S V
G

Inhaltsverzeichnis

Teil I

Algebraische Grundlagen

1 Körper und Körpererweiterungen

Definition 1.1 Sei k ein Körper und $\varphi : \mathbb{Z} \to k$ der kanonische Ringhomomorphismus $(1 \mapsto 1)$ von $\mathbb{Z}$ nach k und $p \in \mathbb{N}_0$ der nichtnegative Erzeuger des Hauptideals Kern(φ). Dann heißt p die **Charakteristik** von k, kurz $p = \text{char}(k)$.

Definition 1.2 Es sei k_2 ein Körper und $k_1 \subseteq k_2$, so dass auch k_1 mit den von k_2 induzierten Verknüpfungen ein Körper ist. Dann nennt man k_1 **Teil-** oder **Unterkörper** von k_2. Entsprechend nennt man k_2 **Erweiterungs-** oder **Oberkörper** von k_1. Das Paar (k_1, k_2) heißt **Körpererweiterung**, schreibe auch k_2/k_1.

Definition 1.3 Es sei k ein Körper und k_0 der bzgl. $\subseteq$ kleinste Teilkörper von k. Dann heißt k_0 **Primkörper** von k.

Proposition 1.4 Ein Primkörper k_0 eines Körpers k ist stets isomorph zu einem $\mathbb{F}_p$ (falls $\text{char}(k) = p > 0$, p prim) oder zu $\mathbb{Q}$ (falls $\text{char}(k) = 0$).

Bemerkung 1.5 Es sei k_2/k_1 eine Körpererweiterung und $A \subset k_2$. Dann ist $k_1(A)$ der bzgl. $\subseteq$ kleinste Teilkörper von k_2, der k_1 und A enthält.

Definition 1.6 $k_1(A)$ heißt der von A über k_1 **erzeugte** Teilkörper und A das **Erzeugendensystem**. Existiert eine endliche Menge A mit $k_2 = k_1(A)$, so heißt die Erweiterung k_2/k_1 **endlich erzeugt**. Existiert sogar ein einelementiges Erzeugendensystem $A = \{\alpha\}$, so spricht man von einer **einfachen** Erweiterung, der Erzeuger α heißt auch **primitives Element**.

Definition 1.7 Sei k_2/k_1 eine Körpererweiterung. Dann heißt jedes $\alpha \in k_2$, für das ein Polynom $p_\alpha \in k_1[Z]$ mit $p_\alpha(\alpha) = 0$ existiert, ein (über k_1) **algebraisches** Element. Ansonsten heißt α **transzendent**. Sind alle $\alpha \in k_2$ algebraisch über k_1, so heißt k_2/k_1 **algebraische Erweiterung**, ansonsten **transzendente Erweiterung**.

Definition 1.8 Es sei k_1 ein Körper. Ein Erweiterungskörper k_2 von k_1 heißt **algebraischer Abschluss** von k_1, wenn gilt:

1. k_2/k_1 ist algebraisch.
2. Jedes nichtkonstante Polynom in $k_2[Z]$ besitzt eine Nullstelle.

Allgemein heißt jeder Körper, der die zweite Eigenschaft hat, **algebraisch abgeschlossen**.

Bemerkung 1.9 Jeder Körper hat einen bis auf Isomorphie eindeutigen algebraischen Abschluss.

Definition 1.10 Es sei k_2/k_1 eine Körpererweiterung. Dann heißt der Körper

$$\{\alpha \in k_2 : \alpha \text{ algebraisch über } k_1\}$$

die **algebraische Hülle** von k_1 in k_2.

Definition 1.11 Es sei k_2/k_1 eine Körpererweiterung sowie $\alpha_1, ..., \alpha_s \in k_2$, $s \in \mathbb{N}$. Dann heißen $\alpha_1, ..., \alpha_s$ bzw. die Menge $\{\alpha_1, ..., \alpha_s\}$ **algebraisch unabhängig** über k_1, falls der Kern des kanonischen Spezialisierungshomomorphismus $k_1[Z_1, ..., Z_s] \to k_2, Z_i \mapsto \alpha_i$, nur das Nullpolynom enthält. Eine beliebige Menge $A \subseteq k_2$ heißt algebraisch unabhängig über k_1, falls jede endliche Teilmenge von A algebraisch unabhängig über k_1 ist.

Über k_1 algebraisch unabhängige Elemente haben somit die Eigenschaft eines Systems von formalen Variablen bzgl. k_1 und sind insbesondere transzendent.

Definition 1.12 Es sei k_2/k_1 eine Körpererweiterung. Dann werden

$$[k_2 : k_1] = \sup\{s \in \mathbb{N}_0 : \exists \alpha_1, ..., \alpha_s \in k_2 : \{\alpha_1, ..., \alpha_s\} \text{ linear unabhängig über } k_1\}$$

als **algebraischer Grad** und

$$\text{transdeg}(k_2/k_1) = \sup\{n \in \mathbb{N}_0 : \exists \alpha_1, ..., \alpha_n \in k_2 : \{\alpha_1, ..., \alpha_n\} \text{ algebraisch unabhängig über } k_1\}$$

als **Transzendenzgrad** von k_2/k_1 bezeichnet. Ist $T \subseteq k_2$ eine bzgl. $\subseteq$ maximale über k_1 algebraisch unabhängige Teilmenge von k_2, so heißt T **Transzendenzbasis** von k_2 über k_1.

Proposition 1.13 Seien k_3/k_2 und k_2/k_1 Körpererweiterungen. Dann gilt:

$$[k_3 : k_1] = [k_3 : k_2] \cdot [k_2 : k_1],$$
$$\text{transdeg}(k_3/k_1) = \text{transdeg}(k_3/k_2) + \text{transdeg}(k_2/k_1).$$

Definition 1.14 Sei k_2/k_1 eine algebraische Körpererweiterung. Ein Element $\alpha \in k_2$ heißt **separabel** über k_1, falls ein Polynom $p_\alpha \in k_1[Z]\backslash\{0\}$ existiert, für das $p_\alpha(\alpha) = 0$ gilt und das nur einfache Nullstellen über dem algebraischen Abschluss von k_1 besitzt. k_2/k_1 heißt **separabel**, wenn für alle $\alpha \in k_2$ solch ein Polynom p_α existiert.

Definition 1.15 Es sei k_2/k_1 eine algebraische Körpererweiterung. Dann heißt der Körper

$$k_1^{\text{sep}} = \{\alpha \in k_2 : \ \alpha \text{ separabel über } k_1\}$$

die **separable Hülle** von k_1 in k_2. Der Grad

$$[k_2 : k_1]_{\text{sep}} := [k_1^{\text{sep}} : k_1]$$

wird als **Separabilitätsgrad** von k_2 über k_1 bezeichnet.

Bemerkung 1.16 Ist $\text{char}(k) = 0$, so ist jede algebraische Körpererweiterung k_2/k_1 separabel, insbesondere ist $k_1^{\text{sep}} = k_2$.

Definition 1.17 Es sei k_2/k_1 eine Körpererweiterung. Dann heißt k_2/k_1 **separabel erzeugt**, wenn eine Transzendenzbasis T von k_2/k_1 existiert, so dass die Erweiterung $k_2/k_1(T)$ separabel algebraisch ist. In diesem Fall nennt man T eine **separierende Tranzendenzbasis**.

2 Ringe und Ideale

Im Folgenden sei R immer ein kommutativer Ring mit 1.

Definition 2.1 R heißt **noethersch**, falls jedes Ideal in R endlich erzeugt ist.

Beispiel 2.2 Körper, endliche Ringe und Hauptidealringe wie z.B. $\mathbb{Z}$ oder $k[X]$ sind noethersch. Der Polynomring $k[Z_1, Z_2, ...]$ in unendlich vielen Variablen ist nicht noethersch.

Definition 2.3 Sei $I \subsetneq R$ ein echtes Ideal. Dann heißt I

- **maximal**, falls R/I ein Körper ist (dazu äquivalent: es gibt kein echtes Ideal J mit $I \subsetneq J \subsetneq R$).
- **prim**, falls R/I nullteilerfrei ist (dazu äquivalent: gilt $ab \in I$, so muss auch $a \in I$ oder $b \in I$ gelten).
- **primär**, falls für alle $a, b \in R$ gilt: aus $ab \in I, a \notin I$, folgt, dass eine Potenz $b^\nu, \nu \in \mathbb{N}$, in I liegt.

Definition 2.4 Es sei $I \subseteq R$ ein Ideal. Dann heißt das Ideal

$$\sqrt{I} = \{a \in R : \exists \nu \in \mathbb{N} \text{ mit } a^\nu \in I\}$$

das **Radikal** von I. Ein Ideal I mit $\sqrt{I} = I$ heißt **radikal**.

Beispiel 2.5

- Für $I = \langle 4 \rangle \subseteq \mathbb{Z}$ ist $\sqrt{I} = \langle 2 \rangle$.
- Es sei $R = k[X, Y]$ und $I = \langle X^2, Y \rangle$. Es ist $\sqrt{I} = \langle X, Y \rangle$.

Definition 2.6 Es sei $Q \subseteq R$ ein Primärideal. Dann heißt $\sqrt{Q}$ das zu Q **assoziierte Primideal**.

Satz 2.7 Es sei R ein noetherscher kommutativer Ring mit 1 und $I \subsetneq R$ ein echtes Ideal. Dann existieren primäre Ideale $Q_1, ..., Q_r \subseteq R$, so dass gilt:

1. $I = Q_1 \cap Q_2 \cap ... \cap Q_r$.
2. Für alle $1 \leq i < j \leq r$ gilt: $\sqrt{Q_i} \neq \sqrt{Q_j}$.
3. Für jedes $j = 1, ..., r$ ist $Q_j \supsetneq \bigcap_{1 \leq i \neq j \leq r} Q_i$, d.h. kein Q_j kann weggelassen werden.

B : siehe etwa [BW1993], Thm. 8.54, 8.55. ■

Jede Darstellung, die diese drei Eigenschaften besitzt, heißt **Primärzerlegung** von I. Man bezeichnet die $\sqrt{Q_i}$ auch als die zu I **assoziierten Primideale**.

Beispiel 2.8

- Ist $R = \mathbb{Z}$, so entspricht der eindeutigen Primfaktorzerlegung

  $$n = p_1^{d_1} \cdots p_k^{d_k}$$

  von $n \in \mathbb{Z}$ die Primärzerlegung

  $$\langle n \rangle = \langle p_1^{d_1} \rangle \cap ... \cap \langle p_k^{d_k} \rangle$$

  des Ideals $\langle n \rangle$. In diesem Fall sind die zu $\langle n \rangle$ assoziierten Primideale gerade die Ideale $\langle p_1 \rangle, ..., \langle p_k \rangle$. Man kann die Primärzerlegung also als Verallgemeinerung der Primfaktorzerlegung auffassen.

- Ist $R = k[X, Y]$ und $I = \langle X^2, XY \rangle$, so sind

  $$\begin{aligned} I &= \langle X \rangle \cap \langle X^2, XY, Y^2 \rangle \\ &= \langle X \rangle \cap \langle X^2 Y \rangle \end{aligned}$$

  zwei mögliche Primärzerlegungen von I mit den assoziierten Primidealen $\langle X \rangle$ und $\langle X, Y \rangle$.

3 Zariski-Topologie und Varietäten

Definition 3.1 Wir betten k in einen **universellen Erweiterungskörper** Ω ein, d.h. Ω ist algebraisch abgeschlossen und die Erweiterung Ω/k hat unendlichen Transzendenzgrad. Es sei $F \subseteq \Omega[Z_1, ..., Z_n]$ gegeben. Wir interessieren uns für die Menge

$$\mathscr{Z}(F) = \{(\alpha_1, ..., \alpha_n) \in \Omega^n : \forall f \in F : f(\alpha_1, ..., \alpha_n) = 0\}$$

der gemeinsamen Nullstellen aller $f \in F$ in Ω^n. Wir bezeichnen eine solche Menge als **algebraische** oder **(Zariski-)abgeschlossene** Menge. Gilt sogar $F \subseteq k[Z_1, ..., Z_n]$, so sprechen wir auch von einer ***k*-abgeschlossenen** Menge.

Definition 3.2 Diejenige Topologie auf Ω^n, in der die abgeschlossenen Mengen gerade die algebraischen Mengen sind, bezeichnet man als **Zariski-Topologie**. Den mit der Zariski-Topologie versehenen Ω^n bezeichnen wir als n-dimensionalen **affinen Raum** $\mathbb{A}^n$. Die von den k-abgeschlossenen Mengen definierte Topologie auf Ω^n heißt ***k*-Topologie**.

Bemerkung 3.3 Für $F \subseteq k[Z_1, ..., Z_n]$ gilt stets $\mathscr{Z}(F) = \mathscr{Z}(F \cdot k[Z_1, ..., Z_n])$. Ferner ist für ein Ideal $I \subseteq k[Z_1, ..., Z_n]$ stets $\mathscr{Z}(I) = \mathscr{Z}(\sqrt{I})$.

Für Zarisiki-abgeschlossenen Mengen genügt es also, Radikalideale zu betrachten.

