Seminar: Computeralgebra 1

Thema 7 :

Berechnung des Minimalplolynoms zu einem Endomorphismus

Die Algorithmen Ordpoly und Minpoly

Hannes Buchholzer

Generalvoraussetzungen:

Seien K ein Körper, R ein euklidischer Ring, V ein K-Vektorraum mit $dimV = n(n \in \mathbb{N})$, $\tau \in End(V)$, und M ein endlich erzeugter Modul über R.

Gliederung:

1. Wiederholung

2. Der Algorithmus Ordpoly

3. Der Algorithmus Minpoly

1 Wiederholung

1. Der Polynomring $K[X]$ ist ein euklidischer Ring, insbesondere ein Hauptidealring (HIR).

2. Das Annulatorideal von M ist $A(M) := \{r \in R \mid rm = 0 \, \forall m \in M\}$.

3. Das Ordnungsideal von $m \in M$ ist $O(m) := \{r \in R \mid r \cdot m = 0\}$. $O(m)$ ist ein Ideal.

4. Ein Element $m \in M$ heißt Torsionselement, wenn $O(m) \supsetneq \{0\}$. Ist jedes $m \in M$ Torsionselement, so heißt M Torsionsmodul.

1 Wiederholung

Definition 1 ($K[X]$-Modul V_τ)
Sei $f \in K[X]$ und $v \in V$. Durch die Definition $f \cdot v := (f(\tau))(v)$ wird V zu einem $K[X]$-Modul, bezeichnet mit V_τ.

Bemerkung 1
1. Für Elemente $k \in K \subset K[X]$ folgt aus diese Definition: $k \cdot v = k \cdot \tau^0(v) = k \star v$, wobei $\star$ die Skalarmultiplikation im K-Vektorraum V bezeichnet.
2. Der Modul V_τ ist endlich erzeugt.
3. Außerdem ist V_τ ein Torsionsmodul.

2. Der Algorithmus Ordpoly

- Definition des Ordnungspolynoms

- Beispiel zur Berechnung des Ordnungspolynoms

- Ordnungspolynom in einem Faktorraum V/U

- Algorithmus Ordpoly

Definition des Ordnungspolynoms

Definition 2 (Ordnungspolynom)
Sei $v \in V$. Das Polynom $o \in K[X]$ heißt Ordnungspolynom von v, wenn gilt:
o ist normiert und $(o) = K[X]o = O(v)$

Bemerkung 2
1. Das Ordnungspolynom ist eindeutig bestimmt, weil $K[X]$ ein H.I.R. ist und weil es normiert ist.

2. Allgemein gilt: Jedes Ideal $I \subset K[X]$ wird von allen Polynomen des kleinsten Grades in I erzeugt.

Beispiel zur Berechnung des Ordnungs-polynoms

Beispiel 1

Hier ist $K = \mathbb{Z}_5$, $V = (\mathbb{Z}_5)^3$ und $End(V) = Mat(3 \times 3, \mathbb{Z}_5)$.

Sei $\tau = A \in Mat(3 \times 3, \mathbb{Z}_5)$, $A := \begin{pmatrix} 3 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 1 & 2 \end{pmatrix}$ und $v \in (\mathbb{Z}_5)^3$, $v := \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$.

Berechne: $Av = \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix}$, $A^2v = \begin{pmatrix} 4 \\ 0 \\ 2 \end{pmatrix}$, $A^3v = \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}$.

Bestimmes s minimal, so daß $v, Av, \ldots, A^sv$ linear abhängig sind. Hier $s = 3$.

$A^3v = v + 4Av + A^2v \quad \Longrightarrow \quad A^3v + 4A^2v + Av + 4v = 0$

$\Longrightarrow \left(A^3 + 4A^2 + A + 4E\right) v = 0 \quad \Longrightarrow \quad (X^3 + 4X^2 + X + 4)v = 0.$

Dann ist $o := X^3 + 4X^2 + X + 4$ das Ordnungspolynom von v.

Ordnungspolynom in V/U

Dies erfordert den Übergang zum $K[X]$-Faktormodul V_τ/U_τ:

1. Die Untermoduln von V_τ sind gerade diejenigen Unterräume U von V die $\tau(U) \subset U$ (d.h. U ist τ-invariant) erfüllen , hier bezeichnet mit U_τ.

