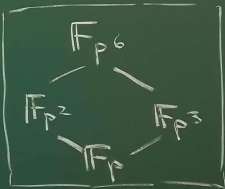


F22TZA4 p Primzahl

(c) ges: Anzahl $a \in \mathbb{F}_{p^6}$ mit $\mathbb{F}_{p^6} = \mathbb{F}_p(a)$

Beh. Für alle $a \in \mathbb{F}_{p^6}$ gilt
die Äquivalenz

$$\mathbb{F}_p(a) = \mathbb{F}_{p^6} \iff a \notin \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}$$



" $\Rightarrow$ " Ang. $a \in \mathbb{F}_{p^2} \Rightarrow \mathbb{F}_p(a) \leq \mathbb{F}_{p^2} \Rightarrow \mathbb{F}_p(a) \neq \mathbb{F}_{p^6}$

Ang. $a \in \mathbb{F}_{p^3} \Rightarrow \mathbb{F}_p(a) \leq \mathbb{F}_{p^3} \Rightarrow \mathbb{F}_p(a) \neq \mathbb{F}_{p^6}$

" $\Leftarrow$ " Sei $a \in \mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$, z. zgl. $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$

$\mathbb{F}_p(a)$ ist Zwischenkörper von $\mathbb{F}_{p^6} | \mathbb{F}_p$, die Zw.

Kor. dieser Erweiterung sind $\mathbb{F}_{p^d}$ mit $d \in \{1, 2, 3, 6\}$
(weil dies die Teiler von 6 sind). Ang. $\mathbb{F}_p(a) = \mathbb{F}_p$
oder $\mathbb{F}_p(a) = \mathbb{F}_{p^2} \Rightarrow \mathbb{F}_p(a) \subseteq \mathbb{F}_{p^2} \Rightarrow a \in \mathbb{F}_{p^2} \downarrow$.
Ang. $\mathbb{F}_p(a) = \mathbb{F}_{p^3} \Rightarrow a \in \mathbb{F}_{p^3} \downarrow$ Also bleibt
 $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$ als einzige Möglichkeit über. ($\rightarrow$ Beh.)

Die Anzahl der gesuchten Elemente ist also gleich

$$\begin{aligned} |\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| &= |\mathbb{F}_{p^6}| - |\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| \\ &= p^6 - |\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}|. \text{ Weiter gilt } |\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| \\ &= |\mathbb{F}_{p^2}| + |\mathbb{F}_{p^3}| - |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}|. \text{ Es gilt weder } \\ &\mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \text{ noch } \mathbb{F}_{p^3} \subseteq \mathbb{F}_{p^2} \text{ (wg. } 2+3, 3+2) \end{aligned}$$

2, 3, 6 |

$$\Rightarrow \mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} \subsetneq \mathbb{F}_{p^2}, \mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} \subsetneq \mathbb{F}_{p^3}$$

(a) = $\mathbb{F}_p$

$$\Rightarrow \mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} \text{ ist echter Teilkörper von } \mathbb{F}_{p^2} \text{ und } \mathbb{F}_{p^3}$$

$\mathbb{F}_{p^2} \downarrow$

$$\Rightarrow \mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} = \mathbb{F}_p, \text{ weil } \mathbb{F}_p \text{ der einzige echte Teilkörper von } \mathbb{F}_{p^2} \text{ (oder } \mathbb{F}_{p^3}) \text{ ist}$$

($\Rightarrow$ Beh.)

$$\Rightarrow |\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| = |\mathbb{F}_{p^2}| + |\mathbb{F}_{p^3}| - |\mathbb{F}_p| = p^2 + p^3 - p$$

gleichs

$$\Rightarrow |\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| = p^6 - (p^2 + p^3 - p) =$$

$p^6 - p^2 - p^3 + p$ ist die gesuchte Elementzahl

$\cup \mathbb{F}_{p^3}$

Übung. Bestimmen Sie die Anzahl der Elemente $a \in \mathbb{F}_{p^{30}}$ mit $\mathbb{F}_p(a) = \mathbb{F}_{p^{30}}$ bzw. $\mathbb{F}_{p^2}(a) = \mathbb{F}_{p^{30}}$.

weder

+2)

(d) Bestimmen Sie die Anzahl der irreduziblen, normierten Polynome vom Grad 6 in $\mathbb{F}_p[x]$.

