Computational Algebraic Geometry

Algebraische Geometrie auf dem Computer

Teil 1

Joachim Wehler

Ludwig-Maximilians-Universität München, Sommersemester 2005

Version 2.0

1 Einleitung

Zielsetzung

Wie viele Gebiete der reinen Mathematik hat auch die Algebraische Geometrie ihren Ursprung in anschaulich gegebenen Objekten. Ausgangspunkt der Algebraischen Geometrie ist das Studium der Nullstellenmengen von Polynomen mit Mitteln der Kommutativen Algebra. Diese geometrischen Objekte heißen affine oder projektive *Varietäten*. Sie lassen sich mit algebraischen Methoden aus der Theorie der Polynomringe behandelt.

Im 20. Jahrhundert hat die Algebraische Geometrie durch die Ideen von Grothendieck eine Neufundierung und zugleich beträchtliche Verallgemeinerung erfahren. Dabei wurde es möglich, nun umgekehrt sehr abstrakte algebraische Sachverhalte in geometrische Aussagen zu übersetzen. Diese gehen weit über die Theorie der Varietäten hinaus. Beispielsweise lassen sich im Begriff des affinen *Schemas* die Primideale eines beliebigen kommutativen Ringes als die Punkte eines topologischen Raumes auffassen und damit geometrisch veranschaulichen. Und das ist nur der Anfang der Übersetzung von Kommutativer Algebra in Algebraische Geometrie.

Mathematische Algorithmen und die Leistungsfähigkeit der Computer sind auf einem Stand, daß heute jeder auch subtile Beispiele der Algebraischen Geometrie auf seinem Notebook berechnen kann. Die Komplexität der Beispiele, die ein Mathematiker am Schreibtisch auf diese Art explizit durchrechnen kann, hat sich gegenüber der Zeit vor zwanzig Jahren um Größenordnungen gesteigert. Diese Steigerung der Rechenfähigkeit des Einzelnen zieht eine entsprechende Erweiterung seines mathematischen Horizontes auch im theoretischen Bereich nach sich.

Diese Vorlesung richtet sich an graduierte Studenten der Mathematik. Vorausgesetzt werden Grundkenntnisse der Algebra, also die Vertrautheit mit Begriffen wie Körper, Polynomring und Ideal. Ziel dieser Vorlesung ist es,

- ausgewählte Begriffe und Sätze der Algebraischen Geometrie an Beispielen vorzustellen
- und diese Beispiele mit Toolunterstützung explizit vorzurechnen.

Das Schwergewicht liegt also nicht auf dem Beweis der mathematischen Sätze, sondern auf der Illustration eines Satzes an nicht-trivialen Beispielen. Die vorliegende Vorlesung ersetzt nicht die „klassische" Vorlesung über Kommutative Algebra oder Algebraische Geometrie, sondern ergänzt sie.

Dieses Skript erweitert die mündlich gehaltene 2-stündige Vorlesung um die meisten Beweise und einige hierfür benötige Hilfssätze, sowie um einen Ausblick auf die Zahlentheorie und die Theorie der Riemannschen Flächen.

Kurven, Flächen, Hyperebenenschnitte

Die Kurven und Flächen der Algebraischen Geometrie sind Nullstellengebilde von einem oder mehreren Polynomen. Reelle ebene Kurven und Flächen im 3-dimensionalen Raum lassen sich leicht mit dem Tool „Surf“ zeichnen. Sie sind die Nullstellenmengen von einem Polynom der Art

$$f \in \boldsymbol{R}[X,Y] \text{ oder } f \in \boldsymbol{R}[X,Y,Z].$$

1.1 Toolbeispiel (Ebenes Achsenkreuz)

- Curves/PlaneCoordinates

Ebenes Koordinatenkreuz =

$$\{(x,y) \in \boldsymbol{R}^2 : x \cdot y = 0\} = \{(x,y) \in \boldsymbol{R}^2 : x = 0\} \cup \{(x,y) \in \boldsymbol{R}^2 : y = 0\}$$

1.2 Toolbeispiel (Kurven 2. Grades in der Ebene)

- Curves/Ellipse

$$\text{Ellipse} = \left\{ (x,y) \in \boldsymbol{R}^2 : \frac{x^2}{a^2} + \frac{y^2}{b^2} - c^2 = 0 \right\},\ a = 2, b = 1, c = \sqrt{10}$$

- Curves/Hyperbola

$$\text{Hyperbel} = \{(x,y) \in \boldsymbol{R}^2 : x \cdot y - 3 = 0\}$$

- Curves/QuadricCurveDeformation

$$\text{Quadratische Kurve} = \{(x,y) \in \boldsymbol{R}^2 : x^2 + a \cdot y^2 - 1 = 0\},$$

mit Parameter $a \in [-2, +2]$.

