Notizen zu den ersten Kapiteln der Vorlesung

Kommutative Algebra und algebraische Geometrie

Entwurf

Sommersemester 2009

Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

Version 22. April 2009

Adresse:
Univ.-Doz. Dr. Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz
4040 Linz
e-mail: erhard.aichinger@jku.at
Version 22.4.2009

Inhaltsverzeichnis

Kapitel 1. Mengenlehre 1
1. Geordnete Mengen 1

Kapitel 2. Kommutative Ringe mit Eins 3
1. Kommutative Ringe mit Eins 3
2. Ideale 4
3. Faktorringe 6

Kapitel 3. Teilbarkeit in kommutativen Ringen 9
1. Definitionen 9
2. Faktorielle Integritätsbereiche 9
3. Zerlegung in irreduzible Elemente 11
4. Eine Anwendung auf die Zahlentheorie 14
5. Teilbarkeit in Polynomringen 16
6. Größter gemeinsamer Teiler 20

Kapitel 4. Multiplikative Idealtheorie in kommutativen Ringen 23
1. Noethersche Ringe 23
2. Summen, Produkte und Quotienten von Idealen 26
3. Primär- und Primideale 27
4. Zerlegung von Idealen 27
5. Eindeutigkeit der Zerlegung in primäre Ideale 29

Kapitel 5. Ringerweiterungen 35
1. Determinanten 35
2. Ganze Erweiterungen 37
3. Algebraische Erweiterungen 42
4. Noethersche Normalisierung 46
5. Der Hilbertsche Nullstellensatz 49

Literaturverzeichnis 53

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 $y \leq x$.

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. □

DEFINITION 2.6. 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 $I = \langle A \rangle$.

SATZ 2.7. *Sei R ein kommutativer Ring mit Eins, und sei $I(R)$ die Menge der Ideale von R. Dann sind äquivalent:*

(1) $(I(R), \subseteq)$ *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). (1)⇒(2): 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 $(I(R), \subseteq)$ die (ACC). □

Definition 2.8. Sei R ein kommutativer Ring mit Eins. R heißt *noethersch*, wenn jedes Ideal von R endlich erzeugt ist.

Definition 2.9. 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 2.10. *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 $r_2 \cdot s_2 = (r_1 + i) \cdot (s_1 + j) = r_1 \cdot s_1 + r_1 \cdot j + i \cdot s_1 + i\dot{j}$. Für $i' := r_1 \cdot j + i \cdot s_1 + i\dot{j}$ 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 $(r+I) \odot (s+I)$.

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. □

2. Faktorielle Integritätsbereiche

DEFINITION 3.4. 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 3.5. *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 3.6. 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 3.7 (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 3.8. *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 3.9 (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 3.7 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 3.8 gilt dann $\alpha = \beta$. □

Satz 3.10. *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 3.8 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 3.5. □

DEFINITION 3.11. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

SATZ 3.12. *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 3.13. *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 3.14. *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 $\{\lambda_1 \begin{pmatrix} c \\ d \end{pmatrix} + \lambda_2 \begin{pmatrix} -d \\ c \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{Z}\}$, dessen Abstand von $\begin{pmatrix} a \\ b \end{pmatrix}$ höchstens $\frac{1}{\sqrt{2}}\sqrt{c^2 + d^2}$ ist. Sei $\begin{pmatrix} c' \\ d' \end{pmatrix}$ 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). $\square$

Wir beweisen nun Satz 3.13:

Beweis von Satz 3.13: 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. $\square$

5. Teilbarkeit in Polynomringen

DEFINITION 3.15. 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 3.16 (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 3.17. *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 3.18. *Sei R ein faktorieller Integritätsbereich, und 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 $p \in R \backslash \{0\}$, 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 3.19. *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 3.18 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 3.18 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 3.20. *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 3.17 verwenden, um $g_1 \in R[x]$ und $r \in R$ zu erhalten, sodass $g = r\,g_1$. $1\,f|r\,g_1$ in $Q(R)[x]$. Nach Satz 3.19 gilt also $f|g_1$ in $R[x]$. Dann gilt natürlich auch $f|g$ in $R[x]$. □

LEMMA 3.21. *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 3.18 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 3.22. *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 3.19 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 3.19 $r|st$. 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 3.21 irreduzibel in $Q(R)[x]$. Da $f|a_1b_1$ 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 3.19 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 3.10 ist $R[x]$ damit faktoriell. □

KOROLLAR 3.23. *Sei R ein faktorieller Integritätsbereich und $k \in \mathbb{N}$. Dann ist $R[x_1, \ldots, x_k]$ faktoriell.*

6. Größter gemeinsamer Teiler

DEFINITION 3.24. 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 3.25. *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 3.8 eine Zerlegung von d. □

LEMMA 3.26. *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 3.27. *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 3.19 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 3.19, 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 3.19 und erhalten $d'_2|d_2$ in $R[x]$. Somit gilt $d'_1 d'_2|d_1 d_2$ in $R[x]$, und somit $d'|d$ in $R[x]$. □

SATZ 3.28. *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.