Definition 3.4 Es sei $\mathfrak{p} \subseteq k[Z_1, ..., Z_n]$ ein Primideal. Dann bezeichnet man $\mathscr{Z}(\mathfrak{p})$ als ***k*-Varietät**. Falls das von $\mathfrak{p}$ in $\Omega[Z_1, ..., Z_n]$ erzeugte Ideal ebenfalls prim ist, spricht man kurz von der **Varietät** $\mathscr{Z}(\mathfrak{p})$. Sind Vund W (k-)Varietäten mit $V \subset W$, so nennt man V eine **(*k*-)Untervarietät** von W.

Satz 3.5 Es sei $W \subseteq \Omega^n$ eine k-abgeschlossene Menge. Dann existieren k-Varietäten $V_1, ..., V_r \subseteq \Omega^n$, so dass sich W schreiben lässt als

$$W = V_1 \cup ... \cup V_r.$$

Fordert man noch $V_i \not\subseteq V_j$ für alle $i \neq j$, so ist diese Darstellung eindeutig. Man spricht in diesem Fall auch von den ***k*-irreduziblen Komponenten** von W.

B : siehe etwa [Lang2002], IX, Thm. 2.2. ■

Bemerkung 3.6 Um eine Zerlegung einer durch ein Ideal I definierten abgeschlossenen Menge in irreduzible Komponenten durchzuführen, kann man sich der Primärzerlegung von I bedienen. Für (Œ) radikales I entspricht die (algebraische) Darstellung

$$I = \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r$$

als Schnitt von Primidealen gerade der (geometrischen) Zerlegung

$$\mathscr{Z}(I) = \mathscr{Z}(\mathfrak{p}_1) \cup ... \cup \mathscr{Z}(\mathfrak{p}_r).$$

Definition 3.7 Sei $\mathfrak{p} \subset k[Z_1, ..., Z_n]$ prim und $V = \mathscr{Z}(\mathfrak{p})$ die durch $\mathfrak{p}$ definierte k-Varietät. Dann heißt

$$\dim(V) := \text{transdeg}\,(\text{Quot}(k[Z_1, ..., Z_n]/\mathfrak{p})/k)$$

die **Dimension** von V. Seien $W \subseteq \Omega^n$ k-abgeschlossen und $V_1, ..., V_r$ die k-irreduziblen Komponenten von W. Dann definieren wir

$$\dim(W) := \max_j\{\dim(V_j)\}.$$

Diese Definition der Dimension über den Transzendenzgrad liegt die Anschauung zugrunde, dass transdeg $(\text{Quot}(k[Z_1, ..., Z_n]/\mathfrak{p})/k)$ der Anzahl der „Freiheitsgrade“ der Varietät V entspricht.

4 Gröbner-Basen

Für algorithmische Belange (d.h. Dekompositionen ausrechnen) benötigen wir einige Grundlagen zu Gröbner-Basen.

Notation: Im Folgenden schreiben wir auch $\boldsymbol{X} := (X_1, ..., X_n)$ usw. .

Definition 4.1 Sei R ein kommutativer Ring mit 1. Betrachte den Polynomring $R[Z_1, ..., Z_n]$. Wir nennen jedes Potenzprodukt

$$\prod_{j=1}^{n} Z_j^{\nu_j} \text{ mit } \nu_j \in \mathbb{N}_0$$

einen **Term** (in $Z_1, ..., Z_n$). Die Menge der Terme sei $\mathsf{T}(Z_1, ..., Z_n)$. Ein Produkt αt mit $\alpha \in R, t \in \mathsf{T}(Z_1, ..., Z_n)$ heißt **Monom** (in $Z_1, ..., Z_n$).

Definition 4.2 Sei $\leq$ eine Totalordnung auf $\mathsf{T}(Z_1, ..., Z_n)$. Dann heißt $\leq$ **Termordnung**, falls gilt:

1. Für alle $t \in \mathsf{T}(\boldsymbol{Z})$ gilt $1 \leq t$.
2. Für alle $t_1, t_2, t_3 \in \mathsf{T}(\boldsymbol{Z})$ impliziert $t_1 \leq t_2$, dass auch $t_1 t_3 \leq t_2 t_3$ gilt.

Beispiel 4.3

- Die Gradfunktion in $k[Z]$.
- Die **lexikographische Ordnung**: Seien $t_\mu := Z_1^{\mu_1} \cdots Z_n^{\mu_n}, t_\nu := Z_1^{\nu_1} \cdots Z_n^{\nu_n}$ aus $\mathsf{T}(\boldsymbol{Z})$. Dann ist $t_\mu \leq_{\text{lex}} t_\nu$, falls $(\nu_1 - \mu_1, ..., \nu_n - \mu_n) = (0, ..., 0)$ oder falls der am weitesten links stehende Eintrag, der $\neq 0$ ist, positiv ist.
- Die **graduiert umgekehrt lexikographische Ordnung**, kurz **grevlex**: Hier ist $t_\mu \leq_{\text{grevlex}} t_\nu$, falls $\sum \mu_i < \sum \nu_i$ oder falls sowohl $\sum \mu_i = \sum \nu_i$ und - sofern vorhanden - der am weitesten rechts stehende Eintrag $\neq 0$ in $(\nu_1 - \mu_1, ..., \nu_n - \mu_n)$ negativ ist.

Definition 4.4 Es sei R ein kommutativer Ring mit 1, $p = \sum_{t \in \mathsf{T}(\boldsymbol{Z})} \alpha_t t \in R[\boldsymbol{Z}] \backslash \{0\}$ und $\leq$ eine Termordnung. Dann bezeichne $\mathsf{T}(p) := \{t \in \mathsf{T}(\boldsymbol{Z}) : \alpha_t \neq 0\}$ die Menge der Terme von p. Der **Leitterm** von p bzgl. $\leq$ ist

$$\mathrm{HT}_{\leq}(p) := \max_{\leq} \mathsf{T}(p).$$

Der **Leitkoeffizient** ist $\alpha_{\mathrm{HT}_{\leq}(p)}$ und

$$\mathrm{HM}_{\leq}(p) := \alpha_{\mathrm{HT}_{\leq}(p)} \cdot \mathrm{HT}_{\leq}(p)$$

das **Leitmonom**. Entsprechend schreibt man für eine Menge M von Polynomen: $\mathrm{HT}(M) = \{\mathrm{HT}(p) : p \in M \backslash \{0\}\}$ usw. .

Definition 4.5 Es sei $I \subseteq k[\boldsymbol{Z}]$ ein Ideal, G ein endliches Erzeugendensystem von I mit $0 \notin G$, sowie $\leq$ eine Termordnung. Dann heißt G eine **Gröbner-Basis** von I bzgl. $\leq$, falls für jedes $p \in \mathrm{HT}(I)$ ein $q \in \mathrm{HT}(G)$ exisitiert mit $q|p$.

Definition 4.6 Es seien $f, g, p \in k[\boldsymbol{Z}]$ mit $f \neq 0, p \neq 0$. Ferner sei $\leq$ eine Termordnung und $P \subseteq k[\boldsymbol{Z}]$. Dann sagen wir

- f **reduziert** zu g modulo p unter Elimination von t, kurz $f \underset{p}{\rightarrow} g[t]$, falls $t \in \mathsf{T}(f)$, $\mathrm{HT}(p)|t$ und $g = f - \frac{\alpha_t \cdot t}{\mathrm{HM}(p)} \cdot p$ für einen Koeffizienten α_t von f.
- f reduziert zu g modulo p, kurz $f \underset{p}{\rightarrow} g$, falls ein $t \in \mathsf{T}(f)$ mit $f \underset{p}{\rightarrow} g[t]$ existiert.
- f reduziert zu g modulo P, kurz $f \underset{P}{\rightarrow} g$, falls ein $p \in P$ existiert mit $f \underset{p}{\rightarrow} g$.

- f ist **reduzierbar** modulo p (bzw. P), falls ein Polynom $h \in k[\boldsymbol{Z}]$ mit $f \underset{p}{\rightarrow} h$ (bzw. $f \underset{P}{\rightarrow} h$) existiert.
- f ist **top-reduzierbar** modulo p (bzw. P), falls ein Polynom $h \in k[\boldsymbol{Z}]$ mit $f \underset{p}{\rightarrow} h[\mathrm{HT}(f)]$ (bzw. $f \underset{P}{\rightarrow} h[\mathrm{HT}(f)]$) existiert.

„Reduktionsketten“ der Form $f \underset{P}{\rightarrow} g_1 \underset{P}{\rightarrow} g_2 \underset{P}{\rightarrow} \ldots \underset{P}{\rightarrow} g$ kürzt man auch durch $f \overset{*}{\underset{P}{\rightarrow}} g$ ab.

Definition 4.7 Seien $f, g \in k[\boldsymbol{Z}], P \subseteq k[\boldsymbol{Z}]$ und $\leq$ eine Termordnung. Dann ist f in **Normalform** modulo P, falls f nicht reduzierbar ist modulo P und g heißt eine Normalform von f modulo P, kurz $g = \mathrm{norm}(f, P)$, falls g in Normalform modulo P ist und $f \overset{*}{\underset{P}{\rightarrow}} g$.

Definition 4.8 Es sei G eine Gröbner-Basis des Ideals $I \subseteq k[\boldsymbol{Z}]$ bzgl. einer Termordnung $\leq$. Dann heißt G **reduzierte Gröbner-Basis** von I bzgl. $\leq$, falls alle Polynome $g \in G$ normiert und in Normalform bzgl. $G \backslash \{g\}$ sind.

Satz 4.9 Für jedes Ideal $I \subseteq k[\boldsymbol{Z}]$ und eine fest gewählte Termordnung $\leq$ existiert genau eine reduzierte Gröbner-Basis von I.

Satz 4.10 Ist G eine Gröbner-Basis bzgl. $\leq$, so besitzt jedes Polynom $p \in k[\boldsymbol{Z}]$ eine eindeutige Normalform modulo G. Insbesondere gilt:

$$\mathrm{norm}(p, G) = 0 \quad \Leftrightarrow \quad p \in \langle G \rangle.$$

$\mathrm{norm}(p, G)$ liefert also eine Möglichkeit, auf Enthaltensein im Ideal I zu testen, und einen Nebenklassenvertreter für jede Nebenklasse $p + I$ in $k[\boldsymbol{Z}]/I$ zu bestimmen.

Definition 4.11 Es sei G eine Gröbner-Basis des Ideals $I \subseteq k[\boldsymbol{Z}]$ bzgl. $\leq$. Dann heißt G **minimal**, wenn jedes $g \in G$ normiert und nicht top-reduzierbar modulo $G \backslash \{g\}$ ist.

Bemerkung 4.12 Gröbner-Basen können effektiv berechnet werden, etwa durch den *Algorithmus von Buchberger* (siehe etwa [BW1993, Eisen1995, Stein2000]). Sie erlauben die Beantwortung zahlreicher algorithmischer Fragen bei Idealen in $k[\boldsymbol{Z}]$, z.B.

- entscheide für $f \in k[\boldsymbol{Z}]$ und $I \subseteq k[\boldsymbol{Z}]$, ob $f \in \sqrt{I}$ ist oder nicht.
- bestimme den Schnitt von Idealen.
- bestimme die Dimension eines Ideals.
- für $I \subseteq k[Z_1, \ldots, Z_n]$ bestimme $I \cap k[Z_j, \ldots, Z_n]$ für $j = 1, \ldots, n$.

Satz 4.13 (Eliminationstheorem)
Es sei $G \subseteq k[Z_1, \ldots, Z_n]$ eine Gröbner-Basis bzgl. der lexikographischen Ordnung $\leq_{\mathrm{lex}}$ (d.h. $Z_1 > Z_2 > \ldots > Z_n$). Dann ist für $i = 1, \ldots, n$ die Menge $G \cap k[Z_i, \ldots, Z_n]$ eine Gröbner-Basis von $\langle G \rangle \cap k[Z_i, \ldots, Z_n]$.

Definition 4.14 Es sei $I \subseteq k[Z_1, ..., Z_n]$ ein Ideal und $i \in \{0, ..., n-1\}$. Dann heißt $I \cap k[Z_{i+1}, ..., Z_n]$ das i-te **Eliminationsideal** von I.

Satz 4.13 besagt, dass eine Gröbner-Basis bzgl. $\leq_{\text{lex}}$ eine „Dreiecksform“, ähnlich der Treppenform beim Gauß-Algorithmus, besitzt. Damit können Lösungen für die einzelnen Unbekannten ausgehend von der bzgl. $\leq_{\text{lex}}$ kleinsten Variablen nacheinander bestimmt werden (vgl. Beispiel A.57 in [Stein2000]).

Dies kann man noch etwas allgemeiner fassen:

Definition 4.15 Es sei $\leq$ eine Termordnung auf $\mathsf{T}(Z_1, ..., Z_n)$ und $i \in \{1, ..., n-1\}$. Dann heißt $\leq$ vom ***i*-Eliminationstyp**, wenn jeder Term, in dem eine der Unbestimmten $Z_1, ..., Z_i$ vorkommt, größer ist als jeder Term in $\mathsf{T}(Z_{i+1}, ..., Z_n)$.

Satz 4.16 Ist $i \in \{1, ..., n-1\}$ und G eine Gröbner-Basis von $I \subseteq k[Z_1, ..., Z_n]$ bzgl. einer Termordnung $\leq$ vom i-Eliminationstyp, so ist $G \cap k[Z_{i+1}, ..., Z_n]$ eine Basis des i-ten Eliminationsideals von I.