1.3 Toolbeispiel (Kurven 3. Grades in der Ebene)

- Curves/CubicCurves

$$\text{Elliptische Kurve} = \{(x,y) \in \boldsymbol{R}^2 : y^2 - x^3 - 1 = 0\}$$

$$\text{Neil Parabel} = \{(x,y) \in \boldsymbol{R}^2 : y^2 - x^3 = 0\}$$

$$\text{Elliptische Kurve} = \{(x,y) \in \boldsymbol{R}^2 : y^2 - x^2 \cdot (x-1) = 0\}$$

- Curves/CubicCurveDefomation

$$\text{Kubische Kurve} = \{(x,y) \in \boldsymbol{R}^2 : y^2 - (x^3 + a \cdot x + a) = 0\},$$

mit Parameter $a \in [-1.2, +1.2]$.

1.4 Toolbeispiel (Flächen 2. Grades im 3-dimensionalen Raum)

- Surfaces/SmoothQuadric

$$\text{Nicht-singuläre Quadrik} = \{(x,y,z) \in \boldsymbol{R}^3 : x^2 + y^2 - z^2 - 2 = 0\}$$

- Surfaces/SingularQuadric

$$\text{Quadratischer Kegel} = \{(x,y,z) \in \boldsymbol{R}^3 : x^2 + y^2 - z^2 = 0\}$$

1.5 **Toolbeispiel** *(Flächen 3. Grades im 3-dimensionalen Raum)*

- Surfaces/SmoothFermatSurface

$$\text{Fermat Fläche} = \left\{ (x, y, z) \in \boldsymbol{R}^3 : x^3 + y^3 - z^3 - 10 = 0 \right\}$$

- Surfaces/WhitneyUmbrella

$$\text{Whitney-Umbrella} = \left\{ (x, y, z) \in \boldsymbol{R}^3 : x^2 \cdot y - z^2 = 0 \right\}$$

Alle Punkte auf der y-Achse sind singulär.

1.6 **Toolbeispiel** *(Hyperebenenschnitte von Flächen im 3-dimensionalen Raum)*

- Surfaces/FamilyOfHyperbolas

Hyperbel als Hyperebenenschnitt einer Fläche:

$$\text{Hyperbel} = \left\{ (x, y, z) \in \boldsymbol{R}^3 : x \cdot y \cdot z - 2 = 0 \right\} \cap H_c$$

mit

$$H_c = \left\{ (x, y, z) \in \boldsymbol{R}^3 : z - c = 0 \right\},\ c \in [\, 0, 0.5 \,]$$

- Surfaces/FamilyOfQuadricCurves

Allgemeine Kurve 2. Grades als Hyperebenenschnitt einer Fläche:

$$\text{Quadrik} = \left\{ (x, y, z) \in \boldsymbol{R}^3 : x^2 + z \cdot y^2 - 1 = 0 \right\} \cap H_c$$

mit

$$H_c = \left\{ (x, y, z) \in \boldsymbol{R}^3 : z - c = 0 \right\},\ c \in \{ -1, 0, 1, 2 \}$$

- Surfaces/FamilyOfCubicCurves

Kurven 3. Grades als Hyperebenenschnitt einer Fläche:

$$\text{Kubische Kurve} = \left\{ (x, y, z) \in \boldsymbol{R}^3 : y^2 - x^2 \cdot (\, x - z \,) = 0 \right\} \cap H_c$$

mit

$$H_c = \left\{ (x, y, z) \in \boldsymbol{R}^3 : z - c = 0 \right\},\ c \in \{ -6, -4, 0, 3 \}$$

- Surfaces/BlowUp

Ausschöpfung einer Fläche durch Hyperebenenschnitte aus Geraden:

$$\text{Gerade} = \left\{ (x, y, z) \in \boldsymbol{R}^3 : x \cdot z - y = 0 \right\} \cap H_c$$

mit

$$H_c = \left\{ (x, y, z) \in \boldsymbol{R}^3 : z - c = 0 \right\},\ c \in [\, -3, 3 \,]$$

2 Affine Varietäten und affine Algebren

Varietäten sind die Nullstellenmengen von einem oder mehreren Polynomen. Als Teilmengen eines Zahlenraumes sind Varietäten anschaulich gegebene *geometrische* Objekte.

