Clemens Heuberger

Symbolic Computation

(Rumpf-)Skriptum

Institut für Mathematik B
Technische Universität Graz

Revision 762: 16.~Mai 2011 14:13:17

Inhaltsverzeichnis

Kapitel~1 wurde von Martin Predota nach der Vorlesung im Sommersemester 1999 verfasst.

Kapitel~2 ist ein sehr vorläufiges Rumpfskriptum, in dem nur die Gliederung des Stoffes und einige Definitionen, Sätze und Algorithmen enthalten sind. Dieser Teil der Vorlesung folgt [11].

Fehler und Verbesserungsvorschläge bitte `clemens.heuberger@tugraz.at` mitzuteilen.

Kapitel 1

Gröbner-Basen

1.1 Einleitung

Der Begriff der GRÖBNER-Basis wurde erstmals 1965 in der Dissertation von Bruno BUCHBERGER eingeführt und 1970 in [3] veröffentlicht. Ihren Namen haben sie von BUCHBERGERs Betreuer Wolfgang GRÖBNER. Zu Beginn der achtziger Jahre wurde die Theorie der GRÖBNER-Basen ein wichtiges Teilgebiet der Computer-Algebra und ist mittlerweile in allen wichtigen Programm-Systemen, die symbolische Berechnungen erlauben, integriert. Als Beispiele wären hier Maple, Mathematica, Axiom oder Reduce anzuführen.

Die wahre Bedeutung, die GRÖBNER-Basen erlangt haben, liegt aber darin, dass man sie berechnen kann. Und eben dies ist BUCHBERGER in [3] gelungen; er stellte einen Algorithmus zur Verfügung.

Die wohl wichtigste Anwendung von GRÖBNER-Basen, die symbolische Lösung von polynomialen Gleichungssystemen, wird im Weiteren genauer behandelt.

Darüberhinaus können wir bemerken, dass es zahlreiche andere Anwendungen von GRÖBNER-Basen gibt und viele Ideen in ganz anderen Bereichen der Symbolic Computation verwendet werden[1].

Beispiel 1.1. (`Loesen-Algebraischer-GLS-haendisch.nb`) Betrachte das Gleichungssystem

$$f_1(X,Y) = 2X^2Y + 3X + 4Y = 0$$
$$f_2(X,Y) = 3XY^2 + 4X + 5Y = 0$$

und führe „Linearkombinationen“ aus:

$$\begin{aligned}
f_3 = 3Yf_1 - 2Xf_2 &= -8X^2 - XY + 12Y^2 &&= 0\\
f_4 = 4f_1 + Yf_3 &= 12X + 16Y - XY^2 + 12Y^3 &&= 0\\
f_5 = 3f_4 + f_2 &= 40X + 53Y + 36Y^3 &&= 0\\
f_6 = 3Y^2f_5 - 40f_2 &= -160X - 200Y + 159Y^3 + 108Y^5 &&= 0\\
f_7 = 4f_5 + f_6 &= 12Y + 303Y^3 + 108Y^5 &&= 0
\end{aligned}$$

$f_7 = 0$ hat 5 (eventuell komplexe) Lösungen, aus f_6 (oder f_5) kann man zu jedem Y ein X finden.

1.2 Polynome

Im Folgenden bezeichnen wir mit K einen Körper und mit $\mathbb{P} := K[X_1, \ldots, X_n]$ den zugehörigen Polynomring. Weiters sei $\mathbb{T} := \left\{ X_1^{a_1} \ldots X_n^{a_n} \;\middle|\; a_1, \ldots, a_n \in \mathbb{N}_0 \right\}$ die Menge der Potenzprodukte.

[1] vgl. 1.7 Allgemeine Eigenschaften NOETHERscher Reduktionsrelationen, Seite 11ff

Für $f \in \mathbb{P}$ und $t \in \mathbb{T}$ ist $\mathrm{C}(f,t)$ der *Koeffizient* von t in f, $\mathrm{M}(f,t) = \mathrm{C}(f,t)t$ das *Monom* von f bei t, $\mathrm{S}(f) := \{t \in \mathbb{T} \mid \mathrm{C}(f,t) \neq 0\}$ der *Träger* (support) von f. Dann gilt $f = \sum_{t \in \mathrm{S}(f)} \mathrm{C}(f,t)t$.

Beispiel 1.2. Betrachten wir $f = 6x^2 + 2xy^2 + y^3 + 4y^2 \in \mathbb{Z}[x,y]$, dann erhalten wir

$$\mathrm{C}(f,x) = 0, \mathrm{C}(f,x^2) = 6, \mathrm{M}(f,x) = 0, \mathrm{M}(f,x^2) = 6x^2, \mathrm{S}(f) = \{x^2, xy^2, y^3, y^2\}.$$

1.3 Ideale

Wir betrachten ein algebraisches Gleichungssystem

$$\begin{aligned} f_1(X_1, \ldots, X_n) &= 0 \\ &\vdots \\ f_r(X_1, \ldots, X_n) &= 0, \end{aligned} \tag{1.1}$$

wobei $f_k \in \mathbb{P}$. Wir schreiben $F := \{f_1, \ldots, f_r\}$ und bezeichnen das Gleichungssystem (1.1) kurz als *das durch F gegebene Gleichungssystem.*

Notation 1.3. Für $F \subseteq \mathbb{P}$ sei

$$\mathrm{Id}(F) = \bigcap_{F \subseteq I \trianglelefteq \mathbb{P}} I$$

das von F erzeugte Ideal.

Proposition 1.4. *Sei $F \subseteq \mathbb{P}$ (bzw. $F \subseteq R$ für einen kommutativen Ring R mit 1). Dann gilt*

$$\mathrm{Id}(F) = \{p_1 f_1 + \cdots + p_s f_s : s \in \mathbb{N}_0, p_1, \ldots, p_s \in \mathbb{P}, f_1, \ldots, f_s \in F\}.$$

Beweis. Bezeichne die Menge auf der rechten Seite mit M. Für f, $g \in M$ folgt offensichtlich $f - g \in M$. Ebenfalls gilt für $f \in M$, $p \in \mathbb{P}$, dass $pf \in M$. Also ist M ein Ideal in $\mathbb{P}$.

Wenn I ein Ideal ist, welches F enthält, so muss es auch M enthalten. Daher gilt $M = \mathrm{Id}(F)$. □

Proposition 1.5. *Seien F, $G \subseteq \mathbb{P}$ mit $\mathrm{Id}(F) = \mathrm{Id}(G)$ und $x_1, \ldots, x_n \in K$. Dann gilt*

$$\forall\, f \in F : f(x_1, \ldots, x_n) = 0 \iff \forall\, g \in G : g(x_1, \ldots, x_n) = 0.$$

Beweis. Aufgrund der Symmetrie ist nur eine Richtung zu zeigen. Nehmen wir also an, dass die linke Aussage gilt und sei $g \in G \subseteq \mathrm{Id}(G) = \mathrm{Id}(F)$. Es gibt ein $s \in \mathbb{N}_0$ sowie $p_1, \ldots, p_s \in \mathbb{P}$ und $f_1, \ldots, f_s \in F$, sodass $g = p_1 f_1 + \cdots + p_s f_s$. Daher gilt

$$g(x_1, \ldots, x_n) = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n) \underbrace{f_i(x_1, \ldots, x_n)}_{=0} = 0.$$

□

Definition 1.6. Sei $I \trianglelefteq \mathbb{P}$ und $F \subseteq P$ mit $I = \mathrm{Id}(F)$. Dann heißt F ein Erzeuger oder eine Basis von I.

Um ein algebraisches Gleichungssystem (1.1) zu lösen, suchen wir also eine Basis $G \subseteq \mathbb{P}$ mit $\mathrm{Id}(G) = \mathrm{Id}(F)$, die „besser“ ist (eine Art Stufenform). Das werden genau Gröbner-Basen sein.

Zunächst soll geklärt werden, ob es für jedes Ideal $I \trianglelefteq \mathbb{P}$ ein endliches Erzeugendensystem gibt.

Definition 1.7. Ein kommutativer Ring R mit 1 heißt *noethersch*, wenn jedes Ideal von R endlich erzeugt ist (d.h. ein endliches Erzeugendensystem besitzt).

Ein Körper K ist immer ein noetherscher Ring, weil er genau zwei Ideale besitzt: Das Nullideal $\{0\} = \mathrm{Id}(\{0\})$ sowie den gesamten Körper $K = \mathrm{Id}(\{1\})$.

Satz 1.8 (Hilbertscher Basissatz)**.** *Sei R noethersch. Dann ist $R[X]$ noethersch.*

Beweis. Nehmen wir an, dass $I \trianglelefteq R[X]$ nicht endlich erzeugt ist. Nun wählen wir $f_i \in I$ als Polynom minimalen Grades, das nicht in $\mathrm{Id}(f_1, \ldots, f_{i-1})$ liegt. Die f_i sind dadurch aufsteigend nach $d_i = \deg f_i$ sortiert.

Wir legen $a_i = \mathrm{C}\left(f_i, X^{d_i}\right)$ fest und betrachten $A = \{a_i \mid i \in \mathbb{N}\}$. Es gilt $\mathrm{Id}(A) \trianglelefteq R$ nach Definition, und weil R NOETHERsch ist, gibt es $b_1, \ldots, b_N \in R$ mit $\mathrm{Id}(A) = \mathrm{Id}(b_1, \ldots, b_N)$ und mit $b_i = \sum_{j=1}^{M} c_{ij} a_j$ weiter $\mathrm{Id}(A) = \mathrm{Id}(b_1, \ldots, b_N) = \mathrm{Id}(a_1, \ldots, a_M)$.

Betrachten wir nun f_{M+1} mit dem Leitkoeffizienten $a_{M+1} = \sum_{i=1}^{M} e_i a_i$ und

$$g = f_{M+1} - \sum_{i=1}^{M} e_i X^{d_{M+1} - d_i} f_i,$$

dann folgt

$$\mathrm{C}(g, X^{d_{M+1}}) = \mathrm{C}(f_{M+1}, X^{d_{M+1}}) - \sum_{i=1}^{M} e_i \, \mathrm{C}(f_i, X^{d_i}) = 0.$$

Damit gilt

- $\deg g \leq d_{M+1} - 1$,
- $g \in I$ und
- $g \notin \mathrm{Id}(f_1, \ldots, f_M)$.

Dies ist aber ein Widerspruch zur Wahl von f_{M+1}, also ist $R[X]$ NOETHERsch. □

Korollar 1.9. *$\mathbb{P} = K[X_1, \ldots, X_n]$ ist ein* NOETHER*scher Ring.*

1.4 Zulässige Ordnungen auf Potenzprodukten

Definition 1.10. Sei $\prec$ eine Totalordnung auf $\mathbb{T}$, dann heißt $\prec$ *zulässig*, wenn

1. $1 \prec t$ für alle $1 \neq t \in \mathbb{T}$
2. Aus $u \prec v$ folgt $tu \prec tv$ für alle $u, v, t \in \mathbb{T}$ und $t \neq 0$. (Monotonie)

Beispiel 1.11. Folgende Ordnungen auf $K[X, Y]$ sind zulässig:

1. Gesamtgrad-Ordnung mit $X \prec Y$:

$$1 \prec X \prec Y \prec X^2 \prec XY \prec Y^2 \prec X^3 \prec X^2Y \prec XY^2 \prec Y^3 \prec \ldots$$

2. Lexikographische Ordnung mit $X \prec Y$:

$$1 \prec X \prec X^2 \prec X^3 \prec \cdots \prec Y \prec XY \prec X^2Y \prec \cdots \prec Y^2 \prec XY^2 \prec \ldots$$

Lemma 1.12 (Dickson)**.** *Sei t_i eine Folge aus $\mathbb{T}$, für die $t_i \nmid t_j$ für alle $i < j$ gilt. Dann ist die Folge endlich.*

Beweis. Wir führen eine vollständige Induktion nach der Anzahl der Variablen n durch:

Für $n = 1$ gilt $t_i = X^{e_i}$ und somit $t_i \nmid t_j$ für $i < j$, also $e_i > e_j$. Daraus folgt $e_1 > e_2 > e_3 > \ldots$, was eine fallende Folge natürlicher Zahlen ist, also ist sie endlich.

Nun zum Schritt $n - 1 \to n$:

Wir schreiben $t_i = X_1^{a_{i1}} \ldots X_n^{a_{in}}$. Wir nehmen an, dass die Folge der t_i unendlich ist. Ist $i < j$, dann existiert ein k, sodass $a_{ik} > a_{jk}$ gilt. Für $i = 1$ gibt es ein k, sodass $a_{1k} > a_{jk}$ resultiert.

Nun gibt es ein k, sodass wir $a_{1k} > a_{jk}$ für unendlich viele j erhalten. Es gibt ein $i_0 \in \mathbb{N}$, sodass wir $a_{i_0 k} = a_{jk}$ für unendliche viele j_l mit $l \in \mathbb{N}$ erhalten. Betrachten wir die Potenzprodukte

$$\frac{t_{j_l}}{X_k^{a_{i_0 k}}}$$

in $n-1$ Variablen $X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n$, dann ergibt sich für $l_1 < l_2$

$$\frac{t_{j_{l_1}}}{X_k^{a_{i_0 k}}} \nmid \frac{t_{j_{l_2}}}{X_k^{a_{i_0 k}}}$$

wegen $t_{j_{l_1}} \nmid t_{j_{l_2}}$. Nach Induktionsvoraussetzung ist diese Folge endlich, was ein Widerspruch zu unserer Annahme ist.

□

Proposition 1.13 (Eigenschaften zulässiger Ordnungen)**.** *Sei $\prec$ eine zulässige Ordnung auf $\mathbb{T}$. Dann gilt*

1. *Für alle $t, u \in \mathbb{T}$ folgt $t \preceq u$ aus $t \mid u$.*
2. *$\succ$ ist eine* NOETHER*sche Relation, d.h. es gibt keine unendliche absteigende Kette $t_1 \succ t_2 \succ \ldots$ für $t_i \in \mathbb{T}$.*

Beweis. 1. Nach der Definition gilt $1 \preceq \frac{u}{t}$ und es folgt $t \preceq u$ durch Monotonie.

2. Sei $t_1 \succ t_2 \succ \ldots$ eine absteigende Kette. Nehmen wir an, dass es $i < j$ gibt, sodass $t_i \mid t_j$. Daraus folgt $t_i \preceq t_j$; dies ist ein Widerspruch zur Voraussetzung einer absteigenden Folge. Also folgt aus dem Lemma von DICKSON (Lemma 1.12), dass die Folge endlich ist.

□

Bemerkung 1.14. Die Proposition besagt nicht, dass die Menge $\{t \mid t \preceq u\}$ für festes $u \in \mathbb{T}$ endlich ist.

1.5 Zulässige Ordnungen auf Polynomen

Definition 1.15. Seien $f \in \mathbb{P}, t, t_1, t_2, u \in \mathbb{T}$ und $\prec$ eine zulässige Termordnung auf $\mathbb{T}$, dann definieren wir

$\mathrm{LPP}(f) := \max \mathrm{S}(f)$ (bzgl. $\prec$)		Leading power product
$\mathrm{LC}(f) := \mathrm{C}(f, \mathrm{LPP}(f))$		Leading coefficient
$\mathrm{LM}(f) := \mathrm{M}(f, \mathrm{LPP}(f)) = \mathrm{LC}(f) \cdot \mathrm{LPP}(f)$		Leading monomial
$\mathrm{R}(f) := f - \mathrm{LM}(f)$		Rest
$\mathrm{H}(f,t) := \sum_{\substack{u \in \mathrm{S}(f) \\ u \succ t}} \mathrm{M}(f,u)$		Higher part
$\mathrm{L}(f,t) := \sum_{\substack{u \in \mathrm{S}(f) \\ u \prec t}} \mathrm{M}(f,u)$		Lower part
$\mathrm{B}(f,t_1,t_2) := \sum_{\substack{u \in \mathrm{S}(f) \\ t_1 \prec u \prec t_2}} \mathrm{M}(f,u)$		Part between

Bemerkung 1.16. Mit obiger Definition gilt für $t_1 \prec t_2$

$$f = \mathrm{H}(f,t) + \mathrm{M}(f,t) + \mathrm{L}(f,t)$$
$$f = \mathrm{H}(f,t_2) + \mathrm{M}(f,t_2) + \mathrm{B}(f,t_1,t_2) + \mathrm{M}(f,t_1) + \mathrm{L}(f,t_1)$$

Beispiel 1.17. Nehmen wir wieder $f = 6x^2 + 2xy^2 + y^3 + 4y^2 \in \mathbb{Z}[x, y]$ mit der lexikographischen Ordnung und $x \succ y$, dann erhalten wir

$$\begin{aligned}
&\mathrm{LPP}(f) = x^2, \mathrm{LC}(f) = 6, \mathrm{LM}(f) = 6x^2,\\
&\mathrm{R}(f) = 2xy^2 + y^3 + 4y^2,\\
&\mathrm{H}(f, x) = 6x^2 + 2xy^2, \mathrm{L}(f, x) = y^3 + 4y^2, \mathrm{B}(f, x, y^2) = y^3
\end{aligned}$$

Definition 1.18 (Fortsetzung von zulässigen Ordnungen)**.** Sei $\prec$ eine feste, zulässige Ordnung auf $\mathbb{T}$ und $f, g \in \mathbb{P}$. Wir definieren $f \prec g$, wenn ein $t \in \mathrm{S}(g) \setminus \mathrm{S}(f)$ existiert, sodass $\mathrm{H}(f, t) = \mathrm{H}(g, t)$ ist.

