Seminar: Computeralgebra 1

Thema 7 : Algorithmus Minpoly und Ordpoly
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 eindlich erzeugter Modul über R.

1 Wiederholung

1. Der Polynomring $K[X]$ ist ein euklidischer Ring, insbesondere ein Hauptidealring (HIR).
2. Das Annihilatorideal 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 $O(m) \supsetneqq \{0\}$. Ist jedes $m \in M$ Torsionselement, so heißt M Torsionsmodul.

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

2.1 Definition des Ordnungspolynoms und Beispiel

Definition 2
Sei $v \in V$ und $o \in K[X]$ normiert mit $(o) = K[X]o = O(v)$. Dann heißt o Ordnungspolynom von 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. Diese sind alle assoziiert, d.h. sie unterscheiden sich nur durch Einheiten und es gibt darunter nur ein normiertes Polynom.

Beispiel 1

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

Dann ist : $Av = \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix}$, $A^2v = \begin{pmatrix} 4 \\ 0 \\ 2 \end{pmatrix}$ und $A^3v = \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}$. Jetzt bestimme durch sukzessiven Test s minimal, so daß $v, Av, \ldots, A^sv$ linear abhängig sind. Hier ist $s = 3$, denn v, Av, A^2v sind noch linear unabhängig. Also ist v, Av, A^2v eine Basis von $(\mathbb{Z}_5)^3$ und A^3v läßt sich in dieser Basis darstellen. Es ist: $A^3v = v + 4Av + A^2v \Rightarrow A^3v - A^2v - 4Av - v = 0 \Rightarrow (A^3 + 4A^2 + 1A + 4E) \cdot v = 0$. Deswegen annuliert das Polynom $o = X^3 + 4X^2 + X + 4$ den Vektor v. Dies ist gleichzeitig das Ordnungspolynom, denn der Grad ist wegen der Minimalität von s minimal. Außerdem ist o normiert.

2.2 Ordnungspolynom in einem Faktorraum V/U

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

1. Dies Untermoduln von V_τ sind gerade diejenigen Unterräume U von V die $\tau(U) \subset U$ 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. (Ganz genauso wie man in $\mathbb{Z}_5$ rechnet).

2.3 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 $o := X^m - f_{m-1}X^{m-1} - \cdots - f_1 X - f_0$.
Dies ist dann das Ordnungspolynom, denn es hat den kleinstmöglichen Grad und ist normiert.

3 Der Algorithmus Minpoly

3.1 Definition des Minimalpolynoms und Beispiel

Definition 3 (Minimalpolynom)
Das normierte Polynom $m \in K[X]$ für das gilt: $K[X]m = A(V_\tau) = \{p \in K[X] \mid p \cdot v = 0 \quad v \in V_\tau\}$ heißt Minimalpolynom von $\tau \in End(v)$.

Beispiel 2 (für den Algorithmus Minpoly)
Gegeben sei eine Basis von dem $\mathbb{Z}_5$-Vekorraum $V = (\mathbb{Z}_5)^4$: $v_0 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $v_1 = \begin{pmatrix} 2 \\ 2 \\ 4 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 3 \\ 3 \\ 2 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}$„ ein Endomorphismus von $A = \tau \in End(V)$: $A = \begin{pmatrix} 3 & 4 & 2 & 4 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ und schließlich noch die Ordnungspolynome zu den Basisvektoren:

$$\begin{array}{ll} o_0 = X^3 + X + 3 = (X+2)(X+4) & o_1 = X^2 + 1 = (X+2)(X+3) \\ o_2 = X^3 + 2X + 2 = (x+2)(X+4)^2 & o_3 = X + 2 \end{array} .$$

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

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

Berechne:

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

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

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

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

3.2 Bestimmung des Minimalpolynoms

Ziel: Bestimmung des Minimalpolynoms von τ aus einer möglichst geringen Anzahl von Ordnungspolynomen.

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.

2. Schritt:

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

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

Satz 1
Sei $e_0, e_1, \ldots, e_k$ ein Erzeugendensystem von dem R-Modul M. Dann gilt :

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

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 einem Resultat aus der Algebra:

$$K[X]m = K[X]s \quad \forall s \in \mathrm{kgV}(o_0, \ldots, o_k)$$

Satz 2
Seien $b_0, \ldots, b_m \in R$. Dann gilt:

$$\bigcap_{i=0}^{m} Rb_i = Rv \qquad \forall\, v \in \mathrm{kgV}(b_0, \ldots, b_m)$$

Bemerkung 3
Seien $r_0, \ldots, r_m, r, s \in R$. Dann gilt:

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

3.3 Bestimmung eines Vektors mit maximalem Ordnungspolynom

Ziel: Bestimmung eines Vektors $v \in V$ der das Minimalpolynom als Ordnungspolynom hat.

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

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

Beispiel 3
Seien $c = 2^3 3^2 5^4$, $d = 2^3 3 7^2 \in \mathbb{Z}$. Dann ist: $t = \mathrm{ggT}(c,d) = 2^3 3 \Rightarrow \frac{c}{t} = 35^4$, $\frac{d}{t} = 7^2$. Weiter ist: $C = r(c, \frac{d}{t}) = r(2^3 3^2 5^4, 7^2) = 2^3 3^2 5^4$ $D = r(d, \frac{c}{t}) = r(2^3 3 7^2, 35^4) = 2^3 7^2$ und $T = \mathrm{ggT}(C,D) = 2^3 \Rightarrow \mathrm{kgV}(C,D) = \frac{CD}{T} = 2^3 3^2 5^4 7^2$.

Satz 4
Seien $v_0, v_1 \in M$ Torsionselemente. Ferner sei $O(v_0) = Rc$ und $O(v_1) = Rd$. Setze: $C := r(c, \frac{d}{\mathrm{ggT}(c,d)})$, $D := r(d, \frac{c}{\mathrm{ggT}(c,d)})$ und $D_2 := \frac{D}{\mathrm{ggT}(C,D)}$. Setze ferner $v := \frac{c}{C} v_0 + \frac{d}{D_2} v_1$. Dann gilt:

$$O(v) = O(v_0) \cap O(v_1) = Ra \quad \forall a \in \mathrm{kgV}(C, D_2)$$

3.4 Algorithmus Minpoly

Sei $v_0, v_1, \ldots, v_n$ eine Basis von V. Dann ist $\overline{v}_0, \overline{v}_1, \ldots, \overline{v}_n$ eine Basis von V_τ / U_τ (auch $U_\tau = \{0\}$ möglich).

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

Schritt 0: Setze v und m wie folgt:

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

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

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

Falls $grad(m) = n$ verlasse Schleife vorzeitig.

Nacharbeit: Normiere m.

Ergebnis:

1. Es ist $m = \mathrm{kgV}(\,ordpol[0], \ldots, ordpol[n-q]\,)$ Also ist $K[X]m = \bigcap_{i=0}^{n} O(v_i) = A(V_\tau)$ nach den Sätzen 1 und 2 . Damit ist m das Minimalpolynom von τ nach der Definition 1.
2. Es ist $O(v) = \bigcap_{i=0}^{n} O(v_i) = K[X]m$ nach Satz 4. Also hat v das Polynom m als Ordnungspolynom.