Beispiel 4.17 Termordnung vom i-Eliminationstyp:
Es sei $1 \leq i < n$ und für alle $t_\mu = Z_1^{\mu_1} \cdots Z_n^{\mu_n}$, $t_\nu = Z_1^{\nu_1} \cdots Z_n^{\nu_n}$ setzen wir

$$t_\mu \leq_{i\text{-elim}} t_\nu :\Leftrightarrow \left[\sum_{j=1}^{i} \mu_i < \sum_{j=1}^{i} \nu_i \text{ oder, falls „=“ gilt, } t_\mu \leq_{\text{grevlex}} t_\nu \right].$$

Damit ist $\leq_{i\text{-elim}}$ eine Termordnung vom i-Eliminationstyp auf $\mathsf{T}(Z_1, ..., Z_n)$.

Satz 4.18 Es gibt unendlich viele Zahlen $n \in \mathbb{N}$ und ein $d > 0$ (etwa $d = 5$), so dass für jedes solche n eine von n linear abhängige Anzahl von Binomen $g_1, ..., g_w$ mit $\deg(g_i) \leq d$ und eine positive Konstante $c \approx 0,5$ existieren, so dass gilt:

1. Jede Gröbner-Basis von $\langle g_1, ..., g_w \rangle$ enthält ein Polynom vom Totalgrad $\geq 2^{2^{cn}}$.
2. Für jede Gröbner-Basis G von $\langle g_1, ..., g_w \rangle$ gilt: $|G| \geq 2^{2^{cn}}$.

Glücklicherweise tritt diese doppelt exponentielle Verhalten bei realen Problemen „fast nie“ auf. Weitere Aufwandsbetrachtungen für Gröbner-Basen findet man bei [vzGG2003].

Teil II

Sequentielle Dekomposition

5 Motivation und Grundlagen

Wir betrachten Systeme der Form

$$\begin{aligned} f_1(A_1, ..., A_m, X_1, ..., X_n) &= 0 \\ &\vdots \\ f_l(A_1, ..., A_m, X_1, ..., X_n) &= 0, \end{aligned}$$

wobei die A_i Parametern entsprechen, die als Eingabe vorgegeben werden und die X_j in Abhängigkeit von den A_i zu bestimmen sind; die Lösungsmenge ist also die Menge $\mathscr{Z}(\langle f_1, ..., f_l\rangle)$ der gemeinsamen Nullstellen von $f_1, ..., f_l$. Dabei ist $\langle f_1, ..., f_l\rangle \subseteq k[A_1, ..., A_m, X_1, ..., X_n]$ Œ über k als prim vorausgesetzt (ansonsten könnten wir in einem ersten Vereinfachungsschritt $\mathscr{Z}(\langle f_1, ..., f_l\rangle)$ in seine irreduziblen Komponenten zerlegen und diese unabhängig voneinander betrachten, da jede Komponente durch ein Primideal beschrieben wird, siehe Bemerkung 3.6).

Es ist das Prinzip der *sequentiellen Dekomposition*, ein solches Gleichungssystem in nacheinander zu lösende, einfachere Teilprobleme zu zerlegen. Im Folgenden soll dafür eine präzise Definition gefunden werden.

Definition 5.1 Es seien $A \subseteq \mathbb{A}^m$ und $X \subseteq \mathbb{A}^n$ zwei k-Varietäten und $R \subseteq A \times X$ eine k-Untervarietät. Dann heißt R eine ***k*-Korrespondenz** zwischen A und X, schreibe dafür $R : A \to X$. Ist $(\alpha_1, ..., \alpha_m, \xi_1, ..., \xi_n) \in R$, so sagen wir $(\alpha_1, ..., \alpha_m) \in A$ **korrespondiert** mit $(\xi_1, ..., \xi_n) \in X$ unter R.

Wir interessieren uns in dieser Sprechweise für die zu vorgegebenen $\boldsymbol{\alpha}$ korrespondierenden Werte $\boldsymbol{\xi}$ unter der durch $\langle f_1, ..., f_l\rangle$ definierten k-Korrespondenz.

Sei nun $\mathfrak{p}$ ein Primideal in $k[\boldsymbol{A}, \boldsymbol{X}]$. Wir wollen ausdrücken, dass eine Dekomposition für alle „generischen“ Punkte $(\boldsymbol{\alpha}, \boldsymbol{\xi}) \in \mathscr{Z}(\mathfrak{p})$ eine Vereinfachung erlaubt.

Definition 5.2 Für ein Primideal $\mathfrak{p} \subset k[\boldsymbol{A}, \boldsymbol{X}]$ bezeichne a_i bzw. x_i das Bild von A_i bzw. X_i unter dem kanonischen Homomorphismus

$$k[\boldsymbol{A}, \boldsymbol{X}] \to k[\boldsymbol{A}, \boldsymbol{X}]/\mathfrak{p} \hookrightarrow \mathrm{Quot}(k[\boldsymbol{A}, \boldsymbol{X}]/\mathfrak{p}) \cong k(\boldsymbol{a}, \boldsymbol{x}).$$

Dann heißt $(\boldsymbol{a}, \boldsymbol{x})$ **generischer Punkt** von $\mathscr{Z}(\mathfrak{p})$.

Den generischen Punkt kann man sich als „Schablone“ für die Lösungen eines Gleichungssystems vorstellen. Er erfüllt gerade soviele algebraische Eigenschaften, wie nötig sind, um eine gemeinsame Nullstelle aller Polynome aus $\mathfrak{p}$ zu sein.

6 Zwischenkörper und Dekomposition

Intuitiv würde man „Dekomposition“ von $\mathfrak{p}$ bzw. der zugehörige Korrespondenz $\mathscr{Z}(\mathfrak{p})$ charakterisieren über einen Zwischenkörper von $k(\boldsymbol{a}, \boldsymbol{x})$ und $k(\boldsymbol{a})$, wobei $(\boldsymbol{a}, \boldsymbol{x})$ ein generischer Punkt von $\mathscr{Z}(\mathfrak{p})$ ist. Ein Problem bei diesem Ansatz besteht darin, dass uns in der Regel nicht alle Elemente von k „kostenfrei“ zur Verfügung stehen. Der naheliegende Ansatz, k durch den Körper k_2 zu ersetzen, der von den Koeffizienten der gegebenen Basis von $\mathfrak{p}$ über dem Primkörper erzeugt wird, ist ebenfalls unbefriedigend, da man von der Basis abhängig ist. Es hat auch keinen Sinn, vom kleinsten Körper zu sprechen, über dem eine Varietät definiert werden kann, wie das anschließende Beispiel 6.1 zeigt.

Beispiel 6.1 $\{x\}$ mit $x \in \mathbb{F}_2(x)$ transzendent über $\mathbb{F}_2$. Es ist

$$\{x\} = \mathscr{Z}(Z - x) = \mathscr{Z}(Z^2 - x^2) = \mathscr{Z}(Z^4 - x^4) = ... = \mathscr{Z}(Z^{2^j} - x^{2^j}) = ...$$

für alle $j \in \mathbb{N}_0$, und wir haben gleichzeitig die folgende absteigende Kette

$$\mathbb{F}_2(x) \supset \mathbb{F}_2(x^2) \supset ... \supset \mathbb{F}_2(x^{2^j}) \supset ...$$

Wir verwenden deshalb für den Körper k_2 in der Dekompositionsdefinition den „minimalen Definitionskörper“:

Definition 6.2 Es sei $I \subseteq k[Z_1, ..., Z_n]$ ein Ideal. Dann enthält die Menge

$\{\tilde{k} \subseteq k : \tilde{k}$ Teilkörper von k und es gibt eine Basis von I, deren sämtliche Koeffizienten in $\tilde{k}$ liegen$\}$

einen kleinsten Körper k_I, der in allen anderen $\tilde{k}$ enthalten ist. Wir nennen k_I den **minimalen Definitionskörper** von I.

Die Existenz von k_I kann etwa über die Berechnung einer reduzierten Gröbner-Basis gezeigt werden.

Definition 6.3 Es sei $k(y_1, ..., y_n)/k$ eine endlich erzeugte Körpererweiterung und

$$\mathfrak{P}_{(y_1,...,y_n)/k} = \{f \in k[Y_1, ..., Y_n] : f(y_1, ..., y_n) = 0\}.$$

Wir nennen $\mathfrak{P}_{(y_1,...,y_n)/k}$ das **von $(\boldsymbol{y_1, ..., y_n})$ über $\boldsymbol{k}$ definierte Ideal** oder das **Relationenideal** von $(y_1, ..., y_n)$.

Definition 6.4 Es seien $R : A \to X$ eine k-Korrespondenz mit zugehörigem Primideal $\mathfrak{p} \subset k[\boldsymbol{A}, \boldsymbol{X}]$, d.h. $R = \mathscr{Z}(\mathfrak{p})$, sowie $(\boldsymbol{a}, \boldsymbol{x})$ ein generischer Punkt von R über $k_\mathfrak{p}$ und $r \in \mathbb{N}$. Eine **sequentielle Dekomposition** der Stelligkeit r von R bzw. $\mathfrak{p} = \mathfrak{P}_{(\boldsymbol{a},\boldsymbol{x})/k_\mathfrak{p}} \cdot k[\boldsymbol{A}, \boldsymbol{X}]$ ist ein Paar

$$\left(\mathfrak{P}_{(\boldsymbol{x})/k_\mathfrak{p}(\boldsymbol{a},\boldsymbol{w})}, \mathfrak{P}_{(\boldsymbol{w})/k_\mathfrak{p}(\boldsymbol{a})}\right) \subseteq k_\mathfrak{p}(\boldsymbol{a}, \boldsymbol{w})[\boldsymbol{X}] \times k_\mathfrak{p}(\boldsymbol{a})[\boldsymbol{W}],$$

mit $\boldsymbol{w} = (w_1, ..., w_r)$, so dass $k_\mathfrak{p}(\boldsymbol{a}) \subseteq k_\mathfrak{p}(\boldsymbol{a}, \boldsymbol{w}) \subseteq k_\mathfrak{p}(\boldsymbol{a}, \boldsymbol{x})$ gilt.

Beispiel 6.5 Betrachte $\mathfrak{p} = \langle X^4 - A\rangle \subseteq \mathbb{Q}(\sqrt{-1})[A, X]$. Es ist $\mathbb{Q}(\sqrt{-1})_{\mathfrak{p}} = \mathbb{Q}$. Die zugehörige Körperkette für festes $A = a$ sieht so aus:

$$\mathbb{Q}(a) \subseteq \mathbb{Q}(a, x^2) \subseteq \mathbb{Q}(a, x) = \mathrm{Quot}(\mathbb{Q}[A, X]/\mathfrak{p}).$$

Dies führt zu der Dekomposition

$$\Big(\langle X^2 - w\rangle, \langle W^2 - a\rangle\Big) \subseteq \mathbb{Q}(w, a)[X] \times \mathbb{Q}(a)[W].$$

Dabei ist $w := x^2$.

Beispiel 6.6 Wir wollen $X_1^2 - X_2^2 - A^2 = 0$ für vorgegebenes $A = a$ lösen. Die zugehörige Körpererweiterung ist

$$\mathbb{Q}(a, x_1, x_2) = \mathrm{Quot}(\mathbb{Q}[A, X_1, X_2]/\langle X_1^2 - X_2^2 - A^2\rangle) \supset \mathbb{Q}(a).$$

Die naheliegende Strategie ist zunächst, etwa X_1 festzulegen und anschließend X_2 zu berechnen. In „Körpersicht“:

$$\mathbb{Q}(a) \subsetneq \mathbb{Q}(a, x_1) \subsetneq \mathbb{Q}(a, x_1, x_2).$$

Die zugehörige Dekomposition besteht aus den Idealen

$$\langle 0\rangle \subset \mathbb{Q}(a)[X_1] \text{ und } \langle x_1^2 - X_2^2 - a^2\rangle \subset \mathbb{Q}(a, x_1)[X_2].$$

Eine solche Dekomposition, die $\langle 0\rangle$ enthält, heißt **entartet**. Das Problem ist hier darin zu sehen, dass ein über $\mathbb{Q}(a)$ rein transzendenter Körper vorkommt, der keine algebraische Vereinfachung bietet. Eine bessere Lösungsstrategie wäre folgende gewesen: Lege $X_1 + X_2$ fest. Auf Körperseite gilt dann $x_1 - x_2 = \frac{a^2}{x_1 + x_2}$, da $a^2 = x_1^2 - x_2^2$.

$$\mathbb{Q}(a) \subsetneq \mathbb{Q}(a, x_1 + x_2) = \mathbb{Q}(a, x_1, x_2).$$

Auch hier taucht eine transzendente Erweiterung auf, aber es ist nur noch eine lineare Gleichung zu lösen.

Um die Idee, dass „gleiche Körper gleiche Vereinfachung bieten“ zu präzisieren, definieren wir den nachfolgenden Äquivalenzbegriff 6.7.

