Notizen zu den ersten 7 Kapiteln der Vorlesung

Kommutative Algebra und algebraische Geometrie

Entwurf

Sommersemester 2013

Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

Mithilfe
Georg Grasegger

Version Mai 2013

Adresse:
Assoz.-Prof. Dr. Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz
4040 Linz
e-mail: erhard.aichinger@jku.at
Version 6.5.2013

Inhaltsverzeichnis

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

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

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

Kommutative Ringe mit Eins

1. Kommutative Ringe mit Eins

Definition 2.1. Eine Algebra $\langle R, +, -, \cdot, 0, 1\rangle$ ist ein *kommutativer Ring mit Eins*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und $0, 1$ Elemente aus R sind, sodass für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$
(2) $x + (-x) = 0$
(3) $(x + y) + z = x + (y + z)$
(4) $x + y = y + x$
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6) $x \cdot y = y \cdot x$
(7) $x \cdot 1 = x$
(8) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Satz 2.2. *Sei $\langle R, +, -, \cdot, 0, 1\rangle$ ein kommutativer Ring mit 1, und seien $x, y \in R$. Dann gilt*

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

Beweis: (1): $-(-x) = -(-x) + 0 = 0 + (-(-x)) = (x + (-x)) + (-(-x)) = x+((-x)+(-(-x)) = x+0 = x$. (2): $x\cdot 0 = x\cdot 0+0 = x\cdot 0+(x\cdot 0+(-x\cdot 0)) = (x\cdot 0+x\cdot 0)+(-x\cdot 0) = x\cdot(0+0)+(-x\cdot 0) = x\cdot 0+(-x\cdot 0) = 0$. (3): Wir verwenden jetzt außer den bei der Definition von kommutativen Ringen verwendeten Gleichungen auch die Folgerungen, dass für alle $z \in R$ auch $(-z) + z = 0$ und $0 + z = z$ gilt. $-(x\cdot y) = -(x\cdot y)+x\cdot 0 = -(x\cdot y)+x\cdot(y+(-y)) = -(x\cdot y)+(x\cdot y+x\cdot(-y)) = (-(x\cdot y)+x\cdot y)+x\cdot(-y) = 0+x\cdot(-y) = x\cdot(-y)$. Mithilfe des Kommutativgesetzes folgt nun auch $(-x) \cdot y = -(x \cdot y)$. □

2. Ideale

Definition 2.3. Sei R ein kommutativer Ring mit Eins. Eine nichtleere Teilmenge I von R ist ein *Ideal* von R, wenn für alle $r \in R$ und $i, j \in I$ gilt, dass $r \cdot i$ und $i + j$ in I sind.

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

Definition 2.4. Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Dann ist das *von A erzeugte Ideal* $\langle A \rangle_R$ definiert durch

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

Satz 2.5. *Sei R ein kommutativer Ring mit Eins, und sei $A \subseteq R$. Dann gilt*

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

Beweis: 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 2.6

(1) (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) $R = \mathbb{Z}_{101}$, $S = \{[75]_{101}\}$.

(2) (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) $S = \{xy + x, 1 + y^2\}$.

(3) (Zornsches Lemma) Sei R ein kommutativer Ring mit Eins. Ein Ideal von R ist *maximal*, wenn es ein maximales Element in

$$\{I \mid I \text{ ist Ideal von } R \text{ und } I \neq R\}$$

ist. Zeigen Sie, dass jedes von R verschiedene Ideal in einem maximalen Ideal von R enthalten ist! Wo verwenden Sie, dass R ein Einselement hat?

Definition 2.7. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Dann ist I *endlich erzeugt*, wenn es eine endliche Menge $A \subseteq R$ gibt, sodass $I = \langle A \rangle$.
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 2.8. *Sei R ein kommutativer Ring mit Eins. Dann sind äquivalent:*

(1) $(\mathsf{Id}\ R, \subseteq)$ *erfüllt die* (ACC).
(2) *Jedes Ideal von R ist endlich erzeugt.*

Beweis: (1)⇒(2): 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 Folgen $\langle I_k \mid k \in \mathbb{N} \rangle$ eine streng monoton wachsende Folge von Idealen von R, im Widerspruch zur (ACC). (2)⇒(1): Sei $\langle I_k \mid k \in \mathbb{N} \rangle$ eine schwach 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 $I \subseteq I_N$. Folglich gilt für alle $k \in \mathbb{N}$ mit $k \geq N$: $I_k \subseteq I \subseteq I_N$. Wegen der Monotonie gilt $I_N \subseteq I_k$. Insgesamt gilt $I_k = I_N$; die Folge der Ideale bleibt also ab dem Index N konstant. Somit erfüllt $(\mathsf{Id}\ R, \subseteq)$ die (ACC). □

Definition 2.9. Sei R ein kommutativer Ring mit Eins. R heißt *noethersch*, wenn jedes Ideal von R endlich erzeugt ist.

Definition 2.10. Sei R ein kommutativer Ring mit Eins. Ein Ideal I von R ist *maximal*, wenn $I \neq R$ und wenn es kein Ideal J mit $I \subseteq J \subseteq R$, $I \neq J$, $J \neq R$ gibt.

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

Satz 2.11. *Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Dann gibt es ein maximales Ideal M von R mit $I \subseteq M$.*

Beweis: 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 $\mathcal{E}$. □

3. Faktorringe

Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Für jedes $r \in R$ definieren wir

$$r + I := \{r + i \mid i \in I\}.$$

Die Menge R/I ist definiert durch

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

Wir bezeichnen dabei $r + I$ als die *Restklasse von r modulo I*. Auf der Menge der Restklassen definieren wir nun eine Operation $\odot$ von $R/I \times R/I$ nach R/I folgendermaßen. Wir definieren

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

Diese Relation m ist eine Funktion von $R/I \times R/I$ nach R/I. 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.

Für $m(r + I, s + I)$ schreiben wir auch $(r + I) \odot (s + I)$.

4. Homomorphiesatz

...

KAPITEL 3

Teilbarkeit in kommutativen Ringen

1. Definitionen

Ein kommutativer Ring mit Eins R ist ein *Integritätsbereich*, wenn er zumindest zwei Elemente hat und für alle a, b mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ gilt.

Definition 3.1. Sei R ein kommutativer Ring mit Eins, und seien $a, b \in R$. Dann gilt $a|b$, wenn es ein $r \in R$ gibt, sodass $b = ra$.

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 $p|ab$ gilt: $p|a$ oder $p|b$.
- 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.*

Beweis: Sei p prim, $p \neq 0$, und seien $s, t \in R$ so, dass $p = st$. Dann gilt $p|st$. Da p prim ist, gilt $p|s$ oder $p|t$. Im Fall $p|s$ 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 $p|t$ erhalten wir analog, dass s invertierbar ist. □

Übungsaufgaben 3.4

(1) (Invertierbare Elemente) Sei R ein kommutativer Ring mit Eins. Zeigen Sie:
   (a) Das Produkt invertierbarer Elemente ist wieder invertierbar.

(b) Ein Element $r \in R$ ist genau dann invertierbar, wenn das von r erzeugte Ideal (r) gleich R ist.

(2) (Integritätsbereiche) Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. (*Hinweis:* Betrachten Sie für $r \neq 0$ die Abbildung $x \mapsto r \cdot x$.)

(3) (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.

(4) (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.

(5) (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. Faktorielle Integritätsbereiche

Definition 3.5. 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 $f_1, \ldots, f_s \in R$, sodass

$$r = f_1 \cdots f_s.$$

(2) Für alle $m, n \in \mathbb{N}$ und für alle irreduziblen $f_1, \ldots, f_m, g_1, \ldots, g_n \in R$ mit

$$f_1 \cdots f_m = g_1 \cdots g_n$$

gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$, sodass für alle $i \in \{1, \ldots, m\}$ gilt: $f_i \sim_R g_{\pi(i)}$.

Lemma 3.6. *Sei R ein faktorieller Integritätsbereich. Dann ist jedes irreduzible Element prim.*

Beweis: Sei f irreduzibel, und seien $a, b \in R$ so, dass $f|ab$. Zu zeigen ist, dass f mindestens eines der Elemente a oder b teilt. Wegen $f|ab$ gibt es $r \in R$, sodass

$$fr = ab.$$

Wenn $a = 0$, so gilt $f|a$; wenn $b = 0$, so gilt $f|b$. Wir nehmen nun an, dass $a \neq 0$ und $b \neq 0$. Wenn a invertierbar ist, dann gilt $fra^{-1} = b$, und somit $f|b$; wenn b invertierbar ist, gilt $f|a$. 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 $fr|a$, und somit $f|a$; wenn fr zu einem b_j assoziiert ist, dann gilt $f|b$.

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 $f|a$ oder $f|b$. □

3. Zerlegung in irreduzible Elemente

Definition 3.7. 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 3.8 (Zerlegung)**.** Sei R ein Integritätsbereich, und sei $I \subseteq R$ eine vollständige Auswahl irreduzibler Elemente von R. Sei $a \in \mathbb{R} \setminus \{0\}$. 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 $\prod_{i \in \emptyset}$ immer gleich 1.

Lemma 3.9. *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) $a|b$.

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

Beweis: 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 $r_1, \ldots, r_s \in R$ sodass $r = u_2 r_1 \cdots r_s$. Es gilt dann

$$u_1 u_2 r_1 \cdots r_s \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}. \tag{3.1}$$

Falls $\{i \in I \mid \beta(i) > 0 \text{ und } i \neq i_0\} = \emptyset$, so ist i_0 invertierbar, im Widerspruch dazu, dass i_0 irreduzibel ist. Wenn die rechte Seite von (3.1) 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. □

Lemma 3.10 (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*.*

Beweis: 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 3.8 erfüllt. Wenn f nicht invertierbar ist, so gibt es $s \in \mathbb{N}$ und irreduzible Elemente $g_1, \ldots, g_s \in R$, sodass

$$f = g_1 \cdots g_s.$$

Seien nun $i_1, \ldots, i_s \in I$ und $u_1, \ldots, u_s$ invertierbare Elemente von R, sodass für alle $j \in \{1, \ldots, s\}$ 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 $\{j \in \{1, \ldots, s\} \mid i_j = i\}$. 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 3.9 gilt dann $\alpha = \beta$. □

Satz 3.11. *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.*

Beweis: (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 $f_1 | g_1 \cdots g_n$. 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 Ring, 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 $a_n | a_{n-1} | \cdots | a_3 | a_2 | a_1$. Sei I eine vollständige Auswahl von irreduziblen Elementen, und sei α_k eine Zerlegung von a_k bezüglich I. Es gilt dann nach Lemma 3.9 für alle $i \in I$: $\alpha_k(i) \leq \alpha_1(i)$. Da es nur endlich viele β mit der Eigenschaft $\beta(i) \leq \alpha_1(i)$ für alle $i \in I$ gibt, gibt es ein $N \in \mathbb{N}$, sodass für $k \geq N$ gilt: $\alpha_k = \alpha_N$. Dann gilt aber auch $(a_k) = (a_N)$. Dass jedes irreduzible Element prim ist, folgt aus Lemma 3.6. □

Definition 3.12. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

Satz 3.13. *Jeder Hauptidealbereich ist faktoriell.*

Beweis: Sei R ein Hauptidealbereich. Da jedes Ideal von R endlich erzeugt ist, erfüllt R die ACC für Ideale, also insbesondere für Hauptideale. Zu zeigen bleibt, dass jedes irreduzible Element von R prim ist. Sei r ein irreduzibles Element von R, und sei P ein maximales Ideal von R mit $(r) \subseteq P \neq R$. Da R ein Hauptidealbereich ist, gibt es $p \in R$, sodass $P = (p)$. Da $r \in (p)$, gibt es ein $s \in R$, sodass $r = s \cdot p$. Da r irreduzibel ist und $(p) \neq R$, kann von s und p nur s invertierbar sein. Da s invertierbar ist, gilt $(p) = (r)$. Das Ideal (r) ist also ein maximales Ideal von R. Somit ist $R/(r)$ ein Körper, also auch ein Integritätsbereich, und (r) ist damit prim. □

4. Eine Anwendung auf die Zahlentheorie

Wir beweisen in dieser Sektion den folgenden Satz:

Satz 3.14. *Sei p eine Primzahl mit $p \equiv 1 \pmod 4$. Dann gibt es $a, b \in \mathbb{N}$, sodass $a^2 + b^2 = p$.*

Wir werden im Beweis den Ring der Gaußschen ganzen Zahlen, einen Unterring des Körpers der komplexen Zahlen, der durch

$$\mathbb{Z}[i] := \{a + b\,i \mid a, b \in \mathbb{Z}\},$$

definiert ist, verwenden.