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 3.29. *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 3.20 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 $Q(R)[x]$. □

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 2.7 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 $jx^n + q \in I$. Da dann auch $(i+j)\,x^n + (p+q)$ in I liegt, gilt $i + j \in I_n$. Ebenso gilt $(r\,x^0) \cdot (i\,x^n + p) \in I$. Folglich gilt $ri\,x^n + r\,p \in I$. Daher gilt $ri \in I_n$. I_n ist also wirklich ein Ideal von R.

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

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

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

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

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

so wählen, dass

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

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

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

gibt. Wir bilden nun die Menge

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

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

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

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

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

DEFINITION 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 $(A : b)_R$.

LEMMA 4.11. *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 4.12. 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 4.13. 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 4.14. 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 4.15. *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 4.16. *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 4.17. 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 4.18. *Sei R ein noetherscher kommutativer Ring mit Eins. Dann ist jedes Ideal von R Durchschnitt endlich vieler schnitt-irreduzibler Ideale.*

SATZ 4.19. *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. □

Satz 4.20. *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 4.21. 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 4.22 (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 4.23. *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 4.24. *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 4.25. *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 4.24 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 4.24 $m = 1$, 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 $\{\sqrt{K_j} \mid j \in \{1, \ldots, n\}\}$ liegt. Es gilt nun:

(5.3) Für alle $i \in \{1, \ldots, m\}$ 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 $j \in \{1, \ldots, n\}$ 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 $\{\sqrt{K_j} \mid j \in \{1, \ldots, n\}\}$ liegt. Das beweist (5.4). Es gilt

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

also

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

und folglich

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

Nach Proposition 4.23 gilt daher

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

Also gilt $\bigcap\{Q_i \mid i \in \{1, \ldots, m\} \setminus \{k\}\} = I \subseteq Q_k$, 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 $k \in \{2, \ldots, m\}$ und ein $l \in \{1, \ldots, n\}$ gibt, sodass $P = \sqrt{Q_k} = \sqrt{K_l}$. Wir zeigen nun, dass für alle $i \in \{1, \ldots, m\}$ und alle $j \in \{1, \ldots, n\}$ 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 4.23 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 4.26 (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 4.27 (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 4.25 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* $i, j \in \{1, \ldots, n\}$ *mit* $i \neq j$ *gibt, sodass* $a_i = a_j$*, so gilt*

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

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

Satz 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*

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

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

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

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

Beweis von Satz 5.3: Für $i \in \{1, \ldots, n\}$ 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

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

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

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

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

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

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

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

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. □

Satz 5.11. *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 5.12. 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.

LEMMA 5.13. *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 5.14. *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 5.13 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 5.15. *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. □

Definition 5.16. 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 5.17. 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 5.18. *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 5.19. *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 $\mathbb{R}[\![i]\!] = \mathbb{C}$.

Satz 5.20. *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 5.19 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 5.19 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 5.19 $x_{\pi(j)}$ 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 $r \in \{i, \dots, m\} \setminus \{i, j\}$. Nun ist also $x_{\sigma(i)}$ algebraisch über

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

Wegen (3.2) ist B algebraisch über $A[\![w_1, \dots, w_{i-1}, x_{\sigma(i+1)}, \dots, x_{\sigma(m)}]\!][\![x_{\sigma(i)}]\!]$, und daher erst recht über $A[\![w_1, \dots, w_{i-1}, w_i, x_{\sigma(i+1)}, \dots, x_{\sigma(m)}]\!][\![x_{\sigma(i)}]\!] = C[\![x_{\sigma(i)}]\!]$. Da wegen Satz 5.15 der Integritätsbereich $C[\![x_{\sigma(i)}]\!]$ algebraisch über C ist, folgt nach Proposition 5.14, dass B algebraisch über C ist. Somit leistet $\sigma|_{\{i+1,\dots,m\}}$ das Gewünschte. □

KOROLLAR 5.21. *Seien A, B Integritätsbereiche mit $A \leq B$, und sei $(x_1, \dots, x_m)$ eine Transzendenzbasis von B über A. Sei $(w_1, \dots, w_r)$ 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 5.20) erhalten wir, dass B algebraisch über $A[\![w_1, \dots, w_m]\!]$ ist. Also ist w_{m+1} algebraisch über $A[\![w_1, \dots, w_m]\!]$. Nach Satz 5.19 ist $(w_1, \dots, w_m, w_{m+1})$ dann algebraisch abhängig. □