Definition 6.7 Sei R eine durch $\mathfrak{p} \subset k[\boldsymbol{A}, \boldsymbol{X}]$ definierte k-Korrespondenz. Ferner seien $(\mathfrak{P}_{(\boldsymbol{x})/k_{\mathfrak{p}}(\boldsymbol{a}, w_1, \ldots, w_r)}, \mathfrak{P}_{(\boldsymbol{w})/k_{\mathfrak{p}}(\boldsymbol{a})})$ und $(\mathfrak{P}_{(\boldsymbol{x})/k_{\mathfrak{p}}(\boldsymbol{a}, v_1, \ldots, v_s)}, \mathfrak{P}_{(\boldsymbol{v})/k_{\mathfrak{p}}(\boldsymbol{a})})$ sequentielle Dekompositionen von R bzw. $\mathfrak{p}$. Wir nennen diese Dekompositionen **äquivalent**, falls $r = s$ und $k_{\mathfrak{p}}(\boldsymbol{a}, \boldsymbol{w}) = k_{\mathfrak{p}}(\boldsymbol{a}, \boldsymbol{v})$.

Somit entspricht die Menge der r-stelligen Dekompositionen von R bzw. $\mathfrak{p}$ modulo Äquivalenz genau der Menge der Zwischenkörper der Erweiterung $k_{\mathfrak{p}}(\boldsymbol{a}, \boldsymbol{x})/k_{\mathfrak{p}}(\boldsymbol{a})$ mit r-elementigem Erzeugendensystem.

Lemma 6.8 Ist $k_{\mathfrak{p}}(\boldsymbol{a}, \boldsymbol{x})/k_{\mathfrak{p}}(\boldsymbol{a})$ endlich und einfach (etwa wenn $\mathrm{char}(k_{\mathfrak{p}}) = 0$ und die Erweiterung endlich ist), so existieren für festes r nur endlich viele nicht äquivalente r-stellige Dekompositionen.

B : benutze den Satz vom primitiven Element, [Lang2002], V, Thm. 4.6. ■

Die Forderung nach „einfach“ kann nicht weggelassen werden, wie das folgende Beispiel 6.9 zeigt:

Beispiel 6.9 $\mathbb{F}_2(x, y)/\mathbb{F}_2(x^2, y^2)$ ist endlich vom Grad 4 und besitzt unendlich viele Zwischenkörper mit einem Erzeuger: Als Erzeuger können Elemente der Form $x^{2n+1} + y$ gewählt werden (hingegen würde etwa x^{2n+1} als Erzeuger für jedes n den gleichen Körper liefern).

7 Berechnung von sequentiellen Dekompositionen

Zur Berechnung einer sequentiellen Dekomposition sind drei Teilschritte erforderlich.

1. *Bestimmung des minimalen Definitionskörpers* $k_\mathfrak{p}$.
   Dies kann leicht über die Berechnung einer reduzierten Gröbner-Basis von $\mathfrak{p}$ erfolgen. Die Koeffizienten der in der Basis enthaltenen Polynome sind die Erzeuger von $k_\mathfrak{p}$ über dem zugehörigen Primkörper.

2. *Finden eines (echten) Zwischenkörpers* $k_\mathfrak{p}(\boldsymbol{a}, \boldsymbol{w})$ *von* $k_\mathfrak{p}(\boldsymbol{a}, \boldsymbol{x})/k_\mathfrak{p}(\boldsymbol{a})$.
   Im Falle einer *endlich-algebraischen und separablen Erweiterung* kann man mit Hilfe der Primärzerlegung Zwischenkörper algorithmisch bestimmen, wie wir in Kapitel 11 sehen werden. Für *rein inseparable Erweiterungen* ist dies wesentlich schwieriger (wir werden diesen Fall nicht betrachten). Im Falle einer *transzendenten Erweiterung* entspricht das Hinzunehmen algebraisch unabhängiger Elemente dem Festlegen freier Parameter. Daher interessieren wir uns in diesem Fall für diejenigen Zwischenkörper, die eine Transzendenzbasis der Erweiterung enthalten. In Kapitel 9 werden wie sehen, wie wir bei gegebenem Relationenideal eine Transzendenzbasis und den Transzendenzgrad bestimmen können. Da separabel algebraische Erweiterungen besonders angenehme Eigenschaften haben, ist es wünschenswert, die Erzeuger des Zischenkörpers so zu wählen, dass darin eine *separierende* Transzendenzbasis von $k(\boldsymbol{a}, \boldsymbol{x})/k(\boldsymbol{a})$ enthalten ist.

3. *Berechnung der Kompositionsfaktoren* $\mathfrak{P}_{(\boldsymbol{w})/k_\mathfrak{p}(\boldsymbol{a})}$ *und* $\mathfrak{P}_{(\boldsymbol{x})/k_\mathfrak{p}(\boldsymbol{a},\boldsymbol{w})}$.
   Da zur Bestimmung von $\mathfrak{P}_{(\boldsymbol{w})/k_\mathfrak{p}(\boldsymbol{a})}$ und $\mathfrak{P}_{(\boldsymbol{x})/k_\mathfrak{p}(\boldsymbol{a},\boldsymbol{w})}$ die selben Methoden angewendet werden können, sprechen wir im Folgenden allgemeiner von einem Relationenideal $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. In Kapitel 8 werden wir sehen, wie für einen gegebenen Zwischenkörper $k(\boldsymbol{g})$ der Erweiterung $k(\boldsymbol{x})/k$ das Relationenideal bestimmt werden kann, und wie wir umgekehrt aus dem bekannten Relationenideal die Erzeuger von $k(\boldsymbol{g})$ erhalten.

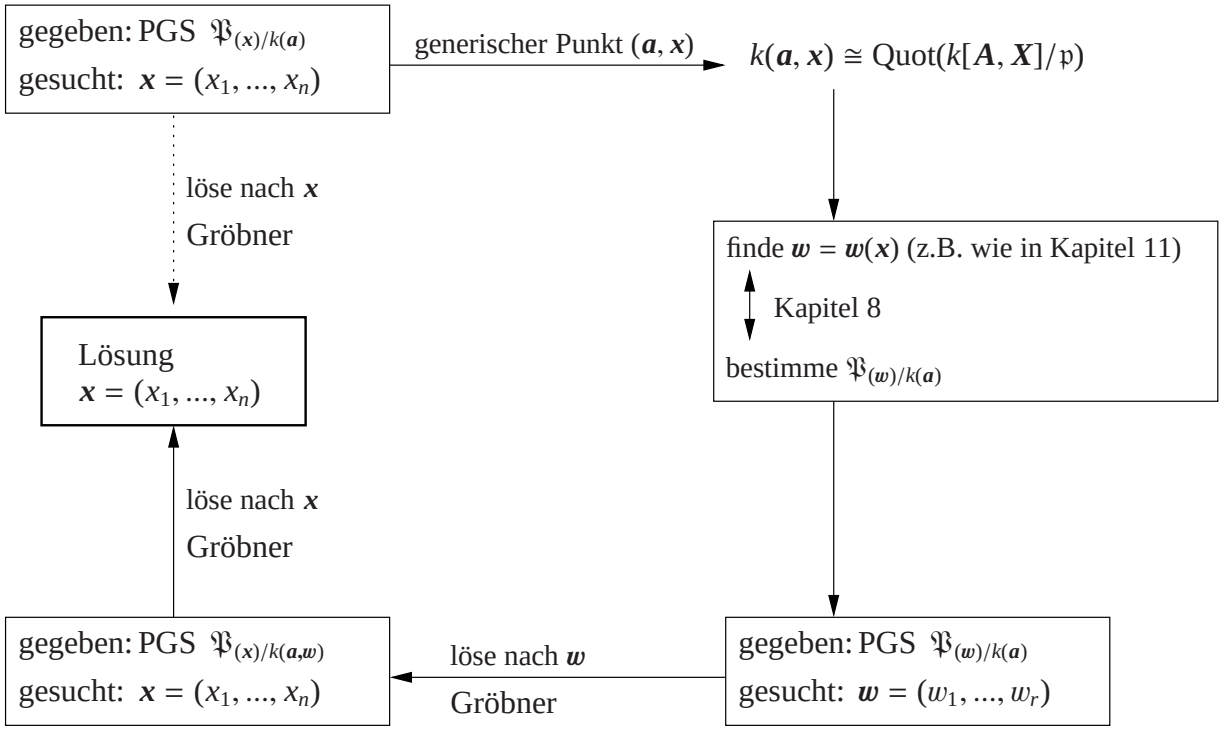
Es sei noch angemerkt, dass es je nach Vorgehen sein kann, dass zuerst die Erzeuger $\boldsymbol{w}(\boldsymbol{x})$ des Zwischenkörpers bekannt sind, aus denen dann $\mathfrak{P}_{(\boldsymbol{w})/k_\mathfrak{p}(\boldsymbol{a})}$ ermittelt werden kann (z.B. wenn man bei transzendente Erweiterungen freie Variablen festlegt), oder, dass man die Erzeuger eines Ideals $\mathfrak{P}_{(\boldsymbol{w})/k_\mathfrak{p}(\boldsymbol{a})}$ kennt, aus deren Koeffizienten man die Erzeuger $\boldsymbol{w}$ des Zwischenkörpers ablesen kann (z.B. wenn man Zwischenkörper über die Primärzerlegung ermittelt).

Desweiteren werden wir in Kapitel 10 sehen, wie man Minimalpolynome bestimmt, die ein nützliches Hilfsmittel beim Rechnen mit algebraischen Erweiterungen darstellen. Man kann damit etwa auf Separabilität testen, algebraische Grade bestimmen, Inverse berechnen oder auf Enthaltensein in einem Ideal testen.

In Kapitel 12 sehen wir, wie man ggf. besonders günstig darzustellende Erzeuger bestimmen kann, mit deren Hilfe einige der Algorithmen aus den anderen Kapiteln wesentlich einfacher durchzuführen sind.

Schließlich wird in Kapitel 13 noch eine alternative Vorgehensweise für die Lösung einiger der hier betrachteten Probleme mit sogenannten *Tag-Variablen* vorgestellt.

Zusammenfassend gehen wir bei der Lösung eines polynomialen Gleichungssystems durch sequentielle Dekomposition nach folgendem Schema vor:



Dieses Vorgehen bietet den Vorteil, dass die Dekomposition für „generischen Probleminstanzen“ gültig bleibt (also unabhängig von den für die Parameter $A_1, ..., A_m$ festgelegten Werten $a_1, ..., a_m$).

Teil III

Rechnen mit Körpererweiterungen

8 Erzeuger für das Relationenideal

Wir haben folgende Ausgangssituation: Gegeben ist eine endlich erzeugte Körpererweiterung $k(x_1, ..., x_n)$ mit bekannten Relationen $\mathfrak{P}_{(\boldsymbol{x})/k}$. Ferner ist ein Teilkörper $k(g_1, ..., g_r)$ gegeben, wobei die g_i als rationale Funktionen (d.h. Brüche) in den x_j gegeben sind.

Um Aussagen über die Erweiterung $k(\boldsymbol{x})/k(\boldsymbol{g})$ zu erhalten, wollen wir die Erzeuger des Relationenideals $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \subseteq k(\boldsymbol{g})[\boldsymbol{Z}]$ bestimmen.

Ein nützliches Hilfsmittel ist das **Erweiterungsideal**

$$\mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/k(\boldsymbol{g})} = \mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \cdot k(\boldsymbol{g})[Z_1, ..., Z_n]_{\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}}.$$

Dabei bezeichnet $k(\boldsymbol{g})[Z_1, ..., Z_n]_{\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}}$ die Lokalisierung von $k(\boldsymbol{g})[Z_1, ..., Z_n]$ nach dem multiplikativen Teilmonoid $k(\boldsymbol{g})[Z_1, ..., Z_n]\backslash\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$, d.h. wir erweitern $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ um Brüche mit Nennern aus $k(\boldsymbol{g})[\boldsymbol{Z}]\backslash\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$.

