FFC 16.6.08

- Minimalpolynom eines lin. Operators / einer Matrix - rationale Normalform

Geg n-dim K-VR V, $\sigma \in End_K(V) = \{\varphi: V \to V \mid \varphi\ K\text{-linear}\}$

bzgl Basis $\mathcal{B}$ habe σ Matrix S

Definieren eine von σ induzierte $K[x]$-Modulstruktur auf V

$f(x)\, v = f(\sigma)\, v$ sei die Skalarmultiplikation. Nennen diesen $K[x]$-Modul V_σ.

Lem: Für K-Unterraum U von V äquivalent

1) U invariant unter σ, d.h $\sigma(U) \subseteq U$

2) U ist $K[x]$-Untermodul von V_σ

Klar da $U \leq (V,+)$ sowieso und Abgeschlossenheit bzgl Skalarmult mit El $\in K[x]$ heißt Abgeschlossenheit bzgl Mult mit El $\in K$ und Anwendg von σ

Def: R kom Ring. Ein R-Modul M heißt zyklisch, wenn er von einem El. erzeugbar ist, d.h $M = Rm$ für ein $m \in M$.

Bem: $M = Rm$ zyklischer R-Modul dann $M \cong R/Ann_R(m)$ wobei $Ann_R\, m = \{r \in R \mid rm = 0\} \trianglelefteq R$ via $f: R \to Rm$ $f(r) = rm$ und 1. Isomorphiesatz.

Lemma: für ~~σ invarianten~~ Teilraum U des K-VR V äquivalent:

1) U σ invarianter Teilraum, der eine σ-zyklische K-Basis hat, d.h Basis der Form: $v, \sigma v, \sigma^2 v, \dots, \sigma^{k-1} v$ ($k = \dim U$).

2) U ein zyklischer $K[x]$-Untermodul von V_σ.

bzw genauer: äquivalent ist:

1') U σ-inv Teilraum mit Basis bzgl der $\sigma|_U$ eine Matrix der Form

$$\begin{pmatrix} 0 & 1 & & 0 \\ 0 & 0 & 1 & \\ \vdots & 0 & \ddots & \ddots \\ 0 & & & 0 \quad 1 \\ a_0 & a_1 & \cdots & a_{k-1} \end{pmatrix}$$

2') U zyklischer $K[x]$ Untermodul $U = K[x]v$ mit $Ann_{K[x]} v = f(x) K[x]$

mit $f(x) = x^k - a_{k-1} x^{k-1} - a_{k-2} x^{k-2} - \dots - a_0$

$1' \to 2'$ Die ersten $k-1$ Zeilen der Matrix von $\sigma|_U$ bedeuten Basis der Form $v, \sigma v, \sigma^2 v, \dots, \sigma^{k-1} v$, letzte Zeile: $\sigma^k v = (a_0 + a_1\sigma + a_2\sigma^2 + \dots + a_{k-1}\sigma^{k-1})\sigma$

Sei $f(x) = x^k - a_{k-1}x^{k-1} - \dots - a_0$ dann $f(\sigma|_U) = 0$ (als lin. Abb $U \to U$) und $\sigma|_U$ ist nicht Nullst. ein $g \in K[x]$ mit $\deg g < k = \deg f$ weil $v, \sigma v, \dots, \sigma^{k-1} v$ K-l.u. und daher $(b_0 + b_1\sigma + \dots + b_{k-1}\sigma^{k-1})v \neq 0$, für alle $b_0, \dots, b_{k-1}$ nicht alle 0.

Also $Ann_{K[x]}(U) = Ann_{K[x]}(v) = K[x]f(x)$

$2' \to 1'$ $U = K[x]v$ (U zyklischer $K[x]$-Modul) heißt $U = \{g(x)v \mid g(x) \in K[x]\}$ wobei man sich auf $g(x)$ mit $\deg g < f$ beschränken kann, da für $g(x) = q(x)f(x) + r(x)$ gilt $g(\sigma)v = r(\sigma)v$ [da ja $f(\sigma)v = 0$]

$U = \{g(\sigma)v \mid g \in K[x] \; \deg g < \deg f = k\}$ also K-VR ist U erzeugt von $v, \sigma v, \dots \sigma^{k-1}v$, und $v, \sigma v, \dots, \sigma^{k-1}v$ sind K-l.u., da $\sigma|_U$ kein Polynom von Grad $< k$ erfüllt.

