

## Symbolisch/numerisches Lösen von Gleichungssystemen

Zusammenfassung der Woche 8.12. - 12.12.

Die Gröbnerbasis von  $\langle f_2, \dots, f_r \rangle : f_1$  enthält nach Satz 3.12 nur Polynome, die nicht von  $x_1$  abhängen! Fügt man  $f_1$  hinzu, dessen Leitterm nur von  $x_1$  abhängt, so ist  $\{f_1, \text{lp}(f_2), \dots, \text{lp}(f_r)\}$  eine Gröbnerbasis bzgl.  $<_{LEX}$  von

$$\mathcal{B} := \langle f_1 \rangle + \langle f_2, \dots, f_r \rangle : f_1,$$

denn die S-Polynome  $S(f, \text{lp}(f_i))$  reduzieren auf 0 wegen des Kriteriums T.

Will man die Varietät eines nulldimensionalen Ideals  $\mathcal{A}$  berechnen und hat man eine Gröbnerbasis von  $\mathcal{A}$  bzgl.  $<_{LEX}$ , dann gibt es nach Satz 3.9 ein  $f_1$  in der Gröbnerbasis, dessen Leitterm  $\text{lt}(f_1)$  eine reine Potenz in  $x_1$  ist, also  $\text{lp}(f_1) = \text{const}$ . Mit den Notationen von Satz 3.12 kann man also eine Gröbnerbasis von  $\mathcal{B} := \langle f_1 \rangle + \langle f_2, \dots, f_r \rangle : f_1$  ablesen. Es gilt

$$\mathcal{A} = \langle f_1 \rangle + \langle f_2, \dots, f_r \rangle \subseteq \langle f_1 \rangle + \langle f_2, \dots, f_r \rangle : f_1 = \mathcal{B}.$$

Also  $V(\mathcal{B}) \subseteq V(\mathcal{A})$ .

Die Varietät  $V(\mathcal{B})$  kann man einfach berechnen, wenn man die gemeinsamen Nullstellen  $\tilde{y}_i = (\tilde{y}_{i2}, \dots, \tilde{y}_{in}) \in \mathbb{C}^{n-1}$  von Polynomen in  $n-1$  Variablen, hier von  $\text{lp}(f_2), \dots, \text{lp}(f_r)$ , berechnen kann. Die fehlende Komponente  $x_1$  der Punkte aus  $V(\mathcal{B})$  bekommt man aus den Nullstellen von  $f_1(x_1, \tilde{y}_{i2}, \dots, \tilde{y}_{in})$ .

Es gilt wegen  $\mathcal{B} = \langle f_1, \text{lp}(f_2), \dots, \text{lp}(f_r) \rangle$  und wegen  $y \in V(\mathcal{A}) \Rightarrow f_1(y) = 0$

$$(1) \quad \begin{aligned} V(\mathcal{A}) \setminus V(\mathcal{B}) = & \{y \in V(\mathcal{A}) \mid \text{lp}(f_2) \neq 0\} \\ & \cup \{y \in V(\mathcal{A}) \mid \text{lp}(f_2) = 0, \text{lp}(f_3) \neq 0\} \\ & \dots \\ & \cup \{y \in V(\mathcal{A}) \mid \text{lp}(f_2) = \dots = \text{lp}(f_{r-1}) = 0, \text{lp}(f_r) \neq 0\}. \end{aligned}$$

**Bemerkung.** Ist  $\mathcal{A}_i$  ein beliebiges nulldimensionales Ideal und  $f$  ein Polynom, dann wird mit  $\mathcal{A}_i : f^*$  die *Saturation* von  $\mathcal{A}_i : f$  bezeichnet. Es ist das Ideal  $\bigcup_{k=1}^{\infty} \mathcal{A}_i : f^k = \mathcal{A}_i : f^s$  für genügend großes  $s \in \mathbb{N}$ . Es gilt (Übungsaufgabe)

$$V(\mathcal{A}_i : f^*) = \{y \in \mathcal{A}_i \mid f(y) \neq 0\}.$$

Mit  $\mathcal{A}_i := \mathcal{A} + \langle \text{lp}(f_2), \dots, \text{lp}(f_i) \rangle$  hat man daher

$$(2) \quad \begin{aligned} V(\mathcal{A}) \setminus V(\mathcal{B}) \\ = V(\mathcal{A} : \text{lp}(f_2)^*) \cup V(\mathcal{A}_2 : \text{lp}(f_3)^*) \cup \dots \cup V(\mathcal{A}_{r-1} : \text{lp}(f_r)^*). \end{aligned}$$

