Institut für Algebra

Skriptum zu den Vorlesungen

Kommutative Algebra und algebraische Geometrie

und

Gröbnerbasen

Wintersemester 2024

Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

Version 2. Oktober 2024

Adresse:
Assoz.-Prof. Dr. Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz
4040 Linz
e-mail: erhard.aichinger@jku.at
Version 1.10.2024

Diese Unterlagen sind im Zuge meiner Vorlesungen *Kommutative Algebra und algebraische Geometrie* und *Gröbnerbasen* entstanden. Teile dieser Unterlagen wurden von Georg Grasegger überarbeitet. Die Kapitel über Gröbnerbasen verdanken viele Anregungen einem unveröffentlichten Vorlesungsskript von Manuel Kauers.

Inhaltsverzeichnis

Teil 1

Kommutative Ringe

KAPITEL 1

Mengenlehre

1. Geordnete Mengen

Eine *geordnete Menge* $(M, \leq)$ ist ein Paar aus einer Menge und einer Ordnungsrelation (also einer reflexiven, transitiven und antisymmetrischen binären Relation) auf M. Die Relation ist $\leq$ ist *linear*, wenn für alle $x, y \in M$ gilt: $x \leq y$ oder $y \leq x$. Man nennt dann M eine *Kette*.

Definition 1.1. Eine geordnete Menge $(M, \leq)$ erfüllt die *Maximalbedingung*, wenn jede nichtleere Teilmenge von M ein maximales Element hat.

$(M, \leq)$ erfüllt also die Maximalbedingung, wenn

$$\forall N \subseteq M : N \neq \varnothing \Rightarrow \exists n \in N : (\forall x \in N : n \leq x \Rightarrow n = x).$$

gilt.

Definition 1.2. Eine geordnete Menge $(M, \leq)$ erfüllt die aufsteigende Kettenbedingung (ACC), wenn es keine injektive Funktion $f : \mathbb{N} \to M$ mit der Eigenschaft $f(i) < f(i+1)$ für alle $i \in \mathbb{N}$ gibt.

$(M, \leq)$ erfüllt also die (ACC), wenn es keine streng mononton wachsende Folge $\langle m_i \mid i \in \mathbb{N} \rangle$ aus M gibt.

Für die folgenden Sätze setzen wir voraus, dass die Axiome der Zermelo-Fränkelschen Mengenlehre mit Auswahlaxiom erfüllt sind.

Proposition 1.3. *Eine geordnete Menge $(M, \leq)$ erfüllt die* (ACC) *genau dann, wenn es für jede schwach monoton wachsende Folge $\langle m_i \mid i \in \mathbb{N} \rangle$ aus M ein $N \in \mathbb{N}$ gibt, sodass für alle $k \in \mathbb{N}$ mit $k \geq N$ gilt: $m_k = m_N$.*

Beweis: Sei $(M, \leq)$ eine geordnete Menge mit (ACC), und sei $\langle m_i \mid i \in \mathbb{N} \rangle$ eine schwach monoton wachsende Folge aus M. Wenn es kein N mit der gewünschten Eigenschaft gibt, so gibt es für alle $N \in \mathbb{N}$ ein $k > N$ mit $m_N < m_k$. Wir definieren nun eine Funktion $g : \mathbb{N} \to \mathbb{N}$ rekursiv. Sei $g(1) := 1$. Für $n \in \mathbb{N}$ definieren wir $g(n+1)$ als ein $k \in \mathbb{N}$ mit $m_{g(n)} < m_k$. Dann ist die Folge $\langle m_{g(n)} \mid n \in \mathbb{N} \rangle$ eine eine streng monoton wachsende Folge aus M, im Widerspruch zur (ACC).

Wenn $(M, \leq)$ die (ACC) nicht erfüllt, so gibt es eine streng monoton wachsende Folge aus M. Diese Folge wird aber nie konstant. □

Satz 1.4. *Für eine geordnete Menge $(M, \leq)$ sind äquivalent:*

(1) *$(M, \leq)$ erfüllt die* (ACC).

(2) $(M, \leq)$ *erfüllt die Maximalbedingung.*

Beweis: (1)⇒(2): Wir nehmen an, dass $(M, \leq)$ die (ACC) erfüllt. Wenn $(M, \leq)$ nun die Maximalbedingung nicht erfüllt, so besitzt M eine nichtleere Teilmenge T ohne maximales Element. Wir definieren nun eine Funktion $f : \mathbb{N} \to T$ rekursiv. Wir wählen $t \in T$ und definieren $f(1) := t$. Für $n \in \mathbb{N}$ definieren wir $f(n+1)$ folgendermaßen: Da $f(n)$ kein maximales Element von T ist, gibt es ein Element $t_1 \in T$, sodass $f(n) < t_1$. Wir definieren nun $f(n+1) := t_1$. Die Funktion f ist streng monoton wachsend, im Widerspruch dazu, dass $(M, \leq)$ die (ACC) erfüllt. (2)⇒(1): Wir nehmen an, dass $(M, \leq)$ die (ACC) nicht erfüllt. Dann gibt es eine streng monoton wachsende Funktion f von $\mathbb{N}$ nach M. Die Menge $T := \{f(i) \mid i \in \mathbb{N}\}$ hat dann kein maximales Element. Also erfüllt $(M, \leq)$ die Maximalbedingung nicht. □

Eine Möglichkeit, maximale Elemente einer Menge zu finden, bietet oft das Lemma von Zorn.

Satz 1.5 (Lemma von Zorn). *Sei $(M, \leq)$ eine geordnete Menge. Wir nehmen an, dass jede linear geordnete Teilmenge L von M eine obere Schranke in M hat. (Das heißt, dass es für jede linear geordnete Teilmenge L ein $m \in M$ gibt, sodass für alle $l \in L$ die Relation $l \leq m$ gilt.) Dann besitzt $(M, \leq)$ ein maximales Element.*

Beweis: Siehe etwa [**Hal76**].

KAPITEL 2

Ringe

1. Definition und Beispiele

DEFINITION 2.1. Eine algebraische Struktur $\mathbf{R} = \langle R, +, -, \cdot, 0\rangle$ ist ein *Ring*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und 0 ein Element aus R ist, sodass für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$ (0 ist rechtsneutral für $+$).
(2) $x + (-x) = 0$ ($-x$ ist additiv rechtsinvers zu x).
(3) $(x + y) + z = x + (y + z)$ ($+$ ist assoziativ).
(4) $x + y = y + x$ ($+$ ist kommutativ).
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ ist assoziativ).
(6) $x \cdot (y + z) = x \cdot y + x \cdot z$ (Linksdistributivgesetz).
(7) $(x + y) \cdot z = x \cdot z + y \cdot z$ (Rechtsdistributivgesetz).

SATZ 2.2. *Sei $\langle R, +, -, \cdot, 0\rangle$ ein Ring, und seien $x, y \in R$. Dann gilt*

(1) $-(-(x)) = x$
(2) $x \cdot 0 = 0 \cdot x = 0$.
(3) $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$.

PROOF. (1): $-(-x) = -(-x) + 0 = 0 + (-(-x)) = (x + (-x)) + (-(-x)) = x + ((-x) + (-(-x)) = x + 0 = x$. (2): Es gilt $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, also $0 = x \cdot 0 + (-(x \cdot 0)) = (x \cdot 0 + x \cdot 0) + (-(x \cdot 0)) = x \cdot 0 + (x \cdot 0 + (-(x \cdot 0))) = x \cdot 0 + 0 = x \cdot 0$. Die Identität $0 \cdot x = 0$ beweist man genauso. (3): Es gilt $(-x) \cdot y + x \cdot y = ((-x) + x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0$, also $(-x) \cdot y = -(x \cdot y)$. Die Identität $x \cdot (-y) = -(x \cdot y)$ beweist man genauso. □

Beispiele für Ringe: Sei V ein Vektorraum. Dann ist $\langle \mathrm{Hom}(V, V), +, -, \circ, 0\rangle$ ein Ring, der *Endomorphismenring* von V. Für einen Körper K und $n \in \mathbb{N}$ ist die Menge der Matrizen $K^{n\times n}$ ein Ring.

DEFINITION 2.3. Sei $\mathbf{R} = \langle R, +, -, \cdot, 0\rangle$ ein Ring.

(1) $e \in R$ ist ein *Einselement* von $\mathbf{R}$, wenn für alle $r \in R$ gilt, dass $e \cdot r = r \cdot e = r$. Wir bezeichnen dann die Struktur $\langle R, +, -, \cdot, 0, 1\rangle$ mit $1 := e$ als *Ring mit Eins*.
(2) Ein Ring mit Eins $\mathbf{R}$ ist ein *Schiefkörper*, wenn $|R| \geq 2$ gilt und es für alle $x \in R$ mit $x \neq 0$ ein $y \in R$ mit $x \cdot y = y \cdot x = 1$ gibt.
(3) $\mathbf{R}$ ist *kommutativ*, wenn für alle $r, s \in R$ gilt: $r \cdot s = s \cdot r$.
(4) Ein *Körper* ist ein kommutativer Schiefkörper.

(5) Ein kommutativer Ring mit Eins $\mathbf{R}$ ist ein *Integritätsbereich*, wenn $|R| \geq 2$ und für alle $r, s \in R$ gilt: $r \cdot s = 0 \Rightarrow (r = 0 \vee s = 0)$.

Wir werden statt $\mathbf{R}$ oft auch einfach R für die algebraische Struktur $\langle R, +, -, \cdot, 0, 1\rangle$ schreiben; mit ab meinen wir $a \cdot b$.

Beispiele für kommutative Ringe mit Eins: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i] = \{a + b\,i \mid a, b \in \mathbb{Z}\}$, der Polynomring $\mathbb{Q}[X]$ über $\mathbb{Q}$ in einer Variablen, der Polynomring $\mathbb{Q}[X_1, \ldots, X_n]$ in n Variablen.

2. Ideale

Definition 2.4. Sei R ein Ring, und sei I eine Untergruppe von $\langle R, +\rangle$. I ist ein

(1) *Linksideal* von R, wenn für alle $r \in R$ und $i \in I$ gilt, dass $ri \in I$.
(2) *Rechtsideal* von R, wenn für alle $r \in R$ und $i \in I$ gilt, dass $ir \in I$.
(3) *Ideal* von R, wenn es ein Links- und ein Rechtsideal ist.

Aus dieser Definition sieht man, dass der Durchschnitt von Idealen von R wieder ein Ideal von R ist.

Definition 2.5. Sei R ein Ring, und sei A eine Teilmenge von R. Dann ist das *von A erzeugte Ideal* $\langle A\rangle_R$ definiert durch

$$\langle A\rangle_R := \bigcap \{I \mid I \text{ Ideal von } R \text{ und } A \subseteq I\}.$$

Für kommutative Ringe mit Eins beschreiben wir nun, welche Elemente in dem von A erzeugten Ideal liegen.

Satz 2.6. *Sei R ein kommutativer Ring mit Eins, und sei $A \subseteq R$. Dann gilt*

$$\langle A\rangle_R = \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}.$$

Proof. Sei $J := \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}$. Da $0 \in J$, und da J abgeschlossen unter $+$ und unter Multipkation mit Elementen von R ist, ist J ein Ideal von R. Außerdem gilt offensichtlich $A \subseteq J$. J ist also ein Ideal von R mit $A \subseteq J$. Aus der Definition von $\langle A\rangle_R$ als Durchschnitt aller solchen Ideale sieht man also $\langle A\rangle_R \subseteq J$.

Um die Inklusion $J \subseteq \langle A\rangle_R$ zu zeigen, wählen wir ein Element $j \in J$. Es gibt also $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$, sodass $j = \sum_{i=1}^{n} r_i a_i$. Aus der Definition von $\langle A\rangle_R$ sehen wir, dass $A \subseteq \langle A\rangle_R$ gilt. Damit liegt jedes a_i in $\langle A\rangle_R$. Da $\langle A\rangle_R$ ein Ideal von R ist, liegt also auch jedes Summand $r_i a_i$ in $\langle A\rangle_R$, und schließlich auch die Summe j. □

Übungsaufgaben 2.7

(1) (Ideale im Matrixring) Zeigen Sie, dass der Ring $R := \mathbb{Q}^{2\times 2}$ aller 2×2-Matrizen über $\mathbb{Q}$ nur die Ideale $\{0\}$ und R hat, und dass jedes Linksideal von der Form $\{L \in \mathbb{Q}^{2\times 2} \mid \mathrm{row}(L) \subseteq U\}$ für einen Unterraum U von $\mathbb{Q}^2$ ist. Dabei ist $\mathrm{row}(L) = \mathrm{coim}(L)$ der von den Zeilen von L erzeugte Unterraum von $\mathbb{Q}^2$.

(2) (Erzeugen von Idealen) Bestimmen Sie jeweils, ob das von der Menge S erzeugte Ideal $\langle S\rangle$ des Rings R gleich dem ganzen Ring R ist!
   (a) $R = \mathbb{Z}$, $S = \{105, 70, 42, 30\}$.
   (b) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(4, 3), (6, 5)\}$.
   (c) $R = \mathbb{Z}_{101}$, $S = \{[75]_{101}\}$.

(3) (Erzeugen von Idealen) Bestimmen Sie jeweils, ob das von der Menge S erzeugte Ideal $\langle S\rangle$ des Rings $\mathbb{R}[X, Y]$ gleich dem ganzen Ring $\mathbb{R}[X, Y]$ ist!
   (a) $S = \{XY, X^3Y + 1\}$.
   (b) $S = \{X^2Y, XY^2 + 1\}$.
   (c) $S = \{XY + X, 1 + Y^2\}$.

DEFINITION 2.8. Sei R ein Ring, und sei I ein Ideal von R. Dann ist I *endlich erzeugt*, wenn es eine endliche Menge $A \subseteq R$ gibt, sodass $I = \langle A\rangle_R$. Wird ein Ideal von einem einzigen Element a erzeugt, so schreiben wir $I = (a)$. Ein Ideal von solcher Form heißt *Hauptideal*.

Wir bezeichnen die Menge aller Ideale eines Rings R mit $\mathsf{Id}\,(R)$.

SATZ 2.9. *Sei R ein Ring. Dann sind äquivalent:*

(1) *Jedes Ideal von R ist endlich erzeugt.*
(2) *Es gibt keine Folge $(I_k)_{k\in\mathbb{N}}$ von Idealen mit $I_k \subset I_{k+1}$ für alle $k \in \mathbb{N}$. (Die Menge der Ideale erfüllt die* aufsteigende Kettenbedingung (ACC)*).*
(3) *Jede nichtleere Teilmenge $\mathcal{I}$ von Idealen von R besitzt ein maximales Element M, das heißt*

$$\forall \mathcal{I} \subseteq \mathsf{Id}\,(R) : \Big(\mathcal{I} \neq \varnothing \Rightarrow \big(\exists M \in \mathcal{I}\ \forall N \in \mathcal{I} : M \subseteq N \Rightarrow M = N\big)\Big).$$

PROOF. (2)⇒(1): Sei I ein Ideal von R, das nicht endlich erzeugt ist. Wir konstruieren nun rekursiv eine Folge $\langle i_k \mid k \in \mathbb{N}\rangle$ von Elementen von I. Wir setzen $i_1 := 0$. Für $n \in \mathbb{N}$ definieren wir nun i_{n+1}. Da das Ideal $\langle\{i_1, \ldots, i_n\}\rangle_R$ endlich erzeugt ist, gilt $\langle\{i_1, \ldots, i_n\}\rangle_R \neq I$. Es gibt also $j \in I$ mit $j \notin \langle\{i_1, \ldots, i_n\}\rangle_R$. Sei i_{n+1} ein solches j.

Wir definieren nun für $k \in \mathbb{N}$ das Ideal I_k durch

$$I_k := \langle\{i_1, \ldots, i_k\}\rangle_R .$$

Dann ist die Folge $\langle I_k \mid k \in \mathbb{N}\rangle$ eine streng monoton wachsende Folge von Idealen von R, im Widerspruch zur (ACC). (1)⇒(2): Sei $\langle I_k \mid k \in \mathbb{N}\rangle$ eine bezüglich $\subseteq$ streng monoton wachsende Folge von Idealen von R. Dann ist $I := \bigcup\{I_k \mid k \in \mathbb{N}\}$ ebenfalls ein Ideal von R. Dieses Ideal I ist nach Voraussetzung endlich erzeugt. Seien $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in I$ so, dass $I = \langle a_1, \ldots, a_m\rangle_R$. Es gibt dann ein $N \in \mathbb{N}$, sodass $\{a_1, \ldots, a_m\} \subseteq I_N$. Dann gilt aber auch $I_{N+1} \subseteq I \subseteq I_N$, im Widerspruch zu $I_N \subset I_{N+1}$. Somit erfüllt $(\mathsf{Id}\ R, \subseteq)$ die (ACC). (2)⇒(3): Sei $\mathcal{I}$ eine nichtleere Menge von Idealen ohne maximales Element. Dann gibt es für jedes $M \in \mathcal{I}$ ein $N \in \mathcal{I}$ mit $M \subset N$. Wir konstruieren nun eine Folge aus $\mathcal{I}$ rekursiv: Sei I_1 ein Element aus $\mathcal{I}$, und für $n \geq 1$ sei I_{n+1} so, dass $I_n \subset I_{n+1}$. Dann ist $(I_n)_{n\in\mathbb{N}}$ eine aufsteigende Kette von Idealen, also erfüllt $\mathsf{Id}\ R$ die aufsteigende Kettenbedingung nicht. (3)⇒(2): Sei $(I_n)_{n\in\mathbb{N}}$ eine Folge von Idealen mit $I_n \subset I_{n+1}$ für alle $n \in \mathbb{N}$. Dann hat $\mathcal{I} := \{I_n \mid n \in \mathbb{N}\}$ kein maximales Element. □

Übungsaufgaben 2.10

Eine *geordnete Menge* $(M, \leq)$ ist ein Paar aus einer Menge und einer Ordnungsrelation (also einer reflexiven, transitiven und antisymmetrischen binären Relation) auf M. Eine geordnete Menge $(M, \leq)$ erfüllt die aufsteigende Kettenbedingung (ACC), wenn es keine injektive Funktion $f : \mathbb{N} \to M$ mit der Eigenschaft $f(i) < f(i+1)$ für alle $i \in \mathbb{N}$ gibt.

(1) Zeigen Sie: Eine geordnete Menge $(M, \leq)$ erfüllt die (ACC) genau dann, wenn es für jede schwach monoton wachsende Folge $\langle m_i \mid i \in \mathbb{N} \rangle$ aus M ein $N \in \mathbb{N}$ gibt, sodass für alle $k \in \mathbb{N}$ mit $k \geq N$ gilt: $m_k = m_N$.
(2) Zeigen Sie: Eine geordnete Menge M erfüllt die (ACC) genau dann, wenn jede nichtleere Teilmenge T von M ein in T maximales Element enthält.

Definition 2.11. Sei R ein kommutativer Ring mit Eins. R heißt *noethersch*[1], wenn jedes Ideal von R endlich erzeugt ist.

Definition 2.12. Sei R ein Ring. Ein Ideal I von R ist *maximal*, wenn $I \neq R$ ist und es kein Ideal J mit $I \subset J \subset R$ gibt.

In einem noetherschen Ring R ist jedes Ideal, das ungleich R ist, in einem maximalen Ideal enthalten. Aus dem Zornschen Lemma[2] folgt, dass das sogar für alle Ringe mit Eins gilt:

Satz 2.13. *Sei R ein Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Dann gibt es ein maximales Ideal M von R mit $I \subseteq M$.*

Proof. Sei

$$\mathcal{E} := \{J \mid J \text{ ist Ideal von } R \text{ und } I \subseteq J \neq R\}.$$

Um zu zeigen, dass $(\mathcal{E}, \subseteq)$ ein maximales Element hat, verwenden wir das Lemma von Zorn. Sei dazu $\mathcal{K}$ eine nichtleere Teilmenge von $\mathcal{E}$, die bezüglich $\subseteq$ linear geordnet ist. Wir setzen

$$S := \bigcup \{K \mid K \in \mathcal{K}\}.$$

Wir zeigen nun, dass S ein Ideal von R ist. Seien $i, j \in S$ und $r \in R$. Da $i \in S$, gibt es $K_1 \in \mathcal{K}$, sodass $i \in K_1$. Ebenso gibt es $K_2 \in \mathcal{K}$, sodass $j \in K_2$. Da $\mathcal{K}$ linear geordnet ist, gilt $K_1 \subseteq K_2$ oder $K_2 \subseteq K_1$. Wenn $K_1 \subseteq K_2$, so liegen $i + j$ und $r \cdot i$ in K_2; falls $K_2 \subseteq K_1$, liegen $i + j$ und $r \cdot i$ in K_1. In beiden Fällen liegen also $i + j$ und $r \cdot i$ in S. Somit ist S ein Ideal von R.

Nun zeigen wir, dass S in $\mathcal{E}$ liegt. Es gilt $I \subseteq S$. Es bleibt also zu zeigen, dass $S \neq R$. Nehmen wir an, $S = R$. Dann gilt $1 \in \bigcup \{K \mid K \in \mathcal{K}\}$. Es gibt also ein $K \in \mathcal{K}$ mit $1 \in K$. Dann gilt $K = R$. Somit gilt $R \in \mathcal{E}$, im Widerspruch zur Definition von $\mathcal{E}$. Es gilt also $S \neq R$, und somit $S \in \mathcal{E}$.

Das Zornsche Lemma liefert nun ein maximales Element M von $\mathcal{E}$. □

[1] Emmy Noether (1882-1935)

[2] Das Zornsche Lemma (Max Zorn (1906-1993), Kazimierz Kuratowski (1896-1980)) besagt:

> Sei $(M, \leq)$ eine geordnete Menge. Wir nehmen an, dass jede linear geordnete Teilmenge L von M eine obere Schranke in M hat. (Das heißt, dass es für jede linear geordnete Teilmenge L ein $m \in M$ gibt, sodass für alle $l \in L$ die Relation $l \leq m$ gilt.) Dann besitzt $(M, \leq)$ ein maximales Element.

ÜBUNGSAUFGABEN 2.14

(1) Sei R ein Ring, sei I ein endlich erzeugtes Ideal von R, und sei J ein Ideal von R mit $J \subseteq I$. Zeigen Sie, dass R ein Ideal M mit $J \subseteq M \subset I$ besitzt, sodass es kein Ideal N mit $M \subset N \subset I$ gibt.

3. Faktorringe und Homomorphiesatz

Sei R ein Ring mit Eins, und sei I ein Ideal von R. Wir definieren eine Relation $\sim_I$ auf R durch

$$a \sim_I b :\Leftrightarrow a - b \in I \text{ für } a, b \in R.$$

LEMMA 2.15. *Sei R ein Ring mit Eins, sei I ein Ideal von R, und sei $r \in R$. Dann gilt:*

(1) *Die Relation $\sim_I$ ist eine Äquivalenzrelation auf R.*
(2) *Die Äquivalenzklasse von r modulo $\sim_I$ ist gegeben durch $r/\sim_I := \{r + i \mid i \in I\}$. Wir schreiben für diese Klasse auch $[r]_I$ oder $r + I$.*

DEFINITION UND SATZ 2.16 (Faktorring). *Sei R ein Ring mit Eins, sei I ein Ideal von R, und sei*

$$R/I := \{r + I \mid r \in R\}$$

die Faktormenge von R modulo $\sim_I$. Wir definieren nun

$$\begin{aligned} (r + I) \oplus (s + I) &:= (r + s) + I \\ \ominus(r + I) &:= (-r) + I \\ (r + I) \odot (s + I) &:= (r \cdot s) + I. \end{aligned}$$

Dann sind die Operationen $\oplus$, $\ominus$ und $\odot$ "wohldefiniert", und die algebraische Struktur $(R/I, \oplus, \ominus, \odot, 0 + I, 1 + I)$ ist ein Ring mit Eins.

PROOF. Wir zeigen nur die Wohldefiniertheit von $\odot$. Sei dazu

$$m := \{\big((r + I, s + I), r \cdot s + I\big) \mid r, s \in R\}.$$

Wir zeigen, dass m eine Funktion von $R/I \times R/I$ nach R/I ist. Dazu zeigen wir, dass für alle $a, b, c_1, c_2 \in R/I$ gilt: Wenn $((a, b), c_1) \in m$ und $((a, b), c_2) \in m$, so gilt $c_1 = c_2$. Seien also $a, b, c_1, c_2 \in R/I$. Dann gibt es $r_1, s_1 \in R$, sodass $r_1 + I = a$, $s_1 + I = b$ und $r_1 \cdot s_1 + I = c_1$. Ebenso gibt es $r_2, s_2 \in R$, sodass $r_2 + I = a$, $s_2 + I = b$ und $r_2 \cdot s_2 + I = c_2$. Da $r_2 \in r_2 + I$, gilt auch $r_2 \in r_1 + I$. Somit gibt es $i \in I$ mit $r_2 = r_1 + i$. Ebenso gibt es $j \in I$ mit $s_2 = s_1 + j$. Es gilt nun $r_2 \cdot s_2 = (r_1 + i) \cdot (s_1 + j) = r_1 \cdot s_1 + r_1 \cdot j + i \cdot s_1 + i \cdot j$. Für $i' := r_1 \cdot j + i \cdot s_1 + i \cdot j$ gilt $i' \in I$. Folglich gilt

$$r_2 \cdot s_2 + I = (r_1 \cdot s_1 + i') + I.$$

Nun gilt für alle $t \in R$, dass $(t + i') + I = t + I$, da $(t + i') + i_1 = t + (i' + i_1) \in t + I$ und $t + i_2 = t + i' + (i_2 - i') \in (t + i') + I$. Also gilt $r_2 \cdot s_2 + I = r_1 \cdot s_1 + I$. Folglich gilt $c_1 = c_2$. Die Relation m ist also wirklich funktional, somit ist $\odot$ wohldefiniert. □

ÜBUNGSAUFGABEN 2.17

(1) Auf der Menge $\mathbb{Q}$ definieren wir die Relation

$$a \sim b :\Leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor .$$

Wir definieren:

$$[a]_\sim \odot [b]_\sim := [a\,b]_\sim$$

Was ist das Problem an dieser "Definition"?

Für zwei Ringe mit Eins R, S ist die Abbildung $h : R \to S$ ein *Homomorphismus*, wenn für alle $r_1, r_2 \in R$ gilt, dass $h(r_1 + r_2) = h(r_1) + h(r_2)$, $h(-r_1) = -h(r_1)$, $h(r_1 \cdot r_2) = h(r_1) \cdot h(r_2)$, $h(0_R) = 0_S$ und $h(1_R) = 1_S$. (Die Bedingungen $h(-r_1) = h(r_1)$ und $h(0_R) = h(0_S)$ sind insofern überflüssig, als sie sich aus den anderen Bedingungen ergeben.) Bijektive (injektive, surjektive) Homomorphismen heißen auch *Isomorphismen* (*Monomorphismen*, *Epimorphismen*), Monomorphismen heißen auch *Einbettungen*. R ist ein *Unterring* von S, wenn $R \subseteq S$, $0_S \in R$, $1_S \in R$, $r_1 +_R r_2 = r_1 +_S r_2$, $r_1 \cdot_R r_2 = r_1 \cdot_S r_2$ für alle $r_1, r_2 \in R$ gilt.

Satz 2.18 (Homomorphiesatz). *Seien R, S Ringe mit Eins, und sei $h : R \to S$ ein Homomorphismus. Dann ist* $\ker(h) := \{r \in R \mid h(r) = 0\}$ *ein Ideal von R,* $\mathrm{im}(h) := h(R)$ *ein Unterring von S, die Ringe $R/\ker(h)$ und* $\mathrm{im}(h)$ *sind isomorph, und $\hat{h}$ mit $\hat{h}(r + \ker(h)) := h(r)$ ist ein Isomorphismus.*

Satz 2.19 (Korrespondenzsatz). *Sei R ein Ring mit Eins, und sei I ein Ideal von R. Sei $\Phi : \{J \in \mathsf{Id}\,(R) \mid I \subseteq J\} \to \mathsf{Id}\,(R/I)$, $\Phi(J) := \{j + I \mid j \in J\}$. Dann ist Φ bijektiv, und es gilt für alle Ideale J_1, J_2 von R mit $I \subseteq J_1$, $I \subseteq J_2$: $J_1 \subseteq J_2 \Leftrightarrow \Phi(J_1) \subseteq \Phi(J_2)$.*

Proof. Wir zeigen zunächst, dass für jedes $J \in \mathsf{Id}\,(R)$ mit $I \subseteq J$ die Menge $\Phi(J)$ ein Ideal von R/I ist: Die Abbildung $\varphi := \{(r + I, r + J) \mid r \in R\}$ ist ein Homomorphismus von R/I nach R/J, und es gilt $\ker(\varphi) = \{r + I \mid r + J = 0 + J\} = \{r + I \mid r \in J\} = \Phi(J)$. Als Kern eines Homomorphismus ist $\Phi(J)$ daher ein Ideal von R/I.

Wir definieren $\Psi : \mathsf{Id}\,(R/I) \to \mathsf{Id}\,(R)$, $\Psi(K) := \bigcup\{r + I \mid r \in R, r + I \in K\} = \bigcup K$. Die Abbildung $\psi = \{(r, (r + I) + K) \mid r \in R\}$ ist ein Homomorphismus von R nach $(R/I)/K$ und es gilt $\ker(\psi) = \{r \in R \mid (r + I) + K = 0 + K\} = \{r \in R \mid r + I \in K\} = \bigcup K$. Für die letzte Gleichheit beobachten wir, dass für jedes $r \in R$ mit $r + I \in K$ gilt, dass $r \in r + I \in K$, also $r \in \bigcup K$; für jedes $s \in \bigcup K$ gibt es ein $t \in R$ mit $s \in t + I \in K$. Wegen $s + I = t + I$ gilt dann $s + I \in K$ und somit $s \in \{r \in R \mid r + I \in K\}$. Somit ist $\Psi(K)$ ein Ideal.

Sei J ein Ideal von R mit $I \subseteq J$. Dann gilt $\Psi(\Phi(J)) = \Psi(\{j + I \mid j \in J\}) = \bigcup\{j + I \mid j \in J\}$. Wegen $I \subseteq J$ gilt $\bigcup\{j + I \mid j \in J\} = J$. Sei nun K ein Ideal von R/I. Dann gilt $\Phi(\Psi(K)) = \Phi(\bigcup K) = \{j + I \mid j \in \bigcup K\} = \{j + I \mid \exists r \in R : j \in r + I \in K\} = \{j + I \mid j + I \in K\} = K$. Daher sind Φ und Ψ zueinander inverse Bijektionen.

Für Ideale $I \subseteq J_1 \subseteq J_2$ von R gilt offensichtlich $\Phi(J_1) \subseteq \Phi(J_2)$. Seien nun $J_1, J_2 \in \mathsf{Id}\,(R)$ so, dass $I \subseteq J_1$, $I \subseteq J_2$ und $\Phi(J_1) \subseteq \Phi(J_2)$. Dann gilt auch $\Psi(\Phi(J_1)) \subseteq \Psi(\Phi(J_2))$ also $J_1 \subseteq J_2$. □

Ein Ring mit Eins R ist *einfach*, wenn er nur die Ideale $\{0\}$ und R hat. Beispiele für einfache Ringe sind Körper und die Matrixringe $K^{n\times n}$ über einem Körper K.

SATZ 2.20. *Sei R ein kommutativer Ring mit Eins mit $|R| \geq 2$. Dann ist R genau dann einfach, wenn R ein Körper ist.*

PROOF. Sei R ein Körper, und sei I ein Ideal von R. Wenn $I \neq 0$, dann gibt es $i \in I$ mit $i \neq 0$. Dann gilt für jedes $r \in R$, dass $r = ri^{-1}i \in I$, also $R = I$.

Wenn R einfach und $r \in R$ mit $r \neq 0$ ist, so ist $I := \{rs \mid s \in R\}$ ein Ideal mit $I \neq \{0\}$, also $1 \in I$. Somit gibt es $s \in R$ mit $rs = 1$. Folglich ist R ein Körper. □

KOROLLAR 2.21. *Sei R ein kommutativer Ring mit Eins, und sei M ein maximales Ideal von R. Dann ist R/M ein Körper.*

4. Ringkonstruktionen

4.1. Polynome und Potenzreihen. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, und seien

$$\begin{aligned} S &:= \{f \mid f : {\mathbb{N}_0}^n \to R\} \\ P &:= \big\{f \in S \mid \{\boldsymbol{e} \in {\mathbb{N}_0}^n \mid f(\boldsymbol{e}) \neq 0\} \text{ ist endlich}\big\}. \end{aligned}$$

Auf S definieren wir Addition und Subtraktion durch

$$(f+g)(\boldsymbol{e}) := f(\boldsymbol{e}) + g(\boldsymbol{e}),\ (f-g)(\boldsymbol{e}) := f(\boldsymbol{e}) - g(\boldsymbol{e})$$

für $f, g \in S$, $\boldsymbol{e} \in {\mathbb{N}_0}^n$. Für $\boldsymbol{a}, \boldsymbol{b} \in {\mathbb{N}_0}^n$ setzen wir $\delta(\boldsymbol{a}, \boldsymbol{b}) := 1$, wenn $\boldsymbol{a} = \boldsymbol{b}$ und $\delta(\boldsymbol{a}, \boldsymbol{b}) := 0$, wenn $\boldsymbol{a} \neq \boldsymbol{b}$. Die Multiplikation ist definiert durch

$$f \cdot g\,(\boldsymbol{e}) \sum_{(\boldsymbol{a},\boldsymbol{b}) \in {\mathbb{N}_0}^n \times {\mathbb{N}_0}^n} \delta(\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{e}) f(\boldsymbol{a}) g(\boldsymbol{b}). \tag{2.1}$$

Für jedes $\boldsymbol{e} \in {\mathbb{N}_0}^n$ gibt es nur endlich viele $(\boldsymbol{a}, \boldsymbol{b}) \in {\mathbb{N}_0}^n \times {\mathbb{N}_0}^n$ mit $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{e}$, daher hat die Summe in (2.1) nur endlich viele Summanden $\neq 0$ und ist somit sinnvoll definiert. Für $e_1, \ldots, e_n \in \mathbb{N}_o$ schreiben wir $\overline{X}^{\boldsymbol{e}} = X_1^{e_1} \cdots X_n^{e_n}$ für die Funktion mit $\overline{X}^{\boldsymbol{e}}(\boldsymbol{e}) = 1$, $\overline{X}^{\boldsymbol{e}}(\boldsymbol{a}) = 0$ für $\boldsymbol{a} \neq \boldsymbol{e}$. Wir schreiben dann $f \in S$ als

$$f = \sum_{\boldsymbol{e} \in {\mathbb{N}_0}^n} f(\boldsymbol{e}) \overline{X}^{\boldsymbol{e}}.$$

Mit $\mathbf{1} := 1X_1^0 \cdots X_n^0$ und $\mathbf{0}$ der konstanten 0-Funktion von ${\mathbb{N}_0}^n$ nach R gilt dann, dass $(S, +, -, \cdot, \mathbf{0}, \mathbf{1})$ ein kommutativer Ring mit Eins ist, der *Ring der formalen Potenzreihen* mit Koeffizienten in R in n Variablen. Er wird mit $R[[X_1, \ldots, X_n]]$ bezeichnet. Die Menge P bildet einen Unterring von S, den *Polynomring in n Variablen* über R. Dieser Polynomring wird mit $R[X_1, \ldots, X_n]$ bezeichnet.

LEMMA 2.22. *Sei R ein kommutativer Ring mit Eins, seien $\boldsymbol{c}, \boldsymbol{d} \in {\mathbb{N}_0}^n$ und $r, s \in R$. Dann gilt $(r\overline{X}^{\boldsymbol{c}}) \cdot (s\overline{X}^{\boldsymbol{d}}) = (rs)\overline{X}^{\boldsymbol{c}+\boldsymbol{d}}$.*

PROOF. Sei $f := r\overline{X}^{\boldsymbol{c}}$ und $g := s\overline{X}^{\boldsymbol{d}}$. Dann gilt

$$\begin{aligned}(f \cdot g)(\boldsymbol{e}) &= \sum_{(\boldsymbol{a},\boldsymbol{b}) \in {\mathbb{N}_0}^n \times {\mathbb{N}_0}^n} \delta(\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{e}) f(\boldsymbol{a}) g(\boldsymbol{b}) \\ &= \delta(\boldsymbol{c}+\boldsymbol{d}, \boldsymbol{e}) f(\boldsymbol{c}) g(\boldsymbol{d}) \\ &= \delta(\boldsymbol{c}+\boldsymbol{d}, \boldsymbol{e}) rs,\end{aligned}$$

und somit $f \cdot g = rs\overline{X}^{\boldsymbol{c}+\boldsymbol{d}}$. □

Sei R ein kommutativer Ring mit Eins, sei T ein kommutativer Ring mit Eins, der R als Unterring enthält, und sei $p \in R[X_1, \ldots, X_n]$. Seien $t_1, \ldots, t_n \in T$. Dann ist die Abbildung $\varepsilon : R[X_1, \ldots, X_n] \to T$,

$$\varepsilon\Big(\sum_{(e_1,\ldots,e_n)\in E} c_{(e_1,\ldots,e_n)} X_1^{e_1} \cdots X_n^{e_n}\Big) := \sum_{(e_1,\ldots,e_n)\in E} c_{(e_1,\ldots,e_n)} t_1^{e_1} \cdots t_n^{e_n}$$

ein Homomorphismus. Die interessante Eigenschaft ist dabei, dass $\varepsilon(p \cdot q) = \varepsilon(p) \cdot \varepsilon(q)$ gilt; diese Eigenschaft ist der Grund, dass wir die Multiplikation wie in (2.1) definiert haben. Wir bezeichnen dann $\varepsilon(p)$ auch als $\hat{p}(t_1, \ldots, t_n)$ oder einfach als $p(t_1, \ldots, t_n)$ und nennen $\hat{p}(t_1, \ldots, t_n)$ die *Auswertung* von p an der Stelle $(t_1, \ldots, t_n)$. Sei nun $U \subseteq T$. Der von R und U *erzeugte* Ring $R[U]$ ist definiert als der Durchschnitt aller Unterringe V von T mit $R \cup U \subseteq V$. Dann gilt

$$R[U] = \{\hat{p}(u_1, \ldots, u_n) \mid n \in \mathbb{N}_0, u_1, \ldots, u_n \in U, p \in R[X_1, \ldots, X_n]\}.$$

4.2. Quotientenkörper. Wir verallgemeinern jetzt die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$. Sei dazu D ein Integritätsbereich. Auf der Menge $\{(a,b) \in D^2 \mid b \neq 0\}$ definieren wir eine Relation durch $(a,b) \sim (c,d) :\Leftrightarrow ad = bc$. Diese Relation ist eine Äquivalenzrelation, und wir kürzen die Klasse $(a,b)/\!\sim$ mit $\frac{a}{b}$ ab. Mit $Q(D)$ bezeichnen wir die Faktormenge $\{(a,b) \in D^2 \mid b \neq 0\}/\!\sim$. Auf $Q(D)$ definieren wir $+$ durch $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, $-$ durch $-\frac{a}{b} := \frac{-a}{b}$, und $\cdot$ durch $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.

SATZ UND DEFINITION 2.23. *Sei D ein Integritätsbereich. Dann ist $\langle Q(D), +, -, \cdot, \frac{0}{1}, \frac{1}{1}\rangle$ ein Körper. Er heißt der* Quotientenkörper *von D.*

SATZ 2.24. *Sei D ein Integritätsbereich, sei K ein Körper, und sei φ ein Monomorphismus von D nach K. Dann ist $\psi : Q(D) \to K$, $\psi(\frac{a}{b}) := \varphi(a) \cdot (\varphi(b))^{-1}$ wohldefiniert und ein Monomorphismus vom Quotientenkörper von D nach K.*

Sei K ein Körper. Den Quotientenkörper des Polynomrings $K[X_1, \ldots, X_n]$ bezeichnet man als den Körper der *rationalen Funktionen vom Transzendenzgrad n über K*, und kürzt ihn mit $K(X_1, \ldots, X_n)$ ab.

ÜBUNGSAUFGABEN 2.25

(1) Sei D ein Integritätsbereich, und sei $S \subseteq D \setminus \{0\}$ eine unter $\cdot$ abgeschlossene Teilmenge von D mit $1 \in S$. Zeigen Sie, dass $S^{-1}D := \{\frac{d}{s} \mid s \in S\}$ ein Unterring von $Q(D)$ ist. Man nennt diesen Unterring die *Lokalisierung* von R nach S.
(2) Beschreiben Sie für $D = \mathbb{Z}$ und $S = \{x \in \mathbb{Z} : 2 \nmid x\}$ jene Elemente von $\mathbb{Q}$, die in $S^{-1}D$ liegen.
(3) Beschreiben Sie für $D = \mathbb{Z}$ und $S = \{2^n \mid n \in \mathbb{N}_0\}$ jene Elemente von $\mathbb{Q}$, die in $S^{-1}D$ liegen.
(4) Welche reellen Zahlen liegen in $S^{-1}\mathbb{Z}$ für $S = \{10^n \mid n \in \mathbb{N}\}$?

KAPITEL 3

Teilbarkeit in Integritätsbereichen

1. Teilbarkeit und prime Elemente

DEFINITION 3.1 (Teilbarkeit). Sei R ein kommutativer Ring mit Eins, und seien $a, b \in R$. Dann gilt $a \mid b$, wenn es ein $r \in R$ gibt, sodass $b = ra$. In diesem Fall ist a ein *Teiler* von b und b ein *Vielfaches* von a.

DEFINITION 3.2. Sei R ein kommutativer Ring mit Eins.

- Ein Element $u \in R$ ist *invertierbar*, wenn es ein $v \in R$ mit $uv = 1$ gibt.
- Ein Element $p \in R$ ist *prim*, wenn es nicht invertierbar ist, und für alle $a, b \in R$ mit $p \mid ab$ gilt: $p \mid a$ oder $p \mid b$.
- Ein Element $r \in R$ ist *irreduzibel*, wenn es nicht invertierbar ist, und für alle $s, t \in R$ mit $r = st$ gilt: s ist invertierbar oder t ist invertierbar.
- Zwei Elemente $a, b \in R$ sind *assoziiert*, wenn es ein invertierbares Element $u \in R$ gibt, sodass $au = b$. Wir schreiben dann $a \sim b$ oder $a \sim_R b$.

LEMMA 3.3. *Sei R ein Integritätsbereich, und sei p ein primes Element von R mit $p \neq 0$. Dann ist p irreduzibel.*

PROOF. Sei p prim, $p \neq 0$, und seien $s, t \in R$ so, dass $p = st$. Dann gilt $p \mid st$. Da p prim ist, gilt $p \mid s$ oder $p \mid t$. Im Fall $p \mid s$ gibt es ein $s_1 \in R$, sodass $ps_1 = s$. Durch Multiplikation dieser Gleichung mit t erhalten wir $ps_1t = st = p$. Also gilt $p(s_1t - 1) = 0$. Wegen $p \neq 0$ ist also t invertierbar. Im Fall $p \mid t$ erhalten wir analog, dass s invertierbar ist. □

ÜBUNGSAUFGABEN 3.4

(1) Sei R ein kommutativer Ring mit Eins. Zeigen Sie jeweils, dass die angeführte Implikation für alle $x, y, z \in R$ gilt.
   (a) $(x \mid y$ und $x \mid z) \Rightarrow x \mid (y + z)$.
   (b) $x \mid y \Rightarrow x \mid zy$.
   (c) $(x \mid y$ und $y \mid z) \Rightarrow x \mid z$.
   (d) $x \mid y \Rightarrow zx \mid zy$.

(2) Sei R ein Integritätsbereich, und seien $x, y, z \in R$ mit $z \neq 0$. Zeigen Sie:
   (a) $x \mid y$ und $y \mid x \Leftrightarrow x$ und y sind assoziiert.
   (b) $x \mid y \Leftrightarrow xz \mid yz$.

(3) (Invertierbare Elemente) Sei R ein kommutativer Ring mit Eins. Zeigen Sie:
   (a) Das Produkt invertierbarer Elemente ist wieder invertierbar.
   (b) Jeder Teiler eines invertierbaren Elements ist invertierbar.
   (c) Ein Element $r \in R$ ist genau dann invertierbar, wenn das von r erzeugte Ideal (r) gleich R ist.

(4) (Invertierbare Elemente) Sei R ein kommutativer Ring mit Eins, sei u invertierbar, und seien v_1, v_2 so, dass $uv_1 = uv_2 = 1$. Zeigen Sie $v_1 = v_2$.
(5) (Assoziierte Elemente) Sei R ein kommutativer Ring mit Eins, und $a_1, a_2, b_1, b_2 \in R$. Wenn $a_1 \sim_R a_2$ und $b_1 \sim_R b_2$, so gilt $a_1 b_1 \sim_R a_2 b_2$.
(6) (Integritätsbereiche) Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. (*Hinweis:* Betrachten Sie für $r \neq 0$ die Abbildung $x \mapsto r \cdot x$.)
(7) (Integritätsbereiche) Zeigen Sie: Jeder Integritätsbereich, der kein Körper ist, besitzt eine unendlich absteigende Kette von Idealen $I_1 \supset I_2 \supset I_3 \supset \cdots$.
(8) (Prime Elemente) Sei R ein Integritätsbereich. Ein Ideal I von R ist *prim*, wenn $I \neq R$ und für alle $a, b \in R$ gilt: $a \cdot b \in I \Rightarrow (a \in I$ oder $b \in I)$. Zeigen Sie:
   (a) Ein Element r ist genau dann prim, wenn das Hauptideal (r) prim ist.
   (b) Wenn r prim und u invertierbar ist, so ist auch $r \cdot u$ prim.
(9) (Einfache Ringe) Ein Ring R ist *einfach*, wenn er keine Ideale außer $\{0\}$ und R hat. Zeigen Sie, dass die beiden folgenden Behauptungen äquivalent sind:
   (a) R ist ein einfacher kommutativer Ring mit Eins, und $|R| \geq 2$.
   (b) R ist ein Körper.
(10) (Irreduzible Elemente) Sei R ein Integritätsbereich, und sei $r \in R$ mit $r \neq 0$.
   (a) Zeigen Sie, dass folgende Bedingungen äquivalent sind.
      (i) r ist irreduzibel.
      (ii) Das Ideal (r) ist ein maximales Element in der Menge aller Hauptideale von R, die ungleich R sind.
   (b) Zeigen Sie: Wenn r irreduzibel ist, ist auch jedes zu r assoziierte Element irreduzibel.

2. Größte gemeinsame Teiler

Definition 3.5. Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Ein Element $d \in R$ ist ein *größter gemeinsamer Teiler* von A, wenn

(1) für alle $a \in A$ gilt $d \mid a$.
(2) für alle $d' \in R$ gilt: $(\forall a \in A : d' \mid a) \Rightarrow d' \mid d$.

Für zwei größte gemeinsame Teiler d_1, d_2 von A gilt also, dass $d_1 \mid d_2$ und $d_2 \mid d_1$. Wenn R ein Integritätsbereich ist, sind d_1 und d_2 assoziiert.

Lemma 3.6. *Sei R ein Integritätsbereich, sei A eine Teilmenge von R, und seien $t \in R \setminus \{0\}$, $d_1, d_2 \in R$. Wir nehmen an, dass d_1 ein größter gemeinsamer Teiler von A und d_2 ein größter gemeinsamer Teiler von $tA = \{ta \mid a \in A\}$ ist. Dann sind td_1 und d_2 assoziiert.*

Proof. Da td_1 jedes Element von tA teilt, gilt $td_1 \mid d_2$. Da t ein gemeinsamer Teiler von tA ist, gilt $t \mid d_2$. Sei $d_3 \in R$ so, dass $td_3 = d_2$. Da td_3 jedes Element in tA teilt und $t \neq 0$, teilt d_3 jedes Element in A, und somit gilt $d_3 \mid d_1$ und somit $td_3 \mid td_1$, also $d_2 \mid td_1$. □

Übungsaufgaben 3.7

(1) Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Ein Element $v \in R$ ist ein *kleinstes gemeinsames Vielfaches* von A, wenn für alle $a \in A$ gilt, dass $a \mid v$, und wenn für alle $v' \in R$, die von allen $a \in A$ geteilt werden, gilt, dass $v \mid v'$. Zeigen Sie: Wenn jede Teilmenge von R einen größten gemeinsamen Teiler hat, so hat auch jede Teilmenge von R ein kleinstes gemeinsames Vielfaches.

3. Euklidische Integritätsbereiche

DEFINITION 3.8. Sei R ein Integritätsbereich. Der Integritätsbereich R ist ein *Euklidischer Bereich*, wenn es eine Funktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$ gibt, sodass folgendes gilt.

(1) Für alle $a, b \in R \setminus \{0\}$ gilt $\delta(a) \leq \delta(a\,b)$.
(2) Für alle $a, b \in R$ mit $a \neq 0$ gibt es $q, r \in R$, sodass
   (a) $b = a\,q + r$, und
   (b) $r = 0$ oder $\delta(r) < \delta(a)$.

SATZ 3.9. *Der Ring $\mathbb{Z}$ ist ein Euklidischer Bereich.*

PROOF. Die Funktion $\delta(z) := |z|$ für $z \in \mathbb{Z} \setminus \{0\}$ leistet das Gewünschte. □

SATZ 3.10. *Sei K ein Körper, und sei $K[X]$ der Polynomring über K. Dann ist $K[X]$ ein Euklidischer Bereich.*

PROOF. Wir setzen $\delta(f) := \deg(f)$. □

DEFINITION 3.11. Sei $\mathbb{Z}[i]$ die Teilmenge der komplexen Zahlen, die durch

$$\mathbb{Z}[i] := \{x + y\,i \mid x, y \in \mathbb{Z}\}$$

definiert ist. Als Operationen verwenden wir die Addition und Multiplikation der komplexen Zahlen. Dann nennen wir $\mathbb{Z}[i]$ den *Ring der Gaußschen ganzen Zahlen*.

SATZ 3.12. *$\mathbb{Z}[i]$ ist ein Euklidischer Bereich.*

PROOF. Als Unterring des Körpers $\mathbb{C}$ ist $\mathbb{Z}[i]$ ein Integritätsbereich. Wir definieren nun $\delta(x + y\,i) := x^2 + y^2$ für alle $x, y \in \mathbb{Z}$. Dann gilt $\delta(z_1 \cdot z_2) = \delta(z_1) \cdot \delta(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}[i]$, und somit ist Eigenschaft (1) von Definition 3.8 erfüllt.

Seien nun $b, a \in \mathbb{Z}[i]$ mit $a \neq 0$, und seien $u', v' \in \mathbb{Q}$ so, dass $b = a \cdot (u' + v'\,i)$. Wir wählen nun $u, v \in \mathbb{Z}$, sodass $|u - u'| \leq \frac{1}{2}$ und $|v - v'| \leq \frac{1}{2}$. Sei nun

$$q := u + v\,i \text{ und } r := b - q\,a.$$

Für alle $x, y \in \mathbb{Q}$ definieren wir $\hat{\delta}(x + y\,i) := x^2 + y^2 = \det(\begin{pmatrix} x & -y \\ y & x \end{pmatrix})$. Dann gilt

$$\begin{aligned}\delta(r) = \delta((u' + v'\,i) \cdot a - (u + v\,i) \cdot a) &= \delta(a \cdot ((u' - u) + (v' - v)\,i)) \\ &= \hat{\delta}(a) \cdot \hat{\delta}((u' - u) + (v' - v)\,i) = \delta(a) \cdot ((u' - u)^2 + (v' - v)^2) \leq \delta(a) \cdot \frac{1}{2}.\end{aligned}$$

Da $a \neq 0$, gilt $\delta(a) = a\overline{a} \neq 0$, und somit gilt $\delta(r) < \delta(a)$. □

DEFINITION 3.13. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

SATZ 3.14. *Jeder Euklidische Bereich ist ein Hauptidealbereich.*

PROOF. Sei R ein Euklidischer Bereich, und sei I ein Ideal von R. Wenn $I = \{0\}$, so gilt $I = (0)$. Wenn $I \neq 0$, so wählen wir ein $a \in I \setminus \{0\}$, für das $\delta(a)$ minimal ist. Sei nun $b \in I$, und seien $q, r \in R$ so, dass $b = q\,a + r$ und ($r = 0$ oder $\delta(r) < \delta(a)$). Da $r = b - q\,a \in I$, kann $\delta(r) < \delta(a)$ wegen der Minimalität von $\delta(a)$ nicht gelten. Also gilt $r = 0$ und $b = q\,a \in (a)$. Somit gilt $I = (a)$. □

SATZ 3.15. *Sei R ein Hauptidealbereich. Dann besitzt jede Teilmenge A von R einen größten gemeinsamen Teiler.*

PROOF. Sei $d \in R$ so, dass (d) das von A erzeugte Ideal ist. Da jedes Element von A in (d) liegt, gilt $\forall a \in A : d \mid a$. Sei nun d' ein weiterer gemeinsamer Teiler von A. Da $d \in \langle A \rangle_R$, gibt es $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$ mit $d = \sum_{i=1}^{n} r_i a_i$. Da d' jedes a_i teilt, gilt dann auch $d' \mid d$. Somit ist d ein größter gemeinsamer Teiler von A. □

In einem Euklidischen Bereich kann für eine endliche Menge die Menge aller größten gemeinsamen Teiler ggTM(A) von $A = \{a_1, \ldots, a_n\}$ dadurch ausrechnen, dass

(1) ggTM$(\varnothing) = \{0\}$, ggTM$(A) =$ ggTM$(A \setminus \{0\})$,
(2) ggTM$(\{a_1, \ldots, a_n\}) =$ ggTM$(\{r_1, a_2, \ldots, a_n\})$, wenn $a_1 \neq 0$, $a_2 \neq 0$, $\delta(a_1) \geq \delta(a_2)$, und $a_1 = qa_2 + r_1$ mit $q \in R$ und ($r_1 = 0$ oder $\delta(r_1) < \delta(a_2)$).

Die Gleichheiten der Form ggTM$(B) =$ ggTM(C) gelten dabei stets deswegen, weil B und C die gleichen gemeinsamen Teiler haben. Durch diese Gleichheiten erhält man ein $d \in R$ mit ggTM$(A) =$ ggTM$(\{d\})$, also ist d ein größter gemeinsamer Teiler. Durch Buchführung erhält man auch $r_1, \ldots r_n \in R$ mit $\sum_{i=1}^{n} r_i a_i = d$ (erweiterter Euklidischer Algorithmus).

Beispiel: Wir berechnen ggT$(147, 33)$, und schreiben das so:

	147	33	
147	1	0	$(147 = 1 \cdot 147 + 0 \cdot 33)$
33	0	1	$(33 = 0 \cdot 147 + 1 \cdot 33)$
15	1	−4	$(15 = 1 \cdot 147 - 4 \cdot 33)$
3	−2	9	$(3 = -2 \cdot 147 + 9 \cdot 33)$
0			

Das ermöglicht noch nicht alle ggT-Berechnungen: obwohl es in $\mathbb{Q}[X, Y]$ stets größte gemeinsame Teiler gibt, kann man diese nicht (direkt) mit dem Euklidischen Algorithmus ausrechnen.

BEISPIEL 3.16. Der Polynomring $\mathbb{Q}[X, Y]$ ist kein Hauptidealbereich.

PROOF. Sei $I := \{p \in \mathbb{Q}[X, Y] \mid \overline{p}(0, 0) = 0\}$. Dann gilt $X \in I$ und $Y \in I$. Wenn I ein Hauptideal ist, so gibt es $f \in I$ mit $f \mid X$ und $f \mid Y$. Also gilt $\deg_X(f) = 0$ und $\deg_Y(f) = 0$, und somit ist f ein konstantes Polynom. Da $f \in I$, gilt $\overline{f}(0, 0) = 0$, und somit $f = 0$. Das ist ein Widerspruch zu $f \mid X$. Somit ist I kein Hauptideal. □

SATZ 3.17. *Sei R ein Hauptidealbereich, und sei $p \in R$ ein irreduzibles Element von R. Dann ist p prim.*

PROOF. Seien $a, b \in R$ so, dass $p \mid a\,b$. Sei $J := \{s\,p + t\,a \mid s, t \in R\}$ das von $\{p, a\}$ erzeugte Ideal von R. Da J ein Hauptideal ist, gibt es $c \in J$ mit $(c) = J$. Dann gilt $c \mid p$ und $c \mid a$. Sei $d \in R$ so, dass $c\,d = p$. Da p irreduzibel ist, ist c invertierbar oder d invertierbar. Wenn c invertierbar ist, so gilt $1 \in J$. Also gibt es $s', t' \in R$ mit $s'p + t'a = 1$. Dann gilt $s'pb + t'ab = b$, und somit $p \mid b$. Wenn d invertierbar ist, so gilt wegen $c \mid a$ auch $p = c\,d \mid a\,d$. Da d invertierbar ist, gilt $a\,d \mid a$, und somit $p \mid a$. □

ÜBUNGSAUFGABEN 3.18

(1) Sei R ein Hauptidealbereich, und sei r ein irreduzibles Element von R.
   (a) Zeigen Sie, dass (r) ein maximales Ideal von R ist.
   (b) Zeigen Sie, dass $R/(r)$ ein Integritätsbereich ist. Was bedeutet das für das Element r?
(2) Zeigen Sie, dass $\mathbb{Z}[X]$ kein Hauptidealbereich ist.

4. Eine Anwendung in der Zahlentheorie

Wir brauchen zunächst folgende Beobachtung:

LEMMA 3.19. *Sei p eine ungerade Primzahl. Dann gilt:*

(1) *Für jedes $x \in \{1, \dots, p-1\}$ gibt es ein $y \in \{1, \dots, p-1\}$ mit $x \cdot y \equiv 1 \pmod p$.*
(2) *Für jedes $x \in \mathbb{Z}$ gilt: wenn $x^2 \equiv 1 \pmod p$, so gilt $x \equiv 1 \pmod p$ oder $x \equiv -1 \pmod p$.*
(3) $(p-1)! \equiv -1 \pmod p$ *und* $(\frac{p-1}{2}!)^2 \equiv (-1)^{\frac{p-3}{2}} \pmod p$.

PROOF. (1) Da $\mathrm{ggT}(x, p) = 1$, gibt es $u, v \in \mathbb{Z}$ mit $ux + vp = 1$. Somit gilt für $y := u \bmod p$, dass $y\,x \equiv 1 \pmod p$. (2) Die Zahl p ist als Primzahl in $\mathbb{Z}$ irreduzibel, und folglich ein primes Element von $\mathbb{Z}$. Wenn also $p \mid x^2 - 1 = (x+1)(x-1)$, so gilt $p \mid x+1$ oder $p \mid x-1$. (3) Für jedes $x \in \{2, \dots, p-2\}$ gibt es ein $y \in \{2, \dots, p-2\}$ mit $x\,y \equiv 1 \pmod p$. Dieses y erfüllt $y \neq x$. Somit gilt $\prod_{i=2}^{p-2} i \equiv 1 \pmod p$, also $(p-1)! \equiv -1 \pmod p$. Für $i \in \{1, \dots, \frac{p-1}{2}\}$ gilt $-i \equiv p - i \pmod p$, also gilt

$$-1 \equiv_p (p-1)! = \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{i=1}^{\frac{p-1}{2}} (p-i)$$
$$\equiv_p (\frac{p-1}{2}!) \cdot (-1)^{\frac{p-1}{2}} \cdot (\frac{p-1}{2}!) = (\frac{p-1}{2}!)^2 \cdot (-1)^{\frac{p-1}{2}}.$$

□

Wir beweisen nun den folgenden Satz:

SATZ 3.20. *Sei p eine Primzahl mit $p \equiv 1 \pmod 4$. Dann gibt es $a, b \in \mathbb{N}$, sodass $a^2 + b^2 = p$.*

PROOF. Sei $x := \frac{p-1}{2}!$. Wegen Lemma 3.19 gilt dann

$$x^2 \equiv -1 \pmod p. \tag{3.1}$$

Im Ring $\mathbb{Z}[i]$ gilt natürlich ebenfalls $p \mid (1 + x^2)$, also $p \mid (1 + x\,i) \cdot (1 - x\,i)$. Da jedes Vielfache von p im Ring $\mathbb{Z}[i]$ einen durch p teilbaren Realteil hat, gilt in $\mathbb{Z}[i]$ weder $p \mid (1 + x\,i)$ noch

$p \mid (1 - x\,i)$. Im Ring $\mathbb{Z}[i]$ ist p also nicht prim. Wegen Satz 3.12 und Satz 3.14 ist $\mathbb{Z}[i]$ ein Hauptidealbereich. Somit ist wegen Satz 14.29 jedes irreduzible Element von $\mathbb{Z}[i]$ prim. Also ist p in $\mathbb{Z}[i]$ nicht irreduzibel. Es gibt folglich $a, b, c, d \in \mathbb{Z}$, sodass $p = (a + b\,i)(c + d\,i)$, und $a + b\,i$ und $c + d\,i$ nicht invertierbar sind. Sei $N(u + v\,i) := u^2 + v^2$ für alle $u, v \in \mathbb{Z}$. Dann gilt

$$p^2 = N(p) = N((a + b\,i)(c + d\,i)) = N(a + b\,i) \cdot N(c + d\,i) = (a^2 + b^2)(c^2 + d^2).$$

Alle Elemente $z \in \mathbb{Z}[i]$ mit $N(z) = 1$ sind invertierbar. Somit muss $a^2 + b^2 = p$ gelten. Die Zahlen $a' := |a|$ und $b' := |b|$ leisten also das Gewünschte. □

KAPITEL 4

Faktorielle Integritätsbereiche

1. Definition und Zerlegung in irreduzible Elemente

DEFINITION 4.1. Sei R ein Integritätsbereich. R ist *faktoriell*, wenn folgendes gilt:

(1) Für alle $r \in R \setminus \{0\}$, die nicht invertierbar sind, gibt es ein $s \in \mathbb{N}$ und irreduzible $f_1, \dots, f_s \in R$, sodass
$$r = f_1 \cdots f_s.$$
(2) Für alle $m, n \in \mathbb{N}$ und für alle irreduziblen $f_1, \dots, f_m, g_1, \dots, g_n \in R$ mit
$$f_1 \cdots f_m = g_1 \cdots g_n$$
gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \dots, m\} \to \{1, \dots, n\}$, sodass für alle $i \in \{1, \dots, m\}$ gilt: $f_i \sim_R g_{\pi(i)}$.

DEFINITION 4.2. Sei R ein Integritätsbereich, und sei $I \subseteq R$. I ist eine *vollständige Auswahl irreduzibler Elemente*, wenn alle $i \in I$ irreduzibel sind und es für jedes irreduzible $f \in R$ genau ein $i \in I$ mit $f \sim_R i$ gibt.

DEFINITION 4.3 (Zerlegung). Sei R ein Integritätsbereich, und sei $I \subseteq R$ eine vollständige Auswahl irreduzibler Elemente von R. Sei $a \in R \setminus \{0\}$. Eine Funktion $\alpha : I \to \mathbb{N}_0$ ist eine *Zerlegung* von a, wenn

(1) $\{i \in I \mid \alpha(i) \neq 0\}$ ist endlich.
(2) $a \sim_R \prod_{i \in I} i^{\alpha(i)}$.

Dabei definieren wir für alle $i \in I$, dass $i^0 := 1$ ist. Ebenso ist ein Produkt $\prod_{i \in \varnothing} r_i$ immer gleich 1. Wir schreiben $\prod_{i \in I} r_i$ nur, wenn $\{i \in I \mid i \neq 1\}$ endlich ist, und meinen damit $\prod_{i \in I, r_i \neq 1} r_i$.

LEMMA 4.4. *Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Seien $a, b \in R \setminus \{0\}$, sei α eine Zerlegung von a bezüglich I und β eine Zerlegung von b bezüglich I. Dann sind äquivalent:*

(1) $a \mid b$.
(2) *Für alle $i \in I$ gilt $\alpha(i) \leq \beta(i)$.*

PROOF. Wir beweisen nur (1)⇒(2). Sei $r \in R$ so, dass $ar = b$. Wir nehmen an, dass es ein $i_0 \in I$ gibt, sodass $\alpha(i_0) > \beta(i_0)$. Dann gilt
$$r \cdot i_0^{\alpha(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} \sim_R i_0^{\beta(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}.$$

Es gibt also ein invertierbares $u_1 \in R$, sodass

$$u_1 \cdot r \cdot i_0^{\alpha(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = i_0^{\beta(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}.$$

Da R ein Integritätsbereich ist und $i_0^{\beta(i_0)} \neq 0$, gilt

$$u_1 \cdot r \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}.$$

Der Ring R ist faktoriell. Also gibt es ein invertierbares Element $u_2 \in R$ und ein $s \in \mathbb{N}_0$ und irreduzible Elemente $r_1, \dots, r_s \in R$ sodass $r = u_2 r_1 \cdots r_s$. Es gilt dann

$$u_1 u_2 r_1 \cdots r_s \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}. \tag{4.1}$$

Falls $\{i \in I \mid \beta(i) > 0 \text{ und } i \neq i_0\} = \varnothing$, so ist i_0 invertierbar, im Widerspruch dazu, dass i_0 irreduzibel ist. Wenn die rechte Seite von (4.1) aus einer positiven Anzahl von Faktoren besteht, können wir verwenden, dass R faktoriell ist. Wir erhalten dann ein $i_1 \in I$ mit $i_1 \neq i_0$ und $i_1 \sim_R i_0$. Das ist unmöglich, da I keine verschiedenen assoziierten Elemente enthält. □

KOROLLAR 4.5 (Eindeutigkeit der Zerlegung). *Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Sei $f \in R \setminus \{0\}$. Dann gibt es genau eine Zerlegung $\alpha : I \to \mathbb{N}_0$ von f.*

PROOF. Wir zeigen zunächst, dass es ein α mit den geforderten Eigenschaften gibt. Wenn f invertierbar ist, so definieren wir α durch $\alpha(i) = 0$ für alle $i \in I$. Es gilt $f \sim_R 1$, also ist (2) aus Definition 4.3 erfüllt. Wenn f nicht invertierbar ist, so gibt es $s \in \mathbb{N}$ und irreduzible Elemente $g_1, \dots, g_s \in R$, sodass

$$f = g_1 \cdots g_s.$$

Seien nun $i_1, \dots, i_s \in I$ und $u_1, \dots, u_s$ invertierbare Elemente von R, sodass für alle $j \in \{1, \dots, s\}$ gilt: $g_j = u_j i_j$. Es gilt dann $f = (u_1 \cdots u_s) \cdot (i_1 \cdots i_s)$. Für $i \in I$ definieren wir $\alpha(i)$ als die Anzahl der Elemente von $\{j \in \{1, \dots, s\} \mid i_j = i\}$. Um die Eindeutigkeit zu zeigen, fixieren wir $\alpha, \beta : I \to \mathbb{N}_0$, sodass beide Funktionen nur an endlich vielen Stellen nicht 0 sind, und

$$\prod_{i \in I} i^{\alpha(i)} \sim_R \prod_{i \in I} i^{\beta(i)}.$$

Wegen Lemma 4.4 gilt dann $\alpha = \beta$. □

SATZ 4.6. *Sei R ein faktorieller Integritätsbereich, und sei $A \subseteq R$. Dann besitzt A einen größten gemeinsamen Teiler.*

PROOF. Sei I eine Auswahl irreduzibler Elemente, und sei für jedes Element $a \in I$ die Abbildung $\alpha_a : I \to \mathbb{N}_0$ eine Zerlegung von a. Wenn $A = \varnothing$, ist 0 ein größter gemeinsamer Teiler. Im Fall $A \neq \varnothing$ ist wegen Lemma 4.4 das Element $d := \prod_{i \in I} i^{\min\{\alpha_a(i) \mid a \in A\}}$ ein größter gemeinsamer Teiler. □

In einem faktoriellen Integritätsbereich besitzt auch jede Menge A ein kleinstes gemeinsames Vielfaches, also ein v, das Vielfaches aller $a \in A$ ist und das jedes weitere gemeinsame Vielfache von A teilt. Wenn für unendlich viele $i \in I$ gilt, dass $\max\{\alpha_a(i) \mid a \in A\} > 0$, so ist $v = 0$, ansonsten kann v mit $v = \prod_{i \in I} i^{\max\{\alpha_a(i) \mid a \in A\}}$ berechnet werden.

Übungsaufgaben 4.7

(1) Sei R ein faktorieller Integritätsbereich, seien $a, b \in R$, sei d ein größter gemeinsamer Teiler von $\{a, b\}$, und sei v ein kleinstes gemeinsames Vielfaches von $\{a, b\}$. Zeigen Sie, dass $dv \sim_R ab$.

2. Beschreibung faktorieller Integritätsbereiche

Faktorielle Integritätsbereiche lassen sich in folgender Weise charakterisieren:

Satz 4.8. *Sei R ein Integritätsbereich. Dann sind äquivalent:*

(1) *R erfüllt die* (ACC) *für Hauptideale, und jedes irreduzible Element von R ist prim.*
(2) *R ist faktoriell.*

Proof. (1)⇒(2). Wir zeigen zunächst, dass sich jedes nicht invertierbare Element $r \neq 0$ in ein Produkt von irreduziblen Elementen zerlegen lässt. Dazu nehmen wir an, dass es ein nicht invertierbares Element $r \neq 0$ gibt, das sich nicht zerlegen lässt. Wir wählen $r \in R \setminus \{0\}$ so, dass (r) maximal in der Menge

$$\{(r') \mid r' \text{ ist nicht invertierbar und nicht Produkt von irreduziblen Elementen}\}$$

ist. Da r nicht invertierbar ist, gilt $(r) \neq R$. Nun wählen wir $s \in R$ so, dass (s) maximal in der Menge

$$\{(s') \mid (r) \subseteq (s') \neq R\}$$

ist. Wir zeigen als erstes, dass s irreduzibel ist. Wenn $s = s_1 s_2$, so gilt $(s) \subseteq (s_1)$ und $(s) \subseteq (s_2)$. Wenn s_1 nicht invertierbar ist, so gilt wegen der Maximalität von (s) die Gleichheit $(s) = (s_1)$. Folglich gibt es $t \in R$, sodass $s_1 = ts$, also $s_1 = ts_1 s_2$. Da $s_1 \neq 0$, ist s_2 invertierbar. Somit ist s irreduzibel. Da $r \in (s)$, gibt es $t_1 \in R$, sodass $r = t_1 s$. Wenn t_1 invertierbar ist, so ist r irreduzibel, im Widerspruch zur Wahl von r. Wenn t_1 nicht invertierbar ist, so gilt $(r) \subseteq (t_1) \neq R$. Wenn nun $(r) = (t_1)$, so gibt es ein $s_1 \in R$ mit $t_1 = s_1 r = s_1 t_1 s$. Da $t_1 \neq 0$, ist dann $s_1 s = 1$ und s somit invertierbar. Also gilt $(r) \neq (t_1)$. Wegen der Maximalität von (r) lässt sich t_1 als Produkt von irreduziblen Elemente schreiben. Fügen wir zu diesem Produkt noch s dazu, haben wir auch r als Produkt irreduzibler Elemente geschrieben, im Widerspruch zur Wahl von r. Somit lässt sich jedes nicht invertierbare Element $\neq 0$ in irreduzible Elemente zerlegen.

Nun zeigen wir die Eindeutigkeit. Seien $m, n \in \mathbb{N}$, und $f_1, \ldots, f_m, g_1, \ldots, g_n$ irreduzible Elemente, sodass $f_1 \cdots f_m = g_1 \cdots g_n$. Wir zeigen durch Induktion nach $\min(m, n)$, dass sich die f_i und g_j zueinander assoziieren lassen. Wenn $m = 1$, so gilt, da f_1 irreduzibel ist, auch $n = 1$, und somit $f_1 = g_1$. Wenn $n = 1$, so gilt analog $m = 1$ und $f_1 = g_1$. Wenn $m \geq 2$ und $n \geq 2$, dann gilt $f_1 \mid g_1 \cdots g_n$. Da f_1 nach Voraussetzung prim ist, teilt es eines der g_i. Da g_i irreduzibel

ist, gilt $f_1 \sim_R g_i$. Es gibt also ein invertierbares $u \in R$, sodass $g_i = u \cdot f_1$. Wir wenden nun die Induktionsvoraussetzung auf $(uf_2) \cdot f_3 \cdots f_m = g_1 \cdots g_{i-1} g_{i+1} \cdots g_n$ an.

(2)⇒(1): Sei R ein faktorieller Integritätsbereich, und sei $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots$ eine Kette von Hauptidealen. Wir nehmen an $(a_1) \neq (0)$. Dann gilt $a_n \mid a_{n-1} \mid \cdots \mid a_3 \mid a_2 \mid a_1$. Sei I eine vollständige Auswahl von irreduziblen Elementen, und sei α_k eine Zerlegung von a_k bezüglich I. Es gilt dann nach Lemma 4.4 für alle $i \in I$: $\alpha_k(i) \leq \alpha_1(i)$. Da es nur endlich viele $\beta : I \to \mathbb{N}_0$ mit der Eigenschaft $\beta(i) \leq \alpha_1(i)$ für alle $i \in I$ gibt, und da die Folgen $(\alpha_k(i))_{k\in\mathbb{N}}$ wegen Lemma 4.4 für alle $i \in I$ schwach monoton fallend sind, gibt es ein $N \in \mathbb{N}$, sodass für $k \geq N$ gilt: $\alpha_k = \alpha_N$. Dann gilt aber auch $(a_k) = (a_N)$.

Wir zeigen nun, dass jedes irreduzible Element von R prim ist. Sei dazu f irreduzibel, und seien $a, b \in R$ so, dass $f \mid ab$. Zu zeigen ist, dass f mindestens eines der Elemente a oder b teilt. Wegen $f \mid ab$ gibt es $r \in R$, sodass

$$fr = ab.$$

Wenn $a = 0$, so gilt $f \mid a$; wenn $b = 0$, so gilt $f \mid b$. Wir nehmen nun an, dass $a \neq 0$ und $b \neq 0$. Wenn a invertierbar ist, dann gilt $fra^{-1} = b$, und somit $f \mid b$; wenn b invertierbar ist, gilt $f \mid a$. Es bleibt der Fall, dass a, b beide $\neq 0$ und beide nicht invertierbar sind. Dann gibt es $m, n \in \mathbb{N}$ und irreduzible Elemente $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$, sodass

$$a = a_1 \cdots a_m \text{ und } b = b_1 \cdots b_n.$$

Falls r invertierbar ist, dann ist fr irreduzibel, und wegen der Eindeutigkeit der Zerlegung zu einem a_i oder b_j assoziiert. Wenn fr zu einem a_i assoziiert ist, dann gilt $fr \mid a$, und somit $f \mid a$; wenn fr zu einem b_j assoziiert ist, dann gilt $f \mid b$.

Wenn r nicht invertierbar ist, dann gibt es $l \in \mathbb{N}$ und irreduzible Elemente $r_1, \ldots, r_l \in R$, sodass

$$fr_1 \cdots r_l = a_1 \cdots a_m \cdot b_1 \cdots b_n.$$

Wegen der Eindeutigkeit der Zerlegung ist f zu einem a_i oder b_j assoziiert. Es gilt also wieder $f \mid a$ oder $f \mid b$. □

Definition 4.9. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

Satz 4.10. *Jeder Hauptidealbereich ist faktoriell.*

Proof. Sei R ein Hauptidealbereich. Da jedes Ideal von R endlich erzeugt ist, erfüllt R die (ACC) für Ideale, also insbesondere für Hauptideale. Wegen Satz 14.29 ist jedes irreduzible Element von R prim. □

3. Teilbarkeit in Polynomringen

In diesem Kapitel zeigen wir, dass für einen faktoriellen Integritätsbereich R der Polynomring $R[X]$ ebenfalls ein faktorieller Integritätsbereich ist.