2. Der Endomorphismus τ muss nun verändert werden: Setze
$$\overline{\tau} \; : \; V_\tau/U_\tau \longrightarrow V_\tau/U_\tau \quad ; \overline{\tau}(\overline{v}) = \overline{\tau(v)}$$
Dies ist die kanonische Definition.

3. Die Addition ist gegeben durch $\overline{v} + \overline{w} = \overline{v+w} \quad \forall\, v, w \in V_\tau$. Und die Multiplikation ist gegeben durch $p \cdot \overline{v} = p(\overline{\tau})(\overline{v}) = \overline{p(\tau)(v)} \quad \forall p \in K[X] \; \forall v \in V$.
$\Rightarrow$ Man rechnet ganz in V_τ und macht erst zum Schluss der Rechnung den Übergang modulo U_τ.

Algorithmus Ordpoly

Sei $\overline{v} \in V_\tau / U_\tau$, und U τ-invariant. Weiter sei $b_0, \ldots\ b_k$ eine Basis von U_τ.
Setzte $i := 0$
Wiederhole solange die Vektoren $b_0, \ldots, b_k, v, \tau(v), \ldots, \tau^i(v)$ linear unabhängig sind (dies wird mit der Funktion gauss getestet) : setzte $i := i + 1$.
Setze $m := i$.
Die Funktion gauss liefert dann einen Vektor f, so daß gilt :

$$\tau^m(v) = f_0 b_0 + \cdots + f_k b_k + f_{k+1} v + \cdots + f_{k+m} \tau^{m-1}(v)$$

Setze $w := (f_0, \ldots, f_k)$ (Anteil in U_τ)
Setze $f := (f_{k+1}, \ldots, f_{k+m})$ (Anteil im direkten Komplement von U_τ).
Dann gilt: $\tau^m(v) - f_{m-1}\tau^{m-1}(v) - \cdots - f_0 v = w_0 b_0 + \cdots + w_k b_k$.
modulo U_τ: $\overline{\tau}^m(\overline{v}) - f_{m-1}\overline{\tau}^{m-1}(\overline{v}) - \cdots - f_0 \overline{v} = \overline{0}$
Setze $o := X^m - f_{m-1}X^{m-1} - \cdots - f_1 X - f_0$.
Dann ist o das Ordnungspolynom.

3. Der Algorithmus Minpoly

- Definition des Minimalpolynoms
- Beispiel zur Berechnung eines Minimalpolynoms
- Theoretische Bestimmung des Minimalpolynoms
- Bestimmung eines maximalen Vektors
- Algorithmus Minpoly

Definition des Minimalpolynoms

<u>Definition</u> 3 (Minimalpolynom)
Sei $\tau \in End(V)$. Das Polynom $m \in K[X]$ heißt Minimalpolynom von τ , wenn gilt: m ist normiert und $(m) = K[X]m = A(V_\tau) = \{p \in K[X] \mid p \cdot v = 0 \quad \forall v \in V_\tau\}$

Beispiel zur Berechnung eines Minimalpolynoms

Beispiel 2
Hier ist $K = \mathbb{Z}_5$, $V = (\mathbb{Z}_5)^4$ und $End(V) = Mat(4 \times 4, \mathbb{Z}_5)$.

Gegeben: Basis von V : $v_0 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $v_1 = \begin{pmatrix} 2 \\ 2 \\ 4 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 3 \\ 3 \\ 2 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

ein Endomorphismus $A = \tau \in Mat(4 \times 4, \mathbb{Z}_5)$, $A := \begin{pmatrix} 3 & 4 & 2 & 4 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

und die Ordnungspolynome zu den Basisvektoren:

$o_0 = X^2 + X + 3 = (X+2)(X+4)$ $\qquad$ $o_1 = X^2 + 1 = (X+2)(X+3)$

$o_2 = X^3 + 2X + 2 = (X+2)(X+4)^2$ $\qquad$ $o_3 = X + 2$

Beispiel (Fortsetzung)

Schritt 0: Setze: $m = o_0$ und $v = v_0$.