Da außerdem $\sigma^k v = (a_{k-1}\sigma^{k-1} + \dots + a_1\sigma + a_0)v$ hat $\sigma|_U$ die Matrix wie in $1'$ (Gefährten M von f).

Da $K[x]$ Euklidischer Ring ist, hat V_σ Darstellung als direkte Summe von zykl. $K[x]$-Moduln $V_\sigma = K[x]/(m_1) \oplus \dots \oplus K[x]/(m_n)$ $m_i \in K[x]$ sod. $m_1 | m_2 | \dots | m_{n-1} | m_n$ ($K[x]$ ist all. erz $K[x]$-Modul, da sogar endl. erz K-VR; V_σ ist Torsionsmodul d.h. $\forall v \in V_\sigma \; \exists f \neq 0 \; f \in Ann_{K[x]} v$ nämlich ist $\chi_\sigma(x)$ das char Polyn. von σ in $Ann_{K[x]} v$ ~~f~~ für alle $v \in V$.

Man bekommt $m_1 \dots m_n$ indem man ein Erzeugendensyst von V_σ nimmt, und ein Erzeugendensyst. des Kerns des $K[x]$-Modul-Epim

$\varphi: K[x] \times \dots \times K[x] \to V_\sigma$

$\varphi(e_i) = g_i$, zB als Erzeugendensyst eine Basis $v_1 \dots v_n$ des K-VR V und als Relation $xv_i - \sigma v_i = 0$

diese Relationen mit den Einträgen der Matrix von σ angeschrieben:

$xv_i - (s_{i1}v_1 + s_{i2}v_2 + \dots + s_{in}v_n) = 0$. D.h. die Zeilen der Relationen Matrix von $v_1 \dots v_n$ als Erzeugendensyst des $K[x]$ Moduls V_σ

Sind: i-te Zeile: $-s_{i1}\ -s_{i2} \dots (x-s_{ii})-s_{i\,i+1} \dots -s_{in}$

Die Relationenmatrix ist also $xI-S = C_\sigma$ (S Matrix von σ bzg Basis $v_1 \dots v_n$) C_σ durch el. Zeilen und Spalten umformungen (Addition von $f(x) Z_i$ zu Z_j für $f \in K[x]$ ($\ast$) und ~~...~~ analog für Spalte) auf Diagonalmatrix mit Einträgen $m_1 | m_2 | \dots | m_{n-1} | m_n$ bringen. Dann $V_\sigma = K[x]/(m_1) \times \dots \times K[x]/(m_n)$ und m_n erzeugt $\mathrm{Ann}_{K[x]} V_\sigma$ d.h $m_n(x) K[x] = \{f(x) \in K[x] \mid f\sigma = 0$ als lineare Abb $V \to V\}$ m_n ist das Minimalpolyn. von σ ~~bzgl~~ bzw auch wenn jede Matrix von σ bzgl einer Basis von V.

Aus der Darstellung $V_\sigma = K[x]/(m_1) \times \dots \times K[x]/(m_n)$ bekommt man eine Darst. von V als direkte Summe von σ-zyklischen Teilräumen $V_\sigma = U_1 \times \dots \times U_n$ sodass $\sigma|_{U_i}$ bzgl einer Basis Matrix G_{m_i} (Gefährtenmatrix von m_i wie in 1') hat.

Bzgl einer ges Basis von V hat also σ die Matrix $\begin{pmatrix} \boxed{G_{m_1}} & & \\ & \ddots & \\ & & \boxed{G_{m_n}} \end{pmatrix}$

Blockdiagonalmatrix mit i-ten Block

$G_{m_i} := \begin{pmatrix} 0 & 1 & & \\ & & \ddots & 1 \\ c_0 & & & c_{k-1} \end{pmatrix}$ von $m_i(x) = x^k - c_{k-1} x^{k-1} - \dots - c_0$

Diese Matrix R_σ von σ bzgl einer Basis von V, der Form:

Blockdiagonalmatrix mit Blöcken $G_{m_1} \dots G_{m_n}$ (G_{m_i}: Gefährtenmatrix von $m_i \in K[x]$) mit $m_1 | m_2 \dots | m_n$ heißt rationale kanonische Form von σ bzw der Matrix von σ (Version mit invarianten Faktoren). (✳)

Offensichtlich haben σ, τ dieselbe rat. kanon Form $\Leftrightarrow$ $V_\sigma \cong V_\tau$ als $K[x]$-Moduln (da die inv. Faktoren eindeutig mit einer Isomorphieklasse von $K[x]$-Modul korrespondieren.