DEFINITION 4.11. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}_0$, und sei $f = \sum_{i=0}^{n} f_i X^i \in R[X]$. Das Polynom f ist *primitiv*, wenn es kein primes $p \in R$ gibt, das alle Koeffizienten f_i $(i = 0, \dots, n)$ teilt.

LEMMA 4.12 (Gaußsches Lemma). *Sei R ein kommutativer Ring mit Eins, und seien $f, g \in R[X]$ primitiv. Dann ist $f \cdot g$ ebenfalls primitiv.*

PROOF. Wir nehmen an, dass $f \cdot g$ nicht primitiv ist. Dann gibt es ein primes $p \in R$, das alle Koeffizienten von $f \cdot g$ teilt. Wir bezeichen mit $[f]_{(p)}$ das Polynom $\sum_{i=0}^{\deg f} (f_i + (p))X^i$ im Ring $R/(p)\,[X]$. Es gilt also dann $[f \cdot g]_{(p)} = 0$. Da (p) prim ist, ist $R/(p)$ ein Integritätsbereich. Daher ist auch $R/(p)[X]$ ein Integritätsbereich (der führende Koeffizient des Produkts zweier Polynome ist das Produkt der führenden Koeffizienten dieser zwei Polynome). Da $[f \cdot g]_{(p)} = [f]_{(p)} \cdot [g]_{(p)}$, muss also $[f]_{(p)}$ oder $[g]_{(p)}$ gleich 0 sein. Wenn $[f]_{(p)}$ gleich 0 ist, dann teilt p alle Koeffizienten von f, und f ist somit nicht primitiv; $[g]_{(p)} = 0$ bedeutet, dass g nicht primitiv ist. □

Für einen faktoriellen Integritätsbereich fixieren wir eine Funktion $\gcd : \mathcal{P}(R) \to R$ mit der Eigenschaft, dass für jedes $A \subseteq R$ das Element $\gcd(A)$ ein größter gemeinsamer Teiler von A ist. Für ein Polynom $f = \sum_{i=0}^{n} f_i X^i \in R[X]$ ist $\mathrm{c}(f) := \gcd(\{f_0, f_1, \dots, f_n\})$ der *Inhalt* von f. Wenn $f \neq 0$, so gibt es dann genau ein Polynom $\tilde{f}$ mit $f = \mathrm{c}(f) \cdot \tilde{f}$. Dieses Polynom $\tilde{f}$ heißt der *primitive Anteil von f*. Wir definieren $\tilde{0} := 1$.

LEMMA 4.13. *Sei R ein faktorieller Integritätsbereich, seien $f, g \in R[X]$ und sei $r \in R$. Dann gilt:*

(1) $\mathrm{c}(rf) \sim_R r\,\mathrm{c}(f)$.
(2) *$\tilde{f}$ ist ein primitives Polynom.*
(3) $\mathrm{c}(fg) \sim_R \mathrm{c}(f)\,\mathrm{c}(g)$.
(4) *Wenn $f \neq 0$ und $g \neq 0$, so gibt ein invertierbares $u \in R$ mit $u\,\widetilde{(fg)} = \tilde{f}\tilde{g}$.*

PROOF. (1) Wegen Lemma 3.6 gilt $\mathrm{c}(rf) = \gcd(\{rf_0, \dots, rf_n\}) \sim_R r \gcd(\{f_0, \dots, f_n\}) = r\,\mathrm{c}(f)$.

(2) Es gilt $\mathrm{c}(f) = \mathrm{c}(\mathrm{c}(f)\tilde{f}) \sim_R \mathrm{c}(f)\,\mathrm{c}(\tilde{f})$. Sei u ein invertierbares Element von R mit $\mathrm{c}(f)u = \mathrm{c}(f)\,\mathrm{c}(\tilde{f})$. Dann gilt $\mathrm{c}(f)(u - \mathrm{c}(\tilde{f})) = 0$. Wenn $\mathrm{c}(f) = 0$, dann gilt $f = 0$ und somit $\tilde{f} = 1$, somit ist $\tilde{f}$ primitiv. Wenn $\mathrm{c}(\tilde{f}) = u$, so teilt jedes prime $p \in R$, das alle Koeffizienten von $\tilde{f}$ teilt, auch u und ist somit invertierbar und damit nicht prim. Also ist $\tilde{f}$ primitiv.

(3) Es gilt $\mathrm{c}(fg) = \mathrm{c}(\mathrm{c}(f)\tilde{f}\,\mathrm{c}(g)\tilde{g}) = \mathrm{c}(\mathrm{c}(f)\,\mathrm{c}(g)\tilde{f}\tilde{g}) \sim_R \mathrm{c}(f)\,\mathrm{c}(g)\,\mathrm{c}(\tilde{f}\tilde{g})$. Wegen Lemma 4.12 ist $\tilde{f}\tilde{g}$ primitiv, also ist $\mathrm{c}(\tilde{f}\tilde{g})$ ein invertierbares Element von R, und somit gilt $\mathrm{c}(f)\,\mathrm{c}(g)\,\mathrm{c}(\tilde{f}\tilde{g}) \sim_R \mathrm{c}(f)\,\mathrm{c}(g)$.

(4) Es gilt $fg = \mathrm{c}(fg)\widetilde{(fg)}$ und $fg = \mathrm{c}(f)\,\mathrm{c}(g)\tilde{f}\tilde{g}$. Wegen (3) gibt es ein invertierbares $u \in R$ mit $\mathrm{c}(fg) = u\,\mathrm{c}(f)\,\mathrm{c}(g)$, also gilt $u\,\mathrm{c}(f)\,\mathrm{c}(g)\widetilde{(fg)} = \mathrm{c}(f)\,\mathrm{c}(g)\tilde{f}\tilde{g}$ und wegen $f, g \neq 0$ somit auch $u\,\widetilde{(fg)} = \tilde{f}\tilde{g}$. □

SATZ 4.14. *Sei R ein faktorieller Integritätsbereich, seien $f, g \in R[X]$, und sei $Q(R)$ der Quotientenkörper von R. Dann sind äquivalent:*

(1) $f \mid g$ *in* $R[X]$.
(2) $f \mid g$ *in* $Q(R)[X]$ *und* $\mathrm{c}(f) \mid \mathrm{c}(g)$.

PROOF. (1)⇒(2): Sei $q \in R[X]$ so, dass $g = qf$. Dann gilt $\mathrm{c}(g) = \mathrm{c}(qf) \sim_R \mathrm{c}(q)\,\mathrm{c}(f)$, also gilt $\mathrm{c}(f) \mid \mathrm{c}(g)$.

(2)⇒(1): In $Q(R)[X]$ gilt $\tilde{f} \mid f \mid g$. Sei $h \in Q(R)[X]$ so, dass $g = h\tilde{f}$, und sei $r \in R \setminus \{0\}$ so, dass $rh \in R[X]$. Dann gilt $rg = (rh)\tilde{f}$. Es gilt dann

$$\begin{aligned}\mathrm{c}(rh) &\sim_R \mathrm{c}(rh)\,\mathrm{c}(\tilde{f})\\ &\sim_R \mathrm{c}(rh\tilde{f})\\ &= \mathrm{c}(rg)\\ &\sim_R r\,\mathrm{c}(g),\end{aligned}$$

Also gilt $r \mid \mathrm{c}(rh)$. Also sind alle Koeffizienten von rh durch r teilbar, und somit gilt $h \in R[X]$. □

KOROLLAR 4.15. *Sei R ein ein faktorieller Integritätsbereich, und seien $f, g \in R[X]$. Wir nehmen an, dass f primitiv ist und dass $f \mid g$ in $Q(R)[X]$ gilt. Dann gilt $f \mid g$ auch in $R[X]$.*

PROOF. Da $\mathrm{c}(f)$ invertierbar ist, ist Bedingung (2) von Satz 4.14 erfüllt. □

LEMMA 4.16. *Sei R ein faktorieller Integritätsbereich, sei $Q(R)$ sein Quotientenkörper, und sei $f \in R[X]$. Dann sind äquivalent:*

(1) *f ist ein irreduzibles Element von $R[X]$.*
(2) *Es gibt ein irreduzibles Element $r \in R$ mit $f = rX^0$, oder f ist primitiv und f ist ein irreduzibles Element von $Q(R)[X]$.*

PROOF. (1)⇒(2): Sei f ein irreduzibles Element von $R[X]$. Es gilt

$$f = \mathrm{c}(f)\tilde{f},$$

daher ist einer der Faktoren $\mathrm{c}(f)$ und $\tilde{f}$ invertierbar in $R[X]$.

Im Fall, dass $\mathrm{c}(f)$ invertierbar ist, zeigen wir, dass f in $Q(R)[X]$ irreduzibel ist.

Wenn f in $Q(R)[X]$ invertierbar ist, so so gilt $\deg(f) = 0$ und daher gilt $f \sim_R \mathrm{c}(f)X^0$, und f ist damit auch in $R[X]$ invertierbar, im Widerspruch dazu, dass f irreduzibel in $R[X]$ ist.

Sei nun g ein Teiler von f in $Q(R)[X]$. Es gibt dann $a \in Q(R) \setminus \{0\}$, sodass ag primitiv ist. Dann gilt in $Q(R)[X]$, dass $ag \mid f$ und wegen der Primitivität von ag daher auch $ag \mid f$ in $R[X]$. Wenn ag invertierbar in $R[X]$ ist, so gilt $\deg(ag) = 0$ und damit $\deg(g) = 0$. Wenn ag zu f in $R[X]$ assoziiert ist, so gilt $f \mid ag$ in $R[X]$, also auch $f \mid g$ in $Q(R)[X]$, und somit sind f und g assoziiert in $Q(R)[X]$. Somit ist f irreduzibel in $Q(R)[X]$.

Im Fall, dass $\tilde{f}$ invertierbar in $R[X]$ ist, gilt wegen $f = \mathrm{c}\, f\tilde{f}$, dass f und $\mathrm{c}(f)$ in $R[X]$ assoziiert sind. in $R[X]$. Somit ist auch $\mathrm{c}(f)$ ein irreduzibles Element in $R[X]$, und damit auch irreduzibel in R.

(2)⇒(1): Wenn r ein irreduzibles Element von R ist, so ist rX^0 irreduzibel in $R[X]$. Wir nehmen nun an, dass f in $Q(R)[X]$ irreduzibel ist und $\mathrm{c}(f)$ in R invertierbar ist. Da f in $Q(R)[X]$ nicht invertierbar ist, ist f auch in $R[X]$ nicht invertierbar. Um zu zeigen, dass f irreduzibel in $R[X]$ ist, wählen wir einen Teiler g von f in $R[X]$. Es gilt dann $\mathrm{c}(g) \mid \mathrm{c}(f)$ in R, also ist $\mathrm{c}(g)$ invertierbar, und g somit primitiv. Wenn $\deg(g) = 0$, so ist g daher gleich uX^0 für ein invertierbares $u \in R$, und somit ist g invertierbar in $R[X]$. Wenn $\deg(g) = \deg(f)$, so gilt $f \mid g$ in $Q(R)[X]$ und somit wegen Satz 4.14 und $\mathrm{c}(f) \mid \mathrm{c}(g)$ in R, auch $f \mid g$ in $R[X]$. Somit sind f und g assoziiert in $R[X]$. Also ist f irreduzibel in $R[X]$. □

Satz 4.17. *Sei R ein faktorieller Integritätsbereich. Dann ist auch $R[X]$ faktoriell.*

Proof. Wir zeigen als erstes, dass $R[X]$ die (ACC) für Hauptideale erfüllt. Sei $a_1 \in R[X] \setminus \{0\}$, und sei $(a_1) \subseteq (a_2) \subseteq \cdots$ eine Folge von Hauptidealen. Für jedes $i \in \mathbb{N}$ wählen wir $r_i \in R$ und ein primitives $b_i \in R[X]$ so, dass $a_i = r_i\, b_i$. Wegen Satz 4.14 ist dann $(r_1)_R \subseteq (r_2)_R \subseteq \cdots$ eine aufsteigende Kette von Idealen in R und $(b_1)_{Q(R)[X]} \subseteq (b_2)_{Q(R)[X]} \subseteq \cdots$ eine aufsteigende Kette von Idealen in $Q(R)[X]$. R ist faktoriell, und erfüllt daher die (ACC) für Hauptideale. Der Ring $Q(R)[X]$ ist ein Polynomring über einem Körper. Als solcher ist er ein Hauptidealbereich (jedes Ideal I wird von jedem Polynom kleinsten Grades in $I \setminus \{0\}$ erzeugt), und somit faktoriell. Es gibt also ein $N \in \mathbb{N}$, sodass für alle $k \geq N$ gilt: $(r_N)_R = (r_k)_R$ und $(b_N)_{Q(R)[X]} = (b_k)_{Q(R)[X]}$. Es gilt also $b_N \mid b_k$ in $Q(R)[X]$ und $r_N \mid r_k$ in R. Somit gilt $a_N \mid a_k$ in $R[X]$, und somit $(a_k)_{R[X]} = (a_N)_{R[X]}$.

Nun zeigen wir, dass jedes irreduzible Element in $R[X]$ prim ist. Sei dazu $f \in R[X]$ irreduzibel, und seien $a, b \in R[X] \setminus \{0\}$ so, dass $f \mid a \cdot b$. Wir wollen nun zeigen, dass f in $R[X]$ entweder a oder b teilt. Wir unterscheiden zwei Fälle nach Lemma 4.16.

Wenn $f = rX^0$ mit einem irreduziblen $r \in R$ ist, so gilt $r = \mathrm{c}(f) \mid \mathrm{c}(a)\,\mathrm{c}(b)$. Da R faktoriell ist, ist r prim in R, und somit gilt $r \mid \mathrm{c}(a)$ oder $r \mid \mathrm{c}(b)$, und folglich $rX^0 \mid a$ oder $rX^0 \mid b$.

Im anderen Fall ist f wegen Lemma 4.16 primitiv und irreduzibel in $Q(R)[X]$. Der Ring $Q(R)[X]$ ist ein Polynomring über einem Körper, folglich euklidisch, daher ein Hauptidealbereich und somit faktoriell. Also ist f prim in $Q(R)[X]$ und es gilt daher $f \mid a$ oder $f \mid b$ in $Q(R)[X]$. Wegen Korollar 4.15 gilt dann $f \mid a$ oder $f \mid b$ in $R[X]$.

Also ist f prim in in $R[X]$. □

Korollar 4.18. *Sei R ein faktorieller Integritätsbereich und $k \in \mathbb{N}$. Dann ist $R[X_1, \ldots, X_k]$ faktoriell.*

4. Größte gemeinsame Teiler im Polynomring

Satz 4.19. *Sei R ein faktorieller Integritätsbereich, und seien $f_1, \ldots, f_n \in R[X] \setminus \{0\}$. Es sei d_1 ein größter gemeinsamer Teiler von $\mathrm{c}(f_1), \ldots, \mathrm{c}(f_n)$ in R, und d_2 ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$ in $Q(R)[X]$. Wir nehmen an, dass d_2 primitiv in $R[X]$ ist. Dann ist $d_1 d_2$ ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$ in $R[X]$.*

PROOF. Wir zeigen zunächst, dass $d_1 d_2$ alle f_i teilt. Sei $i \in \{1, \ldots, n\}$. Da $d_1 \mid \mathrm{c}(f_i)$ in R und $d_2 \mid f_i$ in $Q(R)[X]$, liefert Satz 4.14 auch $d_1 d_2 \mid f_i$ in $R[X]$.

Sei nun $d' \in R[X]$ so, dass d' in $R[X]$ alle f_i teilt. Dann gilt wegen Satz 4.14, dass $\mathrm{c}(d')$ alle $\mathrm{c}(f_i)$ in R teilt, und dass $\tilde{d'}$ alle f_i in $Q(R)[X]$ teilt. Da d_1 ein größter gemeinsamer Teiler in R ist, gilt $\mathrm{c}(d') \mid d_1$ in R. Da d_2 ein größter gemeinsamer Teiler in $Q(R)[X]$ ist, gilt $\tilde{d'} \mid d_2$ in $Q(R)[X]$. Außerdem gilt $d_1 \mid \mathrm{c}(d_1 d_2)$. Wegen Satz 4.14 gilt daher $d' \mid d_1 d_2$ in $R[X]$. □

ÜBUNGSAUFGABEN 4.20

(1) (Größter gemeinsamer Teiler) Seien $f, g \in \mathbb{Q}[X, Y]$ gegeben durch

$$\begin{aligned} f &= XY^2 + X^2Y^3 \\ g &= Y + XY + XY^2 + X^2Y^2. \end{aligned}$$

   (a) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X)[Y]$.
   (b) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(Y)[X]$.
   (c) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}[X, Y]$.
   (d) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X, Y)$.

   Dabei ist $\mathbb{Q}(X)$ der Quotientenkörper von $\mathbb{Q}[X]$.

(2) (Größter gemeinsamer Teiler) Seien $f, g \in \mathbb{Q}[X, Y]$ gegeben durch

$$\begin{aligned} f &= XY + X^3Y + X^2Y^2 + XY^3 \\ g &= X + X^3 + Y + 2X^2Y + 2XY^2 + Y^3 \end{aligned}$$

   (a) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X)[Y]$.
   (b) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(Y)[X]$.
   (c) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}[X, Y]$.
   (d) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X, Y)$.

(3) (Größter gemeinsamer Teiler) Berechnen Sie größte gemeinsame Teiler von $f = 3220 + 5520X + 2300X^2 + 460X^3 + 460X^4$ und $g = -230 - 230X + 46X^3 + 46X^4$ in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

KAPITEL 5

Restklassenringe

1. Restklassenringe von $\mathbb{Z}$

DEFINITION 5.1 ($\mathbb{Z}_n$). Sei $\mathbb{Z}$ der Ring der ganzen Zahlen, sei $n \in \mathbb{N}$, und sei (n) das von n erzeugte Hauptideal von $\mathbb{Z}$. Dann bezeichnen wir den Ring $\mathbb{Z}/(n)$ als den *Ring der ganzen Zahlen modulo* n, und kürzen ihn mit $\mathbb{Z}_n$ ab.

Wir bezeichnen das Element $x + (n)$ auch mit $[x]_n$; $\mathbb{Z}_n$ hat genau die n Elemente $[0]_n, [1]_n, \ldots, [n-1]_n$. Wir schreiben $a \equiv_n b$ oder $a \equiv b \pmod{n}$, wenn $n \mid a - b$.

THEOREM 5.2 (Invertierbarkeit). *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $[a]_n$ genau dann invertierbar in $\mathbb{Z}_n$, wenn* $\gcd(a, n) = 1$.

PROOF. Wenn $\gcd(a, n) = 1$, so gibt es nach dem Euklidischen Algorithmus u und v in $\mathbb{Z}$, sodass $ua + vn = 1$. Dann gilt $[u]_n[a]_n = [1]_n$. Wenn $[a]_n$ invertierbar ist, dann gibt es ein $x \in \mathbb{Z}$ mit $[x]_n[a]_n = [1]_n$, also $n \mid xa - 1$. Dann gilt auch $\gcd(a, n) \mid xa - 1$ und wegen $\gcd(a, n) \mid xa$ auch $\gcd(a, n) \mid 1$, also $\gcd(a, n) = 1$. □

Da in jedem kommutativen Ring mit Eins das Produkt invertierbarer Elemente wieder invertierbar ist, erhalten wir:

LEMMA 5.3. *Seien a, b invertierbare Elemente aus $\mathbb{Z}_n$. Dann ist auch $a \cdot b$ invertierbar.*

DEFINITION 5.4 (Euler'sche φ−Funktion). Sei $n \in \mathbb{N}$. Wir definieren $\varphi(1) := 1$ und, wenn $n > 1$,

$$\varphi(n) := |\{a \in \mathbb{Z}_n \,:\, a \text{ invertierbar}\}| = |\{x \in \{1, 2, \ldots, n-1\} \,:\, \gcd(x, n) = 1\}|.$$

Beispiele: $\varphi(12) = |\{1, 5, 7, 11\}| = 4$ und $\varphi(8) = |\{1, 3, 5, 7\}| = 4$.

THEOREM 5.5 (Satz von Euler). *Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$,* $\gcd(a, n) = 1$. *Dann gilt:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

So gilt etwa $7^{\varphi(12)} = 7^4 \equiv_{12} 1$ und $3^{\varphi(5)} = 3^4 \equiv_5 1$.

PROOF. Beweis von Satz 5.5: Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Wir nehmen an, dass $\gcd(a, n) = 1$. Sei

$$I := \{x \in \mathbb{Z}_n \mid x \text{ ist invertierbar}\}.$$

Wir wissen bereits, dass $|I| = \varphi(n)$. Wir definieren

$$\begin{array}{rccc} f & : & I & \longrightarrow & I \\ & & x & \longmapsto & x \cdot [a]_n \end{array}$$

und zeigen, dass f injektiv ist. Dazu fixieren wir $x, y \in I$ mit $f(x) = f(y)$. Das heißt: $x \cdot [a]_n = y \cdot [a]_n$. Da $\gcd(a, n) = 1$, gibt es $b \in \mathbb{Z}$ mit $[a]_n \cdot [b]_n = [1]_n$. Wir erhalten also $x \cdot [a]_n \cdot [b]_n = y \cdot [a]_n \cdot [b]_n$ und damit $x = y$. Daher ist f injektiv. Die Funktion f ist folglich eine bijektive Abbildung von I nach I. Es gilt also:

$$\prod_{x \in I} x = \prod_{x \in I} f(x) = \prod_{x \in I} (x \cdot [a]_n) = \left(\prod_{x \in I} x \right) \cdot ([a]_n)^{\varphi(n)}.$$

Sei $y \in \mathbb{Z}_n$ das Inverse zu $\prod_{x \in I} x$. Dann gilt:

$$y \cdot \prod_{x \in I} x = y \cdot \left(\prod_{x \in I} x \right) \cdot ([a]_n)^{\varphi(n)},$$

und somit $[1]_n = ([a]_n)^{\varphi(n)}$ und folglich $1 \equiv a^{\varphi(n)} \pmod{n}$. □

KOROLLAR 5.6. *Sei p eine Primzahl, und sei $z \in \mathbb{Z}$. Dann gilt*

$$z^p \equiv z \pmod{p}.$$

Falls p kein Teiler von z ist, gilt

$$z^{p-1} \equiv 1 \pmod{p}.$$

PROOF. Wir wählen eine Primzahl p und $z \in \mathbb{Z}$ und nehmen an, dass p die Zahl z nicht teilt. Wir wissen, dass $\varphi(p) = p - 1$, und daher gilt nach dem Satz von Euler

$$z^{p-1} \equiv 1 \pmod{p}.$$

Da $p \mid (z^{p-1} - 1)$, gilt auch $p \mid (z^p - z)$, und somit $z^p \equiv z \pmod{p}$.

Wenn $p \mid z$, dann teilt p sowohl z als auch z^p. □

ÜBUNGSAUFGABEN 5.7

(1) ([RU87]) Zeigen Sie, dass für jede natürliche Zahl n die Zahl $n^5 - n$ ein Vielfaches von 30 ist.
(2) Zeigen Sie, dass für alle $a, b \in \mathbb{Z}_p$ gilt:
$$(a + b)^p = a^p + b^p.$$
(3) Seien m, n natürliche Zahlen. Wann ist $2^m - 1$ ein Teiler von $2^n - 1$?

2. Das RSA-Verfahren

THEOREM 5.8. *Seien p, q Primzahlen, $p \neq q$ und seien $a \in \mathbb{Z}$, $s \in \mathbb{N}_0$. Dann gilt:*

$$a^{1+s(p-1)(q-1)} \equiv a \pmod{pq}.$$

Beweis:

- *1. Fall:* $\gcd(a, pq) = 1$*:* Wir wissen, dass $a^{p-1} \equiv 1 \pmod{p}$ gilt (Satz von Euler), daher gilt auch $(a^{p-1})^{(q-1)\cdot s} \equiv 1 \pmod{p}$. Somit ist p ein Teiler von $a^{(p-1)\cdot(q-1)\cdot s} - 1$ und damit auch von $a^{(p-1)\cdot(q-1)\cdot s+1} - a$. Ebenso zeigen wir
$$q \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

Damit gilt insgesamt:

$$pq \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

- *2. Fall:* $\gcd(a, pq) = p$: Da der $\gcd(a, q) = 1$ ist, gilt mit dem Satz von Euler $a^{q-1} \equiv 1 \pmod{q}$, und somit $a^{(q-1)\cdot(p-1)} \equiv 1 \pmod{q}$. Das heißt

$$q \mid a^{(q-1)\cdot(p-1)\cdot s} - 1.$$

  Wir wissen, dass $p \mid a$. Daher gilt $pq \mid \left(a^{(q-1)\cdot(p-1)\cdot s} - 1\right) \cdot a$.
- *3. Fall:* $\gcd(a, pq) = q$: Beweis genauso wie im 2. Fall.
- *4. Fall:* $\gcd(a, pq) = pq$: Dann ist zu zeigen, dass $0 \equiv 0 \pmod{pq}$. □

Beim RSA-Verschlüsselungsverfahren wählt der Systementwerfer zwei Primzahlen p, q, sodass $n = p\,q$ nicht in verfügbarer Zeit faktoriserbar ist, berechnet $\phi := (p-1)(q-1)$, wählt für e eine beliebige Zahl mit $1 < e < \phi$ und $\gcd(e, \phi) = 1$, und berechnet d so, dass $d\,e \equiv 1 \pmod{\phi}$.

Der öffentliche Schlüssel ist (n, e), der private Schlüssel (n, d). Die Verschlüsselungsfunktion ist gegeben durch $E : \mathbb{Z}_n \to \mathbb{Z}_n$, $E(m) := m^e$, die Entschlüsselungsfunktion durch $D : \mathbb{Z}_n \to \mathbb{Z}_n$, $D(c) := c^d$.

Übungsaufgaben 5.9

(1) Sei $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, wobei die p_i lauter verschiedene Primzahlen sind, und sei $s \in \mathbb{N}$. Zeigen Sie, dass für alle $a \in \mathbb{Z}$ gilt:
$$a^{1+s\cdot\prod_{i=1}^{k}(p_i-1)} \equiv a \pmod{n}.$$
(2) Für das RSA-Verfahren wählen wir $p = 5, q = 11$ und $k = 13$. Chiffrieren Sie $(01, 22, 03, 08)$ und dechiffrieren Sie das Ergebnis!
(3) Frau Huber sendet Herrn Müller mit dem RSA-Verfahren die Nachricht PMOXY. Herr Müller weiß, dass Frau Huber das RSA-Verfahren mit $(n = 35, k = 5)$ verwendet hat (A=0, Z=25). Entschlüsseln Sie die Nachricht! (*Bemerkung:* Warum ist es überhaupt ungünstig, einzelne Buchstaben zu verschlüsseln?)
(4) (Mathematica) Entschlüsseln Sie (verbotenerweise) die Nachricht $(2, 3, 5, 7, 11, 13)$, die mit $k = 13$ und $pq = 1334323339$ verschlüsselt wurde.
(5) (Mathematica) [**LP98**, p. 265] In einem RSA-System ist $n = pq = 32954765761773295963$ und $k = 1031$. Bestimmen Sie t, und entschlüsseln Sie die Nachricht

    899150261120482115

    (A = 0, Z = 25).
(6) Sei n eine ungerade Primzahl, und seien $r, s \in \mathbb{N}$ so, dass $n - 1 = 2^s \cdot r$ und r ungerade ist. Sei a eine ganze Zahl, die kein Vielfaches von n ist. Zeigen Sie, dass dann $a^r \equiv 1 \pmod{n}$ gilt, oder dass es ein $j \in \{0, 1, \ldots, s-1\}$ mit $a^{2^j \cdot r} \equiv -1 \pmod{n}$ gibt. *Hinweis:* Dieser Satz ist die Basis für den *Rabin-Miller Test*, um nachzuprüfen, ob eine Zahl eine Primzahl ist.

3. Die Multiplikativität der Eulerschen φ-Funktion

Theorem 5.10 (Multiplikativität der φ-Funktion). *Seien* $n, m \in \mathbb{N}$. *Wenn* $\gcd(n, m) = 1$, *dann gilt* $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

Wir benutzen im Beweis das direkte Produkt von Ringen:

SATZ UND DEFINITION 5.11. *Seien R_1 und R_2 Ringe mit Eins. Wir definieren auf der Menge $R_1 \times R_2$ Operationen durch*

$$\$\binom{r_1}{r_2} +_{R_1\times R_2} \binom{s_1}{s_2} := \binom{r_1+_{R_1}s_1}{r_2+_{R_2}s_2}, \quad \binom{r_1}{r_2} \cdot_{R_1\times R_2} \binom{s_1}{s_2} := \binom{r_1\cdot_{R_1}s_1}{r_2\cdot_{R_2}s_2}, \quad -_{R_1\times R_2} \binom{r_1}{r_2} := \binom{-_{R_1}r_1}{-_{R_2}r_2}.$$

Dann ist $\langle R_1 \times R_2, +_{R_1\times R_2}, -_{R_1\times R_2}, \cdot_{R_1\times R_2}, \binom{0_{R_1}}{0_{R_2}}, \binom{1_{R_1}}{1_{R_2}}\rangle$ ein Ring mit Eins. Er ist das direkte Produkt von R_1 und R_2.

In $\mathbb{Z}_4 \times \mathbb{Z}_5$ rechnet man zum Beispiel $\binom{[3]_4}{[4]_5} \cdot \binom{[2]_4}{[3]_5} = \binom{[2]_4}{[2]_5}$.

THEOREM 5.12. *Seien $n, m \in \mathbb{N}$ mit $\gcd(n,m) = 1$. Dann ist die Abbildung*

$$\begin{array}{rccc} \psi & : & \mathbb{Z}_{nm} & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m \\ & & [x]_{nm} & \longmapsto & ([x]_n, [x]_m) \end{array}$$

ein Isomorphismus dieser Ringe mit Eins.

PROOF. Wir zeigen als erstes, dass ψ wohldefiniert ist. Dazu zeigen wir, dass für alle $y, z \in \mathbb{Z}$ mit $[y]_{nm} = [z]_{nm}$ auch die Gleichheiten $[y]_n = [z]_n$ und $[y]_m = [z]_m$ gelten. Seien dazu $y, z \in \mathbb{Z}$ mit $[y]_{nm} = [z]_{nm}$. Dann gilt $nm \mid y - z$, also $n \mid y - z$ und $m \mid y - z$ und somit $[y]_n = [z]_n$ und $[y]_m = [z]_m$.

Wir zeigen nun, dass ψ ein Homomorphismus ist und überprüfen dazu die Homomorphismuseigenschaft für $+$. Es gilt

$$\begin{aligned} \psi([x]_{nm} + [y]_{nm}) &= \psi([x+y]_{nm}) \\ &= ([x+y]_n, [x+y]_m) \\ &= ([x]_n + [y]_n, [x]_m + [y]_m) \\ &= \binom{[x]_n}{[x]_m} + \binom{[y]_n}{[y]_m} \\ &= \psi([x]_{nm}) + \psi([y]_{nm}). \end{aligned}$$

Die Homomorphismuseigenschaft für $\cdot$ zeigt man genau so.

Als nächstes zeigen wir, dass ψ bijektiv und damit ein Isomorphismus ist. Da beide Mengen endlich und gleich groß sind, reicht es, zu zeigen, dass ψ injektiv ist. Wir nehmen also $\psi([x]_{nm}) = \psi([y]_{nm})$ an. Dann gilt $([x]_n, [x]_m) = ([y]_n, [y]_m)$, und somit $n \mid x - y$ und $m \mid x - y$. Da $\gcd(n,m) = 1$, gilt dann $nm \mid x - y$, und folglich $[x]_{nm} = [y]_{nm}$. Die Abbildung ψ ist also injektiv, somit surjektiv und damit bijektiv. □

BEWEIS VON SATZ 5.10. Seien $n, m \in \mathbb{N}$ so, dass $\gcd(n,m) = 1$. Wir berechnen als erstes die Anzahl der invertierbaren Elemente von $\mathbb{Z}_n \times \mathbb{Z}_m$: Wir zeigen, dass $\binom{a}{b} \in \mathbb{Z}_n \times \mathbb{Z}_m$ genau dann invertierbar ist, wenn a invertierbar in $\mathbb{Z}_n$ und b invertierbar in $\mathbb{Z}_m$ ist. Dazu fixieren wir zunächst $\binom{a}{b} \in \mathbb{Z}_n \times \mathbb{Z}_m$ und nehmen an, dass $\binom{a}{b}$ invertierbar ist; es gibt also $\binom{c}{d} \in \mathbb{Z}_n \times \mathbb{Z}_m$, sodass $\binom{a}{b} \cdot \binom{c}{d} = 1_{\mathbb{Z}_n\times\mathbb{Z}_m} = \binom{[1]_n}{[1]_m}$. Daher ist a in $\mathbb{Z}_n$ invertierbar (mit Inversem c), ebenso b in $\mathbb{Z}_m$ (mit Inversem d). Nun fixieren wir $a \in \mathbb{Z}_n$, $b \in \mathbb{Z}_m$, beide invertierbar. Falls $ac = [1]_n$, und $bd = [1]_m$, dann ist $\binom{c}{d}$ das Inverse zu $\binom{a}{b}$. In $\mathbb{Z}_n$ gibt es $\varphi(n)$ invertierbare Elemente, in $\mathbb{Z}_m$ gibt es $\varphi(m)$ invertierbare Elemente, und somit gibt es in $\mathbb{Z}_n \times \mathbb{Z}_m$ genau $\varphi(n) \cdot \varphi(m)$ invertierbare Elemente.

Wir bestimmen nun die Anzahl der invertierbaren Elemente in $\mathbb{Z}_{nm}$: Der Ring $\mathbb{Z}_{nm}$ besitzt nach der Definition von φ genau $\varphi(nm)$ invertierbare Elemente.

Wegen Satz 5.12 sind die Ringe $\mathbb{Z}_{nm}$ und $\mathbb{Z}_n \times \mathbb{Z}_m$ isomorph und besitzen somit gleich viele invertierbare Elemente. Somit gilt $\varphi(nm) = \varphi(n) \cdot \varphi(m)$. □

Aus der Primfaktorzerlegung von $n = \prod_{i \in A} p_i^{\alpha_i}$ mit $\alpha_i \geq 1$ für alle $i \in A$ und aus $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ für Primzahlen p und $\alpha > 0$ kann man jetzt leicht $\varphi(n)$ durch

$$\begin{aligned}
\varphi(n) &= \varphi\left(\prod_{i \in A} p_i^{\alpha_i}\right) \\
&= \prod_{i \in A} \varphi\left(p_i^{\alpha_i}\right) \\
&= \prod_{i \in A} p_i^{\alpha_i} \left(1 - \tfrac{1}{p_i}\right) \\
&= \prod_{i \in A} p_i^{\alpha_i} \cdot \prod_{i \in A} \left(1 - \tfrac{1}{p_i}\right) \\
&= n \cdot \prod_{i \in A} \left(1 - \tfrac{1}{p_i}\right)
\end{aligned}$$

berechnen.

Beispiel 5.13. $\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4 = 2 \cdot 2 = \varphi(3) \cdot \varphi(4)$.

4. Zerlegungen

Lemma 5.14. *Sei R ein Ring, und seien A, B Ideale von R. Dann ist $A + B := \{a + b \mid a \in A, b \in B\}$ ein Ideal von R.*

Satz 5.15. *Sei R ein Ring, und seien A, B Ideale von R mit $A + B = R$. Dann sind die Ringe $R/(A \cap B)$ und $R/A \times R/B$ isomorph.*

Proof. Sei $h : R \to R/A \times R/B$, $h(r) := (r+A, r+B)$. Dann gilt $\ker(h) = A \cap B$. Wir zeigen nun, dass h surjektiv ist. Seien dazu $r, s \in R$. Wegen $A + B = R$ gibt es $a \in A$ und $b \in B$ mit $a + b = r - s$. Also gilt $s + b = r - a$ und somit gilt $h(r - a) = (r + a + A, s + b + B) = (r + A, s + B)$. Wegen des Homomorphiesatzes sind $R/\ker(h)$ und $h(R)$ isomorph. □

Der *Chinesische Restsatz* (Satz 5.17) bestimmt die Lösbarkeit bestimmter Systeme von Kongruenzen. Dazu brauchen wir zunächst einen Zusammenhang zwischen gcd, lcm und der Summe und dem Durchschnitt von Hauptidealen.

Satz 5.16. *Sei R ein Hauptidealbereich, und seien $a, b \in R$.*

(1) $(a) + (b) = (\gcd(a, b))$.
(2) $(a) \cap (b) = (\operatorname{lcm}(a, b))$.
(3) $(a) + ((b) \cap (c)) = ((a) + (b)) \cap ((a) + (c))$.

Proof. (1) Sei d ein Erzeuger von $(a) + (b)$. Dann gilt $a \in (d)$ und $b \in (d)$, also $d \mid a$ und $d \mid b$. Sei d' ein weiterer Teiler von a und b. Dann gilt $(a) \subseteq (d')$ und $(b) \subseteq (d')$, also $(a) + (b) \subseteq (d')$ und somit $(d) \subseteq (d')$. Folglich gilt $d \in (d')$, also $d' \mid d$. Daher ist d ein größter gemeinsamer Teiler von $\{a, b\}$. Da $\gcd(a, b)$ auch ein größter gemeinsamer Teiler von

$\{a, b\}$ ist, sind d und $\gcd(a, b)$ assoziiert in R und erzeugen daher das gleiche Ideal. Somit gilt $(d) = (\gcd(a, b))$.

(2) Sei v ein Erzeuger von $(a) \cap (b)$. Dann gilt $v \in (a)$ und $v \in (b)$, also $a \mid v$ und $b \mid v$. Sei v' ein weiteres gemeinsames Vielfaches von $\{a, b\}$. Dann gilt $v' \in (a) \cap (b)$, also $v' \in (a) \cap (b)$. Somit gilt $v' \in (v)$, also $v \mid v'$. Daher ist v ein kleinstes gemeinsames Vielfaches von $\{a, b\}$. Da alle kleinsten gemeinsamen Vielfachen zueinander assoziiert sind und daher das gleiche Ideal erzeugen, gilt $(v) = (\operatorname{lcm}(a, b))$.

(3) Sei I eine Auswahl irreduzibler Elemente von R und sei $a = \prod_{i \in I} i^{\alpha(i)}$, $b = \prod_{i \in I} i^{\beta(i)}$, $c = \prod_{i \in I} i^{\gamma(i)}$. Dann gilt

$$\begin{aligned}
(a) + ((b) \cap (c)) &= (a) + (\operatorname{lcm}(b, c)) \\
&= (a) + (\prod_{i \in I} i^{\max(\beta(i), \gamma(i))}) \\
&= (\gcd(a, \prod_{i \in I} i^{\max(\beta(i), \gamma(i))})) \\
&= (\gcd(\prod_{i \in I} i^{\alpha(i)}, \prod_{i \in I} i^{\max(\beta(i), \gamma(i))})) \\
&= (\prod_{i \in I} i^{\min(\alpha(i), \max(\beta(i), \gamma(i)))}) \\
&= (\prod_{i \in I} i^{\max(\min(\alpha(i), \beta(i)), \min(\alpha(i), \gamma(i)))} \\
&= (\operatorname{lcm}(\prod_{i \in I} i^{\min(\alpha(i), \beta(i))}, \prod_{i \in I} i^{\min(\alpha(i), \gamma(i))})) \\
&= (\prod_{i \in I} i^{\min(\alpha(i), \beta(i))}) \cap (\prod_{i \in I} i^{\min(\alpha(i), \gamma(i))}) \\
&= (\gcd(a, b)) \cap (\gcd(a, c)) \\
&= ((a) + (b)) \cap ((a) + (c)).
\end{aligned}$$

□

Für $n \in \mathbb{N}_0$ ist $\underline{n} := \{1, 2, \ldots, n\}$. In einem Ring R schreiben wir $x \equiv y \pmod{m}$, wenn $x - y$ in dem von m erzeugten Hauptideal liegt.

Satz 5.17 (Chinesischer Restsatz). *Sei R ein Hauptidealbereich, sei $n \in \mathbb{N}$, und seien $a_1, \ldots, a_n, m_1, \ldots, m_n \in R$. Dann sind äquivalent:*

(1) *Es gibt $x \in R$ mit $x \equiv a_i \pmod{m_i}$ für alle $i \in \underline{n}$.*
(2) *Für alle $i, j \in \underline{n}$ liegt $a_i - a_j$ im Ideal $(m_i) + (m_j)$.*

Proof. (1)⇒(2): Es gilt $a_j - a_j = (a_i - x) + (x - a_j) \in (m_i) + (m_j)$. (2)⇒(1): Induktion nach n. Wenn $n = 1$, so leistet $x := a_1$ das Gewünschte. Sei nun $n \geq 2$. Nach Induktionsvoraussetzung gibt es ein x_0 mit $x_0 \equiv a_i \pmod{m_i}$ für $i \in \underline{n-1}$. Für $i \in \underline{n-1}$ gilt $x_0 \equiv_{(m_i)} a_i \equiv_{(m_i)+(m_n)} a_n$,

also $x_0 - a_n \in (m_i) + (m_n)$. Somit gilt

$$x_0 - a_n \in \bigcap_{i \in \underline{n-1}} \big((m_i) + (m_n)\big).$$

Wegen Satz 5.16 gilt daher auch

$$x_0 - a_n \in \Big(\bigcap_{i \in \underline{n-1}} (m_i)\Big) + (m_n).$$

Seien $y \in \bigcap_{i \in \underline{n-1}} (m_i)$ und $z \in (m_n)$ so, dass $x_0 - a_n = y + z$. Dann gilt $x_0 - y = a_n + z$, und somit erfüllt $x := a_n + z$ die Bedingung $x \equiv a_i \pmod{m_i}$ für alle $i \in \underline{n}$. □

Algorithmisch kann man Systeme von Kongruenzen über einem Euklidischen Bereich R mit linearer Algebra über R, also mit der Hermite-Normalform lösen.

KAPITEL 6

Übersicht über einige Klassen von Ringen

Wir fassen die wichtigsten Eigenschaften von Integritätsbereichen zusammen.

SATZ 6.1. *Sei R ein Integritätsbereich. Dann gilt:*

(1) *R ist Körper $\Rightarrow$ R ist ein Euklidischer Bereich.*
(2) *R ist ein Euklidischer Bereich $\Rightarrow$ R ist ein Hauptidealbereich.*
(3) *R ist ein Hauptidealbereich $\Rightarrow$ R ist faktoriell.*

PROOF. (1) Wir setzen $\delta(x) = 1$ für alle $x \in R \setminus \{0\}$.

(2) Satz 3.14.

(3) Satz 4.10. □

Übersicht über einige Klassen von Ringen:

Kommutative Ringe mit Eins:
Es gilt: Produkt primitiver Polynome ist primitiv (Lemma 4.12). Faktorringe modulo maximalen Idealen sind Körper.

Beispiele für kommutative Ringe mit Eins, die keine Integritätsbereiche sind: $\mathbb{Z}_n$ für $n \notin \{0\} \cup \mathbb{P} \cup \{-p \mid p \in \mathbb{P}\}$, $\mathbb{Q}[X_1, \ldots, X_n]/(f)$, wenn f nicht 0 und nicht irreduzibel ist.

Integritätsbereiche:
Es gilt: prime Elemente $\neq 0$ sind irreduzibel; $a \mid b$ und $b \mid a$ impliziert, dass a und b assoziiert sind.

Beispiele für Integritätsbereiche, die nicht faktoriell sind: $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b, \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^2 + 5) \cong \{\begin{pmatrix} a & -\sqrt{5}b \\ \sqrt{5}b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$. Da $X^2 + 5$ irreduzibel und somit prim ist, ist dieser Ring ein Integritätbereich. Wegen $\det(AB) = \det(A)\det(B)$ gilt für jedes invertierbare Element $\det(\begin{pmatrix} a & -\sqrt{5}b \\ \sqrt{5}b & a \end{pmatrix}) \in \{-1, +1\}$, also $a^2 + 5b^2 = 1$, und somit $a \in \{-1, +1\}$ und $b = 0$. Die Elemente $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ sind alle irreduzibel, nicht assoziiert, und es gilt $2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.

Faktorielle Integritätsbereiche:
Es gilt: irreduzible Elemente sind prim, (ACC) für Hauptideale, gcd's und lcm's existieren immer.

Beispiele für faktorielle Integritätsbereiche, die keine Hauptidealbereiche sind: $\mathbb{Z}[X]$, $\mathbb{Q}[X_1, \ldots, X_n]$ für $n \geq 2$.

Hauptidealbereiche:
Es gilt: (ACC) für Ideale, Idealverband ist distributiv, also $I + (J \cap K) = (I + J) \cap (I + K)$

und $I \cap (J + K) = (I \cap J) + (I \cap K)$ für alle Ideale I, J, K, Chinesischer Restsatz (Satz 5.17), $\gcd(A)$ ist in der Form $\sum_{i=1}^{n} r_i a_i$ mit $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$ darstellbar.

Beispiel für einen Hauptidealbereich, der nicht Euklidisch ist: $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ (J. C. Wilson, 1973).

Euklidische Bereiche:
Es gilt: gcd's können mit dem Euklidischen Algorithmus ausgerechnet werden.

Beispiele für Euklidische Bereiche, die keine Körper sind: $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}[X], \mathbb{Q}[[X]]$.

Körper:
Es gilt: Für einen Körper K ist der Polynomring $K[X]$ euklidisch, K ist einfach.

Beispiele: $\mathbb{Q}$, $\mathbb{Z}_p$ für p prim, $D/(r)$ für einen Hauptidealbereich D und ein irreduzibles Element r, also etwa $\mathbb{Q}[X]/(X^2 - 2)$, R/M für einen kommutativen Ring mit Eins R und ein maximales Ideal M, Quotientenkörper eines Integritätsbereiches.

KAPITEL 7

Multiplikative Idealtheorie in kommutativen Ringen

1. Noethersche Ringe

DEFINITION 7.1. Ein kommutativer Ring mit Eins R ist *noethersch*, wenn die geordnete Menge $\langle \mathsf{Id}\ R, \subseteq \rangle$ die ACC erfüllt.

LEMMA 7.2. *Sei R ein kommutativer Ring mit Eins. Dann sind äquivalent:*

(1) *R ist noethersch.*
(2) *Jedes Ideal von R ist endlich erzeugt.*
(3) *Jede nichtleere Menge von Idealen von R hat ein bezüglich $\subseteq$ maximales Element.*

Beweis: Nach Satz 1.4 sind (1) und (3) äquivalent. Satz 2.9 liefert, dass R genau dann noethersch ist, wenn jedes Ideal von R endlich erzeugt ist. □

SATZ 7.3 (Hilberts Basissatz). *Sei R ein noetherscher kommutativer Ring mit Eins. Dann ist auch der Polynomring $R[x]$ noethersch.*

Beweis: Wir zeigen, dasss jedes Ideal von $R[x]$ endlich erzeugt ist. Sei dazu I ein Ideal von $R[x]$. Für jedes $n \in \mathbb{N}_0$ bilden wir nun die Menge

$$I_n := \{r \in R \mid \exists p \in R[x] : \deg(p) \leq n-1 \text{ und } r\,x^n + p \in I\}.$$

I_n enthält also 0 und alle führenden Koeffizienten von Polynomen vom Grad n in I.

Wir zeigen nun als erstes, dass jedes I_n ein Ideal von R ist. Seien dazu $n \in \mathbb{N}_0$, $i, j \in I_n$ und $r \in R$. Es gibt dann $p, q \in R[x]$ mit $\deg(p) \leq n-1$ und $\deg(q) \leq n-1$, sodass $i\,x^n + p \in I$ und $jx^n + q \in I$. Da dann auch $(i+j)\,x^n + (p+q)$ in I liegt, gilt $i + j \in I_n$. Ebenso gilt $(r\,x^0) \cdot (i\,x^n + p) \in I$. Folglich gilt $ri\,x^n + r\,p \in I$. Daher gilt $ri \in I_n$. I_n ist also wirklich ein Ideal von R.

Nun zeigen wir, dass für alle $n \in \mathbb{N}_0$ gilt:

$$I_n \subseteq I_{n+1}.$$

Sei dazu $r \in I_n$. Dann gibt es $p \in R[x]$ mit $\deg(p) \leq n-1$, sodass $r\,x^n + p \in I$. Folglich gilt $x \cdot (r\,x^n + p) \in I$, also $r\,x^{n+1} + x \cdot p \in I$. Da $\deg(x \cdot p) \leq n$, liegt r in I_{n+1}. Da R noethersch ist, erfüllt die Menge der Ideale von R die (ACC). Es gibt also ein $N \in \mathbb{N}$, sodass für alle $m \geq N$ die Gleichheit $I_m = I_N$ gilt.

Wir bilden nun eine endliche Erzeugermenge von I. Da die Ideale I_n endlich erzeugt sind, können wir für jedes $i \in \{0, \ldots, N\}$ ein $m_i \in \mathbb{N}_0$ und Elemente

$$r_{i,1}, r_{i,2}, \ldots, r_{i,m_i} \in I_i \setminus \{0\},$$

so wählen, dass

$$\langle r_{i,1}, r_{i,2}, \ldots, r_{i,m_i} \rangle_R = I_i.$$

Für jedes $r_{i,j}$ mit $i \in \{0, \ldots, N\}$ und $j \in \{1, \ldots, m_i\}$ wählen wir nun ein $f_{i,j} \in I$ so, dass es ein $p \in R[x]$ mit $\deg(p) \leq i - 1$ und

$$f_{i,j} = r_{i,j}\, x^i + p$$

gibt. Wir bilden nun die Menge

$$F := \{f_{i,j} \mid 0 \leq i \leq N, 1 \leq j \leq m_i\}.$$

Nun zeigen wir, dass die Menge F das Ideal I erzeugt. Dazu zeigen wir die folgende Behauptung durch Induktion nach n.

Für alle $n \in \mathbb{N}_0$ liegen alle $g \in I$ mit $\deg(g) \leq n$ in $\langle F \rangle_{R[x]}$.

Sei dazu $n = 0$ und $g \in I$ mit $\deg(g) = 0$. Dann gibt es ein $g_0 \in R$, sodass $g = g_0\, x^0$. Da $g = g_0 x^0 + 0$ in I liegt, gilt $g_0 \in I_0$. I_0 wird von $r_{0,1}, \ldots, r_{0,m_0}$ erzeugt. Daher gibt es $\alpha_{0,1}, \ldots, \alpha_{0,m_0}$, sodass

$$\sum_{j=1}^{m_i} \alpha_{0,j} r_{0,j} = g_0.$$

Für alle $j \in \{0, \ldots, m_0\}$ gilt $f_{0,j} = r_{0,j}\, x^0$. In $R[x]$ gilt also

$$\sum_{j=1}^{m_i} \alpha_{0,j}\, x^0 \cdot f_{0,j} = g_0\, x^0 = g.$$

Daher gilt $g \in \langle F \rangle_R$.

Für den Induktionsschritt wählen wir $n \in \mathbb{N}$. Sei $g = \sum_{i=0}^{n} g_i\, x^i$ ein Polynom in I mit $\deg g = n$. Dann gilt $g_n \in I_n$.

Wir behandeln nun zuerst den Fall $n \leq N$. Da g_n in I_n liegt, läßt es sich durch die ausgewählten Erzeuger von I_n darstellen; es gibt also $\alpha_{n,1}, \ldots, \alpha_{n,m_n} \in R$, sodass

$$g_n = \sum_{j=1}^{m_n} \alpha_{n,j} \cdot r_{n,j}.$$

Jedes Polynom $f_{n,j}$ hat Grad n und führenden Koeffizienten $r_{n,j}$. Daher hat das Polynom

$$s := \sum_{j=1}^{m_n} \alpha_{n,j}\, x^0 \cdot f_{n,j}$$

Grad n und führenden Koeffizienten g_n. Daher gilt $\deg(g - s) \leq n - 1$. Da g und s beide in I liegen, gilt auch $g - s \in I$. Nach Induktionsvoraussetzung gilt also $g - s \in \langle F \rangle_R$. Da s als Summe von Vielfachen der $f_{n,j}$ in $\langle F \rangle_R$ liegt, gilt auch $g = (g - s) + s \in \langle F \rangle_R$. Somit ist die Behauptung im Fall $n \geq N$ gezeigt.

Im Fall $n > N$ liegt g_n in I_N. Es gibt also $\alpha_{N,1}, \ldots, \alpha_{N,m_N} \in R$, sodass

$$g_n = \sum_{j=1}^{m_N} \alpha_{N,j} \cdot r_{N,j}.$$

Jedes Polynom $f_{N,j}$ hat Grad N und führenden Koeffizienten $r_{N,j}$. Daher hat das Polynom

$$s = \sum_{j=1}^{m_N} \alpha_{N,j}\, x^0 \cdot f_{N,j}$$

Grad N und führenden Koeffiziente g_n. Das Polynom $x^{n-N} \cdot s$ hat daher Grad n und führenden Koeffizienten g_n. Daher gilt $\deg(g - x^{n-N} \cdot s) \leq n-1$. Da g und $x^{n-N} \cdot s$ beide in I liegen, gilt auch $g - x^{n-N} \cdot s \in I$. Nach Induktionsvoraussetzung gilt also $g - x^{n-N} \cdot s \in \langle F \rangle_R$. Da s als Summe von Vielfachen der $f_{n,j}$ in $\langle F \rangle_R$ liegt, gilt auch $g = (g - x^{n-N} \cdot s) + x^{n-N} \cdot s \in \langle F \rangle_R$. Daher gilt auch im Fall $n > N$, dass g in $\langle F \rangle_R$ liegt.

Somit wird das Ideal I von der endlichen Menge F erzeugt. □

KOROLLAR 7.4. *Sei k ein Körper, $n \in \mathbb{N}$. Dann ist der Polynomring $k[x_1, \ldots, x_n]$ noethersch.*

Beweis: Wir zeigen durch Induktion nach n, dass $k[x_1, \ldots, x_n]$ noethersch ist.

Für $n = 0$ ist $k[x_1, \ldots, x_n]$ eine isomorphe Kopie von k. Da der Körper k nur die Ideale $\{0\}$ und k hat und diese durch $\{0\}$ beziehungsweise $\{1\}$ erzeugt werden, ist k noethersch. Für $n \geq 1$ ist der Polynomring $k[x_1, \ldots, x_n]$ isomorph zu $k[x_1, \ldots, x_{n-1}][x_n]$. Da nach Induktionsvoraussetzung $k[x_1, \ldots, x_{n-1}]$ noethersch ist, ist wegen des Hilbertschen Basissatzes auch $k[x_1, \ldots, x_{n-1}][x_n]$, und somit $k[x_1, \ldots, x_{n-1}, x_n]$ noethersch. □

2. Summen, Produkte und Quotienten von Idealen

DEFINITION 7.5. Sei R ein kommutativer Ring mit Eins, und seien I, J Ideale von R. Wir definieren $I + J$ durch

$$I + J := \{i + j \mid i \in I, j \in J\}.$$

LEMMA 7.6. *Sei R ein kommutativer Ring mit Eins, und seien I, J Ideale von R. Dann $I + J$ ein Ideal von R. Außerdem ist $I + J$ das von $I \cup J$ erzeugte Ideal.*

DEFINITION 7.7. Sei R ein kommutativer Ring mit Eins, und seien I, J Ideale von R. Wir definieren $I \cdot J$ durch

$$I \cdot J := \{\sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N}_0, i_1, \ldots, i_n \in I, j_1, \ldots, j_n \in J\}.$$

BEMERKUNG 7.8. Sei R ein kommutativer Ring mit Eins, und seien I, J Ideale von R. Dann ist $I \cdot J$ ein Ideal von R. Außerdem gilt $I \cdot J \subseteq I \cap J$.

DEFINITION 7.9. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Dann definieren wir für jedes $n \in \mathbb{N}_0$ ein Ideal I^n durch

$$I^0 := R,\ I^k = I^{k-1} \cdot I \text{ für } k \geq 1.$$

DEFINITION 7.10. Sei R ein kommutativer Ring mit Eins, sei A ein Ideal von R, und sei B eine Teilmenge von R. Wir definieren

$$(A : B)_R := \{r \in R \mid \forall b \in B : rb \in A\}.$$

$(A : B)_R$ ist der *noethersche Quotient* von A und B.

Wenn $B = \{b\}$, so schreiben wir für $(A : \{b\})_R$ auch einfach $(A : b)_R$.

ÜBUNGSAUFGABEN 7.11

(1) (Quotienten von Idealen) Berechnen Sie:
   (a) $((12) : (4))$.
   (b) $((4) : (12))$.
   (c) $((12) : (30))$.
   (d) Berechnen Sie für alle $a, b \in \mathbb{Z}$:$((a) : (b))$.
(2) (Produkt von Idealen) Sei R ein kommutativer Ring mit Eins, und seien A, B Ideale von R mit $A = \langle a_1, \ldots, a_m \rangle$ und $B = \langle b_1, \ldots, b_n \rangle$. Zeigen Sie, dass das Ideal $A \cdot B$ von der Menge $S = \{a_i b_j \mid (i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}\}$ erzeugt wird.
(3) (Berechnen des Schnitts zweier Ideale) Sei R ein kommutativer Ring mit 1, und seien I und J Ideale von R. Seien $\hat{I}$ und $\hat{J}$ die Ideale von $R[x]$, die durch

$$\begin{aligned} \hat{I} &= \{\textstyle\sum_{k=0}^{n} i_k x^k \mid n \in \mathbb{N}_0, i_0, \ldots, i_n \in I\}, \\ \hat{J} &= \{\textstyle\sum_{k=0}^{n} j_k x^k \mid n \in \mathbb{N}_0, j_0, \ldots, j_n \in J\} \end{aligned}$$

   gegeben sind.
   (a) Zeigen Sie, dass $\hat{I}$ ein Ideal von $R[x]$ ist.
   (b) Nehmen Sie an, dass $\{a_1, \ldots, a_m\}$ eine Basis von I ist. Geben Sie eine Basis von $\hat{I}$ an!
   (c) Nehmen Sie an, dass $\{b_1, \ldots, b_n\}$ eine Basis von J ist. Geben Sie eine Basis von $\hat{J} \cdot (x - 1)$ an!
   (d) Zeigen Sie

$$\{r \in R \mid r\, x^0 \in \hat{I} \cdot (x) + \hat{J} \cdot (x - 1)\} = I \cap J.$$

LEMMA 7.12. *Sei R ein kommutativer Ring mit Eins, sei A ein Ideal von R, und sei B eine Teilmenge von R. Dann ist $(A : B)_R$ ein Ideal von R.*

3. Primär- und Primideale

DEFINITION 7.13. Sei R ein kommutativer Ring mit Eins, und sei Q ein Ideal von R. Q ist *primär*, wenn

(1) $Q \neq R$,
(2) Für alle $a, b \in R$ mit $ab \in Q$ gilt $a \in Q$, oder es gibt ein $n \in \mathbb{N}$, sodass $b^n \in Q$.

DEFINITION 7.14. Sei R ein kommutativer Ring mit Eins, und sei P ein Ideal von R. P ist *prim*, wenn

(1) $P \neq R$,
(2) Für alle $a, b \in R$ mit $ab \in P$ gilt $a \in P$ oder $b \in P$.

DEFINITION 7.15. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Dann ist das *Radikal von I* gegeben durch

$$\sqrt{I} := \{r \in R \mid \exists n \in \mathbb{N} : r^n \in I\}.$$

SATZ 7.16. *Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Dann ist $\sqrt{I}$ ein Ideal von R, und es gilt $I \subseteq \sqrt{I}$. Wenn $I \neq R$, gilt außerdem $\sqrt{I} \neq R$.*

SATZ 7.17. *Sei R ein kommutativer Ring mit Eins, und sei Q ein primäres Ideal von R. Dann gilt:*

(1) $\sqrt{Q}$ *ist prim.*
(2) *Für jedes prime Ideal* P *von* R *mit* $Q \subseteq P$ *gilt auch* $\sqrt{Q} \subseteq P$.

4. Zerlegung von Idealen

Definition 7.18. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Das Ideal I ist *schnitt-irreduzibel* wenn für alle Ideale A, B von R mit $A \cap B = I$ gilt: $A = I$ oder $B = I$.

Satz 7.19. *Sei R ein noetherscher kommutativer Ring mit Eins. Dann ist jedes Ideal von R Durchschnitt endlich vieler schnitt-irreduzibler Ideale.*

Satz 7.20. *Sei R ein noetherscher kommutativer Ring mit Eins, und sei I ein schnitt-irreduzibles Ideal von R mit $I \neq R$. Dann ist I primär.*

Beweis: Nehmen wir an, dass I nicht primär ist. Dann gibt es $a, b \in R$, sodass $ab \in I$, $a \notin I$ und für alle $n \in \mathbb{N}$ auch $b^n \notin I$ gilt.

Für jedes $n \in \mathbb{N}$ ist die Menge $(I : b^n)_R$ ein Ideal von R. Außerdem gilt für alle $n \in \mathbb{N}$

$$(I : b^n)_R \subseteq (I : b^{n+1})_R. \tag{7.1}$$

Um (7.1) zu zeigen, wählen wir $n \in \mathbb{N}$ und $r \in (I : b^n)_R$. Dann gilt $rb^n \in I$. Dann gilt auch $rb^{n+1} \in I$, also $r \in (I : b^{n+1})_R$. Das beweist (7.1). Da R noethersch ist, gibt es also ein $k \in \mathbb{N}$ mit $(I : b^k)_R = (I : b^{k+1})_R$. Sei nun

$$\begin{aligned} B &:= \left\langle b^k \right\rangle_R \\ A &:= \langle a \rangle_R . \end{aligned}$$

Wir zeigen nun als erstes, dass sich I als Schnitt zweier Ideale darstellen läßt. Es gilt nämlich

$$I = (I + A) \cap (I + B). \tag{7.2}$$

Die Inklusion $\subseteq$ von (7.2) gilt, da I sowohl Teilmenge von $I + A$ als auch $I + B$ ist. Um $\supseteq$ zu zeigen, wählen wir $x \in (I + A) \cap (I + B)$. Da x in $I + A$ und in $I + B$ liegt, gibt es $i_1, i_2 \in I$ und $r_1, r_2 \in R$, sodass

$$x = i_1 + r_1 a = i_2 + r_2 b^k.$$

Dann gilt

$$xb = i_1 b + r_1 ab.$$

Da $ab \in I$, gilt $xb \in I$. Da $xb = i_2 b + r_2 b^{k+1}$, gilt auch $r_2 b^{k+1} \in I$. Somit liegt r_2 in $(I : b^{k+1})_R$, und somit auch in $(I : b^k)_R$. Dann gilt $r_2 b^k \in I$. Damit liegt aber auch $x = i_2 + r_2 b^k$ in I. Das beweist (7.2).

Da $a \in I + A$ und $a \notin I$, gilt $I \neq I + A$. Da $b^k \in I + B$ und $b^k \notin I$, gilt $I \neq I + B$. Die Gleichung (7.2) zeigt also, dass I nicht schnitt-irreduzibel ist. □

Übungsaufgaben 7.21

(1) (Prime Ideale) Zeigen Sie, dass jedes prime Ideal eines kommutativen Ringes mit Eins auch schnitt-irreduzibel ist.
(2) (Prime Ideale) Sei $R := \mathbb{Q}[x, y, z]$. Zeigen Sie:

(a) $\langle x, y\rangle$ ist prim.
(b) $\langle x^2y, xy^3\rangle$ ist nicht prim.

(3) (Primäre Ideale) Sei $R := \mathbb{Q}[x, y]$. Bestimmen Sie für jedes der folgenden Ideale, ob es primär und ob es schnitt-irreduzibel ist.
(a) $A = \langle x^4, x^2y, y^3\rangle$.
(b) $B = \langle x^4, y^3\rangle$.
(c) $C = \langle x^2y\rangle$.

SATZ 7.22. *Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, seien $Q_1, \dots, Q_n$ primäre Ideale von R mit $\sqrt{Q_1} = \cdots = \sqrt{Q_n}$. Sei $Q := Q_1 \cap \cdots \cap Q_n$. Dann ist Q primär, und $\sqrt{Q} = \sqrt{Q_1} = \cdots = \sqrt{Q_n}$.*

5. Eindeutigkeit der Zerlegung in primäre Ideale

DEFINITION 7.23. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, und seien $Q_1, \dots, Q_n$ und I Ideale von R mit $I \neq R$. Die Folge $(Q_1, \dots, Q_n)$ ist eine *Darstellung von I durch größte Primärkomponenten* [**vdW67**], wenn

(1) Alle Q_i sind primär,
(2) $I = Q_1 \cap \cdots \cap Q_n$,
(3) Für alle $i \in \{1, \dots, n\}$ gilt

$$Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n \not\subseteq Q_i,$$

(4) Für alle $i, j \in \{1, \dots, n\}$ mit $i \neq j$ gilt $\sqrt{Q_i} \neq \sqrt{Q_j}$.

SATZ 7.24 (Lasker-Noether). *Sei R ein noetherscher kommutativer Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Dann gibt es eine Darstellung von I durch größte Primärkomponenten.*

PROPOSITION 7.25. *Sei R ein kommutativer Ring mit Eins, sei B ein primäres Ideal von R, und sei A ein Ideal von R mit $A \not\subseteq \sqrt{B}$. Dann gilt $(B : A)_R = B$.*

Beweis: Sei $x \in (B : A)_R$. Wir wählen $a \in A$ mit $a \notin \sqrt{B}$. Es gilt $xa \in B$. Da B primär ist, gilt entweder $x \in B$ oder es gibt ein $n \in \mathbb{N}$, sodass $a^n \in B$. Im zweiten Fall gilt $a \in \sqrt{B}$. □

PROPOSITION 7.26. *Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, sei I ein primäres Ideal, und sei $(Q_1, \dots, Q_n)$ eine Darstellung von I durch größte Primärkomponenten. Dann gilt $n = 1$.*

Beweis: Wir nehmen $n \geq 2$ an. Sei $i \in \{1, \dots, n\}$ so, dass $\sqrt{Q_i}$ minimal in $\{\sqrt{Q_j} \mid j \in \{1, \dots, n\}\}$ ist. Wir zeigen nun, dass für alle $i \in \{1, \dots, n\}$ mit $j \neq i$ gilt:

$$\sqrt{Q_j} \not\subseteq \sqrt{Q_i}. \tag{7.3}$$

Sei dazu j so, dass $\sqrt{Q_j} \subseteq \sqrt{Q_i}$. Wegen der Minimalität von $\sqrt{Q_i}$ gilt dann $\sqrt{Q_j} = \sqrt{Q_i}$ und somit $j = i$. Das beweist (7.3). Es gibt also $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in R$, sodass für alle $j \in \{1, \dots, n\} \setminus \{i\}$ gilt

$$a_j \in \sqrt{Q_j} \text{ und } a_j \notin \sqrt{Q_i}.$$

Sei ρ_j so, dass $a_j^{\rho_j} \in Q_j$, und sei

$$\rho := \max \{\rho_j \mid j \in \{1, \dots, n\} \setminus \{i\}\}.$$

Falls $Q_i \subseteq I$, so können alle anderen Q_j aus der Darstellung von I weggelassen werden. Also gilt in diesem Fall $n = 1$ im Widerspruch zur Annahme $n \geq 2$.

Somit gilt also $Q_i \not\subseteq I$. Sei $q \in Q_i$ mit $q \notin I$. Es gilt

$$q(a_1 \cdots a_{i-1} a_{i+1} \cdots a_n)^\rho \in Q_1 \cap \cdots \cap Q_m = I.$$

Da I primär ist, gibt es ein $\sigma \in \mathbb{N}$ mit

$$(a_1 \cdots a_{i-1} a_{i+1} \cdots a_n)^{\rho\sigma} \in I.$$

Da $I \subseteq Q_i \subseteq \sqrt{Q_i}$, gilt

$$(a_1 \cdots a_{i-1} a_{i+1} \cdots a_n)^{\rho\sigma} \in \sqrt{Q_i}.$$

Das Ideal $\sqrt{Q_i}$ ist prim, also liegt ein a_j in $\sqrt{Q_i}$. Das ist ein Widerspruch zur Wahl der a_j. Der Fall $n > 1$ kann also nicht eintreten. □

LEMMA 7.27. *Sei R ein kommutativer Ring mit Eins, seien $m, n \in \mathbb{N}$, und sei I ein Ideal von R mit $I \neq R$. Seien $(Q_1, \dots, Q_m)$ und $(K_1, \dots, K_n)$ Folgen von Idealen von R. Wir nehmen an, dass $(Q_1, \dots, Q_m)$ und $(K_1, \dots, K_n)$ Darstellungen von I durch größte Primärkomponenten sind, und dass $\sqrt{Q_1}$ minimal in*

$$\{\sqrt{Q_j} \mid i \in \{j, \dots, m\}\}$$

ist. Dann gilt $m = n$, und es gibt es eine bijektive Abbildung $\pi : \{1, \dots, m\} \to \{1, \dots, n\}$, sodass $Q_1 = K_{\pi(1)}$ und für alle $i \in \{1, \dots, m\}$ gilt:

$$\sqrt{Q_i} = \sqrt{K_{\pi(i)}}.$$

Beweis: Wir gehen mit Induktion nach $\min(m, n)$ vor. Sei $\min(m, n) = 1$.

Wir betrachten zuerst den Fall $m = 1$. Dann gilt wegen Proposition 7.26 auch $n = 1$. Somit gilt $I = Q_1$ und $I = K_1$, also leistet $\pi = \mathrm{id}_{\{1\}}$ das Gewünschte. Ebenso gilt im Fall $n = 1$ nach Proposition 7.26 $m = 1$, und somit $I = Q_1 = K_1$. Damit haben wir den Induktionsanfang $\min(m, n) = 1$ gezeigt.

Für den Induktionsschritt nehmen wir nun an, $m \geq 2$ und $n \geq 2$. Sei $\mathcal{M}$ die Menge der maximalen Elemente in

$$\{\sqrt{Q_i} \mid i \in \{1, \dots, m\}\} \cup \{\sqrt{K_j} \mid j \in \{1, \dots, n\}\}. \tag{7.4}$$

Wir zeigen nun, dass es ein $P \in \mathcal{M}$ mit $P \neq \sqrt{Q_1}$ gibt. Nehmen wir im Widerspruch dazu an, dass $\sqrt{Q_1}$ das einzige einzige maximale Element der Menge in (7.4) ist, Dann gilt $\sqrt{Q_1} \geq \sqrt{Q_2}$, und wegen der Minimalität von $\sqrt{Q_1}$ somit $\sqrt{Q_1} = \sqrt{Q_2}$. Das steht im Widerspruch dazu, dass $(Q_1, \dots, Q_n)$ eine Zerlegung in größte Primärkomponenten ist.

Wir zeigen als erstes, dass P in beiden der in (7.4) vereinigten Mengen enthalten ist. Nehmen wir dazu an, dass $k \in \{1, \dots, m\}$ so ist, dass $P = \sqrt{Q_k}$ und P nicht in $\{\sqrt{K_j} \mid j \in \{1, \dots, n\}\}$ liegt. Es gilt nun:

$$\text{Für alle } i \in \{1, \dots, m\} \text{ mit } i \neq k \text{ gilt } Q_k \not\subseteq \sqrt{Q_i}. \tag{7.5}$$

Um (7.5) zu beweisen, nehmen wir $Q_k \subseteq \sqrt{Q_i}$ an. Dann gilt $\sqrt{Q_k} \subseteq \sqrt{Q_i}$, und somit erhalten wir aus der Maximalität von $\sqrt{Q_k}$ die Gleichheit $\sqrt{Q_k} = \sqrt{Q_i}$, im Widerspruch zu einer der Zerlegungseigenschaften. Das beweist (7.5). Ebenso gilt

$$\text{Für alle } j \in \{1, \dots, n\} \text{ gilt } Q_k \not\subseteq \sqrt{K_j}. \tag{7.6}$$

Denn $\sqrt{Q_k} \subseteq \sqrt{K_j}$ bedeutet wegen der Maximalität von $\sqrt{Q_k}$, dass $\sqrt{Q_k} = \sqrt{K_j}$, im Widerspruch dazu dass P nicht in $\{\sqrt{K_j} \mid j \in \{1, \dots, n\}\}$ liegt. Das beweist (7.6). Es gilt

$$(I : Q_k) = (I : Q_k),$$

also

$$(Q_1 \cap \dots \cap Q_m : Q_k) = (K_1 \cap \dots \cap K_n : Q_k),$$

und folglich

$$\bigcap\{(Q_i : Q_k) \mid i \in \{1, \dots, m\} \setminus \{k\}\} = \bigcap\{(K_j : Q_k) \mid j \in \{1, \dots, n\}.$$

Nach Proposition 7.25 gilt daher

$$\bigcap\{Q_i \mid i \in \{1, \dots, m\} \setminus \{k\}\} = \bigcap\{K_j \mid j \in \{1, \dots, n\}\}.$$

Also gilt $\bigcap\{Q_i \mid i \in \{1, \dots, m\} \setminus \{k\}\} = I \subseteq Q_k$, im Widerspruch zu einer Zerlegungseigenschaft. Ebenso führt der Fall, dass P unter den $\sqrt{K_j}$, aber nicht unter den $\sqrt{Q_i}$ vorkommt, auf einen Widerspruch.

Wir wissen also, dass es ein $k \in \{2, \dots, m\}$ und ein $l \in \{1, \dots, n\}$ gibt, sodass $P = \sqrt{Q_k} = \sqrt{K_l}$. Wir zeigen nun, dass für alle $i \in \{1, \dots, m\}$ und alle $j \in \{1, \dots, n\}$ mit $i \neq k$, $j \neq l$ gilt:

$$Q_k \cdot K_l \not\subseteq \sqrt{Q_i} \text{ und } Q_k \cdot K_l \not\subseteq \sqrt{K_j}.$$

Dazu zeigen wir als erstes $Q_k \not\subseteq \sqrt{Q_i}$. Wenn $Q_k \subseteq \sqrt{Q_i}$, so gilt $\sqrt{Q_k} \subseteq \sqrt{Q_i}$, und daher wegen der Maximalität von P auch $\sqrt{Q_k} = \sqrt{Q_i}$, im Widerspruch zu $k \neq i$. Also gilt $Q_k \not\subseteq \sqrt{Q_i}$. Ebenso gilt $K_l \not\subseteq \sqrt{Q_i}$. Denn wenn $K_l \subseteq \sqrt{Q_i}$, so gilt $\sqrt{K_l} \subseteq \sqrt{Q_i}$ und somit wegen der Maximalität von $P = \sqrt{K_l}$ auch $\sqrt{K_l} = \sqrt{Q_i}$. Dann gilt $\sqrt{Q_k} = \sqrt{Q_i}$ und somit $k = i$, im Widerspruch zu $k \neq i$. Es gibt also $q_1 \in Q_k \setminus \sqrt{Q_i}$ und $q_2 \in K_l \setminus \sqrt{Q_i}$. Da $\sqrt{Q_i}$ prim ist, gilt $q_1 q_2 \in Q_k \cdot K_l$ und $q_1 q_2 \notin \sqrt{Q_i}$. Ebenso beweist man $Q_k \cdot K_l \not\subseteq \sqrt{K_j}$ für $j \neq l$. Es gilt

$$I = \bigcap\{Q_i \mid i \in \{1, \dots, m\}\} = \bigcap\{K_j \mid j \in \{1, \dots, n\}\}.$$

Wir berechnen $(I : Q_k \cdot K_l)$. Nach Proposition 7.25 erhalten wir

$$\begin{aligned} &Q_1 \cap \dots \cap Q_{k-1} \cap (Q_k : Q_k \cdot K_l) \cap Q_{k+1} \cap \dots \cap Q_m \\ &\qquad = K_1 \cap \dots \cap K_{l-1} \cap (K_l : Q_k \cdot K_l) \cap K_{l+1} \cap \dots \cap K_n. \end{aligned}$$

Da $Q_k \cdot K_l \subseteq Q_k$, gilt $(Q_k : Q_k \cdot K_l) = R$, und ebenso $(K_l : Q_k \cdot K_l) = R$. Wir erhalten also zwei Darstellungen von $(I : Q_k \cdot K_l)$, eine durch $m - 1$ und eine durch $n - 1$ Primärkomponenten. Nach Induktionsvoraussetzung gibt es also ein $\pi' : \{1, \dots, m\} \setminus \{k\} \to \{1, \dots, n\} \setminus \{l\}$, sodass $Q_1 = K_{\pi'(1)}$ und $\sqrt{Q_i} = \sqrt{K_{\pi'(i)}}$ für alle $i \in \{1, \dots, m\} \setminus \{k\}$. Daher leistet $\pi := \pi' \cup \{(k, l)\}$ das Gewünschte. □

THEOREM 7.28 (Erster Eindeutigkeitssatz). *Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Seien $(Q_1, \ldots, Q_n)$ und $(K_1, \ldots, K_m)$ Folgen von Idealen von R. Wir nehmen an, dass $(Q_1, \ldots, Q_n)$ und $(K_1, \ldots, K_m)$ Darstellungen von I durch größte Primärkomponenten sind. Dann gilt $n = m$, und es gibt es eine bijektive Abbildung $\pi : \{1, \ldots, n\} \to \{1, \ldots, m\}$, sodass für alle $i \in \{1, \ldots, n\}$ gilt:*

$$\sqrt{Q_i} = \sqrt{K_{\pi(i)}}.$$

THEOREM 7.29 (Zweiter Eindeutigkeitssatz). *Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Seien $(Q_1, \ldots, Q_n)$ und $(K_1, \ldots, K_m)$ Folgen von Idealen von R. Wir nehmen an, dass $(Q_1, \ldots, Q_n)$ und $(K_1, \ldots, K_n)$ Darstellungen von I durch größte Primärkomponenten sind, sodass für alle $j \in \{1, \ldots, n\}$ gilt:*

$$\sqrt{Q_j} = \sqrt{K_j}.$$

Sei $i \in \{1, \ldots, n\}$ so, dass $\sqrt{Q_i}$ minimal in $\{\sqrt{Q_j} \mid j \in \{1, \ldots, n\}\}$ ist. Dann gilt $Q_i = K_i$.