Hat man eine Basis  $\{a_1, \dots, a_m\}$  des Ideals  $\mathcal{A}_i$ , dann kann man eine Basis der Saturation  $\mathcal{A}_i : f^*$  berechnen, indem man für das Ideal  $\langle a_1, \dots, a_m, 1 - t \cdot f \rangle \subset \mathbb{C}[x_1, \dots, x_n, t]$  eine Gröbnerbasis bzgl. einer Eliminationsordnung für  $T' = [x_1, \dots, x_n]$  berechnet (Definition 3.12). Die Polynome in der Gröbnerbasis, die nur von  $x_1, \dots, x_n$  abhängen, bilden eine Gröbnerbasis von  $\mathcal{A}_i : f^*$ . Hier geht es auch einfacher, denn die betrachteten Ideale  $\mathcal{A}_i$  sind nulldimensional. Wegen  $\mathcal{A}_i \subseteq \mathcal{A}_i : f$  enthält  $\mathcal{A}_i : f$  mehr Polynome. Die findet man, indem man die Normalmenge  $\mathcal{N}_i$  von  $\mathcal{A}_i$  berechnet und dann lineare Abhängigkeiten unter den  $\text{NF}(t_k \cdot f, \mathcal{A}_i)$ ,  $t_k \in \mathcal{N}_i$ , sucht, denn es gilt

$$\sum_{t_k \in \mathcal{N}_i} \lambda_k \text{NF}(t_k f, \mathcal{A}_i) = 0 \Rightarrow \sum_{t_k \in \mathcal{N}_i} \lambda_k t_k \in \mathcal{A}_i : f.$$

Man erhält so eine Basis von  $\mathcal{A}'_i := \mathcal{A}_i : f$ . Dann verfährt man analog mit  $\mathcal{A}'_i$  und bekommt eine Basis von  $\mathcal{A}''_i : f = \mathcal{A} : f^2$  usw. Man bricht ab, sobald für ein  $s$  gilt  $\mathcal{A}_i : f^s = \mathcal{A}_i : f^{s+1}$ , denn dann folgt  $\mathcal{A}_i : f^s = \mathcal{A}_i : f^k$  für alle  $k > s$ .

**Definition 3.13** (Dreiecksbasen)

Man nennt eine Polynommenge  $\{f_1, \dots, f_r\}$  eine *Dreiecksbasis*, wenn  $r = n$  gilt und wenn  $\{f_1, \dots, f_n\}$  eine Gröbnerbasis bzgl. einer lexikographischen Ordnung für ein nulldimensionales Ideal ist.

Wegen Satz 3.9 hat dann (evtl. nach Ummummerierung) jedes  $f_i$  als Leitterm ein  $x_i^{m_i}$  für ein  $m_i \in \mathbb{N}$ . Wegen der lexikographischen Ordnung gilt dann ( $x_n <_{LEX} x_{n-1} <_{LEX} \dots <_{LEX} x_1$  angenommen)

$$f_i \in \mathbb{C}[x_i, x_{i+1}, \dots, x_n], \quad i = 1, \dots, n.$$

Hat man ein Ideal mit Dreiecksbasis  $\{f_1, \dots, f_n\}$ , dann kann man seine Varietät dadurch berechnen, dass man der Reihe nach Nullstellen von Polynomen einer Veränderlicher berechnet. Die  $n$ -ten Komponenten der Punkte aus  $V(\langle f_1, \dots, f_n \rangle)$  sind die Nullstellen von  $f_n$ . Es seien  $\tilde{x}_i$ ,  $i = 1, \dots, m_n$ . Jedes  $\tilde{x}_i$  gehört zu einem Punkt (oder mehreren Punkten) der Varietät. Deren  $n-1$ -te Komponente bekommt man als Nullstelle von  $f_{n-1}(x_{n-1}, \tilde{x}_i)$  usw.