DEFINITION 5.22. 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 5.23. *Sei k ein unendlicher Körper, $n \in \mathbb{N}$, und sei $p \in k[t_1, \dots, t_n]$ mit $p \neq 0$. Dann gibt es ein $\mathbf{v} \in k^n$ mit $\overline{p}(\mathbf{v}) \neq 0$.*

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 $l := \deg_{t_n}(p)$

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

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 5.24. *Sei k ein Körper, und sei B ein kommutativer Ring mit Eins mit $k \leq B$. Sei $n \in \mathbb{N}$, $\mathbf{x} = (x_1, \ldots, x_n)$ 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 $k[\![\overline{f_2}(\mathbf{x}), \ldots, \overline{f_n}(\mathbf{x})]\!]$,*
(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 $k[\![\overline{f_2}(\mathbf{x}), \ldots, \overline{f_n}(\mathbf{x}), x_1]\!] = B$.)

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

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

Das Polynom $K \in k[a_2,\ldots,a_n]$ ist nicht das Nullpolynom, also gibt es nach Lemma 5.23 ein $(\alpha_2,\ldots,\alpha_n) \in k^{n-1}$, sodass $\overline{K}(\alpha_2,\ldots,\alpha_n) \neq 0$. Das Polynom $q := q'(t_1,\ldots,t_n,\alpha_2,\ldots,\alpha_n)$ ist also ein Polynom in $k[t_1,\ldots,t_n]$, das von der Form $b_N t_1^N + \sum_{i=0}^{N-1} b_i(t_2,\ldots,t_n)t_1^i$ ist.

Es gilt

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

Das bedeutet

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

Also ist x_1 ganz über $k[\![x_2 - \alpha_2 x_1, \ldots, x_n - \alpha_n x_1]\!]$. 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 $d > \max\{i_j \mid i \in I, j \in \{1,\ldots,n\}\}$ und $f_j := t_j - t_1^{d^{j-1}}$ wählen. □

Satz 5.25 (Noethersche Normalisierung). *Sei k ein Körper, sei B ein kommutativer Ring mit Eins mit $k \leq B$, und seien $x_1,\ldots,x_n \in B$ so, dass $k[\![x_1,\ldots,x_n]\!] = B$. Dann gibt es $r \in \{0,\ldots,n\}$ und $f_1,\ldots,f_n \in k[t_1,\ldots,t_n]$, sodass für $y_j := \overline{f_j}(x_1,\ldots,x_n)$ gilt:*

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

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

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

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

Daher gibt es nach Lemma 5.24 $f_1,\ldots,f_{n-1} \in k[t_1,\ldots,t_n]$, sodass x_n ganz über $k[\![\overline{f_1}(x_1,\ldots,x_n),\ldots,\overline{f_{n-1}}(x_1,\ldots,x_n)]\!]$ ist, und

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

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

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

ist

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

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

Da x_n ganz über

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

ist, gilt:

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

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

5. Der Hilbertsche Nullstellensatz

Satz 5.26 (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 $\mathbf{x} \in K^n$, sodass für alle $f \in I$ gilt: $\overline{f}(\mathbf{x}) = 0$.*

Beweis: Sei M ein maximales Ideal von $k[t_1, \ldots, t_n]$ mit $I \subseteq M \neq k[\mathbf{t}]$, und sei $K := k[\mathbf{t}]/M$. 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 5.27 (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 $\mathbf{x} \in k^n$ gilt:*

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

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

Satz 5.28 (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) $g \in \sqrt{\langle f_1, \ldots, f_s \rangle_{k[\mathbf{t}]}}$.
(2) $1 \in \langle f_1, \ldots, f_s, g \cdot u - 1 \rangle_{k[\mathbf{t}, u]}$.

Beweis: (1)⇒(2). Sei $I := \langle f_1, \ldots, f_s, g \cdot u - 1 \rangle_{k[\mathbf{t}, u]}$. 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 $a_1, \ldots, a_s, b \in k[\mathbf{t}, u]$, 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 5.29 (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 $\mathbf{x} \in k^n$ mit $\overline{f_1}(\mathbf{x}) = \cdots = \overline{f_s}(\mathbf{x}) = 0$ gilt, dass $g(\mathbf{x}) = 0$, so liegt g im Radikal von $\langle f_1, \ldots, f_s\rangle_{k[\mathbf{t}]}$.*

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 $1 \in \langle f_1, \ldots, f_s, g \cdot u - 1\rangle_{k[\mathbf{t},u]}$. Also liegt nach dem Satz von Rabinowitsch (Satz 5.28) g im Radikal von $\langle f_1, \ldots, f_s\rangle_{k[\mathbf{t}]}$. □

Literaturverzeichnis

[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.

[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.