Sei $M = \{a \in \mathbb{F}_{p^6} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^6}\}$ und $P = \{f \in \mathbb{F}_p[x] \mid f \text{ normiert, irred., } \deg(f) = 6\}$.

Für jedes $a \in M$ ist das Minimalpolynom $m_{a, \mathbb{F}_p} \in \mathbb{F}_p[x]$ irreduzibel, außerdem $\deg(m_{a, \mathbb{F}_p}) =$

$[\mathbb{F}_p(a) : \mathbb{F}_p] = [\mathbb{F}_{p^6} : \mathbb{F}_p] = 6 \rightarrow$ erhalte durch $a \mapsto m_{a, \mathbb{F}_p}$ eine Abb. $\phi: M \rightarrow P$

Beh.: (1) ϕ ist surjektiv

(2) Jedes $f \in P$ hat genau 6 Urbilder unter ϕ .

Aus der Beh. folgt $|M| = 6 \cdot |P| \Rightarrow$

$$|P| = \frac{1}{6} |M| \stackrel{(c)}{=} \frac{1}{6} (p^6 - p^2 - p^3 + p)$$

zu (1) Sei $f \in P$, also irreduzibel, normiert.

$\deg(f) = 6$. Sei $\mathbb{F}_p^{\text{alg}} = \mathbb{F}_{p^6}$ ein algebraischer Abschluss von $\mathbb{F}_p$ (und somit auch von $\mathbb{F}_p$) und $a \in \mathbb{F}_p^{\text{alg}}$ eine Nullstelle von f . f normiert und irred. $\Rightarrow f = \mu_{a, \mathbb{F}_p}$

$$\Rightarrow [\mathbb{F}_p(a) : \mathbb{F}_p] = \deg f = 6$$

$$\Rightarrow |\mathbb{F}_p(a)| = p^6 \Rightarrow \mathbb{F}_p(a) = \mathbb{F}_{p^6}$$

(weil $\mathbb{F}_{p^6} | \mathbb{F}_p$ lt. V. für jedes $n \in \mathbb{N}$ genau einen Zwischenkörper mit p^n Elt. hat)

$$\rightarrow a \in \mathbb{F}_{p^6}, \phi(a) = \mu_{a, \mathbb{F}_p} = 1$$

zu (2) Sei $f \in \mathbb{F}_p$. Über $\mathbb{F}_{p^6}$ zerfällt f in Linearfaktoren. (1) $\Rightarrow$ Jede Nullstelle von f liegt in $\mathbb{F}_{p^6}$, und nach Def. ist jede Nullstelle von f ein Urbild von 1 bzgl. ϕ .

Es genügt also z.zg.: f hat in $\mathbb{F}_{p^6}$ sechs verschiedene Nullstellen, d.h. keine mehrfachen. Dies ist der Fall, weil jedes irreduzible Polynom über einem Körper separabel ist. $\square$

→

F26T2A3 Sei $r \in \mathbb{N}$, $c \in \mathbb{F}_{2^r}$

$P = x^2 + x + c \in \mathbb{F}_{2^r}[x]$. Außerdem seien

$T: \mathbb{F}_{2^r} \rightarrow \mathbb{F}_{2^r}$ und $\phi: \mathbb{F}_{2^r} \rightarrow \mathbb{F}_{2^r}$

definiert durch $T(a) = \sum_{i=0}^{r-1} a^{2^i}$, $\phi(a) = a^2 + a$

für alle $a \in \mathbb{F}_{2^r}$. Zeigen Sie:

(a) ϕ und T sind additive Gruppenhom.