Andererseits entspringen aus einer Varietät eine Reihe *algebraischer* Objekte. Betrachtet man z.B. alle Polynome, die auf der Varietät verschwinden, so hat man der Varietät ein Ideal in einem Polynomring zugeordnet.

Nun läßt sich dieser Weg auch in der umgekehrten Richtung gehen: Man ordnet einem Ideal eines Polynomringes das gemeinsame Nullstellengebilde aller Elemente des Ideals zu und erhält so eine Varietät.

Dieses Wechselspiel zwischen Nullstellengebilden als geometrischen Objekten und Idealen als algebraischen Objekten ist charakteristisch für die Algebraische Geometrie.

Dabei treten zwei Körper als freie Parameter der Theorie auf: Ein Grundkörper k für die Koeffizienten der Polynome und ein Erweiterungskörper K für die Koordinaten der Nullstellen:

$$k \subset K .$$

Wir werden in diesem Kapitel stets fordern, daß K der algebraische Abschluß von k ist:

$$K = \overline{k} .$$

Eine typische Situation ist der Fall

$$k = \boldsymbol{Q} \text{ und } K = \overline{\boldsymbol{Q}} .$$

Hier betrachten wir Polynome mit rationalen Koeffizienten und studieren ihre Nullstellen als Punkte mit Koordinaten in den algebraischen Zahlen.

Eine andere Variante - näher an der Funktionentheorie - ist der Fall

$$k = K = \boldsymbol{C} .$$

Man studiert die komplexen Nullstellen von Polynomen mit komplexen Koeffizienten.

Bei Fragen aus der Zahlentheorie spielen eine wichtige Rolle die Fälle

$$\mathrm{k} = \boldsymbol{F}_p \text{ und } \mathrm{K} = \overline{\boldsymbol{F}_p}, \ p \text{ eine Primzahl,}$$

mit dem endlichen Körper $\boldsymbol{F}_p$ mit p Elementen.

In diesem Kapitel sei k ein Körper und $K \supset k$ sein algebraischer Abschluß. Wir bezeichnen mit

$$\boldsymbol{A}^n = \boldsymbol{A}^n(K) := K^n, n \in \boldsymbol{N} ,$$

den n-dimensionalen K-Vektorraum. Er heißt in der Algebraischen Geometrie der *n-dimensionale affine Raum mit Koordinaten aus* K. Die Bezeichnung macht deutlich, daß der Nullpunkt dieses Raumes in der Algebraischen Geometrie keine ausgezeichnete Rolle spielt.

Alle Ringe werden als kommutative Ringe mit 1-Element vorausgesetzt.

Varietäten und Koordinatenringe

Ausgehend von der Geometrie definieren wir in diesem Abschnitt algebraische Varietäten als die Nullstellenmengen von Polynomen.

2.1 Definition (Affine Varietät und reguläre Abbildung)

i) Eine *affine k-Varietät* X ist die Nullstellenmenge einer endlichen oder unendlichen Menge von Polynomen

$$f_j \in k[X_1, ..., X_n],\ j \in J,$$

im affinen Raum $\boldsymbol{A}^n(K)$. Man schreibt

$$X = \{ x \in \boldsymbol{A}^n(K) : f_j(x) = 0 \text{ für alle } j \in J \}.$$

Der Körper k heißt *Definitionskörper*, der Körper K heißt *Koordinatenkörper* von X. Affine Varietäten, die Nullstellengebilde eines einzigen, nicht konstanten Polynoms sind, heißen *Hyperflächen* bzw. im Falle eines linearen Polynoms *Hyperebenen*.

ii) Eine *k-reguläre Abbildung* zwischen zwei affinen k-Varietäten $X \subset \boldsymbol{A}^n(K)$ und $Y \subset \boldsymbol{A}^m(K)$ ist eine Abbildung

$$g : X \longrightarrow Y,$$

die durch Polynome mit Koeffizienten aus dem Definitionskörper k gegeben werden kann, d.h. es existieren Polynome

$$g_1, ..., g_m \in k[X_1, ..., X_n]$$

mit

$$g(x) = (g_1(x), ..., g_m(x)) \in Y \text{ für alle } x \in X.$$

Eine k-reguläre Abbildung heißt *k-Isomorphimus*, wenn sie eine k-reguläre Abbildung als Umkehrabbildung hat.

