

F23T2AS (V) Übung auch: F22T2A4

Sei $\mathbb{F}_2^{\text{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_2$ und $\mathbb{F}_{64}$ der einkl. bestimmte Erweiterungskörper von $\mathbb{F}_2^{\text{alg}}$ mit 64 Elementen.

Bestimmen Sie die Anzahl

- (a) der Elemente $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_{64} = \mathbb{F}_2(\alpha)$
- (b) der $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_{64}^* = \langle \alpha \rangle$
- (c) der $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_{64} = \mathbb{F}_8(\alpha)$
- (d) des normierten Polynome in $\mathbb{F}_8[x]$ vom Grad 2

2.
al
←
kör
geg
 $\mathbb{F}_2(\alpha)$
 $\mathbb{F}_2 \subseteq \mathbb{F}_2^{\text{alg}}$
 $\Rightarrow$
Ang.
Möglich

F23T2A5 (V) Übung auch: F22T2A4 aber

(e) die Anzahl der ^{normierten} irreduziblen Polynome vom Grad 2 in $\mathbb{F}_8[x]$

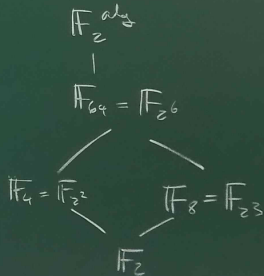
zu (a) Für jedes $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$ gilt offenbar $\alpha \in \mathbb{F}_{64}$.

Beh. Für alle $\alpha \in \mathbb{F}_{64}$ gilt

$$\mathbb{F}_2(\alpha) = \mathbb{F}_{64} \Leftrightarrow \alpha \notin \mathbb{F}_4 \cup \mathbb{F}_8$$

" $\Rightarrow$ " Ang. $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$, aber $\alpha \in \mathbb{F}_4 \cup \mathbb{F}_8$.

1. Fall: $\alpha \in \mathbb{F}_4 \Rightarrow \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_4 \nmid$ da $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$.



A4 aber $\mathbb{F}_{64} \not\subseteq \mathbb{F}_4$

2. Fall: $\alpha \in \mathbb{F}_8 \Rightarrow \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_8 \nmid$ da $\mathbb{F}_2(\alpha) \subseteq \mathbb{F}_8$
aber $\mathbb{F}_{64} \not\subseteq \mathbb{F}_8$

" $\Leftarrow$ " Wsk. $\alpha \notin \mathbb{F}_4 \cup \mathbb{F}_8$ $\alpha \in \mathbb{F}_{64} \Rightarrow \mathbb{F}_2(\alpha)$ ist Teilkörper von $\mathbb{F}_{64} = \mathbb{F}_{2^6}$. Lt. Vorlesung sind die Teilkörper von $\mathbb{F}_{2^6}$ geg. durch $\mathbb{F}_{2^n}$, wobei $n \in \mathbb{N}$ die Teiler von 6 durchläuft $\Rightarrow$

$\mathbb{F}_2(\alpha) \in \{ \mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{64} \}$ Ang. $\mathbb{F}_2(\alpha) = \mathbb{F}_2 \Rightarrow \alpha \in \mathbb{F}_2$

$\mathbb{F}_2 \subseteq \mathbb{F}_4 \Rightarrow \alpha \in \mathbb{F}_4 \nmid$ da $\alpha \notin \mathbb{F}_4 \cup \mathbb{F}_8$ Ang. $\mathbb{F}_2(\alpha) = \mathbb{F}_4 \Rightarrow \alpha \in \mathbb{F}_4 \nmid$

Ang. $\mathbb{F}_2(\alpha) = \mathbb{F}_8 \Rightarrow \alpha \in \mathbb{F}_8 \nmid$ Also bleibt als einzige

Möglichkeit nur $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$ ($\Rightarrow$ Beh.)

2A4 aber $\mathbb{F}_{64} \not\subseteq \mathbb{F}_4$

Aus der Beh. folgt, dass $|\mathbb{F}_{64} \setminus (\mathbb{F}_4 \cup \mathbb{F}_8)| = |\mathbb{F}_{64}| - |\mathbb{F}_4 \cup \mathbb{F}_8| = 64 - |\mathbb{F}_4 \cup \mathbb{F}_8|$ die gesuchte Anzahl ist.

