27.11.13

Repetitorium WiSe 2013/14

Lineare Algebra-Teil: Polynome

- (Abstrakte) Definition des Polynomrings $K[X]$ über einem Körper K:
  Ein Polynom über einem Körper K ist eine Folge $(a_m)_{m\in\mathbb{N}_0}$ von Elementen aus K, bei der fast alle Glieder 0 (:d.h. alle Glieder bis auf endlich viele sind $=0$).
  Die $a_m \in K$ heißen Koeffizienten des Polynoms.
  Die Menge $K[X]$ der Polynome ist bzgl. üblicher Addition und Skalarmultiplikation ein K-VR. Algebraisch interessant wird sie durch die Def. $(a_m)\cdot(b_m) := \left(\sum_{k+l=m} a_k b_l\right)$ für die Ringmultiplikation in $K[X]$.
  Mit dieser Verknüpfung wird $K[X]$ zu einem nullteilerfreien kommutativen Ring ("Polynomring" genannt) mit Einselement.
  Unter einem Monom X^i verstehen wir die Folge, deren i-tes Glied 1 und deren restliche Glieder 0 sind, $\underbrace{X^0 = 1}_{(1,0,0,\dots)}$ ist das Einselement in $K[X]$ $\leadsto K \subseteq K[X]$
- Prinzip des Koeffizientenvergleichs: Zwei Polynome sind (nach Definition) gleich, wenn sie dieselben Koeffizienten haben.
  $a_0 + a_1 \underbrace{X}_{(0,1,0,\dots)} + a_2X^2 + \dots = (a_0, a_1, \dots)$
- Bezeichnungen im Polynomring:
  Der Grad eine Polynoms (a_m) ist die größte Zahl m mit $a_m \neq 0$, falls sie existiert. Dann heißt a_m Leitkoeffizient von (a_m).
  Ist $a_m = 1$, so heißt das Polynom normiert.
  Gradformel: $\deg f\cdot g = \deg f + \deg g$
  Das Nullpolynom ist das Polynom, das nur Nullen als Koeffizienten hat.
  Der Grad des Nullpolynoms wird (gelegentlich) als $-\infty$ definiert.
  Ist m der Grad von (a_m), schreiben wir auch
  $f = \sum_{m=0}^{m} a_m X^m$ für das Polynom, die Ringmultiplikation entspricht dann der üblichen Cauchy-Multiplikation wie bei Reihen.
- Polynomring in mehreren Variablen wird induktiv definiert: $K[X_1,\dots,X_{n+1}] := K[X_1,\dots,X_n][X_{n+1}]$
  ist Ring statt Körper, Konstruktion $R[X]$ wie oben

- Teilbarkeit im Polynomring: $g \in K[X]$ heißt Teiler von $f \in K[X]$, d.h. $g|f$, falls ein $h \in K[X]$ ex. mit $f = g \cdot h$.
  Für $\deg f \geq 1$ heißt f irreduzibel (über K), falls für alle $g, h \in K[X]$ mit $f = g \cdot h$ stets $h \in K \setminus \{0\}$ oder $g \in K \setminus \{0\}$ folgt. Sonst heißt f reduzibel.
  Somit: Ist f reduzibel, so ex. nichttriviale Teiler (mit $\deg \geq 1$) g, h mit $f = g \cdot h$.
  Bsp.: $f = (X^2-1) \cdot X$ reduzibel, $f = \underbrace{X^2+1}_{(X-i)(X+i) \text{ reduzibel über } \mathbb{C}}$ irreduzibel (über $\mathbb{R}$).

- ggT/kgV in $K[X]$: • Ist $f \neq 0$ oder $g \neq 0$, so heißt das normierte Polynom (damit h eindeutig bestimmt) $h \in K[X]$ mit (i) $h|f$ und $h|g$, (ii) für alle $s \in K[X]$ gilt: $s|f$ und $s|g \Rightarrow s|h$ der größte gemeinsame Teiler der Polynome f und g, in Zeichen: $h = \mathrm{ggT}(f,g)$, entsprechend $\mathrm{ggT}(f_1, \dots, f_m)$ für $f_1, \dots, f_m \in K[X]$
  - Ist $f \neq 0$ oder $g \neq 0$, so heißt das normierte Polynom (normiert damit k eindeutig bestimmt) $k \in K[X]$ mit (i) $f|k$ und $g|k$, (ii) für alle $s \in K[X]$ gilt: $f|s$ und $g|s \Rightarrow k|s$ das kleinste gemeinsame Vielfache der Polynome f und g, in Zeichen: $k = \mathrm{kgV}(f,g)$, entsprechend $\mathrm{kgV}(f_1, \dots, f_m)$ für $f_1, \dots, f_m \in K[X]$.