Proposition 8.1 Es seien $g_1(\boldsymbol{Z}), ..., g_r(\boldsymbol{Z}) \in k(\boldsymbol{Z})$ beliebige Darstellungen der Erzeuger $g_1, ..., g_r \in k(\boldsymbol{x})$ in den $x_1, ..., x_n$. Man erhält also $g_i = g_i(\boldsymbol{x})$ durch Einsetzen von $\boldsymbol{x}$ in $\boldsymbol{Z}$. Dann gilt über $k(\boldsymbol{g})[Z_1, ..., Z_n]_{\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}}$:

$$\mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/k(\boldsymbol{g})} = \langle g_1(\boldsymbol{Z}) - g_1(\boldsymbol{x}), ..., g_r(\boldsymbol{Z}) - g_r(\boldsymbol{x})\rangle + \langle\mathfrak{P}_{(\boldsymbol{x})/k}\rangle.$$

B : „$\supseteq$“: Offensichtlich gilt schon $\langle\mathfrak{P}_{(\boldsymbol{x})/k}\rangle \subseteq \mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/k(\boldsymbol{g})}$.
Sei $g_i(\boldsymbol{Z}) = \frac{n_i(\boldsymbol{Z})}{d_i(\boldsymbol{Z})}$ mit $n_i \in k[\boldsymbol{Z}], d_i \in k[\boldsymbol{Z}]\backslash\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. Dann gilt

$$g_i(\boldsymbol{Z}) - g_i(\boldsymbol{x}) = \frac{1}{d_i(\boldsymbol{Z})} \underbrace{(n_i(\boldsymbol{Z}) - g_i(\boldsymbol{x})d_i(\boldsymbol{Z}))}_{\in\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}}.$$

„$\subseteq$“: Schreibe abkürzend $I := \langle g_1(\boldsymbol{Z}) - g_1(\boldsymbol{x}), ..., g_r(\boldsymbol{Z}) - g_r(\boldsymbol{x})\rangle + \langle\mathfrak{P}_{(\boldsymbol{x})/k}\rangle$.
Wähle $\frac{n(\boldsymbol{Z})}{d(\boldsymbol{Z})} \in \mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ mit $n(\boldsymbol{Z}) \in k(\boldsymbol{g})[\boldsymbol{Z}]$ und $d(\boldsymbol{Z}) \in k(\boldsymbol{g})[\boldsymbol{Z}]\backslash\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. Dann existiert ein geeignetes $\alpha \in k[\boldsymbol{g}]$ und ein $\tilde{n}(\boldsymbol{Z}) \in k[\boldsymbol{g}][\boldsymbol{Z}]$ mit $n = \alpha^{-1}\tilde{n}$. Da I unter Multiplikation mit α^{-1} abgeschlossen ist, genügt es zu zeigen, dass $\tilde{n}(\boldsymbol{Z}) \in I$ gilt, um $\frac{n(\boldsymbol{Z})}{d(\boldsymbol{Z})} \in I$ zu erhalten: Es ist für geeignete $\alpha_{\boldsymbol{\mu},\boldsymbol{\nu}} \in k$:

$$\begin{aligned}
\tilde{n}(\boldsymbol{Z}) &= \tilde{n}(\boldsymbol{g}(\boldsymbol{x}), \boldsymbol{Z}) \\
&= \sum_{\boldsymbol{\mu}\in\mathbb{N}_0^n, \boldsymbol{\nu}\in\mathbb{N}_0^r} \alpha_{\boldsymbol{\mu},\boldsymbol{\nu}} \prod_{i=1}^{n} Z_i^{\mu_i} \prod_{j=1}^{r} g_j(\boldsymbol{x})^{\nu_j} \\
&=: \sum_{\boldsymbol{\mu},\boldsymbol{\nu}} \alpha_{\boldsymbol{\mu},\boldsymbol{\nu}} \boldsymbol{Z}^{\boldsymbol{\mu}} \boldsymbol{g}(\boldsymbol{x})^{\boldsymbol{\nu}}.
\end{aligned}$$

Nach Annahme ist $\tilde{n}(\boldsymbol{g}(\boldsymbol{x}), \boldsymbol{x}) = 0 \in k(\boldsymbol{x})$. Ersetzen wir jedes x_i durch Z_i, so erhalten wir (wegen Isomorphie) $\tilde{n}(\boldsymbol{g}(\boldsymbol{Z}), \boldsymbol{Z}) = 0 \in \mathrm{Quot}(k[\boldsymbol{Z}]/\mathfrak{P}_{(\boldsymbol{x})/k})$, d.h. es gibt ein geeignetes $p \in \mathfrak{P}_{(\boldsymbol{x})/k} \cdot k[\boldsymbol{Z}]_{\mathfrak{P}_{(\boldsymbol{x})/k}}$ mit $p = \tilde{n}(\boldsymbol{g}(\boldsymbol{Z}), \boldsymbol{Z})$. Damit gilt dann:

$$\begin{aligned} p = \tilde{n}(\boldsymbol{g}(\boldsymbol{Z}), \boldsymbol{Z}) &= \sum_{\mu,\nu} \alpha_{\mu,\nu} \boldsymbol{Z}^{\mu} \boldsymbol{g}(\boldsymbol{Z})^{\nu} \\ &= \sum_{\mu,\nu} \alpha_{\mu,\nu} \boldsymbol{Z}^{\mu} \prod_j g_j(\boldsymbol{Z})^{\nu_j} \\ &= \sum_{\mu,\nu} \alpha_{\mu,\nu} \boldsymbol{Z}^{\mu} \prod_j (g_j(\boldsymbol{x}) + (g_j(\boldsymbol{Z}) - g_j(\boldsymbol{x})))^{\nu_j} \end{aligned}$$

und Ausmultiplizieren führt auf

$$\underbrace{\sum_{\mu,\nu} \alpha_{\mu,\nu} \boldsymbol{Z}^{\mu} \prod_j g_j(\boldsymbol{x})^{\nu_j}}_{=\tilde{n}(\boldsymbol{g}(\boldsymbol{x}),\boldsymbol{Z})} + \underbrace{\sum a_l (g_j(\boldsymbol{Z}) - g_j(\boldsymbol{x}))}_{\in I} - p = 0$$

mit geeigneten $a_l \in k[\boldsymbol{g}(\boldsymbol{x}), \boldsymbol{g}(\boldsymbol{Z}), \boldsymbol{Z}]$. Damit ist wie gewünscht $\tilde{n}(\boldsymbol{Z}) \in I$. ■

Unser Ziel ist es, Erzeuger für $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ zu bestimmen.

Definition 8.2 Sei $I \subseteq k[\boldsymbol{Z}]$ ein Ideal und $f \in k[\boldsymbol{Z}]$. Die **Saturierung** von I bzgl. f ist

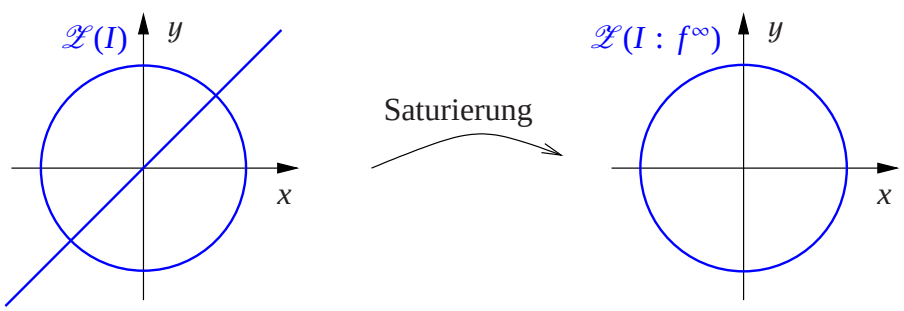
$$I : f^{\infty} = \{g \in k[\boldsymbol{Z}] : \exists \mu \in \mathbb{N} : f^{\mu} g \in I\}.$$

Die Saturierung berechnet man, indem man eine Unbekannte λ hinzunimmt und dann λ in $I \cdot k[\lambda, \boldsymbol{Z}] + \langle \lambda f - 1 \rangle$ eliminiert.

Beispiel 8.3

- Ist $f \in I$, so ist $I : f^{\infty} = R$.
- Ist $\mathfrak{p} \subset R$ ein Primideal und $f \in R \backslash \mathfrak{p}$, so ist $\mathfrak{p} : f^{\infty} = \mathfrak{p}$.

Beispiel 8.4 Eine geometrische Interpretation der Saturierung: Es sei $I \subseteq \mathbb{R}[X, Y]$ und $\mathscr{Z}(I)$ sei die Vereinigung des Einheitskreises mit der Ursprungsgeraden. Sei $f = X - Y$. Durch die Saturierung $I : f^{\infty}$ erhält man den Einheitskreis $\mathscr{Z}(I : f^{\infty}) = \mathscr{Z}(\langle X^2 + Y^2 - 1 \rangle)$.



Proposition 8.5 Es seien $g_1(\boldsymbol{Z}), ..., g_r(\boldsymbol{Z})$ wie in Proposition 8.1 und $g_i = \frac{n_i}{d_i}$ mit $n_i \in k[\boldsymbol{Z}], d_i \in k[\boldsymbol{Z}]\backslash\mathfrak{P}_{(\boldsymbol{x})/k}$ für $i = 1, ..., r$. Dann ist

$$\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} = (\langle n_1(\boldsymbol{Z}) - g_1(\boldsymbol{x})d_1(\boldsymbol{Z}), ..., n_r(\boldsymbol{Z}) - g_r(\boldsymbol{x})d_r(\boldsymbol{Z})\rangle + \langle\mathfrak{P}_{(\boldsymbol{x})/k}\rangle) : \left(\prod_{i=1}^{r} d_i(\boldsymbol{Z})\right)^{\infty}.$$

B : Schreibe

$$J := (\langle n_1(\boldsymbol{Z}) - g_1(\boldsymbol{x})d_1(\boldsymbol{x}), ..., n_r(\boldsymbol{Z}) - g_r(\boldsymbol{x})d_r(\boldsymbol{x})\rangle + \langle\mathfrak{P}_{(\boldsymbol{x})/k}\rangle) : \left(\prod_{i=1}^{r} d_i(\boldsymbol{Z})\right)^{\infty}.$$

„$\supseteq$“: Wegen $n_i(\boldsymbol{x}) - g_i(\boldsymbol{x})d_i(\boldsymbol{x}) = 0$ genügt jedes $p \in J$ für ein $\mu \in \mathbb{N}$ der Gleichung

$$\underbrace{\left(\prod d_i(\boldsymbol{x})\right)^{\mu}}_{\neq 0} p(\boldsymbol{x}) = 0,$$

also ist $p(\boldsymbol{x}) = 0$ und damit $p \in \mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$.

„$\subseteq$“: Sei $n(\boldsymbol{Z}) \in \mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. Es gibt $\alpha, \tilde{n}(\boldsymbol{Z})$ wie im Beweis von Proposition 8.1, so dass $n(\boldsymbol{Z}) = \alpha^{-1}\tilde{n}(\boldsymbol{Z})$ gilt und es genügt, $\tilde{n} \in J$ zu zeigen. Wie im Beweis von Proposition 8.1 erhält man

$$\tilde{n}(\boldsymbol{Z}) + \sum a_l(g_j(\boldsymbol{Z}) - g_j(\boldsymbol{x})) = p \in \mathfrak{P}_{(\boldsymbol{x})/k} \cdot k[\boldsymbol{Z}]_{\mathfrak{P}_{(\boldsymbol{x})/k}}.$$

mit geeigneten $a_l \in k[\boldsymbol{g}(\boldsymbol{x}), \boldsymbol{g}(\boldsymbol{Z}), \boldsymbol{Z}]$. Multiplikation mit einer geeigneten Potenz $(\prod d_i)^{\mu}$ ergibt

$$(\prod d_i)^{\mu}\tilde{n}(\boldsymbol{Z}) + \sum \tilde{a}_l(n_j(\boldsymbol{Z}) - g_j(\boldsymbol{x})d_j(\boldsymbol{Z})) = \tilde{p} \in \mathfrak{P}_{(\boldsymbol{x})/k} \cdot k[\boldsymbol{Z}]_{\mathfrak{P}_{(\boldsymbol{x})/k}}.$$

Auf der linken Seite steht ein Polynom, folglich ist auch $\tilde{p}$ ein Polynom. Setzt man x_i für Z_i ein, so ist die linke Seite gleich 0 und damit auch $\tilde{p}(\boldsymbol{x}) = 0$. Also ist $\tilde{p} \in \mathfrak{P}_{(\boldsymbol{x})/k}$ und damit ist $\tilde{n}(\boldsymbol{Z}) \in J$. ■

In Proposition 8.5 haben wir gesehen, wie man aus gegebenen Körpererzeugern $\boldsymbol{g}$ das Relationenideal bestimmen kann. Proposition 8.6 liefert gewissermaßen die „Umkehrung“ dazu, nämlich, wie man aus einem gegebenem Relationenideal die Erzeuger des zugehörigen Erweiterungskörpers bestimmen kann.

Proposition 8.6 Sei P eine Menge von Erzeugern von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ und k' derjenige Körper, der durch Adjunktion der Koeffizienten von P zu k entsteht. Dann ist $k' = k(\boldsymbol{g})$.

B : „$\subseteq$“: Ist klar nach Definition von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$.

„$\supseteq$“: Skizze: Wähle eine endliche Teilmenge $P' \subseteq P$ aus, die $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ erzeugt. Berechnen wir mit Buchbergers Algorithmus eine Gröbner-Basis von $\langle P'\rangle$, so enthält diese nach Konstruktion des Algorithmus nur Koeffizienten aus k'. Sein nun $g(\boldsymbol{x}) = \frac{n(\boldsymbol{x})}{d(\boldsymbol{x})} \in k(\boldsymbol{g})$ beliebig mit $n(\boldsymbol{Z}), d(\boldsymbol{Z}) \in k[\boldsymbol{Z}]\backslash\mathfrak{P}_{(\boldsymbol{x})/k}$. Nun nehmen wir ein neues transzendentes Element λ zu k' hinzu und bilden die Normalform von $n(\boldsymbol{Z}) - \lambda d(\boldsymbol{Z})$ modulo der berechneten Gröbner-Basis. Man überprüft leicht, dass diese Normalform linear in λ ist und bei Substitution

$\lambda \mapsto g(\boldsymbol{x})$ verschwindet. Die Normalform sei $a(\boldsymbol{Z}) - \lambda b(\boldsymbol{Z})$ mit $a(\boldsymbol{Z}), b(\boldsymbol{Z}) \in k'[\boldsymbol{Z}]$. Œ dürfen wir $b(\boldsymbol{Z}) \neq 0$ voraussetzen und erhalten

$$a(\boldsymbol{Z}) - g(\boldsymbol{x})b(\boldsymbol{Z}) = 0 \quad \text{bzw.} \quad g(\boldsymbol{x}) = \frac{a(\boldsymbol{Z})}{b(\boldsymbol{Z})},$$

d.h. $g(\boldsymbol{x}) \in k'$. ■

Um eine „kanonische“ Erzeugermenge von $k(\boldsymbol{g})$ über k zu erhalten, die unabhängig von einer Termordnung ist, kann man ausnutzen, dass $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ nur endlich viele verschiedene reduzierte Gröbner-Basen hat: Verwende die Vereinigung der Koeffizienten aller reduzierten Gröbner-Basen.