**Definition 3.14** (Zerlegung in Dreiecksbasen)

Ist  $\mathcal{A}$  ein nulldimensionales Ideal und gilt

$$V(\mathcal{A}) = V(\mathcal{A}_1) \cup V(\mathcal{A}_2) \cup \dots \cup V(\mathcal{A}_m)$$

wobei jedes  $\mathcal{A}_i$  eine Dreiecksbasis als Basis besitzt, dann nennt man diese Zerlegung von  $V(\mathcal{A})$  *Zerlegung in Dreiecksbasen*. (Eigentlich: Zerlegung in Varietäten von Idealen, die eine Dreiecksbasis als Basis besitzen.)

Die Zerlegung von  $V(\mathcal{A})$  in  $V(\mathcal{B})$  und in  $V(\mathcal{A}) \setminus V(\mathcal{B})$  nach (2) ist Ausgangspunkt für eine Zerlegung in Dreiecksbasen, die in einigen Computeralgebrasystemen (Singular, REDUCE, ...) verwendet wird. Man geht dabei rekursiv nach der Anzahl der Variablen vor.

Bevor man  $V(\mathcal{A})$  in Dreiecksbasen zerlegen kann, müssen erst die Dreiecksbasenzerlegungen der  $V(\mathcal{A}_i : \mathbf{lp}(f_{i+1})^*)$  aus (2) gefunden werden mit  $\mathcal{A}_1 := \mathcal{A}$  und  $\mathcal{A}_{i+1} := \mathcal{A}_i + \langle \mathbf{lp}(f_{i+1}) \rangle$ . Nach (1) ist die Zerlegung von  $V(\mathcal{A})$  disjunkt.  $V(\mathcal{B})$  ist nicht leer, weil  $\mathcal{B} \neq \langle 1 \rangle$  gilt. Einige der  $V(\mathcal{A}_i : \mathbf{lp}(f_{i+1})^*)$  können leer sein. Die übrigen sind, weil in  $V(\mathcal{A}) \setminus V(\mathcal{B}) \neq V(\mathcal{A})$ , echte (und disjunkte) Teilmengen von  $V(\mathcal{A})$ . Wenn  $V(\mathcal{A}_i : \mathbf{lp}(f_{i+1})^*)$  nicht leer ist, wendet man auf  $\mathcal{A}_i : \mathbf{lp}(f_{i+1})^*$  die selbe Zerlegungstechnik wie auf  $\mathcal{A}$  an, ausgehend von der minimalen Gröbnerbasis bzgl  $<_{LEX}$  von  $\mathcal{A}_i : \mathbf{lp}(f_{i+1})^*$  usw. Diese immer feineren Zerlegungen enden nach endlich vielen Schritten, weil es eine Zerlegung der endlich vielen Punkte von  $V(\mathcal{A})$  ist. Eine Zerlegung von  $V(\tilde{\mathcal{A}})$  in die entsprechenden Varietäten  $V(\tilde{\mathcal{B}})$  und die  $V(\tilde{\mathcal{A}}_i : \mathbf{lp}(\tilde{f}_{i+1})^*)$  ist genau dann nicht mehr möglich, wenn die  $V(\tilde{\mathcal{A}}_i : \mathbf{lp}(\tilde{f}_{i+1})^*)$  alle leer sind. Am Ende dieser Zerlegungsschritte hat man  $V(\mathcal{A})$  zerlegt in endlich viele Varietäten vom Typ  $V(\mathcal{B})$ , wo  $\mathcal{B}$  erzeugt wird von einem Polynom  $f_1$  mit Leiterterm  $x_1^m$  für ein  $m \in \mathbb{N}$  und Polynomen  $\mathbf{lp}(f_2), \dots, \mathbf{lp}(f_r)$ , die nur von  $x_2, \dots, x_n$  abhängen.

Die Varietäten vom Typ  $V(\mathcal{B})$  kann man nun in Dreiecksbasenvarietäten zerlegen, wenn man für jedes Ideal  $\langle \mathbf{lp}(f_2), \dots, \mathbf{lp}(f_r) \rangle$ , dessen Basis aus Polynomen in nur  $n - 1$  Variablen  $x_2, \dots, x_n$  besteht, eine Zerlegung in Dreiecksbasen,

$$V(\langle \mathbf{lp}(f_2), \dots, \mathbf{lp}(f_r) \rangle) = \bigcup_{i=1}^m V(\langle g_{i1}, \dots, g_{i,n-1} \rangle) \subset \mathbb{C}[x_2, \dots, x_n]$$

bestimmen kann. Man muss nur  $f_1$  zu jeder dieser Basen hinzufügen,

$$\begin{aligned} V(\mathcal{B}) &= V(\langle f_1 \rangle + \langle \mathbf{lp}(f_2), \dots, \mathbf{lp}(f_r) \rangle) \\ &= \bigcup_{i=1}^m V(\langle f_1, g_{i1}, \dots, g_{i,n-1} \rangle) \subset \mathbb{C}[x_1, \dots, x_n]. \end{aligned}$$