Proposition 1.19. *Sei $\prec$ die Fortsetzung einer zulässigen Ordnung auf $\mathbb{T}$. Dann gilt*

1. *$\prec$ ist eine Halbordnung (d.h. $\prec$ ist transitiv und höchstens eine der Aussagen $f \prec g, f = g, f \succ g$ ist wahr).*
2. *$\succ$ ist* NOETHER*sch, d.h. absteigende Folgen von Polynomen sind endlich.*
3. *Für alle $p \in \mathbb{P} \setminus \{0\}$ gilt $p \succ 0$.*

Beweis. 1. Wir beweisen zunächst Transitivität. Sei $f \prec g \prec h$, $t_1 \in \mathrm{S}(g) \setminus \mathrm{S}(f)$, $\mathrm{H}(f, t_1) = \mathrm{H}(g, t_1)$, $t_2 \in \mathrm{S}(h) \setminus \mathrm{S}(g)$ mit $\mathrm{H}(g, t_2) = \mathrm{H}(h, t_2)$.

Betrachte zunächst den Fall $t_1 \prec t_2$. In diesem Fall ist $\mathrm{C}(f, t_2) = \mathrm{C}(g, t_2)$ da ja $\mathrm{H}(f, t_1) = \mathrm{H}(g, t_1)$, also $t_2 \in \mathrm{S}(h) \setminus \mathrm{S}(f)$. Da $\mathrm{H}(f, t_2) = \mathrm{H}(g, t_2) = \mathrm{H}(h, t_2)$, folgt $f \prec h$.

Im anderen Fall $t_1 \succ t_2$. Da $\mathrm{H}(g, t_2) = \mathrm{H}(h, t_2)$ folgt $\mathrm{C}(g, t_1) = \mathrm{C}(h, t_1)$, also $t_1 \in \mathrm{S}(h) \setminus \mathrm{S}(f)$. Weiters gilt $\mathrm{H}(h, t_1) = \mathrm{H}(g, t_1) = \mathrm{H}(f, t_1)$, also wieder $f \prec h$.

Der dritte Fall $t_1 = t_2$ kann nicht auftreten, denn $t_2 \notin \mathrm{S}(g)$, aber $t_1 \in \mathrm{S}(g)$. Somit ist die Transitivität bewiesen.

Da aus $f \prec g$ nach Definition $f \neq g$ folgt und aus $f \prec g$ und $g \prec f$ nach Transitivität $f \prec f$ folgt, ist $\prec$ eine Halbordnung.

2. NOETHERsche Induktion:

Sei $p_{11} \succ p_{12} \succ \ldots$ eine unendliche absteigende Folge von Polynomen, dann folgt $p_{11} \succ p_{1k}$ für alle $k \in \mathbb{N} \setminus \{1\}$. Nun gibt es ein $t \in \mathrm{S}(p_{11})$, sodass für unendlich viele k_l mit $l \in \mathbb{N}$ $t \in \mathrm{S}(p_{11}) \setminus \mathrm{S}(p_{1k_l})$ und $\mathrm{H}(p_{11}, t) = \mathrm{H}(p_{1k_l}, t)$ gilt. Definieren wir

$$p_{2l} := p_{1k_l} - \mathrm{H}(p_{1k_l}, t) = p_{1k_l} - \mathrm{H}(p_{11}, t),$$

dann erhalten wir

- $\mathrm{LPP}(p_{21}) \prec \mathrm{LPP}(p_{11})$, wegen $\mathrm{LPP}(p_{21}) \prec t \preceq \mathrm{LPP}(p_{11})$
- $p_{21} \succ p_{22} \succ \ldots$ ist nach Konstruktion eine absteigende Folge.

Setzen wir das fort, so können wir immer eine unendliche absteigende Folge mit $\mathrm{LPP}(p_{11}) \succ \mathrm{LPP}(p_{21}) \succ \mathrm{LPP}(p_{31}) \succ \ldots$ erzeugen. Wegen Proposition 1.13 kann es eine solche Folge nicht geben, da die Ordnung auf Potenzprodukten NOETHERsch ist, also auch $\prec$.

3. Sei $t = \mathrm{LPP}(p)$, dann gilt $0 = \mathrm{H}(p, t) = \mathrm{H}(0, t)$ und $t \in \mathrm{S}(p) \setminus \mathrm{S}(0)$.

$\tilde{}$

□

1.6 Reduktion von Polynomen

Der Plan zur Lösung von algebraischen Gleichungssystemen sah vor, zu einem gegebenen Ideal $\mathrm{Id}(F)$ eine „bessere“ Basis G zu finden. Dazu ist es zunächst notwendig, überhaupt feststellen zu können, ob ein gegebenes Polynom g Element des Ideals $\mathrm{Id}(F)$ ist.

Beispiel. Sei $f_1 = 2X^2Y + 3X + 4Y$, $f_2 = 3XY^2 + 4X + 5Y$, $f_3 = 40X + 53Y + 36Y^3$, $f_4 = 12Y + 303Y^3 + 108Y^5$ und $g = -8X^2 - XY + 12Y^2$. Gilt $g \in \mathrm{Id}(f_1, f_2, f_3, f_4)$? (`Ideal-Membership-haendisch.nb`).

Definition 1.20. Seien $g, h \in \mathbb{P}$.

1. Sei $f \in \mathbb{P}$ und $t \in \mathbb{T}$. g kann durch f an t auf h reduziert werden, $g \longrightarrow_{f,t} h$, wenn
   (a) $t \in \mathrm{S}(g)$,
   (b) $\mathrm{LPP}(f) \mid t$ und
   (c) $h = g - \frac{\mathrm{M}(g,t)}{\mathrm{LM}(f)} f$.
2. Sei $f \in \mathbb{P}$. g kann durch f auf h reduziert werden, $g \longrightarrow_f h$, wenn es ein $t \in \mathbb{T}$ mit $g \longrightarrow_{f,t} h$ gibt.
3. Sei $F \subseteq \mathbb{P}$. g kann durch F auf h reduziert werden, $g \longrightarrow_F h$, wenn es ein $f \in F$ mit $g \longrightarrow_f h$ gibt.
4. Sei $F \subseteq \mathbb{P}$. g heißt *reduziert* bezüglich F, $\underline{g}_F$, wenn es kein $h \in \mathbb{P}$ mit $g \longrightarrow_F h$ gibt.

Beispiel 1.21. Seien $g := X^2Y^2 - Y^3$, $f_1 := X^2Y - Y^2$, $f_2 := XY^2 - X^2$ und betrachte die Gesamtgrad-Ordnung mit $X \prec Y$. Dann gilt $g \longrightarrow_{f_1} 0$ und $g \longrightarrow_{f_2} X^3 - Y^3$. Letzteres ist reduziert bzgl. $\{f_1, f_2\}$.

Proposition 1.22. *Seien $g, h \in \mathbb{P}, F \subseteq \mathbb{P}$, dann gilt:*

1. *Wenn g durch f an t auf h reduziert werden kann, dann folgt $\mathrm{M}(h,t) = 0$.*
2. *Wenn g durch F auf h reduziert werden kann, dann folgt $h \prec g$.*
3. *Die Reduktion bezüglich F, $\longrightarrow_F$, ist* NOETHER*sch, d.h. es gibt keine unendliche Folge $g_1 \longrightarrow_F g_2 \longrightarrow_F \dots$*

Beweis. 1.

$$\begin{aligned} h &= g - \frac{\mathrm{M}(g,t)}{\mathrm{LM}(f)} f = g - \frac{t\,\mathrm{C}(g,t)}{\mathrm{LPP}(f)\,\mathrm{LC}(f)} \left(\mathrm{LC}(f)\,\mathrm{LPP}(f) + \mathrm{R}(f)\right) \\ &= g - t\,\mathrm{C}(g,t) - \frac{\mathrm{C}(g,t)}{\mathrm{LC}(f)} \cdot \underbrace{\frac{t}{\mathrm{LPP}(f)}\,\mathrm{R}(f)}_{\prec \frac{t}{\mathrm{LPP}(f)}\,\mathrm{LPP}(f) = t} \\ &= \mathrm{H}(g,t) + \mathrm{M}(g,t) + \mathrm{L}(g,t) - t\,\mathrm{C}(g,t) - \frac{\mathrm{C}(g,t)}{\mathrm{LC}(f)} \cdot \frac{t}{\mathrm{LPP}(f)}\,\mathrm{R}(f) \\ &= \mathrm{H}(g,t) + \mathrm{L}(g,t) - \frac{\mathrm{C}(g,t)}{\mathrm{LC}(f)} \cdot \frac{t}{\mathrm{LPP}(f)}\,\mathrm{R}(f). \end{aligned}$$

2. Da $\mathrm{H}(h,t) = \mathrm{H}(g,t)$ und $t \in \mathrm{S}(g) \setminus \mathrm{S}(h)$.
3. Da $\longrightarrow_F \subseteq \succ$, folgt das aus Proposition˜1.19.

□

Bemerkung 1.23. Es gibt einen Algorithmus, der g durch F auf ein h reduziert, sodass h bezüglich F reduziert ist.

Definition 1.24. Seien $g, h \in \mathbb{P}$ und $F \subseteq \mathbb{P}$.

1. g kann in endlich vielen Schritten durch F auf h reduziert werden, $g \longrightarrow_F^\star h$, wenn $g = g_0, g_1, \ldots, g_{n-1}, g_n = h$ mit $n \geq 0$ existieren, sodass $g_i \longrightarrow_F g_{i+1}$ für alle $0 \leq i \leq n-1$ gilt.
2. g und h sind durch F in endlich vielen Schritten verbindbar, $g \longleftrightarrow_F^\star h$, wenn $g = g_0, g_1, \ldots, g_{n-1}, g_n = h$ mit $n \geq 0$ existieren, sodass $g_i \longrightarrow_F g_{i+1}$ oder $g_{i+1} \longrightarrow_F g_i$ für alle $0 \leq i \leq n-1$ gilt.

Bemerkung 1.25. $\longrightarrow_F^\star$ ist die reflexive, transitive Hülle von $\longrightarrow_F$ und $\longleftrightarrow_F^\star$ ist die reflexive, transitive, symmetrische Hülle von $\longrightarrow_F$

Proposition 1.26 (Eigenschaften der Reduktion)**.** *1. Für $a \in K\backslash\{0\}$ ist $\longrightarrow_f$ gleichwertig mit $\longrightarrow_{af}$.*

2. Seien $a \in K\backslash\{0\}$ und $t \in \mathbb{T}$, dann folgt $atg \longrightarrow_f ath$ aus $g \longrightarrow_f h$.

3. Sei $p \in \mathbb{P}$ und gelte $g \longrightarrow_f h$, dann existiert ein $q \in \mathbb{P}$, sodass

$$g + p \longrightarrow_f^\star q \overset{\star}{}_f\!\longleftarrow h + p$$

gilt.

Bemerkung 1.27. Eigenschaft 3. heißt *Summenhalbverträglichkeit.*

Beweis. 1. und 2. sind klar

3. Sei $t \in S(g)$ mit $g \longrightarrow_{f,t} h$.

   Fall 1: $\mathrm{C}(p,t) = 0$:

   Es folgt $\mathrm{C}(g+p,t) = \mathrm{C}(g,t) \neq 0$ und daraus $g + p \longrightarrow_{f,t} h_1$ mit

$$h_1 = g + p - \frac{\mathrm{M}(g+p,t)}{\mathrm{LM}(f)} f = g - \frac{\mathrm{M}(g,t)}{\mathrm{LM}(f)} f + p = h + p$$

   und wir sind fertig.

   Fall 2: $\mathrm{C}(p,t) \neq 0$ und $\mathrm{C}(g+p,t) \neq 0$:

   Es gilt $g + p \longrightarrow_{f,t} h_1$ mit

$$h_1 = g + p - \frac{\mathrm{M}(g,t)}{\mathrm{LM}(f)} f - \frac{\mathrm{M}(p,t)}{\mathrm{LM}(f)} f = h + p - \frac{\mathrm{M}(p,t)}{\mathrm{LM}(f)} f.$$

   Als nächstes wollen wir $h+p$ reduzieren, was wegen $\mathrm{C}(h+p,t) = \mathrm{C}(h,t)+\mathrm{C}(p,t) = \mathrm{C}(p,t) \neq 0$ erlaubt ist, und wir erhalten $h + p \longrightarrow_{f,t} h_2$ mit

$$h_2 = h + p - \frac{\mathrm{M}(p,t)}{\mathrm{LM}(f)} f$$

   und weiter

$$g + p \longrightarrow_{f,t} h_1 = h_2 \overset{}{}_{f,t}\!\longleftarrow h + p.$$

   Fall 3: $\mathrm{C}(p,t) \neq 0$ und $\mathrm{C}(g+p,t) = 0$:

   Wegen $\mathrm{C}(h+p,t) = \mathrm{C}(p,t) \neq 0$ darf $h+p$ in t reduziert werden. Wir erhalten $h+p \longrightarrow_{f,t} h_2$ mit

$$\begin{aligned} h_2 &= h + p - \frac{\mathrm{M}(p,t)}{\mathrm{LM}(f)} f = g - \frac{\mathrm{M}(g,t)}{\mathrm{LM}(f)} f + p - \frac{\mathrm{M}(p,t)}{\mathrm{LM}(f)} f \\ &= g + p - \underbrace{\frac{\mathrm{M}(g+p,t)}{\mathrm{LM}(f)} f}_{=0} \end{aligned}$$

   also $h + p \longrightarrow_f g + p$.

□

Notation 1.28. Sind $f, g \in \mathbb{P}$ zwei Polynome, dann schreiben wir $f \equiv_F g$ für $f \equiv g \mod \mathrm{Id}(F)$, was zu $f - g \in \mathrm{Id}(F)$ äquivalent ist.

Proposition 1.29. *Seien $F \subseteq \mathbb{P}$ und $g, h \in \mathbb{P}$. Dann ist $g \equiv_F h$ äquivalent zu $g \longleftrightarrow_F^\star h$.*

Beweis. ($\Leftarrow$): Es gilt

$$g = h + \sum_{i=1}^{n} a_i t_i f_i$$

für $a_i \in K, t_i \in \mathbb{T}$ und $f_i \in F$, also folgt $g - h \in \mathrm{Id}(F)$.

($\Rightarrow$): Es gelte $g \equiv_F h$, dann erhalten wir

$$g = h + \sum_{i=1}^{N} a_i t_i f_i$$

für $a_i \in K, t_i \in \mathbb{T}$ und $f_i \in F$. Sei

$$g_k := \sum_{i=1}^{k} a_i t_i f_i,$$

dann behaupten wir, dass $g \longleftrightarrow_F^\star g + g_k$ für $0 \leq k \leq n$ gilt. Dies beweisen wir nun durch Vollständige Induktion nach k.

Für $k = 0$ gilt $g \longleftrightarrow_F^\star g$.

Nun zum Schritt von $k-1$ nach k.

Dabei wissen wir $a_k t_k f_k \longrightarrow_F 0$ und aus der Summenhalbverträglichkeit (vgl. Proposition 1.26 3.) folgt

$$\underbrace{g + g_{k-1} + a_k t_k f_k}_{g+g_k} \longrightarrow_F^\star q \overset{\star}{_F\longleftarrow} g + g_{k-1}$$

und weiter mit der Induktionsvoraussetzung

$$g \longleftrightarrow_F^\star g + g_{k-1} \longleftrightarrow_F^\star g + g_k.$$

□

1.7 Allgemeine Eigenschaften noetherscher Reduktionsrelationen

Definition 1.30. Sei X eine Menge und $\longrightarrow$ eine Relation auf X, also $\longrightarrow \subseteq X \times X$. Dann heißt $\longrightarrow$ eine *Reduktionsrelation* auf X. Statt $(f, g) \in \longrightarrow$ schreiben wir $f \longrightarrow g$.

x heißt *reduziert*, wir schreiben $\underline{x}$, wenn es kein $y \in X$ mit $x \longrightarrow y$ gibt.

Weiters sei $\mathrm{RF} : X \to X$ mit $x \longrightarrow^\star \mathrm{RF}(x)$ und $\mathrm{RF}(x)$ ist reduziert.

x und y haben einen gemeinsamen Nachfolger, $x \downarrow^\star y$, wenn es ein q mit

$$x \longrightarrow^\star q \overset{\star}{\longleftarrow} y$$

gibt.