Beweis: Wir betrachten die Folgen $(Q'_1, \ldots, Q'_n)$ und $(K'_1, \ldots, K'_n)$, die durch $Q'_1 := Q_i$, $Q'_i := Q_1$, $Q'_j = Q_j$ für $j \in \{1, \ldots, n\} \setminus \{1, i\}$ und $K'_1 := K_i$, $K'_i := K_1$, $K'_j = K_j$ für $j \in \{1, \ldots, n\} \setminus \{1, i\}$ gegeben sind. Wegen Lemma 7.27 gibt es eine bijektive Abbildung π, sodass $\sqrt{Q'_j} = \sqrt{K'_{\pi(j)}}$ für alle $j \in \{1, \ldots, n\}$ und $Q'_1 = K'_{\pi(1)}$. Daraus erhalten wir eine bijektive Abbildung σ, sodass für alle $j \in \{1, \ldots, n\}$ die Gleichheit $\sqrt{Q_j} = \sqrt{K_{\sigma(j)}}$ gilt, und weiters $Q_i = K_{\sigma(i)}$. Es gilt also $\sqrt{K_{\sigma(i)}} = \sqrt{Q_i} = \sqrt{K_i}$. Da $(K_1, \ldots, K_n)$ eine Darstellung durch größte Primärkomponenten ist, gilt $i = \sigma(i)$. Also gilt $Q_i = K_i$. □

KAPITEL 8

Ringerweiterungen

1. Determinanten

Determinanten kann man nicht nur für Matrizen über Körpern, sondern auch für Matrizen über kommutativen Ringen mit Eins definieren. Die Menge S_n sei die Menge aller Permutationen der Menge $\{1, \ldots, n\}$. Für jede Permutation π definieren wir die *Signatur* von π durch

$$\operatorname{sgn}(\pi) := \prod_{\substack{(i,j)\in\{1,\ldots,n\}^2 \\ i>j}} \frac{\pi(i) - \pi(j)}{i - j}.$$

DEFINITION 8.1. Sei R ein kommutativer Ring mit Eins, und sei A eine $n \times n$-Matrix. Dann definieren wir die *Determinante* von A durch

$$\det(A) := \sum_{\pi\in S_n} (-1)^{\operatorname{sgn}(i)} \prod_{i=1}^{n} A_{i,\pi(i)}.$$

Wir werden im folgenden drei Eigenschaften der Determinante brauchen. Für $v_1, \ldots, v_n \in R^n$ schreiben wir $(v_1, \ldots, v_n)$ für die $n \times n$-Matrix, deren Spaltenvektoren $v_1, \ldots, v_n$ sind.

SATZ 8.2. *Sei R ein kommutativer Ring mit Eins, und seien $a_1, \ldots, a_n, v, w \in R^n$ und $r \in R$. Dann gilt:*

(1) *(Multilinearität)*

$$\det((a_1, \ldots, a_{i-1}, v + w, a_{i+1}, \ldots, a_n)) = \det((a_1, \ldots, a_{i-1}, v, a_{i+1}, \ldots, a_n)) + \det((a_1, \ldots, a_{i-1}, w, a_{i+1}, \ldots, a_n))$$

(2) *(R-Homogenität)*

$$\det((a_1, \ldots, a_{i-1}, r\,v, a_{i+1}, \ldots, a_n)) = r \cdot \det((a_1, \ldots, a_{i-1}, v, a_{i+1}, \ldots, a_n)).$$

(3) *Wenn es $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gibt, sodass $a_i = a_j$, so gilt*

$$\det((a_1, \ldots, a_n)) = 0.$$

Beweisskizze: Da in jedem Summanden in der Definition der Determinante genau einer der Faktoren $A_{1,i}, A_{2,i}, \ldots, A_{n,i}$ vorkommt (nämlich $A_{\pi^{-1}(i),i}$), gelten (1) und (2). Für den Beweis von (3) sei A die Matrix $(a_1, \ldots, a_n)$. Da die i-te und die j-te Spalte der Matrix gleich sind, gilt für alle $k \in \{1, \ldots, n\}$ und alle $\pi \in S_n$, dass $A_{k,\,(i,j)\circ\pi\,(k)} = A_{k,\,\pi(k)}$. Somit unterscheiden sich die Summanden in der Definition der Determinante für π und $(i, j) \circ \pi$ nur durch das Vorzeichen und kürzen sich also weg. □

SATZ 8.3. *Sei R ein kommutativer Ring mit Eins Sei A eine $n \times n$ Matrix mit Einträgen aus R. Dann gibt es eine $n \times n$-Matrix B mit Einträgen aus R, sodass*

$$B \cdot A = \begin{pmatrix} \det(A) & 0 & 0 & \dots & 0 \\ 0 & \det(A) & 0 & \dots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \det(A) \end{pmatrix}.$$

Wir werden als Abkürzung für die $n \times n$-Matrix

$$\begin{pmatrix} r & 0 & 0 & \dots & 0 \\ 0 & r & 0 & \dots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & r \end{pmatrix}$$

mit $r \in R$ auch oft kürzer $r\,\boldsymbol{I}_n$ schreiben.

Beweis von Satz 8.3: Für $i \in \{1, \dots, n\}$ sei

$$e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{-te Zeile}$$

der i-te Einheitsvektor. Die Vektoren $a_1, \dots, a_n$ seien die Spaltenvektoren der Matrix A; es gilt also $A = (a_1, \dots, a_n)$. Sei nun B die Matrix, die durch

$$B(i,j) := \det\left((a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n)\right)$$

definiert ist. Sei $C := B \cdot A$, und seien $i, k \in \{1, \dots, n\}$. Wir berechnen nun den Eintrag $C(i,k)$. Es gilt

$$\begin{aligned} C(i,k) &= \sum_{j=1}^{n} B(i,j) \cdot A(j,k) \\ &= \sum_{j=1}^{n} \det\left((a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n)\right) \cdot A(j,k). \end{aligned}$$

Somit erhalten wir aus dem Satz 8.2

$$\begin{aligned} C(i,k) &= \sum_{j=1}^{n} \det\left((a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n)\right) \cdot A(j,k) \\ &= \det\left((a_1, \dots, a_{i-1}, \sum_{j=1}^{n} A(j,k)\, e_j, a_{i+1}, \dots, a_n)\right). \end{aligned}$$

Der Vektor $\sum_{j=1}^{n} A(j,k)\, e_j$ ist genau der k-te Spaltenvektor a_k von A. Wenn $k = i$, so ist $C(i,k)$ also genau $\det(A)$. Wenn $k \neq i$, so sind in der Matrix

$$(a_1, \ldots, a_{i-1}, a_k, a_{i+1}, \ldots, a_n))$$

die i-te und k-te Spalte gleich. Diese Matrix hat nach Satz 8.2 die Determinante 0. □

2. Ganze Erweiterungen

Seien A, B kommutative Ringe mit Eins. Wir schreiben $A \leq B$, wenn A ein Unterring von B (mit dem gleichen Einselement) ist.

Definition 8.4. Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $S = \langle s_i \mid i \in I \rangle$ eine Folge von Elementen von B. Dann ist $A[\![S]\!]$ der Durchschnitt aller Unterringe R von B mit $A \cup \{s_i \mid i \in I\} \subseteq R$.

Definition 8.5. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$, und sei $x \in B$. Das Element x ist *ganz über* A, wenn x Nullstelle eines Polynoms in $A[t]$ mit führendem Koeffizienten 1 ist.

Definition 8.6. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. B ist *ganz über* A, wenn alle $b \in B$ ganz über A sind.

Für einen kommutativen Ring mit Eins B, $A \subseteq B$ und $b \in B$ definieren wir

$$A \cdot b := \{ab \mid a \in A\}.$$

Satz 8.7. *Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Wenn x ganz über A ist, so gibt es $n \in \mathbb{N}$ und $b_0, \ldots, b_{n-1} \in B$ mit $b_0 = 1$, sodass*

$$A[\![x]\!] = A \cdot 1 + A \cdot b_1 + \cdots + A \cdot b_{n-1}. \tag{8.1}$$

Beweis: Sei n der Grad eines Polynoms mit führendem Koeffizienten 1, das x als Nullstelle hat, und sei $b_i := x^i$. Für die Inklusion $\supseteq$ der Gleichung (8.1) beobachten wir, dass $A \subseteq A[\![x]\!]$ und $x \in A[\![x]\!]$. Da $A[\![x]\!]$ ein Ring ist, liegt folglich jedes Element auf der rechten Seite von (8.1) in $A[\![x]\!]$.

Für $\subseteq$ zeigen wir, dass die rechte Seite ein Unterring von B ist. Die Abgeschlossenheit unter $+$ und $-$ ist offensichtlich. Wir zeigen nun, dass auch das Produkt zweier Elemente aus $A \cdot x^0 + \cdots + A \cdot x^{n-1}$ wieder in $A \cdot x^0 + \cdots + A \cdot x^{n-1}$ liegt. Seien dazu $\sum_{i=1}^{n-1} a_i x^i$ und $\sum_{i=1}^{n-1} a_i' x^i \in \sum_{i=1}^{n-1} A \cdot x^i$. Das Produkt dieser beiden Elemente ist

$$\sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_i a_j' x^{i+j}.$$

Wir zeigen nun, dass für alle $m \in \mathbb{N}_0$ gilt: $x^m \in \sum_{i=1}^{n-1} A \cdot x^i$. Wir gehen mit Induktion nach m vor. Wenn $m \leq n-1$, so liegt $x^m = 1 \cdot x^m$ klarerweise in $A \cdot x^m$. Wenn $m \geq n$, so wählen wir

ein Polynom $p(t) = 1\,t^n + p_{n-1}t^{n-1} + \cdots + p_0 t^0 \in A[t]$, das x als Nullstelle hat. Dann gilt

$$\begin{aligned} x^m &= x^m - x^{m-n} \cdot 0 \\ &= x^m - x^{m-n}(x^n + p_{n-1}x^{n-1} + \cdots + p_0 x^0). \\ &= -p_{n-1}x^{m-1} - \cdots - p_0 x^{m-n}. \end{aligned}$$

Nach Induktionsvoraussetzung liegt jedes x^i mit $i \leq m-1$ in $\sum_{i=1}^{n-1} A \cdot x^i$, und folglich auch $-p_{n-1}x^{m-1} - \cdots - p_0 x^{m-n}$. Also gilt $x^m \in \sum_{i=1}^{n-1} A \cdot x^i$.

Damit haben wir gezeigt, dass $\sum_{i=1}^{n-1} A \cdot x^i$ abgeschlossen unter $\cdot$ ist. $\sum_{i=1}^{n-1} A \cdot x^i$ ist also ein Unterring von B, der A und x enthält. Daher gilt auch $\subseteq$ in (8.1). □

Satz 8.8. *Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Sei $x \in B$ so, dass es $n \in \mathbb{N}$ und $b_0, \ldots, b_{n-1} \in B$ gibt, sodass*

(1) $b_0 = 1$,
(2) $\sum_{i=0}^{n-1} A \cdot b_i$ *ist abgeschlossen unter* $\cdot$,
(3) $x \in \sum_{i=0}^{n-1} A \cdot b_i$.

Dann ist x ganz über A.

Beweis: Sei $i \in \{0, \ldots, n-1\}$. Aufgrund der Voraussetzungen liegt auch xb_i in $\sum_{i=0}^{n-1} A \cdot b_i$. Es gibt also $a_{i,0}, \ldots, a_{i,n-1} \in A$, sodass

$$xb_i = a_{i,0}b_0 + \cdots + a_{i,n-1}b_{n-1}. \tag{8.2}$$

Sei M die $n \times n$-Matrix über A, die durch

$$M := \begin{pmatrix} a_{0,0} & \cdots & a_{0,n-1} \\ \vdots & & \vdots \\ a_{n-1,0} & \cdots & a_{n-1,n-1} \end{pmatrix}$$

definiert ist. Die Gleichungen aus (8.2) lassen sich mit dieser Matrix zusammengefasst als

$$x \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = M \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

schreiben. Es gilt also

$$\left(\begin{pmatrix} x & 0 & 0 & \ldots & 0 \\ 0 & x & 0 & \ldots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & x \end{pmatrix} - M \right) \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = 0. \tag{8.3}$$

Aus Satz 8.3 erhalten wir eine $n \times n$-Matrix L mit Einträgen aus B, sodass

$$L \cdot (x\,\boldsymbol{I}_n - M) = \begin{pmatrix} \det(x\,\boldsymbol{I}_n - M) & 0 & 0 & \dots & 0 \\ 0 & \det(x\,\boldsymbol{I}_n - M) & 0 & \dots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \det(x\,\boldsymbol{I}_n - M) \end{pmatrix}.$$

Durch Multiplikation der Gleichung (8.3) von links mit L erhalten wir

$$\begin{pmatrix} \det(x\,\boldsymbol{I}_n - M) & 0 & 0 & \dots & 0 \\ 0 & \det(x\,\boldsymbol{I}_n - M) & 0 & \dots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \det(x\,\boldsymbol{I}_n - M) \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = 0.$$

Da $b_0 = 1$, folgt aus dieser Gleichung

$$\det(x\,\boldsymbol{I}_n - M) = 0. \tag{8.4}$$

Wir betrachten nun das Polynom $p \in A[t]$, das durch

$$p(t) := \det\left(\begin{pmatrix} t & 0 & 0 & \dots & 0 \\ 0 & t & 0 & \dots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & t \end{pmatrix} - M \right)$$

gegeben ist. Die Matrix auf der rechten Seite der letzten Gleichung ist dabei eine Matrix mit Einträgen aus dem Polynomring $A[t]$. Aus der Definition der Determinante sieht man, dass p ein Polynom vom Grad n mit führendem Koeffizienten 1 ist. Wegen der Gleichung (8.4) gilt $\overline{p}(x) = 0$. Das Polynom p bezeugt also, dass x ganz über A ist. □

Satz 8.9. *Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Sei $x \in B$ so, dass x ganz über A ist. Dann ist $A[\![x]\!]$ ganz über A.*

Beweis: Sei $y \in A[\![x]\!]$. Da x ganz über A ist, gibt es wegen Satz 8.7 $n \in \mathbb{N}$ und $b_0, \dots, b_{n-1} \in B$, sodass $A[\![x]\!] = \sum_{i=1}^{n} A \cdot b_i$ und $b_0 = 1$. Da y in $\sum_{i=1}^{n} A \cdot b_i$ liegt, ist y nach Satz 8.8 ganz über A. □

Allgemeiner gilt:

Satz 8.10. *Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$, und seien $x, y \in B$. Wenn x ganz über A ist, und y ganz über $A[\![x]\!]$ ist, so ist y ganz über A.*

Beweis: Da y ganz über $\mathbb{A}[\![x]\!]$ ist, gibt es $n \in \mathbb{N}$ und $c_0, \dots, c_{n-1} \in B$ mit $c_0 = 1$ und

$$(A[\![x]\!])[\![y]\!] = \sum_{i=0}^{n-1} A[\![x]\!] \cdot c_i.$$

Da x ganz über A ist, gibt es $m \in \mathbb{N}$ und $b_0, \ldots, b_{m-1} \in B$ mit $b_0 = 1$ und

$$A[\![x]\!] = \sum_{j=0}^{m-1} A \cdot b_j.$$

Insgesamt gilt also

$$(A[\![x]\!])[\![y]\!] = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} A \cdot (b_j c_i).$$

Da y in dieser endlichen Summe liegt, ist y nach Satz 8.8 ganz über A. □

Übungsaufgaben 8.11

(1) Sei $q \in \mathbb{Q}$ eine rationale Zahl, die ganz über $\mathbb{Z}$ ist. Zeigen Sie $q \in \mathbb{Z}$.
(2) Sei $R := \mathbb{Q}[x,y]/I$, wobei $I := \langle x^2 + xy + 1 \rangle$. Mit Q bezeichnen wir den Unterring $\{q + I \mid q \in \mathbb{Q}\}$. Zeigen Sie:
   (a) $x + I$ ist nicht ganz über Q.
   (b) $x + I$ ist ganz über $Q[\![y + I]\!]$.
(3) Sei $R := \mathbb{Z}[\![\sqrt[3]{2}]\!]$, und sei $x := 5 + \sqrt[3]{2}$. Da $x \in \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}(\sqrt[3]{2})^2$ und da $\mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}(\sqrt[3]{2})^2$ ein Unterring von $\mathbb{R}$ ist, ist auch x ganz über $\mathbb{Z}$. Im folgenden Beispiel konstruieren wir ein Polynom in $\mathbb{Z}[t]$ mit führendem Koeffizienten 1, das x als Nullstelle hat.
   (a) Sei $b_0 := 1$, $b_1 := \sqrt[3]{2}$, $b_2 := (\sqrt[3]{2})^2$. Finden Sie eine 3×3-Matrix A, sodass
   $$\begin{pmatrix} b_0 x \\ b_1 x \\ b_2 x \end{pmatrix} = A \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix}.$$
   (b) Berechnen Sie das charakteristische Polynom von A.
(4) (Ringerweiterungen) Wir betrachten den Ring $\mathbb{Q}[x]$ und seine Unterringe $\mathbb{Q}[\![x^3 - 3x^2 + 2x]\!]$ und $\mathbb{Q}$.
   (a) Ist $\mathbb{Q}[x]$ ganz über $\mathbb{Q}[\![x^3 - 3x^2 + 2x]\!]$?
   (b) Ist $\mathbb{Q}[\![x^3 - 3x^2 + 2x]\!]$ ganz über $\mathbb{Q}$?

Satz 8.12. *Seien A, B, C kommutative Ringe mit Eins, sodass $A \leq B \leq C$. Wenn B ganz über A, und C ganz über B ist, so ist C ganz über A.*

Sei $x \in C$. Da x ganz über B ist, gibt es $n \in \mathbb{N}$ und $b_0, \ldots, b_{n-1} \in B$, sodass

$$x^n + \sum_{i=0}^{n-1} b_i x^i = 0. \tag{8.5}$$

Diese Gleichung belegt, dass x ganz über $A[\![b_0, \ldots, b_{n-1}]\!]$ ist. Da b_0 ganz über A ist, ist b_0 auch ganz über $A[\![b_1, \ldots, b_{n-1}]\!]$. Da also x ganz über $A[\![b_1, \ldots, b_{n-1}]\!][\![b_0]\!]$ und b_0 ganz über $A[\![b_1, \ldots, b_{n-1}]\!]$ ist, ist x wegen Satz 8.10 auch ganz über $A[\![b_1, \ldots, b_{n-1}]\!]$. Wir zeigen nun allgemein mit Induktion nach i, dass für alle $i \in \{1, \ldots, n\}$ gilt:

$$x \text{ ist ganz über } A[\![b_i, b_{i+1}, \ldots, b_{n-1}]\!]. \tag{8.6}$$

Für $i = 0$ ergibt sich das aus der Gleichung 8.5. Wir nehmen nun an, dass $i \leq n - 1$ und x ganz über $A[\![b_i, b_{i+1}, \ldots, b_{n-1}]\!] = (A[\![b_{i+1}, \ldots, b_{n-1}]\!])[\![b_i]\!]$ ist. Da b_i ganz über A ist, gilt auch:

$$b_i \text{ ist ganz über } A[\![b_{i+1}, \ldots, b_{n-1}]\!].$$

Somit ist x nach Satz 8.10 auch ganz über $A[\![b_{i+1}, \ldots, b_{n-1}]\!]$. Somit gilt (8.6) für alle $i \in \{0, \ldots, n\}$. Für $i := n$ erhalten wir, dass x ganz über A ist. □

3. Algebraische Erweiterungen

DEFINITION 8.13. Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $e \in B$. Das Element e ist *algebraisch* über A, wenn es ein $p \in A[t]$ mit $p \neq 0$ gibt, sodass $\overline{p}(e) = 0$. B ist *algebraisch* über A, wenn alle $b \in B$ algebraisch über A sind.

ÜBUNGSAUFGABEN 8.14

(1) Sei R ein Ring, der $\mathbb{C}[t]$ als Unterring (mit demselben Einselement) enthält. Wir nehmen an, dass R ganz über $\mathbb{C}[t]$ ist. Zeigen Sie, dass R kein Körper ist. *Hinweis:* Wenn R ein Körper ist, so ist $\frac{1}{t}$ in R. Also ist $\frac{1}{t}$ ganz über $\mathbb{C}[t]$. Verwenden Sie jetzt das Polynom in $\mathbb{C}[t][t_1]$, dessen Nullstelle $\frac{1}{t}$ ist, um zu zeigen, dass t algebraisch über $\mathbb{C}$ ist – Widerspruch.

LEMMA 8.15. *Seien A, B Integritätsbereiche mit $A \leq B$. Dann sind äquivalent:*

(1) *B ist algebraisch über A.*
(2) *$Q(B)$ ist algebraisch über $Q(A)$.*

Beweis: (1)⇒(2): Seien $p, q \in B$ mit $q \neq 0$. Wir zeigen, dass $\frac{p}{q}$ algebraisch über $Q(A)$ ist. Da q algebraisch über A ist, gibt es ein Polynom $f \in A[t]$ vom Grad $n \geq 1$, sodass

$$\overline{f}(q) = 0.$$

Für $g(x) := x^n \cdot f(\frac{1}{x})$ gilt $\overline{g}(\frac{1}{q}) = 0$. Also ist $\frac{1}{q}$ algebraisch über A, und somit ganz über $Q(A)$. Das Element p ist ganz über $Q(A)$, also auch über $Q(A)[\![\frac{1}{q}]\!]$. Also ist $Q(A)[\![\frac{1}{q}]\!][\![p]\!]$ ganz über $Q(A)$. Da $\frac{p}{q} \in Q(A)[\![\frac{1}{q}]\!][\![p]\!]$, ist $\frac{p}{q}$ ganz über $Q(A)$. (2)⇒(1): Sei $b \in B$. Dann ist b Nullstelle eines Polynoms f in $Q(A)[t] \setminus \{0\}$, und nach Multiplikation mit den Nennern der Koeffizienten von f auch eines Polynoms $g \in A[t] \setminus \{0\}$. □

PROPOSITION 8.16. *Seien A, B, C Integritätsbereiche mit $A \leq B \leq C$. Wenn B algebraisch über A und C algebraisch über B ist, so ist C algebraisch über A.*

Beweis: Nach Lemma 8.15 ist $Q(B)$ algebraisch, also ganz, über $Q(A)$, und $Q(C)$ ganz über $Q(B)$. Also ist $Q(C)$ ganz über $Q(A)$, und somit ist C algebraisch über A. □

SATZ 8.17. *Seien A, B Integritätsbereiche mit $A \leq B$, sei $x \in B$. Wenn x algebraisch über A ist, so ist auch $A[\![x]\!]$ algebraisch über A.*

Beweis: Da x algebraisch über A ist, gibt es ein $n \in \mathbb{N}$ und ein Polynom $p = \sum_{i=0}^{n} p_i\, t^i \in A[t]$ von Grad n, sodass

$$\sum_{i=0}^{n} p_i\, x^i = 0.$$

In $Q(B)$ gilt dann

$$\sum_{i=0}^{n} \frac{p_i}{p_n}\, x^i = 0. \tag{8.7}$$

Es gilt $Q(A) \leq Q(B)$. Nach (8.7) ist $\frac{x}{1}$ ganz über $Q(A)$. Wegen Satz 8.9 ist also $Q(A)[\![\frac{x}{1}]\!]$ ganz über $Q(A)$.

Wir zeigen nun, dass $A[\![x]\!]$ algebraisch über A ist. Sei dazu $y \in A[\![x]\!]$. Dann liegt $\frac{y}{1}$ in $Q(A)[\![\frac{x}{1}]\!]$. Es gibt also ein Polynom $q \in Q(A)[t]$ vom Grad $n \geq 1$, sodass $\overline{q}(\frac{y}{1}) = 0$. Durch Multiplikation mit allen Nennern der Koeffizienten von q erhalten wir ein Polynom $q' \in A[t]$ vom Grad $n \geq 1$, sodass $\overline{q'}(y) = 0$. Daher ist y algebraisch über A. □

LEMMA 8.18. *Seien A, C Integritätsbereiche mit $A \leq C$. Dann ist die Menge $B := \{b \in C \mid b$ ist algebraisch über $A\}$ ein Unterring von C.*

Beweis: Seien $x_1, x_2 \in B$. Da x_2 algebraisch über A ist, ist x_2 auch algebraisch über $A[\![x_1]\!]$. Somit ist nach Satz 8.17 auch $A[\![x_1]\!][\![x_2]\!] = A[\![x_1, x_2]\!]$ algebraisch über $A[\![x_1]\!]$. Ebenso ist nach Satz 8.17 der Ring $A[\![x_1]\!]$ algebraisch über A. Nach Proposition 8.16 ist daher $A[\![x_1, x_2]\!]$ algebraisch über A. Da $\{x_1 + x_2, x_1 - x_2, x_1 \cdot x_2\} \subseteq A[\![x_1, x_2]\!]$, liegen Summe, Differenz und Produkt von x_1 und x_2 in B. Daher ist B ein Unterring von C. □

DEFINITION 8.19. Seien A, B kommutative Ringe mit Eins mit $A \leq B$. Eine Folge $S = \langle s_i \mid i \in I\rangle$ von Elementen aus B ist *algebraisch unabhängig über A*, wenn für alle $n \in \mathbb{N}$, für alle $p \in A[t_1, \ldots, t_n] \setminus \{0\}$ und für alle paarweise verschiedenen $i_1, \ldots, i_n \in I$ gilt:

$$\overline{p}(s_{i_1}, \ldots, s_{i_n}) \neq 0.$$

DEFINITION 8.20. Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei S eine Folge von Elementen aus B. S ist eine *Transzendenzbasis* von B über A, wenn S maximal unter den algebraisch unabhängigen Folgen aus B ist.

PROPOSITION 8.21. *Seien A, B kommutative Ringe mit Eins mit $A \leq B$. Dann besitzt B eine Transzendenzbasis über A.*

Beweis: Sei $\mathcal{S}$ eine Kette über A algebraisch unabhängiger Folgen, und sei $S := \bigcup \mathcal{S}$.

Wenn $S = \langle s_i \mid i \in I\rangle$ algebraisch abhängig ist, gibt es $i_1, \ldots, i_n \in I$, und $p \in A[t_1, \ldots, t_n]$ mit $p \neq 0$, sodass $\overline{p}(s_{i_1}, \ldots, s_{i_n}) = 0$. Es gibt nun ein Element $S' \in \mathcal{S}$, das $\langle s_{i_k} \mid k \in \{1, \ldots, n\}\rangle$ enthält. Daher ist S' algebraisch abhängig.

Also ist S algebraisch unabhängig. Somit liefert das Zornsche Lemma eine Transzendenzbasis von B. □

SATZ 8.22. *Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $S = \langle s_i \mid i \in I\rangle$ eine über A algebraisch unabhängige Teilfolge von B. Sei $e \in B$, und sei $j \notin I$. Sei $S' := S \cup \{(j, e)\}$. Dann sind äquivalent:*

(1) *S' ist algebraisch abhängig über A.*
(2) *e ist algebraisch über $A[\![S]\!]$.*

Beweis: (1)⇒(2): Seien $n \in \mathbb{N}_0$, $i_1, \ldots, i_n$ paarweise verschiedene Elemente aus I und $f \in A[t_1, \ldots, t_{n+1}]$ so, dass $f \neq 0$ und $\overline{f}(s_{i_1}, \ldots, s_{i_n}, e) = 0$. Sei nun

$$f(t_1, \ldots, t_{n+1}) = \sum_{j=0}^{m} u_j(t_1, \ldots, t_n) {t_{n+1}}^j.$$

Dann gilt

$$\sum_{j=0}^{m} \overline{u_j}(s_{i_1}, \ldots, s_{i_n}) e^j = 0.$$

Für das Polynom $g := \sum_{j=0}^{m} \overline{u_j}(s_{i_1}, \ldots, s_{i_n}) t^j \in A[\![S]\!][t]$ gilt, da S algebraisch unabhängig ist, $g \neq 0$ und $\overline{g}(e) = 0$. Somit ist e algebraisch über $A[\![S]\!]$.

(2)⇒(1): Sei $g \in A[\![S]\!][t]$ so, dass $g \neq 0$ und $\overline{g}(e) = 0$. Jedes Element in $A[\![S]\!]$ lässt sich in der Form $\overline{u}(s_{i_1}, \ldots, s_{i_n})$ mit $n \in \mathbb{N}$ und $u \in A[t_1, \ldots, t_n]$ schreiben. Also lässt sich das Polynom g schreiben als

$$g = \sum_{k=0}^{\deg(g)} \overline{u_k}(s_{i_1}, \ldots, s_{i_m}) t^k.$$

wobei $m \in \mathbb{N}$ und die i_j paarweise verschieden sind. Wir betrachten nun das Polynom $g' \in A[t_1, \ldots, t_{m+1}]$, das durch

$$g'(t_1, \ldots, t_{m+1}) = \sum_{k=0}^{\deg(g)} u_k(t_1, \ldots, t_m) {t_{m+1}}^k$$

definiert ist. Es gilt $g' \neq 0$ und $\overline{g'}(s_{i_1}, \ldots, s_{i_m}, e) = 0$. Folglich ist $S \cup \{(j, e)\}$ algebraisch abhängig über A. □

Die Voraussetzung, dass S algebraisch unabhängig ist, wird für die Implikation (1)⇒(2) wirklich gebraucht. Wenn nämlich $A \leq B$ Integritätsbereiche sind, und $b_1, b_2 \in B$ algebraisch abhängig sind, so muss deswegen aber b_2 nicht algebraisch über $A[\![b_1]\!]$ sein. Als Beispiel sei $A := \mathbb{R}$, $B := \mathbb{C}(t)$, $b_1 := i, b_2 := t$. Für $f(t_1, t_2) := t_1^2 t_2 + t_2$ gilt $\overline{f}(i, t) = 0$. Trotzdem ist t nicht algebraisch über $\mathbb{R}[\![i]\!] = \mathbb{C}$.

LEMMA 8.23. *Seien A, B Integritätsbereiche mit $A \leq B$, und sei $X \subseteq B$ so, dass $A[\![X]\!] = B$. Sei U eine maximale Teilfolge aus X mit der Eigenschaft, dass U algebraisch unabhängig ist. Dann ist U eine Transzendenzbasis von B über A.*

Beweis: Wegen Satz 8.22 ist jedes $x \in X$ algebraisch über $A[\![U]\!]$. Die über $A[\![U]\!]$ algebraischen Elemente von B bilden nach Lemma 8.18 einen Unterring von B. Dieser Unterring enthält alle Elemente von X und A. Somit enthält dieser Unterring ganz $A[\![X]\!]$, und ist somit gleich B. □

SATZ 8.24. *Seien A, B Integritätsbereiche mit $A \leq B$, sei $(x_1, \ldots, x_m)$ eine Transzendenzbasis von B über A, sei $r \in \mathbb{N}$, und sei $(w_1, \ldots, w_r)$ eine über A algebraisch unabhängige Folge von Elementen aus B. Dann gibt es für alle $i \in \{0, 1, \ldots, \min(r, m)\}$ eine injektive Abbildung $\pi : \{i+1, \ldots, m\} \to \{1, \ldots, m\}$, sodass B algebraisch über*

$$A[\![w_1, \ldots, w_i, x_{\pi(i+1)}, \ldots, x_{\pi(m)}]\!]$$

ist.

Beweis: Induktion nach i. Für $i = 0$ setzen wir $\pi := \mathrm{id}_{\{1,\ldots,m\}}$. Da $(x_1, \ldots, x_m)$ eine Transzendenzbasis von B über über A ist, gilt für jedes $e \in B$, dass
$(x_1, \ldots, x_m, e)$ algebraisch abhängig über A ist. Dann ist e nach Satz 8.22 algebraisch über $A[\![x_1, \ldots, x_m]\!]$.

Sei nun $i \geq 1$. Wir nehmen an, dass

$$B \text{ algebraisch über } A[\![w_1, \ldots, w_{i-1}, x_{\pi(i)}, \ldots, x_{\pi(m)}]\!] \tag{8.8}$$

ist. Wir wollen nun eines der $x_{\pi(j)}$ durch w_i ersetzen. Dazu wählen wir eine Menge $K = \{k_1, \ldots, k_l\}$ als eine Teilmenge von $\{i, i+1, \ldots, m\}$, die maximal bezüglich $\subseteq$ mit der Eigenschaft ist, dass

$$(w_1, \ldots, w_{i-1}, w_i, x_{\pi(k_1)}, \ldots, x_{\pi(k_l)}) \text{ algebraisch unabhängig}$$

ist; da $(w_1, \ldots, w_i)$ algebraisch unabhängig ist, gibt es ein solches K.

Falls $K = \{i, i+1, \ldots, m\}$, so ist

$$(w_1, \ldots, w_i, x_{\pi(i)}, \ldots, x_{\pi(m)})$$

algebraisch unabhängig. Wegen (8.8) ist w_i algebraisch über $A[\![w_1, \ldots, w_{i-1}, x_{\pi(i)}, \ldots, x_{\pi(m)}]\!]$. Nach Satz 8.22 ist dann $(w_1, \ldots, w_i, x_{\pi(i)}, \ldots, x_{\pi(m)})$ algebraisch abhängig über A.

Daher gibt es ein $j \in \{i, i+1, \ldots, m\}$, sodass $j \notin K$. Wegen der Maximalität von K gilt also

$$\begin{aligned}&(w_1, \ldots, w_i, x_{\pi(k_1)}, \ldots, x_{\pi(k_l)}) \text{ ist algebraisch unabhängig über } A, \text{ und}\\ &(w_1, \ldots, w_i, x_{\pi(k_1)}, \ldots, x_{\pi(k_l)}, x_{\pi(j)}) \text{ ist algebraisch abhängig über } A.\end{aligned}$$

Daher ist nach Satz 8.22 $x_{\pi(j)}$ algebraisch über $A[\![w_1, \ldots, w_i, x_{\pi(k_1)}, \ldots, x_{\pi(k_l)}]\!]$, folglich über $A[\![w_1, \ldots, w_i, x_{\pi(i)}, \ldots, x_{\pi(j-1)}, x_{\pi(j+1)}, \ldots, x_{\pi(m)}]\!]$. Wir definieren nun

$$\sigma : \{i, \ldots, m\} \to \{1, \ldots, m\}$$

durch $\sigma(j) := \pi(i)$, $\sigma(i) := \pi(j)$, und $\sigma(r) = \pi(r)$ für $r \in \{i, \ldots, m\} \setminus \{i, j\}$. Nun ist also $x_{\sigma(i)}$ algebraisch über

$$C := A[\![w_1, \ldots, w_i, x_{\sigma(i+1)}, \ldots, x_{\sigma(m)}]\!].$$

Wegen (8.8) ist B algebraisch über $A[\![w_1, \ldots, w_{i-1}, x_{\sigma(i+1)}, \ldots, x_{\sigma(m)}]\!][\![x_{\sigma(i)}]\!]$, und daher erst recht über $A[\![w_1, \ldots, w_{i-1}, w_i, x_{\sigma(i+1)}, \ldots, x_{\sigma(m)}]\!][\![x_{\sigma(i)}]\!] = C[\![x_{\sigma(i)}]\!]$. Da wegen Satz 8.17 der Integritätsbereich $C[\![x_{\sigma(i)}]\!]$ algebraisch über C ist, folgt nach Proposition 8.16, dass B algebraisch über C ist. Somit leistet $\sigma|_{\{i+1,\ldots,m\}}$ das Gewünschte. □

KOROLLAR 8.25. *Seien A, B Integritätsbereiche mit $A \leq B$, und sei $(x_1, \ldots, x_m)$ eine Transzendenzbasis von B über A. Sei $(w_1, \ldots, w_r)$ eine über A algebraisch unabhängige Folge von Elementen aus B. Dann gilt $r \leq m$.*

Beweis: Wir nehmen an $r > m$. Aus dem Austauschsatz (Satz 8.24) erhalten wir, dass B algebraisch über $A[\![w_1, \ldots, w_m]\!]$ ist. Also ist w_{m+1} algebraisch über $A[\![w_1, \ldots, w_m]\!]$. Nach Satz 8.22 ist $(w_1, \ldots, w_m, w_{m+1})$ dann algebraisch abhängig. □

DEFINITION 8.26. Seien A, B Integritätsbereiche mit $A \leq B$. Wenn B eine endliche Transzendenzbasis über A besitzt, so ist der *Transzendenzgrad* von B über A die Anzahl der Elemente dieser Basis. Andernfalls ist der Transzendenzgrad ∞.

4. Noethersche Normalisierung

LEMMA 8.27. *Sei k ein unendlicher Körper, $n \in \mathbb{N}$, und sei $p \in k[t_1, \ldots, t_n]$ mit $p \neq 0$. Dann gibt es ein $\boldsymbol{v} \in k^n$ mit $\overline{p}(\boldsymbol{v}) \neq 0$.*

Beweis: Wir verwenden Induktion nach n. Falls $n = 1$, ist p ein Polynom in einer Variablen, das nicht das Nullpolynom ist. Ein solches Polynom hat nur endlich viele Nullstellen; da k unendlich ist, bleibt also eine Nichtnullstelle übrig. Falls $n > 1$, so schreiben wir mit $l := \deg_{t_n}(p)$

$$p = \sum_{i=0}^{l} p_i(t_1, \ldots, t_{n-1}) t_n^i.$$

Nun hat p_l nach Induktionsvoraussetzung eine Nichtnullstelle $(v_1, \ldots, v_{n-1})$. Das Polynom

$$p' := \sum_{i=0}^{l} \overline{p_i}(v_1, \ldots, v_{n-1}) t^i$$

in $k[t]$ ist also nicht das Nullpolynom, da sein Koeffizient vom Grad l ungleich 0 ist. Ein univariates Polynom, das nicht das Nullpolynom ist, hat nur endlich viele Nullstellen; es bleibt vom unendlichen Körper k also eine Nichtnullstelle v_n übrig. Der Vektor $(v_1, \ldots, v_n)$ ist also dann eine Nichtnullstelle von p. □

LEMMA 8.28. *Sei k ein Körper, und sei B ein kommutativer Ring mit Eins mit $k \leq B$. Sei $n \in \mathbb{N}$, $\boldsymbol{x} = (x_1, \ldots, x_n)$ eine Folge von Elementen aus B, und sei $p \in k[t_1, \ldots, t_n]$ so, dass*

$$\overline{p}(x_1, \ldots, x_n) = 0$$

und $p \neq 0$. Dann gibt es Polynome $f_2, \ldots, f_n \in k[t_1, \ldots, t_n]$ und $g_1, \ldots, g_n \in k[t_1, \ldots, t_n]$, sodass folgendes gilt:

1. *x_1 ist ganz über $k[\![\overline{f_2}(\boldsymbol{x}), \ldots, \overline{f_n}(\boldsymbol{x})]\!]$,*
2. *Für alle $j \in \{1, \ldots, n\}$ gilt*

$$t_j = g_j(t_1, f_2(t_1, \ldots, t_n), \ldots, f_n(t_1, \ldots, t_n)).$$

(Das bedeutet, dass $k[\![\overline{f_2}(\boldsymbol{x}), \ldots, \overline{f_n}(\boldsymbol{x}), x_1]\!] = k[\![x_1, \ldots, x_n]\!]$.)

Wenn k unendlich ist, so kann man alle f_i linear wählen.

Beweis: Wir betrachten zunächst den Fall, dass k unendlich ist. Sei I eine endliche Teilmenge von ${\mathbb{N}_0}^n$, und sei $\langle c_i \mid i \in I \rangle : I \to k$ so, dass

$$p = \sum_{(i_1, \ldots, i_n) \in I} c(i_1, \ldots, i_n) t_1^{i_1} \cdots t_n^{i_n}.$$

Für ein passendes $(\alpha_2, \ldots, \alpha_n) \in k^{n-1}$ gilt nun, dass das Polynom

$$q(t_1, \ldots, t_n) := p(t_1, t_2 + \alpha_2 t_1, \ldots, t_n + \alpha_n t_1)$$

von der Form $b_N t_1^N + \sum_{i=0}^{N-1} b_i(t_2,\dots,t_n)t_1^i$ mit $b_N \in k$, $b_i \in k[t_2,\dots,t_n]$ ist. Um das zu zeigen, bilden wir ein Polynom q' in $k[t_1,\dots,t_n,a_2,\dots,a_n]$.

$$\begin{aligned} q' &:= p(t_1, t_2 + a_2t_1, \dots, t_n + a_nt_1) \\ &= \sum_{(i_1,\dots,i_n)\in I} c(i_1,\dots,i_n)t_1^{i_1}(t_2 + a_2t_1)^{i_2}\cdots(t_n + a_nt_1)^{i_n}. \end{aligned}$$

Sei N der totale Grad von p. Dann erhalten wir den Koeffizienten K von t_1^N in q' durch

$$K = \sum_{\substack{(i_1,\dots,i_n)\in I \\ i_1+\cdots+i_n=N}} c(i_1,\dots,i_n)a_2^{i_2}a_3^{i_3}\cdots a_n^{i_n}.$$

Das Polynom $K \in k[a_2,\dots,a_n]$ ist nicht das Nullpolynom, also gibt es nach Lemma 8.27 ein $(\alpha_2,\dots,\alpha_n) \in k^{n-1}$, sodass $\overline{K}(\alpha_2,\dots,\alpha_n) \neq 0$. Das Polynom $q := q'(t_1,\dots,t_n,\alpha_2,\dots,\alpha_n)$ ist also ein Polynom in $k[t_1,\dots,t_n]$, das von der Form $b_N t_1^N + \sum_{i=0}^{N-1} b_i(t_2,\dots,t_n)t_1^i$ ist.

Es gilt

$$\overline{q}(x_1, x_2 - \alpha_2x_1, \dots, x_n - \alpha_nx_1) = 0.$$

Das bedeutet

$$b_N x_1^N + \sum_{i=0}^{N-1} \overline{b_i}(x_2 - \alpha_2x_1,\dots,x_n - \alpha_nx_1)x_1^i = 0.$$

Also ist x_1 ganz über $k[\![x_2 - \alpha_2x_1,\dots,x_n - \alpha_nx_1]\!]$. Somit leisten $f_j := x_j - \alpha_jx_1$ und $g_1 := t_1$, $g_j := x_j + \alpha_jx_1$ das Gewünschte.

Wenn k endlich ist, so kann man $g_j := t_j + t_1^{d^{j-1}}$ mit $d > \max\{i_j \mid i \in I, j \in \{1,\dots,n\}\}$ und $f_j := t_j - t_1^{d^{j-1}}$ wählen. □

Satz 8.29 (Noethersche Normalisierung). *Sei k ein Körper, sei B ein kommutativer Ring mit Eins mit $k \leq B$, und seien $x_1,\dots,x_n \in B$ so, dass $k[\![x_1,\dots,x_n]\!] = B$. Dann gibt es $r \in \{0,\dots,n\}$ und $f_1,\dots,f_n \in k[t_1,\dots,t_n]$, sodass für $y_j := \overline{f_j}(x_1,\dots,x_n)$ gilt:*

(1) *$(y_1,\dots,y_r)$ ist algebraisch unabhängig über k,*
(2) *B ist ganz über $k[\![y_1,\dots,y_r]\!]$.*

Beweis: Induktion nach n. Wenn $(x_1,\dots,x_n)$ algebraisch unabhängig ist, so gilt für $r := n$ und $f_j := t_j$ ($j \in \{1,\dots,n\}$) das Gewünschte.

Wenn $\boldsymbol{x} = (x_1,\dots,x_n)$ algebraisch abhängig ist, so gibt es ein $p \in k[t_1,\dots,t_n]$ mit $p \neq 0$, sodass

$$\overline{p}(x_1,\dots,x_n) = 0.$$

Daher gibt es nach Lemma 8.28 $f_1,\dots,f_{n-1} \in k[t_1,\dots,t_n]$, sodass x_n ganz über $k[\![\overline{f_1}(x_1,\dots,x_n),\dots,\overline{f_{n-1}}(x_1,\dots,x_n)]\!]$ ist, und

$$k[\![\overline{f_1}(\boldsymbol{x}),\dots,\overline{f_{n-1}}(\boldsymbol{x}),x_n]\!] = B.$$

Nach Induktionsvoraussetzung gibt es nun $g_1, \dots, g_r \in k[t_1, \dots, t_{n-1}]$, sodass $k[\![\overline{f_1}(\boldsymbol{x}), \dots, \overline{f_{n-1}}(\boldsymbol{x})]\!]$ ganz über

$$k[\![\overline{g_1}\big(\overline{f_1}(\boldsymbol{x}), \dots, \overline{f_{n-1}}(\boldsymbol{x})\big), \dots, \overline{g_r}\big(\overline{f_1}(\boldsymbol{x}), \dots, \overline{f_{n-1}}(\boldsymbol{x})\big)]\!]$$

ist

Für $h_j := g_j(f_1, \dots, f_{n-1}) \in k[t_1, \dots, t_n]$ gilt also:

$$k[\![\overline{f_1}(\boldsymbol{x}), \dots, \overline{f_{n-1}}(\boldsymbol{x})]\!] \text{ ist ganz über } k[\![\overline{h_1}(\boldsymbol{x}), \dots, \overline{h_r}(\boldsymbol{x})]\!].$$

Da x_n ganz über

$$k[\![\overline{f_1}(\boldsymbol{x}), \dots, \overline{f_{n-1}}(\boldsymbol{x})]\!]$$

ist, gilt:

$$k[\![\overline{f_1}(\boldsymbol{x}), \dots, \overline{f_{n-1}}(\boldsymbol{x})]\!][\![x_n]\!] \text{ ist ganz über } k[\![\overline{h_1}(\boldsymbol{x}), \dots, \overline{h_r}(\boldsymbol{x})]\!].$$

Folglich ist B ganz über $k[\![\overline{h_1}(\boldsymbol{x}), \dots, \overline{h_r}(\boldsymbol{x})]\!]$. □

Übungsaufgaben 8.30

(1) Finden Sie eine Noethersche Normalisierung von $R = \mathbb{Q}[x, y, z]/I$ über $\mathbb{Q}$, wobei $I = \langle x^5 + xyz + 1\rangle$. Finden Sie also $r \in \mathbb{N}_0$ und $y_1, \dots, y_r \in R$, sodass $(y_1, \dots, y_r)$ algebraisch unabhängig ist und R ganz über $\mathbb{Q}[\![y_1, \dots, y_r]\!]$ ist.
(2) Finden Sie eine Noethersche Normalisierung von $R = \mathbb{Q}[x, y, z]/I$ über $\mathbb{Q}$, wobei $I = \langle xyz + 1\rangle$. *Hinweis:* Zeigen Sie, dass R ganz über $\mathbb{Q}[\![(y - x) + I, (z - x) + I]\!]$ ist. Um zu zeigen, dass $\big((y - x) + I, (x - z) + I\big)$ algebraisch unabhängig ist, verwenden Sie, dass $(x + I, y + I)$ eine Transzendenzbasis von R über $\mathbb{Q}$ ist.

5. Der Hilbertsche Nullstellensatz

Satz 8.31 (Hilberts Nullstellensatz – Schwache Form). *Sei k ein Körper, und sei I ein Ideal von $k[t_1, \dots, t_n]$ mit $1 \notin I$. Dann gibt es eine algebraische Körpererweiterung K von k und $\boldsymbol{x} \in K^n$, sodass für alle $f \in I$ gilt: $\overline{f}(\boldsymbol{x}) = 0$.*

Beweis: Sei M ein maximales Ideal von $k[t_1, \dots, t_n]$ mit $I \subseteq M \neq k[\boldsymbol{t}]$, und sei $K := k[\boldsymbol{t}]/M$. K ist ein Körper, und $(x_1, \dots, x_n) := (t_1 + M, \dots, t_n + M)$ ist eine Nullstelle aller Polynome in I. Es bleibt zu zeigen, dass K algebraisch über k ist: Seien dazu $r \in \{0, \dots, n\}$ und $y_1, \dots, y_r \in K$ so, dass K ganz über $k[\![y_1, \dots, y_r]\!]$ ist, und $(y_1, \dots, y_r)$ algebraisch unabhängig ist. Wenn $r = 0$, so ist K ganz über k, also algebraisch. Wenn $r \geq 1$, so gilt wegen der Unabhängigkeit der y_i, dass $y_1 \neq 0 + M$. Also gibt es ein $z_1 \in K$ mit $z_1 \cdot y_1 = 1 + M$. Da z_1 ganz über $k[\![y_1, \dots, y_r]\!]$ ist, gibt es $m \in \mathbb{N}$ und $f_1, \dots, f_{m-1} \in k[t_1, \dots, t_r]$, sodass

$$z_1^m + \sum_{i=0}^{m-1} \overline{f_i}(y_1, \dots, y_r) z_1^i = 0 + M.$$

Durch Multiplikation mit y_1^m erhalten wir

$$1 + \sum_{i=0}^{m-1} \overline{f_i}(y_1, \dots, y_r) y_1^{m-i} = 0 + M.$$

Das Polynom $g \in k[t_1, \ldots, t_r]$, das durch

$$g := 1 + \sum_{i=0}^{m-1} f_i(t_1, \ldots, t_r) t_1^{m-i}$$

gegeben ist, erfüllt $g \neq 0$ und $\overline{g}(y_1, \ldots, y_r) = 0$. Dann ist $(y_1, \ldots, y_r)$ algebraisch abhängig. □

Satz 8.32 (Grundlage des automatischen Beweisens geometrischer Sätze). *Sei k ein algebraisch abgeschlossener Körper, seien $n \in \mathbb{N}$, $r, s \in \mathbb{N}_0$,*
$f_1, \ldots, f_s, h_1, \ldots, h_r, g \in k[t_1, \ldots, t_n]$. Dann sind äquivalent:

(1) *Für alle $\boldsymbol{x} \in k^n$ gilt:*

$$\big(f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0,\ h_1(\boldsymbol{x}) \neq 0, \ldots, h_r(\boldsymbol{x}) \neq 0\big) \Longrightarrow g(\boldsymbol{x}) = 0.$$

(2) *1 liegt in dem von*

$$(f_1, \ldots, f_s, h_1 \cdot u_1 - 1, \ldots, h_r \cdot u_r - 1, g \cdot v - 1)$$

erzeugten Ideal von $k[t_1, \ldots, t_n, u_1, \ldots, u_r, v]$.

Beweis: (1)⇒(2): Wenn 1 nicht in dem Ideal liegt, so haben die Polynome nach Satz 8.31 eine Nullstelle $(\boldsymbol{x}, \boldsymbol{y}, z)$ in k^{n+r+1}. Es gilt dann $f_1(\boldsymbol{x}) = \ldots = f_s(\boldsymbol{x}) = 0, h_1(\boldsymbol{x}) \neq 0, \ldots, h_r(\boldsymbol{x}) \neq 0, g(\boldsymbol{x}) \neq 0$, im Widerspruch zu (1). (2)⇒(1): Wenn $\boldsymbol{x} \in k^n$ so ist, dass $f_1(\boldsymbol{x}) = \ldots = f_s(\boldsymbol{x}) = 0$, $h_1(\boldsymbol{x}) \neq 0, \ldots, h_r(\boldsymbol{x}) \neq 0$, und $g(\boldsymbol{x}) \neq 0$, so hat jedes Polynom in der Erzeugermenge des Ideals die Nullstelle $(x_1, \ldots, x_n, y_1, \ldots, y_r, z)$, wobei $y_i := \frac{1}{h_i(\boldsymbol{x})}$ und $z := \frac{1}{g(\boldsymbol{x})}$. Somit hat auch 1 diese Nullstelle, ein Widerspruch. □

Satz 8.33 (Rabinowitschs Trick). *Sei k ein Körper, $s, n \in \mathbb{N}$, und seien $f_1, \ldots, f_s \in k[t_1, \ldots, t_n]$. Dann sind äquivalent:*

(1) $g \in \sqrt{\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{t}]}}$.
(2) $1 \in \langle f_1, \ldots, f_s, g \cdot u - 1 \rangle_{k[\boldsymbol{t}, u]}$.

Beweis: (1)⇒(2). Sei $I := \langle f_1, \ldots, f_s, g \cdot u - 1 \rangle_{k[\boldsymbol{t}, u]}$. Wegen (1) gibt es ein $r \in \mathbb{N}$, sodass $g^r \in I$. Folglich gilt auch $g^r \cdot u^r \in I$. Da $g \cdot u \equiv 1 \pmod{I}$, gilt auch $(g \cdot u)^r \equiv 1^r \pmod{I}$, und somit $1 \in I$. (2)⇒(1) Wenn $g = 0$, so liegt g klarerweise im Radikal. Wenn $g \neq 0$, so gibt es Polynome $a_1, \ldots, a_s, b \in k[\boldsymbol{t}, u]$, sodass

$$\sum_{i=1}^{s} a_i(t_1, \ldots, t_n, u) f_i(t_1, \ldots, t_n) + b(t_1, \ldots, t_n, u)(g(t_1, \ldots, t_n) \cdot u - 1) = 1.$$

Wir werten jetzt beide Seiten im rationalen Funktionenkörper $Q(k[x_1, \ldots, x_n])$ an der Stelle $(x_1, \ldots, x_n, \frac{1}{g(x_1, \ldots, x_n)})$ aus, und erhalten

$$\sum_{i=1}^{s} a_i\big(x_1, \ldots, x_n, 1/g(x_1, \ldots, x_n)\big) f_i(x_1, \ldots, x_n) = 1.$$

Es gibt nun $r \in \mathbb{N}$ und $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$, sodass

$$a_i(x_1, \ldots, x_n, 1/g(x_1, \ldots, x_n)) = \frac{h_i(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)^r}.$$

Dann liegt g^r in dem von $(f_1, \ldots, f_s)$ erzeugten Ideal von $k[t_1, \ldots, t_n]$.

SATZ 8.34 (Hilberts Nullstellensatz – Starke Form). *Sei k ein algebraisch abgeschlossener Körper, sei $n \in \mathbb{N}$, und seien $f_1, \ldots, f_s \in k[t_1, \ldots, t_n]$. Wenn für alle $\boldsymbol{x} \in k^n$ mit $\overline{f_1}(\boldsymbol{x}) = \cdots = \overline{f_s}(\boldsymbol{x}) = 0$ gilt, dass $g(\boldsymbol{x}) = 0$, so liegt g im Radikal von $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{t}]}$.*

Beweis: Sei u eine neue Variable. $f_1 = \ldots = f_s = 0$, $g \cdot u = 1$ ist unlösbar, also gilt wegen der schwachen Form des Nullstellensatzes $1 \in \langle f_1, \ldots, f_s, g \cdot u - 1 \rangle_{k[\boldsymbol{t},u]}$. Also liegt nach dem Satz von Rabinowitsch (Satz 8.33) g im Radikal von $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{t}]}$. □

6. Ein Satz über injektive und surjektive polynomiale Abbildungen

Wir beweisen in dieser Sektion den folgenden erstaunlichen Satz.

SATZ 8.35 (Satz von Ax und Grothendieck [**Ax68**]). *Sei k ein algebraisch abgeschlossener Körper, $n \in N$, $f_1, \ldots, f_n \in k[t_1, \ldots, t_n]$ so, dass die Abbildung $F : k^n \to k^n, (x_1, \ldots, x_n) \mapsto (f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \ldots, f_n(\boldsymbol{x}))$ injektiv ist. Dann ist F auch surjektiv.*

Wir brauchen für diesen Satz einige einfache Lemmata.

LEMMA 8.36. *Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $x \in B$ algebraisch über A. Dann gibt es $a \in A \setminus \{0\}$, sodass ax ganz über A ist.*

Beweis: Sei $p = \sum_{i=0}^{n} a_i \, t^i$ so, dass $a_n \neq 0$ und $p(x) = 0$. Dann gilt

$$\begin{aligned} 0 &= a_n^{n-1} \cdot \sum_{i=0}^{n} a_i x^i \\ &= a_n^n x^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i} a_n^i x^i. \end{aligned}$$

Folglich gilt für $q := t^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i} t^i$, dass $q(a_n x) = 0$. □

LEMMA 8.37. *Sei D ein faktorieller Integritätsbereich, sei $Q(D)$ sein Quotientenkörper, und sei $x \in Q(D)$ ganz über D. Dann gilt $x \in D$.*

Beweis: Sei $x = \frac{y}{z}$ mit $y, z \in D$ so, dass y, z keinen primen Teiler gemeinsam haben. Wenn z in D invertierbar ist, so gilt $x = y \cdot i(z) \in D$. Wenn z in D nicht invertierbar ist, gibt es ein primes $p \in D$ mit $p \mid z$. Es gilt dann $p \nmid y$. Seien $a_{n-1}, \ldots, a_o \in D$ so, dass $(\frac{y}{z})^n + \sum_{i=0}^{n-1} a_i (\frac{y}{z})^i = 0$. Dann gilt $y^n = -\sum_{i=0}^{n-1} y^i z^{n-i}$, und somit $z \mid y^n$ und somit $p \mid y^n$. Da p prim ist, gilt $p \mid y$. Widerspruch. □

LEMMA 8.38. *Seien A, B kommutative Ringe mit Eins mit $A \leq B$, sei B ganz über A, und seien $b_1, \ldots, b_n \in B$ so, dass $B = A[\![b_1, \ldots, b_n]\!]$. Sei I ein Ideal von A. Wir nehmen an, dass $\langle I \rangle_B = B$. Dann gilt $I = A$.*

Beweisskizze: Durch wiederholte Anwendung von Satz 8.7 erhalten wir $m \in \mathbb{N}$ und $x_1, \ldots, x_m \in B$, sodass $x_1 = 1$ und $B = \sum_{i=1}^{m} A \cdot x_i$.

Wir zeigen nun, dass es für jedes $y \in B$ Elemente $i_1, \dots, i_m \in I$ gibt, sodass

$$y = \sum_{l=1}^{m} i_l x_l. \tag{8.9}$$

Wegen $y \in \langle I \rangle_B$ gibt es $r \in \mathbb{N}$, $b_1, \dots, b_r \in B$ und $j_1, \dots, j_r \in I$, sodass $y = \sum_{k=1}^{r} b_k j_k$. Da $b_k \in \sum_{l=1}^{m} A \cdot x_l$, gibt es $a_{k,1}, \dots, a_{k,m} \in A$, sodass $y = \sum_{k=1}^{r} (\sum_{l=1}^{m} a_{k,l} x_l)\, j_k = \sum_{l=1}^{m} (\sum_{k=1}^{r} a_{k,l} j_k) x_l$. Wir setzen nun $i_l := \sum_{k=1}^{r} a_{k,l} j_k$, und erhalten so die Darstellung in (8.9).

Aus dieser Darstellung für $y \in \{x_1, \dots, x_m\}$ erhalten wir eine Matrix $T \in I^{m \times m}$, sodass

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = T \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Da $x_1 = 1$, erhalten wir $\det(E_m - T) = 0$. Wenn wir diese Gleichung im Faktorring A/I betrachten, so gilt $1 \equiv 0 \pmod{I}$. Also gilt $1 \in I$. □

LEMMA 8.39. *Sei k ein endlicher Körper, und sei B ein kommutativer Ring mit Eins mit $k \leq B$. Wir nehmen an, dass es $n \in \mathbb{N}_0$ und $x_1, \dots, x_n \in B$ gibt mit $B = k[\![x_1, \dots, x_n]\!]$. Dann hat B ein Ideal J mit $J \neq B$, sodass B/J nur endlich viele Elemente hat.*

Beweis: Nach Satz 8.29 gibt es $r \in \mathbb{N}_0$ und $y_1, \dots, y_r \in B$, sodass $(y_1, \dots, y_r)$ algebraisch unabhängig über k sind, und B ganz über $k[\![y_1, \dots, y_r]\!]$ ist. Da $k[\![y_1, \dots, y_r]\!]$ isomorph zum Polynomring $k[t_1, \dots, t_r]$ ist, gilt für das von $\{y_1, \dots, y_r\}$ erzeugte Ideal I von $k[\![y_1, \dots, y_r]\!]$, dass $1 \notin I$. Nach Lemma 8.38 (für $A := k[\![y_1, \dots, y_r]\!]$) gilt daher auch für das von $\{y_1, \dots, y_r\}$ erzeugte Ideal J von B, dass $1 \notin J$. Da $1 \notin J$, gilt $k \cap J = \{0\}$. Folglich ist $k' := \{\alpha + J \mid \alpha \in k\}$ zu ein zu k isomorpher Unterring von B/J. Wir wissen, dass für jedes $i \in \{1, \dots, n\}$ das Element x_i ganz über $k[\![y_1, \dots, y_r]\!]$ sind. Folglich ist jedes $x_i + J$ ganz über $k[\![y_1, \dots, y_r]\!]/J = k'$. Wegen $B = k[\![x_1, \dots, x_n]\!]$ gilt auch $B/J = k'[\![x_1 + J, \dots, x_n + J]\!]$. Sei d_i der Grad eines Polynoms p_i in $k'[t]$ mit führendem Koeffizienten 1 und $p_i(x_i + J) = 0$. Daher lässt sich jedes Element von B/J in der Form $\sum_{i_1 < d_1, \dots, i_n < d_n} \alpha_{i_1,\dots,i_n} (x_1 + J)^{i_1} \cdots (x_n + J)^{i_n}$ mit allen $\alpha_{i_1,\dots,i_n} \in k'$ schreiben. Somit hat B/J nur endlich viele Elemente. □

LEMMA 8.40. *Sei B ein Integritätsbereich mit $\mathbb{Z} \leq B$, und seien $x_1, \dots, x_n \in B$ so, dass $B = \mathbb{Z}[\![x_1, \dots, x_n]\!]$. Dann hat B ein Ideal J mit $J \neq B$, sodass B/J nur endlich viele Elemente hat.*

Beweis: Sei $Y =: (y_1, \dots, y_r)$ eine maximale Teilfolge von $(x_1, \dots, x_n)$ mit der Eigenschaft, dass Y algebraisch unabhängig über $\mathbb{Z}$ ist. Dann ist nach Satz 8.22 jedes x_i algebraisch über $\mathbb{Z}[\![Y]\!]$. Also gibt es wegen Lemma 8.36 $q_1, \dots, q_n \in \mathbb{Z}[\![Y]\!] \setminus \{0\}$, sodass jedes $q_i x_i$ ganz über $\mathbb{Z}[\![Y]\!]$ ist. Sei $q := q_1 q_2 \cdots q_n$. In $Q(B)$ gilt $B = \mathbb{Z}[\![x_1, \dots, x_n]\!] \leq \mathbb{Z}[\![Y]\!][\![q_1 x_1, \dots, q_n x_n]\!][\![\frac{1}{q}]\!]$.

Da $q \in \mathbb{Z}[\![Y]\!]$ und da Y algebraisch unabhängig über $\mathbb{Z}$ ist, gibt es genau ein $q' \in \mathbb{Z}[t_1, \dots, t_r]$ mit $q = q'(y_1, \dots, y_r)$. Sei p eine Primzahl, die zumindest einen Koeffizienten von q' nicht teilt. Wir zeigen nun, dass p in B nicht invertierbar ist. Nehmen wir an, dass es $i(p) \in B$ gibt, sodass $i(p) \cdot p = 1$. Dann gilt $i(p) \in F[\![\frac{1}{q}]\!]$ mit $F := \mathbb{Z}[\![Y]\!][\![q_1 x_1, \dots, q_n x_n]\!]$. Somit gibt es $m \in \mathbb{N}$ und

$f_0, \ldots, f_m \in F$, sodass

$$i(p) = \sum_{i=0}^{m} f_i(\frac{1}{q})^i,$$

und somit $q^m \cdot i(p) = \sum_{i=0}^{m} f_i q^{m-i} \in F$. Wir betrachten nun das Element $\frac{q^m}{p} \in Q(B)$. Wegen $q^m i(p)p = q^m$, gilt $q^m \cdot i(p) = \frac{q^m}{p}$. Nun gilt $q \in \mathbb{Z}[\![Y]\!]$ und $p \in \mathbb{Z}[\![Y]\!]$. Also gilt $\frac{q^m}{p} \in Q(\mathbb{Z}[\![Y]\!])$. Da F ganz über $\mathbb{Z}[\![Y]\!]$ ist, ist $\frac{q^m}{p}$ ganz über $\mathbb{Z}[\![Y]\!]$. Da $\mathbb{Z}[\![Y]\!]$ isomorph zu $\mathbb{Z}[t_1, \ldots, t_r]$ und somit faktoriell ist, gilt wegen Lemma 8.37 auch $\frac{q^m}{p} \in \mathbb{Z}[\![Y]\!]$. Daher teilt p alle Koeffizienten von $(q')^m$. Folglich teilt p auch alle Koeffizienten von q', im Widerspruch zur Wahl von p. Somit ist p in B nicht invertierbar.

Sei I das von p erzeugte Ideal von B. Dann gilt $I \cap \mathbb{Z} = p \cdot \mathbb{Z}$. Sei $k' := \{z + I \mid z \in \mathbb{Z}\}$. Dann ist k' ein Körper mit p Elementen, und es gilt $B/I = k'[\![x_1 + I, \ldots, x_n + I]\!]$. Wegen Lemma 8.39 hat B/I ein Ideal K, sodass $(B/I)/K$ endlich ist. Sei $J := \bigcup_{(b+I)\in K} b + I$. Dann ist B/J isomorph zu $(B/I)/K$, und somit endlich. □

KOROLLAR 8.41.

(1) *Sei R ein endlich erzeugter kommutativer Ring mit Eins. Dann hat R ein Ideal J mit $1 \notin J$, sodass R/J ein endlicher Ring ist.*
(2) *Ein Körper K, der als Ring endlich erzeugt ist, ist endlich.*

Beweis: Wir beweisen zunächst (2). Der von 1 erzeugte Unterring von K ist ein Integritätsbereich, also isomorph zu $\mathbb{Z}_p$ mit p Primzahl, oder zu $\mathbb{Z}$. Nun ergibt Lemma 8.39 oder Lemma 8.40, dass K ein Ideal J mit $J \neq K$ besitzt, modulo dem K endlich ist. Als Körper besitzt K nur die Ideale 0 und K, also gilt $J = 0$ und K ist endlich. Für (1) wählen wir ein maximales Ideal M von R. Dann ist $K := R/M$ ein durch endlich viele Elemente erzeugter Körper, also nach (2) endlich. □

Beweis von Satz 8.35: Wir nehmen an, dass F injektiv und nicht surjektiv ist. Da F injektiv ist, gibt es nach dem Nullstellensatz für jedes $i \in \{1, \ldots, n\}$ ein $m_i \in \mathbb{N}$ und Polynome $p_1, \ldots, p_n \in k[x_1, \ldots, x_n, y_1, \ldots, y_n] = k[\boldsymbol{x}, \boldsymbol{y}]$, sodass

$$(x_i - y_i)^{m_i} = \sum_{j=1}^{n} p_j(\boldsymbol{x}, \boldsymbol{y}) \cdot (f_j(\boldsymbol{x}) - f_j(\boldsymbol{y})). \tag{8.10}$$

Da F nicht surjektiv ist, gibt es ein $(a_1, \ldots, a_n)$, das nicht im Bildbereich von F liegt. Folglich gibt es wegen des Nullstellensatzes $q_1, \ldots, q_n \in k[t_1, \ldots, t_n]$, sodass

$$1 = \sum_{j=1}^{n} q_j(\boldsymbol{t}) \cdot (f_j(t_1, \ldots, t_n) - a_j). \tag{8.11}$$

Sei nun B der von 1 und den Koeffizienten von p_j, f_j, q_j ($j \in \{1, \ldots, n\}$) und $a_1, \ldots, a_n$ erzeugte Unterring von k. Nach Korollar 8.41 hat B ein Ideal $J \neq B$, sodass B/J ein endlicher Körper ist. Wir betrachten nun die Abbildung

$$F_1 : (B/J)^n \mapsto (B/J)^n, (z_1, \ldots, z_n) \mapsto (f_1(\boldsymbol{z}), \ldots, f_n(\boldsymbol{z})).$$

Wegen (8.11) gibt es kein $\boldsymbol{z} \in (B/J)^n$, sodass $F_1(\boldsymbol{z}) = (a_1 + J, \ldots, a_n + J)$. Wegen (8.10) ist die Abbildung F_1 injektiv. Die Abbildung F_1 ist also injektiv und nicht surjektiv, im Widerspruch zur Endlichkeit von B/J. Somit kann es keine injektive und nicht surjektive Abbildung F geben; jede injektive Abbildung $F : k^n \to k^n$ ist also surjektiv. □

7. Unterkörper des Körpers univariater rationaler Funktionen

LEMMA 8.42. *Sei K ein Körper, und seien $p, q \in K[t]$ mit $\mathrm{ggT}_{K[t]}(p, q) = 1$. Sei $K\left(\frac{p}{q}\right)$ der von $\frac{p}{q}$ erzeugte Unterkörper von $K(t)$. Sei $m := \deg(p), n := \deg(q)$. Wenn $\max(m, n) \geq 1$, so ist $K(t)$ algebraisch über $K\left(\frac{p}{q}\right)$, und es gilt $[K(t) : K(\frac{p}{q})] = \max(m, n)$.*

Beweis: Wir definieren ein Polynom $f \in K(t)[x]$ durch $f(x) := q(x) \cdot \frac{p(t)}{q(t)} - p(x)$. Es gilt $f \in K\left(\frac{p}{q}\right)[x]$ und $f(t) = 0$. Wenn $m > n$, so ist der führende Koeffizient von f gleich $-p_m$, wenn $m < n$, so ist der führende Koeffizient von f gleich $-q_n \frac{p}{q}$. In jedem dieser beiden Fälle ist der Grad von f gleich $\max(m, n)$. Wenn $m = n$, so gilt für den Koeffizienten f_n von x^n in f, dass $f_n = p_n - \frac{p}{q} q_n$. Wenn $f_n = 0$, so gilt $\frac{p_n}{q_n} = \frac{p}{q}$. Dann gilt wegen $\mathrm{ggT}_{K[t]}(p, q) = 1$, dass $\deg p = \deg q = 0$, im Widerspruch zu $\max(m, n) \geq 1$. Insgesamt gilt also $\deg(f) = \max(m, n)$.

Wir zeigen nun, dass f ein irreduzibles Polynom in $K\left(\frac{p}{q}\right)[x]$ ist. Der Körper $K\left(\frac{p}{q}\right)$ ist isomorph zum Körper $K(s)$. Es reicht also zu zeigen, dass $\bar{f} = q(x)s - p(x)$ irreduzibel über $K(s)$ ist. Sei dazu a ein Teiler von $\bar{f}$ in $K(s)[x]$ mit $\deg_x(a) \geq 1$. Wir nehmen an, dass a ein primitives Element des Rings $K[s]\,[x]$ ist. Da $a \mid \bar{f}$ in $K(s)[x]$, gilt wegen Satz 4.14 auch $a \mid \bar{f}$ in $K[s][x]$. Folglich gilt $\deg_s(a) \in \{0, 1\}$. Wenn $\deg_s(a) = 0$, so gilt $a|q$ und $a|p$ in $K[x]$, also $\deg_x(a) = 0$, im Widerspruch zu $\deg(a) \geq 1$. Wenn $\deg_s(a) = 1$, so schreiben wir $a = a_1(x)s + a_2(x)$. Es gibt dann $b \in K[x]$ mit $a \cdot b = \bar{f}$. Dann gilt $b|p$ und $b|q$, folglich ist b konstant, und somit $\deg_x(a) = \deg_x(\bar{f})$. Damit hat $\bar{f}$ in $K(s)[x]$ keine Teiler, deren Grad verschieden von 0 und von $\deg_x(\bar{f})$ ist, und ist somit irreduzibel über $K(s)$. □

SATZ 8.43 (Satz von Lüroth). *Sei K ein Körper, und sei L ein Unterkörper des Körpers $K(t)$ mit $L \neq K$. Dann ist L isomorph zu $K(t)$.*

Beweisidee: Siehe [**Gar86**, p. 145]. Wir geben hier so viel vom Beweis an, wie für die algorithmische Bestimmung eines $u \in K(t)$ mit $K(u) = L$ nötig ist. Sei $s \in L \setminus K$. Dann gibt es Polynome $p, q \in K[t] \setminus \{0\}$, sodass $s = \frac{p(t)}{q(t)}$, und $\mathrm{ggT}_{K[t]}(p, q) = 1$. Da $s \notin K$, ist t algebraisch über $K(s)$, und folglich auch über L.

Sei nun $m \in L[x]$ das Minimalpolynom von t über L, und sei n sein Grad. Wegen $m \in L[x] \subseteq K(t)[x]$ gibt es $p_0, \ldots, p_{n-1}, q_0, \ldots, q_{n-1} \in K[t]$, sodass alle $\frac{p_i}{q_i}$ in L liegen, und

$$m = x^m + \sum_{i=0}^{n-1} \frac{p_i(t)}{q_i(t)} x^i.$$

Durch Multiplikation mit $q_0(t) \cdot q_{n-1}(t)$ und Herausziehen des größten gemeinsamen Teilers der Koeffizienten erhalten wir $\beta \in K(t) \setminus \{0\}$ und $a_0, \ldots, a_n \in K[t]$ mit $\beta\, m = f$ und

$$f = \sum_{i=0}^{n} a_i(t)\, x^i,$$

sodass f ein primitives Polynom in $K[t][x]$ ist. Wegen $\beta = a_n$ gilt $a_n \frac{p_i}{q_i} = a_i$, und somit $\frac{a_i}{a_n} \in L$ für alle $i \in \{1, \ldots, n-1\}$. Zumindest ein $\frac{a_i}{a_n}$ liegt nicht in K: denn wären alle $\frac{a_i}{a_n}$ Elemente von K, so läge das Minimalpolynom m von t über L in $K[x]$, und t wäre algebraisch über K. Wir wählen nun i so, dass $\frac{a_i}{a_n} \notin K$, setzen $u := \frac{a_i}{a_n}$. Man kann dann zeigen, dass $K(u) = L$.