$[\mathbb{F}_2 \subseteq \mathbb{F}_4 \text{ (da } 4=2^2, 2=2^1, 1 \text{ teilt } 2), \text{ ebenso } \mathbb{F}_2 \subseteq \mathbb{F}_8$
 $\Rightarrow \mathbb{F}_2 \subseteq \mathbb{F}_4 \cap \mathbb{F}_8]$ Der Durchschnitt $\mathbb{F}_4 \cap \mathbb{F}_8$ ist
ein ger. Teilkörper von $\mathbb{F}_4$ und $\mathbb{F}_8 \Rightarrow \mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_{2^n}$
mit $n \in \mathbb{N}$, $n|2$ und $n|3 \Rightarrow n=1 \Rightarrow \mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$
also: $|\mathbb{F}_4 \cap \mathbb{F}_8| = 2 \Rightarrow |\mathbb{F}_4 \cup \mathbb{F}_8| = |\mathbb{F}_4| + |\mathbb{F}_8|$
 $- |\mathbb{F}_4 \cap \mathbb{F}_8| = 4 + 8 - 2 = 10$. Die gesuchte Elemente-
zahl ist also $64 - 10 = 54$.

$\mathbb{F}_8 = \mathbb{F}_{2^3}$

zu (b) Für alle $\alpha \in \mathbb{F}_2^{\text{alg}}$ folgt aus $\mathbb{F}_{64}^* = \langle \alpha \rangle$, dass α in $\mathbb{F}_{64}^*$ liegt. Gesucht ist also die Anzahl der erzeugenden Elemente der Gruppe $\mathbb{F}_{64}^*$.

Laut Vorlesung ist $\mathbb{F}_{64}^*$ eine zyklische Gruppe der Ordnung 63. bekannt: Jede zyklische Gruppe der Ordnung n besitzt genau $\varphi(n)$ erzeugende Elemente, für jedes $n \in \mathbb{N}$. Die gesuchte Anzahl ist also $\varphi(63) = \varphi(7) \cdot \varphi(9) = 6 \cdot 6 = 36$.

vor

Ang.

also

Die ge

$|\mathbb{F}_{64}^*|$

zu (d)

in $\mathbb{F}_8$

$a, b \in$

Paare

nome de

zu (e)

Polynome

[allgem.: p Primzahl, $n \in \mathbb{N} \Rightarrow \varphi(p^n) = p^{n-1}(p-1) \Rightarrow \varphi(9) = \varphi(3^2) = 3^1 \cdot 2 = 6$]

zu (c) ges.: Anzahl $x \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_{64} = \mathbb{F}_8(x)$
 Jedes Element mit dieser Eigenschaft liegt
 in $\mathbb{F}_{64}$. Beh.: Für alle $x \in \mathbb{F}_{64}$ gilt die
 Äquivalenz $\mathbb{F}_8(x) = \mathbb{F}_{64} \Leftrightarrow x \notin \mathbb{F}_8$

" $\Rightarrow$ " Ang. $\mathbb{F}_8(x) = \mathbb{F}_{64}$ und $x \in \mathbb{F}_8$.

$x \in \mathbb{F}_8 \Rightarrow \mathbb{F}_8(x) = \mathbb{F}_8 \Rightarrow \mathbb{F}_{64} = \mathbb{F}_8$ $\downarrow$

" $\Leftarrow$ " Es gilt $\mathbb{F}_8 \subseteq \mathbb{F}_8(x) \subseteq \mathbb{F}_{64}$, d.h.
 $\mathbb{F}_8(x)$ ist Teilkörper von $\mathbb{F}_{64} = \mathbb{F}_{2^6}$ und $\mathbb{F}_8$ ist
 Teilkörper von $\mathbb{F}_8(x) \Rightarrow \exists n \in \mathbb{N}$ mit
 $\mathbb{F}_8(x) = \mathbb{F}_{2^n}$ und $n \mid 6$ $\mathbb{F}_8 = \mathbb{F}_{2^3}$ Teilkörper.

1.1

Die
Grad

(x -

dieser
factor

2-cl

(8
2)

es no

c \in \mathbb{F}_2

Teil(d)

Polynom

von $\mathbb{F}_{2^n} \Rightarrow 3 \mid n$ $3 \mid n$ und $n \mid 6 \Rightarrow n \in \{3, 6\}$

Ang. $n=3 \Rightarrow \mathbb{F}_8(x) = \mathbb{F}_{2^3} = \mathbb{F}_8 \Rightarrow x \in \mathbb{F}_8 \downarrow$
also: $n=6 \Rightarrow \mathbb{F}_8(x) = \mathbb{F}_{2^6} = \mathbb{F}_{64} \quad (\Rightarrow \text{Beh.})$