Bemerkung 1.31. $\longrightarrow$ heißt eine NOETHERsche Relation, wenn es keine unendlichen absteigenden Ketten gibt.

Satz 1.32. *Sei $\longrightarrow$ NOETHERsch. Dann sind folgende Aussagen äquivalent:*

1. *Aus $x \longleftrightarrow^\star y$ folgt $x \downarrow^\star y$.* *(CHURCH-ROSSER-Eigenschaft)*
2. *Aus $x \longleftrightarrow^\star y$ folgt $\mathrm{RF}(x) = \mathrm{RF}(y)$.* *(CHURCH-ROSSER-Normalform-Eigenschaft)*

3. *Aus* $x \overset{\star}{\longleftarrow} z \longrightarrow^\star y$ *folgt* $x \downarrow^\star y$. *(Konfluenz)*

4. *Aus* $x \longleftarrow z \longrightarrow^\star y$ *folgt* $x \downarrow^\star y$. *(Semilokale Konfluenz)*

5. *Aus* $x \longleftarrow z \longrightarrow y$ *folgt* $x \downarrow^\star y$. *(Lokale Konfluenz)*

Beweis. Die Implikationen 2. $\Rightarrow$ 1., 1. $\Rightarrow$ 3., 3. $\Rightarrow$ 4. und 4. $\Rightarrow$ 5. sind klar und werden nicht näher behandelt.

1. $\Rightarrow$ 2.:

Es gilt

$$\mathrm{RF}(x) \overset{\star}{\longleftarrow} x \longleftrightarrow^\star y \longrightarrow^\star \mathrm{RF}(y).$$

Daraus folgt $\mathrm{RF}(x) \longleftrightarrow^\star \mathrm{RF}(y)$, es resultiert weiter $\mathrm{RF}(x) \downarrow^\star \mathrm{RF}(y)$ wegen 1. und schließlich $\mathrm{RF}(x) = \mathrm{RF}(y)$, da $\mathrm{RF}(x)$ und $\mathrm{RF}(y)$ reduziert sind.

3. $\Rightarrow$ 1:

Es gelte $x \longleftrightarrow^\star y$ in n Schritten, also $x \longleftrightarrow^n y$.

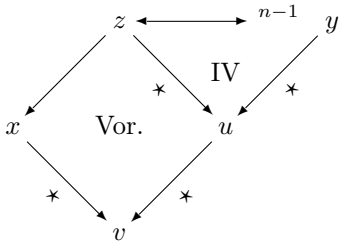
Nun führen wir eine Vollständige Induktion nach n durch. Der Fall $n = 0$ ist klar, also betrachten wir $n > 0$. Dabei erhalten wir zwei mögliche Situationen:

$$x \longrightarrow z \longleftrightarrow^{n-1} y \qquad \text{und} \qquad x \longleftarrow z \longleftrightarrow^{n-1} y$$

für ein z. Im ersten Fall folgt aus der Induktionsvoraussetzung, dass es ein u mit

$$x \longrightarrow z \longrightarrow^\star u \overset{\star}{\longleftarrow} y$$

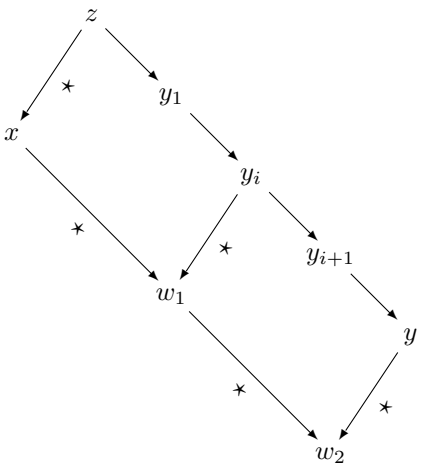
gibt, und im zweiten Fall gibt es u, v mit



In beiden Fällen erhalten wir also $x \downarrow^\star y$.

4. $\Rightarrow$ 3.:

Nehmen wir an, dass x und y keinen gemeinsamen Nachfolger haben. Sei y_i so gewählt, dass x und y_i einen gemeinsamen Nachfolger haben, jedoch x und y_{i+1} keinen. Dann ist w_1 gemeinsamer Nachfolger von x und y_i und mit 4. gibt es auch einen gemeinsamen Nachfolger von w_1 (und damit von x) und y_{i+1}, was ein Widerspruch ist, also haben x und y einen gemeinsamen Nachfolger.

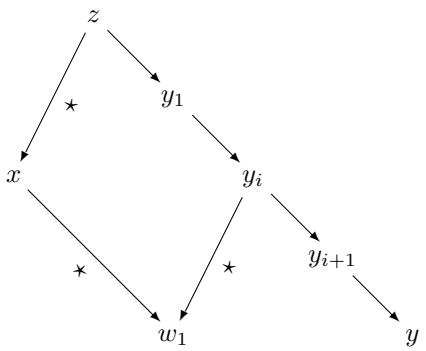


5. $\Rightarrow$ 4.:

Nehmen wir an, x und y haben keinen gemeinsamen Nachfolger, dann gibt es ein i, sodass x und y_i einen gemeinsamen Nachfolger haben, nicht aber x und y_{i+1}, also existiert ein w_1 mit

$$x \longrightarrow^\star w_1 \ {}^\star\!\longleftarrow y_i.$$

Mit



gilt speziell

$$w_1 \ {}^\star\!\longleftarrow y_i \longrightarrow y_{i+1}.$$

Nun haben w_1 und y_{i+1} keinen gemeinsamen Nachfolger; da $y_i \neq z$ laut Voraussetzung gilt, haben wir aber eine unendliche absteigende Kette von Problemfällen, was einen Widerspruch zur Voraussetzung, dass $\longrightarrow$ NOETHERsch ist, darstellt. Somit haben x und y einen gemeinsamen Nachfolger.

□

Definition 1.33. Sei $\succ$ eine NOETHERsche Partialordnung auf X. Wir definieren $x \overset{\prec w}{\longleftrightarrow}^\star y$, wenn es $x = x_0, x_1, \ldots, x_{n-1}, x_n = y$ für $n \geq 0$ mit $x_i \longleftrightarrow x_{i+1}$, $0 \leq i \leq n-1$ und $x_i \prec w$ für alle $0 \leq i \leq n$ gibt.

Proposition 1.34. *Sei $\longrightarrow$ eine Reduktionsrelation auf X und $\succ$ eine* NOETHER*sche Partialordnung auf x mit $\longrightarrow \subseteq \succ$. Dann sind äquivalent:*

1. *Aus $x \longleftarrow z \longrightarrow y$ folgt $x \downarrow^\star y$.* *(Lokale Konfluenz)*
2. *Aus $x \longleftarrow z \longrightarrow y$ folgt $x \overset{\prec z}{\longleftrightarrow}^\star y$.* *(Lokale Verbindbarkeit)*

Beweis. 1. $\Rightarrow$ 2.:

Es gilt

$$w \ {}^\star\!\longleftarrow x \longleftarrow z \longrightarrow y \longrightarrow^\star w,$$

also resultiert 2., weil x, y, w Nachfolger von z sind.

2. $\Rightarrow$ Konfluenz

Es gelte die Lokale Verbindbarkeit. Nun führen wir eine NOETHERsche Induktion auf $\prec$ mit der Induktionsvoraussetzung

$$\text{für alle } \tilde{x}, \tilde{y}, \tilde{z} \text{ folge } \tilde{x} \downarrow^\star \tilde{y} \text{ aus } \tilde{z} \prec z \text{ und } \tilde{x} \ {}^\star\!\longleftarrow \tilde{z} \longrightarrow^\star \tilde{y} \tag{1.2}$$

durch.

Stellen wir uns nun die Situation

$$x \ {}^\star\!\longleftarrow z \longrightarrow^\star y$$

vor. Falls $x = z$ oder $y = z$ gilt, sind wir fertig. Sei also $x \neq z$ und $y \neq z$, dann erhalten wir

$$x \ {}^\star\!\longleftarrow x_1 \longleftarrow z \longrightarrow y_1 \longrightarrow^\star y.$$

Wegen der Lokalen Verbindbarkeit gibt es $u_1, \ldots, u_n \prec z$ mit

$$x_1 = u_1 \longleftrightarrow \ldots \longleftrightarrow u_n = y_1.$$

Nun führen wir eine Vollständige Induktion nach n durch, um zu zeigen, dass

$$\text{aus } u_1 \longleftrightarrow \ldots \longleftrightarrow u_n \text{ und } u_i \prec z \text{ für alle } 1 \leq i \leq n \text{ folgt } u_1 \downarrow^\star u_n \tag{1.3}$$

für alle n und alle $u_1, \ldots, u_n \in X$ gilt.

Der Fall $n = 1$ ist klar.

Nun wollen wir von n auf $n+1$ schließen. Dazu seien $u_1, \ldots, u_{n+1} \in X$, wobei $u_i \prec z$ für $1 \leq i \leq n+1$ und

$$u_1 \longleftrightarrow \ldots \longleftrightarrow u_{n+1}$$

gilt. Es gibt zwei Fälle, in denen die Existenz eines Nachfolgers v zu u_1 und u_{n+1} folgendermaßen gezeigt werden kann:

$$u_1 \longleftrightarrow \ldots \longleftrightarrow u_n \longleftarrow u_{n+1}$$

und mit der zweiten Induktionsvoraussetzung gibt es ein v mit

$$u_1 \longrightarrow^\star v \stackrel{\star}{\longleftarrow} u_n \stackrel{\star}{\longleftarrow} u_{n+1}.$$

Im zweiten Fall erhalten wir wegen der zweiten Induktionsvoraussetzung ein v_1 mit

$$u_1 \longrightarrow^\star v_1 \stackrel{\star}{\longleftarrow} u_n \longrightarrow u_{n+1}$$

und wegen (1.2)

$$v_1 \longrightarrow^\star v \stackrel{\star}{\longleftarrow} u_{n+1}$$

Damit ist (1.3) gezeigt. Nach (1.2) gibt es ein v_2 mit $v \longrightarrow^\star v_2 \stackrel{\star}{\longleftarrow} y$ und ein v_3 mit $x \longrightarrow^\star v_3 \stackrel{\star}{\longleftarrow} v_2 \stackrel{\star}{\longleftarrow} y$. □

1.8 Gröbner-Basen und S-Polynome

Definition 1.35. Eine Teilmenge $F \subseteq \mathbb{P}$ heißt GRÖBNER-*Basis* von $\mathrm{Id}(F)$, wenn $\longrightarrow_F$ die CHURCH-ROSSER-Eigenschaft hat.

Definition 1.36. Seien $f_1, f_2 \in \mathbb{P}$ normiert. Dann heißt

$$\mathrm{SP}(f_1, f_2) := \frac{w}{\mathrm{LPP}(f_1)} f_1 - \frac{w}{\mathrm{LPP}(f_2)} f_2,$$

das S-Polynom von f_1 und f_2, wobei w das kleinste gemeinsame Vielfache von $\mathrm{LPP}(f_1)$ und $\mathrm{LPP}(f_2)$ ist.

Satz 1.37 (Hauptsatz über Gröbner-Basen)**.** *Seien $F \subseteq \mathbb{P}$ normierte Polynome. $\mathrm{RF}_F : \mathbb{P} \to \mathbb{P}$ erfülle, dass $g \longrightarrow_F^\star \mathrm{RF}_F(g)$ für alle $g \in \mathbb{P}$ gilt und $\mathrm{RF}_F(g)$ reduziert ist. Dann sind äquivalent:*

1. *F ist eine* GRÖBNER-*Basis.*
2. *Für alle $g \in \mathrm{Id}(F)$ gilt $\mathrm{RF}_F(g) = 0$.*
3. *Für alle $g \in \mathrm{Id}(F)$ gilt $g \longrightarrow_F^\star 0$.*
4. *Für alle $f_1, f_2 \in F$ gilt $\mathrm{SP}(f_1, f_2) \longrightarrow_F^\star 0$.*
5. *Für alle $f_1, f_2 \in F$ gilt $\mathrm{RF}_F(\mathrm{SP}(f_1, f_2)) = 0$.*
6. *Es gilt $\{\mathrm{LPP}(f) \mid f \in \mathrm{Id}(F)\} = \{u \cdot \mathrm{LPP}(f) \mid f \in F, u \in \mathbb{T}\}$.*

Beweis. 1. $\Rightarrow$ 2.:

Sei $g \in \mathrm{Id}(F)$, dann folgt $g \equiv_F 0$ und mit Proposition 1.29 $g \longleftrightarrow_F^\star 0$. Weiters gilt $\mathrm{RF}_F(g) = \mathrm{RF}_F(0) = 0$ wegen Satz 1.32.

2. $\Rightarrow$ 3. ist klar.

3. $\Rightarrow$ 4.:

$\mathrm{SP}(f_1, f_2) \in \mathrm{Id}(F)$, also $\mathrm{SP}(f_1, f_2) \longrightarrow_F^\star 0$.

4. $\Rightarrow$ 1.:

Wir müssen zeigen, dass $g_1 \overset{\prec h}{\longleftrightarrow}_F^\star g_2$ aus

$$g_1 \ {}_{f_1,t_1}\!\longleftarrow h \longrightarrow_{f_2,t_2} g_2$$

folgt.

Fall 1: $t_1 \prec t_2$:

Es gilt

$$g_1 = h - \frac{\mathrm{C}(h, t_1)t_1}{\mathrm{LPP}(f_1)} f_1,$$

dann folgt $\mathrm{C}(g_1, t_2) = \mathrm{C}(h, t_2) \neq 0$, weshalb eine Reduktion $g_1 \longrightarrow_{f_2,t_2} g_3$ möglich ist. Nun folgt

$$g_2 = h - \frac{\mathrm{C}(h, t_2)t_2}{\mathrm{LPP}(f_2)} f_2 \downarrow^\star g_1 - \frac{\mathrm{C}(h, t_2)t_2}{\mathrm{LPP}(f_2)} f_2 = g_3$$

aus $h \longrightarrow_{f_1,t_1}^\star g_1$ und der Summenhalbverträglichkeit.

Fall 2: $t_1 \succ t_2$ verläuft analog zu Fall 1.

Fall 3: $t_1 = t_2 = t$:

Es gilt

$$g_1 \ {}_{f_1,t}\!\longleftarrow h \longrightarrow_{f_2,t} g_2$$

und da t sowohl durch $\mathrm{LPP}(f_2)$ als auch durch $\mathrm{LPP}(f_1)$ geteilt werden kann, resultiert

$$w := \mathrm{kgV}(\mathrm{LPP}(f_1), \mathrm{LPP}(f_2)) \mid t.$$

Schreiben wir $t = uw$, dann gilt

$$g_1 = h - \frac{\mathrm{C}(h, t)t}{\mathrm{LPP}(f_1)} f_1 = h - \mathrm{C}(h, t)uu_1 f_1$$

und

$$g_2 = h - \mathrm{C}(h, t)uu_2 f_2$$

mit

$$u_1 = \frac{w}{\mathrm{LPP}(f_1)} \qquad u_2 = \frac{w}{\mathrm{LPP}(f_2)}.$$

Nun bilden wir $g_2 - g_1 = \mathrm{C}(h, t)u\,\mathrm{SP}(f_1, f_2)$ und beachten $\mathrm{LPP}(g_2 - g_1) \prec t \preceq \mathrm{LPP}(h)$ wegen der Konstruktion. Da $\mathrm{SP}(f_1, f_2)$ auf 0 reduziert werden kann, existieren $g_2 - g_1 = p_0, \ldots, p_N = 0$ mit $p_i \longrightarrow_F p_{i+1}$ für $0 \leq i \leq N - 1$ und $\mathrm{LPP}(p_i) \prec t$. Damit erhalten wir aus Proposition 1.26 3.

$$p_i + g_1 \downarrow^\star p_{i+1} + g_1$$

für $0 \leq i \leq N - 1$ und es gilt $g_1 \longleftrightarrow_F^\star g_2$.

Betrachten wir $\mathrm{H}(p_i + g_1, t) = \mathrm{H}(g_1, t) = \mathrm{H}(h, t)$, $t \in \mathrm{S}(h)$ und $\mathrm{C}(p_i + g_1, t) = \mathrm{C}(g_1, t) = 0$, dann folgt $p_i + g_1 \prec h$ und es resultiert

$$g_2 = p_0 + g_1 \overset{\prec h}{\longleftrightarrow}_F^\star p_1 + g_1 \overset{\prec h}{\longleftrightarrow}_F^\star \ldots \overset{\prec h}{\longleftrightarrow}_F^\star p_N + g_1 = g_1,$$

und damit

$$g_2 \overset{\prec h}{\longleftrightarrow}_F^\star g_1.$$

2. $\Rightarrow$ 5.:

Es gilt $\mathrm{SP}(f_1, f_2) \in \mathrm{Id}(F)$.

5. $\Rightarrow$ 4. ist klar.