Lemma 3.15. *Der Ring $\mathbb{Z}[i]$ ist ein Hauptidealring.*

Beweis: Für jedes Element $a + b\,i \in \mathbb{Z}[i]$ definieren wir seine Norm durch $N(a + b\,i) := a^2 + b^2$. Aus $N(z) = z\overline{z}$ sieht man leicht, dass $N(z_1 z_2) = N(z_1)N(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}[i]$ gilt. Sei nun I ein Ideal von $\mathbb{Z}[i]$ mit $I \neq \{0\}$. Wir wählen ein Element $c + d\,i$ aus $I \setminus \{0\}$, für das $N(c + d\,i)$ minimal ist. Nun zeigen wir

$$I = \{\lambda_1(c + d\,i) + \lambda_2(-d + c\,i) \mid \lambda_1, \lambda_2 \in \mathbb{Z}\}. \tag{4.1}$$

Die Inklusion $\supseteq$ folgt daraus, dass $(\lambda_1 + \lambda_2\,i)(c + d\,i)$ in I liegt. Um $\subseteq$ zu beweisen, wählen wir einen Punkt $a + b\,i \in I$. Es gibt einen Vektor in $\{\lambda_1 \binom{c}{d} + \lambda_2 \binom{-d}{c} \mid \lambda_1, \lambda_2 \in \mathbb{Z}\}$, dessen Abstand von $\binom{a}{b}$ höchstens $\frac{1}{\sqrt{2}}\sqrt{c^2 + d^2}$ ist. Sei $\binom{c'}{d'}$ ein solcher Vektor. Da $c' + d'\,i \in I$ liegt, liegt auch $(a - c') + (b - d')\,i$ in I. Es gilt $N((a - c') + (b - d')\,i) \leq \frac{1}{2}(c^2 + d^2)$. Da $c + d\,i$ minimale Norm in I hat, gilt $(a - c') + (b - d')\,i = 0$. Somit liegt $a + b\,i$ in der rechten Seite von (4.1). □

Wir beweisen nun Satz 3.14:

Beweis von Satz 3.14: Wir zeigen als erstes, dass es ein $x \in \mathbb{Z}$ gibt, sodass

$$x^2 \equiv -1 \pmod p. \tag{4.2}$$

Die multiplikative Gruppe des Körpers $\mathbb{Z}_p$ ist zyklisch. Sei $\alpha \in \mathbb{Z}$ so, dass $[\alpha]_p$ ein Erzeuger dieser Gruppe ist. Wir setzen $x := \alpha^{\frac{p-1}{4}}$ und erhalten aus dem Satz von Fermat $x^4 \equiv 1 \pmod p$. Es gilt also $p|(x^4 - 1)$, also $p|(x^2 + 1)(x - 1)(x + 1)$. Wenn $x \equiv 1 \pmod p$ oder $x \equiv -1 \pmod p$, so gilt $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod p$. Dann ist $[\alpha]_p$ kein Erzeuger von $\mathbb{Z}_p^*$. Folglich gilt $p|(x^2 + 1)$, und wir haben (4.2) bewiesen. (Eine andere Variante, die nicht verwendet, dass $\mathbb{Z}_p^*$ zyklisch ist, ist zu zeigen, dass $x := \frac{p-1}{2}!$ die Gleichung (4.2) erfüllt.) Nun wählen wir ein x, das die Gleichung (4.2) erfüllt. Im Ring $\mathbb{Z}[i]$ gilt natürlich ebenfalls $p|(1+x^2)$, also $p|(1+x\,i)\cdot(1-x\,i)$. Da jedes Vielfache von p im Ring $\mathbb{Z}[i]$ einen durch p teilbaren Realteil hat, gilt in $\mathbb{Z}[i]$ weder $p|(1 + x\,i)$ noch $p|(1 - x\,i)$. Im Ring $\mathbb{Z}[i]$ ist p also nicht prim. Da

$\mathbb{Z}[i]$ als Hauptidealbereich auch faktoriell ist, ist jedes irreduzible Element von $\mathbb{Z}[i]$ prim. Somit ist p in $\mathbb{Z}[i]$ nicht irreduzibel. Es gibt also $a, b, c, d \in \mathbb{Z}$, sodass $p = (a + b\,i)(c + d\,i)$, und $a + b\,i$ und $c + d\,i$ nicht invertierbar sind. Es 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. □

5. Teilbarkeit in Polynomringen

Definition 3.16. 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 $(i = 0, \ldots, n)$ teilt.

Lemma 3.17 (Gaußsches Lemma)**.** *Sei R ein kommutativer Ring mit Eins, und seien $f, g \in R[x]$ primitiv. Dann ist $f \cdot g$ ebenfalls primitiv.*

Beweis: 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. □

Lemma 3.18. *Sei R ein faktorieller Integritätsbereich, und sei $f \in R[x]$ mit $f \neq 0$. Dann gibt es $r \in R$, $g \in R[x]$, sodass g primitiv ist und $f = rg$.*

Beweis: Sei f_i ein Koeffizient von f, der $\neq 0$ ist. Sei $g \in R[x]$ so, dass das vom $i$ten Koeffizienten erzeugte Hauptideal (g_i) maximal in

$$\{(g_i') \mid g' \in R[x] \text{ und } \exists r \in R : rg' = f\}$$

ist, und sei $r \in R$ so, dass $rg = f$. Wenn g nicht primitiv ist, dann gibt es ein primes $p \in R$ und $h \in R[x]$, sodass $g = ph$. Für den $i$ten Koeffizienten gilt dann $g_i = ph_i$. Da $(g_i) \subseteq (h_i)$ und da $rp\,h = f$, gilt wegen der Maximalität von (g_i), dass $(g_i) = (h_i)$ ist. Also gibt es $s \in R$, sodass $s\,g_i = h_i$, und somit $sp\,h_i = h_i$. Da

$h_i \neq 0$, ist p damit invertierbar, im Widerspruch dazu, dass p prim ist. Also ist g primitiv. □

Lemma 3.19. *Sei R ein faktorieller Integritätsbereich, seien $g_1, g_2 \in R[x]$ primitive Polynome $\neq 0$ und seien $r_1, r_2 \in R$. Wenn $r_1 g_1 = r_2 g_2$, dann sind r_1 und r_2 in R assoziiert.*

Beweis: Wir fixieren $g_1, g_2 \in R[x] \setminus \{0\}$ und betrachten die Menge

$$A = \{(r_1, r_2) \in R \times R \mid r_1 g_1 = r_2 g_2 \text{ und } r_1 \not\sim_R r_2\}$$

Wenn diese Menge leer ist, dann ist der Satz bewiesen. Wenn die Menge nicht leer ist, dann wählen wir ein $(r_1, r_2) \in A$ so, dass (r_1) maximal in $\{(r_1') \mid (r_1', r_2') \in A\}$ ist. Da $g_1 \neq 0$, $g_2 \neq 0$ und R ein Integritätsbereich ist, gilt $r_1 \neq 0$.

Wenn r_1 invertierbar ist, dann ist $r_1 g_1$ primitiv. Wenn nun r_2 nicht invertierbar ist, dann gibt es ein primes $p \in R$, sodass $p | r_2$. Dann ist jeder Koeffizient von $r_2 g_2$ durch p teilbar, im Widerspruch dazu, dass $r_1 g_1$ primitiv ist. Also ist r_2 invertierbar und damit zu r_1 assoziiert.

Wenn r_1 nicht invertierbar ist, so gibt es ein primes $p \in R \setminus \{0\}$, sodass $p | r_1$. Wegen $r_1 g_1 = r_2 g_2$ teilt p alle Koeffizienten von $r_2 g_2$. Da p nicht alle Koeffizienten von g_2 teilt, muss es r_2 teilen. Es gibt also s_1, s_2, sodass $p s_1 = r_1$ und $p s_2 = r_2$. Es gilt $p s_1 \, g_1 = p s_2 \, g_2$. Wegen $p \neq 0$ gilt $s_1 g_1 = s_2 g_2$. Wenn $(r_1) = (s_1)$, so gibt es $t \in R$, sodass $t r_1 = s_1$, und somit $s_1 = t p s_1$. Dann ist p invertierbar, ein Widerspruch. Somit gilt $(r_1) \subseteq (s_1)$ und $(r_1) \neq (s_1)$. Wegen der Maximalität von (r_1) sind s_1 und s_2 assoziiert, es gibt also ein invertierbares $u \in R$ mit $u s_1 = s_2$. Dann gilt auch $u p s_1 = p s_2$, also $u r_1 = r_2$. Dann sind auch r_1 und r_2 in R assoziiert, im Widerspruch zur Annahme, dass (r_1, r_2) in A liegt.

Die Menge A ist also leer; damit ist der Satz bewiesen. □

Satz 3.20. *Sei R ein faktorieller Integritätsbereich, und seien $f, g \in R[x] \setminus \{0\}$. Seien $r, s \in R$ und seien f_1, g_1 primitive Polynome in $R[x]$ so, dass $f = r \, f_1$ und $g = s \, g_1$. Sei $Q(R)$ der Quotientenkörper von R. Dann sind äquivalent:*

(1) *$f | g$ in $R[x]$.*
(2) *$f_1 | g_1$ in $Q(R)[x]$ und $r | s$.*

Beweis: (1)⇒(2): Es gibt $h \in R[x]$, sodass $g = h \cdot f$. Wegen $g \neq 0$ gilt $s \neq 0$. Dann gilt $g_1 = s^{-1} \, g = s^{-1} \, (h \cdot f) = s^{-1} r \, (h \cdot f_1)$. Also gilt $f_1 | g_1$ in $Q(R)[x]$. Außerdem

gilt $h \cdot (r\, f_1) = s\, g_1$. Wir wählen $t \in R$ und $h_1 \in R[x]$ so, dass h_1 primitiv ist, und $t\, h_1 = h$. Es gilt dann $(t\, h_1) \cdot (r\, f_1) = s\, g_1$, also $rt\, (h_1 \cdot f_1) = s\, g_1$. Wegen des Gaußschen Lemmas ist $h_1 \cdot f_1$ primitiv. Somit sind wegen Lemma 3.19 die Elemente rt und s in R assoziiert. Damit gilt aber $r|s$.

(2)⇒(1): Wir wissen, dass es ein $h_1 \in Q(R)[x]$ gibt, sodass $f_1 \cdot h_1 = g_1$. Wir multiplizieren nun mit dem Produkt aller Nenner, die in den Koeffizienten von h_1 auftreten. Sei d dieses Produkt. Es gilt dann

$$f_1 \cdot (d\, h_1) = d\, g_1$$

und $d\, h_1 \in R[x]$. Sei nun $e \in R$ und sei h_2 ein primitives Polynom in $R[x]$ mit der Eigenschaft

$$e\, h_2 = d\, h_1.$$

Dann gilt

$$f_1 \cdot (e\, h_2) = d\, g_1,$$

also

$$e\, (f_1 \cdot h_2) = d\, g_1.$$

Wegen des Gaußschen Lemmas ist $f_1 \cdot h_2$ primitiv. Aus Lemma 3.19 erhalten wir, dass e und d assoziiert sind. Es gibt also ein invertierbares $u \in R$, sodass $e = du$. Somit gilt

$$du\, h_2 = d\, h_1.$$

Da $d \neq 0$, gilt $u\, h_2 = h_1$. Somit liegt h_1 in $R[x]$. Damit gilt $f_1|g_1$ auch in $R[x]$. Wegen $r|s$ gilt also auch $r\, f_1|s\, g_1$ in $R[x]$ und somit $f|g$. □

Korollar 3.21. *Sei R ein ein faktorieller Integritätsbereich, und seien $f, g \in R[x]$. Wir nehmen an, dass f primitiv ist und dass $f|g$ in $Q(R)[x]$ gilt. Dann gilt $f|g$ auch in $R[x]$.*

Beweis: Im Fall $g = 0$ gilt offensichtlich $f \cdot 0 = g$, also teilt f das Polynom g in $R[x]$. Wenn $g \neq 0$, so können wir Lemma 3.18 verwenden, um $g_1 \in R[x]$ und $r \in R$ zu erhalten, sodass $g = r\, g_1$. Wegen $1\, f|r\, g_1$ in $Q(R)[x]$ gilt nach Satz 3.20 $f|g_1$ in $R[x]$. Dann gilt natürlich auch $f|g$ in $R[x]$. □

Lemma 3.22. *Sei R ein faktorieller Integritätsbereich, sei $Q(R)$ sein Quotientenkörper, und sei f ein primitives Polynom in $R[x] \setminus \{0\}$. Dann sind äquivalent:*

(1) *f ist ein irreduzibles Element von $R[x]$.*
(2) *f ist ein irreduzibles Element von $Q(R)[x]$.*

Beweis: (1)⇒(2): Wir nehmen an, dass f ein irreduzibles Element von $R[x]$ ist. Seien nun $g, h \in Q(R)[x]$ so, dass

$$f = g \cdot h.$$

Wir multiplizieren mit allen Nennern von g und h und erhalten $c, d \in R$, sodass

$$cd\, f = (c\, g) \cdot (d\, h),$$

$c, d \neq 0$, und $c\, g \in R[x]$, $d\, h \in R[x]$. Wir wählen $c_1, d_1 \in R$ und primitive Polynome $g_1, h_1 \in R[x]$ so, dass $c_1\, g_1 = c\, g$ und $d_1\, h_1 = d\, h$. Es gilt dann

$$cd\, f = c_1 d_1\, (g_1 \cdot h_1).$$

Wegen des Gaußschen Lemmas ist $g_1 \cdot h_1$ primitiv. Also sind cd und $c_1 d_1$ wegen Lemma 3.19 assoziiert. Es gibt also ein invertierbares Element $u \in R$, sodass

$$cd\, f = ucd\, (g_1 \cdot h_1).$$

Da R ein Integritätsbereich ist, gilt $cd \neq 0$ und somit

$$f = u\, (g_1 \cdot h_1).$$

Somit gilt $g_1 | f$ und $h_1 | f$ in $R[x]$. Da f irreduzibel in $R[x]$ ist, ist entweder g_1 oder h_1 invertierbar in $R[x]$, also vom Grad 0. Wenn g_1 Grad 0 hat, ist g in $Q(R)[x]$ invertierbar; wenn h_1 Grad 0 hat, ist h in $Q(R)[x]$ invertierbar. Damit ist f also irreduzibel in $Q(R)[x]$.