Hinweis. [Har1977] verwendet statt des Begriffes „affine Varietät“ den Begriff „algebraische Teilmenge des $\boldsymbol{A}^n$“. Eine affin-algebraische Varietät im Sinne von [Har1977] ist zusätzlich *irreduzibel*; siehe Definition 3.20.

2.2 Bemerkung (Ideal und Varietät)

i) Eine affine *k-Varietät* ist einerseits eine Teilmenge des $\boldsymbol{A}^n(K)$. Die Punkte dieser Teilmenge haben ihre Koordinaten in dem algebraisch-abgeschlossenen Körper K. Der Definitionskörper k gehört jedoch auch zur Definition.

Durch die explizite Angabe des Grundkörpers k wird ausgedrückt, daß man sich dieses Nullstellengebilde durch Polynome definiert denkt, die über einem Teilkörper k definiert sind. k-reguläre Abbildungen zwischen k-Varietäten müssen durch Polynome gegeben werden, die ebenfalls über k definiert sind.

ii) Zusammen mit den Polynomen $f_j \in k[X_1, ..., X_n]$, $j \in J$, welche eine affine Varietät X definieren, verschwinden auf X auch alle Polynome aus dem von den definierenden Polynomen erzeugten Ideal

$$I := \langle f_j : j \in J \rangle \subset k[X_1,..., X_n],$$

es gilt also

$$X = \{ x \in \boldsymbol{A}^n(K) : f(x) = 0 \text{ für alle } f \in I \}.$$

Jedes Ideal $I \subset k[X_1,..., X_n]$ ist nach dem Hilbertschen Basissatz *endlich* erzeugt, d.h. es gibt endlich viele Polynome

$$g_1,..., g_k \in k[X_1, ..., X_n] \text{ mit } I = \langle g_1,..., g_k \rangle$$

([CLO1997] Chap. 2, §5). Sie können sukzessive aus der vorgegebenen Familie $(f_j)_{j \in J}$ ausgewählt werden. Daher kann das Nullstellengebilde einer unendlichen Menge von Polynomen auch bereits durch endlich viele Polynome beschrieben werden.

iii) Allgemein ordnet man jedem Ideal

$$I \subset k[X_1,..., X_n]$$

eine affine k-Varietät zu, die man als

$$Var(I) := \{ x \in \boldsymbol{A}^n(K) : f(x) = 0 \text{ für alle } f \in I \}$$

bezeichnet. Dabei kann es verschiedene Ideale geben

$$I_1 \neq I_2 \subset k[X_1,..., X_n],$$

welche dieselbe Varietät

$$X := Var(I_1) = Var(I_2) \subset \boldsymbol{A}^n(K)$$

definieren. Unter allen diesen Idealen gibt es ein größtes Ideal, das *Verschwindungsideal* von X:

$$Id(X) := \langle f \in k[X_1,..., X_n] : f(x) = 0 \text{ für alle } x \in X \rangle.$$

iv) Eine reguläre Abbildung zwischen zwei affinen Varietäten wird stets *global* durch einen einzigen Satz von Polynomen repräsentiert, d.h. sie wird von einer regulären Abbildung

$$\boldsymbol{A}^n(K) \longrightarrow \boldsymbol{A}^m(K)$$

zwischen den einbettenden affinen Räumen induziert.