Der Rekursionsanfang ist gesichert, denn für  $n = 1$  ist jedes Ideal  $\mathcal{A}$  Hauptideal,  $\mathcal{A} = \langle f \rangle$ . Daher ist  $\{f\}$  minimale Gröbnerbasis von  $\mathcal{A}$  und zugleich Dreiecksbasis.

**Bemerkung.** Die Zerlegung einer Varietät in Teilvarietäten kann man auch beim Buchbergeralgorithmus einsetzen, wenn man nicht die Gröbnerbasis eines Ideals sucht, sondern nur die Varietät. Wenn man den Buchbergeralgorithmus mit der Eingabemenge  $\{f_1, \dots, f_r\}$  startet, dann kann man bei der Berechnung eines neuen Kandidaten  $h$  für die Gröbnerbasis,

$$S(f_i, f_j) \xrightarrow{*}_{\mathcal{F}} h \neq 0$$

(der dann als  $f_{r+1}$  in die weitere Rechnung einging) dieses  $h$  auf Faktorisierbarkeit prüfen. Gilt  $h = p \cdot q$ , dann kann man die Rechnung auf zwei verschiedenen Weisen fortsetzen. Zum einen mit  $p$  als  $f_{r+1}$ , zum anderen mit  $q$ . Man macht sich klar, dass in einem Fall der Output Gröbnerbasis ist für  $\langle f_1, \dots, f_r, p \rangle$  und im anderen Fall für  $\langle f_1, \dots, f_r, q \rangle$ . Die Vereinigung der zugehörigen Varietäten ist  $V(f_1, \dots, f_r)$ . Die Berechnung der Gröbnerbasis mit  $p$  bzw.  $q$  anstelle von  $h$  ist in der Regel bedeutend schneller, so dass es sich lohnt, (jedes  $h \neq 0$  auf Faktorisierbarkeit zu prüfen und) die Faktorisierung  $h = p \cdot q$  zu berechnen und den Buchbergeralgorithmus mit jedem der beiden Faktoren fortzusetzen. Findet man mehrere faktorisierte  $h$ 's, so verzweigt man den Buchbergeralgorithmus entsprechend häufiger. Dieser "faktorisierende" Buchbergeralgorithmus ist in verschiedenen Computeralgebrasystemen implementiert unter Namen wie `groebnerf`, `fsolve`, ...

## KAPITEL 2

### §4 Eigenwertmethoden

Wir betrachten wieder ein nulldimensionales Ideal  $\mathcal{A} \subseteq K[x_1, \dots, x_n]$  mit  $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ , und wollen das Problem, die Varietät von  $\mathcal{A}$ ,  $V(\mathcal{A}) \subseteq \mathbb{C}^n$ , zu bestimmen, in ein (numerisch lösbares) Eigenwertproblem umwandeln.

#### 4.1 Der Fall $n = 1$

Jedes Ideal  $\mathcal{A} \subset K[x]$  ist ein Hauptideal,  $\mathcal{A} = \langle \varphi \rangle$ . Sei

$$\varphi(x) = x^d + \sum_{k=0}^{d-1} a_k x^k.$$

Dann ist die Normalmenge  $\mathcal{N} = \{1, x, \dots, x^{d-1}\}$ . Rechnung gibt

$$x \begin{pmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{d-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \ddots & \ddots & \\ 0 & 0 & & 0 & 1 \\ -a_0 & -a_1 & \dots & & -a_{d-1} \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{d-1} \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \varphi(x) \end{pmatrix}.$$

Für jede Nullstelle  $y$  von  $\varphi$  gilt dann

$$y \begin{pmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^{d-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \dots & & -a_{d-1} \end{pmatrix} \begin{pmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^{d-1} \end{pmatrix},$$

d.h.,  $y$  ist Eigenwert mit zugehörigem Eigenvektor

$$v(y) := \begin{pmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^{d-1} \end{pmatrix}.$$

zur Frobenius-Begleitmatrix für das Polynom  $\varphi$ .