Teil 2

Algorithmische Methoden

KAPITEL 9

Resultants

Resultants reduce some problems on polynomials to linear algebra. Let R be a commutative ring with unit, let $m \in \mathbb{N}$, and let $R_{<m}[x]$ be the R-module of univariate polynomials over R of degree less then m. Let $f, g \in R[x]$ with $\deg(f) \leq m$, $\deg(g) \leq n$. We define a mapping

$$\Phi : R_{<n}[x] \times R_{<m}[x] \to R_{<n+m}[x]$$

by $\Phi(v, w) = fv + gw$. Let

$$\begin{aligned} B &:= ((x^{n-1}, 0), \ldots, (x^0, 0), (0, x^{m-1}), \ldots, (0, x^0)), \\ C &:= (x^{m+n-1}, \ldots, x^0). \end{aligned}$$

For $(v, w) \in R_{<n}[x] \times R_{<m}[x]$, let $(v, w)_B$ be the coordinates of (v, w) with respect to B, and for $u \in R_{<n+m}[x]$ let $(u)_C$ be the coordinates of u with respect to C. The *Sylvester matrix* is the transpose of the representation matrix of Φ with respect to B and C, and hence defined by the identity

$$(\mathrm{Syl}^{[m,n]}(f, g))^T \cdot (v, w)_B = (fv + gw)_C.$$

The *resultant* of f and g is defined by $\mathrm{res}^{[m,n]}(f, g) := \det(\mathrm{Syl}^{[m,n]}(f, g))$.

As an example, let $f := x^4 - 11x^3 + 42x^2 - 64x + 32$, $g = x^2 - 8x + 15$. Let $m = 4, n = 2$. Then

$$\mathrm{Syl}^{[4,2]}(f, g) = \begin{pmatrix} 1 & -11 & 42 & -64 & 32 & 0 \\ 0 & 1 & -11 & 42 & -64 & 32 \\ 1 & -8 & 15 & 0 & 0 & 0 \\ 0 & 1 & -8 & 15 & 0 & 0 \\ 0 & 0 & 1 & -8 & 15 & 0 \\ 0 & 0 & 0 & 1 & -8 & 15 \end{pmatrix}.$$

For $f = f_0 x^m + \cdots + f_m x^0$ and $g = g_0 x^n + \cdots + g_n x^0$, the Sylvester matrix is an $(n+m) \times (n+m)$-matrix of the following form:

$$\mathrm{Syl}^{[m,n]}(f, g) = \begin{pmatrix} f_0 & \cdots & \cdots & \cdots & f_m & & \\ & \ddots & & & & \ddots & \\ & & f_0 & \cdots & \cdots & \cdots & f_m \\ g_0 & \cdots & \cdots & g_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & g_0 & \cdots & \cdots & g_n \end{pmatrix}.$$

THEOREM 9.1. *Let R be a commutative ring, let $m, n \in \mathbb{N}$, and let $f, g \in R[x]$ with $\deg(f) \leq m$, $\deg(g) \leq n$. Then $\mathrm{res}^{[m,n]}(f, g)x^0$ lies in the ideal of $R[x]$ generated by f and g.*

Proof: Let $S := \mathrm{Syl}^{[m,n]}(f,g)$. Since $S^{\mathrm{ad}}S = \mathrm{res}^{[m,n]}(f,g)\,\boldsymbol{I}_{n+m}$, we have $S^T \cdot y = (0,\ldots,0,\mathrm{res}^{[m,n]}(f,g))^T$, where y is the last row of S^{ad}. Let v,w be polynomials in $R[x]$ with $(v,w)_B = y$. Then $(0,\ldots,0,\mathrm{res}^{[m,n]}(f,g))^T = S^T y = (fv+gw)_C$, and therefore $fv+gw = \mathrm{res}^{[m,n]}(f,g)x^0$. □

THEOREM 9.2. *Let k be a field, let $m,n \in \mathbb{N}$, and let $f = \sum_{i=0}^{m} f_{m-i}x^i$ and $g = \sum_{i=0}^{n} g_{n-i}x^i$ be polynomials in $k[x]$ with $f_0 \neq 0$ or $g_0 \neq 0$. Then f,g have a common divisor $d \in k[x]$ of positive degree if and only if $\mathrm{res}^{[m,n]}(f,g) = 0$.*

PROOF. If d is a divisor of positive degree, then $f(g/d) - g(f/d) = 0$ and $\deg(f/d) < m$, $\deg(g/d) < n$. Hence $\mathrm{Syl}^{[m,n]}(f,g)^T(g/d,-f/d)_B = 0$. Thus the rows of $\mathrm{Syl}^{[m,n]}(f,g)$ are linearly dependent, and hence the determinant of this matrix is 0.

For the "if" direction, we assume $\det(\mathrm{Syl}^{[m,n]}(f,g)) = 0$. Then the rows of $\mathrm{Syl}^{[m,n]}(f,g)$ are linearly dependent, and therefore there is $y \in k^{n+m}$ with $y \neq 0$ and $\mathrm{Syl}^{[m,n]}(f,g)^T \cdot y = 0$. Let $a \in k_{<n}[x]$, $b \in k_{<m}[x]$ with $(a,b)_B = y$. Then

$$fa + gb = 0 \tag{9.1}$$

and ($a \neq 0$ or $b \neq 0$). Let d be the gcd of f and g in $k[x]$.

Case $f_0 \neq 0$: Then f/d divides $(g/d)b$, and since f/d and g/d are coprime, f/d divides b. If $b = 0$, we have $fa = 0$ and thus $a = 0$, a contradiction. If $b \neq 0$, we have $\deg(f/d) = \deg(f) - \deg(d) \leq \deg(b) < m$, and thus $\deg(d) \geq 1$.

Case $g_0 \neq 0$: Then g/d divides $(f/d)a$, and since f/d and g/d are coprime, g/d divides a. Hence $\deg(g/d) \leq \deg(a) < n$, which implies $\deg(d) > 0$. □

LEMMA 9.3. *Let R be the polynomial ring $\mathbb{Z}[a_1,\ldots,a_m,b_1,\ldots,b_n]$, and let $f := \prod_{i=1}^{m}(x-a_i)$ and $g := \prod_{j=1}^{n}(x-b_j) \in R[x]$. Then $\mathrm{res}^{[m,n]}(f,g) = \prod_{(i,j)\in \underline{m}\times\underline{n}}(a_i - b_j)$.*

Proof: By expanding $\prod_{i=1}^{m}(x-a_i)$ and $\prod_{j=1}^{n}(x-b_j)$ and computing the resultant, we obtain $r \in \mathbb{Z}[a_1,\ldots,a_m,b_1,\ldots,b_n]$ with $r(\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n) = \mathrm{res}^{[m,n]}(f,g)$. By Theorem 9.2, for all $(\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n) \in \mathbb{C}^{m+n}$, $i \in \underline{m}$, $j \in \underline{n}$ with $\alpha_i = \beta_j$, we have $r(\overline{\alpha},\overline{\beta}) = 0$. Hilbert's Nullstellensatz implies that for all i,j, we have $r \in \sqrt{\langle a_i - b_j\rangle_{\mathbb{C}[\boldsymbol{a},\boldsymbol{b}]}}$. Since the total degree of $a_i - b_j$ is 1, the polynomial $a_i - b_j$ is irreducible in $\mathbb{C}[a_1,\ldots,a_m,b_1,\ldots,b_n]$. Thus $a_i - b_j$ divides r in $\mathbb{C}[a_1,\ldots,a_m,b_1,\ldots,b_n]$. Since $\mathbb{C}[a_1,\ldots,a_m,b_1,\ldots,b_n]$ is a unique factorisation domain and all mn polynomials $a_i - b_j$ are coprime, we have $\prod_{(i,j)\in\underline{m}\times\underline{n}}(a_i - b_j) \mid r$.

Let $l \in \underline{m}$. When computing $r = \mathrm{res}^{[m,n]}(\prod(x-a_i),\prod(x-b_j))$, we see that a_l occurs in n rows of $\mathrm{Syl}^{[m,n]}(\prod(x-a_i),\prod(x-b_j))$, and in each entry of the Sylvester matrix, a_l occurs with degree 1. Hence $\deg_{a_l}(r) \leq n$. Similarly, $\deg_{b_l} \leq m$ for all $l \in \underline{n}$. Writing $r = q \cdot \prod_{(i,j)\in\underline{m}\times\underline{n}}(a_i - b_j)$, we see that q has degree 0 in each of its variables, and must therefore by a constant in k. It remains to prove that $q = 1$. To this end, we set $a_0 = \ldots = a_m = 0$ and $b_0 = \ldots = b_n = 1$. The

matrix $\mathrm{Syl}^{[m,n]}(x^m,(x-1)^n)$ is equal to

$$\mathrm{Syl}^{[m,n]}(f,g)=\begin{pmatrix} 1 & 0 & \dots & \dots & 0 & & \\ & \ddots & & & & \ddots & \\ & & 1 & \dots & \dots & \dots & 0 \\ * & \dots & * & (-1)^n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & * & \dots & * & (-1)^n \end{pmatrix},$$

and therefore $\mathrm{res}^{[m,n]}(x^m,(x-1)^n)=(-1)^{mn}$. This implies $q=1$. □

THEOREM 9.4. *Let R be a commutative ring with unit, let $m,n\in\mathbb{N}$, $f_0,g_0,\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_n\in R$ with $f=f_0\prod_{i=1}^m(x-\alpha_i)$ and $g=g_0\prod_{i=1}^n(x-\beta_i)$. Then $\mathrm{res}^{[m,n]}(f,g)=f_0^n g_0^m\prod_{(i,j)\in\underline{m}\times\underline{n}}(\alpha_i-\beta_j)$.*

Let S be the subring generated by $\{\alpha_i \mid i\in\underline{m}\}\cup\beta_j \mid j\in\underline{n}\}$. Then S is a homomorphic image of $\mathbb{Z}[a_1,\dots,a_m,b_1,\dots,b_n]$ via the homomorphism given by $\varphi(a_i)=\alpha_i$ and $\varphi(b_j)=\beta_j$. Applying this homomorphism to the result of Lemma 9.3, we obtain $\mathrm{res}^{[m,n]}(\prod_{i=1}^m(x-\alpha_i),\prod_{i=1}^n(x-\beta_i))=\prod_{(i,j)\in\underline{m}\times\underline{n}}(\alpha_i-\beta_j)$. Since the coefficients of f appear in n rows of the Sylvester matrix, multiplying $\prod_{i=1}^m(x-\alpha_i)$ with f_0 leads to a multiplication of the resultant with f_0^n. A similar argument for g_0 yields the result. □

ÜBUNGSAUFGABEN 9.5

(1) Let $f:=x^4-11x^3+42x^2-64x+32$, $g:=x^2-8x+15$. Find $v,w\in\mathbb{Z}[x]$ such that $fv+gw=24x^0$.
Hint: $S=\begin{pmatrix} 1 & -11 & 42 & -64 & 32 & 0\\ 0 & 1 & -11 & 42 & -64 & 32\\ 1 & -8 & 15 & 0 & 0 & 0\\ 0 & 1 & -8 & 15 & 0 & 0\\ 0 & 0 & 1 & -8 & 15 & 0\\ 0 & 0 & 0 & 1 & -8 & 15 \end{pmatrix}$, $S^{\mathrm{ad}}=\begin{pmatrix} 1667 & -2085 & -1643 & 7278 & -10080 & 4448\\ 139 & 555 & -139 & -114 & 1440 & -1184\\ -37 & 435 & 37 & -546 & 1440 & -928\\ -29 & 195 & 29 & -282 & 672 & -416\\ -13 & 75 & 13 & -114 & 264 & -160\\ -5 & 27 & 5 & -42 & 96 & -56 \end{pmatrix}$, $\mathrm{res}^{[4,2]}(f,g)=24$.

(2) Using resultants, find a polynomial f in $\{ap+bq \mid a,b\in\mathbb{Q}[x,y]\}\cap\mathbb{Q}[y]$ with $f\neq 0$.

$$p=x^2y+2xy,\quad q=2x^2+xy+1.$$

For the following problems, we set

$$\begin{aligned} B &:= ((x^{n-1},0),\dots,(x^0,0),(0,x^{m-1}),\dots,(0,x^0)),\\ C &:= (x^{m+n-1},\dots,x^0). \end{aligned}$$

(3) Let k be a field, $m,n\in\mathbb{N}$, $\deg(f)=m$, $\deg(g)=n$, and let d be the gcd of f and g in $k[x]$. Show that the row space of $\mathrm{Syl}^{[m,n]}(f,g)$ is equal to

$$\{(p)_C \mid p\in k_{<m+n}[x], p \text{ lies in the ideal of } k[x] \text{ generated by } f,g\},$$

and also equal to

$$\{(p)_C \mid p\in k_{<m+n}[x],\ d\mid p\}.$$

(4) Let k be a field, $m,n\in\mathbb{N}$, $f,g\in k[x]$ with $\deg(f)=m$, $\deg(g)=n$, and let d be the gcd of f and g in $k[x]$. Show that the rank of $\mathrm{Syl}^{[m,n]}(f,g)$ is $m+n-\deg(d)$.

(5) (Gcd-computation via linear algebra) Let k be a field, $m,n\in\mathbb{N}$, $f,g\in k[x]$ with $\deg(f)=m$, $\deg(g)=n$, and let d be the gcd of f and g in $k[x]$. Let H be a matrix in row echelon form such that the row space of H is equal to the row space of $\mathrm{Syl}^{[m,n]}(f,g)$. (For example, H could be the Hermite normal form of $\mathrm{Syl}^{[m,n]}(f,g)$.) Show that the last nonzero row r of H contains the polynomial d (in the sense $r^T=(d)_C$).

(6) Compute $\gcd(x^5 - 2x^3, x^4 - x^2 - 2)$ in $\mathbb{Q}[x]$ by finding a matrix in echelon form with the same row space as the Sylvester matrix of these two polynomials.

(7) Compute $\gcd(2x^3 + 5x^2 - 4x - 3, x^4 + 2x^3 - x^2 + 4x - 6)$ in $\mathbb{Q}[x]$ by finding a matrix in echelon form with the same row space as the Sylvester matrix of these two polynomials.

(8) Let k be a field of characteristic 0, let $f \in k[x]$ with $\deg(f) = m > 1$, and let K be a field in which f splits into linear factors. Show that f has a double root $\alpha \in K$ (meaning that $(x - \alpha)^2 \mid f$) if and only if $\operatorname{res}^{[m,m-1]}(f, f') = 0$.

(9) Give a criterion when $x^2 + px + q \in \mathbb{Q}[x]$ has a double root in $\mathbb{C}$.

(10) Give a polynomial $p \in \mathbb{C}[a, b, c, d]$ with $p \neq 0$ such that every matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathbb{C}^{2\times 2}$ with $p(\alpha, \beta, \gamma, \delta) \neq 0$ is diagonalisable over $\mathbb{C}$. *Hint:* It is sufficient that all eigenvalues are distinct.

(11) In $\mathbb{Q}[x, y]$, the polynomials x and y have only constant common divisors. Nevertheless, there are no $a, b \in \mathbb{Q}[x, y]$ with $1 = ax + by$. Show the following statement:

> If $f, g \in \mathbb{Q}[x, y]$ have no nonconstant common divisor in $\mathbb{Q}[x, y]$, then there are $a, b \in \mathbb{Q}[x, y]$ with $af + bg \in \mathbb{Q}[x] \setminus \{0\}$.

KAPITEL 10

Gröbnerbasen

1. Grundlagen aus der Mengenlehre und der Ordnungstheorie

Sei X eine Menge, und sei p eine natürliche Zahl. Dann bezeichnen wir mit $\binom{X}{p}$ die Menge aller p-elementigen Teilmengen von X, also

$$\binom{X}{p} = \{Y \mid Y \subseteq X \text{ und } |Y| = p\}.$$

Satz 10.1 (Satz von Ramsey, [Ram29]). *Sei X eine unendliche Menge, und seien $p, t \in \mathbb{N}$. Sei $F : \binom{X}{p} \to \{1, \ldots, t\}$. Dann gibt es eine unendliche Teilmenge Y von X, sodass F auf $\binom{Y}{p}$ konstant ist.*

Beweis: Induktion nach p. Für $p = 1$ sehen wir, dass $X = \bigcup_{i=1}^{t} \{x \in X \mid F(\{x\}) = i\}$. Da X also Vereinigung von t Mengen ist, muss eine dieser Mengen unendlich sein. Diese unendliche Menge ist das gesuchte Y.

Induktionsschritt: Sei $p \geq 2$, und sei F eine Färbung der p-elementigen Teilmengen von X mit t Farben. Für jedes $a \in X$ definieren wir eine Färbung G_a der $(p-1)$-elementigen Teilmengen von $X \setminus \{a\}$ durch

$$G_a(M) := F(M \cup \{a\})$$

für alle $M \in \binom{X \setminus \{a\}}{p}$. Nun definieren wir eine Folge $(x_i)_{i \in \mathbb{N}_0}$ aus X, und eine Folge $(Y_i)_{i \in \mathbb{N}_0}$ von Teilmengen von X. Wir definieren $Y_0 := X$, und wählen x_0 als ein Element von X. Wir werden nun die Folgen $(x_i)_{i \in \mathbb{N}_0}$ und $(Y_i)_{i \in \mathbb{N}_0}$ so definieren, dass jedes Y_i eine unendliche Teilmenge von X ist, und dass $x_i \in Y_i$. Wir definieren die Folgen rekursiv. Sei dazu $i \in \mathbb{N}_0$. Da $Y_i \setminus \{x_i\}$ unendlich ist, gibt es nach Induktionsvoraussetzung eine unendliche Teilmenge Y_{i+1} von $Y_i \setminus \{x_i\}$, sodass alle $(p-1)$-elementigen Teilmengen von Y_{i+1} die gleiche Farbe unter der Färbung G_{x_i} haben. Das Element x_{i+1} wählen wir aus Y_{i+1}.

Wir betrachten nun die Menge

$$Z := \{x_i \mid i \in \mathbb{N}_0\}.$$

Für jede p-elementige Teilmenge A von Z definieren wir den *kleinsten Index in A*, $\mathrm{ind}(A)$, als das kleinste $j \in \mathbb{N}_0$, sodass $x_j \in A$. Wir zeigen nun:

$$\text{Für alle } A, B \in \binom{Z}{p} \text{ mit } \mathrm{ind}(A) = \mathrm{ind}(B) \text{ gilt } F(A) = F(B).$$

Sei dazu $i := \mathrm{ind}(A)$. Alle x_j mit $j > i$ liegen in Y_{i+1}. Folglich ist A eine Teilmenge von $Y_{i+1} \cup \{x_i\}$. Ebenso ist B eine Teilmenge von $Y_{i+1} \cup \{x_i\}$. Wegen der Konstruktion von Y_{i+1} ist $G_{x_i}(A \setminus \{x_i\}) = G_{x_i}(B \setminus \{x_i\})$. Also gilt $F(A) = F(B)$.

Nun betrachten wir die Abbildung $h : \mathbb{N}_0 \to \{1, \ldots, t\}$, die durch

$$h(i) := F(\{x_i, \ldots, x_{i+p-1}\})$$

für $i \in \mathbb{N}_0$ definiert ist. Es gibt eine unendliche Teilmenge J von $\mathbb{N}_0$, sodass $h|_J$ konstant ist. Wir behaupten nun, dass

$$Y := \{x_j \mid j \in J\}$$

die gewünschten Eigenschaften erfüllt.

Seien dazu C und D p-elementige Teilmengen von Y, und seien $c_1 < \cdots < c_p$ und $d_1 < \cdots < d_p$ so, dass $C = \{x_{c_1}, x_{c_2}, \ldots, x_{c_p}\}$ und $D = \{x_{d_1}, x_{d_2}, \ldots, x_{d_p}\}$. Da $\operatorname{ind}(C) = c_1 = \operatorname{ind}(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$, gilt

$$F(C) = F(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$$

und ebenso

$$F(D) = F(\{x_{d_1}, x_{d_1+1}, \ldots, x_{d_1+p-1}\}).$$

Also gilt $F(C) = h(c_1)$ und $F(D) = h(d_1)$. Da x_{c_1} in Y liegt, gilt $c_1 \in J$; ebenso gilt $d_1 \in J$, und folglich $h(c_1) = h(d_1)$. Also haben C und D die gleiche Farbe. □

Eine geordnete Menge $(M, \leq)$ erfüllt die (DCC) (absteigende Kettenbedingung, *descending chain condition*), wenn es keine unendliche echt absteigende Folge $m_1 > m_2 > m_3 > \cdots$ von Elementen aus M gibt. Zwei Elemente $s, t \in M$ sind *unvergleichbar*, wenn weder $s \leq t$ noch $t \leq s$ gilt. Wir schreiben dafür $s \parallel t$. Eine Teilmenge T von M ist eine *Antikette*, wenn alle $t_1, t_2 \in T$ mit $t_1 \neq t_2$ unvergleichbar sind.

Sei $m \in \mathbb{N}$. Auf ${\mathbb{N}_0}^m$ definieren wir die Ordnungsrelation $\sqsubseteq$. Seien $\boldsymbol{a} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ und $\boldsymbol{b} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$. Dann gilt $\boldsymbol{a} \sqsubseteq \boldsymbol{b}$, wenn für alle $i \in \{1, \ldots, m\}$ gilt: $\boldsymbol{a}_i \leq \boldsymbol{b}_i$. Wir betrachten nun die geordnete Menge $({\mathbb{N}_0}^m, \sqsubseteq)$.

LEMMA 10.2. *Sei $m \in \mathbb{N}$ und sei $S = \langle \boldsymbol{a}^{(i)} \mid i \in \mathbb{N} \rangle$ eine Folge von Elementen aus ${\mathbb{N}_0}^m$. Dann gibt es eine unendliche Folge $t_1 < t_2 < \cdots$ von natürlichen Zahlen, sodass $\langle \boldsymbol{a}^{(t_i)} \mid i \in \mathbb{N} \rangle$ eine bezüglich $\sqsubseteq$ schwach monoton wachsende unendliche Teilfolge von S ist.*

Beweis: Für $i \in \mathbb{N}$ und $k \in \{1, \ldots, m\}$ bezeichnen wir die k-te Komponente von $\boldsymbol{a}^{(i)}$ mit $\boldsymbol{a}_k^{(i)}$.

Wir färben nun jede 2-elementige Teilmenge $\{i, j\}$ von $\mathbb{N}$ mit $i < j$ mit einer von 2^m Farben. As Farben wählen wir die Funktionen von $\{1, \ldots, m\}$ nach $\{\mathbf{1}, \mathbf{2}\}$. Wir definieren nun die Farbe $C(\{i, j\})$ der Menge $\{i, j\}$ durch

$$C(\{i, j\})\,(k) := \begin{cases} \mathbf{1} & \text{wenn } \boldsymbol{a}_k^{(i)} \leq \boldsymbol{a}_k^{(j)}, \\ \mathbf{2} & \text{wenn } \boldsymbol{a}_k^{(i)} > \boldsymbol{a}_k^{(j)}. \end{cases}$$

Nach dem Satz von Ramsey, Satz 10.1, hat $\mathbb{N}$ eine unendliche Teilmenge T, sodass alle 2-elementigen Teilmengen von T die gleiche Farbe C haben.

Wir zeigen nun, dass $C(k) = \mathbf{1}$ für alle $k \in \{1, \ldots, m\}$ gilt. Nehmen wir an, es gibt ein k mit $C(k) = \mathbf{2}$. Seien $t_1 < t_2 < t_3 < \ldots$ die Elemente von T. Wenn $C(k) = \mathbf{2}$, dann gilt

$$\boldsymbol{a}_k^{(t_1)} > \boldsymbol{a}_k^{(t_2)} > \boldsymbol{a}_k^{(t_3)} > \cdots,$$

im Widerspruch dazu, dass $(\mathbb{N}, \leq)$ die (DCC) erfüllt.

Da also $C(k) = \mathbf{1}$ für alle k, gilt $\boldsymbol{a}^{(t_1)} \sqsubseteq \boldsymbol{a}^{(t_2)} \sqsubseteq \boldsymbol{a}^{(t_3)} \sqsubseteq \cdots$. □

Satz 10.3 (Dicksons Lemma, cf. [**Dic13**, Lemma A]). *Sei $m \in \mathbb{N}$. Dann sind alle Antiketten in $({\mathbb{N}_0}^m, \sqsubseteq)$ endlich.*

Beweis: Nach Lemma 10.2 kann $({\mathbb{N}_0}^m, \sqsubseteq)$ keine unendliche Antikette enthalten. □

Übungsaufgaben 10.4

(1) (Satz von Ramsey) Zeigen Sie, dass jede reelle Zahlenfolge eine streng monoton fallende, eine streng monoton steigende oder eine konstante (unendliche) Teilfolge enthält.
Using Ramsey's Theorem, prove that every sequence $(x_i)_{i\in\mathbb{N}}$ of real numbers has a strictly monotonically increasing, a strictly monotonically decreasing, or a constant subsequence. *Hint:* Colour the two element subsets of $\mathbb{N}$.

(2) (Geometrie) Wir nennen eine Teilmenge T von $\mathbb{N}\times\mathbb{N}$ eine *Viertelebene*, wenn es $m, n \in \mathbb{N}$ gibt, sodass

$$T = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \geq m \text{ und } y \geq n\}.$$

Zeigen Sie, dass jede Vereinigung von beliebig vielen Viertelebenen eine Vereinigung von endlich vielen Viertelebenen ist.
We call a subset T of $\mathbb{N} \times \mathbb{N}$ a *quarter plane* if there are $m, n \in \mathbb{N}$ such that $T = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \geq m \text{ and } y \geq n\}$. Show that every union of arbitrary many quarter planes is a union of only finitely many of these quarter planes.

Definition 10.5. Eine Teilmenge I von ${\mathbb{N}_0}^m$ ist ein *Ordnungsfilter*, wenn für alle $\boldsymbol{a} \in I$ und $\boldsymbol{b} \in {\mathbb{N}_0}^m$ mit $\boldsymbol{a} \sqsubseteq \boldsymbol{b}$ auch $\boldsymbol{b} \in I$ gilt.

Für eine Teilmenge I von ${\mathbb{N}_0}^m$ bezeichnen wir mit $\mathcal{M}(I)$ die Menge aller minimalen Elemente von I. Für eine Teilmenge M von $\mathbb{N}_0^m$ definieren wir $\mathcal{U}(M)$ durch $\mathcal{U}(M) := \{\boldsymbol{a} \in \mathbb{N}_0^m \mid \text{ es gibt } \boldsymbol{z} \in M, \text{ sodass } \boldsymbol{z} \leq \boldsymbol{a}\}$. $\mathcal{U}(M)$ ist stets ein Ordnungsfilter.

Lemma 10.6. *Sei $I \subseteq {\mathbb{N}_0}^m$ ein Ordnungsfilter bezüglich $\sqsubseteq$. Dann ist $\mathcal{M}(I)$ endlich, und es gilt $I = \mathcal{U}(\mathcal{M}(I))$.*

Beweis: $\mathcal{M}(I)$ ist eine Antikette, und daher wegen des Dicksonschen Lemmas (Satz 10.3) endlich. Sei nun $\boldsymbol{i} \in I$. Da $(\mathbb{N}_0^m, \sqsubseteq)$ keine unendlich absteigenden Ketten hat, gibt es ein minimales Element $\boldsymbol{z} \in I$ mit $\boldsymbol{z} \leq \boldsymbol{i}$. Daher gilt $\boldsymbol{i} \in \mathcal{U}(\mathcal{M}(I))$. Da $\mathcal{M}(I) \subseteq I$, erhalten wir die Inklusion $\mathcal{U}(\mathcal{M}(I)) \subseteq I$ unmittelbar aus der Tatsache, dass I ein Ordnungsfilter ist. □

Satz 10.7. *Let $m \in \mathbb{N}$. Dann hat die Menge $\mathbb{N}_0^m$ keine unendliche aufsteigende Kette $U_1 \subset U_2 \subset U_3 \ldots$ von Ordnungsfiltern.*

Sei $U := \bigcup\{U_i \mid i \in \mathbb{N}\}$. Die Menge U ist ein Ordnungsfilter. Daher ist die Menge $\mathcal{M}(U)$ der bezüglich $\sqsubseteq$ minimalen Elemente von U endlich. Es gibt also ein $j \in \mathbb{N}$, sodass $\mathcal{M}(U) \subseteq U_j$. Daher gilt $\mathcal{U}(\mathcal{M}(U)) \subseteq \mathcal{U}(U_j)$, und folglich $U \subseteq U_j$. □

Übungsaufgaben 10.8

(1) Let $\langle A, \leq \rangle$ be a partially ordered set, and let $\mathcal{U}$ be the set of upward closed subsets of A. Show that the following are equivalent:
   (a) $\langle A, \leq \rangle$ has no infinite descending chain and no infinite antichain.
   (b) $\langle \mathcal{U}, \subseteq \rangle$ has no infinite ascending chain.

2. Multivariate Polynomdivision

DEFINITION 10.9. Sei $n \in \mathbb{N}$, und sei $\leq$ eine Ordnung auf ${\mathbb{N}_0}^n$. Die Ordnung $\leq$ ist *zulässig*, wenn folgendes gilt:

(1) $\leq$ ist linear.
(2) Für alle $\alpha, \beta \in {\mathbb{N}_0}^n$ mit $\alpha \sqsubseteq \beta$ gilt auch $\alpha \leq \beta$.
(3) Für alle $\alpha, \beta, \gamma \in {\mathbb{N}_0}^n$ mit $\alpha \leq \beta$ gilt auch $\alpha + \gamma \leq \beta + \gamma$.

LEMMA 10.10. *Sei $n \in \mathbb{N}$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Dann erfüllt $({\mathbb{N}_0}^n, \leq)$ die* (DCC).

Sei $\boldsymbol{a}^{(1)} > \boldsymbol{a}^{(2)} > \cdots$ eine bezüglich $\leq$ unendliche absteigende Kette in ${\mathbb{N}_0}^n$. Nach Lemma 10.2 gibt es $t_1, t_2 \in \mathbb{N}$ mit $t_1 < t_2$, sodass $\boldsymbol{a}^{(t_1)} \sqsubseteq \boldsymbol{a}^{(t_2)}$. Da $\leq$ zulässig ist, gilt $\boldsymbol{a}^{(t_1)} \leq \boldsymbol{a}^{(t_2)}$, im Widerspruch zu $\boldsymbol{a}^{(t_1)} > \boldsymbol{a}^{(t_2)}$. □

DEFINITION 10.11. Sei k ein kommutativer Ring mit Eins, und sei R der Polynomring $k[x_1, \ldots, x_n]$. Für $\alpha = (\alpha_1, \ldots, \alpha_n) \in {\mathbb{N}_0}^n$ definieren wir $\boldsymbol{x}^\alpha$ durch

$$\boldsymbol{x}^\alpha := {x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n}.$$

DEFINITION 10.12. Sei $n \in \mathbb{N}$, sei k ein kommutativer Ring mit Eins, sei I eine endliche Teilmenge von ${\mathbb{N}_0}^n$, sei $c : I \to k$, sei

$$f = \sum_{\alpha \in I} c_\alpha \boldsymbol{x}^\alpha$$

ein Element von $k[x_1, \ldots, x_n]$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Dann definieren wir den *Multigrad* von f bezüglich $\leq$ durch

$$\text{DEG}(f) := (-1, \ldots, -1), \text{ wenn } f = 0,$$

und

$$\text{DEG}(f) := \max\nolimits_{\leq} \{\alpha \in {\mathbb{N}_0}^n \mid c_\alpha \neq 0\}, \text{ wenn } f \neq 0.$$

DEFINITION 10.13. Sei $n \in \mathbb{N}$, sei k ein kommutativer Ring mit Eins, und sei

$$f = \sum_{\alpha \in {\mathbb{N}_0}^n} c_\alpha \boldsymbol{x}^\alpha$$

ein Element von $k[x_1, \ldots, x_n]$ mit $f \neq 0$, und sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$. Sei γ der Multigrad von f. Dann definieren wir

$$\begin{aligned} \text{LM}(f) &:= \boldsymbol{x}^\gamma, \\ \text{LC}(f) &:= c_\gamma, \\ \text{LT}(f) &:= c_\gamma \boldsymbol{x}^\gamma. \end{aligned}$$

DEFINITION 10.14. Sei $n \in \mathbb{N}$, sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$, sei $s \in \mathbb{N}$, und seien $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Eine Folge $(a_1, \ldots, a_s, r) \in k[x_1, \ldots, x_n]^{s+1}$ ist eine *Standarddarstellung* von f durch $(f_1, \ldots, f_s)$ bezüglich $\leq$, wenn folgendes gilt:

(1) $f = \sum_{i=1}^{s} a_i f_i + r$.
(2) $r = 0$, oder es gibt eine endliche Teilmenge I von ${\mathbb{N}_0}^n$, sodass
$$r = \sum_{\alpha \in I} c_\alpha \boldsymbol{x}^\alpha$$
gilt, und dass für alle $\alpha \in I$ und alle $i \in \{1, \ldots, s\}$ mit $f_i \neq 0$ das Monom $\boldsymbol{x}^\alpha$ kein Vielfaches von $\text{LM}(f_i)$ ist.
(3) Für alle $i \in \{1, \ldots, s\}$ gilt $\text{DEG}(a_i f_i) \leq \text{DEG}(f)$.

Das Polynom r heißt auch *Rest* der Darstellung.

ÜBUNGSAUFGABEN 10.15

(1) Seien $f, p, q \in \mathbb{Q}[x, y]$ gegeben durch
$$\begin{aligned} f &= x^3y^3 + 1 \\ p &= 1 + 3x + 2x^2 + x^2y + x^3y \\ q &= xy^2 + x^2y^2 \end{aligned}$$
Wir ordnen die Monome lexikographisch mit $x > y$. Finden Sie $a_1, a_2, r \in \mathbb{Q}[x, y]$, sodass $f = a_1\,p + a_2\,q + r$, $\text{DEG}(a_1\,p) \leq \text{DEG}(f)$, $\text{DEG}(a_2\,q) \leq \text{DEG}(f)$ und kein Term in r ein Vielfaches von $\text{LT}(p)$ oder $\text{LT}(q)$ ist.
Let $f, p, q \in \mathbb{Q}[x, y]$ be defined by
$$\begin{aligned} f &= x^3y^3 + 1 \\ p &= 1 + 3x + 2x^2 + x^2y + x^3y \\ q &= xy^2 + x^2y^2 \end{aligned}$$
We order the monomials lexicographically with $x > y$. Find $a_1, a_2, r \in \mathbb{Q}[x, y]$ with $f = a_1\,p + a_2\,q + r$, $\text{DEG}(a_1\,p) \leq \text{DEG}(f)$, $\text{DEG}(a_2\,q) \leq \text{DEG}(f)$ such that no monomial in r is a multiple of $\text{LT}(p)$ or $\text{LT}(q)$.
(2) Seien $f, p, q \in \mathbb{Q}[x, y]$ gegeben durch
$$\begin{aligned} f &= x^3y^2 \\ p &= 1 + x^3y + 3x^2y^5 \\ q &= 2x^2y + x^2y^2 \end{aligned}$$
Wir ordnen die Monome lexikographisch mit $x > y$. Finden Sie $a_1, a_2, r \in \mathbb{Q}[x, y]$, sodass $f = a_1\,p + a_2\,q + r$, $\text{DEG}(a_1\,p) \leq \text{DEG}(f)$, $\text{DEG}(a_2\,q) \leq \text{DEG}(f)$ und kein Term in r ein Vielfaches von $\text{LT}(p)$ oder $\text{LT}(q)$ ist.
Let $f, p, q \in \mathbb{Q}[x, y]$ be defined by
$$\begin{aligned} f &= x^3y^2 \\ p &= 1 + x^3y + 3x^2y^5 \\ q &= 2x^2y + x^2y^2 \end{aligned}$$
We order the monomials lexicographically with $x > y$. Find $a_1, a_2, r \in \mathbb{Q}[x, y]$ with $f = a_1\,p + a_2\,q + r$, $\text{DEG}(a_1\,p) \leq \text{DEG}(f)$, $\text{DEG}(a_2\,q) \leq \text{DEG}(f)$ such that no monomial in r is a multiple of $\text{LT}(p)$ or $\text{LT}(q)$.
(3) Sei $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. Wir ordnen die Monome lexikographisch mit $x > y$.

(a) Zeigen Sie, dass der Rest r bei einer Darstellung $f = a_1 f_1 + a_2 f_2 + r$ wie in den vorigen Beispielen nicht eindeutig bestimmt ist.

(b) Finden Sie ein Polynom im Ideal $\langle f_1, f_2 \rangle$, das nicht das Nullpolynom ist und das keinen Term enthält, der ein Vielfaches von xy oder y^2 ist.

Let $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. We order the monomials lexicographically with $x > y$.

(a) Show that the remainder r in a standard expression $f = a_1 f_1 + a_2 f_2 + r$ as in the previous examples is not uniquely determined.

(b) Find a polynomial $p \neq 0$ in the ideal $\langle f_1, f_2 \rangle$ that contains no term that is a multiple of xy or y^2.

(4) Im folgenden Beispiel zeigen wir, dass der Rest der Division von f durch ein Hauptideal $\langle f_1 \rangle$ eindeutig bestimmt ist. Zeigen Sie also: Sei $\leq$ eine zulässige Ordnung, sei k ein Körper, $n \in \mathbb{N}$, und seien $f, f_1 \in k[x_1, \ldots, x_n]$, $f_1 \neq 0$. Seien $a, b, r, s \in k[x_1, \ldots, x_n]$ so, dass $f = a\, f_1 + r = b\, f_1 + s$. Wir nehmen an, dass kein Term von r und kein Term von s durch $\mathrm{LT}(f_1)$ teilbar ist. Zeigen Sie $r = s$!

SATZ 10.16. *Sei $n \in \mathbb{N}$, sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$, sei $s \in \mathbb{N}$, und seien $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Dann gibt es eine Standarddarstellung $(a_1, \ldots, a_s, r)$ von f durch $(f_1, \ldots, f_s)$.*

Beweis: Seien $s \in \mathbb{N}$ und $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Wir zeigen nun, dass jedes Polynom f eine Standarddarstellung durch $(f_1, \ldots, f_s)$ besitzt. Als zulässige Ordnung erfüllt $\leq$ die (DCC), folglich enthält jede nichtleere Teilmenge von ${\mathbb{N}_0}^n$ ein bezüglich $\leq$ minimales Element.

Sei nun f ein Polynom mit minimalem Multigrad (bezüglich $\leq$), das keine Standarddarstellung durch $(f_1, \ldots, f_s)$ besitzt.

1. Fall: $f = 0$: Da $0 = \sum_{i=1}^{s} 0 f_i + 0$ eine Standarddarstellung ist, kann dieser Fall nicht eintreten.

2. Fall: $f \neq 0$: In diesem Fall gehen wir so vor: sei $g \in k[\boldsymbol{x}]$ so, dass

$$f = \mathrm{LT}(f) + g.$$

Wir werden aus einer Standarddarstellung von g eine Standarddarstellung von f bauen. Dazu unterscheiden wir zwei Fälle.

2.1. Fall: Es gibt ein $i \in \{1, \ldots, s\}$, sodass $f_i \neq 0$ und $\mathrm{LM}(f_i) | \mathrm{LM}(f)$: Dann gilt

$$\mathrm{DEG}(f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i) < \mathrm{DEG}(f).$$

Wegen der Minimalität von f gibt es $b_1, \ldots, b_s \in k[\boldsymbol{x}]$, sodass folgendes gilt:

$$f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i = \sum_{j=1}^{s} b_j f_j + r,$$

für alle $j \in \{1, \ldots, s\}$ gilt $\mathrm{DEG}(b_j f_j) \leq \mathrm{DEG}(f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i)$, und kein Monomom in r ist durch ein $\mathrm{LM}(f_j)$ mit $j \in \{1, \ldots, s\}$ teilbar.

Dann gilt

$$f = \Big(\sum_{\substack{j \in \{1,\ldots,s\} \\ j \neq i}} b_j f_j \Big) + \left(b_i + \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} \right) f_i + r$$

Da $\textsc{Deg}(b_i f_i + \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i)$ höchstens gleich dem Multigrad eines der Summanden ist, und $\textsc{Deg}(b_i f_i) < \textsc{Deg}(f)$ und $\textsc{Deg}(\frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i) = \textsc{Deg}(f)$, ist

$$(b_1, \ldots, b_{i-1},\ b_i + \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)},\ b_{i+1}, \ldots, b_s, r)$$

eine Standarddarstellung von f durch $(f_1, \ldots, f_s)$, im Widerspruch zur Wahl von f.

2.2. Fall: Es gibt kein $i \in \{1, \ldots, s\}$, sodass $f_i \neq 0$ und $\textsc{Lm}(f_i) | \textsc{Lm}(f)$: Es gilt $\textsc{Deg}(f - \textsc{Lt}(f)) < \textsc{Deg}(f)$. Wegen der Minimalität von f besitzt $f - \textsc{Lt}(f)$ eine Standarddarstellung

$$f - \textsc{Lt}(f) = \sum_{j=1}^{s} b_j f_j + r.$$

Da das Mononom $\textsc{Lm}(f)$ durch kein $\textsc{Lm}(f_i)$ teilbar ist, ist

$$f = \sum_{j=1}^{s} b_j f_j + (r + \textsc{Lt}(f))$$

eine Standarddarstellung von f, im Widerspruch zur Wahl von F. Folglich besitzt jedes Polynom eine Standarddarstellung bezüglich $(f_1, \ldots, f_s)$. □

3. Monomiale Ideale

Definition 10.17. Sei $n \in \mathbb{N}$, sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Das Ideal I ist *monomial*, wenn es eine Teilmenge A von ${\mathbb{N}_0}^n$ gibt, sodass $I = \langle \{ \boldsymbol{x}^\alpha \mid \alpha \in A \} \rangle_{k[\boldsymbol{x}]}$.

Satz 10.18. *Sei $n \in \mathbb{N}$, sei k ein Körper, sei I ein monomiales Ideal von $k[x_1, \ldots, x_n]$, und sei $A \subseteq {\mathbb{N}_0}^n$ so, dass*

$$I = \langle \{ \boldsymbol{x}^\alpha \mid \alpha \in A \} \rangle_{k[\boldsymbol{x}]}.$$

Dann gibt es eine endliche Teilmenge B von A, sodass

$$I = \left\langle \{ \boldsymbol{x}^\beta \mid \beta \in B \} \right\rangle_{k[\boldsymbol{x}]}.$$

Beweis: Wir nehmen an, es gibt keine solche endliche Teilmenge B von A. Wir wählen $\alpha_1 \in A$. Nun konstruieren wir rekursiv eine Folge $\langle \alpha_i \mid i \in \mathbb{N} \rangle$ aus A in folgender Weise: Sei $i \geq 2$. Es gilt nun

$$\{ \boldsymbol{x}^\alpha \mid \alpha \in A \} \not\subseteq \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{i-1}} \rangle_{k[\boldsymbol{x}]}.$$

Nehmen wir an, es gilt $\subseteq$: Dann gilt $I = \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{i-1}} \rangle_{k[\boldsymbol{x}]}$, im Widerspruch zur Annahme, dass es keine solche endliche Teilmenge von A gibt. Wir wählen α_i als ein $\alpha \in A$, sodass

$$\boldsymbol{x}^\alpha \notin \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{i-1}} \rangle_{k[\boldsymbol{x}]}$$

Wegen Lemma 10.2 gibt es nun k, l in $\mathbb{N}$ mit $k < l$ und $\alpha_k \sqsubseteq \alpha_l$. Dann gilt $\boldsymbol{x}^{\alpha_l} \in \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{l-1}} \rangle_{k[\boldsymbol{x}]}$, im Widerspruch zur Wahl von α_l. □

Korollar 10.19. *Sei $n \in \mathbb{N}$, sei k ein Körper, und sei I ein monomiales Ideal von $k[x_1, \ldots, x_n]$. Dann ist I endlich erzeugt.*

DEFINITION 10.20. Sei $n \in \mathbb{N}$, k ein Körper, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I eine Teilmenge von $k[x_1, \ldots, x_n]$. Dann definieren wir

$$\operatorname{LT}(I) \quad := \quad \{\operatorname{LT}(f) \mid f \in I, f \neq 0\}.$$

SATZ 10.21. *Sei $n \in \mathbb{N}$, k ein Körper, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I ein Ideal von $k[x_1, \ldots, x_n]$. Dann gibt es $t \in \mathbb{N}_0$ und $g_1, \ldots, g_t \in I \setminus \{0\}$, sodass $\langle \operatorname{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$.*

Beweis: Sei $J := \langle \operatorname{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \operatorname{LM}(I) \rangle_{k[\boldsymbol{x}]}$. Klarerweise gilt dann für

$$A := \{\alpha \in {\mathbb{N}_0}^n \mid \text{ es gibt } f \in I, \text{ sodass } \operatorname{LM}(f) = \boldsymbol{x}^\alpha\}$$

die Gleichheit $J = \langle \{\boldsymbol{x}^\alpha \mid \alpha \in A\} \rangle_{k[\boldsymbol{x}]}$. Es gibt also nach Satz 10.18 eine endliche Teilmenge $B = \{\beta_1, \ldots, \beta_t\}$ von A, sodass

$$J = \left\langle \{\boldsymbol{x}^{\beta_i} \mid i \in \{1, \ldots, t\}\} \right\rangle_{k[\boldsymbol{x}]}.$$

Für jedes $i \in \{1, \ldots, t\}$ wählen wir nun ein $g_i \in I$, sodass $g_i \in I$ und $\operatorname{LM}(g_i) = \boldsymbol{x}^{\beta_i}$. Dann gilt $J = \langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. □

LEMMA 10.22. *Sei $n \in \mathbb{N}$, sei k ein Körper, sei I ein monomiales Ideal von $k[x_1, \ldots, x_n]$, und sei $A \subseteq {\mathbb{N}_0}^n$ so, dass*

$$I = \langle \{\boldsymbol{x}^\alpha \mid \alpha \in A\} \rangle_{k[\boldsymbol{x}]}.$$

Sei B eine endliche Teilmenge von ${\mathbb{N}_0}^n$, und sei $f = \sum_{\beta \in B} c_\beta \boldsymbol{x}^\beta \in k[x_1, \ldots, x_n]$. Dann sind äquivalent:

(1) *$f \in I$.*
(2) *Für alle $\beta \in B$ mit $c_\beta \neq 0$ gibt es ein $\alpha \in A$, sodass $\alpha \sqsubseteq \beta$.*

Beweis: (2)⇒(1): Da jeder Summand $c_\beta \boldsymbol{x}^\beta$ nach Voraussetzung in I liegt, liegt auch f in I. (1)⇒(2): Sei $f \in I$. Dann gibt es $m \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_m \in A$ und $p_1, \ldots, p_m \in k[x_1, \ldots, x_n]$, sodass

$$f = \sum_{i=1}^{m} p_i \cdot \boldsymbol{x}^{\alpha_i}.$$

Durch Ausmultiplizieren der rechten Seite sieht man, dass es für jedes in f auftretende Monom $\boldsymbol{x}^\beta$ ein j und $\gamma \in {\mathbb{N}_0}^n$ gibt, sodass

$$\boldsymbol{x}^\beta = \boldsymbol{x}^{\alpha_j + \gamma}.$$

Also gilt $\alpha_j \sqsubseteq \beta$. □

SATZ 10.23. *Sei $n \in \mathbb{N}$, sei k ein Körper, sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $t \in \mathbb{N}_0$, und seien $g_1, \ldots, g_t \in I \setminus \{0\}$ so, dass $\langle \operatorname{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. Dann gilt $I = \langle g_1, \ldots, g_t \rangle_{k[\boldsymbol{x}]}$.*

Beweis: Die Inklusion $\supseteq$ folgt aus der Tatsache, dass jedes g_i in I liegt. Für den Beweis von $\subseteq$ wählen wir $f \in I$. Sei $f = \sum_{i=1}^{t} a_i g_i + r$ eine Standarddarstellung von f durch $(g_1, \ldots, g_t)$. Wenn $r = 0$, so liegt f im von $\{g_1, \ldots, g_t\}$ erzeugten Ideal. Wir nehmen nun an, $r \neq 0$. Es gilt $r = f - \sum_{i=1}^{t} a_i g_i \in I$. Folglich gilt $\operatorname{LT}(r) \in \operatorname{LT}(I)$. Nach Voraussetzung gilt also

$$\operatorname{LT}(r) \in \langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle_{k[\boldsymbol{x}]}.$$

Wegen Lemma 10.22 gibt es also ein $i \in \{1, \dots, t\}$, sodass $\text{LT}(g_i) | \text{LT}(r)$. Dann kann r aber nicht der Rest einer Standarddarstellung von f durch $(g_1, \dots, g_t)$ sein. Der Fall $r \neq 0$ kann also nicht eintreten. □

SATZ 10.24 (Hilbertscher Basissatz für Polynomringe über Körpern). *Sei k ein Körper, $n \in \mathbb{N}$. Dann ist jedes Ideal von $k[x_1, \dots, x_n]$ endlich erzeugt.*

Beweis: Sei I ein Ideal von $k[x_1, \dots, x_n]$. Nach Satz 10.21 gibt es $t \in \mathbb{N}_0$ und $g_1, \dots, g_t \in I \setminus \{0\}$, sodass $\langle \text{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. Wegen Satz 10.23 erzeugen dann die Polynome $g_1, \dots, g_t$ das Ideal I. □

ÜBUNGSAUFGABEN 10.25

(1) (Monomial ideals) Let A be a subset of ${\mathbb{N}_0}^n$, let I be the ideal of $k[x_1, \dots, x_n]$ that is generated by $\{\boldsymbol{x}^\alpha \mid \alpha \in A\}$, and let $f = \sum_{\beta \in {\mathbb{N}_0}^n} c_\beta \boldsymbol{x}^\beta \in k[x_1, \dots, x_n]$. Show that the following are equivalent:
   (a) $f \in I$.
   (b) For each $\beta \in {\mathbb{N}_0}^n$ with $c_\beta \neq 0$, there is an $\alpha \in A$ such that $\alpha \sqsubseteq \beta$.
   (c) For each $\beta \in {\mathbb{N}_0}^n$, the term $c_\beta \boldsymbol{x}^\beta$ is an element of I.

(2) Find the leading term ideal $\langle \text{LT}(I) \rangle_{k[\boldsymbol{x}]}$ for the following ideals I.
   (a) $I = \langle x^5 + 5x^4 - x^3 - 15x^2 - 6x,\ x^7 - 3x^5 \rangle_{\mathbb{Q}[x]}$ in the univariate polynomial ring $\mathbb{Q}[x]$.
   (b) $I = \{f \in \mathbb{Q}[x, y] \mid f(-1, 2) = 0\}$, lexicographic ordering, $x > y$.

(3) Show the following result:
   Let k be a field, let $n \in \mathbb{N}$, let $(f_1, \dots, f_s)$ be a sequence of polynomials from $k[x_1, \dots, x_n]$, let $f \in k[x_1, \dots, x_n]$, and let r be the remainder of a standard expression of f by $(f_1, \dots, f_s)$. Show that 0 is a remainder of a standard expression of f by $(f_1, \dots, f_s, r)$.

4. Gröbnerbasen

DEFINITION 10.26. Sei k ein Körper, $n \in \mathbb{N}$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I ein Ideal von $k[x_1, \dots, x_n]$. Eine endliche Teilmenge $G = \{g_1, \dots, g_t\}$ von $k[x_1, \dots, x_n]$ ist eine *Gröbnerbasis* von I bezüglich $\leq$, wenn

(1) $G \subseteq I \setminus \{0\}$,
(2) $\langle \text{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$.

Nach Satz 10.21 besitzt jedes Ideal eine Gröbnerbasis. Wenn nun I ein Ideal von $k[x_1, \dots, x_n]$, und G eine Gröbnerbasis von I ist, so gilt nach Satz 10.23 auch $\langle G \rangle_{k[\boldsymbol{x}]} = I$.

SATZ 10.27. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \dots, x_n]$. Sei $t \in \mathbb{N}_0$, und sei $G = \{g_1, \dots, g_t\}$ eine Gröbnerbasis von I. Sei $r \in I$ so, dass kein Monom in r durch irgendein $\text{LT}(g_i)$ teilbar ist. Dann gilt $r = 0$.*

Beweis: Wenn $r \neq 0$, so liegt $\text{LT}(r) \in \text{LT}(I)$, also in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Wegen Lemma 10.22 gibt es also ein $i \in \{1, \dots, t\}$, sodass $\text{LT}(g_i) | \text{LT}(r)$. Das steht im Widerspruch zu den Voraussetzungen an r. □

SATZ 10.28. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \dots, x_n]$. Sei $t \in \mathbb{N}_0$, und sei $G = \{g_1, \dots, g_t\}$ eine Gröbnerbasis von I. Seien $r_1, r_2 \in k[x_1, \dots, x_n]$ so, dass*

(1) $r_1 - r_2 \in I$,
(2) *Kein Monom in* r_1 *ist durch irgendein* $\text{LT}(g_i)$ *teilbar,*
(3) *Kein Monom in* r_2 *ist durch irgendein* $\text{LT}(g_i)$ *teilbar.*

Dann gilt $r_1 = r_2$.

Beweis: Wir nehmen an, $r_1 - r_2 \neq 0$. Dann gilt $\text{LM}(r_1 - r_2) \in \text{LT}(I)$. Da G eine Gröbnerbasis ist, gilt also $\text{LM}(r_1 - r_2) \in \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Das führende Monom von $r_1 - r_2$ muss auch in einem der Polynome r_1 oder r_2 vorkommen. Somit enthält eines der r_i ein Monom in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Nach Lemma 10.22 ist dieses Monom durch eines der $\text{LM}(g_i)$ teilbar. Das steht im Widerspruch zu den Voraussetzungen an r_1 und r_2. □

KOROLLAR 10.29. *Sei* k *ein Körper, sei* $n \in \mathbb{N}$, *und sei* I *ein Ideal von* $k[x_1, \ldots, x_n]$. *Sei* $t \in \mathbb{N}_0$, *und sei* $G = \{g_1, \ldots, g_t\}$ *eine Gröbnerbasis von* I. *Sei* $f \in k[x_1, \ldots, x_n]$, *und seien*

$$f = \sum_{i=1}^{t} a_i g_i + r_1 = \sum_{i=1}^{t} b_i g_i + r_2$$

Standarddarstellungen von f *durch* $(g_1, \ldots, g_t)$. *Dann gilt* $r_1 = r_2$. *Wenn außerdem* $f \in I$, *so gilt* $r_1 = r_2 = 0$.

Beweis: Da $r_1 - r_2 \in I$, folgt die erste Behauptung aus Satz 10.28. Wenn $f \in I$ gilt, so folgt $r_1 = 0$ aus Satz 10.27. □

DEFINITION 10.30. Sei $n \in \mathbb{N}$, sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$, sei $s \in \mathbb{N}$, und seien $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Ein Polynom $r \in k[x_1, \ldots, x_n]$ ist ein *möglicher Rest bei einer Standarddarstellung von* f *durch* $(f_1, \ldots, f_s)$ *bezüglich* $\leq$, wenn es eine Standarddarstellung $f = \sum_{i=1}^{s} a_i f_i + r$ von f durch $(f_1, \ldots, f_s)$ bezüglich $\leq$ gibt.

SATZ 10.31. *Sei* k *ein Körper und* G *eine Gröbnerbasis des Ideals* I *von* $k[x_1, \ldots, x_n]$. *Sei* $X = \{\boldsymbol{x}^\alpha | \alpha \in {\mathbb{N}_0}^n\}$. *Dann ist* $X \setminus \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ *eine Basis des* k*-Vektorraumes* $k[x_1, \ldots, x_n]/I$.

Beweis: Sei $f \in k[\boldsymbol{x}]$. Da f eine Standarddarstellung durch G mit Rest r besitzt, und da in einer Standarddarstellung kein Monom des Rests r in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ liegt, liegt $f + I = r + I$ in der linearen Hülle von $X \setminus \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Sei M eine endliche Teilmenge von $X \setminus \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ und $\sum_{m \in M} \alpha_m (m + I) = 0 + I$. Dann gilt $f := \sum_{m \in F} \alpha_m m \in I$. Somit ist $f = 0 + r$ mit $r = \sum_{m \in F} \alpha_m m$ eine Standarddarstellung von f durch G mit Rest r, und somit $r = 0$. Also sind alle $\alpha_m = 0$ und $X \setminus \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ daher linear unabhängig. □

KOROLLAR 10.32. *Sei* k *ein Körper und* G *eine Gröbnerbasis des Ideals* I *von* $k[x_1, \ldots, x_n]$. *Der* k*-Vektorraum* $k[x_1, \ldots, x_n]/I$ *ist genau dann endlichdimensional, wenn es für jedes* $j \in \underline{n}$ *ein* $d_j \in \mathbb{N}_0$ *gibt, sodass* $x_j^{d_j} \in \text{LT}(G)$.

Beweis: Sei $X = \{\boldsymbol{x}^\alpha | \alpha \in {\mathbb{N}_0}^n\}$. Wenn alle $x_j^{d_j} \in \text{LT}(G)$ sind, so gilt $X \setminus \langle LT(G) \rangle_{k[\boldsymbol{x}]} \subseteq \{\boldsymbol{x}^\alpha \mid \alpha_j < d_j \text{ für alle } j\}$. Somit hat $k[x_1, \ldots, x_n]$ eine endliche Basis.

Wenn $k[x_1, \ldots, x_n]/I$ Dimension d hat, so sind für jedes $j \in \underline{n}$ die Restklassen $1 + I, x_j + I, \ldots, x_j^d + I$ linear abhängig, und es gibt somit $f \in k[x_j]$ mit $f \neq 0$ und $f \in I$. Somit gibt es

$e_j \in \mathbb{N}_0$ mit $\text{LM}(f) = x_j^{e_j}$. Also gilt $x_j^{e_j} \in \langle \text{LT}(I)\rangle_{k[\boldsymbol{x}]} = \langle \text{LT}(G)\rangle_{k[\boldsymbol{x}]}$, und somit gibt es ein d_j, sodass $x_j^{d_j} \in \text{LT}(G)$

SATZ 10.33. *Sei k ein Körper, sei I ein Ideal von $k[\boldsymbol{x}]$ mit $1 \notin I$. Dann sind äquivalent:*

(1) *$k[x_1, \ldots, x_n]/I$ ist ein endlichdimensionaler Vektorraum über k.*
(2) *$k[x_1, \ldots, x_n]/I$ ist algebraisch über k.*
(3) *Jedes prime Ideal P von $k[\boldsymbol{x}]$ mit $I \subseteq P \subset k[\boldsymbol{x}]$ ist maximal.*

Beweis: (1)⇒(2). Sei $f + I \in k[\boldsymbol{x}]/I$ und sei d die Dimension von $k[\boldsymbol{x}]/I$ als Vektorraum über k. Dann sind $1+I, f+I, f^2+I, \ldots, f^d+I$ linear abhängig, und folglich gibt es $p(t) = \sum_{i=0}^{d} \alpha_i t^i$ mit $p(f + I) = 0$.

(2)⇒(3). Wir zeigen, dass für jedes $y \notin P$ das Element $y + P$ invertierbar in $k[\boldsymbol{x}]/P$ ist. Es gibt $f(t) = \sum_{i=0}^{m} \alpha_i t^i \in k[t] \setminus \{0\}$ mit $f(y + P) = 0 + P$, also $f(y) \in P$. Sei l minimal mit $\alpha_l \neq 0$. Dann gilt $f(y) = \sum_{i=l}^{m} \alpha_l y^l = y^l \sum_{i=l}^{m} \alpha_l y^{m-l}$. Da P prim ist und $y_l \notin P$, gilt $\alpha_l + y(\alpha_{l+1} + \cdots + \alpha_m y^{m-l-1}) \in P$, und somit ist $(y+P)\cdot(-\frac{1}{\alpha_l}(\alpha_{l+1} + \cdots + \alpha_m y^{m-l-1} + P) = 1+P$. Also ist $k[\boldsymbol{x}]/P$ ein Körper, und P somit maximal.

(3)⇒(2). Sei M ein maximales Ideal von $k[\boldsymbol{x}]$ mit $M \geq I$. Wegen des Nullstellensatzes gibt es einen Körper K, der algebraisch über k ist, und in dem M eine Nullstelle $(\xi_1, \ldots, \xi_n) \in K^n$ hat. Dann ist $k(\xi_1, \ldots, \xi_n)$ isomorph zu $k(x_1, \ldots, x_n)/M$, und $k(x_1, \ldots, x_n)/M$ somit algebraisch über k.

Sei nun $u \in k[\boldsymbol{x}]$. Aus der Primärzerlegung von I erhalten wir prime Ideale $P_1, \ldots, P_m$ von $k[\boldsymbol{x}]$ mit

$$\sqrt{I} = P_1 \cap \ldots \cap P_m.$$

Für jedes $j \in \underline{m}$ ist P_j maximal. Also ist $k(x_1, \ldots, x_n)/P_j$ algebraisch über k, und es gibt somit $f_j \in k[t] \setminus \{0\}$ mit $f_j(u) \in P_j$. Also gilt $\left(\prod_{j=1}^{m} f_j\right)(u) \in \sqrt{I}$, und somit gibt es $n \in \mathbb{N}$ mit $\left(\prod_{j=1}^{m} f_j\right)^n (u) \in I$.

(2)⇒(1). Sei G eine Gröbnerbasis von I. Für jedes x_j gibt es ein Polynom $p_j \in k[t]$ mit $p_j(x_j) \in I$. Sei d_j der Grad von p_j. Dann gilt $x_j^{d_j} \in \text{LT}(I) \subseteq \langle \text{LT}(G)\rangle_{k[\boldsymbol{x}]}$. Wegen Korollar 10.32 ist $k[x_1, \ldots, x_n]/I$ daher endlichdimensional. □

ÜBUNGSAUFGABEN 10.34

(1) Let k be a field , and let $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n] \setminus \{0\}$.
   (a) Show the following statment: If F is a Groebner basis of $\langle F\rangle$ and
   $$\text{LT}(f_i) \in \langle \text{LT}(f_1), \ldots, \text{LT}(f_{i-1}), \text{LT}(f_{i+1}), \ldots, \text{LT}(f_s)\rangle,$$
   then $F \setminus \{f_i\}$ is a Groebner basis of $\langle F\rangle$, too.
   (b) Is this assertion still valid if one replaces the words "Groebner basis" both times by "basis"?

5. Die Eliminationseigenschaft von Gröbnerbasen

Wir werden im folgenden oft Ordnungen verwenden, in denen Terme, die bestimmte Variablen enthalten, stets größer als jene Terme sind, die diese Variablen nicht enthalten.

DEFINITION 10.35. Sei $\leq$ eine zulässige Ordnung der Monome in $k[\boldsymbol{x}, \boldsymbol{y}]$. Wir sagen, dass $\leq$ eine *Blockordnung* mit $\boldsymbol{x}$ vor $\boldsymbol{y}$ ist, wenn sodass für alle $\alpha \in {\mathbb{N}_0}^m$ und $\beta \in {\mathbb{N}_0}^n$ mit $\alpha \neq (0, \ldots, 0)$ die Eigenschaft $\boldsymbol{x}^\alpha > \boldsymbol{y}^\beta$ gilt. Wir schreiben dann, dass die Ordnung $\boldsymbol{x} >> \boldsymbol{y}$ erfüllt.

SATZ 10.36. *Sei k ein Körper, sei I ein Ideal von $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$, sei $\leq$ eine Blockordnung mit $\boldsymbol{x} >> \boldsymbol{y}$ der Monome von $k[\boldsymbol{x}, \boldsymbol{y}]$, und sei G eine Gröbnerbasis von I bezüglich dieser Ordnung. Dann ist $G \cap k[\boldsymbol{y}]$ eine Gröbnerbasis des Ideals $I \cap k[\boldsymbol{y}]$ von $k[\boldsymbol{y}]$.*

Beweis: Sei $G_{\boldsymbol{y}} := G \cap k[\boldsymbol{y}]$. Wir zeigen nun, dass für alle $f \in I \cap k[\boldsymbol{y}]$ mit $f \neq 0$ auch $\mathrm{LT}(f) \in \langle \mathrm{LT}(G_{\boldsymbol{y}}) \rangle_{k[\boldsymbol{y}]}$ gilt. $f = \sum_{i=1}^{t} a_i g_i$ eine Standarddarstellung von f durch G. Da für alle i mit $a_i g_i \neq 0$ gilt, dass $\mathrm{DEG}(a_i g_i) \leq \mathrm{DEG}(f)$, und da in f keine der Variablen $x_1, \ldots, x_m$ vorkommt, kommt wegen der Eigenschaft der Ordnung auch in $a_i g_i$ keine der Variablen $x_1, \ldots, x_m$ vor. Es gilt also

$$f = \sum_{\substack{i=1 \\ a_i g_i \neq 0}}^{t} a_i g_i,$$

wobei alle in dieser Summe auftretenden a_i und g_i in $k[\boldsymbol{y}]$ liegen.

Für zumindest einen der Summanden muss $\mathrm{DEG}(a_j g_j) = \mathrm{DEG}(f)$ gelten. Dann gilt $\mathrm{LT}(g_j) | \mathrm{LT}(f)$ in $k[\boldsymbol{y}]$, und somit liegt $\mathrm{LT}(f)$ in $\langle \mathrm{LT}(G_{\boldsymbol{y}}) \rangle_{k[\boldsymbol{y}]}$. □

6. Existenz universeller Gröbnerbasen (optional)

Wir zeigen in dieser Sektion den folgenden Satz.

SATZ 10.37. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Dann gibt es eine endliche Teilmenge G von $k[x_1, \ldots, x_n]$, sodass G bezüglich jeder zulässigen Ordnung von ${\mathbb{N}_0}^n$ eine Gröbnerbasis ist.*

Dazu brauchen wir zunächst einen Satz über die Ordnungsfilter auf $\mathbb{N}_0^m$. Aus Satz 10.7 wissen wir bereits, dass es keine unendliche aufsteigende Kette $U_1 \subset U_2 \subset \cdots$ von Ordnungsfiltern auf ${\mathbb{N}_0}^m$ gibt. Wir zeigen nun, dass es auch keine unendlichen Antiketten von Ordnungsfiltern auf ${\mathbb{N}_0}^m$ gibt.

SATZ 10.38 (cf. [**Mac01**, Theorem 1.2]). *Sei $m \in \mathbb{N}$, und sei $\mathcal{L}$ die Menge der Ordnungsfilter von $\mathbb{N}_0^m$. Dann hat $(\mathcal{L}, \subseteq)$ keine unendliche Antikette.*

Beweis: Wenn $m = 1$, so ist die Menge der Ordnungsfilter linear geordnet; Antiketten haben höchstens ein Element.

Sei nun $m \geq 2$. Für jedes Ordnungsfilter F of $\mathbb{N}_0^m$ definieren wir eine Funktion $\Phi_F : \mathbb{N}_0^{m-1} \to \mathbb{N}_0 \cup \{\infty\}$ durch

$$\Phi_F(\boldsymbol{a}) := \begin{cases} \min\{c \in \mathbb{N}_0 \mid (\boldsymbol{a}, c) \in F\} & \text{wenn es ein } c' \in \mathbb{N} \text{ mit } (\boldsymbol{a}, c') \in F \text{ gibt ,} \\ \infty & \text{sonst.} \end{cases}$$

für $\boldsymbol{a} \in \mathbb{N}_0^{m-1}$. Wir zeigen zuerst, dass für alle $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}_0^{m-1}$ mit $\boldsymbol{a} \leq \boldsymbol{b}$ auch $\Phi_F(\boldsymbol{a}) \geq \Phi_F(\boldsymbol{b})$ gilt. Sei dazu $c := \Phi_F(\boldsymbol{a})$. Wir nehmen an, dass $c \neq \infty$. Es gilt $(\boldsymbol{a}, c) \in F$. Da F ein Ordnungsfilter ist, gilt auch $(\boldsymbol{b}, c) \in F$, und folglich $\Phi_F(\boldsymbol{b}) \leq c = \Phi_F(\boldsymbol{a})$. Außerdem gilt für Ordnungsfilter F, G of $\mathbb{N}_0^m$ die Inklusion $F \subseteq G$ genau dann, wenn $\Phi_F(\boldsymbol{a}) \geq \Phi_G(\boldsymbol{a})$ für alle $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}_0^{m-1}$.

Sei nun $\langle F_i \mid i \in \mathbb{N} \rangle$ eine unendliche Antikette in $\mathcal{L}$. Für $i, j \in \mathbb{N}$ mit $i < j$ gilt daher $F_j \not\subseteq F_i$. Daher gibt es ein $\boldsymbol{a}^{(i,j)} \in \mathbb{N}_0^{m-1}$, sodass

$$\Phi_{F_j}(\boldsymbol{a}^{(i,j)}) < \Phi_{F_i}(\boldsymbol{a}^{(i,j)}).$$

Für $i, j, k \in \mathbb{N}$ mit $i < j < k$ färben wir nun die 3-elementige Menge $\{i, j, k\}$ mit einer von 2^{m-1} Farben. Als Farben wählen wir die Funktionen von $\{1, \ldots, m-1\}$ nach $\{\mathbf{1}, \mathbf{2}\}$. Für $l \in \{1, \ldots, m-1\}$ bezeichnen wir die l-te Komponente von $\boldsymbol{a}^{(i,j)}$ mit $\boldsymbol{a}_l^{(i,j)}$. Wir definieren jetzt die Farbe von $\{i, j, k\}$ durch

$$C(\{i,j,k\})(l) := \begin{cases} \mathbf{1} & \text{, wenn } \boldsymbol{a}_l^{(i,j)} \leq \boldsymbol{a}_l^{(j,k)}, \\ \mathbf{2} & \text{, wenn } \boldsymbol{a}_l^{(i,j)} > \boldsymbol{a}_l^{(j,k)}. \end{cases}$$

Nach dem Satz von Ramsey (Satz 10.1 hat $\mathbb{N}$ eine unendliche Teilmenge T, sodass alle 3-elementigen Teilmengen von T die gleiche Farbe C haben. Wir zeigen nun, dass $C(l) = \mathbf{1}$ für alle $l \in \{1, \ldots, m-1\}$ gilt.

Im Widerspruch dazu nehmen wir an, dass es ein l mit $C(l) = \mathbf{2}$ gibt. Seien $t_1 < t_2 < t_3 \ldots$ die Elemente von T. Wenn $C(l) = \mathbf{2}$, so gilt

$$\boldsymbol{a}_l^{(t_1,t_2)} > \boldsymbol{a}_l^{(t_2,t_3)} > \boldsymbol{a}_l^{(t_3,t_4)} > \cdots .$$

Damit haben wir eine unendliche absteigende Kette natürlicher Zahlen konstruiert, was unmöglich ist.

Es gilt also für alle $r \in \mathbb{N}$ die Ungleichung $\boldsymbol{a}^{(t_r,t_{r+1})} \leq \boldsymbol{a}^{(t_{r+1},t_{r+2})}$. Sei nun $r \in \mathbb{N}$. Wegen der Wahl von $\boldsymbol{a}^{(t_r,t_{r+1})}$ gilt nun

$$\Phi_{F_{t_r}}(\boldsymbol{a}^{(t_r,t_{r+1})}) > \Phi_{F_{t_{r+1}}}(\boldsymbol{a}^{(t_r,t_{r+1})}).$$

Da $\boldsymbol{a}^{(t_r,t_{r+1})} \leq \boldsymbol{a}^{(t_{r+1},t_{r+2})}$, gilt auch

$$\Phi_{F_{t_{r+1}}}(\boldsymbol{a}^{(t_r,t_{r+1})}) \geq \Phi_{F_{t_{r+1}}}(\boldsymbol{a}^{(t_{r+1},t_{r+2})}).$$

Damit ist die Folge $\langle \Phi_{F_{t_i}}(\boldsymbol{a}^{(t_i,t_{i+1})}) \mid i \in \mathbb{N} \rangle$ eine unendliche absteigende Kette $\mathbb{N}_0 \cup \{\infty\}$, was unmöglich ist.

Folglich kann es keine unendliche Antikette $\langle F_i \mid i \in \mathbb{N} \rangle$ von Ordnungsfiltern von $\mathbb{N}_0^m$ geben. □

KOROLLAR 10.39. *Sei k ein Körper. Dann besitzt die Menge der monomialen Ideale von $k[x_1, \ldots, x_n]$ keine unendliche Antikette.*

Beweis: Wir ordnen jedem monomialen Ideal I von $k[x_1, \ldots, x_n]$ das Ordnungsfilter $F(I) := \{\alpha \in {\mathbb{N}_0}^n \mid \boldsymbol{x}^\alpha \in I\}$ zu.

Für monomiale Ideale mit $F(I) \subseteq F(J)$ gilt auch auch $I \subseteq J$: Sei dazu $p \in I$. Wegen Lemma 10.22 liegt jedes Monom von p in I. Also liegt der Exponent jedes Monoms in $F(I)$. Wegen

$F(I) \subseteq F(J)$ liegt der Exponent eines jeden Monoms von p auch in $F(J)$. Also liegt jedes Monom von p in J, also gilt auch $p \in J$.

Aufgrund dieser Eigenschaft ist F injektiv. Einer unendlichen Antikette in $k[x_1, \ldots, x_n]$ wird also durch F eine unendliche Antikette von Ordnungsfiltern auf ${\mathbb{N}_0}^n$ zugeordnet. Eine solche unendliche Antikette gibt es aber wegen Satz 10.38 nicht. □

Beweis von Satz 10.37: Wir bilden für jede zulässige Ordnung $\leq$ auf ${\mathbb{N}_0}^n$ die Menge

$$F(\leq) := \langle \mathrm{LT}_{\leq}(I) \rangle_{k[\boldsymbol{x}]}.$$

Die Menge

$$\mathcal{F} = \{ F(\leq) \mid \leq \text{ ist zulässig } \}$$

ist eine Menge von monomialen Idealen. Sei $\mathcal{F}_{\max}$ die Menge der maximalen Elemente von $\mathcal{F}$. Wegen Korollar 10.39 ist $\mathcal{F}_{\max}$ endlich.

Seien nun $\leq_1, \ldots, \leq_m$ zulässige Ordnungen, sodass $\mathcal{F}_{\max} = \{F(\leq_1), \ldots, F(\leq_m)\}$. Nach Satz 11.17 besitzt I nun bezüglich jeder dieser Ordnungen $\leq_i$ eine reduzierte Gröbnerbasis G_i. Sei nun $G = G_1 \cup \ldots \cup G_m$.