Das Verschwindungsideal einer affinen Varietät hat die Eigenschaft:

$$f \in k[X_1,..., X_n] \text{ und } f^k \in Id(X) \text{ für ein } k \in \boldsymbol{N} \Rightarrow f \in Id(X).$$

2.3 Definition (Radikal)

Es sei $I \subset R$ ein Ideal in einem Ring R. Die Menge

$$\sqrt{I} := \{ f \in R : f^k \in I \text{ für ein } k \in \boldsymbol{N} \}.$$

ist ein Ideal und heißt das *Radikal* von I. Das Ideal I heißt *reduziert*, wenn

$$I = \sqrt{I}\ , \text{d.h. } f \in R \ \ and \ \ f^k \in I \ \text{ für ein } k \in \boldsymbol{N} \Rightarrow f \in I\ .$$

Der Ring R heißt *reduziert*, wenn sein Nullideal reduziert ist:

$$\langle\ 0\ \rangle = \sqrt{\langle\ 0\ \rangle}\ ,$$

d.h. wenn R keine *nilpotenten* Elemente enthält.

Das Verschwindungsideal einer affinen Varietät ist reduziert

$$Id(X) = \sqrt{Id(X)}\ .$$

Wir behandeln in den folgenden Beispielen einige der in Kapitel 1 gezeichneten Kurven und Flächen als reguläre Abbildungen. Es sei immer $k = \boldsymbol{Q}$ der Definitionskörper und $K = \boldsymbol{C}$ der Koordinatenkörper.

Toolbeispiel 2.4 zeigt, wie reguläre Abbildungen zwischen k-Varietäten für die Berechnung mit Tools wie Singular oder Macaulay2 aus der Sprache der Geometrie in die Sprache der Kommutativen Algebra zu übersetzen sind. Das Ergebnis sind Morphismen von k-Algebren.

2.4 Toolbeispiel (Neil Parabel)

ad Toolbeispiel 1.3, Neil Parabel.

Die Neil Parabel ist die affine Varietät

$$Z := \{\,(x, y) \in \boldsymbol{A}^2 : y^2 - x^3 = 0\,\}.$$

Die Projektion auf die x–Achse

$$pr_1 : \boldsymbol{A^2} \longrightarrow \boldsymbol{A^1},\ (x, y) \mapsto x$$

induziert eine reguläre Abbildung

$$g_1 : \boldsymbol{Z} \longrightarrow \boldsymbol{A^1}\ .$$

Diese ist surjektiv, aber nicht injektiv. Ebenso induziert die Projektion auf die y–Achse

$$pr_2 : \boldsymbol{A^2} \longrightarrow \boldsymbol{A^1},\ (x, y) \mapsto y$$

eine reguläre Abbildung

$$g_2 : \boldsymbol{Z} \longrightarrow \boldsymbol{A^1}\ .$$

Sie ist surjektiv, aber nicht injektiv.

Die Abbildung

$$g_3 : \boldsymbol{A^1} \longrightarrow \boldsymbol{A^2},\ g(t) = (t^2, t^3)$$

ist regulär. Sie bildet die affine Gerade $\boldsymbol{A^1}$ bijektiv auf die Neil Parabel

$$Z := \{\,(x, y) \in \boldsymbol{A}^2 : y^2 - x^3 = 0\,\}$$

ab. Die Umkehrabbildung

$$h : Z \longrightarrow \boldsymbol{A^1},\ h(x, y) = \begin{cases} \dfrac{y}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

ist allerdings nicht regulär. Daher ist die Abbildung

$$g_3 : \boldsymbol{A}^1 \longrightarrow Z$$

kein Isomorphismus affiner Varietäten. Wir werden in Toolbeispiel 3.14, Teil i) sehen, daß die affine Gerade und die Neil Parabel auch bzgl. keiner anderen regulären Abbildung isomorph sind.

Toolbeispiel Singular-Script

- RegularMap/NeilParabola

Reguläre Abbildungen werden in Singular und anderen Tools zur symbolischen Rechnung nicht als Abbildungen zwischen den affinen Räumen

$$g : \boldsymbol{A}^n(K) \longrightarrow \boldsymbol{A}^m(K),\ x = (x_1,...,x_n) \mapsto (g_1(x),...,g_m(x)),$$

definiert, sondern als kontravariante, k-lineare Abbildungen zwischen den Polynomringen über dem Definitionskörper

$$\varphi : k[Y_1,...,Y_m] \longrightarrow k[X_1,...,X_n],\ Y_i \mapsto g_i .$$

Der Ringmorphismus φ beschreibt den Rückzug der Koordinatenfunktionen von $\boldsymbol{A}^m(K)$ zu Funktionen auf $\boldsymbol{A}^n(K)$. Computertools wie Macaulay2 oder Singular verwenden die algebraische Darstellung von Varietäten durch ihre Koordinatenringe und repräsentieren einen Morphismus zwischen zwei Varietäten durch die induzierte Abbildung zwischen den Koordinatenringen. Für einen solchen Morphismus zwischen affinen k-Algebren sind als Input folgende Größen anzugeben:

- Ein Polynomring für den Definitionsbereich,
- ein Polynomring für den Wertebereich
- und diejenigen Polynome im Wertebereich, welche die Bilder der Variablen des Definitionsbereiches darstellen.