  Bsp.: $\mathrm{ggT}(x^2-1, x^2-2x+1) = x-1$, $\mathrm{kgV}(x(x+1), \underbrace{x^2+2x+1}_{(x+1)^2}) = x \cdot (x+1)^2$.

- Einsetzen von Ringelementen in Polynome / Nullstellen:
  Sei $f = \sum_{i=0}^{m} a_i X^i$ ein Polynom über K, sei R ein Ring mit $K \subseteq R$ (z.B. ein Erweiterungskörper von K), und $\alpha \in R$ beliebig.
  Die Abbildung $K[X] \longrightarrow R$, $\underbrace{\sum_{i=0}^{m} a_i X^i}_{f} \mapsto \underbrace{\sum_{i=0}^{m} a_i \alpha^i}_{f(\alpha)}$ heißt Einsetzungsabbildung (zu α) (und ist ein Ringhomom.).
  Ein $\alpha \in R$ heißt Nullstelle von f, falls $\underbrace{\sum_{i=0}^{m} a_i \alpha^i}_{\in R} = 0$ gilt.

- Der Körper K heißt algebraisch abgeschlossen, wenn in $K[X]$ jedes Polynom vom Grad ≥ 1 eine Nullstelle hat.
  Fundamentalsatz der Algebra: $\mathbb{C}$ ist algebraisch abgeschlossen.
  ($\rightsquigarrow$ Polynome vom Grad ≥ 1 über Körper, der nicht alg. abg. ist, brauchen keine Nullstelle zu haben, z.B. X^2+1 über $\mathbb{R}$)

Zur Untersuchung des Polynomrings $K[X]$ sind nun Begriffe der Ringtheorie erforderlich:

- Definition Ideal: Ist R ein kommutativer Ring mit 1, so heißt eine Teilmenge $I \subseteq R$ ein Ideal von R, wenn gilt:
  $I \neq \emptyset$, $\forall a,b \in I: a-b \in I$, $\forall r \in R \, \forall a \in I: ra \in I$.
  Bsp.: $\{X^2 f \mid f \in K[X]\} = I$ ist Ideal in $K[X]$
- Sind $a_1,\dots,a_m \in R$, so ist die Menge
  $(a_1,\dots,a_m) := \{a_1 y_1 + \dots + a_m y_m \mid y_1,\dots,y_m \in R\}$ ein Ideal von R,
  das von $a_1,\dots,a_m$ erzeugte Ideal.
- Jedes Ideal der Form $(a) = \{ay \mid y \in R\}$ heißt (das von a erzeugte) Hauptideal.
- R heißt Hauptidealring, falls jedes Ideal von R ein Hauptideal ist.
  Bsp.: $\{X^2 f \mid f \in K[X]\} = (X^2)$ ist Hauptideal
- Ein Ideal I von R heißt maximal,
  falls $I \neq R$ und es kein Ideal $J \neq R$ gibt mit $I \subsetneq J \subsetneq R$.

- Ideale sind u.a. wichtig, weil dann die Mengen $R/I := \{a + I \mid a \in R\}$ kommutative Ringe mit Einselement $1_R + I$ ergeben.
  R/I heißt dann Faktorring von R nach dem Ideal I.
  Bsp.: $R = \mathbb{Z}$, $I = 2\mathbb{Z} \rightsquigarrow R/I = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$ der Ring (sogar Körper) mit 2 Elementen.

$\overbrace{\mathbb{Z}/m\mathbb{Z}}$ Körper $\Leftrightarrow$ m prim

Satz: $I \subseteq R$ maximal $\Leftrightarrow R/I$ Körper [$\rightsquigarrow$ z.B. alle endlichen Körper können so konstruiert werden]

Sätze zu Idealen im Polynomring $K[X]$:

1. Lemma von Euklid (d.h. es gibt eine Euklidische Funktion in $K[X]$, d.h. Division mit Rest ist möglich in $K[X]$ ("Polynomdivision"):
   Sind $f, g \in K[X]$, $g \neq 0$, so gibt es eindeutig bestimmte Polynome q und r in $K[X]$ mit $f = q \cdot g + r$ und $\deg r < \deg g$.
   [Koeff. von q, r sind durch die Glg. festgelegt.]