Schritt 1: Setze: $c := m = (X+2)(X+4) = X^2 + X + 3$
$d := o_1 = (X+2)(X+3) = X^2 + 1$

Berechne:

$$\begin{aligned}
t &:= \mathrm{ggT}(c,d) = X+2 \\
C &:= \mathrm{r}(c, \frac{d}{t}) = \mathrm{r}(c\,,\ (X+3)\,) = (X+2)(X+4) = X^2+X+3 \\
D &:= \mathrm{r}(d, \frac{c}{t}) = \mathrm{r}(d\,,\ (X+4)\,) = (X+2)(X+3) = X^2+1 \\
T &:= \mathrm{ggT}(C,D) = X+2 \\
D_2 &:= \frac{D}{T} = X+3 \\
m &:= CD_2 = (X+2)(X+3)(X+4) = X^3+4X^2+X+4 \\
v &:= \frac{c}{C}\cdot v + \frac{d}{D_2}\cdot v_1 = 1\cdot\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + (X+2)\begin{pmatrix}2\\2\\4\\1\end{pmatrix} = \begin{pmatrix}0\\4\\1\\4\end{pmatrix}
\end{aligned}$$

Beispiel (Fortsetzung)

Schritt 2: Setze: $c := m = (X+2)(X+3)(X+4) = X^3 + 4X^2 + X + 4$
$d := o_2 = (X+2)(X+4)^2 = X^3 + 2X + 2$

Berechne:

$$
\begin{aligned}
t &:= \mathrm{ggT}(c,d) = (X+2)(X+4) = X^2 + X + 3 \\
C &:= \mathrm{r}(c, \frac{d}{t}) = \mathrm{r}(\,c,\ (X+4)\,) = (X+2)(X+3) = X^2 + 1 \\
D &:= \mathrm{r}(d, \frac{c}{t}) = \mathrm{r}(\,d,\ (X+3)\,) = (X+2)(X+4)^2 = X^3 + 2X + 2 \\
T &:= \mathrm{ggT}(C,D) = X + 2 \\
D_2 &:= \frac{D}{T} = (X+4)^2 = X^2 + 3X + 1 \\
m &:= CD_2 = (X+2)(X+3)(X+4)^2 = X^4 + 3X^3 + 2X^2 + 3X + 1 \\
v &:= \frac{c}{C} \cdot v + \frac{d}{D_2} \cdot v_2 = (X+4)\begin{pmatrix} 0 \\ 4 \\ 1 \\ 4 \end{pmatrix} + (X+2)\begin{pmatrix} 3 \\ 3 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 2 \\ 4 \end{pmatrix}
\end{aligned}
$$

Hier Abbruch der Berechnungen, denn das Minimalpolynom m kann nach der Theorie nicht mehr größer werden.

Bestimmung des Minimalpolynoms

1. Schritt:

Es sei $m \in K[X]$ das Minimalpolynom von τ. Dann gilt

$$K[X]m = A(V_\tau) = \bigcap_{v \in V} O(v) \tag{1}$$

nach Definition.

Bestimmung des Minimalpolynoms

2. Schritt:

Sei $E = (e_0, e_1, \ldots, e_k)$ ein endliches Erzeugendensystem von V_τ. Wegen dem Satz 1 , reicht es den Schnitt in (1) nur über das Erzeugendensystem E zu bilden:

$$K[X]m = \bigcap_{i=0}^{k} O(e_i)$$

<u>Satz</u> 1

Sei $e_0, e_1, \ldots, e_k$ ein Erzeugendensystem von dem R-Modul M. Dann gilt :

$$A(M) = \bigcap_{i=0}^{k} O(e_i)$$

Bestimmung des Minimalpolynoms

3. Schritt:

Sei $o_i \in K[X]$ das Ordnungspolynom von e_i für $i = 0, \ldots, k$ d.h. $K[X]o_i = O(e_i) \quad (i = 0, \ldots, k)$. Dann gilt nach Satz 2 :

$$K[X]m = \bigcap_{i=0}^{k} K[X]o_i = K[X] \cdot \mathrm{kgV}(o_0, \ldots, o_k)$$

$\Longrightarrow \quad m \in \mathrm{kgV}(o_0, \ldots, o_k)$

Satz 2

Seien $b_0, \ldots, b_m \in R$. Dann gilt:

$$\bigcap_{i=0}^{m} Rb_i = R \cdot \mathrm{kgV}(b_0, \ldots, b_m)$$

Bestimmung des Minimalpolynoms

<u>**Bemerkung**</u> **3**

Seien $r_0, \ldots, r_m, r, s \in R$. Dann gilt:

$$\begin{aligned} \mathrm{kgV}(r_0, \ldots, r_m) &= \mathrm{kgV}(r_0, \mathrm{kgV}(r_1, \ldots, r_m)) \\ \mathrm{kgV}(r, s) &= \frac{rs}{\mathrm{ggT}(r, s)} \end{aligned}$$