3. $\Rightarrow$ 6.:

Sei $f \in F, u \in \mathbb{T}$, dann folgt $u \cdot \mathrm{LPP}(f) = \mathrm{LPP}(uf)$ mit $uf \in \mathrm{Id}(F)$, also $\{\mathrm{LPP}(f) \mid f \in \mathrm{Id}(F)\} \supseteq \{u \cdot \mathrm{LPP}(f) \mid f \in F, u \in \mathbb{T}\}$. Nun bleibt noch die umgekehrte Teilmengenrelation zu zeigen: Sei $g \in \mathrm{Id}(f)$, dann gilt $g \longrightarrow_F^\star 0$ wegen 3., und damit existiert ein $f \in F$ mit $\mathrm{LPP}(f) \mid \mathrm{LPP}(g)$.

6. $\Rightarrow$ 2.:

Sei $g \in \mathrm{Id}(f)$, dann resultiert $\mathrm{RF}_F(g) \in \mathrm{Id}(F)$ und wegen 6. folgt

$$\mathrm{LPP}\left(\mathrm{RF}_F(g)\right) = u \cdot \mathrm{LPP}(f)$$

für ein $u \in \mathbb{T}, f \in F$, falls $\mathrm{RF}_F(g) \neq 0$. Wir können somit $\mathrm{RF}_F(g)$ nach f reduzieren, also $\mathrm{RF}_F(g) = 0$. □

1.9 Algorithmus zur Berechnung von Gröbner-Basen

Sei G die Menge der derzeitigen Basis und S die Menge der zu überprüfenden S-Polynome. Dann lautet der Algorithmus von Buchberger:

Algorithmus 1.1 Buchberger-Algorithmus zur Berechnung von Gröbner-Basen

Gegeben: Endliche Menge $F \subseteq \mathbb{P}$
Gesucht: $G \subseteq \mathbb{P}$ mit $\mathrm{Id}(F) = \mathrm{Id}(G)$ und G Gröbner-Basis

```
G := F
S := {{f1, f2} | f1 ≠ f2 ∈ G}
while S ≠ ∅ do
  Wähle {f1, f2} ∈ S
  S := S\{f1, f2}
  r := RF_G(SP(f1/LC(f1), f2/LC(f2)))
  if r ≠ 0 then
    S := S ∪ {{r, f} | f ∈ G}
    G := G ∪ {r}
  end if
end while
```

Proposition 1.38. *Der Algorithmus von* Buchberger *terminiert nach endlich vielen Schritten, es gilt* $\mathrm{Id}(F) = \mathrm{Id}(G)$ *und* G *ist eine* Gröbner-*Basis.*

Beweis. Sei g_i die Folge der hinzugefügten Polynome. Nun gilt $\mathrm{LPP}(g_i) \nmid \mathrm{LPP}(g_j)$ für alle $i < j$, da sonst g_j bezüglich $F \cup \{g_1, \ldots, g_{j-1}\}$ nicht reduziert wäre. Nach dem Lemma von Dickson (Lemma 1.12) ist die Folge $\mathrm{LPP}(g_i)$, $i \geq 1$, endlich, weshalb der Algorithmus terminiert.

Aus $F \subseteq G$ folgt $\mathrm{Id}(F) \subseteq \mathrm{Id}(G)$. Durch die Konstruktion gilt $r \in \mathrm{Id}(F)$ für jedes hinzugefügte r, also $\mathrm{Id}(F) = \mathrm{Id}(G)$.

Es sind alle S-Polynome überprüft, also ist G eine Gröbner-Basis.

□

Definition 1.39. Sei $F \subseteq \mathbb{P}$ eine Gröbner-Basis. F heißt *reduzierte* Gröbner-Basis, wenn alle $f \in F$ bezüglich $F\backslash\{f\}$ reduziert sind.

Proposition 1.40. *Sei* F *eine* Gröbner-*Basis und* $f \in F$*. Dann ist* $F\backslash\{f\} \cup \{\mathrm{RF}_{F\backslash\{f\}}(f)\}$ *eine* Gröbner-*Basis desselben Ideals.*

Beweis. Sei $h := \mathrm{RF}_{F\backslash\{f\}}(f)$ und $G := F\backslash\{f\} \cup \{h\}$. Da $f \equiv_{F\backslash\{f\}} \mathrm{RF}_{F\backslash\{f\}}(f)$ gilt, erzeugen F und G dasselbe Ideal.

Sei $g \in \mathrm{Id}(F)$ und $r := \mathrm{RF}_G(g) \neq 0$. Dann gibt es ein $\tilde{r}$, sodass $r \longrightarrow_f \tilde{r}$ gilt. Nun gibt es aber ein $t \in \mathrm{S}(r)$, sodass $\mathrm{LPP}(f) \mid t$ gilt. Da wir nach h nicht reduzieren können, gilt $\mathrm{LPP}(h) \neq \mathrm{LPP}(f)$. Somit existiert jedoch ein $\tilde{f} \in F \backslash \{f\}$, welches $\mathrm{LPP}(f)$ eliminiert und es folgt $\mathrm{LPP}(\tilde{f}) \mid \mathrm{LPP}(f) \mid t$ und somit ist r nicht nach G reduziert, was ein Widerspruch zu unserer Voraussetzung ist.

□

Bemerkung 1.41. Proposition 1.40 führt sofort zu einem Algorithmus zur Berechnung einer reduzierten GRÖBNER-Basis: Man berechnet eine GRÖBNER-Basis nach dem BUCHBERGER-Algorithmus, und, solange die Basis nicht reduziert ist, ersetzt man sie nach Proposition 1.40. Dieser Algorithmus terminiert, weil $\longrightarrow$ NOETHERsch ist.

Definition 1.42. Sei $F \subseteq \mathbb{P}$. Wir bezeichnen die durch den BUCHBERGER-Algorithmus gebildete GRÖBNER-Basis von $\mathrm{Id}(F)$ mit $\mathrm{GB}(F)$ und die nach obigem Algorithmus berechnete reduzierte GRÖBNER-Basis mit $\mathrm{RGB}(F)$.

Proposition 1.43. *Seien $F, G \subseteq \mathbb{P}$ reduzierte* GRÖBNER*-Basen, deren Elemente normiert sind. Genau dann ist $\mathrm{Id}(F) = \mathrm{Id}(G)$, wenn $F = G$ gilt.*

Beweis. ($\Leftarrow$) folgt sofort.

($\Rightarrow$):

Seien $F = \{f_1, \ldots, f_r\}$ und $G = \{g_1, \ldots, g_s\}$. Nun können wir die Elemente so umnummerieren, dass $\mathrm{LPP}(f_1) \prec \cdots \prec \mathrm{LPP}(f_r)$ bzw. $\mathrm{LPP}(g_1) \prec \cdots \prec \mathrm{LPP}(g_s)$ gilt, da F und G reduzierte GRÖBNER-Basen sind. Nehmen wir an, es gilt für ein gewisses $k \geq 1$, dass $f_i = g_i$ für $i = 1, \ldots, k-1$ ist. Nun betrachten wir $f_k \in \mathrm{Id}(F) = \mathrm{Id}(G)$ und es folgt

$$f_k \longrightarrow_{g_l} \tilde{f}_k \longrightarrow^\star_G 0.$$

Dabei muss $l \geq k$ gelten, da wir sonst $g_l = f_l$ haben, was ein Widerspruch zur Reduziertheit von F ist. Folglich ist $\mathrm{LPP}(g_l) \preceq \mathrm{LPP}(f_k)$ für ein $l \geq k$ und analog $\mathrm{LPP}(f_{\tilde{l}}) \preceq \mathrm{LPP}(g_k)$ für ein $\tilde{l} \geq k$. Daraus resultiert $\mathrm{LPP}(f_k) = \mathrm{LPP}(g_k)$ und weiter $f_k \longrightarrow_{g_k} f_k - g_k$.

Nehmen wir an, dass $f_k - g_k \neq 0$ ist. Aus $f_k - g_k \longrightarrow^\star_F 0$ folgt

$$f_k - g_k \longrightarrow^\star_{\{f_1 = g_1, \ldots, f_{k-1} = g_{k-1}\}} 0,$$

was ein Widerspruch zur Reduziertheit der GRÖBNER-Basis ist, weil alle Potenzprodukte von $f_k - g_k$ von f_k oder von g_k stammen.

□

Beispiel 1.44. (`Groebner-Bsp.mws`, `Groebner-Bsp.nb`) Man bestimme eine GRÖBNER-Basis bezüglich der lexikographischen Termordnung mit $x \prec y$ und bezüglich der Gesamtgrad-Termordnung mit $x \prec y$ von

$$\mathrm{Id}(x^2 + y^2 + 5, xy - 2).$$

```
> with(Groebner):
> f1:=x^2+y^2+5:
> f2:=x*y-2:
> gbasis([f1,f2], plex(y,x));
```

$$[x^4 + 5x^2 + 4, 2y + x^3 + 5x]$$

```
> gbasis([f1,f2], tdeg(y,x));
```

$$[yx - 2, y^2 + x^2 + 5, x^3 + 2y + 5x]$$

1.10 Idealoperationen mit Gröbner-Basen

1.10.1 Ideale

Proposition 1.45. *Seien $F, G \subseteq \mathbb{P}$ und $f, g \in \mathbb{P}$.*

1. *$f \in \mathrm{Id}(F)$ genau dann, wenn $\mathrm{RF}_{\mathrm{GB}(F)}(f) = 0$ gilt.*
2. *$f \equiv_F g$ ist äquivalent zu $\mathrm{RF}_{\mathrm{GB}(F)}(f) = \mathrm{RF}_{\mathrm{GB}(F)}(g)$.*
3. *Es gilt $\mathrm{Id}(F) \subseteq \mathrm{Id}(G)$ genau dann, wenn $\mathrm{RF}_{\mathrm{GB}(G)}(f) = 0$ für alle $f \in F$ ist.*
4. *$\mathrm{Id}(F) = \mathrm{Id}(G)$ ist äquivalent zu $\mathrm{RGB}(F) = \mathrm{RGB}(G)$.*
5. *$\mathrm{Id}(F)$ ist genau dann ein Hauptideal, wenn die reduzierte* Gröbner-*Basis von F $\mathrm{RGB}(F)$ einelementig ist.*

Die Beweise der einzelnen Aussagen folgen aus dem Hauptsatz über Gröbner-Basen (Satz 1.37) und aus Proposition 1.43.

1.10.2 Eliminationsideale

Definition 1.46. Sei $I \trianglelefteq \mathbb{P}$ ein Ideal, $1 \leq \ell \leq n$. Dann heißt

$$I_\ell := I \cap K[X_1, \ldots, X_\ell]$$

ℓ-tes *Eliminationsideal*.

Definition. Sei $\prec$ eine Termordnung auf $\mathbb{T}[X_1, \ldots, X_n]$ und $1 \leq \ell \leq n$. Dann heißt $\prec$ eine *Eliminationstermordnung bezüglich $X_{\ell+1}, \ldots, X_n$*, wenn für alle $t \in \mathbb{T}[X_1, \ldots, X_\ell]$ und alle $u \in \mathbb{T}[X_1, \ldots, X_n] \setminus \mathbb{T}[X_1, \ldots, X_\ell]$ gilt, dass $t \prec u$.

Beispiel. Die lexikographische Termordnung mit $X_1 \prec \cdots \prec X_n$ ist für jedes $1 \leq \ell \leq n$ eine Eliminationstermordnung bezüglich $X_{\ell+1}, \ldots, X_n$.

Proposition 1.47. *Sei $1 \leq \ell \leq n$ und sei G* Gröbner-*Basis von $I \trianglelefteq \mathbb{P}$ bezüglich einer Eliminationstermordnung bezüglich $X_{\ell+1}, \ldots, X_n$. Dann gilt*

1. *$G_\ell := G \cap K[X_1, \ldots, X_\ell]$ ist* Gröbner-*Basis von I_ℓ.*
2. *Ist G eine reduzierte* Gröbner-*Basis, dann ist G_ℓ eine reduzierte* Gröbner-*Basis von I_ℓ.*

Beweis. 1. Es gilt $G_\ell \subseteq I_\ell$.

Sei $f \in I_\ell$, dann folgt $f \longrightarrow_G^\star 0$. In der Reduktion kommen nur Potenzprodukte $\preceq \mathrm{LPP}(f)$ vor, welche aufgrund der Termordnung alle in $K[X_1, \ldots, X_\ell]$ enthalten sind, und es kann nicht bezüglich eines $g \in G \setminus G_\ell$ reduziert werden. Somit resultiert $f \longrightarrow_{G_\ell}^\star 0$ und damit ist G_ℓ wegen des Hauptsatzes über Gröbner-Basen (Satz 1.37) Gröbner-Basis.

2. Ist klar.

□

1.11 Algebraische Gleichungssysteme

Definition 1.48. Sei $I \trianglelefteq \mathbb{P}$ ein Ideal. Dann heißt

$$V(I) := \{(c_1, \ldots, c_n) \in K^n \mid f(c_1, \ldots, c_n) = 0 \quad \forall f \in I\}$$

Nullstellenmenge von I.

Haben wir ein Gleichungssystem in n Unbekannten $X_1, \ldots, X_n$ gegeben, dann hat eine zugehörige reduzierte GRÖBNER-Basis G von I bezüglich der lexikographischen Termordnung mit $X_1 \prec X_2 \prec \cdots \prec X_n$ etwa folgendes Aussehen:

$$\begin{gathered} g_1(X_1) \\ g_{21}(X_1, X_2), \ldots, g_{2s_2}(X_1, X_2) \\ \vdots \\ g_{n1}(X_1, \ldots, X_n), \ldots, g_{ns_n}t(X_1, \ldots, X_n), \end{gathered}$$

wobei die $s_i \geq 0$ für $2 \leq i \leq n$ ganze Zahlen sind.

Der Lösungsweg ist dann folgender: Man löst die erste Gleichung nach X_1, setzt jede Lösung in die übrigen Gleichungen ein, erweitert (wenn möglich) die Lösung durch ein passendes X_2 etc.

Dazu können wir uns folgende Fragen stellen:

- Gibt es eine Lösung?
- Gibt es unendlich viele Lösungen?
- Funktioniert der Erweiterungsschritt immer?
- Was wissen wir über Polynome, die auf $V(I)$ verschwinden?

Diese Fragen werden wir im Folgenden beantworten.

Definition 1.49. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht konstante Polynom in $K[X]$ eine Nullstelle in K besitzt.

Beispiel 1.50. $\mathbb{C}$ ist algebraisch abgeschlossen.

Bemerkung 1.51. Ist ein Körper K algebraisch abgeschlossen, dann ist K unendlich.

1.11.1 Resultanten

Definition 1.52. Sei R ein ZPE-Ring, $f, g \in R[X]$ mit

$$f = \sum_{i=0}^{m} a_i X^i, \qquad g = \sum_{j=0}^{n} b_j X^j,$$

wobei $a_m \neq 0$ und $b_n \neq 0$ gilt. Dann ist die *Resultante* von f und g durch

$$\operatorname{Res}_X(f,g) := \begin{vmatrix} a_0 & a_1 & a_2 & \ldots & a_{m-1} & a_m & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & a_2 & \ldots & a_{m-1} & a_m & 0 & \ldots & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & \ldots & a_{m-1} & a_m & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & a_0 & a_1 & a_2 & \ldots & a_{m-1} & a_m \\ b_0 & b_1 & b_2 & \ldots & b_{n-1} & b_n & 0 & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & b_2 & \ldots & b_{n-1} & b_n & 0 & \ldots & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & \ldots & b_{n-1} & b_n & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & b_0 & b_1 & b_2 & \ldots & b_{n-1} & b_n \end{vmatrix}$$

definiert, wobei die Koeffizienten von f über n und die Koeffizienten von g über m Zeilen wiederholt werden.

Bemerkung 1.53. Es gilt $\mathrm{Res}_X(f,g) \in R$.

Lemma 1.54. *Sei R ein ZPE-Ring, $f, g \in R[X]$. Dann gibt es $A, B \in R[X]$, nicht beide 0, sodass $\deg A < \deg g$, $\deg B < \deg f$ und $Af + Bg = \mathrm{Res}_X(f,g)$ gilt.*

Beweis. Es bezeichne S jene Matrix, deren Determinante die Resultante ist. Dann folgt

$$\begin{aligned}&(c_0, \ldots, c_{n-1}, d_0, \ldots, d_{m-1})S \\ &\quad = (c_0a_0, c_0a_1 + c_1a_0, \ldots, c_{n-1}a_m) + (d_0b_0, d_0b_1 + d_1b_0, \ldots, d_{m-1}b_n) \end{aligned} \tag{1.4}$$

wobei $c_0a_0, c_0a_1 + c_1a_0, \ldots, c_{n-1}a_m$ die Koeffizienten von Af mit $A = \sum c_iX^i$ und $d_0b_0, d_0b_1 + d_1b_0, \ldots, d_{m-1}b_n$ die Koeffizienten von Bg mit $B = \sum d_jX^j$ sind.