$(X-\alpha)$ abspalten geht ev. mehrfach $\rightsquigarrow$ Korollar: Ist $\alpha \in K$ eine Nullstelle von f, so ist $(X-\alpha)$ Linearfaktor von f, d.h. $f = (X-\alpha) \cdot g$. [Bew.: Div. mit Rest: $f = (X-\alpha) \cdot g + c$, $\deg c = 0$ und $0 = f(\alpha) = \underbrace{(\alpha - \alpha)}_{=0} g(\alpha) + c = c$] $\|$

2. <u>Anzahl der Nullstellen von f in $K[X]$:</u> Ist $f \in K[X]$, $\deg f = n \geq 0$, so hat f höchstens n Nullstellen in K (mit Vielfachheiten gezählt!).
[Für jede Nst. spaltet man einen Linearfaktor ab. Diese werden zu einem Polynom vom Grad der Nullstellenanzahl aufmultipliziert, welches ein Teiler von f ist.]
3. <u>$K[X]$ ist ein Hauptidealring:</u> Jedes Ideal I von $K[X]$ hat die Form $I = (f) = \{h \cdot f \mid h \in K[X]\}$ für ein $f \in K[X]$.
[das normierte Polynom $f \in I$ vom kleinsten Grad erzeugt $I \neq 0$: für jedes $g \in I, g \neq 0$, gilt $g = f \cdot q + r$ mit $r = g - f \cdot q \in I$, also $r = 0$. Es folgt $g = f q \in (f)$.]
<u>Allgemeiner:</u> Jeder euklidische Ring (d.h. der eine Division mit Rest zuläßt) ist ein Hauptidealring.
4. <u>Satz über die eindeutige Zerlegbarkeit von Polynomen in irreduzible Polynome:</u>
("$K[X]$ ist ein faktorieller Ring", allg: Hauptidealringe sind faktoriell)
Ist $f \in K[X] \setminus K$, so läßt sich f eindeutig (bis auf die Reihenfolge) als Produkt von über K irreduziblen Polynomen darstellen.
$(X-\alpha)(X-\bar{\alpha}) = X^2 + \alpha\bar{\alpha}$

Ist insbesondere K algebraisch abgeschlossen, so läßt sich f als Produkt von Linearfaktoren darstellen. (Insb. für $K = \mathbb{C}$)
5. In $K[X]$ gilt: $I \subseteq K[X]$ maximal $\Leftrightarrow$ I wird von irreduziblem Polynom erzeugt
6. <u>Euklidischer Algorithmus</u> zur Bestimmung von $ggT(f,g)$:
Führe sukzessive Division mit Rest durch: $f = g q_1 + r_1$, $g = r_1 q_2 + r_2$, $r_1 = r_2 q_2 + r_3$, $r_2 = r_3 q_3 + r_4 \ldots$ der letzte Rest $\underline{\underline{r_n}} \neq 0$ ist dann "der" ggT (ev. noch normieren nötig)

<u>Einsetzen von Matrizen und Endomorphismen in Polynome:</u>

Sei K Körper, V ein K-VR, $\dim V = n$, $\varphi \in \mathrm{End}(V)$, $A \in K^{n \times n}$.
Für $m \in \mathbb{N}_0$ def. wir $\varphi^0 := id$, $\varphi^{m+1} := \varphi^m \circ \varphi$, $A^0 := I_n$, $A^{m+1} := A^m \cdot A$.
$\leadsto$ φ^m = m-fache Hintereinanderausführung von φ, $A^m = \underbrace{A \cdots A}_{m \text{ mal}}$

<u>Einsetzen:</u> Ist $f \in K[X]$, $f = \sum_{i=0}^{n} a_i X^i$, so sei $f(\varphi) := \sum_{i=0}^{n} a_i \varphi^i$ und $f(A) := \sum_{i=0}^{n} a_i A^i$

Erhalten so $f(\varphi) \in \mathrm{End}(V)$ und $f(A) \in K^{m\times m}$, beachte: $K^{m\times m}$, $\mathrm{End}(V)$ sind Ringe mit 1

