Tutorium 2

1 Der Polynomring

Wiederholung. Eine Einheit eines Rings ist ein multiplikativ invertierbares Element. Zum Beispiel sind $\{1, -1\}$ die Einheiten in $\mathbb{Z}$, und alle Zahlen außer der 0 in jedem Körper.

Im Polynomring $R[X]$ sind die Einheiten gerade die Einheiten des Grundrings R.

Bemerkung. Im folgenden geht es um Polynomringe über *Körpern* (falls nicht anders erwähnt).

Definition. Seien $f, g \in \mathbb{K}[X]$.

(i) g heißt Teiler von f:

$$f = g \cdot h \text{ für ein } h \in \mathbb{K}[X]$$

Man schreibt dann auch $g \mid f$ ("g teilt f").

(ii) f heißt irreduzibel:

$$f = g \cdot h \quad \Rightarrow \quad g \text{ oder } h \text{ ist Einheit}$$

(iii) f, g heißen teilerfremd:

$$h \mid f \text{ und } h \mid g \quad \Rightarrow \quad h \text{ ist Einheit}$$

Lemma. Das Polynom $f = (X - a_1) \cdot \ldots \cdot (X - a_n) \in \mathbb{K}[X]$ hat genau die (normierten) Teiler

$$(X - a_{i_1}) \cdot \ldots \cdot (X - a_{i_k}) \qquad 1 \leq i_1 < \ldots < i_k \leq n$$

Satz (Division mit Rest)**.** Seien $f, g \in \mathbb{K}[X]$, $g \neq 0$. Dann existieren $q, r \in \mathbb{K}[X]$ mit

$$f = q \cdot g + r \qquad \text{und} \qquad \mathrm{Grad}(r) < \mathrm{Grad}(g)$$

q und r erhält man über die bekannte Polynomdivision aus der Schule.

Definition. Seien $f, g \in \mathbb{K}[X]$.

(i) $h \in \mathbb{K}[X]$ heißt gemeinsamer Teiler von f und g:

$$h \mid f \quad \text{und} \quad h \mid g$$

(ii) $h \in \mathbb{K}[X]$ heißt größter gemeinsamer Teiler von f und g:

h ist gemeinsamer Teiler und jeder andere gemeinsame Teiler teilt h

Normiert ist dieser im Polynomring eindeutig bestimmt, wir schreiben dafür $\mathrm{ggT}(f, g)$.

Satz (Euklids Algorithmus)**.** Seien $f, g \in \mathbb{K}[X]$, und $f = q \cdot g + r$ via Division mit Rest. Dann gilt:

$$\mathrm{ggT}(f, g) = \mathrm{ggT}(g, r)$$

Der ggT lässt also iterativ berechnen, und man erhält $\lambda, \mu \in \mathbb{K}[X]$, so dass:

$$\mathrm{ggT}(f, g) = \lambda f + \mu g$$

Aufgabe 1. Stellen Sie den ggT der Polynome $f := X^4 + X$ und $g := X^5 - X^4 + 2X^3 + 1$ aus $\mathbb{R}[X]$ als solche “Linearkombination” von f und g dar.

Lösung. Wiederholte Division mit Rest ergibt:

$$\begin{aligned}
g &= (X-1) \cdot f \;+\; \underbrace{2X^3 - X^2 + X + 1}_{=:r_1} & \mathrm{ggT}(g, f) &= \mathrm{ggT}(f, r_1) \\
f &= (\frac{1}{2}X + \frac{1}{4}) \cdot r_1 \;+\; \underbrace{-\frac{1}{4}X^2 + \frac{1}{4}X - \frac{1}{4}}_{=:r_2} & &= \mathrm{ggT}(r_1, r_2) \\
r_1 &= (-8X - 4) \cdot r_2 & &= \mathrm{ggT}(r_2, 0)
\end{aligned}$$

Es gilt also: $\mathrm{ggT}(f, g) = X^2 - X + 1$ (normiert!). Weiter:

$$\begin{aligned}
r_2 &= f \;-\; (\frac{1}{2}X + \frac{1}{4}) \cdot r_1 \\
&= f \;-\; (\frac{1}{2}X + \frac{1}{4}) \cdot (g \;-\; (X-1) \cdot f) \\
&= (1 + (\frac{1}{2}X + \frac{1}{4})(X-1)) \cdot f \;-\; (\frac{1}{2}X + \frac{1}{4}) \cdot g \\
&= (\frac{1}{2}X^2 - \frac{1}{4}X + \frac{3}{4}) \cdot f \;-\; (\frac{1}{2}X + \frac{1}{4}) \cdot g
\end{aligned}$$

Und wir erhalten:

$$\begin{aligned}
\mathrm{ggT}(f, g) &= (-4) \cdot r_2 \\
&= (-2X^2 + X - 3) \cdot f \;+\; (2X + 1) \cdot g
\end{aligned}$$

als gesuchte Darstellung.