(2)⇒(1): Sei f ein primitives Polynom in $R[x] \setminus \{0\}$. Wir nehmen an, dass f irreduzibel in $Q(R)[x]$ ist. Seien nun $g, h \in R[x]$ so, dass $f = g \cdot h$. Da f irreduzibel in $Q(R)[x]$ ist, ist entweder g oder h invertierbar in $Q(R)[x]$, also ein konstantes Polynom $\neq 0$. Wir nehmen an, g ist konstant. Wenn der konstante Koeffizient von g nicht invertierbar ist, dann ist er durch ein primes Element p von R teilbar. Dann ist aber auch jeder Koeffizient von $f = g \cdot h$ durch p teilbar, im Widerspruch dazu, dass f primitiv ist. Folglich ist g ein konstantes Polynom in $R[x]$ mit einem in R invertierbaren konstanten Koeffizienten. Somit ist g in $R[x]$ invertierbar. Im Fall, dass h konstant ist, erhalten wir, dass h in $R[x]$ invertierbar ist. Insgesamt erhalten wir, dass f irreduzibel in $R[x]$ ist. □

Satz 3.23. *Sei R ein faktorieller Integritätsbereich. Dann ist auch $R[x]$ faktoriell.*

Beweis: 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 3.20 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 Hauptidealring (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 $b_N | b_k$ in $Q(R)[x]$ und $r_N | r_k$ in R. Somit gilt $a_N | a_k$ 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 $f | a \cdot b$. Wir wollen nun zeigen, dass f in $R[x]$ entweder a oder b teilt.

Seien f_1, a_1, b_1 primitive Polynome in $R[x]$ und $r, s, t \in R$ so, dass $r\, f_1 = f$, $s\, a_1 = a$, $t\, b_1 = b$. Das Polynom f ist irreduzibel, also ist entweder r oder f_1 invertierbar in $R[x]$.

In dem Fall, dass f_1 invertierbar in $R[x]$ ist, ist ist f_1 ein Polynom vom Grad 0; sein konstanter und einziger Koeffizient ist ein invertierbares Element von R. Das Polynom f_1 ist also primitiv und es gilt nach Satz 3.20 $r | st$. Da f irreduzibel in $R[x]$ ist, ist r irreduzibel in R. R ist faktoriell, somit ist r prim, und es gilt $r | s$ oder $r | t$. Falls $r | s$, so gilt $r | sa_1$, und somit $r | a$ und damit $f | a$. Der Fall $r | t$ liefert analog $f | b$.

In dem Fall, dass f_1 nicht invertierbar in $R[x]$ ist, muss r invertierbar in $R[x]$, und damit in R, sein. Das Polynom f ist also primitiv, und folglich wegen Lemma 3.22 irreduzibel in $Q(R)[x]$. Da $f | a_1 b_1$ in $Q(R)[x]$ und f in $Q(R)[x]$ prim ist, gilt $f | a_1$ oder $f | b_1$ in $Q(R)[x]$. Wenn $f | a_1$ in $Q(R)[x]$, gilt nach Satz 3.20 auch $f | a_1$ in $R[x]$, und somit auch $f | a$. Wenn $f | b_1$ in $Q(R)[x]$, erhalten wir $f | b$.

Somit ist f prim. Nach Satz 3.11 ist $R[x]$ damit faktoriell. □

Korollar 3.24. *Sei R ein faktorieller Integritätsbereich und $k \in \mathbb{N}$. Dann ist $R[x_1, \ldots, x_k]$ faktoriell.*

6. Größter gemeinsamer Teiler

Definition 3.25. Sei R ein Integritätsbereich, sei $n \in \mathbb{N}$, und seien $f_1, \ldots, f_n \in R$. Dann ist $d \in R$ ein *größter gemeinsamer Teiler* von $f_1, \ldots, f_n$, wenn

(1) $d|f_1, \ldots, d|f_n$.
(2) Für alle $d' \in R$ mit $d'|f_1, \ldots, d'|f_n$ gilt $d'|d$.

Satz 3.26. *Sei R ein faktorieller Ring, sei $n \in \mathbb{N}$, und seien $f_1, \ldots, f_n \in R$. Dann gibt es einen größten gemeinsamen Teiler von $f_1, \ldots, f_n$.*

Beweisskizze: Wir erhalten aus den Zerlegungen von $f_1, \ldots, f_n$ und Lemma 3.9 eine Zerlegung von d. □

Lemma 3.27. *Sei R ein faktorieller Integritätsbereich, und seien $f_1, \ldots, f_n \in R$, und sei $t \in R$, $t \neq 0$. Wenn d ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$ in R ist, so ist td ein größter gemeinsamer Teiler von $tf_1, \ldots, tf_n$ in R.*

Beweis: Sei h ein größter gemeinsamer Teiler von $tf_1, \ldots, tf_n$ in R. Da t alle tf_i teilt, gilt $t|h$. Somit gibt es ein $g \in R$, sodass $h = tg$. Es gilt nun $tg|tf_1$. Da R ein Integritätsbereich ist, gilt auch $g|f_1$. Ebenso teilt g alle anderen f_i. Das Element g ist also ein gemeinsamer Teiler von $f_1, \ldots, f_n$. Folglich gilt $g|d$. Also gilt $tg|td$; das bedeutet $h|td$.

Da d alle f_i teilt, teilt td alle tf_i. Somit teilt td den größten gemeinsamen Teiler von $tf_1, \ldots, tf_n$; das bedeutet $td|h$.

Wegen $h|td$ und $td|h$ sind h und td also assoziiert. Somit ist mit h auch td ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$. □

Satz 3.28. *Sei R ein faktorieller Integritätsbereich, und seien $f_1, \ldots, f_n \in R[x] \setminus \{0\}$. Seien $r_1, \ldots, r_n \in R$ und $g_1, \ldots, g_n$ primitive Elemente in $R[x]$ so, dass $f_1 = r_1 g_1, \ldots, f_n = r_n g_n$.*

Es sei d_1 ein größter gemeinsamer Teiler von $r_1, \ldots, r_n$ in R, und d_2 ein größter gemeinsamer Teiler von $g_1, \ldots, g_n$ 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 $R[x]$.

Beweis: Wir zeigen zunächst, dass $d_1 d_2$ alle f_i teilt. Sei $i \in \{1, \ldots, n\}$. Da $d_1|r_i$ in R und $d_2|g_i$ in $Q(R)[x]$, liefert Satz 3.20 auch $d_1 d_2|f_i$ in $R[x]$.

Sei nun $d' \in R[x]$ so, dass d' in $R[x]$ alle f_i teilt. Wir wählen $d'_1 \in R$ und ein primitives $d'_2 \in R[x]$ so, dass $d' = d'_1 d'_2$. Dann gilt wegen Satz 3.20, dass d'_1 alle r_i in R teilt, und dass d'_2 alle g_i in $Q(R)[x]$ teilt. Da d_1 ein größter gemeinsamer

Teiler in R ist, gilt $d_1'|d_1$ in R. Da d_2 ein größter gemeinsamer Teiler in $Q(R)[x]$ ist, gilt $d_2'|d_2$ in $Q(R)[x]$. Wir verwenden wieder Satz 3.20 und erhalten $d_2'|d_2$ in $R[x]$. Somit gilt $d_1'd_2'|d_1d_2$ in $R[x]$, und somit $d'|d$ in $R[x]$. □

Satz 3.29. *Sei R ein faktorieller Integritätsbereich, und sei $f = \sum_{i=0}^{n} f_i x^i$ ein Element von $R[x] \setminus \{0\}$. Sei d ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$, und sei $g \in R[x]$ so, dass $d\,g = f$. Dann ist g primitiv.*

Beweis: Sei p ein primes Element von R, das alle Koeffizienten $g_1, \ldots, g_n$ von g teilt. Dann teilt pd alle Koeffizienten von f. Somit teilt pd den größten gemeinsamen Teiler dieser Koeffizienten; es gilt also $pd|d$. Da $d \neq 0$ gilt dann $p|1$. Dann ist p invertierbar, im Widerspruch dazu, dass p prim ist.

Somit teilt kein primes P alle Koeffizienten von g. Somit ist g primitiv. □

Satz 3.30. *Sei R ein faktorieller Integritätsbereich, und seien $f, g \in R[x] \setminus \{0\}$. Sei d ein größter gemeinsamer Teiler von f und g in $R[x]$. Dann ist d auch ein größter gemeinsamer Teiler von f und g in $Q(R)[x]$.*

Beweis: Das Polynom d ist offensichtlich ein gemeinsamer Teiler von f und g in $Q(R)[x]$. Um zu beweisen, dass d ein größter gemeinsamer Teiler von f und g in $Q(R)[x]$ ist, wählen wir ein $t \in Q(R)[x]$ mit $t|f$ und $t|g$ in $Q(R)[x]$. Wir können nun ein primitives $t_1 \in R[x]$ und $a, b \in R \setminus \{0\}$ finden, sodass $t = \frac{a}{b}t_1$. Es gilt $t_1|f$ und $t_1|g$ in $Q(R)[x]$. Wegen des Korollars 3.21 gilt also auch $t_1|f$ und $t_1|g$ in $R[x]$. Folglich gilt $t_1|d$ in $R[x]$. Also gilt $t_1|d$ in $Q(R)[x]$, und somit $t|d$ in $Q(R)[x]$ Somit ist d ein Vielfaches jedes gemeinsamen Teilers von f und g in $Q(R)[x]$. Also ist d ein größter gemeinsamer Teiler von f und g in $Q(R)[x]$. □

Übungsaufgaben 3.31

(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 4

Multiplikative Idealtheorie in kommutativen Ringen

1. Noethersche Ringe

Definition 4.1. Ein kommutativer Ring mit Eins R ist *noethersch*, wenn die geordnete Menge $\langle \mathsf{Id}\ R, \subseteq \rangle$ die ACC erfüllt.

Lemma 4.2. *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 2.8 liefert, dass R genau dann noethersch ist, wenn jedes Ideal von R endlich erzeugt ist. □

Satz 4.3 (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 $j x^n + q \in I$. 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.

$$\text{Für alle } n \in \mathbb{N}_0 \text{ liegen alle } g \in I \text{ mit } \deg(g) \leq n \text{ in } \langle F \rangle_R.$$

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 4.4. *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 4.5. 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 4.6. *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 4.7. 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 4.8. 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 4.9. 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 4.10. 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 4.11

(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 4.12. *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 4.13. 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 4.14. 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 4.15. 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 4.16. *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 4.17. *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 4.18. 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 4.19. *Sei R ein noetherscher kommutativer Ring mit Eins. Dann ist jedes Ideal von R Durchschnitt endlich vieler schnitt-irreduzibler Ideale.*

Satz 4.20. *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 $n \in \mathbb{N}$

$$(I : b^n)_R \subseteq (I : b^{n+1})_R. \tag{4.1}$$

Um (4.1) 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 (4.1). 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

$$I = (I + A) \cap (I + B). \tag{4.2}$$

Die Inklusion $\subseteq$ von (4.2) 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 (4.2).

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 (4.2) zeigt also, dass I nicht schnitt-irreduzibel ist. □

Übungsaufgaben 4.21

(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) $\langle x^2 y, xy^3\rangle$ 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) $A = \langle x^4, x^2 y, y^3\rangle$.
   (b) $B = \langle x^4, y^3\rangle$.
   (c) $C = \langle x^2 y\rangle$.

Satz 4.22. *Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, seien $Q_1, \ldots, Q_n$ 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 4.23. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, und seien $Q_1, \ldots, Q_n$ und I Ideale von R mit $I \neq R$. Die Folge $(Q_1, \ldots, Q_n)$ 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 $i \in \{1, \ldots, n\}$ 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 $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt $\sqrt{Q_i} \neq \sqrt{Q_j}$.

Satz 4.24 (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 4.25. *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 4.26. *Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, sei I ein primäres Ideal, und sei $(Q_1, \ldots, Q_n)$ eine Darstellung von I durch größte Primärkomponenten. Dann gilt $n = 1$.*

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

$$\sqrt{Q_j} \not\subseteq \sqrt{Q_i}. \tag{5.1}$$

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 (5.1). Es gibt also $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in R$, sodass für alle $j \in \{1, \ldots, n\} \setminus \{i\}$ 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

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

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 4.27. *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 $(Q_1, \ldots, Q_m)$ und $(K_1, \ldots, K_n)$ Folgen von Idealen von R. Wir nehmen an, dass $(Q_1, \ldots, Q_m)$ und $(K_1, \ldots, K_n)$ Darstellungen von I durch größte Primärkomponenten sind, und dass $\sqrt{Q_1}$ minimal in*

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

ist. Dann gilt $m = n$, und es gibt es eine bijektive Abbildung $\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$, sodass $Q_1 = K_{\pi(1)}$ und für alle $i \in \{1, \ldots, m\}$ 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 4.26 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 4.26 $m = 1$, 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

$$\{\sqrt{Q_i} \mid i \in \{1, \ldots, m\}\} \cup \{\sqrt{K_j} \mid j \in \{1, \ldots, n\}\}. \tag{5.2}$$

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 (5.2) 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 $(Q_1, \ldots, Q_n)$ eine Zerlegung in größte Primärkomponenten ist.