Die Projektion

$$pr_1 : \boldsymbol{A}^2 \longrightarrow \boldsymbol{A}^1,\ (x, y) \mapsto x$$

wird also als Ringmorphismus

$$k[T] \longrightarrow k[X,Y],\ T \mapsto X ,$$

beschrieben und die Parametrisierung

$$\boldsymbol{A}^1 \longrightarrow \boldsymbol{A}^2,\ g(t) = (t^2, t^3)$$

als Ringmorphismus

$$k[X,Y] \longrightarrow k[T],\ X \mapsto T^2, Y \mapsto T^3 .$$

Die Projektion affiner Räume pr_1 induziert durch Komposition mit der Inklusion der Varietät die reguläre Abbildung

$$g_1 = \left[Z \xrightarrow{\subset} \boldsymbol{A}^2 \xrightarrow{pr_1} \boldsymbol{A}^1\right].$$

Kontravariant wird diese Abbildung auf dem Niveau der Polynomringe durch die Komposition mit der Quotientenabbildung beschrieben:

$$\varphi_1 = \left[k[T] \longrightarrow k[X,Y] \longrightarrow k[X,Y] \Big/ \left\langle Y^2 - X^3 \right\rangle \right].$$

Man hat die Isomorphie

$$k[X,Y] \Big/ \left\langle Y^2 - X^3 \right\rangle \xrightarrow{\cong} k\left[U^2, U^3\right],\ X \mapsto U^2, Y \mapsto U^3.$$

Daher wir die k -reguläre Abbildung

$$g_1 : Z \longrightarrow \boldsymbol{A}^1, (x.y) \mapsto x,$$

kontravariant durch den Morphismus von k -Algebren

$$k[T] \xrightarrow{\cong} k\left[U^2, U^3\right], T \mapsto U^2$$

beschrieben. Die k -reguläre Abbildung

$$g_3 : \boldsymbol{A}^1 \longrightarrow Z, t \mapsto \left(t^2, t^3\right),$$

wird kontravariant als Morphismus von k -Algebren durch die Inklusion

$$\varphi_3 : k\left[U^2, U^3\right] \xrightarrow{\subset} k[U]$$

beschrieben.

Das Beispiel wirft folgende Fragen auf:

- Was bedeuten die algebraischen Eigenschaften der Injektivität bzw. Surjektivität des zugehörigen Morphismus von k -Algebren für die geometrischen Eigenschaften der regulären Abbildung? Siehe Satz 2.16.
- Wie ist die Dimension einer Varietät definiert, wie berechnet man sie?
- Wie sind die Singularitäten einer Varietät definiert, wie berechnet man sie?

Toolbeispiel 2.5 behandelt eine reguläre Abbildung, die nicht endlich ist.

2.5 Toolbeispiel (Hyperbel)

ad Toolbeispiel 1.2, Hyperbel.

Die erste Projektion

$$pr_1 : \boldsymbol{A}^2 \longrightarrow \boldsymbol{A}^1, (x, y) \mapsto x$$

der affinen Ebene auf die affine Gerade induziert eine reguläre Abbildung

$$g : Z \longrightarrow \boldsymbol{A}^1$$

der Hyperbel

$$Z := \left\{ (x, y) \in \boldsymbol{A}^2 : x \cdot y - 1 = 0 \right\}.$$

Das Bild der regulären Abbildung

$$g(Z) = \boldsymbol{A}^1 - 0 \subset \boldsymbol{A}^1$$

ist keine affine Varietät: Denn jedes Polynom, das auf $\boldsymbol{A}^1 - 0$ verschwindet, verschwindet auch im Nullpunkt. In diesem Beispiel gilt für den Quotienten

$$k[X,Y]/\langle X\cdot Y-1\rangle \xrightarrow{\cong} k\left[U,\frac{1}{U}\right],\ X\mapsto U, Y\mapsto \frac{1}{U}.$$

Die von der Projektion auf die x–Achse induzierte reguläre Abbildung wird kontravariant durch den Ringmorphismus

$$k[U] \xrightarrow{\subset} k\left[U,\frac{1}{U}\right]$$

beschrieben. Faßt man vermöge dieser Abbildung den Wertebereich $k\left[U,\frac{1}{U}\right]$ als $k[U]$ -Modul auf, so ist dieser Modul nicht endlich-erzeugt.