9 Berechnung von (separierenden) Transzendenzbasen

Wie bereits erwähnt entspricht das Hinzunehmen algebraisch unabhängiger Elemente dem festlegen freier Parameter. Ist (etwa aus Proposition 8.5) ein Relationenideal $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ bekannt, so wäre es aufgrund der angenehmen algebraischen Eigenschaften von separabel algebraischen Erweiterungen wünschenswert, wenn wir eine separierende Transzendenzbasis von $k(\boldsymbol{x})/k(\boldsymbol{g})$ bestimmen könnten.

Gesucht sind transdeg$(k(\boldsymbol{x})/k(\boldsymbol{g}))$ und eine (separierende) Transzendenzbasis.

Kennt man eine Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$, so kann eine Transzendenzbasis von $k(\boldsymbol{x})/k(\boldsymbol{g})$ wie folgt berechnet werden:

Algorithmus 9.1 Berechnung einer Transzendenzbasis

Eingabe: Gröbner-Basis G von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \subseteq k(\boldsymbol{g})[Z_1, ..., Z_n]$.
Ausgabe: Transzendenzbasis B von $k(\boldsymbol{x})/k(\boldsymbol{g})$ (und somit transdeg$(k(\boldsymbol{x})/k(\boldsymbol{g})) = |B|$).

$B := \emptyset$
for $i \in \{1, ..., n\}$
  if $\mathrm{HT}(G) \cap \mathsf{T}(\{Z_j : x_j \in B \cup \{x_i\}\}) = \emptyset$
  then $B := B \cup \{x_i\}$
return B

Insbesondere erhalten wir so auch eine Möglichkeit, nur mit Hilfe des Relationenideals $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ zu überprüfen, ob die Erweiterung $k(\boldsymbol{x})/k(\boldsymbol{g})$ algebraisch ist (nämlich wenn transdeg$(k(\boldsymbol{x})/k(\boldsymbol{g})) = 0$ ist) oder nicht.

Beispiel 9.2 Seien x_1, x_2, x_3 algebraisch unabhängig über $\mathbb{F}_4$ und

$$(g_1, g_2, g_3) := \left(x_1^2 + x_2, \quad \frac{x_2}{x_3}, \quad \frac{x_1^4x_2^2 + x_1^2x_3^2 + x_2^4 + x_2x_3^2}{x_2x_3}\right).$$

Verwendet man eine umgekehrt lexikographische Ordnung, d.h. $Z_1 > Z_2 > Z_3$, so erhält man folgende reduzierte Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{x})/\mathbb{F}_4(\boldsymbol{g})}$:

$$G = \{Z_1^2 + \frac{x_2}{x_3}Z_3 + x_1^2 + x_2, \quad Z_2 + \frac{x_2}{x_3}Z_3\}.$$

Dann ist $\mathrm{HT}(G) = \{Z_1^2, Z_2\}$. Der obige Algorithmus 9.1 liefert $B = \{x_3\}$, d.h. es ist $\mathrm{transdeg}(\mathbb{F}_4(\boldsymbol{x})/\mathbb{F}_4(\boldsymbol{g})) = 1$ (und damit $\mathrm{transdeg}(\mathbb{F}_4(\boldsymbol{g})/\mathbb{F}_4) = 2$, vgl. Proposition 1.13).

Satz 9.3 Es sei $k(x_1, ..., x_n)/k$ eine endlich erzeugte Körpererweiterung. Ihr Transzendenzgrad sei t. Ferner sei $P \subseteq k[Z_1, ..., Z_n]_{\mathfrak{P}_{(\boldsymbol{x})/k}}$ ein endliches Erzeugendensystem für $\mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/k} \subseteq k[\boldsymbol{Z}]_{\mathfrak{P}_{(\boldsymbol{x})/k}}$. Dann sind äquivalent:

1. $k(\boldsymbol{x})/k$ ist separabel erzeugt.
2. Der Rang der Matrix
$$M = \left(\frac{\partial p}{\partial Z_i}(\boldsymbol{x})\right)_{p\in P, i=1,...,n}$$
ist $n - t$.

Ist $k(\boldsymbol{x})/k$ nicht separabel erzeugt, so ist der Rang von M kleiner als $n - t$.

Folgerung 9.4 Die Matrix M aus Satz 9.3 sei vom Rang $n - m$. Weiterhin seien $P' \subseteq P$ und $L' \subseteq \{1, ..., n\}$ mit $|P'| = |L'| = n - m$ so gewählt, dass

$$\det\left(\frac{\partial p}{\partial Z_i}(\boldsymbol{x})\right)_{p\in P', i\in L'} \neq 0$$

ist. Dann bilden, sofern $k(\boldsymbol{x})/k$ separabel erzeugt ist, die x_j, $j \notin L'$, eine separierende Transzendenzbasis von $k(\boldsymbol{x})/k$.

Beispiel 9.5 (Fortsetzung von Beispiel 9.2) Es ergibt sich „durch Ablesen“ (vgl. Proposition 8.1) folgende Basis für $\mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/\mathbb{F}_4(\boldsymbol{g})}$:

$$Z_1^2 + Z_2^2 + x_1^2 + x_2, \quad \frac{Z_2}{Z_3} + \frac{x_2}{x_3},$$
$$\frac{Z_1^4Z_2^2 + Z_1^2Z_3^2 + Z_2^4 + Z_2Z_3^2}{Z_2Z_3} + \frac{x_1^4x_2^2 + x_1^2x_3^2 + x_2^4 + x_2x_3^2}{x_2x_3}$$

(beachte, dass wegen $\mathrm{char}(\mathbb{F}_4) = 2$ gilt „$+ = -$“).

Das ergibt folgende Matrix:

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & \frac{1}{x_3} & \frac{x_2}{x_3^2} \\ 0 & \frac{x_1^4x_2^2+x_1^2x_3^2+x_2^4}{x_2^2x_3} & \frac{x_1^4x_2^2+x_1^2x_3^2+x_2^4+x_2x_3^2}{x_2^2x_3} \end{pmatrix}.$$

Der Rang dieser Matrix ist $2 = 3 - 1 = n - t$.

Da die Erweiterung $\mathbb{F}_4(\boldsymbol{x})/\mathbb{F}_4(\boldsymbol{g})$ vom Transzendenzgrad $t = 1$ ist, folgt, dass die Erweiterung separabel erzeugt ist. Die separierende Transzendenzbasis ist durch $\{x_1\}$ gegeben.

Bemerkung 9.6 Nimmt man zu $k(\boldsymbol{g})$ ein neues Element y hinzu, so kann man nun leicht prüfen, ob y algebraisch über $k(\boldsymbol{g})$ ist. Dies ist nämlich genau dann der Fall, wenn

$$\text{transdeg}(k(\boldsymbol{x})/k(\boldsymbol{g})) = \text{transdeg}(k(\boldsymbol{x})/k(\boldsymbol{g}, y))$$

gilt.

10 Rechnen mit algebraischen Erweiterungen

Lemma 10.1 Es sei $k(\boldsymbol{x})/k(\boldsymbol{g})$ eine algebraische Erweiterung und G eine Gröbner-Basis (bzgl. einer beliebigen Termordnung) von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. Dann ist

$$[k(\boldsymbol{x}) : k(\boldsymbol{g})] = |\{t \in \mathsf{T}(Z_1, ..., Z_n) : \forall s \in \text{HT}(G) : s \not| t\}|.$$

Insbesondere gilt für $p_1, ..., p_n \in G$ mit $\text{HT}(p_i) = Z_i^{\nu_i}$ die Abschätzung

$$[k(\boldsymbol{x}) : k(\boldsymbol{g})] \leq \prod_{i=1}^{n} \nu_i.$$

Wir betrachten nun mit dem *Minimalpolynom* ein wichtiges Hilfsmittel:

Bemerkung 10.2 Ist k_2/k_1 eine Körpererweiterung und $x \in k_2$ algebraisch über k_1, so existiert ein eindeutig bestimmtes normiertes Polynom kleinsten Grades $m \in k_1[Z]$ mit $m(x) = 0$. m ist prim und somit irreduzibel. Man nennt m das **Minimalpolynom** von x.

Bemerkung 10.3 Es ist $\deg(m) = [k_1(x) : k_1]$. Ist insbesondere $k_2 = k_1(x_1, ..., x_n)$ und m_i das Minimalpolynom von x_i, so gilt

$$[k_2 : k_1] = \prod_{i=1}^{n} \deg(m_i).$$

Man kann also den Grad einer algebraischen Erweiterung bestimmen, wenn man bereits die Minimalpolynome kennt.

Sei nun ein Element $f \in k(\boldsymbol{x})$ gegeben, welches algebraisch über $k(\boldsymbol{g})$ liegt. Wir interessieren uns dafür, wie man das Minimalpolynom von f bestimmen kann.
Hierzu werden wir folgende einfache Beobachtung ausnutzen:

Bemerkung 10.4 Es seien $A_1, ..., A_l$ neue formale (d.h. transzendente) Parameter über $k(\boldsymbol{g})$, $\alpha_1, ..., \alpha_l \in k(\boldsymbol{g})$ und G eine Gröbner-Basis von $\langle G \rangle \subseteq k(\boldsymbol{g})[\boldsymbol{Z}]$. Ferner seien $p_1, ..., p_s \in k(\boldsymbol{g})[\boldsymbol{Z}]$ sowie $h_1, ..., h_s \in k(\boldsymbol{g})[\boldsymbol{A}]$. Dann liefert die Spezialisierung $A_i \mapsto \alpha_i$ in der Normalform von $\sum_{i=1}^{s} h_i(\boldsymbol{A}) p_i(\boldsymbol{Z})$ modulo G gerade die Normalform von $\sum_{i=1}^{s} h_i(\boldsymbol{\alpha}) p_i(\boldsymbol{Z})$ modulo G.

Diese Bemerkung besagt im Prinzip, dass die Operationen „Bilden der Normalform“ und „Einsetzen“ kommutieren.

Sei nun eine Körpererweiterung $k(\boldsymbol{x})/k(\boldsymbol{g})$ gegeben, sowie $f(\boldsymbol{x})$ algebraisch über $k(\boldsymbol{g})$. Gesucht ist das Minimalpolynom $m(Y)$ von f. Es sei

$$m(Y) = Y^\alpha + \sum_{i=0}^{\alpha-1} \lambda_i Y^i \in k(\boldsymbol{g})[Y].$$

Für $f = \frac{n(\boldsymbol{x})}{d(\boldsymbol{x})}$ ist wegen $m(f) = 0$ insbesondere

$$\left(\frac{n(Z_1, ..., Z_n)}{d(Z_1, ..., Z_n)}\right)^\alpha + \sum_{i=0}^{\alpha-1} \lambda_i \left(\frac{n(Z_1, ..., Z_n)}{d(Z_1, ..., Z_n)}\right)^i \in \mathfrak{P}^{\mathrm{e}}_{(\boldsymbol{x})/k(\boldsymbol{g})}.$$

Äquivalent dazu können wir fordern:

$$d(\boldsymbol{Z})^\alpha \cdot \left(\left(\frac{n(\boldsymbol{Z})}{d(\boldsymbol{Z})}\right)^\alpha + \sum_{i=0}^{\alpha-1} \lambda_i \left(\frac{n(\boldsymbol{Z})}{d(\boldsymbol{Z})}\right)^i\right) \in \mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$$

(wir können bei „hinreichend gekürzter Darstellung von f“ von $d(\boldsymbol{Z}) \notin \mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ ausgehen).

Ob die letztgenannte Bedingung erfüllt ist, können wir durch einfache Normalformbildung modulo einer Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ verifizieren. Finden wir irgendwelche Koeffizienten λ_i, die dieser Bedingung genügen, so sind diese λ_i notwendigerweise die Koeffizienten des Minimalpolynoms von $f = \frac{n(\boldsymbol{x})}{d(\boldsymbol{x})}$ (da das Minimalpolynom eindeutig bestimmt ist).

Da der Grad α a priori nicht bekannt ist, können wir wie folgt vorgehen, um das Minimalpolynom zu finden:

Algorithmus 10.5 Bestimmung des Minimalpolynoms

Führe für $\beta = 1, 2, ...$ folgende Schritte aus:

1. Einführung neuer (algebraisch unabhängiger) Parameter $A_0, A_1, ..., A_{\beta-1}$ über $k(\boldsymbol{x})$.

2. Berechnung der Normalform $N(\boldsymbol{Z}) \in k(\boldsymbol{g})[\boldsymbol{A}][\boldsymbol{Z}]$ von

   $$d(\boldsymbol{Z})^\beta \cdot \left(\left(\frac{n(\boldsymbol{Z})}{d(\boldsymbol{Z})}\right)^\beta + \sum_{i=0}^{\beta-1} A_i \left(\frac{n(\boldsymbol{Z})}{d(\boldsymbol{Z})}\right)^i\right)$$

   modulo einer Gröbner-Basis G von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. Die Normalform ist linear in den A_i, da diese in der Gröbner-Basis nicht vorkommen. Bei dieser Berechnung werden die A_i wie Konstanten behandelt.