Es bleibt zu zeigen, dass G bezüglich jeder zulässigen Ordnung auf ${\mathbb{N}_0}^n$ eine Gröbnerbasis von I ist. Sei also $\leq$ eine zulässige Ordnung. Wir zeigen, dass für alle $f \in I$ mit $f \neq 0$ gilt, dass $\mathrm{LT}_{\leq}(f)$ in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$ liegt. Sei also $f \in I$. Da $\mathcal{F}$ die (ACC) erfüllt, ist $F(\leq)$ in einem maximalen Element von $\mathcal{F}$ als Teilmenge enthalten. Es gibt also ein $i \in \{1, \ldots, m\}$, sodass $F(\leq) \subseteq F(\leq_i)$ Klarerweise gilt $\mathrm{LT}_{\leq}(f) \in \mathrm{LT}_{\leq}(I)$, also auch $\mathrm{LT}_{\leq}(f) \in \langle \mathrm{LT}_{\leq}(I) \rangle_{k[\boldsymbol{x}]}$. Da $\langle \mathrm{LT}_{\leq}(I) \rangle_{k[\boldsymbol{x}]} \subseteq \langle \mathrm{LT}_{\leq_i}(I) \rangle_{k[\boldsymbol{x}]}$, gilt $\mathrm{LT}_{\leq}(f) \in \langle \mathrm{LT}_{\leq_i}(I) \rangle_{k[\boldsymbol{x}]}$. Nun ist G_i eine Gröbnerbasis bezüglich $\leq_i$. Somit liegt $\mathrm{LT}_{\leq}(f)$ in $\langle \mathrm{LT}_{\leq_i}(G_i) \rangle_{k[\boldsymbol{x}]}$. Es gibt also ein $g \in G_i$, sodass

$$\mathrm{LT}_{\leq_i}(g) | \mathrm{LT}_{\leq}(f).$$

Wir betrachten nun $\mathrm{LT}_{\leq}(g)$. Da $g \in I$, gilt $\mathrm{LT}_{\leq}(g) \in \mathrm{LT}_{\leq}(I)$. Da $\langle \mathrm{LT}_{\leq}(I) \rangle_{k[\boldsymbol{x}]} \subseteq \langle \mathrm{LT}_{\leq_i}(I) \rangle_{k[\boldsymbol{x}]}$, gilt somit auch

$$\mathrm{LT}_{\leq}(g) \in \langle \mathrm{LT}_{\leq_i}(I) \rangle.$$

Da G_i eine Gröbnerbasis von I bezüglich $\leq_i$ ist, gibt es ein $h \in G_i$, sodass $\mathrm{LT}_{\leq_i}(h) | \mathrm{LT}_{\leq}(g)$. Nun ist G_i eine reduzierte Gröbnerbasis. Daher ist kein Monom in g durch ein $\mathrm{LT}_{\leq_i}(g')$ mit $g' \in G_i \setminus \{g\}$ teilbar. Also gilt $g = h$. Dann gilt aber $\mathrm{LT}_{\leq_i}(g) | \mathrm{LT}_{\leq}(g)$. Da $\mathrm{LT}_{\leq_i}(g)$ maximal bezüglich Teilbarkeit unter den in g auftretenden Monomen ist, gilt $\mathrm{LT}_{\leq_i}(g) = \mathrm{LT}_{\leq}(g)$. Also gilt auch $\mathrm{LT}_{\leq}(g) | \mathrm{LT}_{\leq}(f)$, und somit $\mathrm{LT}_{\leq}(f) \in \langle \mathrm{LT}_{\leq}(G) \rangle_{k[\boldsymbol{x}]}$. □

KAPITEL 11

Konstruktion von Gröbnerbasen

1. Subtraktionspolynome und Buchbergers Algorithmus

Wir fixieren für die Sektionen 1 und 2 eine zulässige Ordnung $\leq$ auf ${\mathbb{N}_0}^n$.

DEFINITION 11.1. Sei k ein Körper, $n \in \mathbb{N}$. Seien $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n) \in {\mathbb{N}_0}^n$. Seien $\gamma = (\gamma_1, \ldots, \gamma_n)$ und $\delta = (\delta_1, \ldots, \delta_n)$ definiert durch $\gamma_i := \max(\alpha_i, \beta_i)$ und $\delta_i := \min(\alpha_i, \beta_i)$ für $i \in \{1, \ldots, n\}$. Wir definieren und durch $\textsc{Lcm}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta) := \boldsymbol{x}^\gamma$ und $\textsc{Gcd}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta) := \boldsymbol{x}^\delta$ Wir schreiben für $\textsc{Lcm}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta)$ auch kürzer $\boldsymbol{x}^\alpha \vee \boldsymbol{x}^\beta$ und für $\textsc{Gcd}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta)$ auch $\boldsymbol{x}^\alpha \wedge \boldsymbol{x}^\beta$.

DEFINITION 11.2. Sei k ein Körper, $n \in \mathbb{N}$, und seien $f, g \in k[x_1, \ldots, x_n] \setminus \{0\}$. Das *S-Polynom* oder *Subtraktionspolynom* von f und g ist definiert durch

$$S(f,g) := \frac{\textsc{Lm}(f) \vee \textsc{Lm}(g)}{\textsc{Lt}(f)} \cdot f - \frac{\textsc{Lm}(f) \vee \textsc{Lm}(g)}{\textsc{Lt}(g)} \cdot g.$$

Das S-Polynom kann auch durch

$$S(f,g) = \frac{\textsc{Lm}(g)}{\textsc{Lm}(f) \wedge \textsc{Lm}(g)} \frac{1}{\textsc{Lc}(f)} f - \frac{\textsc{Lm}(f)}{\textsc{Lm}(f) \wedge \textsc{Lm}(g)} \frac{1}{\textsc{Lc}(g)} g$$

oder

$$\textsc{Lc}(f)\, S(f,g) = \frac{\textsc{Lm}(g)}{\textsc{Lm}(f) \wedge \textsc{Lm}(g)} f - \frac{\textsc{Lc}(f)}{\textsc{Lc}(g)} \frac{\textsc{Lm}(f)}{\textsc{Lm}(f) \wedge \textsc{Lm}(g)} g \tag{11.1}$$

berechnet werden.

LEMMA 11.3. *Sei k ein Körper, $n \in \mathbb{N}$, und seien $f, g \in k[x_1, \ldots, x_n] \setminus \{0\}$. Sei γ so, dass $\boldsymbol{x}^\gamma = \textsc{Lcm}(\textsc{Lm}(f), \textsc{Lm}(g))$. Dann gilt $\textsc{Deg}(S(f,g)) < \gamma$.*

Beweis: Seien $f_1, g_1 \in k[x]$ so, dass $f = \textsc{Lt}(f) + f_1$ und $g = \textsc{Lt}(g) + g_1$. Dann gilt

$$\begin{aligned}
S(f,g) &= \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(f)}}{\textsc{Lc}(f)} \cdot f - \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(g)}}{\textsc{Lc}(g)} \cdot g \\
&= \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(f)}}{\textsc{Lc}(f)} \cdot \textsc{Lt}(f) - \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(g)}}{\textsc{Lc}(g)} \cdot \textsc{Lt}(g) + \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(f)}}{\textsc{Lc}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(g)}}{\textsc{Lc}(g)} \cdot g_1 \\
&= \boldsymbol{x}^{\gamma - \textsc{Deg}(f)} \cdot \textsc{Lm}(f) - \boldsymbol{x}^{\gamma - \textsc{Deg}(g)} \cdot \textsc{Lm}(g) + \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(f)}}{\textsc{Lc}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(g)}}{\textsc{Lc}(g)} \cdot g_1 \\
&= \boldsymbol{x}^\gamma - \boldsymbol{x}^\gamma + \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(f)}}{\textsc{Lc}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(g)}}{\textsc{Lc}(g)} \cdot g_1 \\
&= \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(f)}}{\textsc{Lc}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \textsc{Deg}(g)}}{\textsc{Lc}(g)} \cdot g_1.
\end{aligned}$$

Diese beiden Summanden haben wegen der Zulässigkeitseigenschaft (3) aus Definition 10.9 Multigrad $\leq \gamma$; keiner dieser Summanden hat Multigrad $= \gamma$. Die Summe hat also Multigrad $< \gamma$. □

LEMMA 11.4. *Seien $f, g, u, v \in k[\boldsymbol{x}]\backslash\{0\}$ so, dass $\mathrm{LM}(uf) = \mathrm{LM}(vg)$. Dann gibt es $a, b, c \in k[\boldsymbol{x}]$, sodass*

$$uf = a\,S(f,g) + bf + cg,$$

$\mathrm{DEG}(aS(f,g)) < \mathrm{DEG}(uf)$, $\mathrm{DEG}(bf) < \mathrm{DEG}(uf)$ und $\mathrm{DEG}(cg) = \mathrm{DEG}(uf)$.

Beweis: Es gilt

$$uf = \mathrm{LT}(u)f + (u - \mathrm{LT}(u))f.$$

Wir setzen $b := u - \mathrm{LT}(u)$. Weiters gilt $\mathrm{LT}(u)f = \mathrm{LC}(u)\mathrm{LM}(u)f$. Da $\mathrm{LM}(u)\mathrm{LM}(f) = \mathrm{LM}(v)\mathrm{LM}(g)$, gilt $\mathrm{LM}(g) \mid \mathrm{LM}(u)\mathrm{LM}(f)$. Sei δ so, dass

$$\boldsymbol{x}^\delta = \mathrm{GCD}(\mathrm{LM}(f), \mathrm{LM}(g)).$$

Dann gilt $\frac{\mathrm{LM}(g)}{\boldsymbol{x}^\delta} \mid \mathrm{LM}(u)\frac{\mathrm{LM}(f)}{\boldsymbol{x}^\delta}$. Es gilt also $\frac{\mathrm{LM}(g)}{\boldsymbol{x}^\delta} \mid \mathrm{LM}(u)$, und somit gibt es $\varepsilon \in \mathbb{N}_0^n$, sodass

$$\frac{\mathrm{LM}(g)}{\boldsymbol{x}^\delta}\boldsymbol{x}^\varepsilon = \mathrm{LM}(u).$$

Daher gilt $\mathrm{DEG}(u) = \mathrm{DEG}(g) - \delta + \varepsilon$. Nun gilt

$$\begin{aligned}\mathrm{LC}(u)\mathrm{LM}(u)f &= \mathrm{LC}(u)\frac{\mathrm{LM}(g)}{\boldsymbol{x}^\delta}\boldsymbol{x}^\varepsilon f \\ &= \mathrm{LC}(u)\boldsymbol{x}^\varepsilon(\frac{\mathrm{LM}(g)}{\boldsymbol{x}^\delta}f).\end{aligned}$$

Nach (11.1) ist das gleich

$$\mathrm{LC}(u)\boldsymbol{x}^\varepsilon\big(\mathrm{LC}(f)S(f,g) + \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)}\frac{\mathrm{LM}(f)}{\boldsymbol{x}^\delta}g\big) \tag{11.2}$$
$$= \mathrm{LC}(u)\mathrm{LC}(f)\boldsymbol{x}^\varepsilon S(f,g) + \mathrm{LC}(u)\boldsymbol{x}^\varepsilon\frac{\mathrm{LC}(f)}{\mathrm{LC}(g)}\frac{\mathrm{LM}(f)}{\boldsymbol{x}^\delta}g.$$

Wir bestimmen nun die Grade der Summanden: Es gilt $\mathrm{DEG}(\boldsymbol{x}^\varepsilon S(f,g)) \leq \varepsilon + \mathrm{DEG}(S(f,g)) < \varepsilon + \mathrm{DEG}(f) + \mathrm{DEG}(g) - \delta = \mathrm{DEG}(f) + \mathrm{DEG}(u) = \mathrm{DEG}(uf)$. Weiters gilt $\mathrm{DEG}(\boldsymbol{x}^\varepsilon\frac{\mathrm{LM}(f)}{\boldsymbol{x}^\delta}g) = \varepsilon + \mathrm{DEG}(f) + \mathrm{DEG}(g) - \delta = \mathrm{DEG}(uf)$. Somit leisten

$$\begin{aligned} a &:= \mathrm{LC}(u)\mathrm{LC}(f)\boldsymbol{x}^\varepsilon, \\ b &:= (u - \mathrm{LT}(u)), \\ c &:= \tfrac{\mathrm{LC}(u)\mathrm{LC}(f)}{\mathrm{LC}(g)}\boldsymbol{x}^\varepsilon\tfrac{\mathrm{LM}(f)}{\boldsymbol{x}^\delta}\end{aligned}$$

das Gewünschte. □

SATZ 11.5 (Buchbergers Kriterium, cf. [Buc70]). *Sei k ein Körper, seien $n, t \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $G = \{g_1, \ldots, g_t\}$ eine endliche Teilmenge von $I \setminus \{0\}$, sodass folgendes gilt:*

(1) $\langle G\rangle_{k[\boldsymbol{x}]} = I$,
(2) *Für alle $i, j \in \{1, \ldots, t\}$ mit $i < j$ ist 0 ein möglicher Rest einer Standarddarstellung von $S(g_i, g_j)$ durch $(g_1, \ldots, g_t)$.*

Dann ist G eine Gröbnerbasis von I.

Beweis: Sei $f \in I$ mit $f \neq 0$. Wir zeigen, dass $\mathrm{LT}(f)$ im Ideal $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle_{k[\boldsymbol{x}]}$ liegt. Da G das Ideal I erzeugt, gibt es $h'_1, \ldots, h'_t \in k[x_1, \ldots, x_n]$, sodass

$$f = \sum_{i=1}^{t} h'_i g_i.$$

Für jede solche Darstellung sei

$$\delta' := \max\{\mathrm{DEG}(h'_i g_i) \mid i \in \{1, \ldots, t\}\}$$

und

$$\eta' := \#\{i \in \{1, \ldots, t\} \mid \mathrm{DEG}(h'_i g_i) = \delta'\}.$$

Wir wählen nun jene Darstellungen von f als $\sum_{i=1}^{t} h'_i f_i$ aus, für die δ' minimal bezüglich der zulässigen Ordnung $\leq$ ist. Unter diesen Darstellungen mit Maximalgrad δ' wählen wir $h_1, \ldots, h_t \in k[x_1, \ldots, x_n]$ so aus, dass auch η' minimal ist. Sei also

$$\begin{aligned} \delta &:= \max\{\mathrm{DEG}(h_i g_i) \mid i \in \{1, \ldots, t\}\}, \\ \eta &:= \#\{i \in \{1, \ldots, t\} \mid \mathrm{DEG}(h_i g_i) = \delta\}. \end{aligned}$$

Es gilt dann $f = \sum_{i=1}^{t} h_i g_i$.

1. Fall: $\eta = 1$: Sei $i \in \{1, \ldots, t\}$ so, dass $\mathrm{DEG}(h_i g_i) = \delta$. Da für $j \neq i$ gilt, dass $\mathrm{DEG}(h_j g_j) < \delta$, erhalten wir $\mathrm{DEG}(f) = \delta$, und somit $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$.

2. Fall: $\eta \geq 2$: Seien $i, j \in \{1, \ldots, t\}$ so, dass $i < j$ und $\mathrm{DEG}(h_i g_i) = \mathrm{DEG}(h_j g_j) = \delta$. Nach Lemma 11.4 gibt es $a, b, c \in k[\boldsymbol{x}]$ mit $\mathrm{DEG}(aS(g_i, g_j)) < \delta$, $\mathrm{DEG}(bg_i) < \delta$, $\mathrm{DEG}(cg_j) = \delta$ und $h_i g_i = aS(g_i, g_j) + bg_i + cg_j$.

Da $S(g_i, g_j)$ nach Voraussetzung eine Standarddarstellung mit Rest 0 besitzt, gibt es Polynome $d_1, \ldots, d_t \in k[\boldsymbol{x}]$, sodass

$$S(g_i, g_j) = \sum_{l=1}^{t} d_l g_l,$$

und $\mathrm{DEG}(d_l g_l) \leq \mathrm{DEG}(S(g_i, g_j))$ für alle $l \in \{1, \ldots, t\}$. Dann gilt $h_i g_i = (\sum_{l=1}^{t} a d_l g_l) + bg_i + cg_j$ und somit

$$\begin{aligned} \sum_{l=1}^{t} h_l g_l &= \Big(\sum_{l \in \{1,\ldots,t\} \setminus \{i\}} h_l g_l\Big) + \Big(\sum_{l=1}^{t} a d_l g_l\Big) + bg_i + cg_j \\ &= \sum_{l \in \{1,\ldots,t\} \setminus \{i,j\}} (h_l + a d_l) g_l + (b + a d_i) g_i + (h_j + c + a d_j) g_j. \end{aligned} \tag{11.3}$$

Für alle $l \in \{1, \ldots, t\}$ gilt $\mathrm{DEG}(a d_l g_l) \leq \mathrm{DEG}(aS(g_i, g_j)) < \mathrm{DEG}(h_i g_i) = \delta$. Außerdem gilt $\mathrm{DEG}(bg_i) < \delta$ und $\mathrm{DEG}((h_j + c + a d_j) g_j) \leq \delta$. Im Fall

$$\mathrm{DEG}((h_j + c + a d_j) g_j) < \delta$$

erhalten wir also eine Darstellung mit kleinerem δ'; im Fall

$$\mathrm{DEG}((h_j + c + a d_j) g_j) = \delta$$

eine Darstellung von f mit gleichem δ', aber kleinerem η'. □

Das Hinzufügen eines möglichen Restes des betrachteten S-Polynoms bewirkt, dass dieses S-Polynom 0 als möglichen Rest hat:

LEMMA 11.6. *Sei k ein Körper, $n \in \mathbb{N}$, sei $(f_1, \ldots, f_s)$ eine Folge von Polynomen aus $k[x_1, \ldots, x_n]$. Sei $f \in k[x_1, \ldots, x_n]$, und sei $r \in k[x_1, \ldots, x_n]$ ein möglicher Rest von f bei einer Standarddarstellung von f durch $(f_1, \ldots, f_s)$. Dann ist 0 ein möglicher Rest von f bei einer Standarddarstellung von f durch $(f_1, \ldots, f_s, r)$.*

Beweis: Sei $f = \sum_{i=1}^{s} a_i f_i + r$ eine Standarddarstellung von f durch $(f_1, \ldots, f_s)$. Da $r = f - \sum_{i=1}^{s} a_i f_i$, gilt $\text{DEG}(r) \leq \text{DEG}(f)$. Also ist $f = \sum_{i=1}^{s} a_i f_i + 1r + 0$ eine Standarddarstellung von f durch $(f_1, \ldots, f_s, r)$ mit Rest 0. □

ALGORITHMUS 11.7 (Buchbergers Algorithmus zur Konstruktion einer Gröbnerbasis).
Eingabe: $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$.
Ausgabe: $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ so, dass $G := \{g_1, \ldots, g_t\}$ eine Gröbnerbasis für $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$ ist.

1: $G \leftarrow (f_1, \ldots, f_s)$
2: $P \leftarrow \varnothing$
3: **while** $\exists f, g \in G : f \neq g$ und $\{f, g\} \notin P$ **do**
4: $\quad P \leftarrow P \cup \big\{\{f, g\}\big\}$
5: $\quad r \leftarrow \begin{cases} \text{Ein möglicher Rest von } S(f,g) \\ \text{bei Standarddarstellung durch } G \end{cases}$
6: $\quad$ **if** $r \neq 0$ **then**
7: $\quad\quad G \leftarrow (G, r)$

SATZ 11.8. *Sei k ein Körper, und seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$. Der Algorithmus 11.7 terminiert und liefert als Ergebnis eine Gröbnerbasis für $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$.*

Beweis: Wir zeigen als erstes, dass der Algorithmus terminiert. Wir betrachten am Beginn jedes Durchlaufs der *while*-Schleife das Paar $(\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}, |\binom{G}{2} \setminus P|)$. Nehmen wir an, die Schleife würde unendlich oft durchlaufen. Wegen des Hilbertschen Basissatzes gibt es keine unendlichen aufsteigenden Ketten von Idealen von $k[x_1, \ldots, x_n]$.

Ab irgendeinem Durchlauf bleibt also $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ konstant. Ab diesem Durchlauf der Schleife kann aber der Fall $r \neq 0$ nicht mehr eintreten. Wenn nämlich r ein möglicher Rest von $S(f, g)$ bei einer Standarddarstellung durch G ist, und $r \neq 0$, so liegt $\text{LT}(r)$ nicht in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Dann gilt aber $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]} \neq \langle \text{LT}(G \cup \{r\}) \rangle_{k[\boldsymbol{x}]}$.

Folglich erniedrigt sich ab diesem Durchlauf die zweite Komponente $|\binom{G}{2} \setminus P|$. Diese Komponente kann nicht negativ werden.

Somit kann die *while*-Schleife nicht unendlich oft durchlaufen werden, also terminiert der Algorithmus.

Wir zeigen nun die Korrektheit des Algorithmus: Am Beginn jedes Durchlaufs der *while*-Schleife gilt, dass für alle $f, g \in G$ mit $\{f, g\} \in P$ das S-Polynom $S(f, g)$ eine Standarddarstellung durch

G mit Rest 0 hat. Das gilt offensichtlich beim ersten Betreten der *while*-Schleife wegen $P = \varnothing$. Im weiteren Verlauf garantiert Lemma 11.6, das diese Bedingung erhalten bleibt.

Wenn die *while*-Schleife verlassen wird, liegen alle Elemente aus $\binom{G}{2}$ in P. Folglich haben alle S-Polynome von Paaren von Polynomen aus G das Polynom 0 als möglichen Rest bei Standarddarstellung durch G. Nach Satz 11.5 ist G daher eine Gröbnerbasis von $\langle G\rangle_{k[\boldsymbol{x}]}$. $\langle G\rangle_{k[\boldsymbol{x}]}$ ist aber während des gesamten Verlaufs des Algorithmus stets $\langle f_1, \ldots, f_s\rangle_{k[\boldsymbol{x}]}$. □

Das folgende Kriterium erspart die Überprüfung der S-Polynome jener Paare, deren führende Monome keine gemeinsamen Variablen enthalten.

LEMMA 11.9. *Sei k ein Körper, sei F eine endliche Teilmenge von $k[x_1, \ldots, x_n]$, und seien $f, g \in F \setminus \{0\}$ so, dass $\operatorname{LCM}(\operatorname{LM}(f), \operatorname{LM}(g)) = \operatorname{LM}(f) \cdot \operatorname{LM}(g)$. Dann ist 0 ein möglicher Rest von $S(f, g)$ bei Standarddarstellung durch F.*

Beweis: Sei $p := f - \operatorname{LT}(f)$ und $q := g - \operatorname{LT}(g)$. Dann gilt

$$\begin{aligned} S(f,g) &= \frac{\operatorname{LM}(g)}{\operatorname{LC}(f)} f - \frac{\operatorname{LM}(f)}{\operatorname{LC}(g)} g \\ &= \frac{\operatorname{LT}(g)}{\operatorname{LC}(f)\operatorname{LC}(g)} f - \frac{\operatorname{LT}(f)}{\operatorname{LC}(f)\operatorname{LC}(g)} g \\ &= \frac{1}{\operatorname{LC}(f)\operatorname{LC}(g)} (\operatorname{LT}(g) f - \operatorname{LT}(f) g). \end{aligned}$$

Es gilt

$$\begin{aligned} \operatorname{LT}(g) f - \operatorname{LT}(f) g &= (g - q) f - (f - p) g \\ &= -qf + pg. \end{aligned}$$

Wir behaupten nun, dass $(-q)f + pg + 0$ eine Standarddastellung von $\operatorname{LT}(g)f - \operatorname{LT}(f)g$ durch (f, g) ist. Wenn $p = 0$, so ist $(-q)f + 0$ eine Standarddarstellulng von $-qf = \operatorname{LT}(g)f - \operatorname{LT}(f)g$.

Wir nehmen nun an, dass $p \neq 0$ und betrachten zuerst den Fall, dass $\operatorname{DEG}(qf) = \operatorname{DEG}(pg)$. Dann gilt $\operatorname{LM}(f) \mid \operatorname{LM}(p)\operatorname{LM}(g)$. Da $\operatorname{LM}(f)$ und $\operatorname{LM}(g)$ keine gemeinsamen Variablen enthalten, gilt $\operatorname{LM}(f) \mid \operatorname{LM}(p)$. Das steht aber im Widerspruch zu $\operatorname{DEG}(p) < \operatorname{DEG}(f)$.

Somit gilt $\operatorname{DEG}(qf) \neq \operatorname{DEG}(pg)$. Damit gilt aber $\operatorname{DEG}(-qf + pg) = \max(\operatorname{DEG}(-qf), \operatorname{DEG}(pg))$. Somit gilt $\operatorname{DEG}(-qf) \leq \operatorname{DEG}(-qf + pg)$ und $\operatorname{DEG}(pg) \leq \operatorname{DEG}(-qf + pg)$. Damit ist aber $(-q)f + pg + 0$ eine Standarddarstellung von $-qf + pg$ durch (f, g) mit Rest 0. □

ÜBUNGSAUFGABEN 11.10

(1) Use Buchberger's criterion to check whether the following sets F are Groebner bases for the ideals $\langle F\rangle_{k[\boldsymbol{x}]}$ they generate.
   (a) $F = \{x^2y + z, yz + 1\}$, lexicographic order, $x > y > z$.
   (b) $F = \{x^2y + z, yz + 1\}$, lexicographic order, $z > y > x$.
   (c) $F = \{x^5y^3, 3x + xy\}$, lexicographic order, $y > x$.
   (d) $F = \{x^2y^3, x^4y, x^3y^2, x^3y^3\}$, lexicographic order, $x > y$.

(2) Let k be a field, and let $f \in k[x_1, \ldots, x_n]$. Show that $\{f\}$ is a Groebner basis for the ideal $\langle f\rangle_{k[\boldsymbol{x}]}$. Can you give a proof that does not use the S-polynomial criterion?

(3) Let G be a finite set of monomials. Show that these monomials form a Groebner basis for the ideal they generate (with respect to every monomial order).
(4) Berechnen Sie eine Gröbnerbasis des Ideals $\langle -1 - x\,y + y^2 + x\,y^2,\ -1 + y^2\rangle$ mit lexikographischer Ordnung $x > y$.
(5) Berechnen Sie eine Gröbnerbasis des Ideals $\langle -1 + a\,b + a^2\,c,\ 2 + b\,c^3\rangle$, mit lexikographischer Ordnung $a > b > c$.
(6) Seien $f_1, f_2, f_3 \in \mathbb{R}[t_1, t_2]$ gegeben durch

$$\begin{aligned} f_1(t_1,t_2) &= {t_1}^2 \\ f_2(t_1,t_2) &= {t_2}^2 \\ f_3(t_1,t_2) &= t_1 \cdot t_2. \end{aligned}$$

Sei I das Ideal von $\mathbb{R}[x_1, x_2, x_3, t_1, t_2]$, das durch $\{x_1 - f_1(t_1,t_2), x_2 - f_2(t_1,t_2), x_3 - f_3(t_1,t_2)\}$ erzeugt wird. Berechnen Sie mit Hilfe der Eliminationseigenschaft von Gröbnerbasen Erzeuger von $I \cap \mathbb{R}[t_1, t_2]$ und $I \cap \mathbb{R}[x_1, x_2, x_3]$.
(7) In this exercise, we verify the claim of Lemma 11.4 in a concrete example. Let

$$\begin{aligned} u &= xy + 4 \\ f &= x^3 + xy \\ v &= x^2y - 3x \\ g &= x^2 + xy^2. \end{aligned}$$

Find $a, b, c \in \mathbb{Q}[x, y]$ such that

$$uf = a\,S(f,g) + bf + cg,$$

$\textsc{Deg}(aS(f,g)) < \textsc{Deg}(uf)$, $\textsc{Deg}(bf) < \textsc{Deg}(uf)$, and $\textsc{Deg}(cg) = \textsc{Deg}(uf)$.
(8) Compute a Gröbner basis of the following ideal I of $\mathbb{Q}[x, y]$ with respect to the lexicographic ordering, $x > y$, where

$$I = \langle -1 - x\,y + y^2 + x\,y^2,\ -1 + y^2\rangle.$$

(9) Compute a Gröbner basis of $\langle a^2b+c+1, a^2c+b\rangle$ in $\mathbb{Q}[a, b, c]$ with respect to the lexicographic ordering, $a > b > c$.
(10) A *binomial* is a polynomial which contains exactly two monomials, such as $xy^2 + 5xy^3z$. Show that an ideal that is generated by monomials and binomials has a Gröbner basis containing only monomials and binomials.
(11) Let I be the ideal of $\mathbb{Q}[x, y]$ generated by $\{x + y^2 + 2, xy + 3\}$. Find generators of the ideals $I \cap \mathbb{Q}[x]$ and $I \cap \mathbb{Q}[y]$ of $\mathbb{Q}[x]$ and $\mathbb{Q}[y]$, respectively.

2. Konstruktion von reduzierten Gröbnerbasen

In dieser Sektion stellen wir einige Resultate zusammen, die es uns erlauben, die Zwischenergebnisse beim Berechnen einer Gröbnerbasis zu vereinfachen. Als Resultate erhalten wir "reduzierte Gröbnerbasen".

LEMMA 11.11. *Seien $f_1, \ldots, f_s$ paarweise verschiedene Elemente von $k[x_1, \ldots, x_n]$, und sei $F := \{f_1, \ldots, f_s\}$. Sei $i \in \{1, \ldots, s\}$, und sei $r_i \in k[x_1, \ldots, x_n]$ ein möglicher Rest von f_i bei einer Standarddarstellung durch $F \setminus \{f_i\}$. Sei $G := (F \setminus \{f_i\}) \cup \{r_i\}$. Dann gilt:*

(1) $\langle G\rangle_{k[\boldsymbol{x}]} = \langle F\rangle_{k[\boldsymbol{x}]}$,
(2) $\langle \textsc{Lt}(F)\rangle_{k[\boldsymbol{x}]} \subseteq \langle \textsc{Lt}(G)\rangle_{k[\boldsymbol{x}]}$,
(3) *Wenn $r_i \neq 0$ und $\textsc{Lm}(r_i) \neq \textsc{Lm}(f_i)$, so gilt $\textsc{Lt}(r_i) \notin \langle \textsc{Lt}(F)\rangle_{k[\boldsymbol{x}]}$.*

(4) *Für alle $q \in k[\boldsymbol{x}]$ gilt: Wenn 0 ein möglicher Rest von q bei einer Standarddarstellung durch F ist, so ist 0 auch ein möglicher Rest von q bei einer Standarddarstellung durch G.*

Beweis: (1) Für $\subseteq$ beobachten wir, dass r_i in $\langle F\rangle_{k[\boldsymbol{x}]}$ liegt. Somit gilt $G \subseteq \langle F\rangle_{k[\boldsymbol{x}]}$. Für $\supseteq$ zeigen wir, $f_i \in \langle G\rangle_{k[\boldsymbol{x}]}$. Wir wissen, dass es $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_s \in k[\boldsymbol{x}]$ gibt, sodass

$$f_i = \sum_{\substack{j=1 \\ j\neq i}}^{s} a_j f_j + r_i.$$

Da $r_i \in G$, gilt $f_i \in \langle G\rangle_{k[\boldsymbol{x}]}$.

(2) Es reicht zu zeigen, dass im Fall $f_i \neq 0$ gilt, dass $\mathrm{LT}(f_i) \in \mathrm{LT}(G)$ liegt. Wir wissen, dass f_i eine Standarddarstellung durch $F \setminus \{f_i\}$ mit Rest r_i besitzt. Somit gibt es $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_s \in k[\boldsymbol{x}]$, sodass

$$f_i = \sum_{\substack{j=1 \\ j\neq i}}^{s} a_j f_j + r_i,$$

und alle Summanden auf der rechten Seite Multigrad $\leq \mathrm{DEG}(f_i)$ haben. Einer der Summanden muss daher Multigrad $\mathrm{DEG}(f_i)$ haben. Ist das $a_j f_j$ für ein $j \neq i$, so gilt $\mathrm{LT}(f_j)|\mathrm{LT}(f_i)$, und somit $\mathrm{LT}(f_i) \in \langle \mathrm{LT}(G)\rangle_{k[\boldsymbol{x}]}$. Wenn $\mathrm{DEG}(r_i) = \mathrm{DEG}(f_i)$, so gilt $\mathrm{LT}(r_i)|\mathrm{LT}(f_i)$, und folglich $\mathrm{LT}(f_i) \in \langle \mathrm{LT}(G)\rangle_{k[\boldsymbol{x}]}$.

(3) Wir nehmen an, dass $r_i \neq 0$. Wenn nun $\mathrm{LT}(r_i) \in \langle \mathrm{LT}(F)\rangle_{k[\boldsymbol{x}]}$, so gibt es ein $k \in \{1, \ldots, s\}$, sodass $\mathrm{LT}(f_k)|\mathrm{LT}(r_i)$. Da r_i ein möglicher Rest einer Standarddarstellung durch $F \setminus \{f_i\}$ ist, muss $k = i$ sein. Es gilt also $\mathrm{LT}(f_i)|\mathrm{LT}(r_i)$, und folglich $\mathrm{DEG}(f_i) \leq \mathrm{DEG}(r_i)$. Da r_i Rest einer Standarddarstellung von f_i ist, gilt aber auch $\mathrm{DEG}(r_i) \leq \mathrm{DEG}(f_i)$. Somit gilt $\mathrm{DEG}(r_i) = \mathrm{DEG}(f_i)$, und somit $\mathrm{LM}(r_i) = \mathrm{LM}(f_i)$.

(4) Wir nehmen an, dass q eine Standarddarstellung

$$q = \sum_{j=1}^{s} a_j f_j + 0$$

durch F mit Rest 0 besitzt. Weiters besitzt f_i eine Standarddarstellung durch $F \setminus \{f_i\}$ mit Rest r_i; es gibt also $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_s$, sodass

$$f_i = \sum_{\substack{l=1 \\ l\neq i}}^{s} b_l f_l + r_i.$$

Insgesamt gilt also

$$q = \sum_{j=1}^{s} a_j f_j + a_i\Big(\sum_{\substack{l=1 \\ l\neq i}}^{s} b_l f_l + r_i\Big),$$

also

$$q = \sum_{\substack{j=1 \\ j\neq i}}^{s} (a_j + a_i b_j) f_j + a_i r_i. \tag{11.4}$$

Es gilt $\text{DEG}(b_j f_j) \leq \text{DEG}(f_i)$, also auch $\text{DEG}(a_i b_j f_j) \leq \text{DEG}(a_i f_i) \leq \text{DEG}(q)$. Wegen $\text{DEG}(r_i) \leq \text{DEG}(f_i)$ gilt auch $\text{DEG}(a_i r_i) \leq \text{DEG}(a_i f_i) \leq \text{DEG}(q)$. Also ist die Darstellung von q in (11.4) eine Standarddastellung von q durch G. □

DEFINITION 11.12. Sei F eine endliche Teilmenge von $k[x_1, \ldots, x_n] \setminus \{0\}$, und sei $f \in F$. Dann ist f *reduziert in* F, wenn kein Monom in f durch ein $\text{LT}(g)$ mit $g \in F \setminus \{f\}$ teilbar ist.

Das Polynom f ist also reduziert in F, wenn

$$f = \sum_{\substack{g\in F \\ g\neq f}} 0 \cdot g + f$$

eine Standarddarstellung von f durch $F \setminus \{f\}$ mit Rest f ist.

DEFINITION 11.13. Sei F eine endliche Teilmenge von $k[x_1, \ldots, x_n] \setminus \{0\}$. F ist *reduziert*, wenn alle $f \in F$ reduziert in F sind.

Wir betrachten nun folgende Prozedur zur Erzeugung einer Gröbnerbasis.

ALGORITHMUS 11.14 (Erzeugen einer Gröbnerbasis mit Vereinfachung).
Eingabe: $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$.
Ausgabe: $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ so, dass $G := \{g_1, \ldots, g_t\}$ eine Gröbnerbasis für $\langle \{f_1, \ldots, f_s\} \rangle_{k[\boldsymbol{x}]}$ ist.

1: $G \leftarrow (f_1, \ldots, f_s)$
2: $P \leftarrow \varnothing$
3: **while** $\exists f, g \in G : f \neq g$ und $\{f, g\} \notin P$ **do**
4: $\quad P \leftarrow P \cup \big\{\{f, g\}\big\}$
5: $\quad r \leftarrow$ Ein möglicher Rest von $S(f, g)$ bei Standarddarstellung durch G
6: $\quad$ **if** $r \neq 0$ **then**
7: $\quad\quad G \leftarrow (G, r)$
8: $\quad$ **while** G ist nicht reduziert und wir wollen G reduzieren **do**
9: $\quad\quad f_1 \leftarrow$ Ein Element von G, das in G nicht reduziert ist
10: $\quad\quad r_1 \leftarrow$ Ein möglicher Rest von f_1 bei Standarddarstellung durch $G \setminus \{f_1\}$
11: $\quad\quad$ **if** $r_1 = 0$ **then**
12: $\quad\quad\quad G \leftarrow G \setminus \{f_1\}$
13: $\quad\quad$ **else**
14: $\quad\quad\quad G \leftarrow (G \setminus \{f_1\}) \cup \{r_1\}$

SATZ 11.15. *Unabhängig davon, wie oft wir im Ablauf des Algorithmus reduzieren wollen, terminiert der Algorithmus 11.14 und liefert eine Gröbnerbasis von* $I := \langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$.

Beweis: Am Beginn jedes Durchlaufs der äußeren *while*-Schleife gilt für alle $\{f, g\} \in P$, dass $S(f, g)$ eine Standarddarstellung durch G mit Rest 0 besitzt, und dass $\langle G \rangle_{k[\boldsymbol{x}]} = I$ ist: klarerweise gilt das beim ersten Betreten der *while*-Schleife. Wegen Lemma 11.6 bleiben diese Bedingungen auch durch das Hinzufügen des Restes r des S-Polynoms $S(f, g)$ erhalten. Nun bleibt diese Bedingung auch bei jedem Durchlauf der inneren *while*-Schleife erhalten: Lemma 11.11 (1) liefert, dass $\langle G \rangle_{k[\boldsymbol{x}]}$ immer gleich dem Ideal I ist. Lemma 11.11 (4) garantiert, dass die S-Polynome aller Paare aus P auch nach dem Reduzieren 0 als möglichen Rest haben. Wenn der Algorithmus terminiert, so wurde die äußere *while*-Schleife verlassen: für alle $\{f, g\} \in \binom{G}{2}$ gilt also $\{f, g\} \in P$; somit hat $S(f, g)$ eine Standarddarstellung durch G mit Rest 0. Nach Satz 11.5 ist G also eine Gröbnerbasis von $\langle G \rangle_{k[\boldsymbol{x}]} = I$.

Wir zeigen nun, dass der Algorithmus für jede Eingabe terminiert. Sei dazu $F = (f_1, \ldots, f_s)$ eine Eingabe, und seien unsere möglichen Wahlen während des Ablaufs des Algorithmus so, dass der Algorithmus nicht hält. Nun betrachten wir zunächst nach jedem Betreten einer der *while*-Schleifen das Ideal $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Wegen Lemma 11.11 (2) wird dieses Ideal von einem Betreten zum nächsten echt größer, oder es bleibt gleich. Da $k[\boldsymbol{x}]$ die (ACC) für Ideale erfüllt, bleibt dieses Ideal ab irgendwann stets konstant.

Ab diesem Punkt betrachten wir die Anzahl der Elemente von G, die in G nicht reduziert sind. Wir behaupten, dass ab diesem Durchlauf die Anzahl der nicht reduzierten Elemente in G nicht mehr größer wird. Zunächst kann ab diesem Durchlauf der Schleife der Fall $r \neq 0$ nicht mehr eintreten. Wenn nämlich r ein möglicher Rest von $S(f, g)$ bei einer Standarddarstellung durch G ist, und $r \neq 0$, so liegt $\text{LT}(r)$ nicht in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Dann gilt aber $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]} \neq \langle \text{LT}(G \cup \{r\}) \rangle_{k[\boldsymbol{x}]}$. Nun überlegen wir uns, warum auch die Anweisungen in der inneren *while*-Schleife die Anzahl der nicht reduzierten Elemente von G nicht erhöhen: Alle in G reduzierten Elemente von $G \setminus \{f_1\}$ sind auch reduziert in $G \setminus \{f_1\}$. Also könnte nur die Anweisung $G \leftarrow (G \setminus \{f_1\}) \cup \{r_1\}$ die Anzahl der nicht reduzierten Elemente von G erhöhen. In diesem Fall gilt $r_1 \neq 0$. Da ja $\text{LT}(G)$ konstant bleibt, bleibt wegen Lemma 11.11 (3) nur mehr der Fall $\text{LM}(r_1) = \text{LM}(f_1)$ übrig. Dann ist aber jedes Element von $(G \setminus \{f_1\}) \cup \{r_1\}$, das in $(G \setminus \{f_1\}) \cup \{r_1\}$ nicht reduziert ist, auch in G nicht reduziert. Keine Anweisung kann also die Anzahl der in G nicht reduzierten Elemente von G mehr erhöhen. Ab irgendeinem Durchlauf bleibt also auch die Anzahl der in G nicht reduzierten Elemente von G konstant.

Ab diesem Durchlauf betrachten wir $|G| + |\binom{G}{2} \setminus P|$. Von den Zuweisungen an G kann nun einzig die Zuweisung $G \leftarrow G \setminus \{f_1\}$ noch ausgeführt werden, da die Zuweisung $G \leftarrow (G \setminus \{f_1\}) \cup \{r_1\}$ ja bewirkt, dass die Anzahl der nicht reduzierten Elemente von G wegen $\text{LM}(r_1) = \text{LM}(f_1)$ um 1 kleiner wird, im Widerspruch dazu, dass die Anzahl der in G nicht reduzierten Elemente konstant bleibt. Jede der Zuweisungen $G \leftarrow G \setminus \{f_1\}$ und $P \leftarrow P \cup \{\{f, g\}\}$ bewirkt aber, dass $|G| + |\binom{G}{2} \setminus P|$ echt kleiner wird. Das kann aber nur endlich oft Also hält der Algorithmus nach diesen endlichen vielen Schritten. □

Wenn wir immer reduzieren wollen, und die führenden Koeffizienten des Ergebnisses auf 1 normieren, so erhalten wir als Ergebnis des Algorithmus 11.14 eine "reduzierte Gröbnerbasis".

DEFINITION 11.16. Sei k ein Körper, und sei G eine endliche Teilmenge von $k[x_1, \ldots, x_n] \setminus \{0\}$. G ist eine *reduzierte Gröbnerbasis* von $\langle G \rangle_{k[\boldsymbol{x}]}$, wenn:

(1) G ist eine Gröbnerbasis von $\langle G \rangle_{k[\boldsymbol{x}]}$,
(2) G ist reduziert,
(3) Alle Polynome $g \in G$ erfüllen $\mathrm{LC}(g) = 1$.

Als Konsequenz aus der Termination und Korrektheit des Algorithmus 11.14 erhalten wir:

SATZ 11.17. *Jedes Ideal von $k[x_1, \ldots, x_n]$ besitzt eine reduzierte Gröbnerbasis.*

Diese reduzierte Gröbnerbasis eines Ideals ist, ähnlich der Zeilenstaffelnormalform eines Unterraums, durch das Ideal eindeutig bestimmt.

SATZ 11.18. *Sei I ein Ideal von $k[x_1, \ldots, x_n]$, sei $\leq$ eine zulässige Ordnung auf $\mathbb{N}_0{}^n$, und seien G, H reduzierte Gröbnerbasen von I bezüglich $\leq$. Dann gilt $G = H$.*

Beweis: Wir nehmen an, dass $I \neq 0$. Als erstes zeigen wir

$$\mathrm{LT}(G) = \mathrm{LT}(H).$$

Sei $G = \{g_1, \ldots, g_r\}$ und $H = \{h_1, \ldots, h_s\}$. Sei nun $g \in G$. Da g eine Standarddarstellung durch H mit Rest 0 besitzt, gibt es $a_1, \ldots, a_s \in k[\boldsymbol{x}]$, sodass $g = \sum_{i=1}^{s} a_i h_i$, und für alle i gilt $\mathrm{DEG}(a_i h_i) \leq \mathrm{DEG}(g)$. Für zumindest einen Summanden muss $\mathrm{DEG}(a_j h_j) = \mathrm{DEG}(g)$ sein. Da h_j eine Standarddarstellung durch G mit Rest 0 besitzt, gibt es $b_1, \ldots, b_r \in k[\boldsymbol{x}]$, sodass $h_j = \sum_{l=1}^{r} b_l g_l$, und für alle l gilt $\mathrm{DEG}(b_l g_l) \leq \mathrm{DEG}(h_j)$. Sei l so, dass $\mathrm{DEG}(h_j) = \mathrm{DEG}(b_l g_l)$. Dann gilt $\mathrm{LT}(g_l) | \mathrm{LT}(h_j)$ und $\mathrm{LT}(h_j) | \mathrm{LT}(g)$. Es gilt also $\mathrm{LT}(g_l) | \mathrm{LT}(g)$. Da G reduziert ist, gilt $g = g_l$. Nun gilt $\mathrm{LM}(g_l) | \mathrm{LM}(h_j)$ und $\mathrm{LM}(h_j) | \mathrm{LM}(g)$. Wegen $g_l = g$ gilt also $\mathrm{LM}(g) = \mathrm{LM}(h_j)$. Folglich gilt $\mathrm{LT}(g) \in \mathrm{LT}(H)$. Damit haben wir $\mathrm{LT}(G) \subseteq \mathrm{LT}(H)$ bewiesen.

Ebenso gilt $\mathrm{LT}(H) \subseteq \mathrm{LT}(G)$. Insgesamt gilt also $\mathrm{LT}(G) = \mathrm{LT}(H)$.

Wir zeigen nun $G \subseteq H$. Sei dazu $g \in G$. Es gibt nun ein Polynom $h \in H$, sodass $\mathrm{LT}(g) = \mathrm{LT}(h)$. Da G reduziert ist, enthält $g - \mathrm{LT}(g)$ kein Monom, das in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$ liegt. Da H reduziert ist, enthält $h - \mathrm{LT}(h)$ kein Monom, das in $\langle \mathrm{LT}(H) \rangle_{k[\boldsymbol{x}]}$ liegt. Wegen $\mathrm{LT}(G) = \mathrm{LT}(H)$ liegt also auch kein Monom von $h - \mathrm{LT}(h)$ in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Somit liegt wegen $\mathrm{LT}(g) = \mathrm{LT}(h)$ kein Monom von $g - h = (g - \mathrm{LT}(g)) - (h - \mathrm{LT}(h))$ in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Somit ist $g - h = \sum_{i=1}^{r} 0 \cdot g_r + (g - h)$ eine Standarddarstellung von $g - h$ durch G mit Rest $g - h$. Da G eine Gröbnerbasis von I ist, und da $g - h \in I$, gilt wegen Korollar 10.29 die Gleichheit $g = h$. Somit gilt $g \in H$.

Ebenso zeigt man $H \subseteq G$. □

ÜBUNGSAUFGABEN 11.19

(1) Bestimmen Sie eine Gröbnerbasis des Ideals $I = \langle f_1, f_2, f_3, f_4\rangle$ von $\mathbb{Q}[x_1, x_2, x_3, x_4, x_5]$.

$$\begin{aligned} f_1 &= x_1 - 5x_2 + 8x_3 + 2x_4 - 2x_5 \\ f_2 &= x_1 - 4x_2 + 6x_3 - 2x_4 \\ f_3 &= -1x_1 + 2x_3 + 2x_4 \\ f_4 &= 5x_1 - 8x_2 + 6x_3 - 5x_5. \end{aligned}$$

(Ordnen Sie die Monome lexikographisch mit $x_1 > \cdots > x_5$.)

(2) Seien $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$. Wir nehmen an, dass $f_1 = f_2 = \cdots = f_s = 0$ unlösbar ist. Sei G eine Gröbnerbasis von $\langle f_1, \ldots, f_s\rangle$. Zeigen Sie, dass G ein konstantes Polynom ungleich 0 enthält!

(3) Bestimmen Sie eine Gröbnerbasis des folgenden Ideals $I = \langle f_1, f_2\rangle$ von $\mathbb{Q}[x]$.

$$\begin{aligned} f_1 &= x - x^3 + x^4 - 2\,x^5 + x^6 \\ f_2 &= x - 2\,x^2 + x^3 - x^4 + x^6. \end{aligned}$$

Let $A = \{x_1 + 2x_2 + 2x_3 + 2x_4 - 15, -2x_1 - 4x_2 + x_3 + 11x_4 - 20, -4x_1 - 8x_2 + 2x_3 + 22x_4 - 40, x_1 + 2x_2 + 5x_3 + 11x_4 - 45\}$.

(1) Compute a reduced Gröbner basis for the ideal of $\mathbb{Q}[x_1, x_2, x_3, x_4]$ that is generated by A. (Lexicographic ordering, $x_1 > x_2 > x_3 > x_4$.)

(2) Compute a basis for the linear subspace of $\mathbb{Q}^4$ that is generated by the rows of the matrix

$$B = \begin{pmatrix} 1 & 2 & 2 & 2 & -15 \\ -2 & -4 & 1 & 11 & -20 \\ -4 & -8 & 2 & 22 & -40 \\ 1 & 2 & 5 & 11 & -45 \end{pmatrix}.$$

(3) Compute the reduced Gröbnerbasis for the ideal of $\mathbb{Q}[x]$ that is generated by $\{x^2 - x - 2, x^3 + x^2 - 6x\}$.

(4) Let G be a finite subset of $\mathbb{Q}[\boldsymbol{x}]$, let $f \in G$, and let r be the remainder in a standard expression of f by $G \setminus \{f\}$.

(a) Show that if G is a Gröbner basis of $\langle G\rangle_{\mathbb{Q}[\boldsymbol{x}]}$, then $(G \setminus \{f\}) \cup \{r\}$ is also a Gröbner basis of $\langle G\rangle_{\mathbb{Q}[\boldsymbol{x}]}$.

(b) Given an example where $(G \setminus \{f\}) \cup \{r\}$ is a Gröbner basis, but G is not a Gröbner basis.

(5) Let F be a finite subset of $\mathbb{Q}[x_1, \ldots, x_n]$, and let f be an element of the ideal J that F generates in $\mathbb{C}[x_1, \ldots, x_n]$. Show that f is also an element of the ideal I that F generates in $\mathbb{Q}[x_1, \ldots, x_n]$.

(6) Let $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$. Show that the system $f_1 = \cdots = f_s = 0$ has no solution in $\mathbb{C}^n$ if and only if the reduced Gröbner basis of $\langle f_1, \ldots, f_s\rangle_{\mathbb{C}[\boldsymbol{x}]}$ is $\{1\}$.

3. Minimalitätseigenschaften

Sei $\leq$ eine zulässige Ordnung auf $\mathbb{N}_0^n$. Wir ordnen nun endliche Teilmengen von $\mathbb{N}_0$ durch

$$A \leq_M B \Leftrightarrow A = B \text{ oder } \max_{\leq}(A \triangle B) \in B.$$

LEMMA 11.20. *Sei $\leq$ eine zulässige Ordnung auf $\mathbb{N}_0^n$. Dann ist $\leq_M$ eine lineare Ordnung auf der Menge $\mathcal{P}_{fin}(A)$ der endlichen Teilmengen von A, und $\leq_M$ erfüllt die* (DCC).

PROOF. Reflexivität und Antisymmetrie von $\leq_M$ sind unmittelbar klar.

Für die Transitivität nehmen wir $A <_M B$ und $B <_M C$ an. Sei $\beta := \max_{\leq}(A \triangle B)$ und $\gamma := \max_{\leq}(B \triangle C)$.

1. Fall: $\gamma < \beta$*:* Dann gilt $\beta \notin B \triangle C$, und somit wegen $\beta \in B$ auch $\beta \in C$. Wegen $\beta \in B$ und $\beta \in A \triangle B$ gilt $\beta \notin A$. Folglich gilt $\beta \in A \triangle C$. Sei nun $\beta' > \beta$. Dann gilt $\beta' \notin A \triangle B$ und $\beta \notin B \triangle C$, und folglich $\beta' \notin (A \triangle B) \triangle (B \triangle C) = A \triangle C$. Also gilt $\beta = \max_{\leq}(A \lhd C)$, und wegen $\beta \in C$ daher auch $A \leq_M C$.

2. Fall: $\gamma = \beta$*:* Wegen $\beta \in B$ und $\gamma \in C$ gilt in diesem Fall $\gamma \notin B \triangle C$. dieser Fall kann daher nicht eintreten.

3. Fall: $\gamma > \beta$*:* Dann gilt $\gamma \notin A \triangle B$, und wegen $\gamma \notin B$ daher auch $\gamma \notin A$. Für alle $\gamma' > \gamma$ gilt $\gamma' \notin A \triangle B$ und $\gamma' \notin B \triangle C$, also $\gamma' \notin (A \triangle B) \triangle (B \triangle C) = A \triangle C$. Also gilt $\gamma = \max_{\leq}(A \lhd C)$, und wegen $\gamma \in C$ daher auch $A \leq_M C$.

Somit ist $\leq_M$ transitiv.

Für alle $A, B \subseteq \mathbb{N}_0^n$ mit $A \neq B$ gilt $\max_{\leq}(A \triangle B) \in A \cup B$ und folglich $B \leq_M A$ oder $A \leq_M B$. Somit ist $\leq_M$ linear.

Sei nun $A_1 >_M A_2 >_M \cdots$ unter allen unendlichen absteigende Ketten eine mit minimalem $\max_{\leq}(A_1)$. Sei $a := \max_{\leq}(A_1)$. Wenn a Element aller A_i ist, so ist $A_1 \setminus \{a\} >_M A_2 \setminus \{a\} >_M \cdots$ eine Kette mit kleinerem maximalen Element des ersten Kettenelements, im Widerspruch zur Minimalität der gewählten Kette. Wenn es ein k mit $a \notin A_k$ gibt, so sei $b := \max_{\leq}(A_k)$. Wenn $b > a$, so gilt $b \in A_k \triangle A_1$ und $b > \max_{\leq}(A_1)$. Somit gilt $\max_{\leq}(A_k \triangle A_1) \notin A_1$, und damit $A_1 \leq_M A_k$, ein Widerspruch. Somit gilt $b < a$. Damit ist aber $A_k >_M A_{k+1} >_M \cdots$ eine Kette mit kleinerem maximalen Element des ersten Kettenelements, im Widerspruch zur Minimalität der gewählten Kette. Somit erfüllt $\leq_M$ die (DCC). □

Definition 11.21. Sei $n \in \mathbb{N}$, $f = \sum_{\alpha \in \mathbb{N}_0{}^n} c_\alpha \boldsymbol{x}^\alpha \in k[x_1, \ldots, x_n]$. Der *Support* von f ist definiert durch $\mathrm{Supp}(f) = \{\alpha \in \mathbb{N}_0{}^n \mid c_\alpha \neq 0\}$.

Für eine zulässige Ordnung $\leq$ auf $\mathbb{N}_0{}^n$ und $f, g \in k[x_1, \ldots, x_n]$ schreiben wir $f \leq_P g$, falls $\mathrm{Supp}(f) \leq_M \mathrm{Supp}(g)$. Die Relation $\leq_P$ ist reflexiv und transitiv, aber für einen Körper k mit $|k| > 2$ nicht antisymmetrisch, und somit eine *Quasiordnung*. Wie für Quasiordnungen üblich, schreiben wir $f <_P g$ für $f \leq_P g$ und $g \not\leq_P f$. Sei F eine Teilmenge von $k[x_1, \ldots, x_n]$. Dann ist ein Element g *minimal* in F bezüglich $\leq_P$, wenn es kein f in F mit $f <_P g$ gibt. Das Polynom g ist also minimal, wenn für alle $f \in F$ mit $f \leq_P g$ auch $g \leq_P f$ gilt.

Satz 11.22 (Minimalitätseigenschaft von reduzierten Gröbnerbasen). *Sei G eine reduzierte Gröbnerbasis des Ideals I von $k[x_1, \ldots, x_n]$ bezüglich der zulässigen Ordnung $\leq$ auf $\mathbb{N}_0^n$. Sei $\leq_P$ die zu dieser Ordnung gehörende Quasiordnung auf $k[x_1, \ldots, x_n]$. Sei $h \in I \setminus \{0\}$, und sei f ein Polynom, das minimal bezüglich $\leq_P$ in der Menge*

$$H = \{f' \in I \,:\, \mathrm{Lt}(f') \mid \mathrm{Lt}(h) \text{ und } \mathrm{Lc}(f') = 1\}$$

ist. Dann gilt $f \in G$.

Proof. Wegen $f \in I$ gibt es ein $g \in G$ mit $\mathrm{Lt}(g) \mid \mathrm{Lt}(f)$. Dann gilt $g \in H$ und wegen der Minimalität von f bezüglich $\leq_P$ daher $\mathrm{Lt}(g) = \mathrm{Lt}(f)$.

Wir zeigen nun $f = g$, und nehmen im Widerspruch dazu an, dass $f \neq g$. Wir zeigen als erstes, dass $\mathrm{Deg}(f - g)$ ein Element von $\mathrm{Supp}(g)$ ist.

Im Fall, dass $\mathrm{Supp}(g) = \mathrm{Supp}(f)$, enthält $f - g$ nur Monome, die bereits in g vorkommen, und somit gilt $\textsc{Deg}(f - g) \in \mathrm{Supp}(g)$.

Im Fall $\mathrm{Supp}(g) \neq \mathrm{Supp}(f)$ gilt wegen der Minimalität von f, dass $\mathrm{Supp}(g) >_M \mathrm{Supp}(f)$. Für alle α mit $\alpha > \textsc{Deg}(f - g)$ verschwindet der Term von $\boldsymbol{x}^\alpha$ nach der Subtraktion von g von f. Folglich muss α entweder sowohl in $\mathrm{Supp}(f)$ als auch in $\mathrm{Supp}(g)$ vorkommen, oder in keiner der beiden Mengen. Somit gilt $\alpha \notin \mathrm{Supp}(f) \triangle \mathrm{Supp}(g)$. Daraus erhalten wir $\max_\leq(\mathrm{Supp}(f) \triangle \mathrm{Supp}(g)) \leq \textsc{Deg}(f - g)$. Nehmen wir nun an, dass $\textsc{Deg}(f - g) \notin \mathrm{Supp}(g)$. Dann muss $\textsc{Lm}(f - g)$ in f vorkommen, und es gilt folglich $\textsc{Deg}(f - g) \in \mathrm{Supp}(f) \triangle \mathrm{Supp}(g)$. Also gilt $\max_\leq(\mathrm{Supp}(f), \mathrm{Supp}(g)) = \textsc{Deg}(f - g)$ und $\textsc{Deg}(f - g) \in \mathrm{Supp}(f)$, und folglich $\mathrm{Supp}(g) \leq_M \mathrm{Supp}(f)$. Da nach Fallannahme $\mathrm{Supp}(f) \neq \mathrm{Supp}(g)$, gilt also $\mathrm{Supp}(g) <_M \mathrm{Supp}(f)$ und somit $g <_P f$, im Widerspruch zur Minimalität von f. Somit führt die Annahme $\textsc{Deg}(f - g) \notin \mathrm{Supp}(g)$ zu einem Widerspruch, und es gilt daher auch im Fall $\mathrm{Supp}(f) \neq \mathrm{Supp}(g)$, dass $\textsc{Deg}(f - g) \in \mathrm{Supp}(g)$.

Es gilt nun gilt $f - g \in I \setminus \{0\}$. Es gibt daher ein $g' \in G$ mit $\textsc{Lt}(g') \mid \textsc{Lt}(f - g)$. Wegen $\textsc{Deg}(f - g) < \textsc{Deg}(g)$ gilt $\textsc{Deg}(g') < \textsc{Deg}(g)$ und folglich $g \neq g'$. Da $\textsc{Deg}(f - g) \in \mathrm{Supp}(g)$, teilt $\textsc{Lt}(g')$ ein in g vorkommendes Monom, im Widerspruch dazu, dass G reduziert ist. □

Korollar 11.23. *Sei k ein Körper, und sei G eine reduzierte Gröbnerbasis des Ideals I von $k[x_1, \ldots, x_n]$ bezüglich der zulässigen Ordnung $\leq$ auf $\mathbb{N}_0^n$. Sei $D := \{\deg_\leq(f) \mid f \in I\}$, und sei M die Menge der minimalen Elemente von D bezüglich $\sqsubseteq$. Dann gilt:*

(1) *Es gibt für jedes $\alpha \in M$ genau ein Polynom $f_\alpha \in I$, das minimal bezüglich $\leq_P$ in*

$$I_\alpha = \{f \in I \mid \textsc{Deg}(f) = \alpha, \textsc{Lc}(f_\alpha) = 1\}$$

ist.

(2) *$G = \{f_\alpha \mid \alpha \in M\}$ und $|G| = |M|$.*

Proof. (1) Sei $\alpha \in M$. Die Menge I_α ist nicht leer. Seien f, g zwei bezüglich $\leq_P$ minimale Elemente aus I_α. Da α minimal in D bezüglich $\sqsubseteq$ ist, gilt $\{f' \in I : \textsc{Lt}(f') \mid \textsc{Lt}(g) \text{ und } \textsc{Lc}(f') = 1\} = I_\alpha$. Folglich liefert Satz 11.22, dass f und g beide Elemente von G sind. Da G reduziert ist, gilt daher $f = g$.

(2) $\supseteq$: Wir haben bereits gezeigt, dass für jedes $\alpha \in M$ jedes minimale Element von I_α in G liegt. Daraus folgt $\supseteq$.

$\subseteq$: Sei nun $g \in G$. Da G reduziert ist, ist $\alpha := \textsc{Deg}(g)$ minimal in D bezüglich $\sqsubseteq$: Wenn $\beta \sqsubset \alpha$ und $\beta \in D$, so gibt es ein Polynom $g' \in G$ mit $\textsc{Lm}(g') | \boldsymbol{x}^\beta$, und somit $\textsc{Lm}(g') \mid \textsc{Lm}(g)$. Also gilt $\alpha \in M$. Es bleibt zu zeigen, dass $g = f_\alpha$. Sei h ein bezüglich $\leq_P$ minimales Element unter den Elementen h' von I_α, die $h' \leq_P g$ erfüllen. Dann gilt $h = f_\alpha$, und somit gilt wegen der bereits gezeigten Inklusion $h \in G$. Da $\textsc{Lm}(h) = \textsc{Lm}(g)$, die Polynome g, h beide in G sind und G reduziert ist, gilt $g = h = f_\alpha$, und somit $g \in \{f_\alpha \mid \alpha \in M\}$. □

KAPITEL 12

Einige Anwendungen von Gröbnerbasen

1. Automatisches Beweisen in der Geometrie

Wir betrachten Sätze in der ebenen Geometrie, wie etwa die Sätze von Thales, Desargues, Pappus, ... Wir beschreiben die Punkte der Ebenen mit Elementen aus $\mathbb{R}^2$.

Viele geometrische Eigenschaften kann man durch Gleichungen ausdrücken.

SATZ 12.1. *Es gibt genau dann eine Gerade, auf der jeder der Punkte* $\binom{x_1}{y_1}$, $\binom{x_2}{y_2}$, $\binom{x_3}{y_3} \in \mathbb{R}^2$ *liegt, wenn* $\det\left(\begin{pmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{pmatrix}\right) = 0$.

SATZ 12.2. *Es gibt genau dann einen Kreis oder eine Gerade, auf der jeder der Punkte* $\binom{x_1}{y_1}$, $\binom{x_2}{y_2}$, $\binom{x_3}{y_3}$, $\binom{x_4}{y_4}$ *liegt, wenn*

$$\det\left(\begin{pmatrix} 1 & x_1 & y_1 & {x_1}^2+{y_1}^2 \\ 1 & x_2 & y_2 & {x_2}^2+{y_2}^2 \\ 1 & x_3 & y_3 & {x_3}^2+{y_3}^2 \\ 1 & x_4 & y_4 & {x_4}^2+{y_4}^2 \end{pmatrix}\right) = 0.$$

ÜBUNGSAUFGABEN 12.3
Formulieren Sie die Bedingungen für folgende geometrische Eigenschaften der Punkte $P_1 = \binom{x_1}{y_1}$, $P_2 = \binom{x_2}{y_2}$, $P_3 = \binom{x_3}{y_3}, P_4 = \binom{x_4}{y_4}$ als Polynomgleichungen in den Variablen $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$.

(1) Das Dreieck $P_1P_2P_3$ ist gleichschenkelig.
(2) P_3 ist der Mittelpunkt von P_1P_2.
(3) P_3 liegt auf der Streckensymmetrale von P_1P_2.
(4) P_1P_2 steht senkrecht auf P_1P_3.
(5) $\overline{P_1P_3} = \overline{P_2P_3}$.
(6) P_4 liegt auf der Winkelsymmetralen des Dreiecks $P_1P_2P_3$ durch P_1.
(7) P_4 liegt auf dem Umkreis des Dreiecks $P_1P_2P_3$.
(8) P_4 liegt auf der Schwerlinie des Dreiecks $P_1P_2P_3$ durch P_1.
(9) P_4 liegt auf der Höhe des Dreiecks $P_1P_2P_3$ auf P_2P_3.

Wir betrachten nun den Satz von Pappus:

> Seien A, B, C Punkte auf einer Geraden, und seien D, E, F Punkte auf einer Geraden. Sei H ein Schnittpunkt von AE und DB, sei I ein Schnittpunkt von AF ubd DC, und sei J ein Schnittpunkt von BF und EC. Dann liegen H, I, J auf einer Geraden.

Wir könnten den Satz so formulieren:

Seien $A, B, C, D, E, F, H, I, J$ Punkte in der Ebene, sodass folgende Punktetripel jeweils auf einer Geraden liegen: (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F). Dann liegen H, I, J auf einer Geraden.

Das stimmt aber nicht. ($A = B = C = D = E = F$, H, I, J beliebig, sodass sie nicht auf einer Geraden liegen.) In folgender Formulierung stimmt der Satz:

SATZ 12.4 (Eine Version des Satzes von Pappus). *Seien $A, B, C, D, E, F, H, I, J$ (nicht notwendigerweise voneinander verschiedene) Punkte in der Ebene, sodass folgende Punktetripel jeweils auf einer Geraden liegen: (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F). Wenn es keine Gerade gibt, die A, B, D enthält, und keine Gerade, die A, B, E enthält, dann liegen H, I, J auf einer Geraden.*

Wir müssen also auch die Bedingung, dass A, B, D *nicht* auf einer Geraden liegen, ausdrücken.

SATZ 12.5 (Grundlage des automatischen Beweisens geometrischer Sätze). *Seien $n \in \mathbb{N}$, $r, s \in \mathbb{N}_0$, $f_1, \ldots, f_s, h_1, \ldots, h_r, g \in \mathbb{C}[t_1, \ldots, t_n]$. Dann sind äquivalent:*

(1) *Für alle $\boldsymbol{x} \in \mathbb{C}^n$ gilt:*
Wenn $f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0$ und $h_1(\boldsymbol{x}) \neq 0, \ldots, h_r(\boldsymbol{x}) \neq 0$, dann gilt $g(\boldsymbol{x}) = 0$.

(2) *Es gibt kein $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{C}^{n+(r+1)}$, sodass*

$$\begin{aligned} f_1(\boldsymbol{x}) &= 0 \\ &\vdots \\ f_s(\boldsymbol{x}) &= 0 \\ h_1(\boldsymbol{x}) \cdot y_1 &= 1 \\ &\vdots \\ h_r(\boldsymbol{x}) \cdot y_r &= 1 \\ g(\boldsymbol{x}) \cdot y_{r+1} &= 1. \end{aligned} \tag{12.1}$$

Beweis: (1)⇒(2): Wir nehmen an, dass das Gleichungssystem (12.1) eine Lösung $(\boldsymbol{x}, \boldsymbol{y})$ in $\mathbb{C}^{n+(r+1)}$ hat. Es gilt dann $f_1(\boldsymbol{x}) = \ldots = f_s(\boldsymbol{x}) = 0, h_1(\boldsymbol{x}) \neq 0, \ldots, h_r(\boldsymbol{x}) \neq 0, g(\boldsymbol{x}) \neq 0$, im Widerspruch zu (1). (2)⇒(1): Wir nehmen an, dass (1) nicht gilt, also, dass es $\boldsymbol{x} \in \mathbb{C}^n$ gibt, sodass $f_1(\boldsymbol{x}) = \ldots = f_s(\boldsymbol{x}) = 0$, $h_1(\boldsymbol{x}) \neq 0$, $\ldots$, $h_r(\boldsymbol{x}) \neq 0$, und $g(\boldsymbol{x}) \neq 0$. Seien $(y_1, \ldots, y_r, y_{r+1})$ definiert durch $y_i := \frac{1}{h_i(\boldsymbol{x})}$ für $i \in \{1, \ldots, r\}$, und sei $y_{r+1} := \frac{1}{g(\boldsymbol{x})}$. Dann ist

$$(x_1, \ldots, x_n, y_1, \ldots, y_r, y_{r+1})$$

eine Lösung des Gleichungssystems (12.1), also gilt (2) nicht. □

Die Lösbarkeit von Gleichungssystemen überprüft man mit folgendem Satz.

SATZ 12.6 (Hilbert, Buchberger). *Seien $m, n \in \mathbb{N}$, und seien $p_1, \ldots, p_n$ Polynome über $\mathbb{R}$ in den Variablen $t_1, \ldots, t_m$, und sei G eine Gröbnerbasis für die Polynome $p_1, \ldots, p_n$ (bezüglich irgendeiner Termordnung). Dann sind folgende beiden Bedingungen äquivalent:*

(1) *Es gibt kein $(x_1, \ldots, x_m) \in \mathbb{C}^m$, sodass*

$$p_1(x_1, \ldots, x_m) = \cdots = p_n(x_1, \ldots, x_m) = 0.$$

(2) *G enthält ein konstantes Polynom ungleich* 0.

Beweis: Wenn G ein konstantes Polynom $c \neq 0$ enthält, so wäre jede gemeinsame Nullstelle von $p_1, \ldots, p_n$ auch eine Nullstelle von c. Da c keine Nullstellen hat, kann also $p_1 = \cdots = p_n = 0$ keine Lösung haben.

Wenn $p_1 = \ldots = p_n = 0$ keine Nullstelle in $\mathbb{C}^m$ hat, so gilt wegen des Hilbertschen Nullstellensatzes, dass $1 \in \langle p_1, \ldots, p_n \rangle_{k[\boldsymbol{x}]}$. Damit muss es ein Polynom $g \in G$ mit $\mathrm{Lt}(g) \mid \mathrm{Lt}(1)$ geben. Dieses g ist also konstant. □

Somit beweist folgender (geringfügig editierter) Mathematica-Dialog den Satz von Pappus.

```
In[1]:= Collinear[P1_,P2_,P3_]:=Det[{P1,P2,P3}]

AA={0,0,1};
BB={b1,b2,1};
CC={c1,c2,1};
DD={d1,d2,1};
EE={e1,e2,1};
FF={f1,f2,1};
GG={g1,g2,1};
HH={h1,h2,1};
II={i1,i2,1};
JJ={j1,j2,1};

System={Collinear[AA,BB,CC],Collinear[DD,EE,FF],Collinear[AA,HH,EE],
Collinear[DD,HH,BB],Collinear[DD,II,CC],Collinear[AA,II,FF],
Collinear[EE,JJ,CC],Collinear[BB,JJ,FF],
Collinear[AA,BB,DD]*z2-1,Collinear[AA,BB,EE]*z3-1,Collinear[HH,II,JJ]*z1-1}


Out[1]= {-b2 c1+b1 c2,-d2 e1+d1 e2+d2 f1-e2 f1-d1 f2+e1 f2,
e2 h1-e1 h2,-b2 d1+b1 d2+b2 h1-d2 h1-b1 h2+d1 h2,
-c2 d1+c1 d2+c2 i1-d2 i1-c1 i2+d1 i2,
f2 i1-f1 i2,-c2 e1+c1 e2+c2 j1-e2 j1-c1 j2+e1 j2,
b2 f1-b1 f2-b2 j1+f2 j1+b1 j2-f1 j2,
-1+(-b2 d1+b1 d2) z2,-1+(-b2 e1+b1 e2) z3,
-1+(-h2 i1+h1 i2+h2 j1-i2 j1-h1 j2+i1 j2) z1}

In[2]:= GB=GroebnerBasis[System,MonomialOrder->DegreeReverseLexicographic]

Out[2]= {1}
```

Übungsaufgaben 12.7

(1) (Automated Geometry Theorem Proving) Thales's Theorem states that in every triangle, the circumcentre lies on on one of the sides if and only if the triangle is right-angled. Give a formulation of this theorem in terms of polynomial equations, and use these equations to prove Thales's Theorem.

(2) (Automated Geometry Theorem Proving) We consider Desargues's Theorem:

Let $S, A, B, C, D, E, F, H, I, J$ points of the plane $\mathbb{R}^2$ such that

(a) S, A, D are collinear.
(b) S, B, E are collinear.
(c) S, C, F are collinear.
(d) A, B, H are collinear.
(e) D, E, H are collinear.
(f) A, C, J are collinear.
(g) D, F, J are collinear.
(h) B, C, I are collinear.
(i) E, F, I are collinear.
(j) E, A, D are not collinear.
(k) F, A, D are not collinear
(l) F, B, E are not collinear
(m) C, A, D are not collinear

Then H, I, J are collinear.

(a) Make a good drawing to explain the content of the theorem.
(b) Prove the theorem using a Gröbner bases computation. *Remark:* Use a computer algebra system.

(3) Let $f, g, h, i \in \mathbb{C}[x_1, \ldots, x_n]$. For each of the following formulae, give a system of polynomial equations whose solvability/non-solvability is equivalent to the formula.

(a) $\forall x_1, \ldots, x_n \in \mathbb{C} : (f(x_1, \ldots, x_n) = 0 \wedge g(x_1, \ldots, x_n) \neq 0) \Rightarrow h(x_1, \ldots, x_n) = 0$.
(b) $\forall x_1, \ldots, x_n \in \mathbb{C} : (f(x_1, \ldots, x_n) = 0 \wedge g(x_1, \ldots, x_n)) = 0) \Rightarrow (h(x_1, \ldots, x_n) \neq 0 \wedge i(x_1, \ldots, x_n) \neq 0)$.
(c) $\forall x_1, \ldots, x_n \in \mathbb{C}$: $f(x_1, \ldots, x_n) = 0 \Rightarrow g(x_1, \ldots, x_n) \neq 0$.
(d) $\forall x_1, \ldots, x_n \in \mathbb{C}$: $f(x_1, \ldots, x_n) \neq 0 \Rightarrow g(x_1, \ldots, x_n) \neq 0$.

(4) Wie übersetzt man die folgende Bedingung in die Frage nach der Lösbarkeit eines Gleichungssystems?

Für alle $x_1, \ldots, x_n \in \mathbb{R}$ gilt: Wenn $f(x_1, \ldots, x_n) = 0$ und $g(x_1, \ldots, x_n) \neq 0$, so gilt $h(x_1, \ldots, x_n) = 0$.

(5) Beim automatischen Beweisen von geometrischen Sätzen mit der Gröbnerbasenmethode führt man die Gültigkeit einer Aussage auf die Lösbarkeit eines (oder mehrerer) Gleichungssysteme zurück. Seien $f_1, \ldots, f_r, g_1, \ldots, g_s, h$ Polynome in $\mathbb{C}[x_1, \ldots, x_k]$. Wie führen Sie die folgenden Aussagen auf die Lösbarkeit von Gleichungssystemen zurück? Geben Sie jeweils die Gleichungssysteme an!

(a) Für alle $x_1, \ldots, x_k$ gilt:

$$\left.\begin{array}{c} f_1(x_1, \ldots, x_k) = 0 \ \wedge \\ \vdots \\ f_r(x_1, \ldots, x_k) = 0 \ \wedge \\ g_1(x_1, \ldots, x_k) \neq 0 \ \wedge \\ \vdots \\ g_s(x_1, \ldots, x_k) \neq 0 \end{array}\right\} \Rightarrow h(x_1, \ldots, x_k) = 0.$$

(b) Für alle $x_1, \ldots, x_k$ gilt:

$$\left.\begin{array}{c} f_1(x_1, \ldots, x_k) = 0 \ \wedge \\ \vdots \\ f_r(x_1, \ldots, x_k) = 0 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} g_1(x_1, \ldots, x_k) \neq 0 \ \wedge \\ \vdots \\ g_s(x_1, \ldots, x_k) \neq 0 \end{array}\right.$$

(c) Für alle $x_1, \ldots, x_k$ gilt:

$$f_1(x_1, \ldots, x_k) = 0 \Rightarrow g_1(x_1, \ldots, x_k) \neq 0.$$

(d) Für alle $x_1, \ldots, x_k$ gilt:

$$f_1(x_1, \ldots, x_k) \neq 0 \Rightarrow g_1(x_1, \ldots, x_k) \neq 0.$$

Geben Sie in den Beispielen (3) und (4) einen Beweis für die Äquivalenz der Implikation mit der Lösbarkeit der Gleichungssysteme.