Wir zeigen als erstes, dass P in beiden der in (5.2) vereinigten Mengen enthalten ist. Nehmen wir dazu an, dass $k \in \{1, \ldots, m\}$ so ist, dass $P = \sqrt{Q_k}$ und P nicht

in $\{\sqrt{K_j} \mid j \in \{1,\dots,n\}\}$ liegt. Es gilt nun:

(5.3) Für alle $i \in \{1,\dots,m\}$ mit $i \neq k$ gilt $Q_k \not\subseteq \sqrt{Q_i}$.

Um (5.3) 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 (5.3). Ebenso gilt

(5.4) Für alle $j \in \{1,\dots,n\}$ gilt $Q_k \not\subseteq \sqrt{K_j}$.

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 (5.4). 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 4.25 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

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

Wir berechnen $(I : Q_k \cdot K_l)$. Nach Proposition 4.25 erhalten wir

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

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 $\pi' : \{1, \ldots, m\} \setminus \{k\} \to \{1, \ldots, n\} \setminus \{l\}$, sodass $Q_1 = K_{\pi'(1)}$ und $\sqrt{Q_i} = \sqrt{K_{\pi'(i)}}$ für alle $i \in \{1, \ldots, m\} \setminus \{k\}$. Daher leistet $\pi := \pi' \cup \{(k, l)\}$ das Gewünschte. □

Satz 4.28 (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:*

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

Satz 4.29 (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 4.27 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 5

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 5.1. 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 5.2. *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)*

$$\begin{aligned}&\det\left((a_1, \ldots, a_{i-1}, v + w, a_{i+1}, \ldots, a_n)\right)\\ &\quad = \det\left((a_1, \ldots, a_{i-1}, v, a_{i+1}, \ldots, a_n)\right) + \det\left((a_1, \ldots, a_{i-1}, w, a_{i+1}, \ldots, a_n)\right)\end{aligned}$$

(2) *(R-Homogenität)*

$$\begin{aligned}&\det\left((a_1, \ldots, a_{i-1}, r\,v, a_{i+1}, \ldots, a_n)\right)\\ &\qquad\qquad = r \cdot \det\left((a_1, \ldots, a_{i-1}, v, a_{i+1}, \ldots, a_n)\right).\end{aligned}$$

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

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

Beweisskizze: Da in jedem Summanden in der Definition der Determinante genau einer der Faktoren $A_{1,i}, A_{2,i}, \dots, A_{n,i}$ vorkommt (nämlich $A_{\pi^{-1}(i),i}$), gelten (1) und (2). Für den Beweis von (3) sei A die Matrix $(a_1, \dots, a_n)$. Da die i-te und die j-te Spalte der Matrix gleich sind, gilt für alle $k \in \{1, \dots, n\}$ 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 5.3. *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 $r\,\mathbf{I}_n$ schreiben.

Beweis von Satz 5.3: 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 $a_1, \ldots, a_n$ seien die Spaltenvektoren der Matrix A; es gilt also $A = (a_1, \ldots, a_n)$. Sei nun B die Matrix, die durch

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

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

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

Somit erhalten wir aus dem Satz 5.2

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

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 5.2 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 5.4. 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 5.5. 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 5.6. 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 5.7. *Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Wenn x ganz über B ist, so gibt es $n \in \mathbb{N}$ und $b_0, \ldots, b_{n-1} \in B$ mit $b_0 = 1$, sodass*

$$A[\![x]\!] = A \cdot 1 + A \cdot b_1 + \cdots + A \cdot b_{n-1}. \tag{2.1}$$

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 (2.1) 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 (2.1) 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 (2.1). $\square$

Satz 5.8. *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

$$xb_i = a_{i,0}b_0 + \cdots + a_{i,n-1}b_{n-1}. \tag{2.2}$$

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 (2.2) 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

$$\left(\begin{pmatrix} x & 0 & 0 & \ldots & 0 \\ 0 & x & 0 & \ldots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & x \end{pmatrix} - M \right) \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = 0. \tag{2.3}$$

Aus Satz 5.3 erhalten wir eine $n \times n$-Matrix L mit Einträgen aus B, sodass

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

Durch Multiplikation der Gleichung (2.3) von links mit L erhalten wir

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

Da $b_0 = 1$, folgt aus dieser Gleichung

$$\det(x\,\mathbf{I}_n - M) = 0. \tag{2.4}$$

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 (2.4) gilt $\overline{p}(x) = 0$. Das Polynom p bezeugt also, dass x ganz über A ist. □

Satz 5.9. *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 5.7 $n \in \mathbb{N}$ 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 5.8 ganz über A. □

Allgemeiner gilt:

Satz 5.10. *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 $c_0, \ldots, c_{n-1} \in B$ 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 5.8 ganz über A. □

Übungsaufgaben 5.11

(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 5.12. *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

$$x^n + \sum_{i=0}^{n-1} b_i x^i = 0. \tag{2.5}$$

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 5.10 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:

$$x \text{ ist ganz über } A[\![b_i, b_{i+1}, \ldots, b_{n-1}]\!]. \tag{2.6}$$

Für $i = 0$ ergibt sich das aus der Gleichung 2.5. 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 5.10 auch ganz über $A[\![b_{i+1}, \ldots, b_{n-1}]\!]$. Somit gilt (2.6) für alle $i \in \{0, \ldots, n\}$. Für $i := n$ erhalten wir, dass x ganz über A ist. □

3. Algebraische Erweiterungen

Definition 5.13. 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 5.14

(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 5.15. *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 5.16. *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 5.15 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 5.17. *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

$$\sum_{i=0}^{n} \frac{p_i}{p_n}\, x^i = 0. \tag{3.1}$$

Es gilt $Q(A) \leq Q(B)$. Nach (3.1) ist $\frac{x}{1}$ ganz über $Q(A)$. Wegen Satz 5.9 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 5.18. *Seien A, C Integritätsbereiche mit $A \leq C$. Dann ist die Menge $B := \{b \in C \mid b \text{ ist algebraisch über } A\}$ 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 5.17 auch $A[\![x_1]\!][\![x_2]\!] = A[\![x_1, x_2]\!]$ algebraisch über $A[\![x_1]\!]$. Ebenso ist nach Satz 5.17 der Ring $A[\![x_1]\!]$ algebraisch über A. Nach Proposition 5.16 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 5.19. 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 5.20. 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 5.21. *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 5.22. *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.

(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 5.23. *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 5.22 ist jedes $x \in X$ algebraisch über $A[\![U]\!]$. Die über $A[\![U]\!]$ algebraischen Elemente von B bilden nach Lemma 5.18 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 5.24. *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 5.22 algebraisch über $A[\![x_1, \ldots, x_m]\!]$.

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

$$B \text{ algebraisch über } A[\![w_1, \ldots, w_{i-1}, x_{\pi(i)}, \ldots, x_{\pi(m)}]\!] \tag{3.2}$$

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 (3.2) ist w_i algebraisch über $A[\![w_1, \ldots, w_{i-1}, x_{\pi(i)}, \ldots, x_{\pi(m)}]\!]$. Nach Satz 5.22 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

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

Daher ist nach Satz 5.22 $x_{\pi(j)}$ 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 (3.2) 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 5.17 der Integritätsbereich $C[\![x_{\sigma(i)}]\!]$ algebraisch über C ist, folgt nach Proposition 5.16, dass B algebraisch über C ist. Somit leistet $\sigma|_{\{i+1,\ldots,m\}}$ das Gewünschte. □

Korollar 5.25. *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 5.24) 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 5.22 ist $(w_1, \ldots, w_m, w_{m+1})$ dann algebraisch abhängig. □

Definition 5.26. 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 5.27. *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 5.28. *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 $k[\![\overline{f_2}(\boldsymbol{x}), \ldots, \overline{f_n}(\boldsymbol{x}), x_1]\!] = B$.)

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

$$\begin{aligned} q' &:= p(t_1, t_2 + a_2 t_1, \ldots, t_n + a_n t_1) \\ &= \sum_{(i_1, \ldots, i_n) \in I} c(i_1, \ldots, i_n) t_1^{i_1} (t_2 + a_2 t_1)^{i_2} \cdots (t_n + a_n t_1)^{i_n}. \end{aligned}$$

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 5.27 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

$$\overline{q}(x_1, x_2 - \alpha_2 x_1, \dots, x_n - \alpha_n x_1) = 0.$$

Das bedeutet

$$b_N x_1^N + \sum_{i=0}^{N-1} \overline{b_i}(x_2 - \alpha_2 x_1, \dots, x_n - \alpha_n x_1)x_1^i = 0.$$

Also ist x_1 ganz über $k[\![x_2 - \alpha_2 x_1, \dots, x_n - \alpha_n x_1]\!]$. Somit leisten $f_j := x_j - \alpha_j x_1$ und $g_1 := t_1$, $g_j := x_j + \alpha_j x_1$ 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 5.29 (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 5.28 $f_1,\dots,f_{n-1} \in k[t_1,\dots,t_n]$, 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 $g_1, \ldots, g_r \in k[t_1, \ldots, t_{n-1}]$, sodass $k[\![\overline{f_1}(\boldsymbol{x}), \ldots, \overline{f_{n-1}}(\boldsymbol{x})]\!]$ ganz über

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

ist

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

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

Da x_n ganz über

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

ist, gilt:

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

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

Übungsaufgaben 5.30

(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 $y_1, \ldots, y_r \in R$, sodass $(y_1, \ldots, y_r)$ algebraisch unabhängig ist und R ganz über $\mathbb{Q}[\![y_1, \ldots, y_r]\!]$ 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 5.31 (Hilberts Nullstellensatz – Schwache Form)**.** *Sei k ein Körper, und sei I ein Ideal von $k[t_1, \ldots, t_n]$ 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 $k[t_1, \ldots, t_n]$ mit $I \subseteq M \neq k[\boldsymbol{t}]$, und sei $K := k[\boldsymbol{t}]/M$. K ist ein Körper, und $(x_1, \ldots, x_n) := (t_1 + M, \ldots, t_n + M)$ ist eine Nullstelle aller Polynome in I. Es bleibt zu zeigen, dass K algebraisch über k ist: Seien dazu $r \in \{0, \ldots, n\}$ und $y_1, \ldots, y_r \in K$ so, dass K ganz über $k[\![y_1, \ldots, y_r]\!]$ ist, und $(y_1, \ldots, y_r)$ 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 $k[\![y_1, \ldots, y_r]\!]$ ist, gibt es $m \in \mathbb{N}$ und $f_1, \ldots, f_{m-1} \in k[t_1, \ldots, t_r]$, sodass

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

Durch Multiplikation mit y_1^m erhalten wir

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

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 5.32 (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 5.31 eine Nullstelle $(\boldsymbol{x}, \boldsymbol{y}, z)$ in k^{s+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 $f_1(\boldsymbol{x}) = \ldots = f_s(\boldsymbol{x}) = 0$, $h_1(\boldsymbol{x}) \neq 0$, …, $h_r(\boldsymbol{x}) \neq 0$, 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 5.33 (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 5.34 (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 5.33) 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 5.35 (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 5.36. *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 5.37. *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 5.38. *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 5.7 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 $i_1, \ldots, i_m \in I$ gibt, sodass

$$y = \sum_{l=1}^{m} i_l x_l. \tag{6.1}$$

Wegen $y \in \langle I \rangle_B$ gibt es $r \in \mathbb{N}$, $b_1, \ldots, b_r \in B$ und $j_1, \ldots, j_r \in I$, sodass $y = \sum_{k=1}^{r} b_k j_k$. Da $b_k \in \sum_{l=1}^{m} A \cdot x_l$, gibt es $a_{k,1}, \ldots, a_{k,m} \in A$, 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 (6.1).

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 modulo I betrachten, so gilt $1 \equiv 0 \pmod{I}$. Also gilt $1 \in I$. □

Lemma 5.39. *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 5.29 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 5.38 (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 5.40. *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 5.22 jedes x_i algebraisch über $\mathbb{Z}[\![Y]\!]$. Also gibt es wegen Lemma 5.36 $q_1, \dots, q_n \in \mathbb{Z}[\![Y]\!] \setminus \{0\}$, 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 $q' \in \mathbb{Z}[t_1, \ldots, t_r]$ mit $q = q'(y_1, \ldots, y_r)$. 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 $F := \mathbb{Z}[\![Y]\!][\![q_1 x_1, \ldots, q_n x_n]\!]$. 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 5.37 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 5.39 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 5.41.

(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 5.39 oder Lemma 5.40, 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 5.35: 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

$$(x_i - y_i)^{m_i} = \sum_{j=1}^{n} p_j(\boldsymbol{x}, \boldsymbol{y}) \cdot (f_j(\boldsymbol{x}) - f_j(\boldsymbol{y})). \tag{6.2}$$

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

$$1 = \sum_{j=1}^{n} q_j(\boldsymbol{t}) \cdot (f_j(t_1, \ldots, t_n) - a_j). \tag{6.3}$$

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 5.41 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 (6.3) gibt es kein $\boldsymbol{z} \in (B/J)^n$, sodass $F_1(\boldsymbol{z}) = (a_1 + J, \ldots, a_n + J)$. Wegen (6.2) 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 5.42. *Sei K ein Körper, und seien $p, q \in K[t]$ mit $\mathrm{ggT}_{K[t]}(p, q) = 1$. Sei $K(\frac{p}{q})$ 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 $K(\frac{p}{q})$, 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 $f \in K(\frac{p}{q})[x]$ 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 $K(\frac{p}{q})[x]$ ist. Der Körper $K(\frac{p}{q})$ 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 3.20 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 5.43 (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 $K(t)$.*

Beweis: 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 $K(u) = L$.