Mit der zu M adjungierten Matrix $M^\star$ gilt $M^\star M = \det M \cdot I$. Verwenden wir nun die erste Zeile von $S^\star$ für $(c_0, \ldots, c_{n-1}, d_0, \ldots, d_{m-1})$, dann resultiert

$$= (\det S, 0, \ldots, 0) = (\mathrm{Res}_X(f,g), 0, \ldots, 0)$$

für (1.4).

Nehmen wir $A = B = 0$ an. Daraus folgt offensichtlich $\mathrm{Res}_X(f,g) = 0$, das heißt S ist singulär. Daher gibt es einen nichtverschwindenden Vektor $x^t = (c_0, \ldots, c_{n-1}, d_0, \ldots, d_{m-1})^t$ mit $x^tS = 0$. Die Einträge des Vektors können als Koeffizienten von A und B gewählt werden. □

Lemma 1.55. *Sei R ein ZPE-Ring, $f, g \in R[X]$. Dann sind folgende Aussagen äquivalent:*

1. *f und g haben einen nicht-konstanten gemeinsamen Teiler.*
2. *Es gibt $A, B \in R[X]$ mit $\deg A < \deg g, \deg B < \deg f$, sodass $Af + Bg = 0$ ist, aber A und B nicht beide verschwinden.*
3. *$\mathrm{Res}_X(f,g) = 0$.*

Beweis. (1) ⇒ (2) Sei $h := \mathrm{ggT}(f,g)$. Wähle $A = g/h$ und $B = -f/h$. Diese erfüllen die Anforderungen. Falls $f = g = 0$, können beliebige Polynome A und B gewählt werden.

(2) ⇒ (1) Sei $Af + Bg = 0$, also $Af = -Bg$. Falls $\mathrm{ggT}(f,g) = 1$, so folgt aus dieser Gleichung $f \mid B$, also ist $B = 0$ oder $\deg B \geq \deg f$, was ausgeschlossen ist. Damit folgt $A = B = 0$, Widerspruch.

(2) ⇒ (3) Wähle $x^t = (c_0, \ldots, c_{n-1}, d_0, \ldots, d_{m-1})$, wobei $A = \sum_{j=0}^{n-1} c_jX^j$ und $B = \sum_{j=0}^{m-1} d_jX^j$. Nach (1.4) folgt $x^tS = 0$, also ist S singulär und hat damit verschwindende Determinante.

(3) ⇒ (2) Folgt aus Lemma˜1.54.

□

1.11.2 Erweiterungssatz

Satz 1.56 (Erweiterungssatz)**.** *Sei K ein algebraisch abgeschlossener Körper, $I = \mathrm{Id}(f_1, \ldots, f_s) \trianglelefteq K[X_1, \ldots, X_n]$ ein Ideal. Schreibe*

$$f_i = g_i(X_1, \ldots, X_{n-1})X_n^{N_i} + \text{ niedere } X_n\text{-Terme}, g_i \neq 0.$$

Wenn $(c_1, \ldots, c_{n-1}) \in V(I_{n-1}) \backslash V(g_1, \ldots, g_s)$, dann gibt es ein $c_n \in K$ mit $(c_1, \ldots, c_n) \in V(I)$.

Beweis. Im Fall $s = 1$ kann man c_n aus der einzigen Gleichung

$$f_1(c_1, \ldots, c_{n-1}, X_n) = g_1(c_1, \ldots, c_{n-1})X_n^{N_i} + \text{ niedere } X_n\text{-Terme}$$

bestimmen, da laut Voraussetzung $g_1(c_1, \ldots, c_{n-1}) \neq 0$.

O.B.d.A. gelte $s \geq 2$ und $g_1(c_1, \ldots, c_{n-1}) \neq 0, g_2(c_1, \ldots, c_{n-1}) \neq 0$ und $\deg_{X_n}(g_2) > \deg_{X_n}(g_i)$ für $3 \leq i \leq n$. Um das zu gewährleisten, ersetzen wir gegebenenfalls f_2 durch $f_2 + X_n^N f_1$ mit einem genügend großen $N \in \mathbb{N}$.

Seien $U_2, \ldots, U_s$ neue Variable. Wegen Lemma 1.54 existieren jetzt $A, B \in K[X_1, \ldots, X_{n-1}, X_n, U_2, \ldots, U_s]$, sodass

$$\mathrm{Res}_{X_n}(f_1, U_2 f_2 + \cdots + U_s f_s) = A f_1 + B(U_2 f_2 + \cdots + U_s f_s). \tag{1.5}$$

Da die Resultante $\in K[X_1, \ldots, X_{n-1}, U_2, \ldots, U_s]$, also X_n nicht vorkommt, kann man sie in der Gestalt

$$\mathrm{Res}_{X_n}(f_1, U_2 f_2 + \cdots + U_s f_s) = \sum_{U \in \mathbb{T}'} R_U(X_1, \ldots, X_{n-1}) U \tag{1.6}$$

mit $\mathbb{T}' = \mathbb{T}(U_2, \ldots, U_s)$ und passenden $R_U \in K[X_1, \ldots, X_{n-1}]$ für $U \in \mathbb{T}'$ schreiben. Kombiniert man (1.5) und (1.6) und führt einen Koeffizientenvergleich in $U_2, \ldots, U_s$ durch, sieht man $R_U \in I$, also $R_U \in I \cap K[X_1, \ldots, X_{n-1}] = I_{n-1}$. Laut Voraussetzung gilt damit $R_U(c_1, \ldots, c_{n-1}) = 0$. Sei jetzt $\tilde{f}_i := f_i(c_1, \ldots, c_{n-1}, X_n) \in K[X_n]$, wir setzen also für die ersten $n-1$ Variablen die gegebenen Werte ein. Da

$$\begin{aligned} \tilde{f}_1 &= g_1(c_1, \ldots, c_{n-1}) X_n^{N_1} + \text{ niedere } X_n\text{-Terme}, \\ U_2 \tilde{f}_2 + \cdots + U_s \tilde{f}_s &= U_2 g_2(c_1, \ldots, c_{n-1}) X_n^{N_2} + \text{ niedere } X_n\text{-Terme (mit } U_2, \ldots, U_s), \end{aligned}$$

haben auch diese beiden Polynome $\in K[U_2, \ldots, U_s][X_n]$ die gleichen Grade N_1 und N_2 in X_n wie die ursprünglichen Polynome f_1 und $U_2 f_2 + \ldots U_s f_s$, weil $g_1(c_1, \ldots, c_{n-1}) \neq 0$ und $g_2(c_1, \ldots, c_{n-1}) \neq 0$. Man kann daher die Resultante bezüglich X_n durch einfaches Einsetzen in (1.6) ausrechnen und erhält folglich

$$\mathrm{Res}_{X_n}(\tilde{f}_1, U_2 \tilde{f}_2 + \cdots + U_s \tilde{f}_s) = 0.$$

Mit Lemma 1.55 gibt es ein nicht konstantes $F \in K[U_2, \ldots, U_s, X_n]$, sodass F Teiler von $\tilde{f}_1(X_n)$ und Teiler von $U_2 \tilde{f}_2(X_n) + \cdots + U_s \tilde{f}_s(X_n)$ ist. Da $\tilde{f}_1 \in K[X_n]$, folgt auch $F \in K[X_n]$. Für ein passendes $Q \in K[U_2, \ldots, U_s, X_n]$ schreibe $F(X_n) Q(U_2, \ldots, U_s, X_n) = U_2 \tilde{f}_2(X_n) + \cdots + U_s \tilde{f}_s(X_n)$. Führen wir nun einen Koeffizientenvergleich nach $U_2, \ldots, U_s$ durch, dann sehen wir, dass $F(X_n)$ Teiler von $\tilde{f}_2(X_n)$ bis $\tilde{f}_s(X_n)$ ist. Folglich gilt für eine Nullstelle c_n von F — eine solche existiert, weil K algebraisch abgeschlossen und F nicht konstant ist — dass $0 = \tilde{f}_i(c_n) = f_i(c_1, \ldots, c_n)$ für $1 \leq i \leq s$. Das heißt $(c_1, \ldots, c_n) \in V(I)$. □

1.11.3 Hilbertscher Nullstellensatz

Lemma 1.57. *Sei K ein algebraisch abgeschlossener Körper und $f \in K[X_1, \ldots, X_n]$ vom Grad d. Dann gibt es eine reguläre Variablentransformation $X_j = \sum_{i=1}^n a_{ij} Y_i$ (wobei $a_{ij} \in K$ mit $\det(a_{ij}) \neq 0$), sodass f in ein Polynom übergeht, in dem Y_n^d mit nichtverschwindendem Koeffizienten auftritt.*

Beweis. Sei $f(X_1, \ldots, X_n) = f_d + \tilde{f}(X_1, \ldots, X_n)$ mit $\deg \tilde{f} < d$ und

$$f_d(X_1, \ldots, X_n) = \sum_{\substack{t \in \mathbb{T} \\ \deg t = d}} c_t t = \sum_{\substack{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n \\ \alpha_1 + \cdots + \alpha_n = d}} c_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

wobei $c_\alpha = c_{X_1^{\alpha_1} \ldots X_n^{\alpha_n}}$. Setzt man den Ansatz $X_j = \sum_{i=1}^n a_{ij} Y_i$ ein, erhält man ein Polynom $g \in K[Y_1, \ldots, Y_n]$. Es gilt

$$C(g, Y_n^d) = \sum_{\substack{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n \\ \alpha_1 + \cdots + \alpha_n = d}} c_\alpha a_{n1}^{\alpha_1} \cdots a_{nn}^{\alpha_n} = f_d(a_{n1}, \ldots, a_{nn}).$$

Wir müssen also nur $a_{n1}, \ldots, a_{nn}$ so wählen, dass $f_d(a_{n1}, \ldots, a_{nn}) \neq 0$. Dass dies immer möglich ist, kann durch Induktion gezeigt werden. Da K algebraisch abgeschlossen ist, hat K insbesondere unendlich viele Elemente. Da ein Polynom $\in K[X]$ vom Grad k höchstens k Nullstellen in K hat, gibt es also eine Nicht-Nullstelle. Für den Induktionsschritt von $n-1$ auf n schreibt man $f_d(X_1, \ldots, X_n) = \sum_{j=0}^{d} g_j(X_1, \ldots, X_{n-1}) X_n^j$. Da nicht alle $g_j = 0$, können $a_{n1}, \ldots, a_{n,n-1}$ nach Induktionsannahme so gewählt werden, dass $g_s(a_{n1}, \ldots, a_{n,n-1}) \neq 0$ für ein $0 \leq s \leq d$. Daher ist das Polynom in X_n $f_d(a_{n1}, \ldots, a_{n,n-1}, X_n) = \sum_{j=0}^{d} g_j(a_{n1}, \ldots, a_{n,n-1}) X_n^j$ nicht das Nullpolynom, es hat daher eine Nicht-Nullstelle a_{nn}. Somit wurden $a_{n1}, \ldots, a_{nn}$ mit den geforderten Eigenschaften gefunden. Ergänzt man den Vektor $(a_{n1}, \ldots, a_{nn})$ zu einer Basis des K^n, hat man eine reguläre Variablentransformation gewonnen. □

Satz 1.58 (Hilbertscher Nullstellensatz, schwache Version)**.** *Sei K algebraisch abgeschlossen, $I \trianglelefteq \mathbb{P}$ ein Ideal. Genau dann ist $I = \mathbb{P}$, wenn $V(I) = \emptyset$ gilt.*

Beweis. ($\Rightarrow$):
Falls $I = \mathbb{P}$ gilt, dann folgt $1 \in I$. Da die Gleichung $1 = 0$ keine Lösung hat, resultiert $V(I) = \emptyset$.
($\Leftarrow$):
Wir führen eine vollständige Induktion nach der Anzahl der Variablen durch.
Im Fall $n = 1$ ist $K[X]$ Hauptidealbereich, $I = \mathrm{Id}(f)$ und $V(I)$ die Menge der Nullstellen von f. Ist $V(I) = \emptyset$, dann muss $f \neq 0$ konstant sein, also $I = \mathbb{P}$.

Nun schließen wir von $n-1$ auf n. Sei $V(I) = \emptyset$ und $I = \mathrm{Id}(f_1, \ldots, f_s)$. Ohne Beschränkung der Allgemeinheit sei f_1 nicht konstant, dann existiert wegen Lemma 1.57 eine reguläre Variablentransformation

$$X_j = \sum_{i=1}^{n} a_{ij} Y_i,$$

sodass f_1 in das Polynom $\tilde{f}_1$ übergeht, in dem Y_n^d mit nichtverschwindendem Koeffizienten auftritt, wobei $d = \deg f_1$ ist. Wir führen diese Variablentransformation auch für $f_2, \ldots, f_s$ durch und erhalten neue Polynome $\tilde{f}_2, \ldots, \tilde{f}_s \in K[Y_1, \ldots, Y_n]$. Damit führen wir I in $\tilde{I} = \mathrm{Id}(\tilde{f}_1, \ldots, \tilde{f}_s)$ über. Jetzt muss $V(\tilde{I}) = \emptyset$ gelten, weil wir ansonsten Lösungen rücktransformieren könnten.

Nun müssen wir $\tilde{I} = K[Y_1, \ldots, Y_n]$ zeigen. Dazu sei $\tilde{I}_{n-1} = \tilde{I} \cap K[Y_1, \ldots, Y_{n-1}]$. Wenn die Nullstellenmenge von $\tilde{I}_{n-1}$ leer ist, dann folgt $1 \in \tilde{I}_{n-1}$ aus der Induktionsvoraussetzung, weiters $1 \in \tilde{I}$ und damit $1 \in I$, was $I = \mathbb{P}$ bedeutet.

Sei also $V(\tilde{I}_{n-1}) \neq \emptyset$ und $(c_1, \ldots, c_{n-1}) \in V(\tilde{I}_{n-1})$. Da $\tilde{f}_1 = k_1 Y_n^d +$ niedere Y_n-Terme laut Konstruktion mit $k_1 \in K \backslash \{0\}$ gilt, folgt $(c_1, \ldots, c_{n-1}) \notin V(\tilde{g}_1, \ldots, \tilde{g}_s)$, wobei die g_i wie im Erweiterungssatz (Satz 1.56) definiert sind. Mit dem Erweiterungssatz existiert nun ein $c_n \in K$ mit $(c_1, \ldots, c_n) \in V(\tilde{I})$, was ein Widerspruch zu $V(\tilde{I}) = \emptyset$ ist, also gilt $\tilde{I} = \tilde{\mathbb{P}}$, was $\tilde{1} \in \tilde{I}$, damit auch $1 \in I$ und somit $I = \mathbb{P}$ bedeutet.

□

Satz 1.59 (Hilbertscher Nullstellensatz, starke Version)**.** *Sei K ein algebraisch abgeschlossener Körper, $I \trianglelefteq \mathbb{P}$ ein Ideal und $f \in \mathbb{P}$. f verschwindet genau dann auf $V(I)$, d. h. $f(c_1, \ldots, c_n) = 0$ für alle $(c_1, \ldots, c_n) \in V(I)$, wenn ein $m \in \mathbb{N}$ existiert, sodass $f^m \in I$ ist.*

Beweis. ($\Leftarrow$):
Gilt $f^m \in I$, folgt für alle $(c_1, \ldots, c_n) \in V(I)$, dass $\big(f(c_1, \ldots, c_n)\big)^m = 0$. Daraus folgt $f(c_1, \ldots, c_n) = 0$.

($\Rightarrow$): Sei $I = \mathrm{Id}(f_1, \ldots, f_s)$ für passende $f_1, \ldots, f_s \in I$. Sei Y eine neue Variable und $\tilde{I} := \mathrm{Id}(f_1, \ldots, f_s, 1 - Yf) \trianglelefteq K[X_1, \ldots, X_n, Y]$. Nehmen wir $V(\tilde{I}) \neq \emptyset$ an und sei $(c_1, \ldots, c_n, y) \in V(\tilde{I})$. Dann gilt $f_1(c_1, \ldots, c_n) = \cdots = f_s(c_1, \ldots, c_n) = 0$, also $(c_1, \ldots, c_n) \in V(I)$. Laut Voraussetzung gilt

$$f(c_1, \ldots, c_n) = 0,$$

und daraus folgt $1 - y \cdot 0 = 0$, was ein Widerspruch ist, also gilt $V(\tilde{I}) = \emptyset$.