(6) (Beweisen geometrischer Sätze) Wir betrachten den Satz von Desargues.

Seien $S, A, B, C, D, E, F, H, I, J$ Punkte der Ebene $\mathbb{R}^2$ mit folgenden Eigenschaften:

(a) S, A, D liegen auf einer Geraden.
(b) S, B, E liegen auf einer Geraden.
(c) S, C, F liegen auf einer Geraden.
(d) A, B, H liegen auf einer Geraden.
(e) D, E, H liegen auf einer Geraden.
(f) A, C, J liegen auf einer Geraden.
(g) D, F, J liegen auf einer Geraden.
(h) B, C, I liegen auf einer Geraden.
(i) E, F, I liegen auf einer Geraden.
(j) E, A, D liegen nicht auf einer Geraden.
(k) F, A, D liegen nicht auf einer Geraden.
(l) F, B, E liegen nicht auf einer Geraden.
(m) C, A, D liegen nicht auf einer Geraden.

Dann liegen H, I, J auf einer Geraden.

(a) Machen Sie eine Skizze für diesen Satz. (Die Skizze wird schön, wenn Sie S als Ausgangspunkt dreier Strahlen zeichnen, A näher bei S liegt als D, E näher bei S liegt als B, und C näher bei S liegt als F.)
(b) Finden Sie ein polynomiales Gleichungssystem, dessen Unlösbarkeit diesen Satz impliziert.
(c) Zeigen Sie dadurch, dass eine Gröbnerbasis des Systems ein konstantes Polynom enthält, dass das System tatsächlich unlösbar ist. (*Himweis*: Verwenden Sie dazu ein Computeralgebrasystem.)

2. Schnitt von Idealen

Wir zeigen, wie wir die Generatoren des Schnitts zweier Ideale von $k[x_1, \ldots, x_n]$ berechnen.

Satz 12.8 (Schnitt von Idealen). *Sei R ein kommutativer Ring mit Eins, und seien I, J Ideale von R. Seien (x) und $(x-1)$ die von x beziehungsweise $x-1$ erzeugten Hauptideale von $R[x]$. Dann gilt*

$$I \cap J = \{r \in R \mid r\, x^0 \in I[x] \cdot (x) + J[x] \cdot (x-1)\}.$$

Beweis: Für $\subseteq$ sei $i \in I \cap J$. Es gilt dann $i\, x^0 = ix - i(x-1)$. Für $\supseteq$ sei $rx^0 = x \cdot \sum_{l=0}^{m} i_l x^l + (x-1) \cdot \sum_{l=0}^{n} j_l x^l$ mit $i_1, \ldots, i_m \in I$ und $j_1, \ldots, j_n \in J$. Wenn wir für $x := 0$ einsetzen, erhalten wir $r = -1 j_0$, also $r \in J$. Wenn wir für $x = 1$ einsetzen, so erhalten wir $r = \sum_{l=0}^{m} i_l$, also $r \in I$. □

Korollar 12.9. *Sei k ein Körper, und seien I, J Ideale von $k[t_1, \ldots, t_n]$. Seien $a_1, \ldots, a_r, b_1, \ldots, b_s \in k[\boldsymbol{t}]$ so, dass $I = \langle a_1, \ldots, a_r \rangle_{k[\boldsymbol{t}]}$ und $J = \langle b_1, \ldots, b_s \rangle_{k[\boldsymbol{t}]}$. Sei*

$$H := \langle a_1 y, \ldots, a_r y, b_1(y-1), \ldots, b_s(y-1) \rangle_{k[\boldsymbol{t}, y]}.$$

Dann gilt $H \cap k[\boldsymbol{t}] = I \cap J$.

Beweis: Wir verwenden Satz 12.8 für $R := k[\boldsymbol{t}]$. □

ÜBUNGSAUFGABEN 12.10

(1) Compute the greatest common divisor of $f = x^4y + x^3y^2 - 2x^2y^2 - 2xy^3 + x + y$ and $g = x^4y - x^3y^3 - 2x^2y^2 + 2xy^4 + x - y^2$ in $\mathbb{Q}[x, y]$ by computing the intersection of $\langle f\rangle_{\mathbb{Q}[x,y]} \cap \langle g\rangle_{\mathbb{Q}[x,y]}$. *Remark:* Use a computer algebra system. Note that in a UFD, we have $(a) \cap (b) = (\operatorname{lcm}(a, b))$ and $\gcd(a, b) = ab/\operatorname{lcm}(a, b)$ for $a, b \neq 0$.

For an ideal I of $k[x_1, \ldots, x_n]$ and $f \in k[x_1, \ldots, x_n]$, we define the *ideal quotient* $(I : f)$ by

$$(I : f) = \{g \in k[\boldsymbol{x}] \mid gf \in I\}.$$

(1) Show that $(I : f) = \{\frac{h}{f} \mid h \in I \cap \langle f\rangle_{k[\boldsymbol{x}]}\}$.
(2) Let $f = x^2$ and $I = \langle x^7y^2, x^9y + 2x^8y\rangle_{k[\boldsymbol{x}]}$. Compute $(I : (f^n))$ for each $n \in \mathbb{N}$.

For an ideal I of $k[x_1, \ldots, x_n]$ and $f \in k[x_1, \ldots, x_n]$, the *saturation* $(I : f^\infty)$ of I with respect to f is defined by

$$(I : f^\infty) = \bigcup_{n\in\mathbb{N}} (I : f^n).$$

(1) Show that $(I : f^\infty) = \langle I \cup \{fy - 1\}\rangle_{k[\boldsymbol{x},y]} \cap k[\boldsymbol{x}]$.
(2) Use this fact to compute $(I : f^\infty)$ for $f = x^2$ and $I = \langle x^7y^2, x^9y + 2x^8y\rangle_{k[\boldsymbol{x}]}$.

3. Finden algebraischer Abhängigkeiten

Die folgenden Sätze bieten Möglichkeiten, zu bestimmen, ob gegebene Elemente eines Rings algebraisch abhängig sind. Als Vorbereitung beweisen wir folgendes Lemma:

LEMMA 12.11. *Sei k ein Körper, sei $\in \mathbb{N}$, sei R ein kommutativer Ring mit Eins mit $k \leq R$, und sei I ein Ideal von R. Sei $f \in k[t_1, \ldots, t_l]$, und seien $\boldsymbol{y}, \boldsymbol{z} \in R^l$ so, dass für alle $i \in \{1, \ldots, l\}$ gilt: $y_i - z_i \in I$. Dann gilt auch $\overline{f}(y_1, \ldots, y_l) - \overline{f}(z_1, \ldots, z_l) \in I$.*

Beweis: Offensichtlich erfüllt jedes konstante Polynom und jedes Polynom der Form $f = t_j$ diese Aussage. Wir zeigen nun, dass die Menge der Polynome, die diese Aussage erfüllen, abgeschlossen unter Addition und Multiplikation ist. Da man alle Polynome als Summen von Produkten von konstanten Polynomen und Variablen erhalten kann, beweist das das Lemma. Sei also $g = f_1 + f_2$. Dann gilt $g(\boldsymbol{y}) - g(\boldsymbol{z}) = f_1(\boldsymbol{y}) - f_1(\boldsymbol{z}) + f_2(\boldsymbol{y}) - f_2(\boldsymbol{z})$. Nach Voraussetzung liegen beide $f_i(\boldsymbol{y}) - f_i(\boldsymbol{z})$ in I. Wenn $g = f_1 \cdot f_2$, so gilt $g(\boldsymbol{y}) - g(\boldsymbol{z}) = f_1(\boldsymbol{y})f_2(\boldsymbol{y}) - f_1(\boldsymbol{z})f_2(\boldsymbol{z}) = f_1(\boldsymbol{y})f_2(\boldsymbol{y}) - f_1(\boldsymbol{y})f_2(\boldsymbol{z}) + f_1(\boldsymbol{y})f_2(\boldsymbol{z}) - f_1(\boldsymbol{z})f_2(\boldsymbol{z}) = f_1(\boldsymbol{y})(f_2(\boldsymbol{y}) - f_2(\boldsymbol{z})) + f_2(\boldsymbol{z})(f_1(\boldsymbol{y}) - f_1(\boldsymbol{z}))$. Beide Summanden liegen in I. □

SATZ 12.12 (Algebraische Abhängigkeit in $k[x_1, \ldots, x_n]/I$). *Sei k ein Körper, seien $r \in \mathbb{N}_0$, $n, s \in \mathbb{N}$, sei $I = \langle g_1, \ldots, g_r\rangle_{k[\boldsymbol{x}]}$, und seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Sei $p \in k[t_1, \ldots, t_s]$, und sei $J := \langle g_1, \ldots, g_r, t_1 - f_1, \ldots, t_s - f_s\rangle_{k[\boldsymbol{t},\boldsymbol{x}]}$. Dann sind äquivalent:*

(1) $p(f_1, \ldots, f_s) \in I$.
(2) $p \in J \cap k[t_1, \ldots, t_s]$.

Beweis: (1)⇒(2): Da für alle $i \in \{1, \ldots, s\}$ gilt: $f_1 \equiv t_1 \pmod{J}$, gilt wegen Lemma 12.11 auch

$$p(f_1, \ldots, f_s) \equiv p(t_1, \ldots, t_s) \pmod{J}.$$

Da $I \subseteq J$, gilt nach (1) auch $p(f_1, \ldots, f_s) \in J$, und somit $p(t_1, \ldots, t_s) \in J$. Da $p(t_1, \ldots, t_s)$ auch in $k[t_1, \ldots, t_s]$ liegt, gilt (2).

(2)⇒(1): Wenn $p \in J$, so gibt es Polynome $a_1, \ldots, a_r, b_1, \ldots, b_s \in k[\boldsymbol{t}, \boldsymbol{x}]$, sodass

$$p(\boldsymbol{t}) = \sum_{i=1}^{r} a_i(\boldsymbol{t}, \boldsymbol{x}) g_i(\boldsymbol{x}) + \sum_{i=1}^{s} b_i(\boldsymbol{t}, \boldsymbol{x})(t_i - f_i).$$

Diese Gleichheit gilt auch, wenn man für die Variable t_i das Polynom f_i einsetzt. Wir erhalten dann

$$p(f_1, \ldots, f_s) = \sum_{i=1}^{r} a_i(f_1, \ldots, f_s, \boldsymbol{x}) g_i(\boldsymbol{x}).$$

Daher gilt $p(f_1, \ldots, f_s) \in I$. □

Übungsaufgaben 12.13

(1) Let $R = \mathbb{Q}[\![x^2 + 1, x^4 + 2]\!] = \{p(x^2 + 1, x^4 + 2) \mid p \in \mathbb{Q}[t_1, t_2]\}$.
   (a) Show that R is isomorphic to $\mathbb{Q}[t_1, t_2]/I$, where $I = \{p \in \mathbb{Q}[t_1, t_2] \mid p(x^2 + 1, x^4 + 2) = 0\}$.
   (b) Compute this ideal I, and find an isomorphism φ from $\mathbb{Q}[t_1, t_2]/I$ to R.

(2) We consider the ring $\mathbb{Q}[x, y, z]/I$ with $I = \langle xz, yz \rangle$.
   (a) Find $f \in \mathbb{Q}[t_1, t_2, t_3]$ such that $f \neq 0$ and $f(x, y, z^3 + x + 1) \in \langle x, y \rangle$.
   (b) Find $g \in \mathbb{Q}[t_1, t_2, t_3]$ with $g \neq 0$ und $g(x, y, z^3 + x + 1) \in \langle z \rangle$.
   (c) Find $h \in \mathbb{Q}[t_1, t_2, t_3]$ mit $h \neq 0$ und $h(x, y, z^3 + x + 1) \in I_1 = \langle z \rangle \cap \langle x, y \rangle$.

(3) Find $f \in \mathbb{Q}[t_1, t_2]$ with $f \neq 0$ such that
   (a) $f(x^3, \frac{1}{x^9 - 1}) = 0$.
   (b) $f(\frac{y^3z^7 + 3y^2z^5 + 3yz^3 + z^4 + z}{(yz^2+1)^4}, \frac{z^2}{(yz^2+1)^2}) = 0$.

(4) Wir betrachten den Ring $\mathbb{Q}[x, y, z]/I$ mit $I = \langle y^3 - z^2, -y^2 + xz, xy - z, x^2 - y \rangle$.
   (a) Zeigen Sie, dass $((x + y) + I)$ algebraisch unabhängig über $\mathbb{Q}$ ist.
   (b) Zeigen Sie, dass $((-x^3 + z + 3) + I)$ algebraisch abhängig über $\mathbb{Q}$ ist.
   (c) Finden Sie ein Polynom $f \in \mathbb{Q}[t_1, t_2]$ mit $f \neq 0$, sodass $\overline{f}((x + y + 1) + I, (x + z) + I) = 0 + I$.

(5) Wir betrachten den Ring $\mathbb{Q}[x, y, z]/I$ mit $I = \langle xz, yz \rangle$.
   (a) Zeigen Sie, dass $(x + I, y + I)$ algebraisch unabhängig über $\mathbb{Q}$ ist.
   (b) Finden Sie $f \in \mathbb{Q}[t_1, t_2, t_3]$ mit $f \neq 0$ und $f(x, y, z^3 + x + 1) \in \langle x, y \rangle$.
   (c) Finden Sie $g \in \mathbb{Q}[t_1, t_2, t_3]$ mit $g \neq 0$ und $g(x, y, z^3 + x + 1) \in \langle z \rangle$.
   (d) Finden Sie $h \in \mathbb{Q}[t_1, t_2, t_3]$ mit $h \neq 0$ und $h(x, y, z^3 + x + 1) \in I_1 = \langle z \rangle \cap \langle x, y \rangle$.

(6) Wir betrachten den Ring $\mathbb{Q}[x, y, z]/I$ mit $I = \langle xz, yz \rangle$.
   (a) Zeigen Sie, dass $(z + I)$ algebraisch unabhängig über $\mathbb{Q}$ ist.
   (b) Zeigen Sie, dass für alle $q(x, y, z) \in \mathbb{Q}[x, y, z]$ gilt, dass $(z + I, q(x, y, z) + I)$ algebraisch abhängig ist. (Hinweis: $\langle xz, yz \rangle = \langle x, y \rangle \cap \langle z \rangle$.)
   (c) Begründen Sie durch Zitieren eines passenden Satzes, dass $\mathbb{Q}[x, y, z]/I$ algebraisch über dem Unterring $\mathbb{Q}[\![z + I]\!]$ ist.

(7) Wir betrachten den Ring $\mathbb{Q}[x, y, z]/I$ mit $I = \langle xz, yz \rangle$.
   (a) Zeigen Sie, dass für alle $q(x, y, z) \in \mathbb{Q}[x, y, z]$ gilt, dass $(x + I, y + I, q(x, y, z) + I)$ algebraisch abhängig ist.
   (b) Begründen Sie durch Zitieren eines passenden Satzes, dass $\mathbb{Q}[x, y, z]/I$ algebraisch über dem Unterring $\mathbb{Q}[\![x + I, y + I]\!]$ ist.

(c) Haben wir jetzt im Widerspruch zu Korollar 8.25 Transzendenzbasen verschiedener Kardinalität gefunden?

KOROLLAR 12.14 (Algebraische Abhängigkeit in $k[x_1,\ldots,x_n]$). *Sei k ein Körper, seien $r \in \mathbb{N}_0$, $n,s \in \mathbb{N}$, und seien $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$. Sei $p \in k[t_1,\ldots,t_s]$, und sei $J := \langle t_1 - f_1,\ldots,t_s - f_s\rangle_{k[\boldsymbol{t},\boldsymbol{x}]}$. Dann sind äquivalent:*

(1) $p(f_1,\ldots,f_s) = 0$.
(2) $p \in J \cap k[t_1,\ldots,t_s]$.

SATZ 12.15 (Algebraische Abhängigkeit im Quotientenkörper). *Sei k ein Körper, und sei R ein Integritätsbereich mit $k \leq R$. Seien $f_1,\ldots,f_s \in R$, und seien $g_1,\ldots,g_s \in R \setminus \{0\}$. Sei $p \in k[t_1,\ldots,t_s]$, und sei*

$$J := \left\langle f_1 - t_1 g_1,\ \ldots,\ f_s - t_s g_s,\ y\prod_{i=1}^{s} g_i - 1 \right\rangle_{R[\boldsymbol{t},y]}.$$

Dann sind äquivalent:

(1) $p(\frac{f_1}{g_1},\ldots,\frac{f_s}{g_s}) = 0$. *Dabei wird im Quotientenkörper $Q(R)$ von R gerechnet.*
(2) $p \in J \cap k[t_1,\ldots,t_s]$.

Beweis: (1)⇒(2): Sei $m := \max\{\deg_{t_i}(p) \mid i \in \{1,\ldots,s\}\}$. Wir definieren ein Polynom $q \in k[a_1,\ldots,a_s,b_1,\ldots,b_s]$ durch

$$q(\boldsymbol{a},\boldsymbol{b}) := \overline{p}(\frac{a_1}{b_1},\ldots,\frac{a_s}{b_s}) \cdot (b_1 \cdots b_s)^m.$$

Wegen $p(\frac{f_1}{g_1},\ldots,\frac{f_s}{g_s}) = 0$ gilt dann $\overline{q}(f_1,\ldots,f_s,\ g_1,\ldots,g_s) = p(\frac{f_1}{g_1},\ldots,\frac{f_s}{g_s}) \cdot (g_1 \cdots g_s)^m = 0$. Da $q \in k[\boldsymbol{a},\boldsymbol{b}]$, gilt wegen $t_i g_i \equiv f_i \pmod{J}$ auch

$$\overline{q}(t_1 g_1,\ldots,t_s g_s,\ g_1,\ldots,g_s) \in J.$$

Das bedeutet

$$p(t_1,\ldots,t_s) \cdot (g_1,\ldots,g_s)^m \in J.$$

Durch Multiplikation mit y^m erhalten wir

$$p(t_1,\ldots,t_s) \cdot (g_1,\ldots,g_s)^m \cdot y^m \in J.$$

Wegen Lemma 12.11 gilt $(g_1,\ldots,g_s)^m \cdot y^m - 1^m \in J$. Also gilt auch $p(t_1,\ldots,t_s) \cdot (g_1,\ldots,g_s)^m \cdot y^m - p(t_1,\ldots,t_s) \in J$. Insgesamt gilt also $p(t_1,\ldots,t_s) \in J$. Somit gilt $p \in J$.

(2)⇒(1): Seien $a_1,\ldots,a_s,b_1,\ldots,b_s \in R[\boldsymbol{t},y]$ so, dass

$$p(\boldsymbol{t}) = \sum_{i=1}^{s} a_i(\boldsymbol{t},y)(f_i - t_i g_i)) + \sum_{i=1}^{s} b_i(\boldsymbol{t},y)(y\prod_{j=1}^{s} g_i - 1).$$

Diese gilt auch, wenn man in $Q(R)$ für $t_i := \frac{f_i}{g_i}$ und für $y_i := \frac{1}{g_1 \cdots g_s}$ einsetzt. Es gilt dann $p(\boldsymbol{t}) = 0$, also (1). □

KOROLLAR 12.16 (Algebraische Abhängigkeit in $k(x_1, \ldots, x_n)$). *Sei k ein Körper, seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, $g_1, \ldots, g_s \in k[x_1, \ldots, x_n] \setminus \{0\}$. Sei $p \in k[t_1, \ldots, t_s]$. Sei*

$$J := \left\langle f_1 - t_1 g_1, \ldots, f_s - t_s g_s, y \prod_{i=1}^{s} g_i - 1 \right\rangle_{k[\boldsymbol{t}, y, \boldsymbol{x}]}.$$

Dann sind äquivalent:

(1) $p(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}) = 0$. *Dabei wird im Körper der rationalen Funktionen, also in $Q(k[x_1, \ldots, x_n]) = k(x_1, \ldots, x_n)$ gerechnet.*
(2) $p \in J \cap k[t_1, \ldots, t_s]$.

Beweis: Wir verwenden Satz 12.15 für $R := k[x_1, \ldots, x_n]$. □

ÜBUNGSAUFGABEN 12.17

(1) (cf. [**CLO92**])
   (a) *Whitney's umbrella* is defined by the parametrization $x = uv, y = v, z = u^2$. Find an equation of the form $p(x, y, z) = 0$ with $p \neq 0$ that is satisfied by all points of this surface.
   (b) Find a (nontrivial) equation satisfied by all points in the plane on the *Folium of Descartes* parametrized by $x = \frac{3t}{1+t^3}, y = \frac{3t^2}{1+t^3}$. *Hint:* Find p with $p(\frac{3t}{1+t^3}, \frac{3t^2}{1+t^3}) = 0$.

4. Zugehörigkeit zu Ring- und Körpererweiterungen

Wir werden uns in dieser Sektion überlegen, wie wir bestimmen können, ob eine rationale Funktion $\frac{a}{b} \in k(t_1, \ldots, t_n)$ in einer gegebenen Körpererweiterung $k(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s})$ liegt.

Zunächst beobachten wir, dass wir aus Satz 12.15 und dem Homomorphiesatz ein Ideal I von $k[x_1, \ldots, x_{s+1}]$ finden können, sodass $k[\![\frac{a}{b}, \frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}]\!]$ isomorph zu $k[x_1, \ldots, x_{s+1}]/I$ ist. Nun werden wir uns überlegen, wie wir im Restklassenring eines Polynomrings rechnen,

DEFINITION 12.18. Sei k ein Körper, seien $n \in \mathbb{N}$, $m \in \mathbb{N}_0$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Das Polynom $p = \sum_{i=0}^{m} p_i(x_2, \ldots, x_n) x_1^i \in k[x_1, \ldots, x_n]$ ist ein *kritisches Polynom für x_1 in I*, wenn

(1) $p \in I$, und
(2) es gibt $j \in \{0, \ldots, m\}$, sodass $p_j(x_2, \ldots, x_n) \notin I$.

DEFINITION 12.19. Sei k ein Körper, seien $n \in \mathbb{N}$, $m \in \mathbb{N}_0$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Das Polynom $p = \sum_{i=0}^{m} p_i(x_2, \ldots, x_n) x_1^i \in k[x_1, \ldots, x_n]$ ist ist ein *kritisches Polynom minimalen Grades für x_1 in I*, wenn

(1) p ist kritisch für x_1 in I, und
(2) Für alle q, die kritisch für x_1 in I sind, gilt $\deg_{x_1}(q) \leq \deg_{x_1}(p)$.

Wenn es ein kritisches Polynom gibt, so finden wir ein kritisches Polynom minimalen Grades mithilfe der Berechnung einer Gröbnerbasis.

SATZ 12.20. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Wir nehmen an, dass es ein kritisches Polynom für x_1 in I gibt. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine Gröbnerbasis von I bezüglich $\leq$. Dann enthält G ein kritisches Polynom minimalen Grades für x_1 in I.*

Beweis: Sei f ein kritisches Polynom für x_1 in I, für das $\text{DEG}(f)$ minimal ist. Da $f \in I$, gilt $\text{LT}(f) \in \text{LT}(I)$. Also gibt es ein $g \in G$, sodass $\text{LT}(g) | \text{LT}(f)$. Sei $f_1 = f - \frac{\text{LT}(f)}{\text{LT}(g)} g$. Nun hat f_1 kleineren Multigrad als f. Wegen der Minimalität von f ist f_1 also nicht kritisch. Es gibt also $m \in \mathbb{N}_0$ und $a_0, \ldots, a_m \in I \cap k[x_2, \ldots, x_n]$, sodass $f_1 = \sum_{i=0}^m a_i(x_2, \ldots, x_n) x_1^i$.

Nehmen wir nun an, g ist nicht kritisch. Dann gibt es $l \in \mathbb{N}_0$ und $b_0, \ldots, b_l \in I \cap k[x_2, \ldots, x_n]$, sodass $g = \sum_{i=0}^l b_i(x_2, \ldots, x_n) x_1^i$. Dann lässt sich auch $\frac{\text{LT}(f)}{\text{LT}(g)} g$ als Summe $\sum_i c_i(x_2, \ldots, x_n) x_1^i$ schreiben, wobei alle $c_i \in I \cap k[x_2, \ldots, x_n]$ liegen. Dann ist $f = f_1 + \frac{\text{LT}(f)}{\text{LT}(g)} g$ nicht kritisch für x_1, im Widerspruch zur Wahl von f.

Also ist g kritisch. Wir zeigen nun, dass g ein kritisches Polynom minimalen Grades ist. Sei dazu p ein kritisches Polynom. Es gilt $\text{DEG}(g) \leq \text{DEG}(f)$ und $\text{DEG}(f) \leq \text{DEG}(p)$, insgesamt also $\text{DEG}(g) \leq \text{DEG}(p)$. Da die Monomordnung zuerst nach dem Grad in x_1 ordnet, gilt also $\deg_{x_1}(g) \leq \deg_{x_1}(p)$. □

Wir finden also in jeder Gröbnerbasis bezüglich einer geeigneten Monomordnung ein kritisches Polynom von minimalem Grad in x_1.

LEMMA 12.21. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine Gröbnerbasis von I bezüglich $\leq$. Wenn G reduziert ist, so ist jedes Polynom in G mit $\deg_{x_1}(p) \geq 1$ kritisch für x_1 in I.*

Beweis: Sei $p = \sum_{i=0}^n p_i(x_2, \ldots, x_n) x_1^i \in G$ mit $n := \deg_{x_1}(p) \geq 1$.

Wenn $p_n \in I$, so gibt es ein $g \in G$ mit $\text{LT}(g) | \text{LT}(p_n)$. Wegen der Eigenschaft der Ordnung gilt $\text{LT}(p) = \text{LT}(p_n) \cdot x_1^n$. Also gilt $\text{LT}(g) | \text{LT}(p)$. Da G reduziert ist, gilt also $g = p$. Dann gilt aber $\deg_{x_1}(p) = 0$, im Widerpruch zu den Voraussetzungen an p.

Es gilt also $p_n \notin I$. Somit ist p kritisch für x_1 in I. □

DEFINITION 12.22. Seien A, B kommutative Ringe mit Eins, und sei $b \in B$. Wir nehmen an, dass b algebraisch über A ist. Ein *Minimalpolynom von b über A* ist ein Polynom p minimalen Grades in $A[t]$, das $p \neq 0$ und $\overline{p}(b) = 0$ erfüllt.

LEMMA 12.23. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $p = \sum_{i=1}^m p_i(x_2, \ldots, x_m) x_1^i \in k[x_1, \ldots, x_n]$. Äquivalent sind:*

1. *$q(t) := \sum_{i=1}^m \overline{p_i}(x_2 + I, \ldots, x_n + I) \cdot t^i$ ist ein Minimalpolynom von $x_1 + I$ über $k[\![x_2 + I, \ldots, x_n + I]\!]$.*
2. *p ist ein kritisches Polynom minimalen Grades für x_1 in I.*

Beweis: Sei $\Phi : k[x_1, \ldots, x_n] \to k[\![x_2 + I, \ldots, x_n + I]\!][t]$, $\Phi(\sum_{i=1}^m p_i(x_2, \ldots, x_n) x_1^i) := \sum_{i=1}^m \overline{p_i}(x_2 + I, \ldots, x_n + I)\, t^i$.

Zunächst gilt $p \in I$ genau dann, wenn $\overline{\Phi(p)}(x_1 + I) = 0$. Für $p \in I$ gilt $\Phi(p) = 0$ genau dann, wenn p nicht kritisch für x_1 in I ist.

Somit ist p genau dann ein kritisches Polynom minimalen Grades für x_1 in I, wenn $\Phi(p)$ ein Minimalpolynom für $x_1 + I$ über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist. □

Wir lösen nun als Anwendung dieser Sätze einige Beispiele.

BEISPIEL 12.24. Bestimmen Sie, ob x^3 im Unterkörper $\mathbb{Q}\big(x^2+2, x^5+x+1\big)$ liegt. Finden Sie gegebenenfalls Polynome $f_1, f_2 \in \mathbb{Q}[t_1, t_2]$, sodass $\frac{f_1(x^2+2,x^5+x+1)}{f_2(x^2+2,x^5+x+1)} = x^3$.

Lösung: Wir betrachten den Ring $R := k[\![x^3, x^2+2, x^5+x+1]\!]$. Sei

$$\begin{array}{rccc} \varphi & : & k[x_1,x_2,x_3] & \longrightarrow & k[x] \\ & & p & \longmapsto & p(x^3, x^2+2, x^5+x+2) \end{array}.$$

Die Abbildung φ ist ein Ringhomomorphismus mit $\varphi(x_1) = x^3$, $\varphi(x_2) = x^2 + 2$, und $\varphi(x_3) = x^5 + x + 2$. Den Kern dieser Abbildung kann man mithilfe von Korollar 12.14 finden. Wir berechnen dazu eine reduzierte Gröbnerbasis von

$$J = \big\langle x_1 - x^3, x_2 - (x^2+2), x_3 - (x^5+x+1)\big\rangle_{k[x,x_1,x_2,x_3]}$$

bezüglich der lexikographischen Ordnung mit $x > x_1 > x_2 > x_3$. Mathematica liefert diese Gröbnerbasis als

$$\begin{aligned} &x_2^5 - 10x_2^4 + 42x_2^3 - 92x_2^2 + 105x_2 - x_3^2 + 2x_3 - 51 \\ &x_1x_3 - x_1 - x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20 \\ &x_1x_2^2 - 4x_1x_2 + 5x_1 - x_2x_3 + x_2 + 2x_3 - 2 \\ &x_1^2 - x_2^3 + 6x_2^2 - 12x_2 + 8 \\ &x + x_1x_2 - 2x_1 - x_3 + 1 \end{aligned}$$

Das Ideal $I = J \cap k[x_1, x_2, x_3]$ wird also wegen der Eliminationseigenschaft, Satz 10.36, von den ersten 4 Polynomen dieser Basis erzeugt. Das Polynom

$$p = x_1x_3 - x_1 - x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20$$

ist aufgrund von Lemma 12.21 ein kritisches Polynom für x_1 in $J \cap k[x_1, x_2, x_3]$. Aufgrund von Satz 12.20 (oder weil p linear in x_1 ist), ist p auch kritisch minimalen Grades. Also ist wegen Lemma 12.23

$$(-x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20 + I)\ t^0 + (x_3 - 1 + I)\ t$$

ein Minimalpolynom von $x_1 + I$ über $k[\![x_2 + I, x_3 + I]\!]$. Wenn wir das in den isomorphen Ring $k[\![x, x^2+2, x^5+x+1]\!]$ übertragen, so ist mit $y_2 := x^2 + 2$ und $y_3 := x^5 + x + 1$ das Polynom

$$(-y_2^4 + 8y_2^3 - 25y_2^2 + 36y_2 - 20)t^0 + (y_3 - 1)t$$

ein Minimalpolynom von x^3 über $k[\![x^2+2, x^5+x+1]\!] = k[\![y_2, y_3]\!]$. Es gilt also

$$x^3 = \frac{y_2^4 - 8y_2^3 + 25y_2^2 - 36y_2 + 20}{y_3 - 1}.$$

Also liegt x^3 in $k\big(x^2+2, x^5+x+1\big)$, und $r(t_1, t_2) := \frac{t_1^4 - 8t_1^3 + 25t_1^2 - 36t_1 + 20}{t_2 - 1}$ erfüllt $r(x^2+2, x^5+x+1) = x^3$. □

Mit diesen Sätzen haben wir also Algorithmen, für $a, f_1, \dots, f_s \in k[\boldsymbol{x}]$ und $b, g_1, \dots, g_s \in k[\boldsymbol{x}]$ folgende Fragen beantworten:

(1) Gilt $\frac{a}{b} \in k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)$?
(2) Ist die Körpererweiterung $k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)\big(\frac{a}{b}\big)$ algebraisch über $k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)$?
(3) Wenn diese Körpererweiterung algebraisch ist, was ist ihr Grad?

Wir finden dazu mithilfe von Satz 12.15 ein Ideal I des Polynomrings $k[x_1, \dots, x_{s+1}]$, sodass $k[x_1, \dots, x_{s+1}]/I$ durch φ isomorph zu $k[\![\frac{a}{b}, \frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}]\!]$ ist, und $\varphi(x_1+I) = \frac{a}{b}$, $\varphi(x_{i+1}+I) = \frac{f_i}{g_i}$ für $i \in \{1, \dots, s\}$. Dann bestimmen wir ein Minimalpolynom für x_1+I über $k[\![x_2+I, \dots, x_{s+1}+I]\!]$, indem wir ein kritisches Polynom p minimalen Grades für x_1 in I bestimmen. Wenn es kein kritisches Polynom für x_1 in I gibt, ist $\frac{a}{b}$ nicht algebraisch über $k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)$. Ansonsten erhalten wir aus p ein Minimalpolynom von $\frac{a}{b}$ über $k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)$. Wenn $\deg_{x_1}(p) = 1$, so liegt $\frac{a}{b} \in k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)$. Wenn $\deg_{x_1}(p) > 1$, so ist $\frac{a}{b}$ algebraisch über $k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)$, und $\deg_{x_1}(p)$ ist der Grad der Körpererweiterung $[k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)\big(\frac{a}{b}\big) : k\big(\frac{f_1}{g_1}, \dots, \frac{f_s}{g_s}\big)]$.

Als letztes fragen wir uns noch, ob $x_1 + I$ ganz über $k[\![x_2+I, \dots, x_n+I]\!]$ ist, und, wenn ja, wie ein Polynom kleinsten Grades mit führendem Koeffizienten 1 aussieht, dass das belegt.

Satz 12.25. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \dots, x_n]$. Wir nehmen an, dass $x_1 + I$ ganz über $k[\![x_2+I, \dots, x_n+I]\!]$ ist, und dass m der minimale Grad eines Polynoms mit führendem Koeffizienten 1 ist, das das belegt. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \dots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine Gröbnerbasis von I bezüglich $\leq$. Dann gibt es ein Polynom $g \in G$ mit $\operatorname{Lm}(g) = x_1^m$.*

Beweis: Sei $f \in k[\![x_2+I, \dots, x_n+I]\!][t]$ ein Polynom minimalen Grades, das belegt, dass x_1+I ganz über $k[\![x_2+I, \dots, x_n+I]\!]$ ist. Wir schreiben f als $\sum_{i=0}^{m-1} \overline{f_i}(x_2+I, \dots, x_n+I)\, t^i + t^m$. Wegen $\overline{f}(x_1+I) = 0$ liegt das Polynom $p := \sum_{i=0}^{m-1} f_i(x_2, \dots, x_n)\, x_1^i + x_1^m$ in I.

Da G eine Gröbnerbasis ist, gibt es ein $g \in G$, sodass $\operatorname{Lt}(g) \mid \operatorname{Lt}(p)$. Dann gibt es ein $m_1 \in \mathbb{N}_0$, sodass $\operatorname{Lt}(g) = x_1^{m_1}$. Nun ist $g(t, x_2+I, \dots, x_n+I)$ ein Polynom vom Grad m_1, das belegt, dass x_1+I ganz über $k[\![x_2+I, \dots, x_n+I]\!]$ ist. Wegen der Minimalität von m gilt $m_1 = m$. □

Wir beobachten, dass wir in unseren Beispielen ein Ideal I immer so konstruiert haben, dass $k[x_1, \dots, x_n]/I$ isomorph zu einem Integritätsbereich ist. In diesem Fall ist das Ideal I prim.

Satz 12.26. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \dots, x_n]$. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \dots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine reduzierte Gröbnerbasis von I bezüglich $\leq$. Dann gilt:*

(1) *x_1+I liegt genau dann in $k[\![x_2+I, \dots, x_n+I]\!]$, wenn G ein Polynom p mit $\operatorname{Lm}(p) = x_1$ enthält.*
(2) *x_1+I ist genau dann ganz über $k[\![x_2+I, \dots, x_n+I]\!]$, wenn es ein $m \in \mathbb{N}$ gibt, sodass G ein Polynom p mit $\operatorname{Lm}(p) = x_1^m$ enthält.*
(3) *x_1+I ist genau dann algebraisch über $k[\![x_2+I, \dots, x_n+I]\!]$, wenn G ein Polynom p mit $\deg_{x_1}(p) \neq 0$ enthält. Der Grad des Minimalpolynoms von x_1+I ist $\min\{\deg_{x_1}(p) \mid p \in G,\ \deg_{x_1}(p) \neq 0\}$.*

(4) *Wir nehmen an, dass I prim ist. Dann ist $k[\![x_1+I,\dots,x_n+I]\!]$ ein Integritätsbereich. Sei K sein Quotientenkörper. Dann liegt x_1+I genau dann in $k(x_2+I,\dots,x_n+I)$, wenn G ein Polynom p mit $\deg_{x_1}(p)=1$ enthält.*

Beweis: (1) Wenn $x_1+p_0(x_2,\dots,x_n)\in I$, so gilt $x_1+I=-\overline{p_0}(x_2+I,\dots,x_n+I)$, also $x_1+I\in k[\![x_2+I,\dots,x_n+I]\!]$. Wenn $x_1+I\in k[\![x_2+I,\dots,x_n+I]\!]$, so ist x_1+I ganz über $k[\![x_2+I,\dots,x_n+I]\!]$, und $t-(x_1+I)$ ist ein Polynom vom Grad 1, das das belegt. Somit gibt es nach Satz 12.25 ein Polynom in G mit $\textsc{Lm}(g)=x_1$.

(2) Dieser Teil ergibt sich genauso aus Satz 12.25.

(3) Ergibt sich aus Satz 12.20, Lemma 12.21 und Lemma 12.23.

(4) Wir nehmen an, es gibt ein Polynom $r=q(x_2,\dots,x_n)\,x_1+p(x_2,\dots,x_n)$ mit $\deg_{x_1}(r)=1$, das in G liegt. Nach Lemma 12.21 ist dieses Polynom auch kritisch. Da $\overline{q}(x_2+I,\dots,x_n+I)\neq 0+I$, gilt dann $x_1+I=\frac{\overline{p}(x_2+I,\dots,x_n+I)}{\overline{q}(x_2+I,\dots,x_n+I)}$. Wir nehmen nun an x_1+I liegt im Quotientenkörper. Dann ist x_1+I algebraisch über $k[\![x_2+I,\dots,x_n+I]\!]$ mit einem Minimalpolynom vom Grad 1. Dann gibt es ein kritisches Polynom p mit $\deg_{x_1}(p)=1$ in I, und wegen Satz 12.20 auch in G. □

Übungsaufgaben 12.27

(1) Let $I:=(x_1^2-3,x_2^2-2)$, and let $R:=\mathbb{Q}[x_1,x_2]/I$.
   (a) Find an Ideal J of $\mathbb{Q}[t_1,t_2,t_3]$ such that $\mathbb{Q}[\boldsymbol{t}]/J$ is isomorphic to R, and an isomorphism φ with $\varphi(t_1+J)=(x_1+x_2)+I$, $\varphi(t_2+J)=x_1+I$, $\varphi(t_3+J)=x_2+I$.
   (b) Find an ideal K of $\mathbb{Q}[s_1]$ such that $\mathbb{Q}[s_1]/K$ is isomorphic to the subring of $\mathbb{Q}[\boldsymbol{t}]/J$ generated by t_1+J via an isomorphism ψ with $\psi(t_1+J)=s_1+K$.
   (c) Find a polynomial witnessing that x_1+x_2+I is integral over $\mathbb{Q}$.

(2) Let $R=\mathbb{Q}[t^5,t^7]$. Find polynomials of minimal degrees that witness that t is algebraic and integral over R.

(3) Find a solution of $6a+9b+20c=53$ in $\mathbb{N}_0^3$ by finding a polynomial $p(t_1,t_2,t_3,t_4)=t_1-t_2^at_3^bt_4^c$ with $p(x^{53},x^6,x^9,x^{20})=0$.

(4) Find the gcd of 147 and 33 and the cofactors by finding a polynomial $p(t_1,t_2,t_3,t_4,t_5)=t_1^d-t_2^{u_1}t_3^{u_2}t_4^{v_1}t_5^{v_2}$ such that $p(x^1,x^{147},\frac{1}{x^{147}},x^{33},\frac{1}{x^{33}})=0$ with minimal nonzero d.

(5) Let

$$f=\left(\left(x^2+y\right)^2+2\right)^3,$$

$$g=\left(\left(x^2+y\right)^2+1\right)^2$$

be polynomials over $\mathbb{Q}$. For each $h\in\{x,x^2+y,(x^2+y)^2\}$, find an ideal I such that $\mathbb{Q}[t_1,t_2,t_3]/I$ is isomorphic to $\mathbb{Q}[\![h,f,g]\!]$ and answer the following questions:
   (a) Is h an element of $\mathbb{Q}[\![f,g]\!]$? How can h be expressed as $p(f,g)$?
   (b) Is h integral over $\mathbb{Q}[\![f,g]\!]$? In this case, find a polynomial in $\mathbb{Q}[\![f,g]\!][t]$ witnessing this fact.
   (c) Is h algebraic over $\mathbb{Q}[\![f,g]\!]$? In this case, find a polynomial in $\mathbb{Q}[\![f,g]\!][t]$ witnessing this fact.
   (d) Do we have $h\in\mathbb{Q}(f,g)$? In this case, find polynomials $p,q\in\mathbb{Q}[X,Y]$ with $h=p(f,g)/q(f,g)$.

(6) Let k be a field, and let R be a subring of k containing 1. Suppose that every $\alpha\in k$ is integral over R. Show that R is a field. *Hint:* What can you say about $\frac{1}{r}$ for $r\in R$?

(7) * [**Eng41**] Let $a,b,q,r,f\in\mathbb{Q}[x]$ such that $\deg(f)>0$, $b\neq 0$, $a=q\cdot b+r$ and $\deg(r)<\deg(b)$. Suppose that $a,b\in\mathbb{Q}[\![f]\!]$. Show that q and r are elements of $\mathbb{Q}[\![f]\!]$.

5. Wechsel des Grundkörpers

In dieser Sektion betrachten wir zwei Körper k, K mit $k \leq K$. Für ein Ideal I von $k[\boldsymbol{x}]$ bezeichnen wir mit $\overline{I}$ das Ideal $\langle I \rangle_{K[\boldsymbol{x}]}$.

SATZ 12.28. *Es gilt:*

(1) $\overline{I} \cap k[\boldsymbol{x}] = I$.
(2) $\overline{I \cap J} = \overline{I} \cap \overline{J}$.
(3) $\overline{I + J} = \overline{I} + \overline{J}$.
(4) *Der k-Vektorraum $k[\boldsymbol{x}]/I$ und der K-Vektorraum $K[\boldsymbol{x}]/\overline{I}$ haben die gleiche Dimension.*

Beweis: (1) Sei $G = \{g_1, \ldots, g_t\}$ eine Gröbnerbasis von I. Dann gilt $\langle G \rangle_{K[\boldsymbol{x}]} = \overline{I}$. Wegen Satz 11.5 ist G auch eine Gröbnerbasis von $\overline{I}$. Let $f \in \overline{I} \cap k[\boldsymbol{x}]$. Dann besitzt f nach Satz 10.16 eine Standarddarstellung $\sum \overline{h}_i g_i$ bezüglich G. Aus dem Beweis von Satz 10.16 sieht man auch, dass man die $\overline{h}_i$ so wählen kann, dass sie nicht nur in $K[\boldsymbol{x}]$, sondern sogar in $k[\boldsymbol{x}]$ liegen. Daher gilt $f \in I$.

(2) Da $\overline{I}$ und $\overline{J}$ sich jeweils von einer endlichen Teilmenge von $k[\boldsymbol{x}]$ erzeugen lassen, gilt das wegen Korollar 12.9 und Satz 10.36 auch für $\overline{I} \cap \overline{J}$. Daher gilt $\overline{I} \cap \overline{J} = \left\langle \overline{I} \cap \overline{J} \cap k[\boldsymbol{x}] \right\rangle_{K[\boldsymbol{x}]} = \langle I \cap J \rangle_{K[\boldsymbol{x}]} = \overline{I \cap J}$.

(3) Es gilt $I \cup J \subseteq \overline{I} + \overline{J}$ und folglich $\overline{I + J} \subseteq \overline{I} + \overline{J}$. Die Inklusion $\overline{I} + \overline{J} \subseteq \overline{I + J}$ ist offensichtlich.

(4) Sei G eine Gröbnerbasis von I in $k[\boldsymbol{x}]$. Dann gilt $\langle G \rangle_{K[\boldsymbol{x}]} = \overline{I}$. Aus dem S-Polynom-Kriterium sieht man, dass G auch eine Gröbnerbasis von $\overline{I}$ ist. Eine Basis K-Vektorraums $K[\boldsymbol{x}]/\overline{I}$ wird von jenen Monomen gebildet, die keine Vielfachen eines Elements in $\mathrm{LT}(G)$ sind. Also gilt $\dim_K(K[\boldsymbol{x}]/\overline{I}) = \dim_k(k[\boldsymbol{x}]/I)$. □

ÜBUNGSAUFGABEN 12.29

(1) Let k be a field and let M be a $k[x,y]$-submodule of $k[x,y] \times k[x,y]$. Let J be the ideal of $k[x,y,e_1,e_2]$ generated by $\{e_1^2, e_1e_2, e_2^2\}$. Show that $I := \{(m_1e_1 + m_2e_2) + J \mid (m_1, m_2) \in M\}$ is an ideal of $k[x,y,e_1,e_2]/J$.
(2) By solving an ideal membership question, determine which of the vectors $(0, x^2y - xy^3)$ and $(x^2 - xy^2, 0)$ lie in the submodule of $\mathbb{Q}[x,y] \times \mathbb{Q}[x,y]$ that is generated by (x^2+1, y) and (xy^2+1, y)
(3) For an $m \times n$-matrix with entries in $\mathbb{Q}[\boldsymbol{x}]$, we let $\mathrm{row}(A) = \{vA \mid v \in \mathbb{Q}[\boldsymbol{x}]^m\}$ be its row module. Compute generators of the intersection

$$\mathrm{row}\begin{pmatrix} xy^2+1 & -4 & x \\ 0 & x & 0 \end{pmatrix} \cap \mathrm{row}\begin{pmatrix} 1 & -4 & x \\ 0 & 4y & -xy \end{pmatrix}.$$

Hint: Intersect the corresponding ideals of $\mathbb{Q}[x,y,e_1,e_2,e_3]$.
(4) Compute a set of generators for the module

$$\{(f_1, f_2) \in \mathbb{Q}[x,y]^2 \mid (x^2y^3 + xy^3 + 3x + 3)f_1 + (xy^5 + xy^3 + 3y^2 + 3)f_2 = 0\}$$

and explain how the solution relates to the gcd of the given polynomials.
(5) Let $n \in \mathbb{N}$ and let A and B be submodules of the $\mathbb{Q}[\boldsymbol{x}]$-module $\mathbb{Q}[\boldsymbol{x}]^n$. Assume:
   (a) $A \subseteq B$

(b) $\forall i \in \{1,\dots,n\}$, $\forall g \in \mathbb{Q}[\boldsymbol{x}]$, $\forall r_{i+1},\dots,r_n \in \mathbb{Q}[\boldsymbol{x}]$:

$$\Big((\underbrace{0,\dots,0}_{i-1}, g, r_{i+1},\dots,r_n) \in B \Longrightarrow$$
$$\exists s_{i+1},\dots,s_n \in \mathbb{Q}[\boldsymbol{x}] \quad : \quad (0,\dots,0,g,s_{i+1},\dots,s_n) \in A \Big).$$

Show that then $A = B$.

(6) Compute generators for the solution module of the linear system

$$\begin{pmatrix} x^2y & x & y^3-x & -y^2 \\ x^2y & -x & y^3+x & -y^2 \\ x^3 & y & xy^2-y & -xy \end{pmatrix} \cdot \boldsymbol{v} = 0.$$

Hint: Let

$$M := \begin{pmatrix} x^2y & x^2y & x^3 & 1\,0\,0\,0 \\ x & -x & y & 0\,1\,0\,0 \\ y^3-x & x+y^3 & xy^2-y & 0\,0\,1\,0 \\ -y^2 & -y^2 & -xy & 0\,0\,0\,1 \end{pmatrix},$$

and compute $\mathrm{row}(M) \cap (\{0\}^3 \times \mathbb{Q}[x,y]^4)$.

(7) For $A \in R^{m\times n}$, let $\mathrm{col}(A) = \{Ax \mid x \in R^n\}$ be the column module of A and $\ker(A) = \{y \in R^n \mid Ay = 0\}$ be the module of solutions of $Ay = 0$. Let I_n be the $n \times n$ identity matrix. Prove the following statement:

Let R be a commutative ring with unit, let $l, m, n \in \mathbb{N}$, and let $F \in R^{l\times n}$, $G \in R^{l\times m}$, $A \in R^{n\times m}$, $B \in R^{m\times n}$ be such that $FA = G$ und $GB = F$. Then we have

$$\ker(F) = \{Ay \mid y \in \ker(G)\} + \mathrm{col}(I_n - AB).$$

Remark: This exercise is used when computing syzygies via the S-polynomial method.

(8) Let $A \in \mathbb{Q}[x,y,z]^{4\times 4}$ be defined by

$$A = \begin{pmatrix} x^2+y & z\left(x^2+y\right) & x^2 & 0 \\ y-z & z(y-z) & 0 & 0 \\ 0 & 0 & x^2z+2y & 0 \\ 0 & 0 & z & 1 \end{pmatrix}.$$

(a) Compute a matrix H in echelon normal form that has the same row module as A.

(b) Use this matrix H to compute $\mathrm{row}(A) \cap (\{0\}^r \times \mathbb{Q}[x,y,z]^{4-r})$ for $r \in \{1,2,3\}$.

(c) Compute module generators for $\ker(A)$.

(9) Let

$$A := \begin{pmatrix} x & 0 & xz+y & 1 \\ x^2 & z & y & 0 \end{pmatrix}.$$

(a) Compute generators for the solution module (over the ring $\mathbb{Q}[x,y,z]$)

$$\{(v_1,v_2,v_3,v_4) \in \mathbb{Q}[x,y,z]^4 \mid A \cdot (v_1,v_2,v_3,v_4)^T = 0\}.$$

(b) Compute a basis for the subvectorspace of $\mathbb{Q}(x,y,z)^4$ (as a vector space over $\mathbb{Q}(x,y,z)$) defined by

$$\{(v_1,v_2,v_3,v_4) \in \mathbb{Q}(x,y,z)^4 \mid A \cdot (v_1,v_2,v_3,v_4)^T = 0\}$$

with all basis vectors lying in $\mathbb{Q}[x,y,z]$.

KAPITEL 13

Strong Gröbner bases over Euclidean domains

1. Introduction

This chapter provides a self-contained introduction to Gröbner bases of submodules of $R[x_1, \ldots, x_n]^k$, where R is a Euclidean domain, and explains how to use these bases to solve linear systems over $R[x_1, \ldots, x_n]$. It is an almost verbatim copy of the article [Aic24].

The computation of Gröbner bases is a broadly applicable method that solves many questions involving polynomials. One such question is solving systems of linear equations over a commutative ring D. Here, for a matrix $A \in D^{r\times s}$ and $b \in D^r$, one would like to compute an $x \in D^s$ with $Ax = b$ (when it exists) and a basis of the module $\ker(A) = \{x \in D^s \mid Ax = 0\}$; then $\{x + k \mid k \in \ker(A)\}$ is the set of solutions of the linear system. When D is a multivariate polynomial ring such as $\mathbb{Z}[x_1, x_2]$ or $\mathbb{Q}[x_1, x_2]$, Gröbner bases are a tool to solve these questions. Being able to solve linear systems over D allows us to determine ideal membership in D (solve $d_1x_1 + \cdots + d_nx_n = d$ over D to find out whether d lies in the ideal generated by $d_1, \ldots, d_n$) and to compute least common multiples (solve $x_1 - d_1x_2 = x_1 - d_2x_3 = 0$ for finding x_1 as a common multiple of d_1, d_2), and hence also greatest common divisors when D is a unique factorization domain.

When D is a field, solving linear equations is accomplished by Gauß's algorithm. When $D = \mathbb{Z}$, solving systems of linear diophantine equations can be done computing the Hermite normal form of a matrix. Both cases are contained in the case that $D = R[x_1, \ldots, x_n] =: R[\boldsymbol{x}]$, where R is a Euclidean domain, and in the present note, we explain how to solve linear systems over $R[\boldsymbol{x}]$. The role of the row echelon form of a matrix (when D is a field) and of the Hermite normal form (when D is a Euclidean domain) will be taken by a matrix whose rows are a Gröbner basis of the module generated by the rows of the matrix. Our approach includes computing Gröbner bases over $\mathbb{Z}$, allowing us to do linear algebra over $\mathbb{Z}[x_1, \ldots, x_n]$. As every finitely generated ring is isomorphic to a quotient $\mathbb{Z}[x_1, \ldots, x_n]$ by an ideal I (which is finitely generated by Hilbert's Basis Theorem), this will allow us to solve linear systems over all finitely generated rings. In fact, the Gröbner basis algorithm presented here (which is a modification of the algorithm given in [Lic12]) will contain both Gauß's algorithm and the Hermite normal form as special instances.

As we do not presuppose any knowledge on Gröbner bases, let us start with a rough description: Given a submodule M of the D-module D^s, a Gröbner basis is a set of generators of M with particularly useful properties. They were introduced by B. Buchberger, who presented an algorithm to compute such bases when $D = k[x_1, \ldots, x_n]$ (k a field) and $s = 1$ [Buc65, Buc70] and named them in honour of his supervisor W. Gröbner. Generalizing to $s > 1$

is then straightforward. The case $D = \mathbb{Z}[x_1, \ldots, x_n]$ provides additional difficulties, as now diophantine linear equations over $\mathbb{Z}$ are included. For this case, several types of Gröbner bases were introduced. We will use "strong Gröbner bases", and one main source for our development is [**Lic12**]. The case that $D = R[x_1, \ldots, x_n]$ for a Euclidean domain R has also been treated in [**KRK88**, **Pan89**]. What our treatment adds to these is that we:

- consider bases of submodules of D^s also for the case $s > 1$,
- provide self-contained proofs of the Gröbner basis criterion Theorem 13.10 and of the uniqueness of reduced strong Gröbner bases,
- explain how reduction and augmentation by S-polynomials can be interleaved in the course of the algorithm, and
- explicitly state how to solve linear systems over D.

The computations will start from a generating set F of a submodule of D^s and compute a set of generators G (a Gröbner basis) with certain desirable properties. The algorithm is a sequence of the following steps, which we illustrate here by examples for the case $D = \mathbb{Z}[x, y]^3$.

- Augmentation: When $f = (10x^2y^2 + y, 0, x)$ and $g = (4x^3y + x^2, 1, 0)$ are in F, then add $h = x\,f - 2y\,g = (2x^3y^2 - 2x^2y + xy, -2y, x^2)$ to F. One important property of h is that the leading coefficient 2 of h is smaller than the leading coefficients 10 of f and 4 of g. Such an h is called an *S-polynomial vector* (from "subtraction", cf. [**Buc70**, p. 376]).
- Reduction: When $f = (10x^2y^2 + y, 0, x)$ and $g = (x - 2y, 1, 0)$ are in F, then replace f by $f' = f - 10xy^2g = (20xy^3 + y, -10xy^2, x)$.

When these simple steps are performed in some proper order, the process will eventually terminate and produce a set of generators G that will have the required properties. Termination is proved using the fact that certain partially ordered sets have no infinite descending chains. The fact that the final result G has the desired properties uses a central theorem on S-polynomials vectors. For the case that R is a field this theorem goes back to [**Buc65**] (cf. [**Buc76**, Theorem 3.3]). It has been adapted to other situations. For the case $R = \mathbb{Z}$, its role is taken by [**Lic12**, Theorem 10], for Euclidean domains by [**KRK88**, Theorem 4.1] or [**Pan89**, Theorem 1.5], and in our presentation by Theorem 13.10. From the vast literature on Gröbner bases, we highlight the monographs [**CLO92**, **BW93**, **AL94**, **GP02**] and the survey paper [**BK10**]. The mathematical content of the present note builds upon [**KRK88**, **Lic12**]; our definition of S-polynomials differs from the one given in [**Lic12**], was inspired by [**Buc84**] and is close to [**KRK88**, Definition CP1]. The proof of Theorem 13.10 was modelled after the proof of Theorem 2.3.10 in [**Smi14**], and the notation using "expressions with remainders" follows [**Eis95**]. I am indebted to M. Kauers for sharing the unpublished notes for his course on Gröbner bases at JKU in 2011 with me. The presentation of how to solve linear systems in Theorem 13.30 was inspired by his lectures on linear algebra.

The goal of the present note is to provide a self-contained presentation of as much of Gröbner basis theory as is needed to solve linear systems of over $\mathbb{Z}[x_1, \ldots, x_n]$ (or $R[x_1, \ldots, x_n]$ for a Euclidean domain R) in Section 8, along with proofs that are ready for the classroom. Some

facts on partial orders go beyond the material one commonly presupposes in an undergraduate course. These facts are collected in Section 9. Most of the theory contained in the present note is well known, but has so far been scattered in various research publications, sometimes also with variations in the definitions. We aim at providing one coherent presentation of these beautiful methods.

2. Basic definitions

We write $\mathbb{N}$ for the set of positive integers and $\underline{k}$ for the set $\{1,\dots,k\}$. For a set G, we write $\binom{G}{2}$ for the set of two-element subsets of G. We write $A \subseteq B$ to say that A is a subset of B, and $A \subset B$ for ($A \subseteq B$ and $A \neq B$). An ordered set $(W,\leq)$ is *well ordered* if $\leq$ is a total order on W and every nonempty subset S of W contains a minimal element.

Definition 13.1. Let R be an integral domain. R is a *Euclidean domain* if there is a well ordered set W and a map $\delta : R \to W$ such that $\delta(0) \leq \delta(r)$ for all $r \in R$, and for all $a,b \in R$ with $a \neq 0$, we have that $\delta(b) \leq \delta(ab)$ and that there exist $q,r \in R$ such that $b = qa + r$ and $\delta(r) < \delta(a)$.

Euclidean domains are often defined with $W := \mathbb{N}_0$ as the codomain of the grading function, but allowing arbitrary well ordered sets includes more domains (cf. [**CNT19**]). Let R be a Euclidean domain. For the polynomial ring $R[\boldsymbol{x}] := R[x_1,\dots,x_n]$, we will consider its module $R[\boldsymbol{x}]^k$, and we will call the elements of this module *polynomial vectors*. For $p \in R[x_1,\dots,x_n]$ and $i \in \underline{k}$, we write $p\,e_i$ for the vector $(0,\dots,0,p,0,\dots,0)$ with p at place i. For $\alpha \in {\mathbb{N}_0}^n$, we write $\boldsymbol{x}^\alpha$ for $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$. The elements of $\{a\boldsymbol{x}^\alpha e_i \mid a \in R\setminus\{0\}, (\alpha,i) \in {\mathbb{N}_0}^n \times \underline{k}\}$ are called *term vectors* and the elements of

$$\mathrm{Mon}(n,k) := \{\boldsymbol{x}^\alpha e_i \mid (\alpha,i) \in {\mathbb{N}_0}^n \times \underline{k}\}$$

are called *monomial vectors*. We say that the monomial vector $\boldsymbol{x}^\alpha e_i$ *divides* the monomial vector $\boldsymbol{x}^\beta e_j$ and write $\boldsymbol{x}^\alpha e_i \mid \boldsymbol{x}^\beta e_j$ if $i = j$ and $\alpha_m \leq \beta_m$ for all $m \in \underline{n}$. This holds if and only if there is a monomial $\boldsymbol{x}^\gamma$ such that $\boldsymbol{x}^\gamma \boldsymbol{x}^\alpha e_i = \boldsymbol{x}^\beta e_j$. In this case, we will also write $\frac{\boldsymbol{x}^\alpha e_i}{\boldsymbol{x}^\beta e_j}$ for $\boldsymbol{x}^\gamma$. We say that the term vector $s = a\boldsymbol{x}^\alpha e_i$ *divides* the term vector $t = b\boldsymbol{x}^\beta e_j$ if a divides b in R and $\boldsymbol{x}^\alpha e_i$ divides $\boldsymbol{x}^\beta e_j$. In this case we write $s \mid t$, and we write $\frac{t}{s}$ for the term $q\boldsymbol{x}^\alpha$ with $(q\boldsymbol{x}^\alpha)s = t$. We can write every element from $R[\boldsymbol{x}]^k$ as a sum $\sum_{(\alpha,i)\in E} c_{(\alpha,i)}\boldsymbol{x}^\alpha e_i$, where E is a finite subset of ${\mathbb{N}_0}^n \times \underline{k}$. A fundamental step working with these polynomial vectors is to *order* the terms in this sum so that we can speak about a *leading term vector*. A requirement for this ordering is that when $\sum_{j=1}^m t_j$ is a sum of terms that are in decreasing order, then so is the sum $\sum_{j=1}^m \boldsymbol{x}^\alpha t_j$ obtained by multiplying with a monomial $\boldsymbol{x}^\alpha$. This is reflected in Condition (3) of the following definition. Condition (2) expresses the requirement that for all monomial vectors m_1, m_2 with $m_1 \mid m_2$, we have $m_1 \leq m_2$.

Definition 13.2. Let $n,k \in \mathbb{N}$, and let $\leq$ be an order on $\mathrm{Mon}(n,k)$. This order $\leq$ is *admissible* if

(1) $\leq$ is a total ordering;
(2) for all $\boldsymbol{x}^\alpha e_i, \boldsymbol{x}^\beta e_j \in \mathrm{Mon}(n,k)$ with $\boldsymbol{x}^\alpha e_i \mid \boldsymbol{x}^\beta e_j$, we have $\boldsymbol{x}^\alpha e_i \leq \boldsymbol{x}^\beta e_j$;

(3) for all $\alpha, \beta, \gamma \in {\mathbb{N}_0}^n$ and for all $i, j \in \underline{k}$ with $\boldsymbol{x}^\alpha e_i \leq \boldsymbol{x}^\beta e_j$, we have $\boldsymbol{x}^{\alpha+\gamma} e_i \leq \boldsymbol{x}^{\beta+\gamma} e_j$.

Seeing $M = \{\boldsymbol{x}^\alpha \mid \alpha \in {\mathbb{N}_0}^n\}$ as a (multiplicative) monoid that acts on $V := \mathrm{Mon}(n, k)$, Condition (2) means $v \leq m \cdot v$ for all $m \in M$ and $v \in V$, and Condition (3) that the ordering is compatible with the monoid operation, i.e., $v_1 \leq v_2 \Rightarrow m \cdot v_1 \leq m \cdot v_2$ for all $m \in M$, $v_1, v_2 \in V$. Sometimes we represent $(M, \cdot)$ simply by the isomorphic monoid $({\mathbb{N}_0}^n, +)$ and $\mathrm{Mon}(n, k)$ by ${\mathbb{N}_0}^n \times \underline{k}$; using this viewpoint we say that an ordering $\leq'$ on ${\mathbb{N}_0}^n \times \underline{k}$ is admissible if the ordering $\leq$ defined by $\boldsymbol{x}^\alpha e_i \leq \boldsymbol{x}^\beta e_j :\Leftrightarrow (\alpha, i) \leq' (\beta, j)$ is admissible. This amounts to claiming that $\leq'$ is total, $(\alpha, i) \leq' (\alpha + \gamma, i)$ and $(\alpha, i) \leq' (\beta, j) \Rightarrow (\alpha + \gamma, i) \leq' (\beta + \gamma, j)$ for all $\alpha, \beta, \gamma \in {\mathbb{N}_0}^n$ and $i, j \in \underline{k}$.

One such ordering is the *lexicographic position over term ordering*, where for two distinct (α, i) and $(\beta, j) \in {\mathbb{N}_0}^n \times \underline{k}$, we have $((\alpha_1, \ldots, \alpha_n), i) <_{\mathrm{lex}} ((\beta_1, \ldots, \beta_n), j)$ if $i > j$ or $(i = j$ and $\alpha_l < \beta_l$ for $l := \min\{m \in \underline{k} \mid \alpha_m \neq \beta_m\})$. Other admissible orderings can be defined by choosing a matrix $U \in \mathbb{R}^{n' \times n}$ and a permutation π of $\underline{k}$ such that $\{\gamma \in \mathbb{Q}^n \mid U\gamma = 0\} = \{0\}$ and the first nonzero entry in every column of U is positive. Then one can define an admissible order $\leq_{U,\pi}$ by $(\alpha, i) \leq_{U,\pi} (\beta, j) :\Leftrightarrow (U\alpha, \pi(i)) \leq_{\mathrm{lex}} (U\beta, \pi(j))$.

For a finite subset E of ${\mathbb{N}_0}^n \times \underline{k}$, an admissible ordering $\leq$ of ${\mathbb{N}_0}^n \times \underline{k}$, a function $c : E \to R$, and an $f \in R[x_1, \ldots, x_n]^k$ with $f \neq 0$ given by $f = \sum_{(\alpha,i) \in E} c_{(\alpha,i)} \boldsymbol{x}^\alpha e_i$, we define

$$\textsc{Deg}(f) := \max_{\leq}\{(\alpha, i) \in {\mathbb{N}_0}^n \times \underline{k} \mid c_{(\alpha,i)} \neq 0\};$$

$\textsc{Deg}(0)$ is not defined.

Suppose that $f \neq 0$ and $(\gamma, i) = \textsc{Deg}(f)$. Then we define

$$\textsc{Lm}(f) := \boldsymbol{x}^\gamma e_i,\ \textsc{Lc}(f) := c_{(\gamma,i)},\ \textsc{Lt}(f) := c_{(\gamma,i)} \boldsymbol{x}^\gamma e_i$$

and call them the *leading monomial vector*, the *leading coefficient* and the *leading term vector*, respectively. All of these are undefined for $f = 0$. An important fact is that an admissible ordering on ${\mathbb{N}_0}^n \times \underline{k}$ is a *well order*, i.e., it is total and has no infinite strictly descending chains. A proof is given in Lemma 13.32. This also implies that for every nonempty subset I of $R[\boldsymbol{x}]^k \setminus \{0\}$, there is at least one $f \in I$ such that there is no $g \in I$ with $\textsc{Deg}(g) < \textsc{Deg}(f)$.

Definition 13.3. Let R be a Euclidean domain, let I be a submodule of $R[x_1, \ldots, x_n]^k$, and let $\leq$ be an admissible order of the monomial vectors. Then $G \subseteq I \setminus \{0\}$ is a *strong Gröbner basis* of I with respect to $\leq$ if and only if for every $f \in I \setminus \{0\}$, there is an element $g \in G$ such that $\textsc{Lt}(g) \mid \textsc{Lt}(f)$.

We write $\langle G \rangle$ for the submodule of $R[\boldsymbol{x}]^k$ generated by G. When G is a strong Gröbner basis of I, then $\langle G \rangle = I$: Suppose that $\langle G \rangle$ is a proper subset of I, and let f be a polynomial vector of minimal degree $\textsc{Deg}(f)$ in $I \setminus \langle G \rangle$ with respect to the admissible ordering $\leq$. The existence of such an f – under the assumption $\langle G \rangle \neq I$ – is justified by Lemma 13.32. Taking $g \in G$ such that $\textsc{Lt}(g) \mid \textsc{Lt}(f)$, we compute $f' := f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(g)} g$. If $f' = 0$, then $f = \frac{\textsc{Lt}(f)}{\textsc{Lt}(g)} g$ lies in $\langle G \rangle$. If $f' \neq 0$, then by minimality, f' lies in $\langle G \rangle$, and hence so does $f = f' + \frac{\textsc{Lt}(f)}{\textsc{Lt}(g)} g$, a contradiction.

When R is a Euclidean domain, $\delta : R \to W$ is the grading function of R and $f \in R[x_1, \ldots, x_n]^k \setminus \{0\}$, we define the *degree with* δ of f by

$$\mathrm{DEG}_\delta(f) := (\mathrm{DEG}(f),\ \delta(\mathrm{LC}(f)));$$

hence $\mathrm{DEG}_\delta(f) \in ({\mathbb{N}_0}^n \times \underline{k}) \times W$. For a subset I of $R[\boldsymbol{x}]^k$, we define $\mathrm{DEG}_\delta(I) := \{\mathrm{DEG}_\delta(f) \mid f \in I \setminus \{0\}\}$. On ${\mathbb{N}_0}^n \times \underline{k} \times W$ we define a partial order by

$$((\alpha, i), d) \sqsubseteq_\delta ((\beta, j), e) :\Longleftrightarrow \boldsymbol{x}^\alpha \mid \boldsymbol{x}^\beta,\ i = j,\ d \leq e. \tag{13.1}$$

Then the partially ordered set $({\mathbb{N}_0}^n \times \underline{k} \times W, \sqsubseteq_\delta)$ is isomorphic to the direct product of n copies of $(\mathbb{N}_0, \leq)$ with $(\{1, \ldots, k\}, =)$ and $(W, \leq)$ in the sense that $((\alpha, i), d) \sqsubseteq_\delta ((\beta, j), e)$ if and only if $\alpha_r \leq \beta_r$ for all $r \in \underline{n}$, $i = j$ and $d \leq e$. Therefore the ordered set $({\mathbb{N}_0}^n \times \underline{k} \times W, \sqsubseteq_\delta)$ has no infinite descending chains and no infinite antichains (Theorem 13.33(1)).

3. Existence of strong Gröbner bases

THEOREM 13.4. *Let R be a Euclidean domain, let I be a submodule of $R[x_1, \ldots, x_n]^k$, and let $\leq$ be an admissible order of the monomial vectors. Then I has a finite strong Gröbner basis with respect to $\leq$.*

PROOF. Let $\mathrm{Min}(\mathrm{DEG}_\delta(I))$ be the set of minimal elements of $\mathrm{DEG}_\delta(I)$ with respect to the partial ordering $\sqsubseteq_\delta$. Since $\mathrm{Min}(\mathrm{DEG}_\delta(I))$ is an antichain of $({\mathbb{N}_0}^n \times \underline{k} \times W, \sqsubseteq_\delta)$, it is finite (cf. Theorem 13.33(2)). Let G be a finite subset of I such that for every $((\alpha, i), d) \in \mathrm{Min}(\mathrm{DEG}_\delta(I))$, there is a $g \in G$ with $(\mathrm{DEG}(g), \delta(\mathrm{LC}(g))) = ((\alpha, i), d)$.

We claim that G is a strong Gröbner basis. To show this, let $f \in I \setminus \{0\}$. Since $(\mathrm{DEG}(f), \delta(\mathrm{LC}(f))) \in \mathrm{DEG}_\delta(I)$, there is an $((\alpha, i), d) \in \mathrm{Min}(\mathrm{DEG}_\delta(I))$ with $((\alpha, i), d) \sqsubseteq_\delta (\mathrm{DEG}(f), \delta(\mathrm{LC}(f)))$. Hence

$$L := \{g \in G \mid \mathrm{DEG}_\delta(g) \sqsubseteq_\delta \mathrm{DEG}_\delta(f)\}$$

is not empty. Let g_1 be an element of L for which $\delta(\mathrm{LC}(g_1))$ is minimal. Since $\mathrm{DEG}_\delta(g_1) \sqsubseteq_\delta \mathrm{DEG}_\delta(f)$, $\mathrm{LM}(g_1)$ divides $\mathrm{LM}(f)$. By the Euclidean property, there are $q, r \in R$ such that $\mathrm{LC}(f) = q\,\mathrm{LC}(g_1) + r$ with $\delta(r) < \delta(\mathrm{LC}(g_1))$. If $r = 0$, then $\mathrm{LC}(g_1) \mid \mathrm{LC}(f)$ and therefore $\mathrm{LT}(g_1)$ divides $\mathrm{LT}(f)$. Then g_1 is the required element from G. If $r \neq 0$, we let

$$h := f - q\frac{\mathrm{LM}(f)}{\mathrm{LM}(g_1)}g_1.$$

Then $h \in I$ and $\mathrm{LT}(h) = r\,\mathrm{LM}(f)$. Then there is $g_2 \in G$ such that $\mathrm{DEG}_\delta(g_2) \sqsubseteq_\delta \mathrm{DEG}_\delta(h)$. Hence $\mathrm{LM}(g_2) \mid \mathrm{LM}(h)$ and $\delta(\mathrm{LC}(g_2)) \leq \delta(r)$, and thus $\delta(\mathrm{LC}(g_2)) < \delta(\mathrm{LC}(g_1))$. Since $\delta(\mathrm{LC}(g_2)) < \delta(\mathrm{LC}(g_1)) \leq \delta(\mathrm{LC}(f))$, we have $g_2 \in L$. This g_2 contradicts the minimality of $\mathrm{LC}(g_1)$. Therefore the case $r \neq 0$ cannot occur. □

4. A criterion for being a strong Gröbner basis

In this section, we prove a criterion (Theorem 13.10) that guarantees that certain sets are strong Gröbner bases. This criterion is then fundamental for constructing these bases in Section 5. Throughout Sections 4 and 5, R will denote a Euclidean domain with grading function δ. We first need a generalization of Euclidean division, i.e., of expressing b as $qa+r$ with $\delta(r) < \delta(a)$, from R to $R[\boldsymbol{x}]$.

Definition 13.5. Let $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$, and let $f \in R[\boldsymbol{x}]^k$. We say that $\rho = ((a_i, m_i, g_i)_{i\in\underline{N}}, r)$ is an *expression* of f by G with remainder r if $N \in \mathbb{N}_0$ and for each $i \in \underline{N}$, we have that $a_i \in R$, m_i is a monomial, $g_i \in G$, $r \in R[\boldsymbol{x}]^k$ and

$$f = \sum_{i=1}^{N} a_i m_i g_i + r.$$

An expression is *Euclidean* with respect to the admissible monomial vector ordering $\leq$ if for all $i \in \underline{N}$, we have $\operatorname{Lm}(m_i g_i) \leq \operatorname{Lm}(f)$, and ($r = 0$ or there is no $g \in G$ such that $\operatorname{Deg}_\delta(g) \sqsubseteq_\delta \operatorname{Deg}_\delta(r)$).

Let us give some examples of expressions in $R[\boldsymbol{x}]^k = (\mathbb{Z}[x,y])^1$, where we order monomials lexicographically with $x > y$ and use the Euclidean grading function $\delta(z) := |z|$. Let $G = \{2x\,e_1, 3y\,e_1\}$. Then $(((-11, y, 2x\,e_1), (5, x, 3y\,e_1), (4, y, 2x\,e_1)), x\,e_1)$ is an Euclidean expression of $xy\,e_1 + x\,e_1$ by G that corresponds to the equality

$$xy\,e_1 + x\,e_1 = -11y(2x\,e_1) + 5x(3y\,e_1) + 4y(2x\,e_1) + x\,e_1.$$

The expression $x\,e_1 = 1x^0(2x\,e_1) + (-x\,e_1)$ is an Euclidean expression of $x\,e_1$ by G with remainder $(-x\,e_1)$, whereas the expression $x\,e_1 = -3x^0(2x\,e_1) + 7x\,e_1$ is an expression of x by G with remainder $7x\,e_1$ which is not Euclidean because $\delta(7) \not\leq \delta(2)$ and thus $\operatorname{Deg}_\delta(7x\,e_1) = \operatorname{Deg}_\delta(7x^1y^0\,e_1) = (((1,0),1),7) \not\sqsubseteq_\delta (((1,0),1),2) = \operatorname{Deg}_\delta(2x\,e_1)$.

We note that in an expression, $a_i = 0$ is allowed. The name *expression* follows the notation of [**Eis95**, Definition 15.6]. We will construct such expressions using Euclidean division.

