+\beta$	X^3+X^2+1
β^2	X^3+X+1
$1+\beta^2$	X^3+X^2+1
$\beta+\beta^2$	X^3+X+1
$1+\beta+\beta^2$	X^3+X^2+1

Das ist die Komplettübersicht, von der wir nur einen Teil werden verwenden müssen.

Wir erhalten nun z. B. folgenden Körperisomorphismus gemäß Lemma 189:

$$\widetilde{\mathbb{F}}_8 = \mathbb{F}_2(\tilde{\lambda}) \xrightarrow{\ \psi\ } \mathbb{F}_8$$

$$\underbrace{\tilde{\lambda}}_{\text{hat Minimalpolynom } X^3+X^2+1} \longmapsto \underbrace{\lambda+1}_{\text{ist Nullstelle von } X^3+X^2+1}$$

Als Körperisomorphismus ist ψ injektiv. Da $|\widetilde{\mathbb{F}}_8| = 8 = |\mathbb{F}_8|$, ist ψ damit schon bijektiv.

Also ist ψ ein Körperisomorphismus von $\widetilde{\mathbb{F}}_8$ nach $\mathbb{F}_8$, wie gesucht.