Satz. Seien $f, g \in \mathbb{K}[X]$. Dann gilt:

$$f,\ g \text{ teilerfremd} \quad \Leftrightarrow \quad \mathrm{ggT}(f, g) = 1 \quad \Leftrightarrow \quad 1 = \lambda f + \mu g \;\; (\lambda,\ \mu \in \mathbb{K}[X])$$

Definition. Sei R ein kommutativer Ring.

(i) $I \subseteq R$ heißt Ideal:

(1) $(I, +)$ ist Untergruppe von $(R, +)$

(2) Für alle $r \in R$, $i \in I$ gilt: $r \cdot i \in I$.

(ii) Ein Ideal I heißt Hauptideal, wenn es sich für ein $a \in R$ in der Form

$$I = \{r \cdot a \mid r \in R\} =: (a)$$

schreiben lässt.

Bemerkung. (i) Man hat immer die Ideale 0 und R.

(ii) **Achtung**: Ein Ideal ist nicht notwendigerweise ein Teilring (die 1 fehlt oftmals).

Satz. Ist $\mathbb{K}$ ein Körper, so ist jedes Ideal in $\mathbb{K}[X]$ ein Hauptideal.

Aufgabe 2. Seien $f = X^2 - 1$ und $g = X^2 - 2X + 1 \in \mathbb{R}[X]$. Zeigen Sie, dass

$$(f, g) := \{\lambda f + \mu g \mid \lambda,\ \mu \in \mathbb{R}[X]\}$$

ein Hauptideal in $\mathbb{R}[X]$ ist, und bestimmen Sie einen Erzeuger.

Lösung. Für jedes $x \in (f, g)$ gilt:

$$\begin{aligned} & h \mid f, h \mid g \quad \Rightarrow \quad h \mid x \\ \Rightarrow \quad & \mathrm{ggT}(f, g) \mid x \\ \Rightarrow \quad & (f, g) \subseteq (\mathrm{ggT}(f, g)) \end{aligned}$$

Wegen $\mathrm{ggT}(f, g) = \lambda f + \mu g$ für gewisse λ, $\mu \in \mathbb{R}[X]$ folgt andererseits auch $(\mathrm{ggT}(f, g)) \subseteq (f, g)$, was die Behauptung zeigt.

Der Erzeuger ist $\mathrm{ggT}(f, g) = X - 1$.

2 Eigenräume

Definition. Sei $\Phi \in \mathrm{End}(V)$ und B eine Basis von V, $\dim V = n$. Dann heißt

$$\mathrm{CP}_\Phi(X) := \det(X \cdot I_n - D_{BB}(\Phi))$$

charakteristisches Polynom von Φ (analog für Matrizen).

Bemerkung. (i) Das charakteristische Polynom ist unabhängig von der Wahl der Basis $\Rightarrow$ Ähnlichkeitsinvariante

(ii) Es hat immer Grad n.

(iii) $\boxed{\mathrm{CP}_\Phi(\lambda) = 0 \quad \Leftrightarrow \quad \lambda \text{ ist EW von } \Phi \quad \Leftrightarrow \quad \mathrm{MP}_\Phi(\lambda) = 0}$

(iv)
$$\boxed{\begin{aligned} & \mathrm{CP}_\Phi(\Phi) = 0 \\ \Rightarrow\ & \mathrm{MP}_\Phi(X) \mid \mathrm{CP}_\Phi(X) \\ \Rightarrow\ & \mathrm{Grad}\, \mathrm{MP}_\Phi(X) \leq n \end{aligned}}$$

Definition. Sei $\Phi \in \mathrm{End}(V), \lambda \in \mathbb{K}$.

(i) **geometrische Vielfachheit** $\mu_g(\Phi, \lambda) := \dim(\mathrm{Eig}(\Phi, \lambda))$

(ii) **algebraische Vielfachheit** $\mu_a(\Phi, \lambda) :=$ "Exponent von $(X - \lambda)$ im charakteristischen Polynom"

Satz. Sei $\lambda \in \mathrm{Spec}(\Phi)$. Dann gilt:

$$1 \leq \mu_g(\Phi, \lambda) \leq \mu_a(\Phi, \lambda)$$

Aufgabe 3. Bestimmen Sie das Minimalpolynom von $A := \begin{pmatrix} 1 & 0 & 0 \\ 1 & 4 & -1 \\ 2 & 3 & 0 \end{pmatrix} \in \mathbb{R}^{3x3}$.

Lösung.

$$\mathrm{CP}_A(X) = \det(X \cdot I_n - A) = \det(\begin{pmatrix} X-1 & 0 & 0 \\ -1 & X-4 & 1 \\ -2 & -3 & X \end{pmatrix}) = (X-1)((X-4)X+3) = (X-1)^2(X-3$$

Wir berechnen $(A-1)(A-3)$, erhalten *nicht* die Nullmatrix, also gilt auch:

$$\mathrm{MP}_A(X) = (X-1)^2(X-3)$$

denn einerseits teilt das Minimalpolynom das charakteristische, und andererseits sind die Nullstellen von Minimalpolynom und charakterischem Polynom ja gleich (nur die Vielfachheit potentiell anders), deshalb mussten wir nur einen Teiler testen.