Die Einsetzabbildungen $K[X] \to \mathrm{End}(V)$, $f \mapsto f(\varphi)$; $K[X] \to K^{m\times m}$, $f \mapsto f(A)$

sind Ringhomomorphismen, d.h. es gelten die Rechenregeln für alle $f, g \in K[X]$, $\varphi \in \mathrm{End}(V)$ [bzw. $K^{m\times m}$]:

(i) $(f+g)(\varphi) = f(\varphi) + g(\varphi)$

(ii) $(f\cdot g)(\varphi) = f(\varphi) \circ g(\varphi)$

Es gilt auch: $f(\varphi) \circ g(\varphi) = g(\varphi) \circ f(\varphi)$ [weil $K[X]$ kommutativ]

Und auch: Ist ${}_{\mathcal{B}}[\varphi]_{\mathcal{B}}$ die Matrix, die $\varphi \in \mathrm{End}(V)$ darstellt bzgl. Basis $\mathcal{B}$, so ist $f({}_{\mathcal{B}}[\varphi]_{\mathcal{B}}) = {}_{\mathcal{B}}[f(\varphi)]_{\mathcal{B}}$.

[denn: wegen ${}_{\mathcal{B}}[\varphi \circ \psi]_{\mathcal{B}} = {}_{\mathcal{B}}[\varphi]_{\mathcal{B}} \cdot {}_{\mathcal{B}}[\psi]_{\mathcal{B}}$ ist ${}_{\mathcal{B}}[\varphi^i]_{\mathcal{B}} = ({}_{\mathcal{B}}[\varphi]_{\mathcal{B}})^i$, die Beh. folgt damit zusammen mit ${}_{\mathcal{B}}[\alpha\psi]_{\mathcal{B}} = \alpha \cdot {}_{\mathcal{B}}[\psi]_{\mathcal{B}}$, ${}_{\mathcal{B}}[\psi_1+\psi_2]_{\mathcal{B}} = {}_{\mathcal{B}}[\psi_1]_{\mathcal{B}} + {}_{\mathcal{B}}[\psi_2]_{\mathcal{B}}$.]

A. Satz: $f \in K[X]$, $A, B \in K^{m\times m}$. Ist $f(A)=0$, B ähnlich zu A, so ist auch $f(B)=0$.

[Denn: $f(A)=0$, $B = S^{-1}AS$ mit einer invbaren Matrix S

$$\Rightarrow B^i = (S^{-1}AS)^i = \underbrace{S^{-1}AS S^{-1}AS \cdots S^{-1}AS}_{i\text{-mal } S^{-1}AS} = S^{-1}A^iS$$

$$\Rightarrow 0 = S^{-1}\underbrace{f(A)}_{=0}S = S^{-1}\sum_{i=0}^m a_i A^i S = \sum_{i=0}^m a_i S^{-1}A^iS = \sum_{i=0}^m a_i B^i.]$$

• Def Minimalpolynom: Sei $\varphi \in \mathrm{End}(V)$.

Beweis, warum das Minimalpolynom existieren muss: Weil die n^2+1 vielen Vektoren $\mathrm{id} = \varphi^0, \varphi^1, \varphi^2, \dots, \varphi^{n^2} \in \underbrace{\mathrm{End}(V)}_{K\text{-VR}}$ $(\cong K^{m\times m}$ mit Matrixdarst.$)$ linear abhängig sind wegen $\dim_K \mathrm{End}(V) = n^2$, ex. eine nichttriviale Linearkombination, die $=0$ ist: $\sum_{i=0}^{n^2} a_i\varphi^i = 0$, nicht alle $a_i=0$. Also ex. auch ein normiertes Polynom $\mu_\varphi \in K[X]$ vom kleinsten Grad mit $\mu_\varphi(\varphi)=0$. Dieses ist eindeutig bestimmt und heißt Minimalpolynom von φ.

[Völlig analog def. man das Minimalpolynom $\mu_A \in K[X]$ von $A \in K^{m\times m}$]

B. Satz: • Ähnliche Matrizen/Endos haben dasselbe Minimalpolynom [wegen Satz A]

• Jedes Polynom f mit $f(\varphi)=0$ ist Vielfaches von μ_φ [$f = q\cdot\mu_\varphi + r \Rightarrow r(\varphi)=0 \Rightarrow r=0$, da μ_φ minimal]