3. Zu jedem Term t von $N(\boldsymbol{Z})$ gehört ein Koeffizient $c_t = c_t(\boldsymbol{A})$. Da für das Minimalpolynom m gelten muss $m(f) = 0$, setzen wir alle $c_t(\boldsymbol{A})$ simultan $= 0$ und erhalten so ein lineares Gleichungssystem mit den Unbestimmten $A_0, ..., A_{\beta-1}$. Sobald dieses LGS lösbar ist, ist das Minimalpolynom gefunden und es ist $\beta = \alpha$.

Bemerkung 10.6 Ist für den Grad des Minimalpolynoms eine obere Schranke bekannt, so können wir statt „Hochzählen“ von β in Algorithmus 10.5 eine binäre Suche verwenden: Ist das LGS unlösbar, so ist β zu klein. Ist das LGS mehrdeutig lösbar, so ist β zu groß.

Bemerkung 10.7 Für den Fall, dass $x_1, ..., x_n$ algebraisch unabhängig sind, gilt:

$$\underbrace{[k(\boldsymbol{g})(f) : k(\boldsymbol{g})]}_{=\alpha} \leq \prod_{i=1}^{r} \deg(g_i(\boldsymbol{x})),$$

wobei $\deg(g_i(\boldsymbol{x}))$ als Maximum der Totalgrade von Zähler und Nenner (gekürzt) definiert ist.

Bemerkung 10.8 Anwendungen des Minimalpolynoms.

- Mit Hilfe des Minimalpolynoms kann man eine Körpererweiterung auf Separabilität testen, vgl. Abschnitt 2.3 in [Stein2000].
- In der Situation von Algorithmus 10.5 kann man über die Bestimmung des Minimalpolynoms auch testen, ob $f \in k(\boldsymbol{x})$ bereits in $k(\boldsymbol{g})$ enthalten ist („Membership Test“). Dies ist nämlich genau dann der Fall, wenn f ein lineares Minimalpolynom hat, also wenn der Algorithmus bei $\beta = 1$ abbricht. Man kann dies aber auch direkt testen:
$$f(\boldsymbol{x}) = \frac{n(\boldsymbol{x})}{d(\boldsymbol{x})} \in k(\boldsymbol{g}) \quad \Leftrightarrow \quad \frac{\mathrm{norm}(n(\boldsymbol{Z}), G)}{\mathrm{norm}(d(\boldsymbol{Z}), G)} = f(\boldsymbol{x}).$$
Auf diese Weise erhält man eine Darstellung von f über $k(\boldsymbol{g})$, siehe Kapitel 13.
- Das Minimalpolynom m von x ermöglicht die Berechnung von x^{-1} in $k(x)$. Es ist nämlich
$$\begin{aligned} m(x) = \sum_{i=0}^{\alpha} a_i x^i = 0 &\Leftrightarrow a_0 = -\sum_{i=1}^{\alpha} a_i x^i \\ &\Leftrightarrow 1 = x x^{-1} = -\sum_{i=1}^{\alpha} \frac{a_i}{a_0} x^i \\ &\Leftrightarrow x^{-1} = -\sum_{i=1}^{\alpha} \frac{a_i}{a_0} x^{i-1} \end{aligned}$$
und $a_0 \neq 0$, da das irreduzible Minimalpolynom nicht 0 als Nullstelle haben kann.

11 Zwischenkörper

Definition 11.1 Falls die Minimalpolynome der Erzeuger $x_1, ..., x_n$ über $k(\boldsymbol{x})$ alle in Linearfaktoren zerfallen und nur einfache Nullstellen haben, so ist $k(\boldsymbol{x})/k(\boldsymbol{g})$ **galoissch**. Wir bezeichnen die Gruppe der Automorphismen von $k(\boldsymbol{x})$, die $k(\boldsymbol{g})$ fix lassen, als **Galois-Gruppe** $\mathrm{Gal}(k(\boldsymbol{x})/k(\boldsymbol{g}))$.

Satz 11.2 Ist $k(\boldsymbol{x})/k(\boldsymbol{g})$ galoissch, so gilt:

$$\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}] = \prod_{\sigma \in \mathrm{Gal}(k(\boldsymbol{x})/k(\boldsymbol{g}))} \langle Z_1 - \sigma(x_1), ..., Z_n - \sigma(x_n) \rangle.$$

Insbesondere gilt folgende Charakterisierung:
Sind $\mathfrak{p}_1, ..., \mathfrak{p}_l$ die assoziierten Primideale von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}]$ und $G_1, ..., G_l$ die zugehörigen reduzierten Gröbner-Basen, dann ist

$$\{G_1, ..., G_l\} = \{ \{Z_1 - \sigma(x_1), ..., Z_n - \sigma(x_n)\} : \sigma \in \mathrm{Gal}(k(\boldsymbol{x})/k(\boldsymbol{g})) \}$$

Die Zwischenkörper von $k(\boldsymbol{x})/k(\boldsymbol{g})$ entsprechen den Untergruppen der Galois-Gruppe $\mathrm{Gal}(k(\boldsymbol{x})/k(\boldsymbol{g}))$.

Beispiel 11.3 Betrachte $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, d.h. $k = \mathbb{Q}$, $k(g) = \mathbb{Q}$ (d.h. $g = 1$) und $k(x_1, x_2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Es ist

$$\mathfrak{P}_{(\sqrt{2}, \sqrt{3})/\mathbb{Q}} = \langle Z_1^2 - 2, Z_2^2 - 3 \rangle.$$

Mit einem Computeralgebrasystem etwa erhalten wir die Primärzerlegung

$$\begin{aligned}\mathfrak{P}_{(\sqrt{2}, \sqrt{3})/\mathbb{Q}} \cdot k(\sqrt{2}, \sqrt{3})[Z_1, Z_2] = {} & \langle Z_1 - \sqrt{2}, Z_2 - \sqrt{3} \rangle \cap \langle Z_1 - \sqrt{2}, Z_2 + \sqrt{3} \rangle \\ & \cap \langle Z_1 + \sqrt{2}, Z_2 - \sqrt{3} \rangle \cap \langle Z_1 + \sqrt{2}, Z_2 + \sqrt{3} \rangle.\end{aligned}$$

Es ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Auch für nicht galoissche Erweiterungen kann man mit Hilfe der Primärzerlegung gewisse Zwischenkörper charakterisieren. Der folgende Satz 11.4 liefert eine Möglichkeit, für eine separabel algebraische Körpererweiterung Zwischenkörper zu finden, nachdem man die Primärzerlegung des Relationenideals $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}]$ berechnet hat. Dies ist besonders für Charakteristik 0 von Interesse, da in diesem Fall jede Körpererweiterung separabel ist.

Um zu testen, ob eine Erweiterung algebraisch und separabel ist, kann man die Verfahren aus den Kapiteln 9 und 10 verwenden.

Satz 11.4 Sei $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}] = Q_1 \cap ... \cap Q_l$ eine Primärzerlegung und $\mathfrak{p}_i$ das zu Q_i assoziierte Primideal. Ferner sei $k(\boldsymbol{h})$ ein Zwischenkörper von $k(\boldsymbol{g})$ und der algebraischen Hülle $k(\boldsymbol{g})^{\mathrm{alg}}$ von $k(\boldsymbol{g})$ in $k(\boldsymbol{x})$. Dann gilt:

1. Ist $k(\boldsymbol{g})^{\mathrm{alg}}/k(\boldsymbol{h})$ separabel, so ist für ein geeignetes $L \subseteq \{1, ..., l\}$

$$\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{h})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}] = \bigcap_{i \in L} \mathfrak{p}_i.$$

2. Ist $k(\boldsymbol{h})/k(\boldsymbol{g})$ separabel, so ist für ein geeignetes $L \subseteq \{1, ..., l\}$

$$\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{h})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}] = \bigcap_{i \in L} Q_i.$$

Wir können im Allgemeinen nicht erwarten, dass ein Erzeugendensystem von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{h})} \cdot k(\boldsymbol{x})[\boldsymbol{Z}]$ bereits mit Koeffizienten aus $k(\boldsymbol{h})$ auskommt. Wir können dies aber durch die Berechnung einer reduzierten Gröbner-Basis erzwingen (siehe auch Proposition 8.6):

Bemerkung 11.5 Die Koeffizienten einer Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{h})}k(\boldsymbol{x})[\boldsymbol{Z}]$ bilden ein Erzeugendensystem von $k(\boldsymbol{h})$ über k.

Bemerkung 11.6 Für den algebraischen Abschluss $k(\boldsymbol{g})^{\mathrm{alg}}$ von $k(\boldsymbol{g})$ existiert ein $i \in \{1, ..., l\}$ mit

$$\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})^{\mathrm{alg}}} \cdot k(\boldsymbol{x})[\boldsymbol{Z}] = \mathfrak{p}_i.$$

12 Finden „schöner“ Körpererzeuger

Hat man einen Zwischenkörper $k(\boldsymbol{h})$ von $k(\boldsymbol{x})/k(\boldsymbol{g})$ gefunden, so stellt sich die Frage, ob man ein besonders günstiges Erzeugendensystem für diese Erweiterung finden kann.

Polynomiale Erzeugendensysteme

Falls ein polynomiales Erzeugendensystem existiert, so hat dies den Vorteil, dass viele Rechnungen damit vereinfacht werden können. Will man etwa die Erzeuger des Relationenideals wie in Proposition 8.5 bestimmen, so erspart man sich das Berechnen der Saturierung, wenn man ein polynomiales Erzeugendensystem verwendet.

Bemerkung 12.1 Es sei $k(\boldsymbol{x})/k(\boldsymbol{g})$ algebraisch mit $g_1, ..., g_l \in k[\boldsymbol{x}]$ sowie $k(h_1, ..., h_s)$ ein Zwischenkörper von $k(\boldsymbol{x})/k(\boldsymbol{g})$. Dann existieren Polynome $p_1, ..., p_s \in k[\boldsymbol{x}]$ mit $k(\boldsymbol{h}) = k(\boldsymbol{g}, \boldsymbol{p})$.

B : Da $k(\boldsymbol{x})/k(\boldsymbol{g})$ algebraisch ist, gilt $\boldsymbol{h} \in k(\boldsymbol{g})[\boldsymbol{x}]$. Daher existieren $\boldsymbol{c} \in k[\boldsymbol{g}]$ mit $p_i := c_i h_i \in k[\boldsymbol{g}][\boldsymbol{x}] = k[\boldsymbol{x}]$, und mit $k(\boldsymbol{g}) \subseteq k(\boldsymbol{h})$ folgt $k(\boldsymbol{h}) = k(\boldsymbol{g}, c_1h_1, ..., c_sh_s)$. ■

Lemma 12.2 Es sei $k(\boldsymbol{h})$ ein algebraisch über $k(\boldsymbol{g})$ liegender Zwischenkörper von $k(\boldsymbol{x})/k(\boldsymbol{g})$. Ferner sei $k[\boldsymbol{x}]$ faktoriell. Sind $\boldsymbol{g} \in k[\boldsymbol{x}]$, so existieren $\boldsymbol{p} \in k[\boldsymbol{x}]$ mit $k(\boldsymbol{h}) = k(\boldsymbol{g}, \boldsymbol{p})$.

B : Es sei ein h_i fest gewählt mit $h_i = \frac{n}{d}$ für $n, d \in k[\boldsymbol{x}]$ teilerfremd, Œ $n \neq 0$. Wir betrachten das Minimalpolynom $m(Y)$ von $\frac{d}{n}$ über $k(\boldsymbol{g})$. Es seien $a_0, ..., a_l, b$ Polynome über k mit

$$m(Y) = b(\boldsymbol{g})^{-1} \sum_{i=0}^{l} a_i(\boldsymbol{g}) Y^i.$$

Multiplizieren wir die Gleichung $m(\frac{d}{n}) = 0$ mit dem Hauptnenner und subtrahieren $a_0(\boldsymbol{g})n^l$ auf beiden Seiten, so ergibt sich

$$-a_0(\boldsymbol{g})n^l = \sum_{i=1}^{l} a_i(\boldsymbol{g}) d^i n^{l-i} = d \cdot \left(\sum_{i=1}^{l} a_i(\boldsymbol{g}) d^{i-1} n^{l-i} \right).$$

Da $k[\boldsymbol{x}]$ faktoriell und n, d teilerfremd sind, folgt dass d ein Teiler von $a_0(\boldsymbol{g})$ ist und mit

$$k(\boldsymbol{g})(\underbrace{h_i}_{=\frac{n}{d}}) = k(\boldsymbol{g})\Big(\underbrace{a_0(\boldsymbol{g})\frac{n}{d}}_{=:p_i\in k[\boldsymbol{x}]}\Big)$$

folgt die Behauptung. ■

Man beachte, dass der Beweis ein konstruktives Verfahren zur Bestimmung der polynomialen Erzeuger von $k(\boldsymbol{h})$ bietet. Die verwendeten Minimalpolynome können mit Algorithmus 10.5 bestimmt werden.