KAPITEL 6

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 6.1 (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 $\mathbb{N}$ mit t Farben. Für jedes $a \in \mathbb{N}$ 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 $Y_{j+1} \cup \{x_i\}$. Ebenso ist B eine Teilmenge von $Y_{j+1} \cup \{x_i\}$. Wegen der Konstruktion von Y_{j+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 $\mathrm{ind}(C) = c_1 = \mathrm{ind}(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$, 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 6.2. *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 6.1, 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 6.3 (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 6.2 kann $({\mathbb{N}_0}^m, \sqsubseteq)$ keine unendliche Antikette enthalten. □

Übungsaufgaben 6.4

(1) (Satz von Ramsey) Zeigen Sie, dass jede reelle Zahlenfolge eine streng monoton fallende, eine streng monoton steigende oder eine konstante (unendliche) Teilfolge enthält.

(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.

Definition 6.5. 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 6.6. *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 6.3) 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 6.7. *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 $U \subseteq U_j$. □

2. Multivariate Polynomdivision

Definition 6.8. 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 6.9. *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 6.2 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 6.10. 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 6.11. 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

$$\textsc{Deg}(f) := (-1, \ldots, -1), \text{ wenn } f = 0,$$

und

$$\textsc{Deg}(f) := \max\nolimits_{\leq}\{\alpha \in {\mathbb{N}_0}^n \mid c_\alpha \neq 0\}, \text{ wenn } f \neq 0.$$

Definition 6.12. 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

$$\begin{aligned} \textsc{Lm}(f) &:= \boldsymbol{x}^\gamma, \\ \textsc{Lc}(f) &:= c_\gamma, \\ \textsc{Lt}(f) &:= c_\gamma \boldsymbol{x}^\gamma. \end{aligned}$$

Definition 6.13. 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 $\textsc{Lm}(f_i)$ ist.
(3) Für alle $i \in \{1, \ldots, s\}$ gilt $\textsc{Deg}(a_i f_i) \leq \textsc{Deg}(f)$.

Das Polynom r heißt auch *Rest* der Darstellung.

Übungsaufgaben 6.14

(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.

(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.

(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 $f = a_1f_1 + a_2f_2 + r$ 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.

(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 $\text{LT}(f_1)$ teilbar ist. Zeigen Sie $r = s$!

Satz 6.15. *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

$$f = \textsc{Lt}(f) + g.$$

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* $\textsc{Lm}(f_i) | \textsc{Lm}(f)$*:* Dann gilt

$$\textsc{Deg}(f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i) < \textsc{Deg}(f).$$

Wegen der Minimalität von f gibt es $b_1, \ldots, b_s \in k[\boldsymbol{x}]$, sodass folgendes gilt:

$$f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i = \sum_{j=1}^{s} b_j f_j + r,$$

für alle $j \in \{1, \ldots, s\}$ gilt $\textsc{Deg}(b_j f_j) \leq \textsc{Deg}(f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i)$, und kein Monomom in r ist durch ein $\textsc{Lm}(f_j)$ mit $j \in \{1, \ldots, s\}$ teilbar.

Dann gilt

$$f = \Big(\sum_{\substack{j \in \{1,\ldots,s\} \\ j \neq i}} b_j f_j \Big) + \left(b_i + \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} \right) f_i + r$$

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 6.16. 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 6.17. *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 6.2 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 6.18. *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 6.19. 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 6.20. *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 6.17 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 6.21. *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 6.22. *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 $\langle \mathrm{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. 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 $\mathrm{LT}(r) \in \mathrm{LT}(I)$. Nach Voraussetzung gilt also

$$\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}.$$

Wegen Lemma 6.21 gibt es also ein $i \in \{1, \ldots, t\}$, sodass $\mathrm{LT}(g_i) | \mathrm{LT}(r)$. Dann kann r aber nicht der Rest einer Standarddarstellung von f durch $(g_1, \ldots, g_t)$ sein. Der Fall $r \neq 0$ kann also nicht eintreten. □

Satz 6.23 (Hilbertscher Basissatz für Polynomringe über Körpern)**.** *Sei k ein Körper, $n \in \mathbb{N}$. Dann ist jedes Ideal von $k[x_1, \ldots, x_n]$ endlich erzeugt.*

Beweis: Sei I ein Ideal von $k[x_1, \ldots, x_n]$. Nach Satz 6.20 gibt es $t \in \mathbb{N}_0$ und $g_1, \ldots, g_t \in I \setminus \{0\}$, sodass $\langle \mathrm{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. Wegen Satz 6.22 erzeugen dann die Polynome $g_1, \ldots, g_t$ das Ideal I. □

4. Gröbnerbasen

Definition 6.24. Sei k ein Körper, $n \in \mathbb{N}$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I ein Ideal von $k[x_1, \ldots, x_n]$. Eine endliche Teilmenge $G = \{g_1, \ldots, g_t\}$ von $k[x_1, \ldots, x_n]$ ist eine *Gröbnerbasis* von I bezüglich $\leq$, wenn

(1) $G \subseteq I \setminus \{0\}$,
(2) $\langle \mathrm{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$.

Nach Satz 6.20 besitzt jedes Ideal eine Gröbnerbasis. Wenn nun I ein Ideal von $k[x_1, \ldots, x_n]$, und G eine Gröbnerbasis von I ist, so gilt nach Satz 6.22 auch $\langle G \rangle_{k[\boldsymbol{x}]} = I$.

Satz 6.25. *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 $r \in I$ so, dass kein Monom in r durch irgendein $\mathrm{LT}(g_i)$ teilbar ist. Dann gilt $r = 0$.*

Beweis: Wenn $r \neq 0$, so liegt $\mathrm{LT}(r) \in \mathrm{LT}(I)$, also in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Wegen Lemma 6.21 gibt es also ein $i \in \{1, \ldots, t\}$, sodass $\mathrm{LT}(g_i) | \mathrm{LT}(r)$. Das steht im Widerspruch zu den Voraussetzungen an r. □

Satz 6.26. *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. Seien $r_1, r_2 \in k[x_1, \ldots, x_n]$ so, dass*

(1) $r_1 - r_2 \in I$,
(2) *Kein Monom in r_1 ist durch irgendein $\mathrm{LT}(g_i)$ teilbar,*
(3) *Kein Monom in r_2 ist durch irgendein $\mathrm{LT}(g_i)$ teilbar.*

Dann gilt $r_1 = r_2$.

Beweis: Wir nehmen an, $r_1 - r_2 \neq 0$. Dann gilt $\mathrm{LM}(r_1 - r_2) \in \mathrm{LT}(I)$. Da G eine Gröbnerbasis ist, gilt also $\mathrm{LM}(r_1 - r_2) \in \langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. 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 $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Nach Lemma 6.21 ist dieses Monom durch eines der $\mathrm{LM}(g_i)$ teilbar. Das steht im Widerspruch zu den Voraussetzungen an r_1 und r_2. □

Korollar 6.27. *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 6.26. Wenn $f \in I$ gilt, so folgt $r_1 = 0$ aus Satz 6.25. □

Definition 6.28. 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.

5. Konstruktion von Gröbnerbasen

Wir fixieren für die Sektionen 5 und 6 eine zulässige Ordnung $\leq$ auf ${\mathbb{N}_0}^n$.

Definition 6.29. Sei k ein Körper, $n \in \mathbb{N}$. Seien $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n) \in {\mathbb{N}_0}^n$. Sei $\gamma = (\gamma_1, \ldots, \gamma_n)$ definiert durch $\gamma_i := \max(\alpha_i, \beta_i)$ für $i \in \{1, \ldots, n\}$. Wir definieren $\textsc{Lcm}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta) := \boldsymbol{x}^\gamma$.

Lemma 6.30. *Sei k ein Körper, $n \in \mathbb{N}$, und seien $\alpha, \beta \in {\mathbb{N}_0}^n$. Sei f ein Polynom mit $\boldsymbol{x}^\alpha | f$ und $\boldsymbol{x}^\beta | f$. Dann gilt $\textsc{Lcm}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta) | f$.*

Beweis: Sei $\gamma \in {\mathbb{N}_0}^n$ so, dass $\boldsymbol{x}^\gamma = \textsc{Lcm}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta)$. Nach Lemma 6.21 gilt für jedes in f vorkommende Monom $\boldsymbol{x}^\mu$, dass $\alpha \sqsubseteq \mu$ und $\beta \sqsubseteq \mu$. Also gilt $\gamma \sqsubseteq \mu$, und somit $\boldsymbol{x}^\gamma | \boldsymbol{x}^\mu$. □

Definition 6.31. 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

$$S(f,g) := \frac{\textsc{Lcm}(\textsc{Lm}(f), \textsc{Lm}(g))}{\textsc{Lt}(f)} \cdot f - \frac{\textsc{Lcm}(\textsc{Lm}(f), \textsc{Lm}(g))}{\textsc{Lt}(g)} \cdot g.$$

Lemma 6.32. *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 6.8 Multigrad $\leq \gamma$; keiner dieser Summanden hat Multigrad $= \gamma$. Die Summe hat also Multigrad $< \gamma$. □

Lemma 6.33. *Sei k ein Körper, seien $n, s \in \mathbb{N}$, und $f_1, \ldots, f_s \in k \setminus \{0\}$, $c_1, \ldots, c_s \in k \setminus \{0\}$, und $\delta, \alpha_1, \ldots, \alpha_s \in {\mathbb{N}_0}^n$ so, dass folgendes gilt:*

(1) *Für alle $i \in \{1, \ldots, s\}$ gilt $\textsc{Deg}(\boldsymbol{x}^{\alpha_i} f_i) = \delta$.*
(2) $\textsc{Deg}(\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i) < \delta$.

Dann gibt es $b_1, \ldots, b_{s-1} \in k$, sodass

$$\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i = \sum_{j=1}^{s-1} b_j \frac{\boldsymbol{x}^{\delta}}{\textsc{Lcm}(\textsc{Lm}(f_j), \textsc{Lm}(f_s))} S(f_j, f_s). \tag{5.1}$$

Beweis Für $j \in \{1, \ldots, s-1\}$ sei $\gamma_j \in {\mathbb{N}_0}^n$ so, dass

$$\boldsymbol{x}^{\gamma_j} = \textsc{Lcm}(\textsc{Lm}(f_j), \textsc{Lm}(f_s)).$$

Dann lässt sich die behauptete Gleichung (5.1) als

$$\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i = \sum_{j=1}^{s-1} b_j \boldsymbol{x}^{\delta - \gamma_j} S(f_j, f_s)$$

schreiben.

In der Summe auf der linken Seite von (5.1) hat jeder Summand Multigrad δ. Da nach Voraussetzung (2) die Summe kleineren Multigrad hat, muss der Koeffizient von $\boldsymbol{x}^{\delta}$ in $\sum_{i=1}^{s-1} c_i \boldsymbol{x}^{\alpha_i} f_i$ gleich 0 sein. Es gilt also

$$\sum_{i=1}^{s} c_i \textsc{Lc}(f_i) = 0.$$

Dann gilt

$$\begin{aligned}
\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i &= \sum_{i=1}^{s-1} \left(c_i \boldsymbol{x}^{\alpha_i} f_i - c_i \frac{\textsc{Lc}(f_i)}{\textsc{Lc}(f_s)} \boldsymbol{x}^{\alpha_s} f_s \right) \\
&\quad + \left(\sum_{i-1}^{s-1} c_i \frac{\textsc{Lc}(f_i)}{\textsc{Lc}(f_s)} \boldsymbol{x}^{\alpha_s} f_s \right) + c_s \boldsymbol{x}^{\alpha_s} f_s \\
&= \sum_{i=1}^{s-1} \left(c_i \boldsymbol{x}^{\alpha_i} f_i - c_i \frac{\textsc{Lc}(f_i)}{\textsc{Lc}(f_s)} \boldsymbol{x}^{\alpha_s} f_s \right) + \left(\sum_{i=1}^{s} c_i \frac{\textsc{Lc}(f_i)}{\textsc{Lc}(f_s)} \right) \boldsymbol{x}^{\alpha_s} f_s.
\end{aligned}$$

Da $\sum_{i=1}^{s} c_i \text{LC}(f_i) = 0$, gilt

$$\begin{aligned}
\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i &= \sum_{i=1}^{s-1} c_i \left(\frac{\boldsymbol{x}^{\delta}}{\text{LM}(f_i)} f_i - \frac{\text{LC}(f_i)}{\text{LC}(f_s)} \frac{\boldsymbol{x}^{\delta}}{\text{LM}(f_s)} f_s \right) \\
&= \sum_{i=1}^{s-1} c_i \text{LC}(f_i) \left(\frac{\boldsymbol{x}^{\delta}}{\text{LT}(f_i)} f_i - \frac{\boldsymbol{x}^{\delta}}{\text{LT}(f_s)} f_s \right) \\
&= \sum_{i=1}^{s-1} c_i \text{LC}(f_i) \boldsymbol{x}^{\delta-\gamma_i} \left(\frac{\boldsymbol{x}^{\gamma_i}}{\text{LT}(f_i)} f_i - \frac{\boldsymbol{x}^{\gamma_i}}{\text{LT}(f_s)} f_s \right) \\
&= \sum_{i=1}^{s-1} c_i \text{LC}(f_i) \boldsymbol{x}^{\delta-\gamma_i} S(f_i, f_s).
\end{aligned}$$

□

Satz 6.34 (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 $\text{LT}(f)$ im Ideal $\langle LT(g_1), \ldots, \text{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$ 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

$$\delta' := \max\{\text{DEG}(h'_i g_i) \mid i \in \{1, \ldots, t\}\}.$$

Seien nun $h_1, \ldots, h_t \in k[x_1, \ldots, x_n]$ so unter allen Darstellungen von f als $\sum_{i=1}^{t} h'_i f_i$, dass δ' minimal wird, und sei

$$\delta := \max\{\text{DEG}(h_i g_i) \mid i \in \{1, \ldots, t\}\}.$$

Es gilt

$$f = \sum_{i=1}^{t} h_i g_i,$$

also $\textsc{Deg}(f) \leq \delta$.