Bestimmung eines maximalen Vektors

Satz 3
Seien $c, d \in R$. Setzte: $t := \text{ggT}(c,d)$, $C := r(c, \frac{d}{t})$ und $D := r(d, \frac{c}{t})$. Dann gilt:

$$\text{kgV}(c,d) = \text{kgV}(C,D)$$

Beispiel 3
Seien $c = 2^3 3^2 5^4$, $d = 2^3 3 7^2 \in \mathbb{Z}$. Dann ist: $t = \text{ggT}(c,d) = 2^3 3 \Rightarrow \frac{c}{t} = 3 5^4$, $\frac{d}{t} = 7^2$. Weiter ist: $C = r(c, \frac{d}{t}) = r(2^3 3^2 5^4, 7^2) = 2^3 3^2 5^4$ $\quad D = r(d, \frac{c}{t}) = r(2^3 3 7^2, 3 5^4) = 2^3 7^2$ und $T = \text{ggT}(C,D) = 2^3$

$\Rightarrow \text{kgV}(C,D) = \frac{CD}{T} = 2^3 3^2 5^4 7^2$.

Bestimmung eines maximalen Vektors

Satz 4

Seien $v_0, v_1 \in M$ Torsionselemente. Ferner sei $O(v_0) = Rc$ und $O(v_1) = Rd$. Setze: $C := r(c, \frac{d}{\text{ggT}(c,d)})$, $D := r(d, \frac{c}{\text{ggT}(c,d)})$ und $D_2 := \frac{D}{\text{ggT}(C,D)}$. Setze ferner $v := \frac{c}{C} v_0 + \frac{d}{D_2} v_1$. Dann gilt:

$$O(v) = O(v_0) \cap O(v_1) = Rc \cap Rd = R \cdot \text{kgV}(c, d)$$

Algorithmus Minpoly

Sei $v_0, v_1, \ldots, v_{n-1}$ eine Basis von V. Dann ist $\overline{v_0}, \overline{v_1}, \ldots, \overline{v_{n-1}}$ ein Erzeugendensystem von V_τ / U_τ (auch $U_\tau = \{0\}$ möglich).Bestimme Minimalpolynom von $\overline{\tau}$.

Vorarbeit: Berechne Ordnungspolynom von $\overline{v_i}$ und speichere es in $ordpol[i]$ für $i = 0, \ldots, n-1$.

Schritt 0: Setze $\overline{v}$ und m wie folgt:

$$\begin{aligned} \overline{v} &:= \overline{v_0} \\ m &:= ordpol[0] \end{aligned}$$

Algorithmus Minpoly

Schritt i: (Für $i = 1, \ldots, n-1$)
Setze: $c := m$ und $d := ordpol[i]$
, wobei $m = \text{kgV}(ordpol[0], \ldots, ordpol[i-1])$
Berechne Hilfsvariblen: $t := \text{ggT}(c, d)$, $C := r(c, \frac{d}{t})$, $D := r(d, \frac{c}{t})$, $T := \text{ggT}(C, D)$ und $D_2 := \frac{D}{T}$.
Berechne neues m und neues $\overline{v}$:

$$\begin{array}{rll} m := & C \cdot D_2 & (\text{ d.h. } m := \text{kgV}(m, orpol[i]) \text{)} \\ \overline{v} := & \frac{c}{C}\overline{v} + \frac{d}{D_2}\overline{v_i} & (\text{ d.h. } O(\overline{v}) = K[X]m \text{)} \end{array}$$

Falls $grad(m) = dimV - dimU$ verlasse Schleife vorzeitig.

Nacharbeit: Normiere m.

Algorithmus Minpoly

Ergebnis:

Es ist $m = \text{kgV}(\,ordpol[0], \ldots, ordpol[n{-}1]\,)$ Also ist $K[X]m = \bigcap_{i=0}^{n-1} K[X]ordpol[i] = \bigcap_{i=0}^{n} O(\overline{v_i}) = A(V_\tau/U_\tau)$ nach den Sätzen 1 und 2 . Damit ist m das Minimalpolynom von $\overline{\tau}$ nach der Definition 1.

Es ist $O(\overline{v}) = \bigcap_{i=0}^{n-1} O(\overline{v_i}) = K[X]m$ nach Satz 4. Also hat $\overline{v}$ das Polynom m als Ordnungspolynom.