Die gesuchte Elementzahl ist also

$$|\mathbb{F}_{64} \setminus \mathbb{F}_8| = |\mathbb{F}_{64}| - |\mathbb{F}_8| = 64 - 8 = 56$$

zu (d) Jedes normierte Polynom vom Grad 2 in $\mathbb{F}_8[x]$ hat die Form $x^2 + ax + b$ mit $a, b \in \mathbb{F}_8$. Insgesamt gibt es $8 \cdot 8 = 64$ Paare $(a, b) \in \mathbb{F}_8 \times \mathbb{F}_8$, also auch 64 Polynome der angegebenen Form.

zu (e) ges. Anzahl der irreduziblen normierten Polynome vom Grad 2 in $\mathbb{F}_8[x]$

1. Möglichkeit: verwende Teil (c)

Die reduziblen normierten Polynome vom Grad 2 sind genau die Polynome der Form $(x-c) \cdot (x-d)$ mit $c, d \in \mathbb{F}_8$. Die Anzahl dieser Polynome mit zwei verschiedenen Linearfaktoren $x-c, x-d$ ist gleich der Anzahl der 2-elementigen Teilmengen von $\mathbb{F}_8$, also gleich $\binom{8}{2} = \frac{8!}{2!6!} = \frac{1}{2} \cdot 7 \cdot 8 = 28$. Außerdem gibt es noch 8 Polynome der Form $(x-c)^2$ mit $c \in \mathbb{F}_8$. insgesamt: $28 + 8 = 36$ reduzible Pol.

Teil d) $64 - 36 = 28$ irreduzible normierte Polynome vom Grad 2

Korrektur 1. Zeile: „verwende Teil (d)“

2. Möglichkeit: verwende $\text{Tr}(\alpha)$

(Ergebnis $\text{Tr}(\alpha)$: Es gibt genau 56 Elemente $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_8(\alpha) = \mathbb{F}_{64}$.) Für jedes $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_8(\alpha) = \mathbb{F}_{64}$ ist das Minimalpolynom $\mu_{\alpha, \mathbb{F}_8}$ ein irreduzibles, normiertes Polynom in $\mathbb{F}_8[x]$. außerdem: $\text{grad}(\mu_{\alpha, \mathbb{F}_8}) = [\mathbb{F}_8(\alpha) : \mathbb{F}_8] = [\mathbb{F}_{64} : \mathbb{F}_8]$. Sei $d = [\mathbb{F}_{64} : \mathbb{F}_8]$.
 $\Rightarrow \mathbb{F}_{64}$ ist d -dim. $\mathbb{F}_8$ -Vektorraum, dieser enthält 8^d Elemente $\Rightarrow 8^d = 64 \Rightarrow d = 2 \Rightarrow \text{grad}(\mu_{\alpha, \mathbb{F}_8}) = 2$.
Also ist jedes $\alpha \in \mathbb{F}_2^{\text{alg}}$ mit der angegebenen Eigenschaft Nullstelle eines irreduziblen, normierten Polynoms vom Grad 2 in $\mathbb{F}_8[x]$.

Umgekehrt hat jedes Polynom dieser Form zwei verschiedene Nullstellen $\alpha, \beta \in \mathbb{F}_2^{\text{alg}}$ mit $\mathbb{F}_8(\alpha) = \mathbb{F}_8(\beta) = \mathbb{F}_{64}$, denn: Jedes irred. Polynom über $\mathbb{F}_2$ (oder $\mathbb{F}_8$) ist separabel.

Ist also $f \in \mathbb{F}_8[x]$ von der angeg. Form, dann gibt es zwei verschiedene $\alpha, \beta \in \mathbb{F}_2^{\text{alg}}$ mit $f(\alpha) = f(\beta) = 0$. außerdem: f ist Min. pol. dieser Elemente $\Rightarrow [\mathbb{F}_8(\alpha) : \mathbb{F}_8] = \text{grad}(f) = 2 \Rightarrow \mathbb{F}_8(\alpha) = \mathbb{F}_{64}$, ebenso $\mathbb{F}_8(\beta) = \mathbb{F}_{64}$.

Insgesamt gibt es also doppelt so viele Elemente mit der Eigenschaft aus Teil (c) wie irred. normierte Pol von Grad 2 in $\mathbb{F}_8[x]$. Die Anzahl der Polynome ist also gleich $\frac{1}{2} \cdot 56 = 28$ $\square$

Übung: Bestimmen Sie die Anzahl der irreduziblen, normierten Polynome vom Grad 4 im Polynomring $\mathbb{F}_3[x]$. (Ergebnis: 18)

2
(f
w
=
no
=
=
Elem
Also
stelle