Laut VL ist das Frobenius-Aut. $\varphi: \mathbb{F}_{2^r} \rightarrow \mathbb{F}_{2^r}$,
 $a \mapsto a^2$ verträglich mit Addition und Multi-
plikation. Seien $a, b \in \mathbb{F}_{2^r}$.

$$\phi(a+b) = (a+b)^2 + (a+b) = \varphi(a+b) + (a+b)$$

$$= \varphi(a) + \varphi(b) + a + b = \varphi(a) + a + \varphi(b) + b$$

$$= \phi(a) + \phi(b)$$

$$T(a+b) = \sum_{i=0}^{r-1} \varphi^i(a+b)$$

Mit φ ist auch φ^i ein Automorphismus, für $0 \leq i \leq r-1$

$$\sum_{i=0}^{r-1} (\varphi^i(a) + \varphi^i(b)) = \sum_{i=0}^{r-1} \varphi^i(a) + \sum_{i=0}^{r-1} \varphi^i(b)$$

$$= T(a) + T(b)$$

$$(b) \quad \mathbb{F}_5[x] \xrightarrow{\phi} \text{im}(T) = \ker(\phi) = \mathbb{F}_2$$

Beh. $\ker(\phi) = \mathbb{F}_2$

$$"\subseteq" \quad a \in \ker(\phi) \Rightarrow a^2 + a = \bar{0} \Rightarrow a(a+1) = \bar{0}$$

$$\Rightarrow a = \bar{0} \text{ oder } a+1 = \bar{0} \Rightarrow a = \bar{0} \text{ oder } a = -1 = \bar{1}$$

$$\Rightarrow a \in \{\bar{0}, \bar{1}\} \Rightarrow a \in \mathbb{F}_2 \quad \text{char}(\mathbb{F}_2) = 2 \uparrow$$

$$"\supseteq" \quad \phi(\bar{0}) = \bar{0}^2 + \bar{0} = \bar{0} \Rightarrow \bar{0} \in \ker(\phi)$$

$$\phi(\bar{1}) = \bar{1}^2 + \bar{1} = \bar{2} = \bar{0} \Rightarrow \bar{1} \in \ker(\phi)$$

allt
Nullstelle
t jede
 ϕ
sechs
fachen.
Polynom



Beh. $\text{im}(T) = \mathbb{F}_2$

" $\subseteq$ " Sei $b \in \text{im}(T)$, d.h. $b = T(a)$ für ein $a \in \mathbb{F}_{2^r}$. Laut Vorlesung gilt für alle $c \in \mathbb{F}_{2^r}$ die Äquivalenz $\varphi(c) = c \Leftrightarrow c \in \mathbb{F}_2$, außerdem $\varphi^r(c) = c \quad \forall c \in \mathbb{F}_{2^r}$. Es gilt

$$\varphi(b) = \varphi(T(a)) = \varphi\left(\sum_{i=0}^{r-1} a z^i\right) =$$

$$\varphi\left(\sum_{i=0}^{r-1} \varphi^i(a)\right) = \sum_{i=0}^{r-1} \varphi^{i+1}(a) =$$

$$\sum_{i=1}^{r-1} \varphi^i(a) + \varphi^r(a) = \sum_{i=1}^{r-1} \varphi^i(a) + a =$$

$$\sum_{i=0}^{r-1} \varphi^i(a) = T(a) = b \Rightarrow b \in \mathbb{F}_2$$

$$"\supseteq" \quad T(\bar{0}) = \sum_{i=0}^{r-1} \varphi^i(\bar{0}) = \sum_{i=0}^{r-1} \bar{0} = \bar{0}$$

$$\Rightarrow \bar{0} \in \text{im}(T) \xrightarrow{\text{s.o.}} \text{im}(T) = \{\bar{0}\}$$

oder $\text{im}(T) = \{\bar{0}, \bar{1}\}$. Angenommen

$\text{im}(T) = \{\bar{0}\}$. Dann wird jedes $a \in \mathbb{F}_{2^r}$

von T auf $\bar{0}$ abgebildet, d.h. das Polynom

$q = \sum_{i=0}^{r-1} x^{2^i}$ vom Grad $2^r - 1$ hat 2^r verschiedene

Nullstellen. $\nleftrightarrow$ da jedes Polynom vom Grad n

in einem Körper höchstens n Nullstellen hat,

$$\begin{aligned} & \Rightarrow a^2 + a = -c \Rightarrow -c \in \ker(\phi) \xrightarrow{(a)} -c \in \ker(T) \Rightarrow \\ & T(c) = T(-(-c)) = -T(-c) = -0 = \bar{0}. \end{aligned}$$

für jedes $n \in \mathbb{N}$, also: $\text{im}(T) = \{\bar{0}, \bar{1}, \bar{2}\}$, und $\mathbb{F}_2 \subseteq \text{im}(T)$