Einfache transzendente Körpererweiterungen

Wir überlegen nun, wie man testen kann, ob eine rein transzendente Körpererweiterung von einem einzigen Element erzeugt wird und wie man dieses ggf. bestimmen kann.

Satz 12.3 (Lüroth)
Es seien $k(\boldsymbol{x})/k$ eine endlich erzeugte rein transzendente Erweiterung mit Transzendenzbasis $\{\boldsymbol{x}\}$ sowie ein Zwischenkörper $k(\boldsymbol{g})$ von $k(\boldsymbol{x})/k$ mit $\mathrm{transdeg}(k(\boldsymbol{g})/k) = 1$ gegeben. Dann ist die Erweiterung $k(\boldsymbol{g})/k$ einfach.

oder eine konstruktive Variante davon:

Seien $k(\boldsymbol{x})/k$ rein transzendent mit Transzendenzbasis $\{\boldsymbol{x}\}$, $k(\boldsymbol{g})$ ein Zwischenkörper von $k(\boldsymbol{x})/k$ sowie G eine reduzierte Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$. Dann sind folgende Aussagen äquivalent:

1. $k(\boldsymbol{g})/k$ ist einfach.
2. $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ ist ein Hauptideal.
3. Es existieren $n(\boldsymbol{Z}), d(\boldsymbol{Z}) \in k[\boldsymbol{Z}]$ und $f \in k(\boldsymbol{g})$ mit
$$G = \{n(\boldsymbol{Z}) - f d(\boldsymbol{Z})\} \quad \text{oder} \quad G = \emptyset.$$

Ist die letztgenannte Bedingung erfüllt, so ist entweder $k(\boldsymbol{g}) = k$ (falls $G = \emptyset$) oder f ist ein primitives Element (d.h. ein Körpererzeuger) von $k(\boldsymbol{g})/k$.

Zusammen mit Proposition 8.5 kann man nun entscheiden, ob $k(\boldsymbol{g})/k$ einfach ist und ggf. f durch das Berechnen eine reduzierten Gröbner-Basis bestimmen.

Beispiel 12.4 Sei $\mathrm{char}(k) = 0$ sowie

$$(g_1, g_2, g_3) =$$
$$\left(\frac{x_1^4 - 2x_1^2x_2 - 2x_1^2 - 8x_1 + x_2^2 - 8}{x_1^2 + 4x_1 + 4}, \frac{x_1^6 - 3x_1^4x_2 + 3x_1^2x_2^2 - x_2^3}{x_1^3 + 6x_1^2 + 12x_1 + 8}, \frac{x_1^4 - 2x_1^2x_2 + x_2^2}{x_1^3 + 3x_1^2 - x_1x_2 + 4x_1 - 2x_2 + 4}\right)$$

mit x_1, x_2 algebraisch unabhängig über k. Eine reduzierte Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{x})/k(\boldsymbol{g})}$ ergibt sich zu

$$\{Z_1^2 - Z_2 - \frac{x_1^2 - x_2}{x_1 + 2}(Z_1 + 2)\}.$$

Nach dem Satz von Lüroth ist $\frac{x_1^2-x_2}{x_1+2}$ Erzeuger von $k(g_1, g_2, g_3)$.

Bemerkung 12.5 Es ist leicht einzusehen, dass jeder nicht in k enthaltene Koeffizient des Polynoms in der reduzierten Gröbner-Basis als primitives Element verwendet werden kann.

13 Verwendung von Tag-Variablen

In diesem Abschnitt betrachten wir eine alternative Vorgehensweise, um einige der Probleme aus den vorherigen Kapiteln zu lösen. Primär gehen wir dabei auf das Problem ein, für ein $f(\boldsymbol{x}) \in k(g_1, ..., g_r)$ eine rationale Darstellung $f = q(\boldsymbol{g})$ zu finden (ähnlich wie bei der Bestimmung des Minimalpolynoms in Kapitel 10). Wir führen dazu sogenannte **Tag-Variablen** $T_1, ..., T_r$ ein.

Bemerkung 13.1 Es seien $f \in k(\boldsymbol{g})$ und $q \in k[\boldsymbol{T}]_{\mathfrak{P}_{(\boldsymbol{g})/k}}$ mit $q(\boldsymbol{g}) = f$ gegeben. Dann sind für $\tilde{q} \in k[\boldsymbol{T}]_{\mathfrak{P}_{(\boldsymbol{g})/k}}$ äquivalent:

1. $\tilde{q}(\boldsymbol{g}) = f$.
2. $q - \tilde{q} \in \mathfrak{P}_{(\boldsymbol{g})/k} \cdot k[Z_1, ..., Z_n]_{\mathfrak{P}_{(\boldsymbol{g})/k}}$.

Zur Charakterisierung *aller* Darstellungen von f in den $\boldsymbol{g}$ genügt es also, eine Darstellung von f zu berechnen sowie eine Basis von $\mathfrak{P}_{(\boldsymbol{g})/k} \cdot k[\boldsymbol{Z}]_{\mathfrak{P}_{(\boldsymbol{g})/k}}$. Um $\mathfrak{P}_{(\boldsymbol{g})/k}$ zu berechnen, können wir den folgenden Satz 13.2 benutzen:

Satz 13.2 Es sei

$$I := \langle n_1(\boldsymbol{Z}) - T_1 d_1(\boldsymbol{Z}), ..., n_r(\boldsymbol{Z}) - T_r d_r(\boldsymbol{Z})\rangle + \langle \mathfrak{P}_{(\boldsymbol{x})/k}\rangle \subseteq k[T_1, ..., T_r, \boldsymbol{Z}],$$

wobei $g_i = \frac{n_i(\boldsymbol{x})}{d_i(\boldsymbol{x})}$. Dann genügt I folgenden Bedingungen:

1. $\mathfrak{P}_{(\boldsymbol{g},\boldsymbol{x})/k} = \{p(\boldsymbol{T}, \boldsymbol{Z}) : p \in \mathfrak{P}_{(\boldsymbol{g}(\boldsymbol{x}),\boldsymbol{x})/k}\} = I : \left(\prod_{i=1}^{r} d_i(\boldsymbol{Z})\right)^{\infty}$.
2. $\mathfrak{P}_{(\boldsymbol{g})/k} = \{p(\boldsymbol{T}) : p \in \mathfrak{P}_{(\boldsymbol{g}(\boldsymbol{x}))/k}\} = \left(I : \left(\prod_{i=1}^{r} d_i(\boldsymbol{Z})\right)^{\infty}\right) \cap k[\boldsymbol{T}]$.

Um $\mathfrak{P}_{(\boldsymbol{g})/k}$ zu bestimmen, berechnen wir zuerst eine Gröbner-Basis des Ideals

$$I + \left\langle 1 - \lambda \prod_{i=1}^{r} d_i(\boldsymbol{Z})\right\rangle$$

in $k[\lambda, \boldsymbol{T}, \boldsymbol{Z}]$ bzgl. einer Termordnung mit $\lambda > \boldsymbol{Z} > \boldsymbol{T}$ und eliminieren λ. Aus der Gröbner-Basis entfernen wir alle Polynome, die einen Term enthalten, der nicht in $\mathsf{T}(\boldsymbol{T})$ liegt. Übrig bleibt die gewünschte Basis von $\mathfrak{P}_{(\boldsymbol{g})/k}$.

Nun kann man jede Darstellung von $f = q(\boldsymbol{g})$ in der Form $f = (q + r)(\boldsymbol{g})$ mit $r \in \mathfrak{P}_{(\boldsymbol{g})/k} \cdot k[\boldsymbol{Z}]_{\mathfrak{P}_{(\boldsymbol{g})/k}}$ angeben.

Wir wollen das Ideal $\mathfrak{P}_{(\boldsymbol{g})/k}$ auch nutzen, um Enthaltensein in $k(\boldsymbol{g})$ zu prüfen („membership test“).

Lemma 13.3 Es sei G eine Gröbner-Basis von $\mathfrak{P}_{(\boldsymbol{g},\boldsymbol{x})/k} \subseteq k[\boldsymbol{T},\boldsymbol{Z}]$ bzgl. einer Termordnung mit $\boldsymbol{Z} > \boldsymbol{T}$. Ferner sei

$$\pi : k[\boldsymbol{T},\boldsymbol{Z}] \to \mathrm{Quot}(k[\boldsymbol{T}]/\langle\mathfrak{P}_{(\boldsymbol{g})/k}\rangle)[\boldsymbol{Z}],$$
$$Z_j \mapsto Z_j, T_i \mapsto \overline{T}_i$$

($\overline{T}_i$ bezeichne die Äquivalenzklasse von T_i). Dann ist $\pi(G)\backslash\{\overline{0}\}$ eine Gröbner-Basis von $\langle\pi(\mathfrak{P}_{(\boldsymbol{g},\boldsymbol{x})/k})\rangle \subseteq \mathrm{Quot}(k[\boldsymbol{T}]/\langle\mathfrak{P}_{(\boldsymbol{g})/k}\rangle)[\boldsymbol{Z}]$ bzgl. der induzierten Termordnung.

Beachte, dass $\mathrm{Quot}(k[\boldsymbol{T}]/\langle\mathfrak{P}_{(\boldsymbol{g})/k}\rangle)[\boldsymbol{Z}] \cong k(\boldsymbol{g})[\boldsymbol{Z}]$ ist. Die Elemente $\boldsymbol{g}$ werden bei diesem Vorgehen durch die formalen Parameter $\boldsymbol{T}$ bzw. deren Restklassen dargestellt. Da wir die Gröbner-Basis $\pi(G)\backslash\{\overline{0}\}$ kennen, können wir Normalformen (also Nebenklassenvertreter) bestimmen und somit in $\mathrm{Quot}(k[\boldsymbol{T}]/\langle\mathfrak{P}_{(\boldsymbol{g})/k}\rangle)[\boldsymbol{Z}]$ effektiv rechnen. Insbesondere können wir feststellen, ob $\pi(f) = \overline{0}$ ist und somit vermeiden, durch $\overline{0}$ zu teilen.

Algorithmus 13.4 Membership Test

Um nun zu entscheiden, ob ein $f(\boldsymbol{x}) \in k(\boldsymbol{x})$ in $k(\boldsymbol{g})$ enthalten ist, können wir wie folgt vorgehen:
Sei $f(\boldsymbol{x}) = \frac{n(\boldsymbol{x})}{d(\boldsymbol{x})}$ mit $n \in k[\boldsymbol{Z}], d(\boldsymbol{Z}) \in k[\boldsymbol{Z}]\backslash\mathfrak{P}_{(\boldsymbol{x})/k}$. Dann ist $f(\boldsymbol{x}) \in k(\boldsymbol{g})$ äquivalent zu der Bedingung

$$\exists q \in \mathrm{Quot}(k[\boldsymbol{T}]/\langle\mathfrak{P}_{(\boldsymbol{g})/k}\rangle) : \pi(n(\boldsymbol{Z})) - q \cdot \pi(d(\boldsymbol{Z})) \in \langle\pi(\mathfrak{P}_{(\boldsymbol{g},\boldsymbol{x})/k})\rangle.$$

Wir gehen ähnlich wie bei der Berechnung des Minimalpolynoms in Algorithmus 10.5 vor:

1. Wir berechnen die Normalform $N(A)$ von $\pi(n(\boldsymbol{Z})) - A \cdot \pi(d(\boldsymbol{Z}))$ modulo der Gröbner-Basis $\pi(G)\backslash\{\overline{0}\}$.

2. Für $f(\boldsymbol{x}) \in k(\boldsymbol{g})$ muss die resultierende Normalform verschwinden, wenn wir den formalen Parameter A durch $q(\boldsymbol{g})$ ersetzen. Folglich setzen wir in dieser Normalform alle Koeffizienten (d.h. die Koeffizienten der $\boldsymbol{Z}$) simultan gleich 0. Wir erhalten ein lineares Gleichungssystem in einer Variablen. Dieses LGS können wir auf Lösbarkeit prüfen. Jede Lösung (zwangsläufig aus $\mathrm{Quot}(k[\boldsymbol{T}]/\langle\mathfrak{P}_{(\boldsymbol{g})/k}\rangle)$) liefert die gewünschte Darstellung $q(\boldsymbol{g})$ von f in den $\boldsymbol{g}$. Ein nicht lösbares LGS bedeutet $f \notin k(\boldsymbol{g})$.

Literatur

[BW1993] B , W :
Gröbner Bases, Springer.

[Bosch2001] B :
Algebra, Springer.

[CLO1992] C , L , O'S :
Ideals, Varieties and Algorithms, Springer.

[vzGG2003] G , G :
Modern Computer Algebra, Cambridge University Press.

[Eisen1995] E :
Commutative Algebra with a View toward Algebraic Geometry, Springer.

[Lang2002] L :
Algebra, Springer.

[Stein2000] S :
Zur algorithmischen Zerlegung polynomialer Gleichungssysteme, Dissertation (Universität Karlsruhe).

[vdWae1993] W :
Algebra II, Springer.

Index