Wegen Satz 1.58 ist $1 \in \tilde{I}$. Folglich existieren $p_1, \ldots, p_{s+1} \in K[X_1, \ldots, X_n, Y]$ mit

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, Y) f_i(X_1, \ldots, X_n) + \\ + (1 - Y f(X_1, \ldots, X_n)) p_{s+1}(X_1, \ldots, X_n, Y).$$

Setzen wir

$$Y = \frac{1}{f(X_1, \ldots, X_n)},$$

dann resultiert

$$1 = \sum_{i=1}^{s} p_i \left(X_1, \ldots, X_n, \frac{1}{f} \right) f_i(X_1, \ldots, X_n).$$

Nehmen wir f^m für ein passendes m als gemeinsamen Nenner, dann erhalten wir

$$f^m = \sum_{i=1}^{s} f^m p_i \left(X_1, \ldots, X_n, \frac{1}{f} \right) f_i(X_1, \ldots, X_n)$$

und es folgt $f^m \in \mathrm{Id}(f_1, \ldots, f_s) = I$ wegen $f^m p_i \left(X_1, \ldots, X_n, \frac{1}{f} \right) \in K[X_1, \ldots, X_n]$. □

1.11.4 Lösung von Gleichungssystemen durch Gröbner-Basen

Proposition 1.60. *Sei $I \trianglelefteq \mathbb{P}$ ein Ideal und G eine reduzierte* Gröbner-*Basis bezüglich einer beliebigen Termordnung. Dann gilt*

1. *Die Nullstellenmenge von I ist genau dann leer, wenn $G = \{1\}$ gilt.*
2. *Folgende Aussagen sind äquivalent:*
   (a) *$V(I)$ ist endlich.*
   (b) *Es existieren $g_1, \ldots, g_n \in G$ und $d_1, \ldots, d_n \in \mathbb{N}_0$, sodass $\mathrm{LPP}(g_i) = X_i^{d_i}$ für $1 \leq i \leq n$ gilt.*
   (c) *$\mathbb{P}/I$ hat endliche K-Vektorraum-Dimension.*

Beweis. 1. Mit der schwachen Version des Hilbertschen Nullstellensatzes (Satz 1.58) folgt sofort $\mathrm{RGB}(\mathbb{P}) = \{1\}$.

2. (a) ⇒ (b)
   Sei $V(I) = \{(c_{1j}, \ldots, c_{nj}) \mid 1 \leq j \leq N\}$. Wir definieren

$$f_i := \prod_{j=1}^{N} (X_i - c_{ij})$$

und damit verschwindet f_i auf $V(I)$. Nach der starken Version des Hilbertschen Nullstellensatzes (Satz 1.59) existiert ein $m_i \in \mathbb{N}$, sodass $f_i^{m_i} \in I$ gilt. Wir betrachten nun $\mathrm{LPP}(f_i^{m_i}) = X_i^{N m_i}$, und da G eine Gröbner-Basis ist, folgt $f_i^{m_i} \longrightarrow_G^\star 0$ wegen des Hauptsatzes über Gröbner-Basen (Satz 1.37). Um $\mathrm{LPP}(f_i^{m_i})$ eliminieren zu können, muss es ein $g_i \in G$ mit der angegebenen Eigenschaft geben.

   (b) ⇒ (c)

   Sei $N := \mathrm{span}\{X_1^{a_1} \ldots X_n^{a_n} \mid 0 \leq a_i < d_i\}$. Wir betrachten die Abbildung $f : N \to \mathbb{P}/I$ mit $p \mapsto p + I$. Diese Abbildung f ist als Hintereinanderausführung der Inklusion von N in $\mathbb{P}$ (jedenfalls ein Vektorraumhomomorphismus) und der Projektion von $\mathbb{P}$ auf $\mathbb{P}/I$ (ein

Ringhomomorphismus, der wegen $K \subseteq \mathbb{P}$ auch ein K-Vektorraumhomomorphismus ist) eine K-lineare Abbildung.

Wir behaupten, dass f surjektiv ist: Sei nämlich $p + I \in \mathbb{P}/I$ und $p_0 = \mathrm{RF}_g(p)$. Dann ist $p \equiv p_0 \pmod{I}$ und damit $p + I = p_0 + I$. Es bleibt zu zeigen, dass $p_0 \in N$. Andernfalls gäbe es ein $t = X_1^{b_1} \dots X_n^{b_n} \in \mathrm{S}(p_0)$ und ein j mit $b_j \geq d_j$. Dann gäbe es ein ein $p_0' \in \mathbb{P}$ mit $p_0 \longrightarrow_{g_j,t} p_0'$, was ein Widerspruch zur Reduziertheit von p_0 ist und damit die Surjektivität von f beweist.

Somit ist $\mathbb{R}/I$ als epimorphes Bild des endlich-dimensionalen K-Vektorraums N ebenfalls endlich-dimensional.

(c) $\Rightarrow$ (a)

Betrachten wir $\{1+I, X_i+I, X_i^2+I, \dots\}$, dann existiert ein d_i, sodass $1+I, X_i+I, \dots, X_i^{d_i}+I$ linear abhängig sind. Damit gibt es ein

$$0 \neq g_i = \sum_{j=0}^{d_i} a_{ij} X_i^j \in I.$$

Sei $(c_1, \dots, c_n) \in V(I)$, dann resultiert $g_i(c_i) = 0$. Also kommt c_i unter den endlich vielen Nullstellen von g_i vor, und somit gibt es nur endlich viele c_i, die auftreten.

□

Proposition 1.61. *Sei K ein algebraisch abgeschlossener Körper, $I \trianglelefteq \mathbb{P}$ ein Ideal und G eine reduzierte* Gröbner*-Basis bezüglich der lexikographischen Termordnung mit $X_1 \prec \dots \prec X_n$. Weiters sei $V(I)$ endlich. Dann hat G folgendes Aussehen:*

$$\begin{gathered} g_1(X_1) \\ g_{21}(X_1, X_2), \dots, g_{2k_2}(X_1, X_2) \\ \vdots \\ g_{n1}(X_1, \dots, X_n), \dots, g_{nk_n}(X_1, \dots, X_n), \end{gathered}$$

wobei $k_i \geq 1$ für $2 \leq i \leq n$. Das Gleichungssystem kann durch den Erweiterungsprozess gelöst werden.

Beweis. Die Existenz von mindestens einem Polynom in jeder Zeile folgt aus Proposition 1.60. Damit existiert ein g_i mit $\mathrm{LPP}(g_i) = X_i^{d_i}$ für ein passendes d_i und wegen der Definition der lexikographischen Termordnung folgt $g_i \in K[X_1, \dots, X_i]$.

Da G eine reduzierte Gröbner-Basis ist, gibt es nur ein Polynom in der ersten Zeile.

Der Erweiterungsschritt nach dem Erweiterungssatz (Satz 1.56) ist möglich, da es nach Proposition 1.60 ein $g_i \in G$ mit $g_i = 1 \cdot X_i^{d_i} +$ niedere X_i-Terme gibt. □

Beispiel 1.62. Man löse das Gleichungssystem $xy = z, xz = y, yz = x$. Zuerst berechnen wir die Gröbner-Basis bezüglich der lexikographischen Termordnung:

```
> eqns:={x*y-z,x*z-y,y*z-x}:
> with(Groebner):
> G:=gbasis(eqns,plex(x,y,z));
```

$$G := [-z + z^3, -y + yz^2, y^2 - z^2, -yz + x]$$

```
> factor(G[1]);
```

$$z(z-1)(z+1)$$

Nun müssen wir eine Fallunterscheidung für $z = 0, z = 1, z = -1$ vornehmen, und es ergibt sich die Lösungsmenge

$$[\{z = 1, y = 1, x = 1\}, \{z = 1, y = -1, x = -1\}, \{y = 1, x = -1, z = -1\},$$
$$\{x = 1, y = -1, z = -1\}, \{x = 0, y = 0, z = 0\}].$$

1.12 Weitere Anwendung — Färben von Graphen

In diesem Unterkapitel zeigen wir die Anwendung von GRÖBNER-Basen auf ein Problem aus der Graphentheorie, nämlich auf die Färbbarkeit eines Graphen mit 3 Farben.

Gegeben sei ein Graph G mit n Knoten, wobei von jedem Knoten mindestens eine Kante ausgeht. Nun sollen die Knoten so mit 3 Farben gefärbt werden, dass keine zwei Knoten, die durch eine Kante verbunden sind, dieselbe Farbe haben.

Sei $\zeta = \mathrm{e}^{\frac{2\pi\,\mathrm{i}}{3}} \in \mathbb{C}$ eine dritte Einheitswurzel, dann wählen wir die dritten Einheitswurzeln $1, \zeta, \zeta^2$ für die drei Farben. Bezeichnet X_i den i-ten Knoten, so muss dieser in $1, \zeta$ oder ζ^2 gefärbt sein, und es gelten die n Gleichungen

$$X_i^3 = 1$$

für $i = 1, \ldots, n$. Sind die beiden Knoten X_i und X_j mit einer Kante verbunden, so müssen sie verschieden gefärbt sein. Es folgt

$$0 = X_i^3 - X_j^3 = (X_i - X_j)(X_i^2 + X_iX_j + X_j^2).$$

Da $X_i - X_j \neq 0$ gelten muss, da die beiden Knoten ansonsten gleich gefärbt wären, erhalten wir

$$X_i^2 + X_iX_j + X_j^2$$

als notwendige und hinreichende Bedingung dafür, dass X_i und X_j verschieden gefärbt sind.

Sei

$$I = \mathrm{Id}(\{X_i^3 - 1 \mid 1 \leq i \leq n\} \cup \{X_i^2 + X_iX_j + X_j^2 \mid (i,j) \in E(G)\}),$$

dann folgt

Satz 1.63. *Der Graph G ist genau dann 3-färbbar, wenn $V(I) \neq \emptyset$ gilt.*

Wegen Proposition 1.60 ist die Aussage des Satzes mit $\mathrm{RGB}(F) \neq \{1\}$ äquivalent, wenn I das von F erzeugte Ideal ist.

Beispiel 1.64. Der Graph $G = (V, E)$ sei durch $V := \{1, \ldots, 8\}$ und $E := \{(1,2), (1,5), (1,6), (2,3), (2,4), (2,8), (3,4), (3,8), (4,5), (4,7), (5,6), (5,7), (6,7), (7,8)\}$ gegeben.

Kann der Graph mit drei Farben derartig gefärbt werden, dass keine zwei benachbarten Punkte die gleiche Farbe haben? Wenn ja, gebe man eine Färbung an.

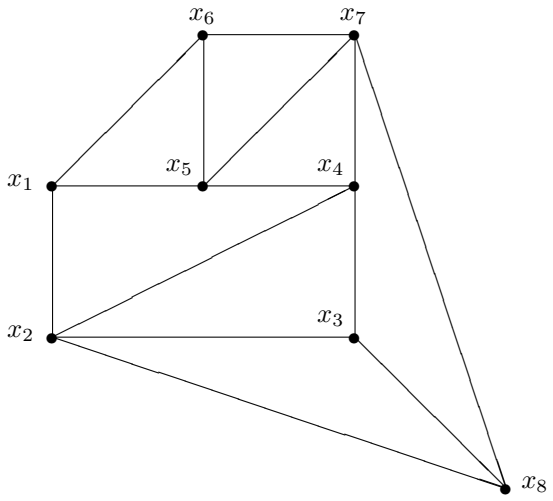


Abbildung 1.1: Der Graph G

Wir erhalten die Polynome $X_i^3 - 1$ für $i = 1, \ldots, 8$ und $X_i^2 + X_i X_j + X_j^2$ für die Paare $(i, j) \in E(G)$. Nun können wir mit Maple die GRÖBNER-Basis H zu dem von den obigen Polynomen erzeugten Ideal bezüglich der lexikographischen Termordnung berechnen. Dazu bezeichne `G` die Menge $X_i^2 + X_i X_j + X_j^2$ für die Paare $(i, j) \in E(G)$:

```
> with(Groebner):
> F := [seq(X[i]^3-1,i=1..8),seq(G[j],j=1..14)]:
> var:=[seq(X[i],i=1..8)]:
> H:=gbasis(F,plex(op(var)));
```

$$H := [X_1 - X_7, X_2 + X_7 + X_8, X_3 - X_7, X_4 - X_8, X_5 + X_7 + X_8,$$
$$X_6 - X_8, X_7^2 + X_7 X_8 + X_8^2, X_8^3 - 1]$$

Da $1 \notin H$ ist, resultiert $V(I) \neq \emptyset$, also ist der Graph G nach Satz 1.63 3-färbbar. Mit Hilfe der GRÖBNER-Basis können wir sofort sagen, wie der Graph gefärbt sein muss. Nehmen wir die 3 Farben rot, blau und grün.

Zuerst müssen wir für X_8 eine Farbe wählen, da dies die einzige allein vorkommende Variable in H ist. Sei also X_8 rot. Dann muss X_7 eine andere Farbe haben, da $X_7^2 + X_7 X_8 + X_8^2 \in H$ ist. Wir wählen blau. Da die Polynome $X_1 - X_7$ und $X_3 - X_7$ in H sind, müssen auch X_1 und X_3 blau sein. Analog erhalten wir rot für X_4 und X_6. Schließlich bleibt für X_2 und X_5 noch grün, da die Polynome $X_2 + X_7 + X_8$ bzw. $X_5 + X_7 + X_8$ in H liegen.

Im gefärbten Graph (Abbildung 1.2) repräsentieren die Zeichen •,♦ bzw. ■ die Farben rot, blau bzw. grün.

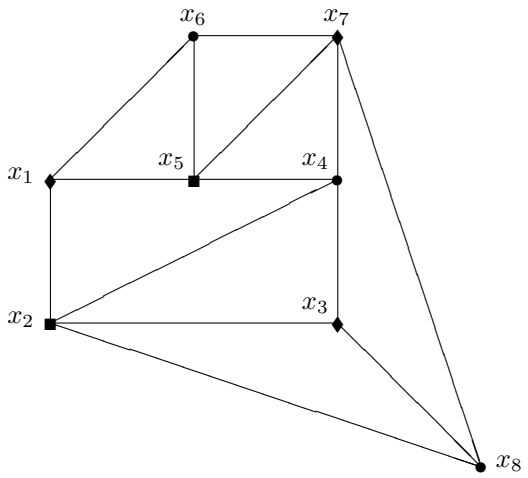


Abbildung 1.2: Der gefärbte Graph G

In diesem Beispiel war aufgrund der Beschaffenheit der GRÖBNER-Basis die Färbung bis auf eventuelle Permutationen der Farben eindeutig. Dies muss jedoch nicht immer so sein[2].

1.13 Ganzzahlige Optimierung und Gröbner-Basen

In diesem Abschnitt soll skizziert werden, wie sich Gröbner-Basis-Ideen auf die ganzzahlige Optimierung anwenden lassen. Man kann ganzzahlige Optimierungsprobleme auch direkt in Idealprobleme in Polynomringen übersetzen und dort Gröbner-Basen anwenden, vgl. ADAMS [1]. Hier soll

[2] vgl. ADAMS [1], Seite 104f

allerdings eine Fassung vorgestellt werden, die ohne Polynome auskommt. Es wird hier keine allgemeine Theorie entwickelt, sondern lediglich eine Möglichkeit zur Lösung skizziert. Der Abschnitt folgt HEMMECKE˜[9].

Definition 1.65. Ein ganzzahliges Programm ist eine Optimierungsaufgabe

$$\mathrm{IP}(A)_{b,c} : \min\{c^t x : Ax = b, x \in \mathbb{N}_0^n\},$$

wobei $c \in \mathbb{Z}^n$, $A \in \mathbb{Z}^{m\times n}$ und $b \in \mathbb{Z}^m$.

Beispiel 1.66. Transport von Gütern A, B und C (in Containern) mit einem Flug. Folgende Restriktionen:

	A	B	C	Maximum
Volumen	2	6	3	23
Gewicht	5	4	4	20
Wert	60	10	10	270
Einnahmen	3	5	4	

Wie viele Container sollen mitgenommen werden?

Seien x_1, x_2, x_3 die Anzahl der Container von A, B, C.

$$\begin{aligned} \max\ & 3x_1 + 5x_2 + 4x_3 \\ \text{wobei } & 2x_1 + 6x_2 + 3x_3 + x_4 \leq 23 \\ & 5x_1 + 4x_2 + 4x_3 + x_5 \leq 20 \\ & 6x_1 + 1x_2 + 1x_3 + x_6 \leq 27 \\ & x_1, x_2, x_3, x_4, x_5, x_6 \in \mathbb{N}_0 \end{aligned}$$

Definition 1.67. Eine Testmenge $T \subseteq \mathbb{Z}^n$ für $\mathrm{IP}(A)$ ist eine Menge mit folgender Eigenschaft:

Sei $b \in \mathbb{Z}^m$, $c \in \mathbb{Z}^n$ und $x \in \mathbb{N}_0^n$ mit $Ax = b$ (d.h. x „zulässig“). Dann ist x genau dann optimal für $\mathrm{IP}(A)_{b,c}$, wenn es *kein* $t \in T$ gibt, sodass

- $x - t$ ist zulässig (d.h. $A(x-t) = b$, $x - t \in \mathbb{N}_0^n$) und
- $c^t(x-t) < c^t x$ (d.h. $c^t t > 0$).