Algorithmus 13.6 (Euclidean division).
Input: $f \in R[\boldsymbol{x}]^k \setminus \{0\}$, $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$, an admissible order $\leq$ of ${\mathbb{N}_0}^n \times \underline{k}$.
Ouput: An Euclidean expression $((a_i, m_i, g_i)_{i\in\underline{N}}, r)$ of f by G.

1: $r \leftarrow f$
2: $\rho \leftarrow ()$
3: **while** $r \neq 0$ and $\exists g \in G : \operatorname{Deg}_\delta(g) \sqsubseteq_\delta \operatorname{Deg}_\delta(r)$ **do**
4: Find some $q, s \in R$ with $\operatorname{Lc}(r) = q \operatorname{Lc}(g) + s$ and $\delta(s) < \delta(\operatorname{Lc}(g))$.
5: $r \leftarrow r - q\frac{\operatorname{Lm}(r)}{\operatorname{Lm}(g)} g$
6: Append $(q, \frac{\operatorname{Lm}(r)}{\operatorname{Lm}(g)}, g)$ to ρ
7: Return (ρ, r)

Lemma 13.7. *For each input f, G, Algorithm 13.6 terminates and yields a Euclidean expression of f by G.*

PROOF. We first prove termination. We say that $f \in R[\boldsymbol{x}]^k$ does not guarantee termination if there is an infinite sequence $r_0 = f, r_1, r_2 \dots$ of values of r produced by the algorithm. Suppose that there is $f \in R[\boldsymbol{x}]^k$ that does not guarantee termination. Among those f that do not guarantee termination, we let L be the set of those f for which $\operatorname{LM}(f)$ is minimal with respect to the admissible ordering $\leq$. Since the admissible order $\leq$ is a well order (Lemma 13.32), every nonempty subset of monomial vectors contains a least element with respect to $\leq$ and thus L is nonempty. The codomain of the grading function δ is also well ordered. Hence among the elements of L, we can choose an f to be of minimal $\delta(\operatorname{LC}(f))$. If in the computation $r_1 = f - q\frac{\operatorname{LM}(f)}{\operatorname{LM}(g)}g$, with $s = \operatorname{LC}(f) - q\operatorname{LC}(g)$, we have $s = 0$, then $\operatorname{LM}(r_1) < \operatorname{LM}(f)$. Then r_1 does not guarantee termination, contradicting the minimality of $\operatorname{LM}(f)$. If $s \neq 0$ and $\delta(s) < \delta(\operatorname{LC}(g))$, we have $\operatorname{LT}(r_1) = s\operatorname{LM}(f)$ and therefore $\delta(\operatorname{LC}(r_1)) = \delta(s) < \delta(\operatorname{LC}(g))$. Since $\operatorname{DEG}_\delta(g) \sqsubseteq_\delta \operatorname{DEG}_\delta(f)$, we have $\delta(\operatorname{LC}(g)) \leq \delta(\operatorname{LC}(f))$. Thus $\delta(\operatorname{LC}(r_1)) < \delta(\operatorname{LC}(f))$. Since r_1 does not guarantee termination, we have a contradiction to the minimality of $\delta(\operatorname{LC}(f))$.

For proving correctness, we observe that throughout the algorithm (ρ, r) is an expression of f by G satisfying the degree bound. When the while-loop is left, then r has the required properties. □

Expressions with remainder 0 will also be called *representations*. The importance of representations in which only one summand has maximal degree was observed in [**Lic12**].

DEFINITION 13.8. Let $f \in R[\boldsymbol{x}]^k \setminus \{0\}$ and $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$. Then $\rho = (a_i, m_i, g_i)_{i \in \underline{N}}$ is a *strong standard representation* of f by G with respect to the monomial vector ordering $\leq$ if $(\rho, 0)$ is an expression of f by G with remainder 0, and in addition,

$$N \geq 1,\ \operatorname{LM}(m_1 g_1) = \operatorname{LM}(f),\ \text{and } \operatorname{LM}(m_i g_i) < \operatorname{LM}(f) \text{ for all } i \in \underline{N} \setminus \{1\}.$$

We will now define S-polynomial vectors; this definition is a slight modification of [**KRK88**, Definition CP1]. For $\alpha, \beta \in {\mathbb{N}_0}^n$, we let $\alpha \sqcup \beta := (\max(\alpha_1, \beta_1), \dots, \max(\alpha_n, \beta_n))$. Hence $\boldsymbol{x}^{\alpha \sqcup \beta}$ is the least common multiple of $\boldsymbol{x}^\alpha$ and $\boldsymbol{x}^\beta$ in $R[\boldsymbol{x}]$.

DEFINITION 13.9 (S-polynomial vectors). Let $f, g \in R[\boldsymbol{x}]^k \setminus \{0\}$ with $f \neq g$, and assume that $\operatorname{LT}(f) = a\boldsymbol{x}^\alpha e_i$ and $\operatorname{LT}(g) = b\boldsymbol{x}^\beta e_j$. Let

$$\alpha' := (\alpha \sqcup \beta) - \beta \text{ and } \beta' := (\alpha \sqcup \beta) - \alpha.$$

Then $h \in R[\boldsymbol{x}]^k$ is an *S-polynomial vector* of the pair (f, g) if one of the following two conditions holds:

(1) $i = j$, $\delta(a) \geq \delta(b)$ and there exists $q \in R$ such that $\delta(a - qb) < \delta(a)$ and

$$h = \boldsymbol{x}^{\beta'} f - q\boldsymbol{x}^{\alpha'} g;$$

(2) $i \neq j$ and $h = 0$.

The polynomial vector h is an S-polynomial vector of the set $\{f, g\}$ if h is an S-polynomial vector of (f, g) or of (g, f).

Concerning item (1), we notice that Euclidean division of a by b in R would yield a q that even satisfies $\delta(a-qb) < \delta(b)$, but for our purposes the weaker condition $\delta(a-qb) < \delta(a)$ suffices.

THEOREM 13.10. *Let $\leq$ be an admissible ordering on $\mathrm{Mon}(n,k)$, and let $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$. We assume that for all $f,g \in G$ with $f \neq g$, there is an S-polynomial vector h of $\{f,g\}$ such that $h=0$ or h has a strong standard representation by G. Then G is a strong Gröbner basis with respect to $\leq$ for the submodule I of $R[\boldsymbol{x}]^k$ that is generated by G.*

PROOF. Let $f \in I \setminus \{0\}$. We will show that there is $g \in G$ with $\mathrm{LT}(g) \mid \mathrm{LT}(f)$. Since $f \in I$, there is $\rho = (a_i, m_i, g_i)_{i \in \underline{N}}$ such that $f = \sum_{i \in \underline{N}} a_i m_i g_i$. Such a ρ is called a *representation* of f by G. Here, no restriction on $\mathrm{DEG}(m_i g_i)$ is made. We measure the complexity of a representation $\rho = (a_i, m_i, g_i)_{i \in \underline{N}}$ using the following complexity parameters:

$$C_1(\rho) := \max\{\mathrm{DEG}(m_i g_i) \mid i \in \underline{N}\}$$

is the maximal degree of $m_i g_i$ appearing in ρ, where the maximum is taken with respect to the admissible ordering of on ${\mathbb{N}_0}^n \times \underline{k}$. We let

$$I_1(\rho) = \{i \in \underline{N} \mid \mathrm{DEG}(m_i g_i) = C_1(\rho)\}$$

be the set of those indices for which this maximum is attained. We define

$$C_2(\rho) := \max\{\delta(\mathrm{LC}(g_i)) \mid i \in I_1(\rho)\}$$

as the maximum of the δ-grades of the leading coefficients of those g_i's for which $\mathrm{DEG}(m_i g_i)$ is maximal. The set

$$I_2(\rho) := \{i \in \underline{N} \mid \mathrm{DEG}(m_i g_i) = C_1(\rho) \text{ and } \delta(\mathrm{LC}(g_i)) = C_2(\rho)\}$$

collects those indices from $I_1(\rho)$ for which this maximum of δ-grades is attained. Finally,

$$C_3(\rho) := \#I_2$$

counts the number of elements of I_2. Now we choose a representation $\rho = (a_i, m_i, g_i)_{i \in \underline{N}}$ of f for which the triple $(C_1(\rho), C_2(\rho), C_3(\rho))$ is minimal with respect to the lexicographic ordering on $({\mathbb{N}_0}^n \times \underline{k}) \times W \times \mathbb{N}$, where the order on ${\mathbb{N}_0}^n \times \underline{k}$ is taken to be the admissible ordering $\leq$. This means that ρ minimizes C_1 with respect to the admissible order on ${\mathbb{N}_0}^n \times \underline{k}$, among those that minimize C_1, ρ minimizes C_2, and so on. Since all three sets ${\mathbb{N}_0}^n \times \underline{k}, W, \mathbb{N}$ are well ordered, i.e., totally ordered without infinite descending chains, such a minimizing ρ exists. Since for every permutation of $\underline{N}$, the representation $\rho' = (a_{\pi(i)}, m_{\pi(i)}, g_{\pi(i)})_{i \in \underline{N}}$ of f has the same complexity parameters as ρ, we may assume

$$\mathrm{DEG}(m_1 g_1) \geq \mathrm{DEG}(m_2 g_2) \geq \cdots \geq \mathrm{DEG}(m_N g_N). \tag{13.2}$$

We now consider several cases:

Case 1: $\#I_1(\rho) = 1$: By the assumption (13.2), we then have $I_1(\rho) = \{1\}$. If $a_1 = 0$, we take the representation $\rho' := (a_i, m_i, g_i)_{i \in \underline{N} \setminus \{1\}}$. Then $C_1(\rho') < C_1(\rho)$, contradicting the minimality of ρ. If $a_1 \neq 0$, then $\mathrm{DEG}(a_1 m_1 g_1) = \mathrm{DEG}(f)$ and $\mathrm{LC}(f) = a_1 \,\mathrm{LC}(g_1)$. Therefore $\mathrm{LT}(g_1) \mid \mathrm{LT}(f)$.

Case 2: $\#I_1(\rho) \geq 2$: Let $l := \#I_1(\rho)$. Then $\mathrm{LM}(m_1 g_1) = \cdots = \mathrm{LM}(m_l g_l)$, and we may assume without loss of generality that

$$\delta(\mathrm{LC}(g_1)) \geq \delta(\mathrm{LC}(g_2)) \geq \cdots \geq \delta(\mathrm{LC}(g_l)). \tag{13.3}$$

Case 2.1: $g_1 = g_2$: Since $\mathrm{LM}(m_1 g_1) = \mathrm{LM}(m_2 g_2)$, we then have $m_1 = m_2$. Hence $\rho' := ((a_1 + a_2, m_2, g_2), (a_3, m_3, g_3), \ldots, (a_N, m_N, g_N))$ is a representation of f with $C_1(\rho') = C_1(\rho)$. Since $\delta(\mathrm{LC}(g_1)) = \delta(\mathrm{LC}(g_2))$, we also have $C_2(\rho') = C_2(\rho)$. Now $C_3(\rho') = C_3(\rho) - 1 < C_3(\rho)$. Then ρ' contradicts the minimality of ρ.

Case 2.2: $g_1 \neq g_2$: Let

$$\mathrm{LT}(g_1) = a\boldsymbol{x}^{\alpha} e_i \text{ and } \mathrm{LT}(g_2) = b\boldsymbol{x}^{\beta} e_j.$$

Since $\mathrm{DEG}(m_1 g_1) = \mathrm{DEG}(m_2 g_2)$, we have $i = j$. By the assumptions, the S-polynomial vector h coming from $\{g_1, g_2\}$ is 0 or has a strong standard representation by G. If $\delta(g_1) > \delta(g_2)$, then h is an S-polynomial vector of the pair (g_1, g_2). If $\delta(\mathrm{LC}(g_1)) = \delta(\mathrm{LC}(g_2))$ and h is an S-polynomial vector of the pair (g_2, g_1), we swap the first two entries in the representation ρ and obtain a representation $\tilde{\rho}$ that still satisfies (13.2) and (13.3). This allows us to assume that h is an S-polynomial vector of the pair (g_1, g_2). Let

$$\alpha' := (\alpha \sqcup \beta) - \beta, \ \ \beta' := (\alpha \sqcup \beta) - \alpha,$$

and let γ be such that $\gamma + (\alpha \sqcup \beta) = \mathrm{DEG}(m_1 g_1)$. Let $q \in R$ be such that $\delta(a - qb) < \delta(a)$ and

$$h = \boldsymbol{x}^{\beta'} g_1 - q\boldsymbol{x}^{\alpha'} g_2.$$

Then

$$\boldsymbol{x}^{\gamma} h = m_1 g_1 - q m_2 g_2,$$

and thus

$$m_1 g_1 = \boldsymbol{x}^{\gamma} h + q m_2 g_2. \tag{13.4}$$

Case 2.2.1: $h = 0$: In this case, $m_1 g_1 = q m_2 g_2$, and thus

$$\rho' := ((a_1 q + a_2, m_2, g_2), (a_3, m_3, g_3), \ldots, (a_N, m_N, g_N))$$

is a representation of f that satisfies $C_1(\rho') = C_1(\rho)$.

Case 2.2.1.1: $\delta(\mathrm{LC}(g_1)) > \delta(\mathrm{LC}(g_2))$: Then $C_2(\rho') = \delta(\mathrm{LC}(g_2)) < \delta(\mathrm{LC}(g_1)) = C_1(\rho')$. Thus ρ' contradicts the minimality of ρ.

Case 2.2.1.2: $\delta(\mathrm{LC}(g_1)) = \delta(\mathrm{LC}(g_2))$: Then $C_2(\rho') = \delta(\mathrm{LC}(g_2))$ and $C_3(\rho') = C_3(\rho) - 1$, contradicting the minimality of ρ.

Case 2.2.2: $h \neq 0$: By the assumptions, h has a strong standard representation $(b_i, n_i, h_i)_{i \in \underline{M}}$ with the h_i's in G. Now from (13.4), we obtain

$$a_1 m_1 g_1 = \sum_{i \in \underline{M}} a_1 b_i (\boldsymbol{x}^{\gamma} n_i) h_i + a_1 q m_2 g_2,$$

and therefore

$$a_1 m_1 g_1 + a_2 m_2 g_2 = \sum_{i \in \underline{M}} a_1 b_i (\boldsymbol{x}^{\gamma} n_i) h_i + (a_1 q + a_2) m_2 g_2.$$

We claim that the representation ρ' coming from

$$f = \big(\sum_{i\in\underline{M}} a_1 b_i(\boldsymbol{x}^\gamma n_i)h_i\big) + (a_1 q + a_2)m_2 g_2 + \sum_{i=3}^{N} a_i m_i g_i$$

has lower complexity than ρ. We know that $\mathrm{Deg}(h) \leq \mathrm{Deg}(\boldsymbol{x}^{\beta'} g_1)$ and thus $\mathrm{Deg}(\boldsymbol{x}^\gamma h) \leq \mathrm{Deg}(m_1 g_1)$. We distinguish cases according to whether this inequality is strict.

Case 2.2.2.1: $\mathrm{Deg}(\boldsymbol{x}^\gamma h) < \mathrm{Deg}(m_1 g_1)$: Then for all $i \in \underline{M}$, we have $\mathrm{Deg}(\boldsymbol{x}^\gamma n_i h_i) < \mathrm{Deg}(m_1 g_1)$. Since $\mathrm{Deg}(m_1 g_1) = \mathrm{Deg}(m_2 g_2)$, we therefore have $C_1(\rho') = C_1(\rho)$. If $\delta(\mathrm{Lc}(g_1)) > \delta(\mathrm{Lc}(g_2))$, we have $C_2(\rho') < C_2(\rho)$, and if $\delta(\mathrm{Lc}(g_1)) = \delta(\mathrm{Lc}(g_2))$, we have $C_2(\rho') = C_2(\rho)$ and $C_3(\rho') = C_3(\rho) - 1 < C_3(\rho)$, contradicting the minimality of ρ.

Case 2.2.2.2: $\mathrm{Deg}(\boldsymbol{x}^\gamma h) = \mathrm{Deg}(m_1 g_1)$: Then $\mathrm{Deg}(\boldsymbol{x}^\gamma n_1 h_1) = \mathrm{Deg}(m_1 g_1)$ and $\mathrm{Deg}(\boldsymbol{x}^\gamma n_i h_i) < \mathrm{Deg}(m_1 g_1)$ for $i \in \{2, \ldots, M\}$. Hence $C_1(\rho') = C_1(\rho)$. Since $\mathrm{Lt}(b_1 n_1 h_1) = \mathrm{Lt}(h)$, we have $\delta(\mathrm{Lc}(h_1)) \leq \delta(b_1 \,\mathrm{Lc}(h_1)) = \delta(\mathrm{Lc}(h))$. From the definition of S-polynomial vectors, we have $\delta(\mathrm{Lc}(h)) < \delta(\mathrm{Lc}(g_1))$, and thus $\delta(\mathrm{Lc}(h_1)) < \delta(\mathrm{Lc}(g_1))$. If $\delta(\mathrm{Lc}(g_1)) > \delta(\mathrm{Lc}(g_2))$, we have $C_2(\rho') < C_2(\rho)$, and if $\delta(\mathrm{Lc}(g_1)) = \delta(\mathrm{Lc}(g_2))$, we have $C_2(\rho') = C_2(\rho)$ and $C_3(\rho') = C_3(\rho) - 1 < C_3(\rho)$, contradicting the minimality of ρ.

Hence in Case 2, we always obtain ρ' with complexity lower than ρ, showing that the case $\#I_1(\rho) \geq 2$ cannot occur. □

5. Construction of strong Gröbner bases

In this section, we assume that a submodule I of $R[\boldsymbol{x}]^k$ is given by a finite set F of generators. (By Hilbert's Basis Theorem, or simply by Theorem 13.4, such a finite F exists.) Our goal is to construct a finite strong Gröbner basis G for $I = \langle F\rangle$. We will proceed by adding polynomials to F in order to obtain a set G such that each 2-element subset of G has an S-polynomial vector with a strong standard representation; then Theorem 13.10 guarantees that we have found a strong Gröbner basis. We start by setting $G := F$. Algorithm 13.11 performs one step of the augmentation of F towards a strong Gröbner basis. In this step, we consider one 2-element subset $\{p, q\}$ of G. The augmentation of G using the set $\{p, q\}$ yields a set H. This set H can be equal to G, or it is equal to $G \cup \{f\}$ for some polynomial vector $f \in \langle F\rangle$, where f is computed from an S-polynomial vector of $\{p, q\}$. Compared to G, the set H has the advantage that in H, either $\{p, q\}$ has an S-polynomial vector that has a strong standard representation, or $\{p, q\}$ still has no strong standard representation by H, but H is, in some sense, *larger* than G, which also brings us closer to termination. The function Augment also returns a Boolean value $x \in \{0, 1\}$, where $x = 0$ indicates that the pair $\{p, q\}$ needs to be reconsidered in a future augmentation step.

To express this idea of the set becoming larger by augmentation, we let W be the codomain of the Euclidean grading function δ. We consider subsets T of $\mathbb{N}_0{}^n \times \underline{k} \times W$ and we say that such a subset T is *upward closed* if for all $s \in T$ and $t \in \mathbb{N}_0{}^n \times \underline{k} \times W$ with $s \sqsubseteq_\delta t$, we have $t \in T$. Since $(\mathbb{N}_0{}^n \times \underline{k} \times W, \sqsubseteq_\delta)$ has no infinite descending chains and no infinite antichains, there is no infinite ascending chain of upward closed subsets of $\mathbb{N}_0{}^n \times \underline{k} \times W$ with respect to $\subseteq$

(cf. Theorem 13.33(3)). For $G \subseteq R[\boldsymbol{x}]^k$, we will consider the upward closed set

$$\textsc{Deg}_\delta(G)\uparrow := \{((\gamma, i), d) \in {\mathbb{N}_0}^n \times \underline{k} \times W \mid \exists g \in G : \textsc{Deg}_\delta(g) \sqsubseteq_\delta ((\gamma, i), d)\}.$$

Algorithmus 13.11 (Augmentation).
Input: A finite subset G of $R[\boldsymbol{x}]^k \setminus \{0\}$, a two element subset $\{p, q\}$ of G, and an admissible order $\leq$ of ${\mathbb{N}_0}^n \times \underline{k}$.
Output: A pair (H, x), where H is a finite set with $G \subseteq H \subseteq \langle G \rangle$ and $x \in \{0, 1\}$ such that the following hold:

(1) If $x = 1$, then $\{p, q\}$ has an S-polynomial vector f such that $f = 0$ or f has a strong standard representation by H.
(2) If $G \neq H$, then $\textsc{Deg}_\delta(G)\uparrow \subset \textsc{Deg}_\delta(H)\uparrow$.
(3) If $G = H$, then $x = 1$.

```
1: function Augment(G, {p, q})
2:     f ← some S-polynomial vector of {p, q}
3:     x ← 0
4:     if f = 0 then
5:         x ← 1
6:     else if ∃g ∈ G : Lt(g) | Lt(f) then
7:         x ← 1
8:         f′ ← f − (Lt(f)/Lt(g)) g
9:         Find a Euclidean expression f′ = Σ_{i=1}^{M} a_i m_i g_i + r by G.
10:        if r ≠ 0 then
11:            G ← G ∪ {r}
12:    else if ∃g ∈ G : Deg_δ(g) ⊑_δ Deg_δ(f) then
13:        Among those g ∈ G with Deg_δ(g) ⊑_δ Deg_δ(f), pick g with minimal δ(Lc(g)).
14:        Find q ∈ R such that δ(Lc(f) − q Lc(g)) < δ(Lc(g)).
15:        f′ ← f − q (Lm(f)/Lm(g)) g
16:        G ← G ∪ {f′}
17:    else
18:        G ← G ∪ {f}
19:    Return (G, x)
```

Lemma 13.12. *Algorithm 13.11 is correct.*

Proof. For proving the first output condition, we assume that $x = 1$. We show that then f is an S-polynomial vector of $\{p, q\}$ with the required conditions. If $f = 0$, this is clearly the case. If $\exists g \in G : \textsc{Lt}(g) \mid \textsc{Lt}(f)$, then in the case $r = 0$, $((\frac{\textsc{Lc}(f)}{\textsc{Lc}(g)}, \frac{\textsc{Lm}(f)}{\textsc{Lm}(g)}, g), (a_1, m_1, g_1), \ldots, (a_M m_M g_M))$ is a strong standard representation of f by G and in the case $r \neq 0$, we note that $\textsc{Lm}(r) \leq \textsc{Lm}(f') < \textsc{Lm}(f)$ and thus $((\frac{\textsc{Lc}(f)}{\textsc{Lc}(g)}, \frac{\textsc{Lm}(f)}{\textsc{Lm}(g)}, g), (a_1, m_1, g_1), \ldots, (a_M m_M g_M), (1, \boldsymbol{x}^0, r))$ is a strong standard representation.

For proving the second output condition, we assume $G \neq H$. If there exists $g \in G$ with $\textsc{Lt}(g) \mid \textsc{Lt}(f)$ and $r \neq 0$, then since r is the remainder of a Euclidean division, $\textsc{Deg}_\delta(r) \notin \textsc{Deg}_\delta(G)\uparrow$, and thus $\textsc{Deg}_\delta(G)\uparrow \subset \textsc{Deg}_\delta(G \cup \{r\})\uparrow = \textsc{Deg}_\delta(H)\uparrow$.

If there is no $g \in G$ with $\operatorname{LT}(g) \mid \operatorname{LT}(f)$, but there is a $g \in G$ such that $\operatorname{DEG}_\delta(g) \sqsubseteq_\delta \operatorname{DEG}_\delta(f)$, then we show that $\operatorname{DEG}_\delta(f') \notin \operatorname{DEG}_\delta(G)\uparrow$. Suppose that there is $g_1 \in G$ with $\operatorname{DEG}_\delta(g_1) \sqsubseteq_\delta \operatorname{DEG}_\delta(f')$. Then $\delta(\operatorname{LC}(g_1)) \leq \delta(\operatorname{LC}(f'))$ and $\operatorname{LM}(g_1) \mid \operatorname{LM}(f')$. Since $\operatorname{LT}(g) \nmid \operatorname{LT}(f)$, we have $\operatorname{LM}(f') = \operatorname{LM}(f)$, and thus $\operatorname{LM}(g_1) \mid \operatorname{LM}(f)$. Furthermore $\operatorname{LC}(f') = \operatorname{LC}(f) - q \operatorname{LC}(g)$ and thus $\delta(\operatorname{LC}(f')) < \delta(\operatorname{LC}(g))$, and from $\operatorname{DEG}_\delta(g) \sqsubseteq_\delta \operatorname{DEG}_\delta(f)$ we obtain $\delta(\operatorname{LC}(g)) \leq \delta(\operatorname{LC}(f))$. Altogether $\delta(\operatorname{LC}(g_1)) \leq \delta(\operatorname{LC}(f')) < \delta(\operatorname{LC}(g)) \leq \delta(\operatorname{LC}(f))$. From this, we obtain $\operatorname{DEG}_\delta(g_1) \sqsubseteq_\delta \operatorname{DEG}_\delta(f)$ and $\delta(\operatorname{LC}(g_1)) < \delta(\operatorname{LC}(g))$, contradicting the minimality of $\delta(\operatorname{LC}(g))$. Thus $\operatorname{DEG}_\delta(f') \notin \operatorname{DEG}_\delta(G)\uparrow$, and therefore $\operatorname{DEG}_\delta(G)\uparrow \subset \operatorname{DEG}_\delta(G \cup \{f'\})\uparrow = \operatorname{DEG}_\delta(H)\uparrow$.

Finally, if $f \neq 0$ and $\exists g \in G : \operatorname{DEG}_\delta(g) \sqsubseteq_\delta \operatorname{DEG}_\delta(f)$ is false, then $\operatorname{DEG}_\delta(f) \notin \operatorname{DEG}_\delta(g)\uparrow$, and thus $\operatorname{DEG}_\delta(G)\uparrow \subset \operatorname{DEG}_\delta(G \cup \{f\})\uparrow = \operatorname{DEG}_\delta(H)\uparrow$.

For proving the third output condition, we assume $G = H$. This happens only if $f = 0$ or if ($f \neq 0$, $\exists g \in G : \operatorname{LT}(g) \mid \operatorname{LT}(f)$ and $r = 0$) because in all other cases, a polynomial vector gets added to G. In both of these cases, x is set to 1. □

Replacing lines 14 and 15 of the algorithm by the following lines may reduce the number of computation steps and still yields a correct algorithm.

14': Compute $d := \gcd(\operatorname{LC}(f), \operatorname{LC}(g)) = a \operatorname{LC}(f) + b \operatorname{LC}(g)$.
15': $f' \leftarrow af + b\frac{\operatorname{LM}(f)}{\operatorname{LM}(g)}g$

ALGORITHMUS 13.13 (Strong Gröbner Basis).
Input: $F \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$, an admissible order $\leq$ of $\mathbb{N}_0{}^n \times \underline{k}$.
Output: $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$ such that G is a strong Gröbner basis of $\langle F \rangle$ with respect to the monomial vector ordering $\leq$.

1: $G \leftarrow F$.
2: $P \leftarrow \varnothing$.
3: **while** $\exists p, q \in G : p \neq q$ and $\{p, q\} \notin P$ **do**
4: $\quad (G, x) \leftarrow \text{AUGMENT}(G, \{p, q\})$
5: $\quad$ **if** $x = 1$ **then**
6: $\quad\quad P \leftarrow P \cup \{\{p, q\}\}$
7: Return G

THEOREM 13.14. *Algorithm 13.13 terminates on every input and produces a correct result.*

PROOF. We first observe that throughout the algorithm, G generates the same submodule as F. Furthermore, each $\{p, q\} \in P$ has an S-polynomial vector f that is 0 or has a strong standard representation: The set $\{p, q\}$ can only be added to P when $x = 1$ and in this case the output condition (1) of AUGMENT guarantees that $\{p, q\}$ has f as required. Hence if the algorithm terminates, all two-element subsets of G have a strong standard representation. Thus by Theorem 13.10, G is then a strong Gröbner basis.

In order to show termination, we let W be the codomain of the Euclidean grading function δ, and we consider the upward closed subset

$$\operatorname{DEG}_\delta(G)\uparrow := \{((\gamma, i), d) \in \mathbb{N}_0{}^n \times \underline{k} \times W \mid \exists g \in G : \operatorname{DEG}_\delta(g) \sqsubseteq_\delta ((\gamma, i), d)\}$$

of $(\mathbb{N}_0{}^n \times \underline{k} \times W, \sqsubseteq_\delta)$. Our claim is that in each execution of the while loop, if G_1 and P_1 are the values of G and P when entering the loop and G_2 and P_2 are the values before the next iteration of the loop, we have $\mathrm{DEG}_\delta(G_1)\uparrow \subset \mathrm{DEG}_\delta(G_2)\uparrow$ or $(\mathrm{DEG}_\delta(G_1)\uparrow = \mathrm{DEG}_\delta(G_2)\uparrow$ and $\#(\binom{G_2}{2} \setminus P_2) < \#(\binom{G_1}{2} \setminus P_1))$. If $G_1 \neq G_2$, then output condition (2) of AUGMENT yields $\mathrm{DEG}_\delta(G)\uparrow \subset \mathrm{DEG}_\delta(H)\uparrow$. If $G_1 = G_2$, then by output condition (3) of AUGMENT, we have $x = 1$ and thus $P_2 = P_1 \cup \{p, q\}$ and therefore $\#(\binom{G_2}{2} \setminus P_2) < \#(\binom{G_1}{2} \setminus P_1)$.

Now suppose that there is an execution of this algorithm that does not terminate. Then we know that from some point onwards, $\mathrm{DEG}_\delta(G)\uparrow$ stays constant, and from this point on, $\#(\binom{G}{2} \setminus P)$ strictly descends forever, which is impossible. □

[**Lic12**, Theorem 11] contains a criterion[1] that generalizes [**Buc70**, p.377, S.2.], which tells that certain S-polynomial vectors need not be considered. We provide a generalization, which, when dealing with polynomial vectors, needs the rather restrictive assumption that both polynomial vectors f, g have entries only in the same component. When speaking of polynomials instead of polynomial vectors, we write the leading term of $p \neq 0$ as $\mathrm{lt}(p)$, the leading monomial as $\mathrm{lm}(p)$, and the degree of p, which is an element in $\mathbb{N}_0^n$, as $\deg(p)$.

THEOREM 13.15. *Let $\tilde{f}, \tilde{g} \in R[\boldsymbol{x}], \alpha, \beta \in \mathbb{N}_0{}^n$, $i \in \underline{k}$, and $a, u \in R$ such that u is a unit in R, $\mathrm{lt}(\tilde{f}) = a\boldsymbol{x}^\alpha$ and $\mathrm{lt}(\tilde{g}) = u\boldsymbol{x}^\beta$. Let $f := \tilde{f}\, e_i$ and $g := \tilde{g}\, e_i$. If $\boldsymbol{x}^\alpha$ and $\boldsymbol{x}^\beta$ are coprime monomials (which means that for all $j \in \underline{n}$ we have $\alpha_j = 0$ or $\beta_j = 0$), then $\{f, g\}$ has an S-polynomial vector that is 0 or has a strong standard representation by $\{f, g\}$.*

PROOF. Let $\tilde{f}_1 := \tilde{f} - \mathrm{lt}(\tilde{f})$ and $\tilde{g}_1 := \tilde{g} - \mathrm{lt}(\tilde{g})$. Then $h = \boldsymbol{x}^\beta f - au^{-1}\boldsymbol{x}^\alpha g$ is an S-polynomial vector of $\{f, g\}$. Suppose $h \neq 0$. We have

$$h = \boldsymbol{x}^\beta f - au^{-1}\boldsymbol{x}^\alpha g = (\boldsymbol{x}^\beta \tilde{f} - au^{-1}\boldsymbol{x}^\alpha \tilde{g})\, e_i = u^{-1}(u\boldsymbol{x}^\beta \tilde{f} - a\boldsymbol{x}^\alpha \tilde{g})\, e_i$$
$$= u^{-1}\big((\tilde{g} - \tilde{g}_1)\tilde{f} - (\tilde{f} - \tilde{f}_1)\tilde{g}\big)e_i = -u^{-1}\tilde{g}_1 f + u^{-1}\tilde{f}_1 g. \tag{13.5}$$

Writing $\tilde{g}_1$ and $\tilde{f}_1$ as sums of terms, we obtain a representation of h. We will show now that it is a strong standard representation. If $f_1 = 0$ or $g_1 = 0$, then this representation has only one summand of degree $\mathrm{DEG}(h)$ and is therefore a strong standard representation. Hence let us assume $f_1 \neq 0$ and $g_1 \neq 0$. We observe that $\mathrm{DEG}(\mathrm{lm}(g_1)f) \neq \mathrm{DEG}(\mathrm{lm}(f_1)g)$: Seeking a contradiction, we assume $\mathrm{DEG}(\mathrm{lm}(g_1)f) = \mathrm{DEG}(\mathrm{lm}(f_1)g)$. Then $\mathrm{lm}(g_1)\,\mathrm{lm}(\tilde{f}) = \mathrm{lm}(f_1)\,\mathrm{lm}(\tilde{g})$, which means $\mathrm{lm}(g_1)\boldsymbol{x}^\alpha = \mathrm{lm}(f_1)\boldsymbol{x}^\beta$. We therefore have $\boldsymbol{x}^\alpha \mid \mathrm{lm}(f_1)\boldsymbol{x}^\beta$. By the assumptions on α and β, we then have $\boldsymbol{x}^\alpha \mid \mathrm{lm}(f_1)$, contradicting $\deg(f_1) < \alpha$.

Therefore, exactly one of $-u^{-1}\tilde{g}_1 f$ and $u^{-1}\tilde{f}_1 g$ has degree $\mathrm{DEG}(-u^{-1}\tilde{g}_1 f + u^{-1}\tilde{f}_1 g)$, which is equal to $\mathrm{DEG}(h)$. Thus by writing $\tilde{g}_1$ and $\tilde{g}_1$ as sums of terms, (13.5) produces a strong standard representation of h with respect to $\{f, g\}$. □

[1] In the statement of [**Lic12**, Theorem 11], the assumption $c_1 \in \{-1, +1\}$ is missing. Without adding this assumption, for $p_1 := 2x+1$ and $p_2 := 4y+1$, we obtain $\mathrm{SPoly}_2(p_1, p_2) = 2yp_1 - xp_2 = 2y - x$, which has no strong standard representation since $2y$ and x are not divisible by any of $2x$ and $4y$. – In the proof given in [**Lic12**, Theorem 11], the S-polynomial of p_1, q_1 is computed (incorrectly) as $\mathrm{SPoly}_2(p_1, p_2) = 4yp_1 - 2xp_2 = 4y - 2x$.

6. Existence and uniqueness of reduced strong Gröbner bases

The construction given in Section 5 has the shortcoming that during the process, polynomial vectors can never be removed from a basis. Also, once we have found a strong Gröbner basis G of I, then we see from Definition 13.3 that every G' with $G \subseteq G' \subseteq I \setminus \{0\}$ is also a strong Gröbner basis. Hence a strong Gröbner basis of I need not be unique. However, we obtain uniqueness if we require that the Gröbner basis is *reduced*. In this section, we prove the existence and uniqueness of such a reduced Gröbner basis; Section 7 is then devoted to its algorithmic construction.

When R is the Euclidean domain $\mathbb{Z}$ with grading function $\delta(z) := |z|$, then 6 may be expressed by 4 either as $6 = 1\cdot 4+2$ or $6 = 2\cdot 4+(-2)$. In order to be able to prefer one of these expressions, one introduces some order on the ring R (cf., e.g., [**Buc84**, p.6] and [**Pan89**, p.62]). We will use orderings that come from refining the grading function δ. When R is a Euclidean domain with grading function $\delta : R \to W$, we assume that we additionally have an injective function $\hat{\delta}$ from R into a well ordered set W' with the property $\hat{\delta}(0) \leq \hat{\delta}(a)$ for all $a \in R$ and

$$\text{for all } a, b \in R : \delta(a) < \delta(b) \Rightarrow \hat{\delta}(a) < \hat{\delta}(b). \tag{13.6}$$

Throughout Sections 6 and 7, we assume that R is a Euclidean domain with the functions δ and $\hat{\delta}$ as above. From a computational point of view, it may be difficult to define such a function $\hat{\delta}$, or, equivalently, to provide a well ordering $\leq_R$ on R satisfying $\delta(a) < \delta(b) \Rightarrow a <_R b$. In the beginning of Section 7, we will address this computational issue. We point out that the given conditions on $\hat{\delta}$, in particular (13.6), have been selected in a way that will allow us to prove that each submodule has a unique reduced strong Gröbner basis.

We will need the following simple fact about Euclidean domains.

LEMMA 13.16. *Let $a, x \in R \setminus \{0\}$ be such that $\delta(ax) \leq \delta(a)$. Then x is a unit of R.*

PROOF. There are $q, r \in R$ with $a = qax + r$ and $\delta(r) < \delta(ax)$. Then $\delta(r) < \delta(a)$. If $r = 0$, then $a = qax$ and thus $qx = 1$ and x is a unit. If $r \neq 0$, then since $r = a(1 - qx)$, we have $\delta(a) \leq \delta(a(1 - qx)) = \delta(r)$, a contradiction. □

DEFINITION 13.17 (Reducibility). We say that $b \in R$ is *reducible* by $A \subseteq R$ if there are $a \in A$ and $q \in R$ such that $\hat{\delta}(b - qa) < \hat{\delta}(b)$. Now let $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$. We say that a term vector $b\boldsymbol{x}^\alpha e_i$ is *reducible* by G if b is reducible by $\{\mathrm{Lc}(g) : \mathrm{Lm}(g) \mid \boldsymbol{x}^\alpha e_i\}$, and that $f \in R[\boldsymbol{x}]^k \setminus \{0\}$ is *reducible* by G if it contains a term vector that is reducible by G.

A polynomial vector p is *normalized* if $p \neq 0$ and $\hat{\delta}(\mathrm{Lc}(p)) \leq \hat{\delta}(u\,\mathrm{Lc}(p))$ for all units u of R. The subset G of $R[\boldsymbol{x}]^k$ is normalized if every $g \in G$ is normalized.

DEFINITION 13.18. Let G be a strong Gröbner basis of the submodule I of $R[\boldsymbol{x}]^k$. Then G is a *reduced strong Gröbner basis* of I if for each $g \in G$, g is normalized and g is not reducible by $G \setminus \{g\}$.

From an admissible ordering of the monomial vectors and the function $\hat{\delta}$, one can define a total order $\leq_P$ on $R[\boldsymbol{x}]^k$. To this end, we order polynomial vectors p, q as follows: for $p \neq q$, let

$\boldsymbol{x}^\gamma e_i := \mathrm{LM}(p-q)$, let a be the coefficient of $\boldsymbol{x}^\gamma e_i$ in p, and let b be the coefficient of $\boldsymbol{x}^\gamma e_i$ in q. Then we say $p <_P q$ if $\hat{\delta}(a) < \hat{\delta}(b)$ and $p \leq_P q$ if $p = q$ or $p <_P q$. The order $\leq_P$ is a well order on $R[\boldsymbol{x}]^k$ (Lemma 13.34).

THEOREM 13.19. *Let I be a submodule of $R[\boldsymbol{x}]^k$, and let $\mathrm{Min}(\mathrm{DEG}_\delta(I))$ be the set of minimal elements of $\mathrm{DEG}_\delta(I)$ with respect to the ordering $\sqsubseteq_\delta$. For every $((\alpha,i),d) \in \mathrm{Min}(\mathrm{DEG}_\delta(I))$, we choose $g_{\alpha,i,d}$ to be the minimal element in I with respect to $\leq_P$ such that $\mathrm{DEG}_\delta(g_{\alpha,i,d}) = ((\alpha,i),d)$. Then*

$$G := \{g_{\alpha,i,d} \mid ((\alpha,i),d) \in \mathrm{Min}(\mathrm{DEG}_\delta(I))\}$$

is finite, and G is the unique reduced strong Gröbner basis of I.

PROOF. As an antichain in the ordered set $(\mathbb{N}_0,\leq)^n \times (\{1,\dots,k\},=) \times (W,\leq)$, the set $\mathrm{Min}(\mathrm{DEG}_\delta(I))$ is finite (Theorem 13.33(2)), and hence G is finite. As in the proof of Theorem 13.4, we see that G is a strong Gröbner basis.

Now we show that G is reduced. Let $g \in G$. We first show that g is normalized. Supposing that g is not normalized, there is a unit $u \in R$ with $\hat{\delta}(u\,\mathrm{LC}(g)) < \hat{\delta}(\mathrm{LC}(g))$. Since u is a unit, $\delta(u\,\mathrm{LC}(g)) = \delta(\mathrm{LC}(g))$. Thus $\mathrm{DEG}_\delta(ug) = \mathrm{DEG}_\delta(g)$, but $ug <_P g$. This contradicts the choice of g. Hence g is normalized.

Next, we show that g is not reducible by $G \setminus \{g\}$. Seeking a contradiction, we suppose that g is reducible by $G \setminus \{g\}$. Then there are a term vector $a\boldsymbol{x}^\alpha e_i$ in G, $h \in G \setminus \{g\}$ and $q \in R$ such that $\mathrm{LM}(h) \mid \boldsymbol{x}^\alpha e_i$ and $\hat{\delta}(a - q\,\mathrm{LC}(h)) < \hat{\delta}(a)$.

Case 1: $a\boldsymbol{x}^\alpha e_i = \mathrm{LT}(g)$: Let b be a greatest common divisor of $\mathrm{LC}(h)$ and $\mathrm{LC}(g)$ in R. Since R is Euclidean, there exist $u, v \in R$ with $u\,\mathrm{LC}(h) + v\,\mathrm{LC}(g) = b$. Thus $\mathrm{LT}(u\frac{\mathrm{LM}(g)}{\mathrm{LM}(h)}h + vg) = b\boldsymbol{x}^\alpha e_i$. Since G is a strong Gröbner basis of I, there is $h_1 \in G$ with

$$\mathrm{LT}(h_1) \mid b\boldsymbol{x}^\alpha e_i. \tag{13.7}$$

Since $b\boldsymbol{x}^\alpha e_i \mid \mathrm{LT}(g)$, we obtain

$$\mathrm{LT}(h_1) \mid \mathrm{LT}(g).$$

Thus $\mathrm{DEG}_\delta(h_1) \sqsubseteq_\delta \mathrm{DEG}_\delta(g)$. Since $\mathrm{DEG}_\delta(g) \in \mathrm{Min}(\mathrm{DEG}_\delta(G))$, we then have $\mathrm{DEG}_\delta(h_1) = \mathrm{DEG}_\delta(g)$. Since G contains only one element f with $\mathrm{DEG}_\delta(f) = ((\alpha,i),\delta(a))$, we have $h_1 = g$. Now by (13.7), we have $\mathrm{LC}(h_1) \mid b$. From the definition of b as a gcd, we have $b \mid \mathrm{LC}(h)$, and thus $\mathrm{LC}(h_1) \mid \mathrm{LC}(h)$ and therefore $\mathrm{LC}(g) \mid \mathrm{LC}(h)$. Hence there is a $q_1 \in R$ such that $\mathrm{LC}(h) = q_1 a$. Therefore,

$$\hat{\delta}(a - qq_1 a) < \hat{\delta}(a). \tag{13.8}$$

By (13.6), we then have $\delta(a - qq_1 a) \leq \delta(a)$, and thus by Lemma 13.16, either $1 - qq_1 = 0$ or $1 - qq_1$ is a unit in R.

Case 1.1: $1 - qq_1 = 0$: Then q_1 is a unit in R and therefore $\mathrm{LC}(h) \mid \mathrm{LC}(g)$. Since $\mathrm{LM}(h) \mid \mathrm{LM}(g)$, we obtain $\mathrm{LT}(h) \mid \mathrm{LT}(g)$ and therefore $\mathrm{DEG}_\delta(h) \sqsubseteq_\delta \mathrm{DEG}_\delta(g)$. From the minimality of $\mathrm{DEG}_\delta(g)$, we obtain $\mathrm{DEG}_\delta(g) = \mathrm{DEG}_\delta(h)$. Since G contains only one element f with $\mathrm{DEG}_\delta(f) = \mathrm{DEG}_\delta(g)$, we have $h = g$, contradicting $h \in G \setminus \{g\}$.

Case 1.2: $1 - qq_1$ is a unit in R: Since g is normalized, we then have $\hat{\delta}(a(1-qq_1)) \geq \hat{\delta}(a)$, contradicting (13.8).

Case 2: $a\boldsymbol{x}^\alpha e_i \neq \mathrm{Lt}(g)$: Then $\mathrm{Deg}(a\boldsymbol{x}^\alpha e_i) < \mathrm{Deg}(g)$. Since $\hat{\delta}(a - q\,\mathrm{Lc}(h)) < \hat{\delta}(a)$, we obtain $g - q\frac{\boldsymbol{x}^\alpha}{\mathrm{Lm}(h)}h <_P g$ and $\mathrm{Lt}(g - q\frac{\boldsymbol{x}^\alpha}{\mathrm{Lm}(h)}h) = \mathrm{Lt}(g)$, and therefore $\mathrm{Deg}_\delta(g - q\frac{\boldsymbol{x}^\alpha}{\mathrm{Lm}(h)}) = \mathrm{Deg}_\delta(g)$. This contradicts the minimality of g with respect to $\leq_P$.

This completes the proof that g is not reducible by $G \setminus \{g\}$.

Therefore G is a reduced strong Gröbner basis. The uniqueness follows from the following lemma. □

Lemma 13.20. *Let I be a submodule of $R[\boldsymbol{x}]^k$, and let G, H be reduced strong Gröbner bases of I. Then $G = H$.*

Proof. By symmetry, it is sufficient to prove $G \subseteq H$. Let $g \in G$. Since $g \in I$, there is $h \in H$ such that $\mathrm{Lt}(h) \mid \mathrm{Lt}(g)$, and since $h \in I$, there is $g_1 \in G$ with $\mathrm{Lt}(g_1) \mid \mathrm{Lt}(h)$. If $g_1 \neq g$, then $\mathrm{Lc}(g)$ is reducible by $\mathrm{Lc}(g_1)$, contradicting the fact that G is reduced. Thus $g_1 = g$, and therefore $\mathrm{Lt}(g) \mid \mathrm{Lt}(h) \mid \mathrm{Lt}(g)$ and thus $\mathrm{Lc}(g)$ and $\mathrm{Lc}(h)$ are associated in R. Since both G and H are normalized, we obtain $\mathrm{Lc}(g) = \mathrm{Lc}(h)$, and thus $\mathrm{Lt}(g) = \mathrm{Lt}(h)$.

We will now show $g = h$. Seeking a contradiction, we suppose $g \neq h$. Since $\mathrm{Lt}(g) = \mathrm{Lt}(h)$, we have $\mathrm{Deg}(g-h) < \mathrm{Deg}(g) = \mathrm{Deg}(h)$. Let $a\boldsymbol{x}^\alpha e_i := \mathrm{Lt}(g-h)$, let b be the coefficient of $\boldsymbol{x}^\alpha e_i$ in g, and let c be the coefficient of $\boldsymbol{x}^\alpha e_i$ in h. Then $a = b - c$. Since $g - h \in I$, there is $g_1 \in G$ with $\mathrm{Lt}(g_1) \mid \mathrm{Lt}(g-h)$. We already know that $\mathrm{Lt}(g) = \mathrm{Lt}(h)$, and thus $\mathrm{Deg}(g-h) < \mathrm{Deg}(g)$. Therefore $g_1 \neq g$. From $\mathrm{Lc}(g_1) \mid b - c$, we obtain $q \in R$ such that $q\,\mathrm{Lc}(g_1) = b - c$ and therefore $c = b - q\,\mathrm{Lc}(g_1)$. Since b is not reducible by $\{\mathrm{Lc}(g_1)\}$, we have $\hat{\delta}(b) \leq \hat{\delta}(c)$. Similarly, since $g - h \in I$, there is $h_1 \in H$ with $\mathrm{Lt}(h_1) \mid \mathrm{Lt}(g-h)$. Since $\mathrm{Lt}(g) = \mathrm{Lt}(h)$, we have $\mathrm{Deg}(g-h) < \mathrm{Deg}(h)$, and thus $h_1 \neq h$. From $\mathrm{Lc}(h_1) \mid \mathrm{Lt}(g-h)$, we obtain $q \in R$ with $q\,\mathrm{Lc}(h_1) = b - c$, and thus $b = c + q\,\mathrm{Lc}(h_1)$. Since c is not reducible by $\{\mathrm{Lc}(h_1)\}$, we have $\hat{\delta}(b) \geq \hat{\delta}(c)$. Altogether, we have $\hat{\delta}(b) = \hat{\delta}(c)$ and thus $b = c$, leading to the contradiction $a = 0$. Thus $g = h$ and therefore $g \in H$. □

7. Construction of reduced strong Gröbner bases

We let R be a Euclidean domain with grading function δ and an additional function $\hat{\delta}$ as in Section 6. For reducing coefficients, we will suppose that with respect to $\hat{\delta}$, we can perform the following two algorithmic tasks:

(1) For $a \in R$, we can find a unit u in R such that $\hat{\delta}(ua)$ is minimal in $\{\hat{\delta}(u'a) \mid u' \text{ is a unit of } R\}$.
(2) For $a, b \in R$, find $q \in R$ such that $\hat{\delta}(b - qa)$ is minimal in $\{\hat{\delta}(b - q'a) \mid q' \in R\}$.

For many Euclidean domains, e.g. for the fields $\mathbb{R}$ or $\mathbb{Q}$, it is difficult to describe such a function $\hat{\delta}$. However, on a field k, it suffices to assume that $\hat{\delta}$ satisfies $\hat{\delta}(0) < \hat{\delta}(1) < \hat{\delta}(x)$ for all $x \in k \setminus \{0,1\}$. Then for $a \in k \setminus \{0\}$, $u := a^{-1}$ minimizes $\hat{\delta}(ua)$ and $q := ba^{-1}$ minimizes $\hat{\delta}(b - qa)$. For $\mathbb{Z}$, we may take $\hat{\delta}(z) := 3|z| - \mathrm{sgn}(z)$, which yields $\hat{\delta}(0) < \hat{\delta}(1) < \hat{\delta}(-1) < \hat{\delta}(2) < \hat{\delta}(-2) < \cdots$.

Then for $a \in \mathbb{Z} \setminus \{0\}$, $u := \operatorname{sgn}(a)$ minimizes $\hat{\delta}(ua)$ and the unique $q \in \mathbb{Z}$ with $-\frac{a}{2} < b - qa \leq \frac{a}{2}$ minimizes $\hat{\delta}(b - qa)$. We note that instead of (2), it would be sufficient to ask for

(2') For $a, b \in R$, find $q \in R$ such that $\hat{\delta}(b - qa) < \hat{\delta}(b)$ if such a q exists, and $q = 0$ if $\hat{\delta}(b)$ is minimal in $\{\hat{\delta}(b - qa) \mid q \in R\}$.

In other words, (2') asks to determine whether b is reducible by $\{a\}$, and, if so, provide a witness $q \in R$ with $\hat{\delta}(b - qa) < \hat{\delta}(b)$. Actually, only (2′) is needed in Algorithm 13.22. But it is clear that iterating a procedure accomplishing (2′), we obtain a procedure accomplishing (2).

For reducing polynomial vectors, we follow [**Lic12**] and use reductions that, when they affect the leading term of a polynomial, eliminate this leading term in one step. We call such reductions *soft*.

Definition 13.21. The polynomial vector $f \in R[\boldsymbol{x}]^k \setminus \{0\}$ is *softly reducible* by G if $f - \operatorname{Lt}(f)$ is reducible by G or there is $g \in G$ such that $\operatorname{Lt}(g) \mid \operatorname{Lt}(f)$. A set $G \subseteq R[\boldsymbol{x}]^k$ is *softly reduced* if no $f \in G$ is softly reducible by $G \setminus \{f\}$.

We will consider the following ordering of finite subsets of $R[\boldsymbol{x}]^k$. We say that $G_1 \leq_S G_2$ if there is an injective map $\phi : G_1 \to G_2$ such that $g \leq_P \phi(g)$ for all $g \in G_1$. This ordering is a well partial ordering (Lemma 13.35). One step of a soft reduction is performed in the following algorithm SoftlyReduce.

Algorithmus 13.22 (Soft reduction).
Input: $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$ such that G is not softly reduced.
Output: $H \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$ such that

(1) $\langle H \rangle = \langle G \rangle$,
(2) Every $g \in G$ has a strong standard representation by H,
(3) $H <_S G$

function SoftlyReduce(G)
  Choose $f, h \in F$ and a term $a\boldsymbol{x}^\alpha e_i$ from f such that $f \neq h$, $\operatorname{Lm}(h) \mid \boldsymbol{x}^\alpha e_i$ and there is $q \in R$ such that ($\boldsymbol{x}^\alpha e_i = \operatorname{Lm}(f)$ and $a - q \operatorname{Lc}(h) = 0$) or ($\boldsymbol{x}^\alpha e_i \neq \operatorname{Lm}(f)$ and $\hat{\delta}(a - q \operatorname{Lc}(h)) < \hat{\delta}(a)$).
  $r \leftarrow f - q \frac{\boldsymbol{x}^\alpha e_i}{\operatorname{Lm}(h)} h$
  if $r = 0$ **then**
    $H \leftarrow G \setminus \{f\}$
  else
    $H \leftarrow (G \setminus \{f\}) \cup \{r\}$
  Return H

Lemma 13.23. *Algorithm 13.22 is correct.*

Proof. Clearly, H and G generate the same submodule.

Next, we show that every $g \in G$ has a strong standard representation. Let $g \in G$. If $g \in H$, then $g = 1\boldsymbol{x}^0 g$ is such a representation. If $g \notin H$, then $g = f$ and

$$f = q\frac{\boldsymbol{x}^\alpha e_i}{\operatorname{LM}(h)}h + 1\boldsymbol{x}^0 r. \tag{13.9}$$

We first assume $r \neq 0$. If $\operatorname{LT}(f) = a\boldsymbol{x}^\alpha e_i$, then $\operatorname{DEG}(\frac{\boldsymbol{x}^\alpha e_i}{\operatorname{LM}(h)}h) = (\alpha, i) = \operatorname{DEG}(f)$ and $\operatorname{DEG}(\boldsymbol{x}^0 r) = \operatorname{DEG}(r) < \operatorname{DEG}(f)$. If $\operatorname{LT}(f) \neq a\boldsymbol{x}^\alpha e_i$, then $\operatorname{DEG}(\frac{\boldsymbol{x}^\alpha e_i}{\operatorname{LM}(h)}h) = (\alpha, i) < \operatorname{DEG}(f)$ and $\operatorname{DEG}(\boldsymbol{x}^0 r) = \operatorname{DEG}(r) = \operatorname{DEG}(f)$. In both cases (13.9) is a strong standard representation of f by H with remainder 0. If $r = 0$, then $f = q\frac{\boldsymbol{x}^\alpha e_i}{\operatorname{LM}(h)}h$ is a strong standard representation.

For proving $H <_S G$, we define $\phi : H \to G$ by $\phi(h) = h$ for $h \in H \setminus \{r\}$, and $\phi(r) = f$ when $r \neq 0$. Since $r <_P f$, the mapping ϕ witnesses $H <_S G$. □

We also need to normalize polynomial vectors. The following procedure normalizes one vector in G.

ALGORITHMUS 13.24 (Normalization).
Input: $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$ such that G contains an element that is not normalized. Output: $H \subseteq R[\boldsymbol{x}]^k \setminus \{0\}, H \neq \varnothing$ such that

(1) $\langle H \rangle = \langle G \rangle$,
(2) Every $g \in G$ has a strong standard representation by H,
(3) $H <_P G$.

```
function NORMALIZE(G)
    Choose g ∈ G such that g is not normalized
    Find a unit u in R such that ug is normalized
    H ← (G \ {g}) ∪ {ug}
    Return H
```

LEMMA 13.25. *Algorithm 13.24 is correct.*

PROOF. It is clear that H and G generate the same submodule.

Furthermore, $g = u^{-1}\boldsymbol{x}^0(ug)$ is a strong standard representation of g by H.

We have $ug <_P g$. Hence $\phi(h) := h$ for $h \in H \setminus \{ug\}$ and $\phi(ug) = g$ witnesses $H <_S G$. □

THEOREM 13.26. *Let G be a softly reduced strong Gröbner basis in which every element is normalized. Then G is reduced.*

PROOF. Let $g \in G$. We have to show that g is not reducible by $G \setminus \{g\}$. Suppose that g is reducible. Then there are $h \in G \setminus \{g\}$, a term $a\boldsymbol{x}^\alpha e_i$ in g and $q \in R$ such that $\operatorname{LM}(h) \mid \boldsymbol{x}^\alpha e_i$ and $\hat{\delta}(a - q\operatorname{LC}(h)) < \hat{\delta}(a)$. If $a\boldsymbol{x}^\alpha e_i \neq \operatorname{LT}(g)$, then $g - \operatorname{LT}(g)$ is reducible by $\{h\}$, and thus g is softly reducible by $G \setminus \{g\}$. If $a\boldsymbol{x}^\alpha e_i = \operatorname{LT}(g)$, then let $d := \gcd(\operatorname{LC}(g), \operatorname{LC}(h))$. There is a polynomial vector f in the module generated by G such that $\operatorname{LT}(f) = d\boldsymbol{x}^\alpha e_i$ and thus there is $g_1 \in G$ with $\operatorname{LT}(g_1) \mid d\boldsymbol{x}^\alpha e_i$. Since G is softly reduced, we then have $g_1 = g$, and thus $a = \operatorname{LC}(g) = \operatorname{LC}(g_1) \mid \operatorname{LC}(h)$. Then $\operatorname{LC}(g) - q\operatorname{LC}(h)$ is a multiple of a. Since $\hat{\delta}(a - q\operatorname{LC}(h)) < \hat{\delta}(a)$, (13.6) implies $\delta(a - q\operatorname{LC}(h)) \leq \delta(a)$, and thus by Lemma 13.16, there is a unit in R such

that $u\,\mathrm{Lc}(g) = \mathrm{Lc}(g) - q\,\mathrm{Lc}(h)$. Since g is normalized, $\hat{\delta}(\mathrm{Lc}(g)) \leq \hat{\delta}(\mathrm{Lc}(g) - q\,\mathrm{Lc}(h))$; this contradicts $\hat{\delta}(\mathrm{Lc}(g) - q\,\mathrm{Lc}(h)) < \hat{\delta}(\mathrm{Lc}(g))$. □

In the computation of a strong Gröbner basis, we may interleave the three steps done in Augment, SoftlyReduce and Normalize as we wish. However, at some point, we may for instance enter the while loop with G normalized and softly reduced: then in this course of the while-loop, we have to use the procedure Augment. Note that the while-condition guarantees that we have at least one choice in every execution of the while-loop.

Algorithmus 13.27 (Reduced Strong Gröbner Basis).
Input: $F \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$, an admissible order $\leq$ of ${\mathbb{N}_0}^n \times \underline{k}$.
Output: $G \subseteq R[\boldsymbol{x}]^k \setminus \{0\}$ such that G is a reduced strong Gröbner basis of the submodule generated by F with respect to the monomial vector ordering $\leq$.

$G \leftarrow F$
$P \leftarrow \varnothing$
while $(\exists p, q \in G : p \neq q$ and $\{p, q\} \notin P)$ or
    (G is not softly reduced) or
    (G is not normalized) **do**
  Do exactly one out of the possible choices from (1),(2),(3):
  (1) $(G, x) \leftarrow \mathrm{Augment}(G, \{p, q\})$
    if $x = 1$ **then** $P \leftarrow P \cup \{\{p, q\}\}$
  (2) $G \leftarrow \mathrm{SoftlyReduce}(G)$
  (3) $G \leftarrow \mathrm{Normalize}(G)$
Return G

Theorem 13.28. *Algorithm 13.27 terminates on every input and produces a correct result.*

Proof. We first show that the algorithm terminates. Seeking a contradiction, we consider an execution that runs forever. In this execution, let G_i be the value of G at the beginning of the ith execution of the while-loop. The output conditions of the three algorithms Augment, SoftlyReduce and Normalize imply that $\mathrm{Deg}_\delta(G_i)\uparrow \subseteq \mathrm{Deg}_\delta(G_{i+1})\uparrow$. Thus there is an $n_1 \in \mathbb{N}$ such that for all $i \geq n_1$, we have $\mathrm{Deg}_\delta(G_i)\uparrow = \mathrm{Deg}_\delta(G_{i+1})\uparrow$.

From this point onwards, the assignments to G in lines 11, 16, 18 in Augment (Algorithm 13.11) will not be executed any more because all of these assignments strictly increase $\mathrm{Deg}_\delta(G)\uparrow$ with respect to $\subseteq$. In other words, G will not be changed any more by Augment, which also follows from output condition (2) of Augment. Hence for all $i \geq n_1$, we have $G_{i+1} \leq_S G_i$. Thus there is $n_2 \in \mathbb{N}$ with $n_2 \geq n_1$ such that for all $i \geq n_2$, $G_{i+1} = G_i$. From this point on, SoftlyReduce and Normalize cannot be called any more because both of them strictly decrease G with respect to $\leq_S$. Hence, the only remaining possible branches are the cases $f = 0$ and and $\exists g \in G : \mathrm{Lt}(f) \mid \mathrm{Lt}(g)$ in the execution of Augment. In detail, only the assignments contained in line 2 to 9 of Augment can be excuted. In both branches $x = 1$ (this can also be seen directly from output condition (3) of Augment), and thus $\#(\binom{G_{i+1}}{2} \setminus P_{i+1}) < \#(\binom{G_i}{2} \setminus P_i)$. Hence, starting from the n_2th execution of the while-loop of

Algorithm 13.27, this nonnegative number strictly decreases forever, which is impossible. Hence the algorithm terminates on every input.

From Lemma 13.36, we obtain that throughout the execution of the algorithm, the set $\{f \in R[\boldsymbol{x}]^k \mid f \text{ has a strong standard representation by } G\}$ increases with respect to $\subseteq$. By the output conditions of all three procedures Augment, SoftlyReduce and Normalize, $\langle G\rangle = \langle F\rangle$. Therefore, when the while-loop is left, G is softly reduced and G is normalized. Furthermore, every two-element subset $\{p, q\}$ of G lies in P and therefore has an S-polynomial vector that is 0 or has a strong standard representation by G. Thus by Theorem 13.10, G is a strong Gröbner basis of $\langle G\rangle$, and by Theorem 13.26, G is reduced. □

8. Linear algebra over $R[\boldsymbol{x}]$

Let D be a commutative ring with unit. By $D^{r\times s}$, we denote the set of $r \times s$-matrices over D. For $A \in D^{r\times s}$, we define $\operatorname{col}(A) = \{Ax \mid x \in D^s\}$ as the *column module* and $\operatorname{row}(A) = \{yA \mid y \in D^r\}$ as the *row module* of A. The set $\ker(A) = \{y \in D^s \mid Ay = 0\}$ is the *kernel* or *null module* of A. We will now compute bases for these modules in the case $D = R[x_1, \dots, x_n]$, where R is a Euclidean domain. We assume that we have the Euclidean grading function δ and $\hat\delta$ for R as in Section 6. As an additional assumption, we assume that $\hat\delta(1)$ is minimal in $\{\hat\delta(u) \mid u \text{ is a unit of } R\}$. For a matrix $A \in R[x_1, \dots, x_n]^{r\times s}$ and admissible monomial orders $\le_1, \dots, \le_s$ on the monomials of $R[\boldsymbol{x}]$, we define the *position over term*-order $\le$ by $\boldsymbol{x}^\alpha e_i \le \boldsymbol{x}^\beta e_j$ if $i > j$ or $(i = j$ and $\alpha \le_i \beta)$. We say that a matrix $H \in R[\boldsymbol{x}]^{r\times s}$ is the *Gröbner normal form* with respect to $(\le_1, \dots, \le_s)$ for A if the rows of H are a reduced strong Gröbner basis of the module $\operatorname{row}(A)$ with respect to $\le$, and the rows are ordered in strictly decreasing order with respect to the total order $\le_P$ defined after Definition 13.18. An example of such a matrix is given in (13.10). The entries of H can be described as follows:

Lemma 13.29. *Let R be a Euclidean domain, let $A \in R[\boldsymbol{x}]^{r'\times s}$, and let $H = (h_{j,i})_{(j,i)\in \underline{r}\times\underline{s}} \in R[\boldsymbol{x}]^{r\times s}$ be the Gröbner normal form of A. For $i \in \underline{s}$, we define the i*th step *of H by*

$$S_i = \{h_{t,i} \mid t \in \underline{r}, h_{t,i} \neq 0, \text{ and } h_{t,1} = \cdots = h_{t,i-1} = 0\}.$$

*The i*th fork ideal *of* $\operatorname{row}(A)$ *is the set*

$$F_i = \{p \in R[\boldsymbol{x}] \mid \exists p_{i+1}, \dots, p_s \in k[\boldsymbol{x}] : (\underbrace{0, \dots, 0}_{i-1}, p, p_{i+1}, \dots, p_s) \in \operatorname{row}(A)\}.$$

Then S_i is a reduced strong Gröbner basis of the ideal F_i of $R[\boldsymbol{x}]$ with respect to $\le_i$.

Proof. Let $p \in F_i$ with $p \neq 0$, and let $\boldsymbol{v} = (\underbrace{0, \dots, 0}_{i-1}, p, p_{i+1}, \dots, p_s) \in \operatorname{row}(A)$. Then $\boldsymbol{v} = p\,e_i + \sum_{j=i+1}^{s} p_j\,e_j$. Let $h_1, \dots, h_r$ be the rows of H. Since $\{h_1, \dots, h_r\}$ is a strong Gröbner basis of $\operatorname{row}(A)$, there is $t \in \underline{r}$ such that $\operatorname{Lt}(h_t) \mid \operatorname{Lt}(\boldsymbol{v}) = \operatorname{Lt}(p\,e_i)$. Then $\operatorname{Lt}(h_t)$ is of the form $a\boldsymbol{x}^\alpha e_i$, and therefore $h_{t,i} \in S_i$. Hence h_t can be written as $(0, \dots, 0, h_{t,i}, h_{t,i+1}, \dots, h_{t,s})$ with $\operatorname{Lt}(h_t) = \operatorname{lt}(h_{t,i})e_i$. (Recall from Section 5 that we write $\operatorname{Lt}(f)$ when f is a polynomial vector in $R[\boldsymbol{x}]^k$ and $\operatorname{lt}(f)$ when f is a single polynomial in $R[\boldsymbol{x}]$.) Hence $\operatorname{lt}(h_{t,i}) \mid \operatorname{lt}(p)$. Thus S_i is a Gröbner basis of F_i.

Now suppose that S_i is not reduced. Then we have $h_{u,i}, h_{v,i} \in S_i$ with $u \neq v$, $q \in R$ and $\alpha \in {\mathbb{N}_0}^n$ such that $\deg(h_{u,i}) \geq \deg(h_{v,i})$ and $h_{u,i} >_p h_{u,i} - q\boldsymbol{x}^\alpha h_{v,i}$, where $\leq_p$ is defined from $\leq_i$ for polynomials in analogy to the definition of $\leq_P$ for polynomial vectors in Section 6. Then $h_u >_P h_u - q\boldsymbol{x}^\alpha h_v$, contradicting the fact that the rows of H are a reduced Gröbner basis. □

This allows us to solve linear systems over $R[\boldsymbol{x}]$. As an example, we consider the linear equation $(10y)z_1 + 0z_2 + (4x)z_3 = 4x^3$, where we look for the set of all solutions $(z_1, z_2, z_3) \in \mathbb{Z}[x, y]^3$. We collect the data from this equation in the matrix

$$A' := \begin{pmatrix} -4x^3 & 1 & 0 & 0 & 0 \\ 10y & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 4x & 0 & 0 & 0 & 1 \end{pmatrix}$$

and we compute the Gröbner normal form (with respect to the lexicographical ordering with $x > y$ in all columns) of A' as

$$H = \begin{pmatrix} 2xy & 0 & x & 0 & -2y \\ 4x & 0 & 0 & 0 & 1 \\ 10y & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & x^2 \\ 0 & 0 & 2x & 0 & -5y \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{13.10}$$

Then we can read from this matrix that $(0, 0, x^2)$ is one solution, and the solution module of $(10y)z_1 + 0z_2 + (4x)z_3 = 0$ is generated, as a $\mathbb{Z}[x, y]$-module, by $(2x, 0, -5y)$ and $(0, 1, 0)$. This is justified by the following theorem, which explains how to solve linear systems in a style that follows [**AL94**, Chapter 3.8].

THEOREM 13.30. *Let R be a Euclidean domain, let $A \in R[\boldsymbol{x}]^{r\times s}$, let $b \in R[\boldsymbol{x}]^{r\times 1}$ and let $\leq_{-1}, \leq_0, \leq_1, \ldots, \leq_s$ be admissible orders on the monomials of $R[\boldsymbol{x}]$. Let $H \in R[\boldsymbol{x}]^{r'\times(r+s+1)}$ be the Gröbner normal form of*

$$A' = \left(\begin{array}{c|c} -b^T & \\ A^T & I_{s+1} \end{array}\right)$$

with respect to the monomial orders $(\underbrace{\leq_{-1}, \ldots, \leq_{-1}}_{r \text{ times}}, \leq_0, \leq_1, \ldots, \leq_s)$. We write H as

$$H = \begin{pmatrix} B & * & * \\ 0 & v & S \\ 0 & 0 & D \end{pmatrix},$$

where B has exactly r columns, v exactly 1 column and D exactly s columns, and furthermore the last line of B is not the zero-vector, and the last entry of v is not 0. Then we have:

(1) *The entries of v are a reduced strong Gröbner basis of the ideal*

$$(\mathrm{col}(A) : b) := \{p \in R[\boldsymbol{x}] \mid p\,b \in \mathrm{col}(A)\}.$$

of $R[\boldsymbol{x}]$ with respect to the monomial order $\leq_0$.

(2) *The system $Ax = b$ has a solution in $R[\boldsymbol{x}]^s$ if and only if $v = (1)$. Then the matrix S has exactly one row s_1, and s_1 is the minimal solution of $Ax = b$ with respect to $\leq_P$, where $\leq_P$ is the total order on polynomial vectors defined from the admissible order $\leq$ that is the position over term order coming from $(\leq_1, \ldots, \leq_s)$.*

(3) *D is in Gröbner normal form and* $\operatorname{row}(D) = \ker(A)$.

PROOF. (1) We first show that $\{p \in R[\boldsymbol{x}] \mid p\,b \in \operatorname{col}(A)\}$ is equal to the $(r+1)$th fork ideal F_{r+1} of A'. To this end, let $a_1, \ldots, a_s \in R[\boldsymbol{x}]^r$ be the column vectors of A. For proving one inclusion, we assume that $p_{r+1} \in F_{r+1}$. Then there are $p_{r+2}, \ldots, p_{r+s+1} \in R[\boldsymbol{x}]$ such that $(0, \ldots, 0, p_{r+1}, p_{r+2}, \ldots, p_{r+s+1})$ is in $\operatorname{row}(A')$, and thus there is $(f_0, f_1, \ldots, f_s) \in R[\boldsymbol{x}]^{s+1}$ such that

$$(f_0, f_1, \ldots, f_s) \cdot A' = (0, \ldots, 0, p_{r+1}, p_{r+2}, \ldots, p_{r+s+1}). \tag{13.11}$$

Considering the first r entries of the right hand side of (13.11), we obtain $-f_0 b + \sum_{i=1}^s f_i a_i = 0$, and hence $f_0 b = \sum_{i=1}^s f_i a_i$, and therefore $f_0 b \in \operatorname{col}(A)$. The $(r+1)$ th column of A' is the first unit vector in $R[\boldsymbol{x}]^{s+1}$. Hence $f_0 = p_{r+1}$, und thus $p_{r+1} b \in \operatorname{col}(A)$ and therefore $p_{r+1} \in (\operatorname{col}(A) : b)$.

Now assume that $p \in (\operatorname{col}(A) : b)$. Then there is $(f_1, \ldots, f_s) \in k[\boldsymbol{x}]^s$ such that $\sum_{i=1}^s f_i a_i = pb$. Therefore the first r columns of $(p, f_1, \ldots, f_s) \cdot A'$ are 0, and therefore the $(r+1)$ th entry of $(p, f_1, \ldots, f_s) \cdot A'$ is an element of F_{r+1}. Since this entry is p, we have $p \in F_{r+1}$.

By Lemma 13.29, the entries of v are a reduced strong Gröbner basis of $F_{r+1} = (\operatorname{col}(A) : b)$ with respect to $\leq_0$.

(2) The system $Ax = b$ has a solution if and only if $b \in \operatorname{col}(A)$, which means $1 \in (\operatorname{col}(A) : b)$. This holds if and only if the reduced Gröbner basis of $(\operatorname{col}(A) : b)$ is $\{1\}$. By item (1), the entries of v are a reduced Gröbner basis of $(\operatorname{col}(A) : b)$. Altogether, $Ax = b$ has a solution in $R[\boldsymbol{x}]^s$ if and only if $v = (1)$.

(3) It is not hard to show that the rows of D are a reduced strong Gröbner basis of the module

$$E := \{(f_{r+2}, \ldots, f_{r+s+1}) \in R[\boldsymbol{x}]^s \mid (0, \ldots, 0, f_{r+2}, \ldots, f_{r+s+1}) \in \operatorname{row}(A')\}.$$

We now show $E = \ker(A)$. For $\subseteq$, we assume $(0, \ldots, 0, f_{r+2}, \ldots, f_{r+s+1}) \in \operatorname{row}(A')$. Then there is $(g_0, g_1, \ldots, g_s) \in R[\boldsymbol{x}]^{s+1}$ with

$$(g_0, g_1, \ldots, g_s) \cdot A' = (0, \ldots, 0, f_{r+2}, \ldots, f_{r+s+1}). \tag{13.12}$$

Hence $g_0 = 0$ and $(g_1, \ldots, g_s) \cdot A^T = 0$, and therefore $(g_1, \ldots, g_s) \in \ker(A)$. Since $(g_1, \ldots, g_s) = (f_{r+2}, \ldots, f_{r+s+1})$, we obtain that $(f_{r+2}, \ldots, f_{r+s+1}) \in \ker(A)$.

If $(g_1, \ldots, g_s) \in \ker(A)$, then $(0, g_1, \ldots, g_s) \cdot A' = (0, \ldots, 0, g_1, \ldots, g_s)$ and thus $(g_1, \ldots, g_s) \in E$. □

The Gröbner normal form generalizes the row echelon normal form of a matrix A over a field k as computed, e.g., in Mathematica [**Wol24**] by `RowReduce [A]`. To see this, we set $R := k$ and consider A as a matrix over $R[x_1]$ (in which x_1 never appears). Similarly, it also generalizes the Hermite normal form of a matrix over $\mathbb{Z}$ (with the elements above the pivot elements

normalized to minimize their absolute values, and preferring 3 over -3). Here we consider A as a matrix over $\mathbb{Z}[x_1]$, and set $R := \mathbb{Z}$, $\delta(z) := |z|$ and $\hat{\delta}(z) = 3|z| - \operatorname{sgn}(z)$ for all $z \in \mathbb{Z}$ to obtain $\hat{\delta}(0) < \hat{\delta}(1) < \hat{\delta}(-1) < \hat{\delta}(2) < \hat{\delta}(-2) < \cdots$. Hence Theorem 13.19 also implies the uniqueness of these normal forms. We note that the Gröbner normal form uses a position over term ordering of the monomial vectors. In the last row of a Gröbner normal form, we find a minimal nonzero element of the row module with respect to the ordering $\leq_P$: such an element then has a maximal amount leading zero components. In other applications, minimal elements with respect to other properties (such as the maximal degree of the components) are searched. Here, a term over position ordering is useful. Such applications are given, e.g., in [**Lic13**] and the fact that a minimal element has been found can often be argued using Theorem 13.19.