1. Fall: $\textsc{Deg}(f) = \delta$*:* Sei $i \in \{1, \ldots, t\}$ so, dass $\textsc{Deg}(h_i g_i) = \delta$. Dann gilt $\textsc{Lt}(g_i) | \textsc{Lt}(f)$, und somit $\textsc{Lt}(f) \in \langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}$.

2. Fall: $\textsc{Deg}(f) < \delta$*:* Für $i \in \{1, \ldots, t\}$ sei $m(i) := \textsc{Deg}(h_i g_i)$. Es gilt dann

$$\begin{aligned} f = \sum_{i=1}^{t} h_i g_i &= \sum_{\substack{i=1 \\ m(i)=\delta}}^{t} h_i g_i + \sum_{\substack{i=1 \\ m(i)<\delta}}^{t} h_i g_i \\ &= \sum_{\substack{i=1 \\ m(i)=\delta}}^{t} \textsc{Lt}(h_i) g_i + \sum_{\substack{i=1 \\ m(i)=\delta}}^{t} (h_i - \textsc{Lt}(h_i)) g_i + \sum_{\substack{i=1 \\ m(i)<\delta}}^{t} h_i g_i. \end{aligned}$$

Alle Summanden der zweiten und dritten Summe haben Multigrad $< \delta$. Da auch $\textsc{Deg}(f) < \delta$, gilt

$$\textsc{Deg}\Big(\sum_{\substack{i=1 \\ m(i)=\delta}}^{t} \textsc{Lt}(h_i) g_i \Big) < \delta.$$

Seien $s \in \mathbb{N}$ und $i_1, \ldots, i_s$ so, dass $i_1 < \cdots < i_s$ und $\{i_j \mid j \in \{1, \ldots, s\}\} = \{i \in \{1, \ldots, t\} \mid m(i) = \delta\}$. Wir verwenden nun Lemma 6.33 für $f_j := g_{i_j}$, $c_j := \textsc{Lc}(h_{i_j})$ und α_j so, dass $\boldsymbol{x}^{\alpha_j} := \textsc{Lm}(h_{i_j})$ $(j \in \{1, \ldots, s\})$. Aus diesem Lemma erhalten wir für $j, l \in \{1, \ldots, t\}$ mit $j < l$ Körperelemente $b_{j,l} \in k$, sodass

$$\sum_{\substack{i=1 \\ m(i)=\delta}}^{t} \textsc{Lt}(h_i) g_i = \sum_{\substack{j,l \in \{1,\ldots,t\} \\ j<l}} b_{j,l} \frac{\boldsymbol{x}^{\delta}}{\textsc{Lcm}(\textsc{Lm}(g_j), \textsc{Lm}(g_l))} S(g_j, g_l).$$

Da $S(g_j, g_l)$ nach Voraussetzung eine Standarddarstellung mit Rest 0 besitzt, gibt es für $j < l$ Polynome $a_{j,l,1}, \ldots, a_{j,l,t} \in k[\boldsymbol{x}]$, sodass

$$S(g_j, g_l) = \sum_{i=1}^{t} a_{j,l,i} \cdot g_i,$$

und $\text{DEG}(a_{j,l,i}g_i) \leq \text{DEG}(S(g_j, g_l))$ für alle $i \in \{1, \ldots, t\}$. Sei nun $\gamma_{j,l} \in {\mathbb{N}_0}^n$ so, dass $\boldsymbol{x}^{\gamma_{j,l}} = \text{LCM}(\text{LM}(g_j), \text{LM}(g_l))$. Also gilt

$$\begin{aligned}
&\sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<l}} b_{j,l}\frac{\boldsymbol{x}^\delta}{\text{LCM}(\text{LM}(g_j),\text{LM}(g_l))}S(g_j,g_l)\\
&\qquad = \sum_{i=1}^{t}\sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<l}} b_{j,l}\frac{\boldsymbol{x}^\delta}{\text{LCM}(\text{LM}(g_j),\text{LM}(g_l))}a_{j,l,i}g_i\\
&\qquad = \sum_{i=1}^{t}\sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<l}} b_{j,l}\boldsymbol{x}^{\delta-\gamma_{j,l}}a_{j,l,i}g_i.
\end{aligned}$$

Wir berechnen nun den Multigrad des (j, l, i)-ten Summanden

$$\sigma(j, l, i) := b_{j,l}\boldsymbol{x}^{\delta-\gamma_{j,l}}a_{j,l,i}g_i.$$

Es gilt $\text{DEG}(\sigma(j, l, i)) \leq \delta - \gamma_{j,l} + \text{DEG}(a_{j,l,i}g_i) \leq \delta - \gamma_{j,l} + \text{DEG}(S(g_j, g_l))$. Wegen Lemma 6.32 gilt $\text{DEG}(S(g_j, g_l)) < \gamma_{j,l}$, also gilt

$$\text{DEG}(\sigma(j, l, i)) < \delta.$$

Daher ist

$$f = \sum_{\substack{i=1\\ m(i)=\delta}}^{t}\Big(\big(\sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<k}} b_{j,l}\boldsymbol{x}^{\delta-\gamma j,l}a_{i,j,l}\big) + (h_i - \text{LT}(h_i))\Big)\cdot g_i + \sum_{\substack{i=1\\ m(i)<\delta}}^{t} h_i g_i$$

eine Darstellung von f, in der jeder Summand Multigrad $< \delta$ hat. Das ist ein Widerspruch zur Wahl von δ. Der 2. Fall kann also nicht eintreten. □

Das Hinzufügen eines möglichen Restes des betrachteten S-Polynoms bewirkt, dass dieses S-Polynom 0 als möglichen Rest hat:

Lemma 6.35. *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 $\textsc{Deg}(r) \leq \textsc{Deg}(f)$. 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 6.36 (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: $P \leftarrow \emptyset$
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: $\quad\quad G \leftarrow (G, r)$
8: $\quad$ **end if**
9: **end while**

Satz 6.37. *Sei k ein Körper, und seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$. Der Algorithmus 6.36 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 $(\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}, |\binom{G}{2} \setminus P|)$. 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 $\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}$ 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 $\textsc{Lt}(r)$ nicht in $\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}$. Dann gilt aber $\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]} \neq \langle \textsc{Lt}(G \cup \{r\}) \rangle_{k[\boldsymbol{x}]}$.

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 $P = \emptyset$. Im weiteren Verlauf garantiert Lemma 6.35, 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 6.34 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 $\langle f_1, \ldots, f_s\rangle_{k[\boldsymbol{x}]}$. □

Übungsaufgaben 6.38

(1) Berechnen Sie eine Gröbnerbasis des Ideals $\langle -1 - x\,y + y^2 + x\,y^2, -1 + y^2\rangle$ mit lexikographischer Ordnung $x > y$.
(2) Berechnen Sie eine Gröbnerbasis des Ideals $\langle -1 + a\,b + a^2\,c,\ 2 + b\,c^3\rangle$, mit lexikographischer Ordnung $a > b > c$.
(3) Seien $g_1, g_2, g_3 \in \mathbb{Q}[x, y]$ gegeben durch

$$\begin{aligned} g_1 &= xy - 1 \\ g_2 &= y^2 + 1 \\ g_3 &= x^2 + 1. \end{aligned}$$

Sei

$$s := 5x^2y^2\,g_1 - 3x^3y\,g_2 - 2xy^3\,g_3,$$

und sei $\delta := (3, 3)$. Wir ordnen die Monome lexikographisch mit $x > y$. Es gilt

$$\textsc{Deg}(s) < \delta.$$

Finden Sie $c_1, c_2 \in \mathbb{Q}$ und $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}_0$, sodass

$$s = c_1\,x^{\alpha_1}y^{\alpha_2}\,S(g_1, g_2) + c_2\,x^{\beta_1}y^{\beta_2}\,S(g_2, g_3)$$

und jeder Summand in dieser Summe Multigrad $< \delta$ hat.

6. 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 6.39. *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) $\langle \mathrm{LT}(F) \rangle_{k[\boldsymbol{x}]} \subseteq \langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$,
(3) *Wenn $r_i \neq 0$ und $\mathrm{LM}(r_i) \neq \mathrm{LM}(f_i)$, so gilt $\mathrm{LT}(r_i) \notin \langle \mathrm{LT}(F) \rangle_{k[\boldsymbol{x}]}$.*
(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 $\text{DEG}(r_i) \leq \text{DEG}(f_i)$. Somit gilt $\text{DEG}(r_i) = \text{DEG}(f_i)$, und somit $\text{LM}(r_i) = \text{LM}(f_i)$.

(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

$$q = \sum_{\substack{j=1 \\ j \neq i}}^{s} (a_j + a_i b_j) f_j + a_i r_i. \tag{6.1}$$

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 (6.1) eine Standarddastellung von q durch G. □

Definition 6.40. 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 6.41. 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 6.42 (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: $P \leftarrow \emptyset$
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: $\quad\quad G \leftarrow (G, r)$
8: $\quad$ **end if**
9: $\quad$ **while** G ist nicht reduziert und wir wollen G reduzieren **do**
10: $\quad\quad f_1 \leftarrow$ Ein Element von G, das in G nicht reduziert ist
11: $\quad\quad r_1 \leftarrow \begin{cases} \text{Ein möglicher Rest von } f_1 \\ \text{bei Standarddarstellung durch } G \setminus \{f_1\} \end{cases}$
12: $\quad\quad$ **if** $r_1 = 0$ **then**
13: $\quad\quad\quad G \leftarrow G \setminus \{f_1\}$
14: $\quad\quad$ **else**
15: $\quad\quad\quad G \leftarrow G \setminus \{f_1\} \cup \{r_1\}$
16: $\quad\quad$ **end if**
17: $\quad$ **end while**
18: **end while**

Übungsaufgaben 6.43

(1) 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!

(2) Bestimmen Sie eine Gröbnerbasis des folgenden Ideals $I = \langle f_1, f_2 \rangle$ von $\mathbb{Q}[x]$.

$$\begin{aligned} f_1 &= x - x^3 + x^4 - 2\,x^5 + x^6 \\ f_2 &= x - 2\,x^2 + x^3 - x^4 + x^6. \end{aligned}$$

(3) (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.)

Satz 6.44. *Unabhängig davon, wie oft wir im Ablauf des Algorithmus reduzieren wollen, terminiert der Algorithmus 6.42 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 6.35 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 6.39 (1) liefert, dass

$\langle G\rangle_{k[\boldsymbol{x}]}$ immer gleich dem Ideal I ist. Lemma 6.39 (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 6.34 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 $\langle \textsc{Lt}(G)\rangle_{k[\boldsymbol{x}]}$. Wegen Lemma 6.39 (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 $\textsc{Lt}(r)$ nicht in $\langle \textsc{Lt}(G)\rangle_{k[\boldsymbol{x}]}$. Dann gilt aber $\langle \textsc{Lt}(G)\rangle_{k[\boldsymbol{x}]} \neq \langle \textsc{Lt}(G \cup \{r\})\rangle_{k[\boldsymbol{x}]}$. 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 $\textsc{Lt}(G)$ konstant bleibt, bleibt wegen Lemma 6.39 (3) nur mehr der Fall $\textsc{Lm}(r_1) = \textsc{Lm}(f_1)$ 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 $\textsc{Lm}(r_1) = \textsc{Lm}(f_1)$ 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 passieren.

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 6.42 eine "reduzierte Gröbnerbasis".

Definition 6.45. 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 $\text{LC}(g) = 1$.