Algorithmus 1.2 Augmentierungsalgorithmus

Gegeben: A, b, c, T Testmenge für $\mathrm{IP}(A)$ und $x \in \mathbb{N}_0^n$ zulässig
Gesucht: Optimallösung x^* für $\mathrm{IP}(A)_{b,c}$

```
while ∃ t ∈ T mit c^t t > 0 und x − t zulässig do
    x := x − t
end while
Return(x).
```

Proposition 1.68. *Falls* $\mathrm{IP}(A)_{b,c}$ *eine Optimallösung besitzt, so löst Algorithmus˜1.2 das Problem* $\mathrm{IP}(A)_{b,c}$ *in endlich vielen Schritten.*

Definition 1.69. Seien $r, s \in \mathbb{Z}^n$. Schreibe $r \sqsubseteq s$, falls $r^{(k)}s^{(k)} \geq 0$ und $\left|r^{(k)}\right| \leq \left|s^{(k)}\right|$ für $k = 1, \ldots, n$ gilt.

Definition 1.70. $G \subseteq \operatorname{Ker} A := \{x \in \mathbb{Z}^n : Ax = 0\}$ hat die *Positive-Summen-Eigenschaft*, wenn jedes $z \in \operatorname{Ker} A$ als

$$z = \sum_{i=1}^{k} a_i g_i$$

mit $a_i \in \mathbb{N}$, $g_i \in G$ und $g_i \sqsubseteq z$ dargestellt werden kann.

Satz 1.71. *Hat G die Positive-Summen-Eigenschaft, so ist G Testmenge.*

Satz 1.72. *Sei $G \subseteq \operatorname{Ker} A$ mit folgenden Eigenschaften:*

- *Für alle $x \in \operatorname{Ker} A$ gibt es eine Darstellung*

$$x = \sum_{i=1}^{k} a_i g_i, \qquad a_i \in \mathbb{N}, g_i \in G.$$

- *Für alle $u, v \in G$ gibt es eine Darstellung*

$$u + v = \sum_{i=1}^{l} b_i h_i, \qquad b_i \in \mathbb{N}, h_i \in G, h_i \sqsubseteq u + v.$$

Dann hat G die Positive-Summen-Eigenschaft.

Algorithmus 1.3 $\mathrm{NF}_G(s)$

Gegeben: $s \in \mathbb{Z}^n$, $G \subseteq \mathbb{Z}^n$, $0 \notin G$
Gesucht: 0, falls es eine Darstellung $s = \sum_{i=1}^{l} a_i g_i$ mit $a_i \in \mathbb{N}$, $g_i \in G$ und $g_i \sqsubseteq s$ gibt; t, falls es eine Darstellung $s = \sum_{i=1}^{l} a_i g_i$, $a_i \in \mathbb{N}$, $g_i \in G \cup \{t\}$ und $g_i \sqsubseteq s$ gibt.

```
while ∃ t ⊑ s, t ∈ G do
    s := s − t
end while
Return(s)
```

Proposition 1.73. *Algorithmus˜1.3 terminiert nach endlich vielen Schritten und ist korrekt.*

Algorithmus 1.4 Complete(F)

Gegeben: $F \subseteq \mathbb{Z}^n$ mit der ersten Eigenschaft von Satz˜1.72
Gesucht: $G \subseteq \mathbb{Z}^n$ mit beiden Eigenschaften von Satz˜1.72

```
G := F
S := {f + g : f, g ∈ G}
while S ≠ ∅ do
    Wähle s ∈ S.
    S := S \ {s}
    t := NF_G(s)
    if t ≠ 0 then
        S := S ∪ {f + t : f ∈ G}
        G := G ∪ {t}
    end if
end while
```

Proposition 1.74. *Algorithmus˜1.4 ist korrekt und terminiert in endlich vielen Schritten.*

Für $u \in \mathbb{Z}$ sei $u^- := \max\{0, -u\}$, für $z \in \mathbb{Z}^n$ ist z^- komponentenweise definiert.

Proposition 1.75. *Algorithmus˜1.5 terminiert in endlich vielen Schritten und ist korrekt.*

Algorithmus 1.5 Bestimmen zulässiger Ausgangslösungen

Gegeben: $z \in \mathbb{Z}^n$ mit $Az = b$, Testmenge T für IP(A)
Gesucht: $z \in \mathbb{N}_0^n$ mit $Az = b$, falls existent, sonst „FAIL“

while es gibt ein $t \in T$, sodass

$$\left\|(z-t)^-\right\|_1 < \left\|z^-\right\|_1$$
$$(z-t)^{(k)} \geq 0, \text{ falls } z^{(k)} \geq 0$$

do
  $z := z - t$
end while
if $\|z^-\|_1 > 0$ **then**
  Return(„FAIL“)
else
  Return(z)
end if

Kapitel 2

Hypergeometrische Identitäten

2.1 Einführung

2.2 Hypergeometrische Reihen

Definition 2.1. Die Reihe $\sum_{k=0}^{\infty} t_k$ heißt *hypergeometrische Reihe*, wenn $t_0 = 1$ und

$$\frac{t_{k+1}}{t_k} = \frac{P(k)}{Q(k)}$$

für gewisse Polynome $P(k)$ und $Q(k)$.

2.3 Die Hypergeometrische Datenbank

2.4 Sister Celine's Method

2.5 Rekursionen für Hypergeometrische Terme

Definition 2.2. $F(n,k)$ heißt *eigentlicher hypergeometrischer Term*, wenn man

$$F(n,k) = P(n,k)\frac{\prod_{s=1}^{\alpha}(a_s n + b_s k + c_s)!}{\prod_{s=1}^{\beta}(u_s n + v_s k + w_s)!} \cdot x^k$$

schreiben kann, wobei $P(n,k)$ ein Polynom, a_s, b_s, c_s, u_s, v_s, w_s feste ganze Zahlen, $\alpha, \beta \in \mathbb{N}_0$ und x eine Unbestimmte ist.

$F(n,k)$ heißt wohldefiniert, wenn kein $a_s n + b_s k + c_s \in -\mathbb{N}_0$.

$F(n,k) = 0$, wenn es wohldefiniert ist und $P(n,k) = 0$ oder ein $u_s n + v_s k + w_s \in -\mathbb{N}_0$.

Satz 2.3. *Sei $F(n,k)$ eigentlicher hypergeometrischer Term. Dann gibt es $I, J \in \mathbb{N}$ und Polynome $a_{ij}(n)$, nicht alle 0, sodass die Rekursion*

$$\sum_{i=0}^{I}\sum_{j=0}^{J} a_{ij} F(n-j, k-i) = 0$$

für alle (n,k), an denen $F(n,k) \neq 0$ und für die alle auftretenden Werte von F wohldefiniert sind, gilt.

Die Werte I, J können wie folgt gewählt werden:

$$J^* = \sum_{s=1}^{\alpha} |b_s| + \sum_{s=1}^{\beta} |v_s|$$
$$I^* = 1 + \deg P + J^* \left(-1 + \sum_{s=1}^{\alpha} |a_s| + \sum_{s=1}^{\beta} |u_s| \right).$$

2.6 Unbestimmte Summation — Der Algorithmus von Gosper

2.6.1 Einführung

2.6.2 Überblick

$$\begin{aligned} s_n &= \sum_{k=0}^{n-1} t_k \\ \frac{t_{n+1}}{t_n} &= r(n) && r(n) \text{ rational} \\ z_{n+1} - z_n &= t_n && z_n \text{ hypergeometrisch} \\ z_n &= y(n) t_n && y(n) \text{ rational} \end{aligned}$$

Satz 2.4. *Sei K ein Körper der Charakteristik 0, $0 \neq r \in K(n)$ eine rationale Funktion. Dann gibt es Polynome $a, b, c \in K[n]$, sodass b und c normiert sind,*

$$r(n) = \frac{a(n)}{b(n)} \frac{c(n+1)}{c(n)},$$

wobei

1. $\mathrm{ggT}(a(n), b(n+h)) = 1$ *für alle* $h \in \mathbb{N}_0$
2. $\mathrm{ggT}(a(n), c(n)) = 1$
3. $\mathrm{ggT}(b(n), c(n+1)) = 1$.

$$\begin{aligned} y(n) &= \frac{b(n-1)x(n)}{c(n)} && x(n) \text{ Polynom} \\ a(n)x(n+1) - b(n-1)x(n) &= c(n) \end{aligned}$$

Algorithmus 2.1 Gosper-Algorithmus, Überblick

Gegeben: t_n hypergeometrischer Term
Gesucht: z_n hypergeometrischer Term mit $z_{n+1} - z_n = t_n$.
$r(n) := t_{n+1}/t_n$
Zerlege $r(n) = a(n)/b(n) \cdot c(n+1)/c(n)$, wobei $\mathrm{ggT}(a(n), b(n+h)) = 1$ für alle $h \in \mathbb{N}_0$.
Suche polynomiale Lösung $x(n)$ von $a(n)x(n+1) - b(n-1)x(n) = c(n)$.
$z_n := \frac{b(n-1)}{c(n)} x(n) t_n$.

2.6.3 Normalform rationaler Funktionen

Algorithmus 2.2 Gosper-Algorithmus, Schritt 2

Gegeben: $r(n)$ rationale Funktion
Gesucht: Zerlegung nach Satz˜2.4.

Schreibe $r(n) = Z \cdot \frac{f(n)}{g(n)}$ für eine Konstante Z und normierte Polynome $f,\ g \in K[n]$ mit $\mathrm{ggT}(f(n), g(n)) = 1$.
$\{h_1 < \cdots < h_N\} := \{h \in \mathbb{N} : \mathrm{Res}_n(f(n), g(n+h)) = 0\}$
$p_0(n) := f(n)$, $q_0(n) := g(n)$
for $j = 1$ to N **do**
  $s_j(n) := \mathrm{ggT}(p_{j-1}(n), q_{j-1}(n+h_j))$
  $p_j(n) := p_{j-1}(n)/s_j(n)$
  $q_j(n) := q_{j-1}(n)/s_j(n-h_j)$
end for
$a(n) = Zp_N(n)$
$b(n) = q_N(n)$
$$c(n) = \prod_{j=1}^{N} \prod_{i=1}^{h_j} s_j(n-i)$$

2.6.4 Schritt 3 des Gosper-Algorithmus

Algorithmus 2.3 Gosper-Algorithmus, Schritt 3

Gegeben: $a(n)$, $b(n)$, $c(n) \in K[n]$
Gesucht: $x \in K[n]$, sodass $a(n)x(n+1) - b(n-1)x(n) = c(n)$, oder Beweis der Nichtexistenz.

Wenn $\mathrm{LT}(a(n)) = \mathrm{LT}(b(n))$, dann schreibe

$$a(n) = \lambda n^k + An^{k-1} + \dots$$
$$b(n-1) = \lambda n^k + Bn^{k-1} + \dots$$

und setze

$$D := \left\{ \frac{B-A}{\lambda}, \deg c - \deg a + 1 \right\},$$

sonst setze

$$D := \{\deg c - \max\{\deg a, \deg b\}\}.$$

$D := D \cap \mathbb{N}_0$. Wenn $D = \emptyset$, dann ist Lösung unmöglich, sonst setze $d = \max D$.
Setze $x(n) = \sum_{l=0}^{d} e_l n^l$ und löse Gleichung durch Koeffizientenvergleich. Wenn unmöglich, dann unlösbar.

2.6.5 Linearkombinationen von hypergeometrischen Termen

Definition 2.5. Zwei hypergeometrische Terme s_n und t_n heißen ähnlich, wenn s_n/t_n eine rationale Funktion in n ist.

Ähnlichkeit von hypergeometrischen Termen ist eine Äquivalenzrelation.

Proposition 2.6. *Sei s_n ein nicht-konstanter hypergeometrischer Term. Dann ist $s_{n+1} - s_n$ ein hypergeometrischer Term, der ähnlich zu s_n ist.*

Proposition 2.7. *Seien s_n und t_n hypergeometrische Terme mit $s_n + t_n \neq 0$. Dann ist $s_n + t_n$ genau dann ein hypergeometrischer Term, wenn s_n und t_n ähnlich sind.*

Daher kann jede Summe einer festen Anzahl von hypergeometrischen Termen als Summe nicht-ähnlicher hypergeometrischer Terme geschrieben werden.

Satz 2.8. *Seien $t_n^{(1)}, \ldots, t_n^{(k)}$ hypergeometrische Terme mit*

$$\sum_{i=1}^{k} t_n^{(i)} = 0.$$

Dann gibt es $1 \leq i < j \leq k$, sodass $t_n^{(i)}$ und $t_n^{(j)}$ ähnlich sind.

Satz 2.9. *Sei t_n ein hypergeometrischer Term. Wenn es keinen hypergeometrischen Term z_n mit $t_n = z_{n+1} - z_n$ gibt, so gibt es auch keine Linearkombination $z_n^{(1)} + \cdots + z_n^{(r)}$ für ein festes r, sodass $t_n = (z_{n+1}^{(1)} + \cdots + z_{n+1}^{(r)}) - (z_n^{(1)} + \cdots + z_n^{(r)})$.*

2.7 Bestimmte Summation. Der Zeilberger-Algorithmus

2.7.1 Einführung

Definition 2.10. Sei $F : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}; (n,k) \mapsto F(n,k)$. Dann definiere

$$(NF)(n,k) := F(n+1,k), \qquad (KF)(n,k) := F(n,k+1).$$

(Vorwärtsshift in n bzw. k.)

2.7.2 Existenz einer Teleskop-Rekursion

Satz 2.11. *Sei $F(n,k)$ ein eigentlicher hypergeometrischer Term. Dann gibt es ein $J \geq 0$, Polynome $a_j(n)$ für $0 \leq j \leq J$, nicht alle null, und eine Funktion $G(n,k)$, sodass $F(n,k)$ der Rekursion*

$$\sum_{j=0}^{J} a_j(n) F(n+j,k) = G(n,k+1) - G(n,k)$$

genügt und $G(n,k)/F(n,k)$ eine rationale Funktion in n und k ist.

2.7.3 Zeilberger-Algorithmus

2.7.4 Beispiele

2.7.5 Die Wilf-Zeilberger-Methode

2.8 Lösen von Rekursionen — Der Algorithmus von Petkovšek (1992)

2.8.1 Einführung

Definition 2.12. $y(n)$ heißt *geschlossene (hypergeometrische) Form*, wenn es eine absolute Konstante r und hypergeometrische Terme $t_n^{(1)}, \ldots, t_n^{(r)}$ gibt, sodass

$$y(n) = t_n^{(1)} + \cdots + t_n^{(r)}.$$

Algorithmus 2.4 Zeilberger-Algorithmus

Gegeben: J (Ordnung der Rekursion), $F(n,k)$
Gesucht: $a_0(n),\ldots,a_J(n)$ und $G(n,k)$ mit

$$t_k := \sum_{j=0}^{J} a_j(n)F(n+j,k) = G(n,k+1) - G(n,k).$$

$$\frac{r_1(n,k)}{r_2(n,k)} = \frac{F(n,k+1)}{F(n,k)}$$
$$\frac{s_1(n,k)}{s_2(n,k)} = \frac{F(n,k)}{F(n-1,k)}$$
$$p_0(k) = \sum_{j=0}^{J} a_j \left[\prod_{i=0}^{j-1} s_1(n+j-i,k) \prod_{r=j+1}^{J} s_2(n+r,k)\right]$$
$$r(k) = r_1(n,k)\prod_{r=1}^{J} s_2(n+r,k)$$
$$s(k) = r_2(n,k)\prod_{r=1}^{J} s_2(n+r,k+1)$$