9. Partial orders

A partially ordered set (A, ρ) is a set A together with a partial order, i.e., a reflexive, transitive and antisymmetric relation ρ. Often, we write $a \leq b$ or $b \geq a$ for $(a, b) \in \rho$, and $a < b$ or $b > a$ when $(a, b) \in \rho$ and $(b, a) \notin \rho$. We say that a and b are *uncomparable* and write $a \perp b$ if $(a, b) \notin \rho$ and $(b, a) \notin \rho$. The sequence $(a_i)_{i\in\mathbb{N}}$ is an *infinite descending chain* in A when $a_i > a_{i+1}$ for all $i \in \mathbb{N}$, and an *infinite antichain* when $a_i \perp a_j$ for all $i, j \in \mathbb{N}$ with $i \neq j$. A partial ordering $\leq$ on A is a *well partial order* if it has no infinite descending chains and no infinite antichains. It is a *well order* if it is total (i.e., has no distinct uncomparable elements) and has no infinite descending chains. For a subset B of the partially ordered set $(A, \leq)$, $b \in B$ is *minimal* in B if there is no $b' \in B$ with $b' < b$. The subset B is *upward closed* if for all $b \in B$ and $a \in A$ with $b \leq a$, we have $a \in B$. The product of (A_1, ρ_1) and (A_2, ρ_2) is the set $A_1 \times A_2$ partially ordered by the relation ρ defined by $((a_1, a_2), (b_1, b_2)) \in \rho :\Leftrightarrow (a_1, b_1) \in \rho_1$ and $(a_2, b_2) \in \rho_2$. Our investigation of these partial orderings is facilitated by Ramsey's Theorem [**Ram29**] (cf. [**Neš95**]): Denote the two element subsets of $\mathbb{N}$ by $\binom{\mathbb{N}}{2}$ and let c be a function from $\binom{\mathbb{N}}{2}$ into a finite set. Then there exists an infinite subset T of $\mathbb{N}$ such that c is constant on $\binom{T}{2}$. All results in this section are well known; some are taken from the survey [**AA20**].

THEOREM 13.31 (Dickson's Lemma [**Dic13**]). *The product of two well partially ordered sets is well partially ordered.*

PROOF. Let $(A, \leq_A)$ and $(B, \leq_B)$ be well partially ordered sets, and let $((a_i, b_i))_{i\in\mathbb{N}}$ be any sequence from $A \times B$. We colour the two element subsets of $\mathbb{N}$ with one of the nine colours from $\{\leq, >, \perp\}^2$ as follows: when $i < j$ then $C(\{i, j\}) = (\leq, \leq)$ if $a_i \leq a_j$ and $b_i \leq b_j$, $C(\{i, j\}) = (\leq, >)$ if $a_i \leq a_j$ and $b_i > b_j$, ... By Ramsey's Theorem there is an infinite subset T of $\mathbb{N}$ such that all two-element subsets of T have the same color c. If this colour c is not $(\leq, \leq)$, then we find an infinite descending chain or an infinite antichain in either A or B. Hence $c = (\leq, \leq)$. This implies that $((a_i, b_i))_{i\in\mathbb{N}}$ is neither an infinite descending chain nor an infinite antichain. □

LEMMA 13.32. *Let $\leq_{\mathrm{a}}$ be an admissible ordering on $\operatorname{Mon}(n, k)$. Then there is no infinite descending chain $m_1 >_{\mathrm{a}} m_2 >_{\mathrm{a}} \cdots$ with respect to this ordering.*

PROOF. Let $(m_i)_{i\in\mathbb{N}}$ be a sequence from $\mathrm{Mon}(n,k)$. We colour two-element subsets $\{i,j\}$ of $\mathbb{N}$ with $i<j$ by $C(\{i,j\})=1$ if $m_i \mid m_j$, $C(\{i,j\})=2$ if $m_j \mid m_i$ and $m_j \neq m_i$, and $C(\{i,j\})=3$ if $m_i \nmid m_j$ and $m_j \nmid m_j$. We use Ramsey's Theorem to obtain an infinite subset T of $\mathbb{N}$ such that all two-element subsets of T have the same colour c. If this colour is 2 or 3, then we obtain an infinite descending chain or an infinite antichain in $\mathrm{Mon}(n,k)$, which is order isomorphic to $(\mathbb{N}_0,\leq)^n \times (\{1,\dots,k\},=)$, contradicting Theorem 13.31. Hence this colour is 1 and thus there are $i,j\in\mathbb{N}$ with $i<j$ such that $m_i \mid m_j$. Then $m_i \leq_{\mathrm{a}} m_j$. Thus $(m_i)_{i\in\mathbb{N}}$ cannot be an infinite descending chain. □

As another consequence, we obtain that the partial order relation $\sqsubseteq_\delta$ defined in (13.1), which is the order of the direct product of n copies of $(\mathbb{N}_0,\leq)$ with $(\{1,\dots,k\},=)$ and $(W,\leq)$ has no infinite descending chain and no infinite antichain:

THEOREM 13.33. *Let $(W,\leq)$ be a well ordered set, and let $\sqsubseteq_\delta$ be the partial ordering on $\mathbb{N}_0{}^n \times \underline{k} \times W$ defined in (13.1). Then we have*

(1) *The order $\sqsubseteq_\delta$ is a well partial order.*
(2) *For every subset D of $\mathbb{N}_0{}^n \times \underline{k} \times W$, the set $\mathrm{Min}(D)$ of minimal elements of D with respect to $\sqsubseteq_\delta$ is finite, and for every $d\in D$ there is $d'\in\mathrm{Min}(D)$ with $d'\sqsubseteq_\delta d$.*
(3) *There is no infinite ascending chain $D_1 \subset D_2 \subset \cdots$ of upward closed subsets of $(\mathbb{N}_0{}^n \times \underline{k} \times W, \sqsubseteq_\delta)$.*

PROOF. (1) $(\mathbb{N}_0{}^n \times \underline{k} \times W, \sqsubseteq_\delta)$ is order isomorphic to the product of n copies of $(\mathbb{N}_0,\leq)$ with $(\underline{k},=)$ and $(W,\leq)$. Since all factors are well partially ordered, Theorem 13.31 implies that $\sqsubseteq_\delta$ is a well partial order. (2) Distinct minimal elements of D of are all uncomparable with respect $\sqsubseteq_\delta$. Since $\sqsubseteq_\delta$ is a well partial order and therefore has no infinite antichains, $\mathrm{Min}(D)$ is finite. Now let $d\in D$. If $\{x\in D \mid x\sqsubseteq_\delta d\}$ has no minimal element, we can construct a sequence $(d_i)_{i\in\mathbb{N}}$ with $d \sqsupset_\delta d_1 \sqsupset_\delta d_2 \sqsupset_\delta \cdots$ of elements from D; such sequences do not exist because $\sqsubseteq_\delta$ is a well partial order, and therefore $\{x\in D \mid x\sqsubseteq_\delta d\}$ has a minimal element, which is then also minimal in D. (3) Let $U_1 \subset U_2 \subset \cdots$ be an infinite ascending chain of upward closed subsets of $\mathbb{N}_0{}^n \times \underline{k} \times W$. Then $U := \bigcup_{i\in\mathbb{N}} U_i$ has a finite set of minimal elements $\mathrm{Min}(U)$. Thus there is $k\in\mathbb{N}$ with $\mathrm{Min}(U)\subseteq U_k$, and therefore $U\subseteq U_k$, which yields the contradiction $U_{k+1}\subseteq U_k$. □

Next, we see that the order $\leq_P$ of polynomial vectors defined before Theorem 13.19 is a well order. For $f=\sum_{(\alpha,i)\in E} c_{(\alpha,i)}\boldsymbol{x}^\alpha e_i$, we let $[\boldsymbol{x}^\alpha e_i]\,f := c_{(\alpha,i)}$ denote the coefficient of $\boldsymbol{x}^\alpha$ of the ith component of f. Then for $p\neq q$, we have $p<_P q$ if $\hat\delta([\mathrm{Lm}(p-q)]\,p) < \hat\delta([\mathrm{Lm}(p-q)]\,q)$ and $p\leq_P q$ if $p=q$ or $p<_P q$.

LEMMA 13.34. *The relation $\leq_P$ is a well order on $R[\boldsymbol{x}]^k$.*

PROOF. The relation $\leq_P$ is clearly reflexive and antisymmetric. For transitivity, we assume $p<_P q<_P r$. Then $\mathrm{Lm}(p-r)=\mathrm{Lm}((p-q)+(q-r))$, and thus $\mathrm{Deg}(p-r)\leq\max(\mathrm{Deg}(p-q),\mathrm{Deg}(q-r))$. If $\mathrm{Lm}(p-q)=\mathrm{Lm}(q-r)$, then $\hat\delta([\mathrm{Lm}(p-q)]\,p)<\hat\delta([\mathrm{Lm}(p-q)]\,q)<\hat\delta([\mathrm{Lm}(p-q)]\,r)$. Hence $[\mathrm{Lm}(p-q)]\,(p-r)\neq 0$. Thus $\mathrm{Deg}(p-r)\geq\mathrm{Deg}(p-q)$, and therefore $\mathrm{Deg}(p-r)=\mathrm{Deg}(p-q)$. Now $\hat\delta([\mathrm{Lm}(p-r)]\,p)<\hat\delta([\mathrm{Lm}(p-r)]\,r)$, and thus $p<_P r$. If $\mathrm{Lm}(p-q)\neq\mathrm{Lm}(q-r)$,

then we first consider the case $\mathrm{DEG}(p-q) < \mathrm{DEG}(q-r)$. Then $\mathrm{DEG}(p-r) = \mathrm{DEG}((p-q)+(q-r)) = \mathrm{DEG}(q-r)$. Since $\mathrm{DEG}(p-q) < \mathrm{DEG}(q-r)$, we have $[\mathrm{LM}(q-r)]\,p = [\mathrm{LM}(q-r)]\,q$. Therefore $\hat{\delta}([\mathrm{LM}(q-r)]\,p) < \hat{\delta}([\mathrm{LM}(q-r)]\,r)$ and thus $p <_P r$. The case $\mathrm{DEG}(p-q) > \mathrm{DEG}(q-r)$ is similar. Thus $\leq_P$ is transitive. It is easy to see that the ordering $\leq_P$ is total. Now let $(f_i)_{i\in\mathbb{N}}$ be an infinite descending chain with respect to $\leq_P$; among such chains, choose one for which $\mathrm{DEG}(f_1)$ is minimal. Then we must have $\mathrm{DEG}(f_1) = \mathrm{DEG}(f_i)$ for all $i \in \mathbb{N}$, since otherwise $(f_j)_{j\geq i}$ would contradict the minimality. Thus $\hat{\delta}(\mathrm{LC}(f_i)) \geq \hat{\delta}(\mathrm{LC}(f_{i+1}))$ for all $i \in \mathbb{N}$. This means that there is $n_1 \in \mathbb{N}$ such that $\hat{\delta}(\mathrm{LC}(f_i)) = \hat{\delta}(\mathrm{LC}(f_{i+1}))$ and therefore $\mathrm{LT}(f_i) = \mathrm{LT}(f_{i+1})$ for all $i \geq n_1$. Then $(f_i - \mathrm{LT}(f_i))_{i\geq n_1}$ is an infinite descending sequence with respect to $\leq_P$, contradicting the minimality of $\mathrm{DEG}(f_1)$. □

After stating Definition 13.21, we have ordered finite subsets F, G of $R[\boldsymbol{x}]^k$ by $F \leq_S G$ if there is an injective $\phi : F \to G$ with $f \leq_P \phi(f)$ for all $f \in F$.

LEMMA 13.35. *The relation $\leq_S$ is a well order on $R[\boldsymbol{x}]^k$.*

PROOF. Reflexivity and transitivity of $\leq_S$ are immediate. For checking that $\leq_S$ is antisymmetric, we assume $F \leq_S G$ and $G \leq_S F$, witnessed by $\phi_1 : F \to G$ and $\phi_2 : G \to F$. Then defining $\phi := \phi_2 \circ \phi_1$, we obtain an injective map $\phi : F \to F$ such that $f \leq \phi(f)$ for all $f \in F$. We claim that $\phi(f) = f$ for all $f \in F$. Let f be minimal in F with respect to $\leq_P$ such that $f \neq \phi(f)$. Then $f <_P \phi(f)$. Since F is finite, ϕ is surjective, and thus there is $g \in F$ with $\phi(g) = f$. Since $\phi(f) >_P f$, we then have $g \neq f$ and therefore since $g \leq_P \phi(g)$, we have $g <_P f$. Since we also have $g \neq \phi(g)$, the polynomial vector g contradicts the minimality of f. Therefore, ϕ is the identity map on F. Hence from $\phi_2 \circ \phi_1 = \mathrm{id}$, we obtain that for each $f \in F$, we have $f \leq_P \phi_1(f) \leq_P \phi_2(\phi_1(f)) = f$, which implies $\phi_1(f) = f$ for all $f \in F$. Thus ϕ_1 is the identity mapping, which implies $F \subseteq G$. Since F and G have the same number of elements, this implies $F = G$, completing the proof that $\leq_S$ is antisymmetric.

Now let $(F_i)_{i\in\mathbb{N}}$ be such that $F_i >_S F_{i+1}$ for all $i \in \mathbb{N}$, and we choose such a chain for which $\#F_1$ is minimal. By this minimality, we then have $\#F_1 = \#F_i$ for all $i \in \mathbb{N}$. Let ϕ_i be an injective mapping from F_{i+1} to F_i with $f \leq \phi_i(f)$ for all $f \in F_{i+1}$. Because of $\#F_i = \#F_{i+1}$, the mapping ϕ_i is bijective, and we have $\phi_i^{-1}(\phi_i(x)) = x \leq_P \phi_i(x)$ for all $x \in F_{i+1}$, and thus $\phi_i^{-1}(y) \leq_P y$ for all $y \in F_i$. Let $\psi_i := \phi_i^{-1} \circ \cdots \circ \phi_2^{-1} \circ \phi_1^{-1}$, and fix $g \in F_1$. Then $(\psi_i(g))_{i\in\mathbb{N}_0}$ is a decreasing sequence in $(R[\boldsymbol{x}]^k, \leq_P)$, and therefore, there is $n_1 \in \mathbb{N}$ such that $(\psi_i(g))_{i\in\mathbb{N}}$ is constant. Let $G_i := F_i \setminus \{\psi_{i-1}(g)\}$. The mappings $\phi_i \setminus \{(\psi_i(g), \psi_{i-1}(g))\}$ witness that $G_{i+1} \leq_S G_i$ for all $i \in \mathbb{N}$. Hence by the minimality of $\#F_1$, the sequence $(G_i)_{i\in\mathbb{N}}$ is constant from some n_2 onwards. Hence from $\max(n_1, n_2)$ onwards, $(F_i)_{i\in\mathbb{N}}$ is constant, a contradiction. □

In proving that S-polynomial vectors that have a strong representation still have a strong representation after applying SOFTLYREDUCE or NORMALIZE, we have needed the following lemma:

LEMMA 13.36. *Let R be a Euclidean domain, let $\leq$ be an admissible term order of R, and let $F, G, H \subseteq R[x_1, \ldots, x_n]^k$. We assume that every $f \in F$ has a strong standard representation*

by G and that every $g \in G$ has a strong standard representation by H. Then every $f \in F$ has a strong standard representation by H.

PROOF. If $f = \sum_{i=1}^{N} a_i n_i g_i$ is a strong standard representation of f by G and $g_i = \sum_{j=1}^{M_i} b_{i,j} m_{i,j} h_{i,j}$ is a strong standard representation of g_i by H, then $f = \sum_{i=1} \sum_{j=1}^{M_i} a_i b_{i,j} (n_i m_{i,j}) h_{i,j}$ is a representation of f by H. To show that it is a strong standard representation, we observe that $\text{DEG}(n_1 m_{1,1} h_{1,1}) = \text{DEG}(n_1) + \text{DEG}(m_{1,1} h_{1,1}) = \text{DEG}(n_1) + \text{DEG}(g_1)$ because $g_1 = \sum_{j=1}^{M_1} b_{1,j} m_{1,j} h_{1,j}$ is a strong standard representation of g_1 by H. Furthermore, we have $\text{DEG}(n_1) + \text{DEG}(g_1) = \text{DEG}(n_1 g_1) = \text{DEG}(f)$ because of the standard representation of f. Similarly, we see that for $(i, j) \neq (1, 1)$, we have $\text{DEG}(n_i m_{i,j} h_{i,j}) < \text{DEG}(f)$. □

KAPITEL 14

Varietäten

1. Lösungsmengen polynomialer Gleichungssysteme

DEFINITION 14.1. Sei k ein Körper, sei $n \in \mathbb{N}$, und sei $F \subseteq k[x_1, \ldots, x_n]$. Dann definieren wir $\mathbb{V}(F)$, die *durch F beschriebene Varietät*, durch $\mathbb{V}(F) = \{\boldsymbol{a} \in k^n \mid \overline{f}(\boldsymbol{a}) = 0 \text{ für alle } f \in F\}$. Eine Teilmenge V von k^n ist eine *Varietät*, wenn es ein $F \subseteq k[x_1, \ldots, x_n]$ gibt, sodass $V = \mathbb{V}(F)$.

LEMMA 14.2. *Sei k ein Körper, sei $M \subseteq k[x_1, \ldots, x_n]$, und sei $I = \langle M \rangle_{k[\boldsymbol{x}]}$. Sei F eine endliche Menge mit $\langle F \rangle_{k[\boldsymbol{x}]} = I$. Dann gilt $\mathbb{V}(M) = \mathbb{V}(I) = \mathbb{V}(F) = \mathbb{V}(\sqrt{I})$.*

DEFINITION 14.3. Sei k ein Körper, $n \in \mathbb{N}$, und sei $S \subseteq k^n$. Wir definieren das *zu S gehörende Ideal* durch $\mathbb{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid \forall \boldsymbol{s} \in S : \overline{f}(\boldsymbol{s}) = 0\}$.

LEMMA 14.4. *Sei k ein Körper, $n \in \mathbb{N}$, und sei $S \subseteq k^n$. Dann ist $\mathbb{I}(S)$ ein Ideal von $k[x_1, \ldots, x_n]$, und es gilt $\mathbb{I}(S) = \sqrt{\mathbb{I}(S)}$.*

LEMMA 14.5. *Sei k ein Körper, $n \in \mathbb{N}$, und seien $P, Q \subseteq k[x_1, \ldots, x_n]$, $S, T \subseteq k^n$. Dann gilt:*

(1) *Wenn $P \subseteq Q$, so gilt $\mathbb{V}(Q) \subseteq \mathbb{V}(P)$.*
(2) *Wenn $S \subseteq T$, so gilt $\mathbb{I}(T) \subseteq \mathbb{I}(S)$.*

LEMMA 14.6. *Sei k ein Körper, $n \in \mathbb{N}$, und sei $P \subseteq k[x_1, \ldots, x_n]$, $S \subseteq k^n$. Dann gilt:*

(1) $P \subseteq \mathbb{I}(\mathbb{V}(P))$.
(2) $S \subseteq \mathbb{V}(\mathbb{I}(S))$.
(3) $\mathbb{I}(\mathbb{V}(\mathbb{I}(S))) = \mathbb{I}(S)$.
(4) $\mathbb{V}(\mathbb{I}(\mathbb{V}(P))) = \mathbb{V}(P)$.

LEMMA 14.7. *Sei k ein Körper, sei $n \in \mathbb{N}$, seien $V, W \subseteq k^n$ Varietäten, und seien I, J Ideale von $k[x_1, \ldots, x_n]$. Dann gilt:*

(1) $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$,
(2) $\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J)$,
(3) $\mathbb{I}(V \cup W) = \mathbb{I}(V) \cap \mathbb{I}(W)$,
(4) $\mathbb{I}(V \cap W) \supseteq \sqrt{\mathbb{I}(V) + \mathbb{I}(W)}$.
(5) *Wenn k algebraisch abgeschlossen ist, gilt $\mathbb{I}(V \cap W) = \sqrt{\mathbb{I}(V) + \mathbb{I}(W)}$.*

DEFINITION 14.8. Sei k ein Körper, $n \in \mathbb{N}$, und sei $P \subseteq k^n$. Dann ist $\mathbb{V}(\mathbb{I}(P))$ der *Zariski-Abschluss* von P. P heißt *Zariski-dicht* in k^n, wenn $\mathbb{V}(\mathbb{I}(P)) = k^n$.

PROPOSITION 14.9. *Sei k ein Körper, $n \in \mathbb{N}$, und sei $P \subseteq k^n$. Sei $W \subseteq k^n$ eine Varietät mit $P \subseteq W$. Dann gilt $\mathbb{V}(\mathbb{I}(P)) \subseteq W$.*

Der Zariski-Abschluss $\mathbb{V}(\mathbb{I}(P))$ von P ist also die kleinste Varietät, die P enthält.

ÜBUNGSAUFGABEN 14.10

(1) Wir betrachten $M = \{(x+1)^2(x+2)^3(x^2+1)^2\}$ und studieren die Lösungsmenge in $\mathbb{Q}^1$ und in $\mathbb{C}^1$.
   (a) Berechnen Sie $\mathbb{I}(\mathbb{V}(M))$ über $\mathbb{Q}$.
   (b) Berechnen Sie $\mathbb{I}(\mathbb{V}(M))$ über $\mathbb{C}$.
(2) (cf. [CLO92]) Sei $M = \{t^2+y^2+z^2+2, 3t^2+4y^2+4z^2+5\}$ und sei $\pi(t,y,z) := (y,z)$.
   (a) Wir rechnen im Körper $\mathbb{C}$. Sei $I := \langle M\rangle_{\mathbb{C}[t,x,y]}$. Zeigen Sie, dass $\mathbb{V}(I \cap \mathbb{C}[y,z]) = \pi(\mathbb{V}(M))$.
   (b) Wir rechnen im Körper $\mathbb{R}$. Sei $I := \langle M\rangle_{\mathbb{R}[t,x,y]}$. Zeigen Sie, dass $\pi(\mathbb{V}(M)) = \varnothing$ und dass $\mathbb{V}(I \cap \mathbb{R}[y,z])$ unendlich ist.
(3) Sei k ein Körper, sei $V \subseteq k^n$ eine Varietät und sei M eine Menge, die Zariski-dicht in V ist. Zeigen Sie, dass für jedes Polynom $f \in k[x_1,\dots,x_n]$ mit $\overline{f}|_M = 0$ auch gilt, dass $\overline{f}|_V = 0$.

SATZ 14.11. *Sei k ein Körper, sei $n \in \mathbb{N}$, seien W, U Varietäten, und sei $\langle V_\alpha \mid \alpha \in A\rangle$ eine Familie von Varietäten. Dann gilt:*

(1) *$\bigcap\{V_\alpha \mid \alpha \in A\}$ ist eine Varietät.*
(2) *$W \cup U$ ist eine Varietät.*

2. Nullstellensätze

SATZ 14.12 (Hilbert). *Sei k ein algebraisch abgeschlossener Körper, sei $n \in \mathbb{N}$ und sei I ein Ideal von $k[x_1,\dots,x_n]$. Dann gilt $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.*

LEMMA 14.13. *Sei R ein kommutativer Ring mit Eins, und seien $M_1,\dots,M_n$ paarweise verschiedene maximale Ideale von R. Sei $M := \bigcap_{i=1}^n M_i$. Dann ist $\Psi : R/M \to \prod_{i=1} R/M_i$, $r + M \mapsto (r + M_i)_{i\in\underline{n}}$ ein Ringisomorphismus.*

Beweis: Wir zeigen, dass die n Einheitsvektoren im Bild von Φ liegen. Sei $i \in \underline{n}$ und $j \neq i$. Da $1 \in M_i + M_j$ gibt es $u_j \in M_j$ und $m_j \in M_i$, sodass $1 = u_j + m_j$. Dann gilt $1 = \prod_{j\in\{1,\dots,n\}\setminus\{i\}}(u_j + m_j) = (\prod_{j\in\{1,\dots,n\}\setminus\{i\}} u_j) + s$ mit $s \in M_i$. Sei $t := \prod_{j\in\{1,\dots,n\}\setminus\{i\}} u_j$. Dann gilt $t \in \bigcap_{j\in\{1,\dots,n\}\setminus\{i\}} M_j$ und $t \equiv_{M_i} 1$. Also gilt $\Phi(t) = (0,0,0,\dots,0,1+M_i,0,0,\dots,0)$. □

LEMMA 14.14. *Sei k ein Körper, und sei F eine endliche Teilmenge von k^n. Sei Φ definiert durch $\Phi : k[x_1,\dots,x_n] \to k^F$, $\Phi(f) = \overline{f}|_F$. Dann ist Φ surjektiv.*

Beweis: Für $a \in k^n$ sei $\Phi_a(f) := f(a)$ und $M_a = \ker(\Phi_a)$. Dann ist M_a ein maximales Ideal von $k[\boldsymbol{x}]$ und es gilt $\ker(\Phi) = \bigcap_{a\in F} M_a =: M$. Nun ist wegen Lemma 14.13 die Abbildung $\Psi : k[\boldsymbol{x}]/\bigcap_{a\in F} M_a \to \prod_{a\in F} k[\boldsymbol{x}]/M_a$ surjektiv. Ebenso ist $\varepsilon : (r_a + M_a)_{a\in F} \mapsto (r_a(a))_{a\in A}$ surjektiv, und daher auch $\Phi = \varepsilon \circ \Psi$. □

LEMMA 14.15. *Sei k ein Körper, und sei $S \subseteq k^n$. Dann gilt*

$$\dim_k(k[x_1,\dots,x_n]/\mathbb{I}(S)) \leq \#S.$$

Wenn S endlich ist, so gilt $\dim_k(k[x_1,\dots,x_n]/\mathbb{I}(S)) = \#S$.

Beweis: Die Abbildung $\Phi : f + \mathbb{I}(S) \mapsto \overline{f}|_S$ ist injektiv, daher gilt $\dim_k(k[x_1, \ldots, x_n]/\mathbb{I}(S)) \leq \#S$. Wenn S endlich ist, so ist die Abbildung Φ nach Lemma 14.14 sogar surjektiv. □

Satz 14.16. *Sei k ein Körper, K ein algebraisch abgeschlossener Körper mit $k \leq K$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$, und sei $\overline{I}$ das von I erzeugte Ideal von $K[\boldsymbol{x}]$. Dann ist $\mathbb{V}_K(I)$ genau dann endlich, wenn $k[\boldsymbol{x}]/I$ ein endlichdimensionaler k-Vektorraum ist. In diesem Fall gilt:*

$$\dim_k(k[\boldsymbol{x}]/I) = \dim_K(K[\boldsymbol{x}]/\overline{I}) \geq \dim_K K[\boldsymbol{x}]/\sqrt{\overline{I}} = \#V_K(I)$$

Beweis: Nach Satz 12.28(4) gilt $\dim_k(k[\boldsymbol{x}]/I) = \dim_K(K[\boldsymbol{x}]/\overline{I})$.

Wir nehmen nun an, dass $K[\boldsymbol{x}]/\overline{I}$ ein endlichdimensionaler k-Vektorraum ist und zeigen, dass $\mathbb{V}_K(I)$ endlich ist. Wegen Satz 10.33 ist $K[\boldsymbol{x}]/\overline{I}$ algebraisch über K. Also gibt es für jede Variable x_j ein $f \in K[t] \setminus \{0\}$ mit $f(x_j) \in \overline{I}$ und $f \neq 0$. Somit ist $\mathbb{V}_K(\overline{I}) = \mathbb{V}_K(I)$ endlich.

Wir nehmen nun an, dass $\mathbb{V}_K(I)$ endlich ist und zeigen, dass $K[\boldsymbol{x}]/\overline{I}$ ein endlichdimensionaler K-Vektorraum ist. Für $S := \mathbb{V}_K(\overline{I}) = \mathbb{V}_K(I)$ liefert Lemma 14.15 $\dim_K(K[\boldsymbol{x}]/\mathbb{I}_K(\mathbb{V}_K(\overline{I})) = \#\mathbb{V}_K(\overline{I})$, und mit Satz 14.12 auch

$$\dim_K(K[\boldsymbol{x}]/\sqrt{\overline{I}}) = \#\mathbb{V}_K(\overline{I}).$$

Wegen Satz 10.33 ist $K[\boldsymbol{x}]/\sqrt{\overline{I}})$ algebraisch über K. Also ist auch $K[\boldsymbol{x}]/\overline{I}$ algebraisch über K, und daher, wieder wegen Satz 10.33, endlichdimensional über K. □

Lemma 14.17. *Sei k ein Körper und X eine endliche Teilmente von k^n. Sei J ein Ideal von $k[\boldsymbol{x}]$. Dann existiert ein $f \in J$ mit $f(y) = 1$ für alle $y \in X \setminus V(J)$.*

Beweis: Für jedes $a \in X \setminus V(J)$ gibt es $f_a \in k[\boldsymbol{x}]$ mit $f_a \in J$ und $f_a(a) \neq 0$. Da $\Phi : k[\boldsymbol{x}] \to k^X$, $f \mapsto \overline{f}|_X$ surjektiv ist, gibt es ein $g_a \in k[\boldsymbol{x}]$ mit $g_a(a) := 1/f_a(a)$, $g_a(y) = 0$ für $y \in X \setminus \{a\}$. Dann leistet $f := \sum_{a \in X \setminus V(J)} g_a f_a$ das Gewünschte. □

Satz 14.18 ([**Cla14**, Theorem 7], "Finitesatz"). *Sei k ein Körper, und X eine endliche Teilmenge von k^n. Sei J ein Ideal von $k[\boldsymbol{x}]$. Dann gilt $I(X \cap V(J)) = I(X) + J$.*

Beweis: Die Inklusion $\supseteq$ ist leicht zu zeigen. Für $\subseteq$ wählen wir $h \in I(X \cap V(J))$. Aus Lemma 14.17 erhalten wir $f \in J$ mit f mit $f(y) = 1$ für alle $y \in X \setminus V(J)$. Für $a \in X \cap V(J)$ gilt wegen $h(a) = 0$ auch $(h - h \cdot f)(a) = 0$. Wenn $a \in X \setminus V(J)$, so gilt $h(a) = h(a)f(a)$. Folglich gilt $h - hf \in I(X)$ und daher $h = (h - hf) + hf \in I(X) + J$. □

Definition 14.19. Sei $n \in \mathbb{N}$, $f = \sum_{\alpha \in \mathbb{N}_0{}^n} c_\alpha \boldsymbol{x}^\alpha \in k[x_1, \ldots, x_n]$. Der *Support* von f ist definiert durch $\mathrm{Supp}(f) = \{\alpha \in \mathbb{N}_0{}^n \mid c_\alpha \neq 0\}$. Das Polynom f besitzt einen *dominierenden Term*, wenn es ein $\alpha \in \mathrm{Supp}(f)$ gibt, sodass für alle $\beta \in \mathrm{Supp}(f)$ gilt, dass $\alpha \sqsupseteq \beta$.

Ein dominierender Term ist bezüglich jeder zulässigen Monomordnung der führende Term. Jedes univariate Polynom $\neq 0$ besitzt einen dominierenden Term.

Lemma 14.20. *Seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Wir nehmen an, dass jedes f_i einen dominierenden Term besitzt. Sei $f \in k[x_1, \ldots, x_n]$, und sei β ein maximales Element in $(\mathrm{Supp}(f), \sqsubseteq)$. Sei $\leq$ eine zulässige Termordnung auf $k[x_1, \ldots, x_n]$. Dann gilt $\boldsymbol{x}^\beta \in \langle \mathrm{LT}_\leq(f_1), \ldots, \mathrm{LT}_\leq(f_s)\rangle_{k[\boldsymbol{x}]}$, oder es gibt eine Standarddarstellung $f = \sum_{i=1}^s h_i f_i + r$ mit $\beta \in \mathrm{Supp}(r)$.*

Beweis: Wir nehmen an, dass $\boldsymbol{x}^\beta \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle_{k[\boldsymbol{x}]}$. Sei f ein Gegenbeispiel, für das $\mathrm{DEG}(f)$ minimal bezüglich $\leq$ ist.

Wenn $\mathrm{LT}(f) \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle_{k[\boldsymbol{x}]}$ und $\mathrm{DEG}(f) = \beta$, so wählen wir eine Standarddarstellung $\sum h_i f_i + r$ von $f - \mathrm{LT}(f)$ und erhalten die Standarddarstellung $f = \sum h_i f_i + (r + \mathrm{LT}(f))$ von f. Wegen $\mathrm{DEG}(r) \leq \mathrm{DEG}(f - \mathrm{LT}(f)) < \mathrm{DEG}(f)$, gilt $\beta = \mathrm{DEG}(f) \in \mathrm{Supp}(r + \mathrm{LT}(f))$.

Wenn $\mathrm{LT}(f) \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle_{k[\boldsymbol{x}]}$ und $\mathrm{DEG}(f) > \beta$, so gilt $\mathrm{DEG}(f - \mathrm{LT}(f)) < \mathrm{DEG}(f)$ und $\beta \in \mathrm{Supp}(f - \mathrm{LT}(f))$. Wegen der Minimalität von f gibt es eine Standarddarstellung $f - \mathrm{LT}(f) = \sum_{i=1}^s h_i f_i + r$ mit $\beta \in \mathrm{Supp}(r)$, und folglich ist $f = \sum h_i f_i + (r + \mathrm{LT}(f))$ eine Standarddarstellung von f mit $\beta \in \mathrm{Supp}(r + \mathrm{LT}(f))$.

Wenn $\mathrm{LT}(f) \in \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle_{k[\boldsymbol{x}]}$, so wählen wir $i \in \underline{s}$ mit $\mathrm{LT}(f_i) \mid \mathrm{LT}(f)$. Im Fall $\beta \in \mathrm{Supp}(\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i)$ verwenden wir, dass f_i einen dominierenden Term besitzt und erhalten daraus $x^\beta \mid \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)}\mathrm{LT}(f_i)$, also $\beta \sqsubseteq \mathrm{DEG}(\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i)$, und folglich $\beta \sqsubseteq \mathrm{DEG}(f)$. Aus der Maximalität von β in $\mathrm{Supp}(f)$ erhalten wir dann $\beta = \mathrm{DEG}(f)$. Daher gilt $\boldsymbol{x}^\beta = \mathrm{LM}(f) \in \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle_{k[\boldsymbol{x}]}$, im Widerspruch zur Annahme. Im Fall $\beta \notin \mathrm{Supp}(\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i)$ sei $f' := f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i$. Dann gilt $\beta \in \mathrm{Supp}(f')$. Wir zeigen nun, dass β maximal in $\mathrm{Supp}(f')$ ist. Sei $\gamma \in \mathrm{Supp}(f')$ mit $\beta \sqsubset \gamma$. Dann gilt $\gamma \in \mathrm{Supp}(\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i)$. Da f_i einen dominierenden Term besitzt, gilt daher $\boldsymbol{x}^\gamma \mid \mathrm{LT}(f)$. Dann ist β aber nicht maximal in $\mathrm{Supp}(f)$, im Widerspruch zur Annahme. Folgich ist β maximal in $\mathrm{Supp}(f')$. Daher gibt es eine Standarddarstellung $f' = \sum_{j=1}^s h_j f_j + r$ mit $\beta \in \mathrm{Supp}(r)$. Dann ist $f = \sum_{j \in \underline{s}\setminus\{i\}} h_j f_j + (h_i + \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)}) f_i + r$ eine Standarddarstellung von f mit $\beta \in \mathrm{Supp}(r)$. □

SATZ 14.21 (Alons kombinatorischer Nullstellensatz, [**Alo99**]). *Sei k ein Körper, seien $S_1, \ldots, S_n$ endliche Teilmengen von k mit $\#S_i = t_i$ und sei $S = S_1 \times \cdots \times S_n$. Sei $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$.*

Dann gilt:

(1) *$G := \{g_1(x_1), \ldots, g_n(x_n)\}$ ist eine universelle Gröbnerbasis für $\mathbb{I}(S)$.*
(2) *Es gibt für jedes $f \in \mathbb{I}(S)$ Polynome $h_1, \ldots, h_n \in k[x_1, \ldots, x_n]$ mit $f = \sum_{i=1}^n h_i g_i$, sodass für den totalen Grad gilt:* $\deg(h_i g_i) \leq \deg(f)$.
(3) [**Las10**, Theorem 2] *(cf.* [**Alo99**, Theorem 1.2]*). Sei $f \in k[x_1, \ldots, x_n]$, und sei α ein maximales Element von* $\mathrm{Supp}(f)$ *bezüglich $\sqsubseteq$. Wenn $\alpha_i < t_i$ für alle $i \in \underline{n}$ gilt, so gilt $f \notin \mathbb{I}(S)$.*

Beweis: (2) Sei $\leq$ eine zulässige Ordnung auf $\mathbb{N}_0{}^n$, und sei $J := \langle G\rangle_{k[\boldsymbol{x}]}$. Es gilt $J \subseteq \mathbb{I}(S)$. Wegen Lemma 11.9 ist G eine Gröbnerbasis von J bezüglich $\leq$ und wegen Satz 10.31 gilt $\dim_k(k[\boldsymbol{x}]/J) = \prod_{i=1}^n t_i$. Wegen Lemma 14.15 gilt auch $\dim_k(k[\boldsymbol{x}]/\mathbb{I}(S)) = \prod_{i=1}^n t_i$. Die Abbildung $\varphi : f + J \mapsto f + \mathbb{I}(S)$ ist ein k-Vektorraumepimorphismus von $k[\boldsymbol{x}]/J$ nach $k[\boldsymbol{x}]/\mathbb{I}(S)$. Da beide Vektorräume die gleiche Dimension haben, ist φ daher auch injektiv, und folglich gilt $\mathbb{I}(S) \subseteq J$. Somit gilt $\mathbb{I}(S) = \langle G\rangle_{k[\boldsymbol{x}]}$.

(2) Wir wählen dazu eine Monomordnung $\leq$, die zuerst nach dem totalen Grad ordnet. Die Standarddarstellung von f bezüglich G leistet dann das Gewünschte.

(3) Wir wählen eine zulässige Ordnung $\leq$ auf ${\mathbb{N}_0}^n$. Da $\boldsymbol{x}^\alpha \notin \left\langle \{x_i^{t_i} \mid i \in \underline{n}\} \right\rangle_{k[\boldsymbol{x}]}$, gibt es wegen Lemma 14.20 eine Standarddarstellung von f bezüglich G mit Rest ungleich 0. Daher gilt wegen Korollar 10.29, dass $f \notin \mathbb{I}(S)$. □

Übungsaufgaben 14.22

(1) (H. Davenport 1935, cf. [**Alo99**, Theorem 3.2]) Sei p eine Primzahl, und seien A, B nichtleere Teilmengen von $\mathbb{Z}_p$. Sei $A+B = \{a+b \mid a \in A, b \in B\}$. Zeigen Sie, dass $|A+B| \geq \min(p, |A|+|B|-1)$. *Hinweis:* Der Fall $|A|+|B| > p$ lässt sich relativ elementar lösen. Im Fall $|A|+|B| \leq p$ betrachten Sie $C \supseteq A+B$ mit $C = |A|+|B|-2$ und das Polynom $\prod_{c \in C}(x+y-c)$.

(2) [**Ter66**] Sei k ein endlicher Körper mit $|k| = q$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Zeigen Sie $\mathbb{I}_k \mathbb{V}_k(J) = J + \langle \{x_i^q - x_i \mid i \in \underline{n}\} \rangle_{k[\boldsymbol{x}]}$.

(3) Sei k ein Körper, und X eine endliche Teilmenge von k^n. Zeigen Sie, dass jedes Ideal $J \supseteq \mathbb{I}(X)$ die Gleichung $\sqrt{J} = J$ erfüllt.

(4) Seien $k \leq K$ Körper, und sei X eine endliche Teilmenge von k^n. Zeigen Sie $\mathbb{I}_K(X) = \langle \mathbb{I}_k(X) \rangle_{K[\boldsymbol{x}]}$. *Hinweis:* Sei $\overline{\mathbb{I}_k(X)} := \langle \mathbb{I}_k(X) \rangle_{K[\boldsymbol{x}]}$. Betrachten Sie $\dim_K(K[\boldsymbol{x}]/\overline{\mathbb{I}_k(X)})$ und $\dim_K(K[\boldsymbol{x}]/\mathbb{I}_K(X))$ und verwenden Sie Satz 12.28.

Satz 14.23. *(Nakayamas Lemma) Sei R ein Noetherscher Ring, und seien M, I Ideale von R mit $M \cdot I = I$. Dann gibt es $r \in R$ mit $r \equiv_M 1$ und $rI = 0$.*

Beweis: Seien $I = \langle i_1, \ldots, i_k \rangle_R$. Da $MI = I$, gilt $i_j \in MI$. Folglich gibt es $m_{j,1} \ldots m_{j,k}$ mit $i_j = \sum_{l=1}^k m_{j,l} i_l$. Sei $M := (m_{j,l})_{j=1 \, l=1}^{k \quad k}$. Also gilt $(i_1, \ldots, i_k)^T = M \cdot (i_1, \ldots, i_k)^T$ und daher für $r := \det(\mathbf{I}_k - M)$ auch $r \cdot (i_1, \ldots, i_k)^T = 0$, also $rI = 0$. Es gilt $r \equiv_M \det(\mathbf{I}_k) = 1$. □

Lemma 14.24. *Sei R ein Noetherscher Ring, sei Q ein primäres Ideal von R, und sei M ein Ideal von R mit $Q \leq M < R$. Dann gilt $\bigcap_{n \in \mathbb{N}} M^n \subseteq Q$.*

Beweis: Wir betrachten zunächst den Fall $Q = 0$. Sei $I := \bigcap_{n \in \mathbb{N}} M^n$. Wir zeigen als erstes

$$I \subseteq MI. \tag{14.1}$$

Sei $MI = Q_1 \cap \cdots \cap Q_r$, wobei alle Q_j primär sind. Wir zeigen nun $I \subseteq Q_j$ für alle $j \in \underline{r}$. Wenn $M \subseteq Q_j$, so gilt wegen $I \subseteq M$ auch $I \subseteq Q_j$. Wenn $M \subseteq \sqrt{Q_j}$, so gibt es, da M endlich erzeugt ist, ein $n \in \mathbb{N}$ mit $M^n \subseteq Q_j$. Dann gilt $I \subseteq Q_j$. Wenn $M \nsubseteq \sqrt{Q_j}$, so gibt es $m \in M \setminus \sqrt{Q_j}$. Sei nun $i \in I$. Wegen $im \in MI \subseteq Q_j$ gilt $i \in Q_j$ oder es gibt ein $n \in \mathbb{N}$ mit $m^n \in Q_j$. Der Fall $m^n \in Q_j$ kann aber wegen $m \notin \sqrt{Q_j}$ nicht eintreten. Somit gilt $I \subseteq Q_j$, und somit gilt (14.1). Folglich gilt $I = MI$ und daher gibt es $r \in R$ mit $r \equiv_M 1$ und $rI = 0$. Sei nun $i \in I$. Da 0 primär ist und $ir = 0$, gilt entweder dass $i = 0$ gilt, oder es gibt ein $n \in \mathbb{N}$ mit $r^n = 0$ gibt. Dann gilt aber auch $1 = 1^n \equiv_M r^n = 0$ und somit $1 \in M$; wegen $M \neq R$ kann dieser zweite Fall nicht eintreten.

Wir betrachten nun den Fall, dass $Q \neq 0$. Dann ist R/Q Noethersch und das Ideal Q/Q primär. Wegen des bereits gezeigten Falls (für den Ring R/Q mit Nullideal Q/Q) gilt $\bigcap_{n \in \mathbb{N}} (M/Q)^n = Q/Q$. Sei nun $y \in \bigcap_{n \in \mathbb{N}} M^n$. Dann gilt $y + Q \in \bigcap_{n \in \mathbb{N}} (M/Q)^n$ und somit $y + Q \in Q/Q$, also $y \in Q$. □

Satz 14.25 (Perfekter Nullstellensatz [**Sha19**]). *Sei I ein Ideal von $k[x_1, \ldots, x_n]$ und $g \notin I$. Dann gibt es einen kommutativen Ring K mit $k \leq K$, sodass*

(1) $\dim_k K$ *ist endlich.*
(2) *Es gibt* $\xi \in K$ *mit* $\xi \in \mathbb{V}_K(I)$ *und* $g(\xi) \neq 0$.

Beweis: Da $g \notin I$ gibt es ein primäres Ideal Q mit $g \notin Q$. Sei M ein maximales Ideal von $k[\boldsymbol{x}]$ mit $Q \leq M$. Da $g \notin Q$, gilt $g \notin \bigcap_{n\in\mathbb{N}} M^n$. Daher gibt es $n \in \mathbb{N}$ mit $g \notin M^n$. Sei $J := M^n$. Wegen des Nullstellensatzes ist $k[x_1, \ldots, x_n]/M$ algebraisch über k (siehe Beweis von Satz 10.33). Wegen der Maximalität von M gilt $\sqrt{M^n} = M$. Es gilt also $\sqrt{J} = M$. Da $k[x_1, \ldots, x_n]/\sqrt{J}$ algebraisch über k ist, ist auch $k[x_1, \ldots, x_n]/J$ algebraisch über k und folglich nach Satz 10.33 auch endlichdimensional. Somit leisten $K := k[x_1, \ldots, x_n]/J$ und $\xi = (x_1 + J, \ldots, x_n + J)$ das Gewünschte. □

3. Zerlegung von Varietäten

Definition 14.26. Sei k ein Körper, $V \subseteq k^n$ eine Varietät. Die Varietät V ist *irreduzibel*, wenn

(1) $V \neq \varnothing$,
(2) Für alle Varietäten V_1, V_2 mit $V = V_1 \cup V_2$ gilt: $V_1 = V$ oder $V_2 = V$.

Satz 14.27. *Sei k ein Körper, $n \in \mathbb{N}$, und sei $V \subseteq k^n$ eine Varietät. Dann ist V Vereinigung endlich vieler irreduzibler Varietäten.*

Satz 14.28. *Sei k ein Körper, $n \in \mathbb{N}$, und seien $V_1, \ldots, V_l, W_1, \ldots, W_m$ irreduzible Varietäten, sodass für alle $i, j \in \{1, \ldots, l\}$ mit $i \neq j : V_i \not\subseteq V_j$ und für alle $i, j \in \{1, \ldots, m\} : W_i \not\subseteq W_j$ gilt. Dann gilt $l = m$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, l\} \to \{1, \ldots, m\}$, sodass für alle i die Gleichheit $V_i = W_{\pi(i)}$ gilt.*

Satz 14.29. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei $V \subseteq k^n$ eine Varietät. Dann ist V genau dann irreduzibel, wenn $\mathbb{I}(V)$ prim ist.*

4. Parametrisierte Varietäten und Implizitisierung

Definition 14.30. Sei k ein Körper, sei $n \in \mathbb{N}$, sei $m \in \mathbb{N}$, und seien $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$, $g_1, \ldots, g_n \in k[t_1, \ldots, t_m] \setminus \{0\}$. Eine Varietät V ist *durch* $((f_1, g_1), \ldots, (f_n, g_n))$ *parametrisiert*, wenn für

$$S := \{(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s})}, \ldots, \frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})}) \mid \boldsymbol{s} \in k^m, \overline{g_1 \cdots g_n}(\boldsymbol{s}) \neq 0\}$$

gilt: $V = \mathbb{V}(\mathbb{I}(S))$.

Lemma 14.31. *Sei k ein unendlicher Körper, seien $m, n \in \mathbb{N}$, und seien $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$, $g_1, \ldots, g_n \in k[t_1, \ldots, t_m] \setminus \{0\}$. Sei*

$$S := \{(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s})}, \ldots, \frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})}) \mid \boldsymbol{s} \in k^m, \overline{g_1 \cdots g_n}(\boldsymbol{s}) \neq 0\},$$

und sei $p \in k[x_1, \ldots, x_n]$. Dann sind äquivalent:

(1) $p \in \mathbb{I}(S)$.
(2) $p(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}) = 0$.

Beweis: Sei $l := \max\{\deg_{x_i}(p) \mid p \in \{1,\dots,n\}\}$. Wir definieren $q \in k[\boldsymbol{a},\boldsymbol{b}]$ durch

$$q(a_1,\dots,a_n,b_1,\dots,b_n) := p(\frac{a_1}{b_1},\dots,\frac{a_n}{b_n}) \cdot (b_1 \cdots b_n)^{l+1}.$$

Im Ring $k[\boldsymbol{a},\boldsymbol{b}]$ ist das Polynom ein Vielfaches von $b_1 \cdots b_n$. Wir beweisen nun als erstes (2)⇒(1). Sei dazu $\boldsymbol{s} \in k^m$ so, dass $\overline{g_1 \cdots g_n}(\boldsymbol{s}) \neq 0$. Wegen (2) gilt $q(f_1,\dots,f_n,g_1,\dots,g_n) = 0$. Also gilt

$$\overline{q}(\overline{f_1}(\boldsymbol{s}),\dots,\overline{f_n}(\boldsymbol{s}),\overline{g_1}(\boldsymbol{s}),\dots,\overline{g_n}(\boldsymbol{s})) = 0.$$

Folglich gilt auch

$$\overline{p}(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s})},\dots\frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})}) = 0.$$

Somit hat p den Punkt $(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s}},\dots\frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})})$ als Nullstelle. Wir zeigen nun (1)⇒(2). Wir beweisen dazu als erstes, dass für alle $\boldsymbol{s} \in k^m$ gilt, dass

$$\overline{q}(\overline{f_1}(\boldsymbol{s}),\dots,\overline{f_n}(\boldsymbol{s}),\overline{g_1}(\boldsymbol{s}),\dots,\overline{g_n}(\boldsymbol{s})) = 0. \tag{14.2}$$

Wenn nämlich $\overline{g_1}(\boldsymbol{s}) \cdots \overline{g_n}(\boldsymbol{s}) = 0$, so ist eines der $\overline{g}_j(\boldsymbol{s}) = 0$. Da $b_j | q$, gilt (14.2). Wenn $\overline{g_1}(\boldsymbol{s}) \cdots \overline{g_n}(\boldsymbol{s}) \neq 0$, so gilt wegen $p \in \mathbb{I}(S)$ auch $\overline{p}(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s})},\dots,\frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})}) = 0$, und somit (14.2). Da k unendlich ist, ist also $q(f_1(\boldsymbol{t}),\dots,f_n(\boldsymbol{t}),g_1(\boldsymbol{t}),\dots,g_n(\boldsymbol{t}))$ das Nullpolynom in $k[\boldsymbol{t}]$. Da $k(\boldsymbol{t})$ ein Integritätsbereich ist und alle $g_i \neq 0$, gilt also $p(\frac{f_1}{g_1},\dots,\frac{f_n}{g_n}) = 0$. □

Lemma 14.31 und Korollar 12.16 ergeben also einen Algorithmus, der eine Basis des zu einer parametrisierten Varietät gehörenden Ideals liefert. Außerdem zeigt Lemma 14.31, dass für unendliche k die durch $((f_1,g_1),\dots,(f_n,g_n))$ parametrisierte Varietät nur von $(\frac{f_1}{g_1},\dots,\frac{f_n}{g_n})$ abhängt.

Übungsaufgaben 14.32

(1) Wir betrachten die Teilmenge P von $\mathbb{C}^3$, die durch

$$P = \{\begin{pmatrix} t_1\,t_2 \\ t_1\,t_3 \\ t_2\,t_3 \end{pmatrix} \mid t_1,t_2,t_3 \in \mathbb{C}\}$$

gegeben ist. Sei J das von $\{x_1 - t_1\,t_2, x_2 - t_1\,t_3, x_3 - t_2\,t_3\}$ erzeugte Ideal von $\mathbb{C}[t_1,t_2,t_3,x_1,x_2,x_3]$.
   (a) Berechnen Sie $J \cap \mathbb{C}[x_1,x_2,x_3]$.
   (b) Berechnen Sie den Zariski-Abschluss $\mathbb{V}(\mathbb{I}(P))$ von P.
   (c) Gilt $P = \mathbb{V}(\mathbb{I}(P))$? (Hinweis: Betrachten Sie den Fall $t_1\,t_2 = 0$).

(2) (cf. [**CLO92**]) *Whitneys Schirmfläche* ist durch die Parametrisierung $x = uv, y = v, z = u^2$ gegeben.
   (a) (Über $\mathbb{R}$) Zeichnen Sie diese Fläche in einem Computeralgebrasystem.
   (b) (Über $\mathbb{C}$) Finden Sie die Gleichung der kleinsten Varietät, die Whitneys Schirmfläche enthält.

(3) Finden Sie eine (nichttriviale) Gleichung, die von allen Punkten im $\mathbb{R}^2$ des *Folium von Descartes* $\left(\frac{3t}{1+t^3}\,\frac{3t^2}{1+t^3}\right)$ erfüllt wird. Können Sie alle Lösungen der Gleichung durch die Parametrisierung erreichen?

Satz 14.33. *Sei k ein unendlicher Körper, seien $(r_1,\dots,r_n) \in k(t_1,\dots,t_m)$. Dann ist die durch $(r_1,\dots,r_n)$ parametrisierte Varietät V irreduzibel.*

Beweis: Sei S die Menge aller durch die Parametrisierung erreichbaren Punkte. Das Ideal $J := \{p \in k[x_1,\dots,x_n] \mid p(r_1,\dots,r_m) = 0\}$ ist prim. Wegen Lemma 14.31 gilt $J = \mathbb{I}(S)$. □

5. Die Dimension einer Varietät

DEFINITION 14.34. Sei k ein Körper, und sei $V \subseteq k^n$ eine Varietät. Sei $I := \mathbb{I}(V)$ das zu V gehörende Ideal. Die *Dimension von* V, $\dim(V)$, ist die maximale Anzahl von über k algebraisch unabhängigen Elementen in $\{x_1 + I, \ldots, x_n + I\}$.

LEMMA 14.35. *Sei k ein unendlicher Körper, sei $n \in \mathbb{N}$, und sei $V \subseteq k^n$ eine Varietät. Seien $i_1 < i_2 \ldots < i_r$ in $\{1, \ldots, n\}$. Dann sind äquivalent:*

(1) *Die Menge $P = \{(v_{i_1}, \ldots, v_{i_r}) \mid (v_1, \ldots, v_n) \in V\}$ ist Zariski-dicht in k^r.*
(2) *$(x_{i_1} + \mathbb{I}(V), \ldots, x_{i_r} + \mathbb{I}(V))$ ist algebraisch unabhängig.*

Beweis: (1)⇒(2): Nehmen wir an, $p \in k[t_1, \ldots, t_r] \setminus \{0\}$ ist so, dass $p(x_{i_1}, \ldots, x_{i_r}) \in \mathbb{I}(V)$. Sei $q(x_1, \ldots, x_n) := p(x_{i_1}, \ldots, x_{i_r})$. Dann liegt q in $\mathbb{I}(V)$, also liegen alle Elemente von P in $\mathbb{V}(p)$. Da k unendlich ist, gilt $\mathbb{V}(p) \neq k^r$. (2)⇒(1): Nehmen wir an, P ist nicht Zariski-dicht. Dann ist P in einer Varietät $\mathbb{V}(f)$ enthalten mit $f \in k[t_1, \ldots, t_r] \setminus \{0\}$. Sei nun $g := f(x_{i_1}, \ldots, x_{i_r})$. Dann gilt für alle $(v_1, \ldots, v_n) \in V$, dass $g(v_1, \ldots, v_n) = 0$. Somit gilt $g \in \mathbb{I}(V)$. Also sind $(x_{i_1} + \mathbb{I}(V), \ldots, x_{i_r} + \mathbb{I}(V))$ algebraisch abhängig. □

LEMMA 14.36. *Sei k ein Körper, sei R ein kommutativer Ring mit Eins mit $k \leq R$, und sei I ein Ideal von R mit $I \neq R$. Seien $Q_1, \ldots, Q_n$ Ideale von R mit $Q_1 \cap \cdots \cap Q_n = I$, und sei $P_i := \sqrt{Q_i}$ für $i \in \{1, \ldots, n\}$. Seien $r_1, \ldots, r_m \in R$. Dann sind äquivalent:*

(1) *$(r_1 + I, \ldots, r_m + I)$ ist algebraisch abhängig.*
(2) *Für alle $i \in \{1, \ldots, n\}$ ist $(r_1 + P_i, \ldots, r_m + P_i)$ algebraisch abhängig.*

Beweisskizze: Wenn $\overline{f_i}(r_1, \ldots, r_m) \in P_i$, so gibt es $n_i \in \mathbb{N}$ mit $\overline{f_i^{n_i}}(r_1, \ldots, r_m) \in Q_i$. Also belegt $f_1^{n_1} \cdots f_m^{n_m}$ die Abhängigkeit von $(r_1 + I, \ldots, r_m + I)$. □

SATZ 14.37. *Sei k ein Körper, sei R ein kommutativer Ring mit Eins mit $k \leq R$, und sei I ein Ideal von R mit $I \neq R$. Seien $x_1, \ldots, x_n \in R$ so, dass $R = k[\![x_1, \ldots, x_n]\!]$.*

Seien $s \in \mathbb{N}_0$ und $y_1, \ldots, y_s \in R$ so, dass $(y_1 + I, \ldots, y_s + I)$ algebraisch unabhängig über k, und R/I ganz über $k[\![y_1 + I, \ldots, y_s + I]\!]$ ist.

Seien $s_1, s_2, s_3 \in \mathbb{N}_0 \cup \{\infty\}$ definiert durch:

(1) *s_1 ist die maximale Anzahl von über k algebraisch unabhängigen Elementen in R/I.*
(2) *s_2 ist die maximale Anzahl von über k algebraisch unabhängigen Elementen in $\{x_1 + I, \ldots, x_n + I\}$ in R/I.*
(3) *s_3 ist die maximale Anzahl von über k algebraisch unabhängigen Elementen in $\{x_1 + \sqrt{I}, \ldots, x_n + \sqrt{I}\}$.*

Dann gilt $s = s_1 = s_2 = s_3$.

Beweis: Sei $\langle z_j + I \mid j \in J\rangle$ eine algebraisch unabhängige Folge in R/I. Seien $Q_1, \ldots, Q_l$ primär mit $I = Q_1 \cap \cdots \cap Q_l$, und sei $P_1 = \sqrt{Q_1}, \ldots, P_l := \sqrt{Q_l}$. Dann gibt es nach Lemma 14.36 ein $m \in \{1, \ldots, l\}$, sodass $\langle z_j + P_m \mid j \in J\rangle$ algebraisch unabhängig ist. Sei nun $H \subseteq \{1, \ldots, n\}$

maximal bezüglich $\subseteq$ mit der Eigenschaft, dass $\langle x_h + P_m \mid h \in H\rangle$ algebraisch unabhängig ist. Da P_m prim ist, ist der Ring R/P_m ein Integritätsbereich. Daher ergibt sich aus Lemma 8.23, dass $k[\![x_1 + P_m, \ldots, x_n + P_m]\!]$ algebraisch über $k[\![\{x_h + P_m \mid h \in H\}]\!]$ ist. Wegen Satz 8.22 ist $\langle x_h + P_m \mid h \in H\rangle$ eine maximale algebraisch unabhängige Folge in R/P_m, also eine Transzendenzbasis. Also gilt nach Korollar 8.25, dass $|J| \leq |H|$. Nun ist auch $\langle x_h + I \mid h \in H\rangle$ eine algebraisch unabhängige Folge in R/I.

Für jede $|J|$-elementige Folge algebraisch unabhängiger Elemente in R/I kann man also eine zumindest ebenso lange Folge algebraisch unabhängiger Elemente in $\{x_1+I, \ldots, x_n+I\}$ finden. Folglich gilt $s_1 \leq s_2$. Da $s_2 \leq s_1$ offensichtlich ist, gilt insgesamt $s_1 = s_2$.

Die Gleichheit $s_2 = s_3$ folgt daraus, dass eine Folge $\langle z_j + I \mid j \in J\rangle$ genau dann algebraisch unabhängig ist, wenn $\langle z_j + \sqrt{I} \mid j \in J\rangle$ algebraisch unabhängig ist.

Die Ungleichung $s \leq s_1$ ist offensichtlich. Sei nun $(z_1 + I, \ldots, z_{s_1} + I)$ eine algebraisch unabhängige Folge aus R/I. Es gibt also ein $m \in \{1, \ldots, l\}$, sodass $(z_1 + P_m, \ldots, z_{s_1} + P_m)$ eine algebraisch unabhängige Folge aus R/P_m ist. Da R/P_m ganz (und somit algebraisch) über $k[\![y_1 + P_m, \ldots, y_s + P_m]\!]$ ist, kann man mit Lemma 8.23 aus $\{y_1 + P_m, \ldots, y_s + P_m\}$ eine Transzendenzbasis von R/P_m mit höchstens s Elementen auswählen. Also gilt nach Korollar 8.25 auch $s_1 \leq s$. □

Wenn V irreduzibel ist, so ist das Ideal $\mathbb{I}(V)$ nach Satz 14.29 prim. Dann ist $k[x_1, \ldots, x_n]/\mathbb{I}(V)$ ein Integritätsbereich. Nach Satz 14.37 ist die Dimension von V genau der Transzendenzgrad dieses Integritätsbereiches über k.

Satz 14.38. *Sei k ein Körper, und seien $V_1, \ldots, V_m$ Untervarietäten von k^n, und sei $V := V_1 \cup \cdots \cup V_m$. Dann gilt* $\dim(V) = \max\{\dim(V_i) \mid i \in \{1, \ldots, m\}\}$.

Beweisskizze: Es gilt $\mathbb{I}(V) = \bigcap\{\mathbb{I}(V_i) \mid i \in \{1, \ldots, m\}\}$. Nach Lemma 14.36 gibt es für eine algebraisch unabhängige Menge der Form $\{x_h + \mathbb{I}(V) \mid h \in H\}$ einen Index $i \in \{1, \ldots, m\}$, sodass auch $\{x_h + \mathbb{I}(V_i) \mid h \in H\}$ algebraisch unabhängig ist. □

Satz 14.39. *Sei k ein Körper, und seien $V, W \subseteq k^n$ irreduzible Varietäten. Dann gilt:*

(1) $\dim(V) \leq n$.
(2) *Wenn $V \neq \varnothing$, $V \subseteq W$ und $V \neq W$, so gilt* $\dim(V) < \dim(W)$.

Beweis: Sei $R := k[x_1, \ldots, x_n]$, $P_1 := \mathbb{I}(W)$ und $P_2 := \mathbb{I}(V)$. Dann gilt $P_1 \subseteq P_2$ und $P_1 \neq P_2$. Wir bilden eine Noether-Normalisierung von R/P_1. Daraus erhalten wir $r \in \mathbb{N}_0$ und $y_1, \ldots, y_r \in R$, sodass P/P_1 ganz über $k[\![y_1 + P_1, \ldots, y_r + P_1]\!]$, und $(y_1 + P_1, \ldots, y_r + P_1)$ algebraisch unabhängig über k ist. Daher ist R/P_2 ganz über $k[\![y_1 + P_2, \ldots, y_r + P_2]\!]$. Wir zeigen nun, dass $(y_1 + P_2, \ldots, y_r + P_2)$ algebraisch abhängig ist. Wir wählen dazu ein $p \in P_2 \setminus P_1$. Wir wissen, dass im Ring R/P_1 das Element $p+P_1$ ganz über $k[\![y_1 + P_1, \ldots, y_r + P_1]\!]$ ist. Es gibt also $n \in \mathbb{N}$, $f_0, \ldots, f_{n-1} \in k[t_1, \ldots, t_r]$, sodass

$$(p + P_1)^n + \sum_{j=0}^{n-1} \overline{f_j}(y_1 + P_1, \ldots, y_r + P_1)\,(p + P_1)^j = 0 + P_1.$$

Es gilt also

$$p^n + \sum_{j=0}^{n-1} f_j(y_1, \ldots, y_r)\, p^j \in P_1.$$

Wenn alle $f_j(y_1, \ldots, y_r)$ in P_1 liegen, so liegt auch p^n in P_1, und, da P_1 prim ist, auch p, im Widerspruch zur Wahl von p. Sei also nun $j \in \{0, \ldots, n-1\}$ minimal mit $f_j(y_1, \ldots, y_r) \notin P_1$. Dann gilt

$$p^n + \sum_{i=j}^{n-1} f_i(y_1, \ldots, y_r)\, p^i \in P_1,$$

also

$$p^j \big(p^{n-j} + \sum_{i=j}^{n-1} f_i(y_1, \ldots, y_r)\, p^{i-j}\big) \in P_1.$$

Da $p \notin P_1$, gilt

$$p^{n-j} + \sum_{i=j}^{n-1} f_i(y_1, \ldots, y_r) p^{i-j} \in P_1.$$

Da $p \in P_2$, sind alle Summanden mit $i > j$ in P_2. Also gilt auch $f_j(y_1, \ldots, y_r) \in P_2$. Da $f_j(y_1, \ldots, y_r) \notin P_1$, gilt $f_j \neq 0$. Das Polynom f_j belegt also, dass $(y_1 + P_2, \ldots, y_r + P_2)$ algebraisch abhängig über k sind. Wegen Lemma 8.23 können wir aus $(y_1 + P_2, \ldots, y_r + P_2)$ eine Teilfolge als Transzendenzbasis von R/P_2 über k auswählen. Da $(y_1 + P_2, \ldots, y_r + P_2)$ algebraisch abhängig ist, enthält diese Folge höchstens $r-1$ Elemente. Also ist der Transzendenzgrad von R/P_2 über k echt kleiner als r. Somit gilt $\dim(W) < \dim(V)$. □

Satz 14.40. *Sei k ein Körper, und seien $m, n \in \mathbb{N}$. Sei $V \subseteq k^m$ eine Varietät, und seien $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$. Sei*

$$P := \{ \begin{pmatrix} \overline{f_1}(\boldsymbol{s}) \\ \vdots \\ \overline{f_n}(\boldsymbol{s}) \end{pmatrix} \mid \boldsymbol{s} \in V \}.$$

Dann gilt $\dim(\mathbb{V}(\mathbb{I}(P))) \leq \dim(V)$.

Satz 14.41. *Sei k ein unendlicher Körper, und sei $W \subseteq k^n$ ein linearer Unterraum von k^n. Sei $\dim_{linear}(W)$ die Dimension von W im Sinn der linearen Algebra, also die Anzahl der Elemente einer Basis von W. Dann gilt* $\dim(W) = \dim_{linear}(W)$.

Satz 14.42. *Sei k ein Körper, und sei $W \subseteq k^n$ eine Varietät. Dann sind äquivalent:*

(1) *W ist endlich.*
(2) $\dim(W) = 0$.
(3) *Der Vektorraum $k[x_1, \ldots, x_n]/\mathbb{I}(W)$ hat endliche Dimension über k.*

Übungsaufgaben 14.43

(1) Sei k ein Körper, $n \in \mathbb{N}$, und sei $V \subseteq k^n$ eine Varietät. Wir nehmen an, dass der Ring $k[x_1, \ldots, x_n]/\mathbb{I}(V)$ algebraisch über k ist. Zeigen Sie, dass V nur endlich viele Punkte enthält. *Hinweis:* Beispiele sind $n = 1, V = \mathbb{V}(x^2 - 5x + 6)$ oder $n = 2, V = \mathbb{V}(x^2 - 5x + 6, y^3 + 5y^3x^4 + x^8)$.

(2) Berechnen Sie jeweils die Dimension der folgenden Varietäten $\mathbb{V}(I)$ in $\mathbb{C}^3$, indem Sie eine Teilmenge von $\{x+I, y+I, z+I\}$ mit maximaler Kardinalität finden, die algebraisch unabhängig ist.
   (a) $I = \langle y^3 - z^2, -y^2 + xz, xy - z, x^2 - y\rangle$.
   (b) $I = \langle x^2 + y^2 + 1, x + y\rangle$.
   (c) $I = \langle xy^2 - x^2 z\rangle$.

SATZ 14.44. *Sei k ein algebraisch abgeschlossener Körper, und sei $W \subseteq k^n$ eine Varietät der Dimension s. Dann gibt es eine Basis $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ von k^n, sodass für alle $(\alpha_1, \ldots, \alpha_s) \in k^s$ die Menge $\{(\alpha_{s+1}, \ldots, \alpha_n) \mid \sum_{i=1}^n \alpha_i \boldsymbol{b}_i \in W\}$ endlich und nicht leer ist.*

Beweisskizze: Da k algebraisch abgeschlossen ist, ist k unendlich. Sei $I := \mathbb{I}(W)$, und sei A eine reguläre $n \times n$-Matrix über k, sodass für $y_i := \sum_{j=1}^n A(i,j)x_j$ gilt, dass $k[x_1, \ldots, x_n]/I$ ganz über $k[\![y_1 + I, \ldots, y_s + I]\!]$ ist. Mit A_s bezeichnen wir die $s \times n$-Matrix, die aus den ersten s Zeilen von A besteht.

Sei $(\alpha_1, \ldots, \alpha_s) \in k^s$ Wir betrachten nun das Ideal J von $k[\![y_1 + I, \ldots, y_s + I]\!]$, das von $\{y_1 - \alpha_1 + I, \ldots, y_s - \alpha_s + I\}$ erzeugt wird. Da der Ring $k[\![y_1 + I, \ldots, y_s + I]\!]$ isomorph zum Polynomring $k[z_1, \ldots, z_s]$ ist, gilt $J \neq k[\![y_1 + I, \ldots, y_s + I]\!]$. Folglich gilt nach Lemma 8.38 auch $1 + I \notin \langle y_1 - \alpha_1 + I, \ldots, y_s - \alpha_s + I\rangle_{k[\boldsymbol{x}]/I}$. Daher gilt auch

$$1 \notin \langle I \cup \{y_1 - \alpha_1, \ldots y_s - \alpha_s\}\rangle_{k[\boldsymbol{x}]}.$$

Somit gibt es wegen des Hilbertschen Nullstellensatzes einen Punkt $\boldsymbol{v} = (v_1, \ldots, v_n)$ in $\mathbb{V}(I)$ mit $A_s \cdot \boldsymbol{v} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$.

Wir zeigen nun, dass es nur endlich viele Punkte $\boldsymbol{v} \in \mathbb{V}(I)$ mit $A_s \cdot \boldsymbol{v} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$ gibt. Da für $t \geq s + 1$ gilt, dass

$$y_t^m + \sum_{i=0}^{m-1} f_i(y_1, \ldots, y_s) y_t^i \in I,$$

gibt es nur endlich viele Lösungen für y_t.

Somit hat das lineare Gleichungssystem $A_s \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$ stets endlich viele Lösungen in $\mathbb{I}(V)$. Der Anfangsteil dieser Lösung ist gegeben als ${A^{-1}}_s \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$. Die Spalten von A^{-1} bilden also die Basis B. □

Literaturverzeichnis

[AA20] E. Aichinger and F. Aichinger, *Dickson's Lemma, Higman's Theorem and Beyond: A survey of some basic results in order theory*, Expo. Math. **38** (2020), no. 4, 537–547.

[Aic24] E. Aichinger, *Strong Gröbner bases and linear algebra in multivariate polynomial rings over Euclidean domains*, 2024, arXiv.org.

[AL94] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[Alo99] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29, Recent trends in combinatorics (Mátraháza, 1995).

[Ax68] James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271.

[BK10] B. Buchberger and M. Kauers, *Gröbner basis*, Scholarpedia **5** (2010), no. 10, 7763.

[Buc65] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Universität Innsbruck, Mathematisches Institut (Dissertation), 1965 (German).

[Buc70] ———, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.

[Buc76] ———, *A theoretical basis for the reduction of polynomials to canonical forms*, ACM SIGSAM Bull. **10** (1976), no. 3, 19–29.

[Buc84] ———, *A critical-pair/completion algorithm for finitely generated ideals in rings*, Logic and machines: decision problems and complexity (Münster, 1983), Lecture Notes in Comput. Sci., vol. 171, Springer, Berlin, 1984, pp. 137–161. MR 775162

[BW93] T. Becker and V. Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993, A computational approach to commutative algebra, In cooperation with Heinz Kredel. MR 1213453

[Cla14] P. L. Clark, *The Combinatorial Nullstellensätze revisited*, Electron. J. Combin. **21** (2014), no. 4, Paper 4.15, 17.

[CLO92] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992, An introduction to computational algebraic geometry and commutative algebra.

[CNT19] C. J. Conidis, P. P. Nielsen, and V. Tombs, *Transfinitely valued Euclidean domains have arbitrary indecomposable order type*, Comm. Algebra **47** (2019), no. 3, 1105–1113. MR 3938544

[Dic13] L. E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, American Journal of Mathematics **35** (1913), no. 4, 413–422.

[Eis95] D. Eisenbud, *Commutative algebra*, Springer-Verlag, New York, 1995.

[Eng41] H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.

[Gar86] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, Cambridge, 1986.

[GP02] G.-M. Greuel and G. Pfister, *A* **singular** *introduction to commutative algebra*, Springer-Verlag, Berlin, 2002, With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh, and UNIX). MR 1930604

[Hal76] P. R. Halmos, *Naive Mengenlehre*, Vandenhoeck & Ruprecht, Göttingen, 1976, Vierte Auflage, Aus dem Englischen übersetzt von Manfred Armbrust und Fritz Ostermann, Moderne Mathematik in elementarer Darstellung, No. 6.

[KRK88] A. Kandri-Rody and D. Kapur, *Computing a Gröbner basis of a polynomial ideal over a Euclidean domain*, J. Symbolic Comput. **6** (1988), no. 1, 37–57. MR 961369

[Las10] M. Lasoń, *A generalization of combinatorial Nullstellensatz*, Electron. J. Combin. **17** (2010), no. 1, Note 32, 6. MR 2729390

[Lic12] D. Lichtblau, *Effective computation of strong Gröbner bases over Euclidean domains*, Illinois J. Math. **56** (2012), no. 1, 177–194. MR 3117024

[Lic13] ———, *Applications of strong Gröbner bases over Euclidean domains*, Int. J. Algebra **7** (2013), no. 5-8, 369–390. MR 3056463

[LP98] R. Lidl and G. F. Pilz, *Applied abstract algebra*, second ed., Springer-Verlag, New York, 1998.

[Mac01] D. Maclagan, *Antichains of monomial ideals are finite*, Proc. Amer. Math. Soc. **129** (2001), no. 6, 1609–1615 (electronic).

[Neš95] J. Nešetřil, *Ramsey theory*, Handbook of combinatorics, Vol. 2, Elsevier, Amsterdam, 1995, pp. 1331–1403.

[Pan89] L. Pan, *On the D-bases of polynomial ideals over principal ideal domains*, J. Symbolic Comput. **7** (1989), no. 1, 55–69. MR 984271

[Ram29] F. P. Ramsey, *On a problem of formal logic*, Proceedings London Mathematical Society (2) **30** (1929), 264–286.

[RU87] R. Remmert and P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser Verlag, Basel, 1987.

[Sha19] O. Shalit, *The perfect Nullstellensatz*, Internet discussions on Noncommutative Analysis (2019), https://noncommutativeanalysis.com/2018/04/22/the-perfect-nullstellensatz/.

[Smi14] J. R. Smith, *Introduction to algebraic geometry*, Five Dimensions Press, 2014 (English).

[Ter66] G. Terjanian, *Sur les corps finis*, C. R. Acad. Sci. Paris Sér. A-B **262** (1966), A167–A169.

[vdW67] B. L. van der Waerden, *Algebra. Teil II*, Unter Benutzung von Vorlesungen von E. Artin und E. Noether. Fünfte Auflage. Heidelberger Taschenbücher, Band 23, Springer-Verlag, Berlin, 1967.

[Wol24] Wolfram Research, Inc., *Mathematica, Version 14.0*, 2024, Champaign, IL.