Lemma: $\sigma, \tau \in \mathrm{End}_K(V)$, dann $V_\sigma \cong V_\tau$ (als $K[x]$-Moduln) $\Leftrightarrow$

$\Leftrightarrow \exists\, \varphi \in \mathrm{Aut}_K(V) \quad \sigma = \varphi^{-1} \circ \tau \circ \varphi^{+1}$

Bew: ($\Rightarrow$) $\varphi: V_\sigma \to V_\tau$ $K[x]$-Modul-Iso d.h φ bijektiv, $\varphi(v+w) = \varphi(v) + \varphi(w)$

$\varphi(f(x) v) = f(x) \varphi(v)$ d.h $\varphi(f(\sigma) v) = f(\tau) \varphi(v)$, φ K-lin, da insb.

$\varphi(kv) = k\varphi(v)$ und $\varphi(\sigma v) = \tau \varphi(v)$ also $\sigma = \varphi^{-1} \tau \varphi$.

(⇐) war $\varphi \in \mathrm{Aut}_K V$ mit $\sigma = \varphi^{-1} \circ \tau \circ \varphi$ dann $\forall v \in V_\sigma$
$\varphi(\sigma v) = \tau(\varphi(v))$ und $\forall k \in K$ $\varphi(kv) = k\varphi(v)$ daher $\forall f \in K[x]$
$\varphi(f(\sigma)v) = f(\tau)\varphi(v)$ φ ist $K[x]$ Modul-Hom $V_\sigma \to V_\tau$
bijektiv nach Vor also $K[x]$-Modul-Iso

Zwei lineare Abb $\sigma, \tau : V \to V$ haben die dieselbe rat. Kanon. Form genau dann, wenn $\exists \varphi : V \to V$ bijektiv K-lin mit $\sigma = \varphi^{-1} \circ \tau \circ \varphi$; analog haben zwei Matrizen $\in M_n(K)$ dieselbe rat. kanon Form genau dann wenn sie ähnlich sind.

Damit ist jetzt die Aussage aus dem vorigen Kapitel: $F : K$ endl.-dim Galois-Erw mit zykl. Gal. Gr. $\mathrm{Aut}_K F = \langle \sigma \rangle$ ist, dann hat F eine K-Basis der Form $v, \sigma v, \ldots \sigma^{n-1} v$ $(n = [F:K])$
weil wir gezeigt haben: minimalpolynom von σ ist $x^n - 1$ und ist, da $\deg = \deg$ des char. Polyn auch gleich dem char. Poly $= \chi_\sigma$, daher ist rat. kanon Form der Matrix σ die Gefährtenmatrix von $x^n - 1$ bzw hat F eine σ-zyklische Basis. Insb für Erw von endlichen Körpern $\mathbb{F}_{q^n} : \mathbb{F}_q$ gilt $\mathbb{F}_{q^n}$ hat $\mathbb{F}_q$-Basis der Form: $v, v^q, \ldots, v^{q^{n-1}}$ (normale Basis)

(*) Da man $\mathrm{diag}(m_1 \ldots m_n)$ aus $xI - S$ (S Matrix von σ bzgl $v_1 \ldots v_n$) durch el Zeilen- und Spalten umformungen, die die Det nicht ändern, bekommt, ist
$\chi_\sigma = \det(xI - S) = \det(\mathrm{diag}(m_1, \ldots, m_n)) = m_1(x) \cdot m_2(x) \cdot \ldots \cdot m_n(x)$
Das ist auch die Det von $xI - R_\sigma$, R_σ die rat. kanon Form von σ.
Das minimalpolyn. einer jeden Blocks C_{m_i} ist jeweils m_i (in Zusammenhang mit Satz von McCoy) das Minipoly ein Blockdiag matrix ist das kgV der Minimalpolynome, also ist das Minipoly von $R_\sigma = \mathrm{kgV}(m_1 \ldots m_n) = m_n$
R_σ ähnlich zu jeder Matrix von $\sigma \Rightarrow m_n$ Minimalpolyn. von σ, $m_1 \cdot \ldots \cdot m_n$ char Polyn. von σ.