Zerlege

$$\frac{r(k)}{s(k)} = \frac{p_2(k)}{p_3(k)}\frac{p_1(k+1)}{p_1(k)},$$

wobei $\mathrm{ggT}(p_2(k),p_3(k+h)) = 1$ für alle $h \in \mathbb{N}_0$.
Löse

$$p_2(k)x(k+1) - p_3(k-1)x(k) = p_0(k)p_1(k)$$

für ein Polynom $x(k)$. (Gradabschätzung, unbestimmter Ansatz für $x(k)$, Koeffizientenvergleich)
if $x(k)$ existiert **then**

$$G(n,k) = \frac{p_3(k-1)}{p_0(k)p_1(k)}x(k)t_k$$

else
Keine Rekursion für dieses J.
end if

Algorithmus 2.5 Poly

Gegeben: $p_1,\ldots,p_r,f$ Polynome in n.
Gesucht: Polynom $y(n)$, sodass $Ly = f$, wobei $L := \sum_{i=0}^{r} p_i N^i$, wenn existiert.
for all $0 \le j \le r$ **do**
$q_j = \sum_{i=j}^{r} \binom{i}{j} p_i$
end for
$b := \max_{0\le j\le r}(\deg q_j - j)$
$$\alpha(x) := \sum_{\deg q_j - j = b} \mathrm{LC}(q_j)x^{\underline{j}}$$
$d_1 := \max\{x \in \mathbb{N}_0 : \alpha(x) = 0\}$
$d := \max\{-b-1, d_1, \deg f - b\}$
Löse $Ly = f$ mittels unbestimmten Ansatzes

$$y(n) := \sum_{i=0}^{d} e_i n^i.$$

2.8.2 Polynomiale Lösungen

2.8.3 Bestimmen hypergeometrischer Lösungen

Algorithmus 2.6 Hyper

Gegeben: $p_1, \ldots, p_r$ Polynome in n.
Gesucht: Hypergeometrischer Term $y(n)$, sodass $Ly = 0$, wobei $L := \sum_{i=0}^{r} p_i N^i$, wenn existent.
for all normierte Faktoren $a(n)$ von $p_0(n)$ und $b(n)$ von $p_r(n-r+1)$ **do**
for all $0 \le i \le r$ **do**

$$P_i(n) := p_i(n) \prod_{j=0}^{i-1} a(n+j) \prod_{j=i}^{r-1} b(n+j)$$

end for
$m := \max_{0 \le i \le r} \deg P_i(n)$
$\alpha_i := \mathrm{C}(P_i(n), n^m)$
$\beta(z) := \sum_{i=0}^{r} \alpha_i z^i$
for all Nullstellen $z \neq 0$ von $\beta(z) = 0$ **do**
if $\sum_{i=0}^{r} z^i P_i(n) c(n+i) = 0$ hat eine polynomiale Lösung $c(n) \neq 0$ **then**

$$S(n) := z \cdot \frac{a(n)}{b(n)} \cdot \frac{c(n+1)}{c(n)}$$

$y(n)$ ist Lösung von $y(n+1) = S(n)y(n)$.
end if
end for
end for

2.8.4 Finden geschlossener Formen

Lemma 2.13. *Seien $p_0(n), \ldots, p_d(n)$ Polynome in n, $L = \sum_{i=0}^{d} p_i(n) N^i$ und h ein hypergeometrischer Term mit $Lh \neq 0$. Dann ist Lh hypergeometrisch und ähnlich zu h.*

Satz 2.14. *Seien $p_0(n), \ldots, p_d(n)$ Polynome in n, $L = \sum_{i=0}^{d} p_i(n) N^i$ und $h = \sum_{i=1}^{r} h_n^{(i)}$ eine hypergeometrische geschlossene Form mit paarweise nicht ähnlichen $h_n^{(i)}$. Dann gilt $Lh = 0$ genau dann, wenn $Lh_n^{(i)} = 0$ für $1 \le i \le r$ gilt.*

Man kann also alle hypergeometrischen geschlossenen Formen h, die $Lh = 0$ lösen, dadurch finden, dass man alle Linearkombinationen von hypergeometrischen Termen $h_n^{(i)}$ bildet, die $Lh_n^{(i)} = 0$ lösen.

Kapitel 3

Faktorisierung von Polynomen

Sei in diesem Kapitel K immer ein Körper der Charakteristik 0 oder ein endlicher Körper der Charakteristik p für eine Primzahl p.

3.1 Quadratfreie Faktorisierung

Definition 3.1. Ein Polynom $f \in K[X]$ heißt quadratfrei, wenn es kein nicht konstantes $Q \in K[X]$ gibt, sodass $Q^2 \mid f$.

Lemma 3.2. *Sei $f \in K[X]$ ein nicht konstantes Polynom. Dann gilt $f' = 0$ genau dann, wenn K endlich ist und $f = Q^p$ für ein $Q \in K[X]$ gilt.*

Satz 3.3. *Sei $f \in K[X]$ ein nicht konstantes Polynom.*

1. *f ist genau dann quadratfrei, wenn* $\mathrm{ggT}(f, f') = 1$.
2. *Das Polynom*
$$Q = \frac{f}{\mathrm{ggT}(f, f')}$$
ist quadratfrei.

Proposition 3.4. *Algorithmus ~3.1 ist korrekt.*

3.2 Faktorisierung über endlichen Körpern

Sei $\mathbb{F}_q$ ein endlicher Körper, $f \in \mathbb{F}_q[X]$ quadratfrei mit Darstellung $f = P_1 \cdots P_r$ für irreduzible Polynome $P_j \in \mathbb{F}_q[X]$.

Satz 3.5. *Die Menge V_f der Polynome $Q \in \mathbb{F}_q[X]$ mit* $\deg Q < \deg f$ *und*
$$Q^q \equiv Q \pmod{f} \tag{3.1}$$
ist ein r-dimensionaler $\mathbb{F}_q$-Vektorraum.

Es gibt eine Bijektion zwischen $\mathbb{F}_q^r$ und V_f: Dem Tupel $(\alpha_1, \ldots, \alpha_r) \in \mathbb{F}_q^r$ entspricht jenes Polynom $Q \in V_f$ mit
$$Q \equiv \alpha_i \pmod{P_i}.$$

Proposition 3.6. *Sei $Q_f = (q_{k\ell})_{0 \le k,\ell \le n-1} \in \mathbb{F}_q^{n \times n}$ jene Matrix, sodass*
$$X^{\ell q} \equiv q_{0\ell} + \cdots + q_{n-1,\ell} X^{n-1} \pmod{f}.$$
Dann löst $B(x) := b_0 + \cdots + b_{n-1}X^{n-1} \in \mathbb{F}_q[X]$ die Kongruenz (3.1) genau dann, wenn $b^t = (b_0, \ldots, b_{n-1})$ ein Eigenvektor von Q_f zum Eigenwert 1 ist.

Proposition 3.7. *Der Berlekamp-Algorithmus ~3.2 ist korrekt und terminiert.*

Algorithmus 3.1 Quadratfreie Faktorisierung

Gegeben: $0 \neq f \in K[X]$

Gesucht: Quadratfreie Polynome $P_1, \ldots, P_k \in K[X]$, $\mathrm{ggT}(P_i, P_j) = 1$ für $i \neq j$ und $e_1, \ldots, e_k$ positive ganze Zahlen, sodass

$$f = P_1^{e_1} \cdots P_k^{e_k}.$$

$C_1 = \mathrm{ggT}(f, f')$
$D_1 = f/C_1$
$n = 1$
while $D_n \neq 1$ **do**
  $D_{n+1} = \mathrm{ggT}(C_n, D_n)$
  $C_{n+1} = C_n/D_{n+1}$
  $P_n = D_n/D_{n+1}$
  $e_n = n$
  $n = n + 1$
end while
$k = n$
if $C_n' = 0$ und C_n nicht konstant **then**
  Bestimme das maximale $e \geq 1$, sodass es ein $H \in K[X]$ mit $C_n = H^{p^e}$ gibt.
  Bestimme rekursiv die quadratfreie Faktorisierung $H = \tilde{P}_1^{\tilde{e}_1} \cdots \tilde{P}_{\tilde{k}}^{\tilde{e}_{\tilde{k}}}$.
  for all $1 \leq j \leq \tilde{k}$ **do**
    $P_{k+j} = \tilde{P}_j$
    $e_{k+j} = p^e \cdot \tilde{e}_j$
  end for
  $k = k + \tilde{k}$
end if

Algorithmus 3.2 Faktorisierung von Polynomen über endlichen Körpern (Berlekamp)

Gegeben: $f \in \mathbb{F}_q[X]$ quadratfrei
Gesucht: $P_1, \ldots, P_r \in \mathbb{F}_q[X]$ irreduzibel, sodass $f = P_1 \cdots P_r$

```
n = deg f
Q_f wie in Proposition~3.6
Wähle Basis b^(1), ..., b^(r) von ker(Q_f − I_n) (Gauß-Elimination), wobei b^(1) = (1, 0, ..., 0)^t.
B_i = Σ_{j=0}^{n−1} b_j^(i) X^j.
G = {f}
for all 2 ≤ s ≤ r do
  for all α ∈ F_q do
    F = G
    G = ∅
    while F ≠ ∅ do
      Wähle g ∈ F
      F = F \ {g}
      d = ggT(B_s − α, g)
      if 1 ≤ deg d < deg g then
        G = G ∪ {d, g/d}
      else
        G = G ∪ {g}
      end if
      if |F ∪ G| = r then
        Return (F ∪ G)
      end if
    end while
  end for
end for
```

3.3 „Liften“ von Faktorisierungen

Definition 3.8. Sei R ein Ring und $f \in R[X]$ ein Polynom vom Grad n. Dann heißt

$$\mathrm{Discr}(f) = \frac{(-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, f')}{\mathrm{LC}(f)}$$

die *Diskriminante* von f.

Proposition 3.9. *Sei R ein ZPE-Ring und $f \in R[X]$. Dann ist f genau dann quadratfrei, wenn* $\mathrm{Discr}(f) \neq 0$.

Satz 3.10 (Hensel-Lifting)**.** *Seien p eine Primzahl und F, G_0, $H_0 \in \mathbb{Z}[X]$ Polynome mit folgenden Eigenschaften:*

- $\mathrm{LC}(G_0) = 1$ *und* $\deg(G_0) + \deg(H_0) = \deg(F)$.
- $p \nmid \operatorname{Res}(G_0, H_0)$ *und* $p \nmid \mathrm{LC}(F)$.
- $F \equiv G_0 \cdot H_0 \pmod{p}$.

Dann gibt es für alle $t \geq 1$ Polynome G_t und $H_t \in \mathbb{Z}[X]$ mit den Eigenschaften

- $\mathrm{LC}(G_t) = 1$ *und* $\deg(G_t) = \deg(G_0)$ *und* $\deg(H_t) = \deg(H_0)$.
- $G_t \equiv G_{t-1} \pmod{p^t}$ *und* $H_t \equiv H_{t-1} \pmod{p^t}$.
- $F \equiv G_t \cdot H_t \pmod{p^{1+t}}$.

Erfüllen weitere Polynome $\widetilde{G_t}$ und $\widetilde{H_t}$ dieselben Bedingungen, so gilt $\widetilde{G_t} \equiv G_t \pmod{p^{t+1}}$ und $\widetilde{H_t} \equiv H_t \pmod{p^{t+1}}$.

3.4 Mignotte-Schranke

Definition 3.11. Sei $f \in \mathbb{C}[X]$ ein Polynom, $f = \sum_{j=0}^{n} a_j X^j$ mit Nullstellen (inkl. Vielfachheiten) $\alpha_1, \ldots, \alpha_n$. Dann heißen

1. $\|f\| := \sqrt{\sum_{j=0}^{n} |a_j|^2}$ die Norm von f,
2. $H(f) := \max_{j=0,\ldots,n} |a_j|$ die Höhe von f,
3. $M(f) := |a_n| \cdot \prod_{j=1}^{n} \max\{1, |\alpha_j|\}$ das Mahler-Maß von f.

Lemma 3.12. $H(f) \leq \|f\| \leq \sqrt{(n+1)} H(f)$

Lemma 3.13. *Sei $f \in \mathbb{C}[X]$ und $z \in \mathbb{C}$. Dann gilt $\|(X+z)f\| = \|(\overline{z}X + 1)f\|$.*

Satz 3.14. *Sei $f \in \mathbb{C}[X]$, $\deg f = n$. Dann gilt*

$$\frac{\|f\|}{\sqrt{\binom{2n}{n}}} \leq M(f) \leq \|f\|.$$

Satz 3.15 (Mignotte)**.** *Sei $g \in \mathbb{C}[X]$ ein Teiler von $f \in \mathbb{C}[X]$ mit $m = \deg g$. Dann gilt*

$$\|g\| \leq \left|\frac{\mathrm{LC}(g)}{\mathrm{LC}(f)}\right| \sqrt{\binom{2m}{m}} \|f\|.$$

Korollar 3.16. *Seien f und g wie in Satz˜3.15. Dann gilt*

$$H(g) \leq \left|\frac{\mathrm{LC}(g)}{\mathrm{LC}(f)}\right| 2^n \|f\|.$$

Algorithmus 3.3 Hensel-Lifting

Gegeben: p, F, $G_0 = \sum_{j=0}^{r} g_j X^j$, $H_0 = \sum_{j=0}^{s} h_j X^j$ wie in Satz˜3.10, $t \geq 0$, $p \nmid \mathrm{LC}(F)$
Gesucht: G_t, $H_t \in \mathbb{Z}[X]$ mit $F \equiv G_t \cdot H_t \pmod{p^{t+1}}$

$n = \deg F$

Setze

$$M = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{r-1} & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \dots & g_{r-1} & g_r & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & g_2 & \dots & g_{r-1} & g_r \\ h_0 & h_1 & h_2 & \dots & h_{s-1} & h_s & 0 & 0 & \dots & 0 \\ 0 & h_0 & h_1 & h_2 & \dots & h_{s-1} & h_s & 0 & \dots & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & \dots & h_{s-1} & h_s & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & h_0 & h_1 & h_2 & \dots & h_{s-1} & h_s \end{pmatrix},$$

wobei die Koeffizienten von G_0 über s und die Koeffizienten von H_0 über r Zeilen wiederholt werden

for all $0 \leq k < t$ **do**

$D = (F - G_k \cdot H_k)/p^{k+1}$

$b_s = \mathrm{C}(D, X^n)$

Definiere $c_0, \dots c_{n-1}$ durch $\sum_{j=0}^{n-1} c_j X^j \equiv D - b_s X^s G_k \pmod{p}$.

Löse $(b_0, \dots, b_{s-1}, a_0, \dots, a_{r-1})M \equiv (c_0, \dots, c_{n-1}) \pmod{p}$.

$G_{k+1} = G_k + p^{k+1} \sum_{j=0}^{r-1} a_j X^j$

$H_{k+1} = H_k + p^{k+1} \sum_{j=0}^{s-1} b_j X^j$

end for

3.5 Faktorisierung in $\mathbb{Z}[X]$

Algorithmus 3.4 Berlekamp-Hensel

Gegeben: $f \in \mathbb{Z}[X]$ quadratfrei.
Gesucht: $g, h \in \mathbb{Z}[X]$ nicht konstant mit $f = g \cdot h$ oder „f ist irreduzibel über $\mathbb{Q}[X]$“

$n = \deg f$
$M = 2^{n+1} \cdot \|f\|$
Wähle Primzahl p mit $p \nmid \mathrm{Discr}(f)$ und $p \nmid \mathrm{LC}(f)$.
Wähle $t \geq 1$ mit $p^t > M$.
Zerlege $f = c \cdot f_1 \cdots f_r$ in $\mathbb{F}_p$ mit irreduziblen normierten f_j, $1 \leq j \leq r$ und einem $c \in \mathbb{F}_p$.
for all Partitionen $\{1, \ldots, r\} = S \cup T$ mit $S \neq \emptyset$ und $T \neq \emptyset$ **do**
  $G_0 = \prod_{j \in S} f_j$
  $H_0 = c \prod_{j \in T} f_j$
  Berechne (Algorithmus˜3.3) $\tilde{g} \in \mathbb{Z}[X]$ und $\tilde{h} \in \mathbb{Z}[X]$ mit $f \equiv \tilde{g} \cdot \tilde{h} \pmod{p^t}$, wobei $H(\tilde{g}) \leq p^t/2$, $H(\tilde{h}) \leq p^t/2$.
  $h = \tilde{h}/\operatorname{cont}(\tilde{h})$
  if $h \mid f$ in $\mathbb{Z}[X]$ **then**
    Return(f/h,h)
  end if
end for
Return(„f ist irreduzibel über $\mathbb{Q}[X]$“)

Proposition 3.17. *Der Berlekamp-Hensel-Algorithmus˜3.4 ist korrekt.*

Literaturverzeichnis

[1] W. Adams, Ph. Loustaunau: *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994

[2] Th. Becker, V. Weispfenning: *Gröbner bases. A computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer, 1993

[3] B. Buchberger: *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. 4, 373-383, 1970

[4] B. Buchberger: *Introduction to Gröbner bases*, in Buchberger, Winkler [5], pp. 3-31

[5] B. Buchberger, F. Winkler (eds.): *Gröbner bases and applications*, London Mathematical Society Lecture Note Series, vol. 251, Cambridge University Press, 1998

[6] F. Chyzak: *Gröbner bases, symbolic summation and symbolic integration*, in Buchberger, Winkler [5], pp. 32-60

[7] D. Cox, J. Little, D. O'Shea: *Ideals, varieties and algorithms. An introduction to computional algebraic geometrie and commutative algebra*, Undergraduate Texts in Mathematics, Springer, 1996

[8] R. Fröberg: *An introduction to Gröbner bases*, Pure and Applied Mathematics, John Wiley & Sons, 1997

[9] R.˜Hemmecke: *On the positive sum property and the computation of Graver test sets*, Math. Program. Ser. B **96** (2003), 247–269.

[10] M. Kofler: *Maple V Release 4 — Einführung und Leitfaden für den Praktiker*, Bonn: Addison-Wesley, 1996

[11] M. Petkovšek, H. Wilf, D. Zeilberger: $A = B$, Wellesley, Massachusetts, 1996, see also http://www.math.temple.edu/˜zeilberg/

[12] F. Winkler: *Polynomial algorithms in computer algebra*, Texts and Monographs in Symbolic Computation, Wien - New York: Springer, 1996