11.3.2021 VORMITTAG

A Ring. Man nehme an, dass $p = \underbrace{1+1+\cdots+1}_{p \text{ mal}} = 0$ in A gilt, wobei p eine Primzahl ist.

z.B: $A = \mathbb{F}_p$, $A = \mathbb{F}_p[x]$, $A = \mathbb{F}_p[x]/(f)$

$Fr_A : A \longrightarrow A$, $a \longmapsto a^p$

$Fr_A(1) = 1^p = 1$

$Fr_A(ab) = (ab)^p = a^p b^p = Fr_A(a)\,Fr_A(b)$

$Fr_A(a+b) = (a+b)^p = a^p + \sum_{0<i<p} \binom{p}{i} a^i b^{p-i} + b^p = a^p + b^p = Fr_A(a) + Fr_A(b)$

$\binom{p}{i}$: diese Zahl ist durch p teilbar

$\Rightarrow Fr_A$ ist ein Ringhomomorphismus

FROBENIUS HOMOMORPHISMUS von A

Beispiel $f = x^5 + x + 1 \in \mathbb{F}_2[x]$, $A = \mathbb{F}_2[x]/(f)$ Ring der $\mathbb{F}_2$-Vektorraum mit Basis $\{1, x, x^2, x^3, x^4\}$

$Fr_A : A \to A$, $a \mapsto a^2$

$\mathbb{F}_2$-linear:
- ok mit der Summe
- $a \in A$, $\lambda \in \mathbb{F}_2$ $\quad Fr_A(\lambda a) = \lambda^2 a^2 = \lambda a^2 = \lambda\, Fr_A(a)$

↑ kleiner Satz von Fermat

Was ist die Abbildungsmatrix Q von Fr_A bezüglich $\{1, x, x^2, x^3, x^4\}$?

$Fr(1) = 1^2 = 1$

$Fr(x) = x^2$

$Fr(x^2) = (x^2)^2 = x^4$

$Fr(x^3) = (x^3)^2 = x^6 = x \cdot x^5$
$= x(x+1) = x^2 + x$

$Fr(x^4) = x^8 = x^3(x+1)$
$= x^4 + x^3$

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Beispiel $f = X^5 + X + 1 \in \mathbb{F}_2[X]$. $A = \mathbb{F}_2[X]/(f)$ Die Abbildungsm. von Fr_A bezüglich $\{1, X, X^2, X^3, X^4\}$ ist

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \in M_5(\mathbb{F}_2) \qquad Q - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Was ist der Eigenraum von Q zum Eigenwert 1? $\ker(Q - I)$

$b \in (\mathbb{F}_2)^5 \qquad Qb = b \qquad (Q - I)b = 0 \qquad b = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}$

$$\begin{cases} 0 = 0 \\ b_1 + b_3 = 0 \\ b_1 + b_2 + b_3 = 0 \\ b_3 + b_4 = 0 \\ b_2 = 0 \end{cases} \qquad \begin{cases} b_2 = 0 \\ b_1 = b_3 = b_4 \end{cases}$$

$\dim \ker(Q - I) = 2$

Eine Basis von $\ker(Q-I)$ ist

$$\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix}, h=\begin{bmatrix}0\\1\\0\\1\\1\end{bmatrix}$$

$$\ker(Q-I) \subseteq (\mathbb{F}_2)^5 \underset{\uparrow}{\simeq} A$$

monomielle Basis

$1 \in A$ $\qquad$ $h = x + x^3 + x^4$

$Qh = h \iff Fr_A(h) = h$ in $A \iff h^2 = h$ in A, $h(h-1) = 0$ in $A = \mathbb{F}_2[x]/(f)$

$\iff$ der Rest der Teilung von $h(h-1)$ durch f ist gleich 0

$\iff f$ teilt $h(h-1) \iff f = \gcd(f, h(h-1))$

Hilfssatz $a,b,c \in \mathbb{K}[x]$

$\gcd(b,c)=1 \Rightarrow$

$\gcd(a,bc)=\gcd(a,b)\cdot\gcd(a,c)$

h und $h-1$ sind relativisch prim:

$\gcd(h,h-1)=\gcd(h,-1)=1$

$\Rightarrow \quad f=\gcd(f,h)\cdot\gcd(f,h-1)$

Zerlegung von f NICHT TRIVIAL!

$\deg\gcd(f,h)\leq\deg h<\deg f$

$\deg\gcd(f,h-1)\leq\deg(h-1)<\deg f$

$\gcd(f,h)=\gcd(x^5+x+1,\ x+x^3+x^4)=x^3+x^2+1$

$\gcd(f,h-1)=x^2+x+1$

$f=(x^3+x^2+1)(x^2+x+1)$

$f = (x-1)(x+1)(x-2)$ $\quad \mathbb{F}_{11}[x]$

$h \rightsquigarrow (x^2-1) \cdot (x-2)$

$h \rightsquigarrow (x^2-3x+2) \cdot (x+1)$

$h \rightsquigarrow (x-1) \cdot (x-1) \cdot (x-2)$

p Primzahl

- Kleiner Satz von Fermat: $\forall a \in \mathbb{F}_p \,,\quad a^p - a = 0$
- $\prod_{0 \le i < p} (x - i) = x^p - x \quad \text{in } \mathbb{F}_p[x]$
- $\forall h \in \mathbb{F}_p[x] \qquad \prod_{0 \le i < p} (h - i) = h^p - h$

Aufgabe 4.1.1,

4.2.1

4.1.2, 4.2.2, 4.2.3