Satz. $\Phi \in \mathrm{End}(V)$ ist genau dann diagonalisierbar, wenn

(i) das charakteristische Polynom in Linearfaktoren zerfällt

(ii) $\mu_g(\Phi, \lambda) = \mu_a(\Phi, \lambda)$ für alle Eigenwerte $\lambda \in \mathrm{Spec}(\Phi)$

Bemerkung. Die erste Bedingung kann man mit mehr Algebra immer hintricksen. Wir nehmen z.B. einfach $\mathbb{C}$ statt $\mathbb{R}$.

Die zweite Bedingung ist äquivalent dazu, dass jeder Eigenraum ein Φ-invariantes Komplement besitzt. Indem wir also unsere Eigenräume solange erweitern, bis das gilt, erhoffen wir uns eine ähnlich einfache Form wie im Falle der Diagonalisierbarkeit.

3 Haupträume

Definition. Sei $\Phi \in \mathrm{End}(V)$, $\lambda \in \mathbb{K}$. Dann heißt

$$H(\Phi, \lambda) := \bigcup_{k=0}^{\infty} \mathrm{Kern}((\Phi - \lambda \cdot \mathrm{id})^k)$$

Hauptraum von Φ zu λ.

Bemerkung. Der Hauptraum $H(\Phi, \lambda)$ ist der kleinste Φ-invarianter Unterraum von V, der den Eigenraum $\mathrm{Eig}(\Phi, \lambda)$ enthält und ein Φ-invariantes Komplement hat.

Lemma. Sei $\Phi \in \mathrm{End}(V)$, λ ein EW von Φ und $e := \mu_a(\Phi, \lambda)$. Dann gelten:

(i) $\dim(H(\Phi, \lambda)) = e$

(ii) $H(\Phi, \lambda) = \mathrm{Kern}((\Phi - \lambda \cdot \mathrm{id})^e)$

(iii) $\mathrm{Bild}((\Phi - \lambda \cdot \mathrm{id})^e)$ ist ein Φ-invariantes Komplement zu $H(\Phi, \lambda)$

Lemma. Sei $\Phi \in \mathrm{End}(V)$ und $\lambda_1, \ldots, \lambda_k$ paarweise verschieden. Dann ist die Summe

$$\sum_{i=1}^{k} H(\Phi, \lambda_i) \quad = \quad \bigoplus_{i=1}^{k} H(\Phi, \lambda_i)$$

direkt.

Lemma. Sei $\Phi \in \mathrm{End}(V)$. Dann sind die folgenden Aussagen äquivalent:

(i) $V = \bigoplus_{\lambda} H(\Phi, \lambda)$

(ii) $\mathrm{CP}_\Phi(X) = \prod_{\lambda} (X - \lambda)^{\dim H(\Phi, \lambda))}$

(iii) $CP_\Phi(X)$ lässt sich als Produkt von Linearfaktoren schreiben

(iv) $MP_\Phi(X)$ lässt sich als Produkt von Linearfaktoren schreiben

Aufgabe 4. Seien Φ, $\Psi \in \mathrm{End}(V)$ zwei kommutierende Endomorphismen, und λ ein Eigenwert von Φ. Zeigen Sie, dass der zugehörige Hauptraum $H(\Phi, \lambda)$ ein Ψ-invarianter Unterraum von V ist.

Beweis. Es gilt

$$
\begin{aligned}
& x \in H(\Phi, \lambda) \\
\Rightarrow\ & x \in Kern((\Phi - \lambda \cdot \mathrm{id})^k) \qquad (k \in \mathbb{N}) \\
\Rightarrow\ & ((\Phi - \lambda \cdot \mathrm{id})^k)(x) = 0 \\
\Rightarrow\ & ((\Phi - \lambda \cdot \mathrm{id})^k)(\Psi(x)) = ((\Phi - \lambda \cdot \mathrm{id})^k \circ \Psi)(x) \overset{!}{=} (\Psi \circ (\Phi - \lambda \cdot \mathrm{id})^k)(x) = \Psi(((\Phi - \lambda \cdot \mathrm{id})^k)(x)) = \Psi(\\
\Rightarrow\ & \Psi(x) \in Kern((\Phi - \lambda \cdot \mathrm{id})^k) \\
\Rightarrow\ & \Psi(x) \in H(\Phi, \lambda)
\end{aligned}
$$

wegen

$$
\begin{aligned}
& (\Phi - \lambda \cdot \mathrm{id}) \circ \Psi \\
= & (\Phi \circ \Psi - \lambda \cdot \mathrm{id} \circ \Psi) \\
= & (\Psi \circ \Phi - \Psi \circ \lambda \cdot \mathrm{id}) \\
= & \Psi \circ (\Phi - \lambda \cdot \mathrm{id})
\end{aligned}
$$

nach Voraussetzung und wegen der Linearität von Φ und Ψ. $\square$