(c) Es gilt $\text{im}(\phi) = \ker(T)$

" $\subseteq$ " Sei $b \in \text{im}(\phi)$, d.h. $b = \phi(a) = a^2 + a$ für ein $a \in \mathbb{F}_{2^r}$

$$\Rightarrow T(b) = T(a^2 + a) = T(a^2) + T(a) =$$

$$\sum_{i=0}^{2^r-1} \varphi^i(a) + \sum_{i=0}^{2^r-1} \varphi^i(a^2) = \sum_{i=0}^{r-1} \varphi^i(a) + \sum_{i=0}^{2^r-1} \varphi^{2^i+1}(a)$$

$$= \sum_{i=0}^{r-1} \varphi^i(a) + \varphi\left(\sum_{i=0}^{2^r-1} \varphi^i(a)\right) = \sum_{i=0}^{r-1} \varphi^i(a) + \sum_{i=0}^{r-1} \varphi^i(a)$$

$$= \bar{0}$$

$$\uparrow \text{char}(\mathbb{F}_2) = 2$$

$$\in \text{im}(T) = \mathbb{F}_2$$

$$\varphi(\bar{0}) = \bar{0}, \varphi(\bar{1}) = \bar{1} \Rightarrow b \in \ker(T)$$

" = " Hom.-satz für Gruppen $\Rightarrow \mathbb{F}_{2^r} / \ker(T) \cong \text{im}(T)$,

$$\mathbb{F}_{2^r} / \ker(\phi) \cong \text{im}(\phi) \Rightarrow \frac{2^r}{|\ker(T)|} = \frac{|\mathbb{F}_{2^r}|}{|\ker(T)|} = |\text{im}(T)| \text{ und}$$

$$\frac{2^r}{|\ker(\phi)|} = \frac{|\mathbb{F}_{2^r}|}{|\ker(\phi)|} = |\text{im}(\phi)| \Rightarrow |\text{im}(\phi)| = \frac{2^r}{|\ker(\phi)|} \stackrel{(b)}{=} \frac{2^r}{|\text{im}(T)|}$$
$$= 2^r \cdot \frac{|\ker(T)|}{2^r} = |\ker(T)| \stackrel{\text{im}(\phi) \subseteq \ker(T)}{\Rightarrow} \text{im}(\phi) = \ker(T)$$

(d) Genau dann hat f eine Nullstelle in $\mathbb{F}_{2^r}$, wenn $T(c) = \bar{0}$ gilt.

" $\Rightarrow$ " Ver. $\Rightarrow \exists a \in \mathbb{F}_{2^r}$ mit $f(a) = \bar{0} \Rightarrow a^2 + a + c = \bar{0}$

$$\Rightarrow a^2 + a = -c \Rightarrow -c \in \text{im}(\phi) \stackrel{(a)}{\Rightarrow} -c \in \ker(T) \Rightarrow$$

$$T(c) = T(-(-c)) = -T(-c) = -\bar{0} = \bar{0}$$

$$\frac{2^n}{|\ker(\phi)|} = \frac{|\mathbb{F}_{2^n}|}{|\ker(\phi)|} = |\operatorname{im}(\phi)| \Rightarrow |\operatorname{im}(\phi)| = \frac{2^n}{|\ker(\phi)|} \stackrel{(b)}{=} \frac{2^n}{|\ker(T)|}$$

$$\text{"}\Leftarrow\text{" } T(c) = \bar{0} \Rightarrow T(-c) = -T(c) = -\bar{0} = \bar{0} \Rightarrow -c \in \ker(T)$$

$$\stackrel{(b)}{\Rightarrow} -c \in \operatorname{im}(\phi) \Rightarrow \exists a \in \mathbb{F}_{2^n} : \phi(a) = -c \Rightarrow a^2 + a = -c$$

$$\Rightarrow a^2 + a + c = \bar{0} \Rightarrow f(a) = \bar{0} \Rightarrow f \text{ hat eine Nullst. in } \mathbb{F}_{2^n}$$

Übung: F21T3AS

□