Als Konsequenz aus der Termination und Korrektheit des Algorithmus 6.42 erhalten wir:

Satz 6.46. *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 6.47. *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

$$\text{LT}(G) = \text{LT}(H).$$

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 $\text{DEG}(a_i h_i) \leq \text{DEG}(g)$. Für zumindest einen Summanden muss $\text{DEG}(a_j h_j) = \text{DEG}(g)$ 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 $\text{DEG}(b_l g_l) \leq \text{DEG}(h_j)$. Sei l so, dass $\text{DEG}(h_j) = \text{DEG}(b_l g_l)$. Dann gilt $\text{LT}(g_l) | \text{LT}(h_j)$ und $\text{LT}(h_j) | \text{LT}(g)$. Es gilt also $\text{LT}(g_l) | \text{LT}(g)$. Da G reduziert ist, gilt $g = g_l$. Nun gilt $\text{LM}(g_l) | \text{LM}(h_j)$ und $\text{LM}(h_j) | \text{LM}(g)$. Wegen $g_l = g$ gilt also

$\text{LM}(g) = \text{LM}(h_j)$. Folglich gilt $\text{LT}(g) \in \text{LT}(H)$. Damit haben wir $\text{LT}(G) \subseteq \text{LT}(H)$ bewiesen.

Ebenso gilt $\text{LT}(H) \subseteq \text{LT}(G)$. Insgesamt gilt also $\text{LT}(G) = \text{LT}(H)$.

Wir zeigen nun $G \subseteq H$. Sei dazu $g \in G$. Es gibt nun ein Polynom $h \in H$, sodass $\text{LT}(g) = \text{LT}(h)$. Da G reduziert ist, enthält $g - \text{LT}(g)$ kein Monom, das in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ liegt. Da H reduziert ist, enthält $h - \text{LT}(h)$ kein Monom, das in $\langle \text{LT}(H) \rangle_{k[\boldsymbol{x}]}$ liegt. Wegen $\text{LT}(G) = \text{LT}(H)$ liegt also auch kein Monom von $h - \text{LT}(h)$ in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Somit liegt wegen $\text{LT}(g) = \text{LT}(h)$ kein Monom von $g - h = (g - \text{LT}(g)) - (h - \text{LT}(h))$ in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. 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 6.27 die Gleichheit $g = h$. Somit gilt $g \in H$.

Ebenso zeigt man $H \subseteq G$. □

Das folgende Kriterium erspart die Überprüfung der S-Polynome jener Paare, deren führende Monome keine gemeinsamen Variablen enthalten.

Lemma 6.48. *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 $\text{LCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g)$. Dann ist 0 ein möglicher Rest von $S(f, g)$ bei Standarddarstellung durch F.*

Beweis: Sei $p := f - \text{LT}(f)$ und $q := g - \text{LT}(g)$. Dann gilt

$$\begin{aligned} S(f,g) &= \frac{\text{LM}(g)}{\text{LC}(f)} f - \frac{\text{LM}(f)}{\text{LC}(g)} g \\ &= \frac{\text{LT}(g)}{\text{LC}(f)\text{LC}(g)} f - \frac{\text{LT}(f)}{\text{LC}(f)\text{LC}(g)} g \\ &= \frac{1}{\text{LC}(f)\text{LC}(g)} (\text{LT}(g) f - \text{LT}(f) g). \end{aligned}$$

Es gilt

$$\begin{aligned} \text{LT}(g) f - \text{LT}(f) g &= (g - q) f - (f - p) g \\ &= qf + pg. \end{aligned}$$

Wir behaupten nun, dass $qf + pg$ eine Standarddastellung von $\text{LT}(g) f - \text{LT}(f) g$ durch (f, g) ist. Wenn $p = q = 0$, ist das offensichtlich.

Wir nehmen nun an, dass $p \neq 0$ und betrachten zuerst den Fall, dass $\text{DEG}(qf) = \text{DEG}(pg)$. Dann gilt $\text{LM}(f)|\text{LM}(p)\text{LM}(g)$. Da $\text{LM}(f)$ und $\text{LM}(g)$ keine gemeinsamen Variablen enthalten, gilt $\text{LM}(f)|\text{LM}(p)$. Das steht aber im Widerspruch zu $\text{DEG}(p) < \text{DEG}(f)$. Somit gilt $\text{DEG}(qf) \neq \text{DEG}(pg)$. Damit gilt aber $\text{DEG}(qf + pg) = \max(\text{DEG}(qf), \text{DEG}(pg))$. Somit gilt also $\text{DEG}(qf) < \text{DEG}(qf + pg)$ und $\text{DEG}(pg) < \text{DEG}(qf + pg)$. Damit ist aber $qf + pg$ eine Standarddarstellung von $qf + pg$ durch (f, g) mit Rest 0.

Der Fall $q \neq 0$ lässt sich genauso behandeln. □

Übungsaufgaben 6.49

(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 $x_1 > \cdots > x_5$.)

7. Die Eliminationseigenschaft von Gröbnerbasen

Satz 6.50. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$. Sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^{m+n}$, sodass für alle $\alpha \in {\mathbb{N}_0}^m$ und $\beta \in {\mathbb{N}_0}^n$ mit $\alpha \neq (0, \ldots, 0)$ gilt: $\boldsymbol{x}^\alpha > \boldsymbol{y}^\beta$. 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 dass $\text{LT}(f) \in \langle \text{LT}(G_{\boldsymbol{y}})\rangle_{k[\boldsymbol{y}]}$ 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 $\text{DEG}(a_i g_i) \leq \text{DEG}(f)$, 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 $\text{DEG}(a_j g_j) = \text{DEG}(f)$ gelten. Dann gilt $\text{LT}(g_j)|\text{LT}(f)$ in $k[\boldsymbol{y}]$, und somit liegt $\text{LT}(f)$ in $\langle \text{LT}(G_{\boldsymbol{y}})\rangle_{k[\boldsymbol{y}]}$. □

Übungsaufgaben 6.51

(1) 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 $I \cap \mathbb{R}[x_1, x_2, x_3]$.

(2) Sei k ein Körper und sei $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n] \setminus \{0\}$.
   (a) Zeigen Sie: Wenn F eine Gröbnerbasis für $\langle F\rangle$ ist und $\text{LT}(f_i) \in \langle \text{LT}(f_1), \ldots, \text{LT}(f_{i-1}), \text{LT}(f_{i+1}), \ldots, \text{LT}($ dann ist auch $F \setminus \{f_i\}$ eine Gröbnerbasis für $\langle F\rangle$.
   (b) Gilt diese Behauptung auch, wenn man das Wort "Gröbnerbasis" beide Male durch "Basis" ersetzt?

Wir geben hier eine erste Anwendung dieser Eigenschaft an: wir zeigen, wie wir die Generatoren des Schnitts zweier Ideale von $k[x_1, \ldots, x_n]$ berechnen.

Satz 6.52 (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 6.53. *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 6.52 für $R := k[\boldsymbol{t}]$. □

8. 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 6.54. *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 6.55 (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 6.54 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 6.56

(1) 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 $\overline{f}((x + y + 1) + I, (x + z) + I) = 0 + I$.

(2) 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 $h(x, y, z^3 + x + 1) \in I_1 = \langle z\rangle \cap \langle x, y\rangle$.

(3) 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.

(4) 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 5.25 Transzendenzbasen verschiedener Kardinalität gefunden?

Korollar 6.57 (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 6.58 (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 6.54 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 6.59 (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 6.58 für $R := k[x_1, \ldots, x_n]$. □

9. 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 6.58 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 6.60. 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 6.61. 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 6.62. *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 $\textsc{Deg}(f)$ minimal ist. Da $f \in I$, gilt $\textsc{Lt}(f) \in \textsc{Lt}(I)$. Also gibt es ein $g \in G$, sodass $\textsc{Lt}(g)|\textsc{Lt}(f)$. Sei $f_1 = f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(g)} g$. 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 $\frac{\textsc{Lt}(f)}{\textsc{Lt}(g)} g$ 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 $f = f_1 + \frac{\textsc{Lt}(f)}{\textsc{Lt}(g)} g$ 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 $\textsc{Deg}(g) \leq \textsc{Deg}(f)$ und $\textsc{Deg}(f) \leq \textsc{Deg}(p)$, insgesamt also $\textsc{Deg}(g) \leq \textsc{Deg}(p)$. 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 kritischen Polynoms von minimalem Grad in x_1.

Lemma 6.63. *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 $\textsc{Lt}(g)|\textsc{Lt}(p_n)$. Wegen der Eigenschaft der Ordnung gilt $\textsc{Lt}(p) = \textsc{Lt}(p_n) \cdot x_1^n$. Also gilt $\textsc{Lt}(g)|\textsc{Lt}(p)$. 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 6.64. 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 6.65. *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 6.66. Bestimmen Sie, ob x^3 im Unterkörper $\mathbb{Q}(x^2 + 2, x^5 + x + 1)$ 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 6.57 finden. Wir berechnen dazu eine reduzierte Gröbnerbasis von

$$J = \langle x_1 - x^3, x_2 - (x^2 + 2), x_3 - (x^5 + x + 1) \rangle_{k[x, x_1, x_2, x_3]}$$

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 6.50, 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 6.63 ein kritisches Polynom für x_1 in $J \cap k[x_1, x_2, x_3]$. Aufgrund von Satz 6.62 (oder weil p linear in x_1 ist), ist p auch kritisch minimalen Grades. Also ist wegen Lemma 6.65

$$(-x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20 + I)\ t^0 + (x_3 - 1 + I)\ t$$

ein MinimalPolyom 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 $a, f_1, \ldots, f_s \in k[\boldsymbol{x}]$ und $b, g_1, \ldots, g_s \in k[\boldsymbol{x}]$ folgende Fragen beantworten:

(1) Gilt $\frac{a}{b} \in k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$?
(2) Ist die Körpererweiterung $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)\big(\frac{a}{b}\big)$ algebraisch über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$?
(3) Wenn diese Körpererweiterung algebraisch ist, was ist ihr Grad?

Wir finden dazu mithilfe von Satz 6.58 ein Ideal I des Polynomrings $k[x_1, \ldots, x_{s+1}]$, sodass $k[x_1, \ldots, x_{s+1}]/I$ durch φ isomorph zu $k[\![\frac{a}{b}, \frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}]\!]$ ist, und $\varphi(x_1 + I) = \frac{a}{b}$, $\varphi(x_{i+1} + I) = \frac{f_i}{g_i}$ für $i \in \{1, \ldots, s\}$. Dann bestimmen wir ein Minimalpolynom für $x_1 + I$ über $k[\![x_2 + I, \ldots, x_{s+1} + I]\!]$, 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 $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$. Ansonsten erhalten wir aus p ein Minimalpolynom von $\frac{a}{b}$ über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$. Wenn $\deg_{x_1}(p) = 1$, so liegt $\frac{a}{b} \in k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$. Wenn $\deg_{x_1}(p) > 1$, so ist $\frac{a}{b}$ algebraisch über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$, und $\deg_{x_1}(p)$ ist der Grad der Körpererweiterung $[k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)\big(\frac{a}{b}\big) : k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)]$.

Als letztes fragen wir uns noch, ob $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist, und, wenn ja, wie ein Polynom kleinsten Grades mit führendem Koeffizienten 1 aussieht, dass das belegt.

Satz 6.67. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Wir nehmen an, dass $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ 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 $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ 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 $f \in k[\![x_2 + I, \ldots, x_n + I]\!][t]$ ein Polynom minimalen Grades, das belegt, dass $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist. Wir schreiben f als $\sum_{i=0}^{m-1} \overline{f_i}(x_2 + I, \ldots, x_n + I)\, t^i + t^m$. Wegen $\overline{f}(x_1 + I) = 0$ liegt das Polynom $p := \sum_{i=0}^{m-1} f_i(x_2, \ldots, x_n)\, x_1^i + x_1^m$ 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 $g(t, x_2 + I, \ldots, x_n + I)$ ein Polynom vom Grad m_1, das belegt, dass $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ 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 $k[x_1, \ldots, x_n]/I$ isomorph zu einem Integritätsbereich ist. In diesem Fall ist das Ideal I prim.

Satz 6.68. *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 reduzierte Gröbnerbasis von I bezüglich $\leq$. Dann gilt:*

1. *$x_1 + I$ liegt genau dann in $k[\![x_2 + I, \ldots, x_n + I]\!]$, wenn G ein Polynom p mit $\operatorname{LM}(p) = x_1$ enthält.*
2. *$x_1 + I$ ist genau dann ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$, 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 $k[\![x_2 + I, \ldots, x_n + I]\!]$, 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 $k[\![x_1 + I, \ldots, x_n + I]\!]$ 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 6.67 ein Polynom in G mit $\mathrm{LM}(g)=x_1$.

(2) Dieser Teil ergibt sich genauso aus Satz 6.67.

(3) Ergibt sich aus Satz 6.62, Lemma 6.63 und Lemma 6.65.

(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 6.63 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 6.62 auch in G. □

10. Existenz universeller Gröbnerbasen

Wir zeigen in dieser Sektion den folgenden Satz.

Satz 6.69. *Sei* k *ein Körper, sei* $n\in\mathbb{N}$*, und sei* I *ein Ideal von* $k[x_1,\dots,x_n]$*. Dann gibt es eine endliche Teilmenge* G *von* $k[x_1,\dots,x_n]$*, 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 6.7 wissen wir bereits, dass es keine undendliche 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 6.70 (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 6.1 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 6.71. *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 6.21 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 6.70 nicht. □

Beweis von Satz 6.69: 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 6.71 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 6.46 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 7

Varietäten

1. Lösungsmengen polynomialer Gleichungssysteme

Definition 7.1. Sei k ein Körper, sei $n \in \mathbb{N}$, und sei $F \subseteq k[x_1, \ldots, x_n]$. Dann definieren wir $\mathsf{V}(F)$, die *durch F beschriebene Varietät*, durch $\mathsf{V}(F) = \{\boldsymbol{a} \in k^n \mid \overline{f}(\boldsymbol{a}) = 0 \text{ für alle } f \in F\}$. Eine Teilmenge V von k^n ist eine *Varietät*, wenn es ein $F \subseteq k[x_1, \ldots, x_n]$ gibt, sodass $V = \mathsf{V}(F)$.

Lemma 7.2. *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 $\mathsf{V}(M) = \mathsf{V}(I) = \mathsf{V}(F) = \mathsf{V}(\sqrt{I})$.*

Definition 7.3. Sei k ein Körper, $n \in \mathbb{N}$, und sei $S \subseteq k^n$. Wir definieren das *zu S gehörende Ideal* durch $\mathsf{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid \forall \boldsymbol{s} \in S : \overline{f}(\boldsymbol{s}) = 0\}$.

Lemma 7.4. *Sei k ein Körper, $n \in \mathbb{N}$, und sei $S \subseteq k^n$. Dann ist $\mathsf{I}(S)$ ein Ideal von $k[x_1, \ldots, x_n]$, und es gilt $\mathsf{I}(S) = \sqrt{\mathsf{I}(S)}$.*

Lemma 7.5. *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 $\mathsf{V}(Q) \subseteq \mathsf{V}(P)$.*
(2) *Wenn $S \subseteq T$, so gilt $\mathsf{I}(T) \subseteq \mathsf{I}(S)$.*

Lemma 7.6. *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) $P \subseteq \mathsf{I}(\mathsf{V}(P))$.
(2) $S \subseteq \mathsf{V}(\mathsf{I}(S))$.
(3) $\mathsf{I}(\mathsf{V}(\mathsf{I}(S))) = \mathsf{I}(S)$.
(4) $\mathsf{V}(\mathsf{I}(\mathsf{V}(P))) = \mathsf{V}(P)$.

Satz 7.7. *Sei k ein algebraisch abgeschlossener Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Dann gilt $\mathsf{I}(\mathsf{V}(I)) = \sqrt{I}$.*

Lemma 7.8. *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) $\mathsf{V}(I \cap J) = \mathsf{V}(I) \cup \mathsf{V}(J)$,
(2) $\mathsf{V}(I + J) = \mathsf{V}(I) \cap \mathsf{V}(J)$,
(3) $\mathsf{I}(V \cup W) = \mathsf{I}(V) \cap \mathsf{I}(W)$,
(4) $\mathsf{I}(V \cap W) \supseteq \sqrt{\mathsf{I}(V) + \mathsf{I}(W)}$.
(5) *Wenn k algebraisch abgeschlossen ist, gilt* $\mathsf{I}(V \cap W) = \sqrt{\mathsf{I}(V) + \mathsf{I}(W)}$.

Definition 7.9. Sei k ein Körper, $n \in \mathbb{N}$, und sei $P \subseteq k^n$. Dann ist $\mathsf{V}(\mathsf{I}(P))$ der *Zariski-Abschluss* von P. P heißt *Zariski-dicht*, wenn $\mathsf{V}(\mathsf{I}(P)) = P$.

Proposition 7.10. *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 $\mathsf{V}(\mathsf{I}(P)) \subseteq W$.*

Der Zariski-Abschluss von P ist also die kleinste Varietät, die P enthält.

Übungsaufgaben 7.11

(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 $\mathsf{I}(\mathsf{V}(M))$ über $\mathbb{Q}$.
   (b) Berechnen Sie $\mathsf{I}(\mathsf{V}(M))$ 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 $\mathsf{V}(I \cap \mathbb{C}[y, z]) = \pi(\mathsf{V}(M))$.
   (b) Wir rechnen im Körper $\mathbb{R}$. Sei $I := \langle M \rangle_{\mathbb{R}[t,x,y]}$. Zeigen Sie, dass $\pi(\mathsf{V}(M)) = \emptyset$ und dass $\mathsf{V}(I \cap \mathbb{R}[y, z])$ 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 $f \in k[x_1, \ldots, x_n]$ mit $\overline{f}|_M = 0$ auch gilt, dass $\overline{f}|_V = 0$.

Satz 7.12. *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. Zerlegung von Varietäten

Definition 7.13. Sei k ein Körper, $V \subseteq k^n$ eine Varietät. Die Varietät V ist *irreduzibel*, wenn

(1) $V \neq \emptyset$,
(2) Für alle Varietäten V_1, V_2 mit $V = V_1 \cup V_2$ gilt: $V_1 = V$ oder $V_2 = V$.

Satz 7.14. *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 7.15. *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 7.16. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei $V \subseteq k^n$ eine Varietät. Dann ist V genau dann irreduzibel, wenn $\mathsf{I}(V)$ prim ist.*

3. Parametrisierte Varietäten und Implizitisierung

Definition 7.17. 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: $V = \mathsf{V}(\mathsf{I}(S))$.

Lemma 7.18. *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) $p \in \mathsf{I}(S)$.
(2) $p(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}) = 0$.

Beweis: Sei $l := \max\{\deg_{x_i}(p) \mid p \in \{1, \ldots, n\}\}$. Wir definieren $q \in k[\boldsymbol{a}, \boldsymbol{b}]$ durch

$$q(a_1, \ldots, a_n, b_1, \ldots, b_n) := p(\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}) \cdot (b_1 \cdots b_n)^{l+1}.$$

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 $q(f_1, \ldots, f_n, g_1, \ldots, g_n) = 0$. Also gilt

$$\overline{q}(\overline{f_1}(\boldsymbol{s}), \ldots, \overline{f_n}(\boldsymbol{s}), \overline{g_1}(\boldsymbol{s}), \ldots, \overline{g_n}(\boldsymbol{s})) = 0.$$

Folglich gilt auch

$$\overline{p}(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s})}, \ldots \frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})}) = 0.$$

Somit hat p den Punkt $(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s}}, \ldots \frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})})$ als Nullstelle. Wir zeigen nun (1)⇒(2). Wir beweisen dazu als erstes, dass für alle $\boldsymbol{s} \in k^m$ gilt, dass

$$\overline{q}(\overline{f_1}(\boldsymbol{s}), \ldots, \overline{f_n}(\boldsymbol{s}), \overline{g_1}(\boldsymbol{s}), \ldots, \overline{g_n}(\boldsymbol{s})) = 0. \tag{3.1}$$

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 (3.1). Wenn $\overline{g_1}(\boldsymbol{s}) \cdots \overline{g_n}(\boldsymbol{s}) \neq 0$, so gilt wegen $p \in \mathsf{I}(S)$ auch $\overline{p}(\frac{\overline{f_1}(\boldsymbol{s})}{\overline{g_1}(\boldsymbol{s})}, \ldots, \frac{\overline{f_n}(\boldsymbol{s})}{\overline{g_n}(\boldsymbol{s})}) = 0$, und somit (3.1). Da k unendlich ist, ist also $q(f_1(\boldsymbol{t}), \ldots, f_n(\boldsymbol{t}), g_1(\boldsymbol{t}), \ldots, g_n(\boldsymbol{t}))$ das Nullpolynom in $k[\boldsymbol{t}]$. Da $k(\boldsymbol{t})$ ein Integritätsbereich ist und alle $g_i \neq 0$, gilt also $p(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}) = 0$. □

Lemma 7.18 und Korollar 6.59 ergeben also einen Algorithmus, der eine Basis des zu einer parametrisierten Varietät gehörenden Ideals liefert. Außerdem zeigt Lemma 7.18, dass für unendliche k die durch $((f_1, g_1), \ldots, (f_n, g_n))$ parametrisierte Varietät nur von $(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n})$ abhängt.

Übungsaufgaben 7.19

(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 $\mathsf{V}(\mathsf{I}(P))$ von P.
   (c) Gilt $P = \mathsf{V}(\mathsf{I}(P))$? (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 7.20. *Sei k ein unendlicher Körper, seien $(r_1, \ldots, r_n) \in k(t_1, \ldots, t_m)$. Dann ist die durch $(r_1, \ldots, r_n)$ parametrisierte Varietät V irreduzibel.*

Beweis: Sei S die Menge aller durch die Parametrisierung erreichbaren Punkte. Das Ideal $J := \{p \in k[x_1, \ldots, x_n] \mid p(r_1, \ldots, r_m) = 0\}$ ist prim. Wegen Lemma 7.18 gilt $J = \mathsf{I}(S)$. □

4. Die Dimension einer Varietät

Definition 7.21. Sei k ein Körper, und sei $V \subseteq k^n$ eine Varietät. Sei $I := \mathsf{I}(V)$ 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 7.22. *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) *$(x_{i_1} + \mathsf{I}(V), \ldots, x_{i_r} + \mathsf{I}(V))$ ist algebraisch unabhängig.*

Beweis: (1)⇒(2): Nehmen wir an, $p \in k[t_1, \ldots, t_r] \setminus \{0\}$ ist so, dass $p(x_{i_1}, \ldots, x_{i_r}) \in \mathsf{I}(V)$. Sei $q(x_1, \ldots, x_n) := p(x_{i_1}, \ldots, x_{i_r})$. Dann liegt q in $\mathsf{I}(V)$, also liegen alle Elemente von P in $\mathsf{V}(p)$. Da k unendlich ist, gilt $\mathsf{V}(p) \neq k^r$. (2)⇒(1): Nehmen wir an, P ist nicht Zariski-dicht. Dann ist P in einer Varietät $\mathsf{V}(f)$ 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 $g \in \mathsf{I}(V)$. Also sind $(x_{i_1} + \mathsf{I}(V), \ldots, x_{i_r} + \mathsf{I}(V))$ algebraisch abhängig. □

Lemma 7.23. *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 7.24. *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 7.23 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 5.23, 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 5.22 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 5.25, 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 5.23 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 5.25 auch $s_1 \leq s$. □

Wenn V irreduzibel ist, so ist das Ideal $\mathsf{I}(V)$ nach Satz 7.16 prim. Dann ist $k[x_1, \ldots, x_n]/\mathsf{I}(V)$ ein Integritätsbereich. Nach Satz 7.24 ist die Dimension von V genau der Transzendenzgrad dieses Integritätsbereiches über k.

Satz 7.25. *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 $\mathsf{I}(V) = \bigcap\{\mathsf{I}(V_i) \mid i \in \{1, \ldots, m\}\}$. Nach Lemma 7.23 gibt es für eine algebraisch unabhängige Menge der Form $\{x_h + \mathsf{I}(V) \mid h \in H\}$ einen Index $i \in \{1, \ldots, m\}$, sodass auch $\{x_h + \mathsf{I}(V_i) \mid h \in H\}$ algebraisch unabhängig ist. □

Satz 7.26. *Sei k ein Körper, und seien $V, W \subseteq k^n$ irreduzible Varietäten. Dann gilt:*

(1) $\dim(V) \leq n$.
(2) *Wenn $V \neq \emptyset$, $V \subseteq W$ und $V \neq W$, so gilt* $\dim(V) < \dim(W)$.

Beweis: Sei $R := k[x_1, \ldots, x_n]$, $P_1 := \mathsf{I}(W)$ und $P_2 := \mathsf{I}(V)$. 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

$$p^j \left(p^{n-j} + \sum_{i=j}^{n-1} f_i(y_1, \ldots, y_r)\, p^{i-j}\right) \in P_1.$$

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 5.23 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 7.27. *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 $\dim(\mathsf{V}(\mathsf{I}(P))) \leq \dim(V)$.

Satz 7.28. *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 7.29. *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 $k[x_1, \ldots, x_n]/\mathsf{I}(W)$ hat endliche Dimension über k.*

Übungsaufgaben 7.30

(1) Sei k ein Körper, $n \in \mathbb{N}$, und sei $V \subseteq k^n$ eine Varietät. Wir nehmen an, dass der Ring $k[x_1, \ldots, x_n]/\mathsf{I}(V)$ algebraisch über k ist. Zeigen Sie, dass V nur endlich viele Punkte enthält. *Hinweis:* Beispiele sind $n = 1, V = \mathsf{V}(x^2 - 5x + 6)$ oder $n = 2, V = \mathsf{V}(x^2 - 5x + 6, y^3 + 5y^3x^4 + x^8)$.

(2) Berechnen Sie jeweils die Dimension der folgenden Varietäten $\mathsf{V}(I)$ 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) $I = \langle xy^2 - x^2z\rangle$.

Satz 7.31. *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 $I := \mathsf{I}(W)$, 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 5.38 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 $\mathsf{V}(I)$ mit $A_s \cdot \boldsymbol{v} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$.

Wir zeigen nun, dass es nur endlich viele Punkte $\boldsymbol{v} \in \mathsf{V}(I)$ 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 $\mathsf{I}(V)$. 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

[Ax68] James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR 0229613 (37 #5187)

[Buc70] B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.

[CLO92] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992, An introduction to computational algebraic geometry and commutative algebra.

[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.

[Gar86] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, Cambridge, 1986.

[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.

[Mac01] D. Maclagan, *Antichains of monomial ideals are finite*, Proc. Amer. Math. Soc. **129** (2001), no. 6, 1609–1615 (electronic).

[Ram29] F. P. Ramsey, *On a problem of formal logic*, Proceedings London Mathematical Society (2) **30** (1929), 264–286.

[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.

Stichwortverzeichnis