Das Beispiel wirf die zusätzliche Frage nach der Bedeutung der Endlichkeit bzw. Nicht-Endlichkeit auf, siehe Satz 3.10.

Toolbeispiel Singular-Script

- RegularMap/Hyperbola

Wenn man sich eine affine Varietät als Nullstellengebilde in einem festen affinen Raum vorstellt, so liegt das zugehörige Verschwindungsideal auch in einem festen Polynomring. Man kann eine affine Varietät aber auch abstrakt betrachten. Dann geht es um die Äquivalenzklasse aller affinen Varietäten - jeweils in einen beliebigen affinen Raum eingebettet -, die unter regulären Abbildungen isomorph sind.

Welche *intrinsischen* Eigenschaften hat eine abstrakte Varietät, d.h. Eigenschaften, die nicht von ihrer Einbettung in einen affinen Raum abhängen?

Die wichtigste intrinsische Eigenschaft einer affinen Varietät ist ihr Koordinatenring:

2.6 Definition (Koordinatenring einer affinen Varietät)

Der *Koordinatenring* einer affinen k -Varietät $X \subset \boldsymbol{A}^n(K)$ ist der Quotientenring

$$k[X] := k[T_1,...,T_n]/Id(X).$$

2.7 Bemerkung (Koordinatenring und induzierte Abbildung)

i) Der Koordinatenring einer affinen k -Varietät $X \subset \boldsymbol{A}^n(K)$ ist eine affine k -Algebra, d.h. eine endlich erzeugte, reduzierte k -Algebra. Der Koordinatenring ist zugleich der Ring der k -regulären Abbildungen

$$g : X \longrightarrow \boldsymbol{A}^1(K).$$

Umgekehrt ist jede endliche-erzeugte k -Algebra Quotient

$$A = k[T_1,...,T_n]/I$$

eines – i.a. nicht eindeutig bestimmten – Polynomringes nach einem Ideal

$$I \subset k[T_1,...,T_n].$$

Das Ideal I ist genau dann reduziert, wenn A reduziert, also eine affine Algeba ist. In diesem Fall erhält man mit

$$X := Var(I) \subset \boldsymbol{A}^n(K)$$

eine affine k-Varietät mit A als Koordinatenring.

ii) Es seien $X \subset \boldsymbol{A}^n(K), Y \subset \boldsymbol{A}^m(K)$ zwei affine k-Varietäten.

Jede k-reguläre Abbildung

$$g : X \longrightarrow Y$$

ist global, d.h. zwischen den einbettenden affinen Räumen definiert. Daher existiert ein kommutatives Diagramm mit Inklusionen

$$\begin{array}{ccc} \boldsymbol{A}^n(K) & \xrightarrow{G} & \boldsymbol{A}^m(K) \\ \uparrow\subset & & \uparrow\subset \\ X & \xrightarrow{g} & Y \end{array}$$

in dem die globale, reguläre Abbildung

$$G : \boldsymbol{A}^n(K) \longrightarrow \boldsymbol{A}^m(K)$$

durch Polynome

$$g_i \in k[X_1,...,X_n], i = 1,...,m,$$

gegeben wird als

$$G = (g_1,...,g_m).$$

Der Rückzug von Polynomen definiert einen Morphismus von k-Algebren

$$k[Y_1,...,Y_m] \xrightarrow{\Phi} k[X_1,...,X_n],\ \Phi(S_i) := S_i \circ G = g_i \in k[X_1,...,X_n].$$

Und dieser induziert wegen

$$\Phi(Id(Y)) \subset Id(X) \Leftrightarrow G(X) \subset Y$$

den gesuchten k-Morphismus zwischen den Koordinatenringen

$$\varphi_g : k[Y] \longrightarrow k[X]$$

als Ergänzung in folgendem kommutativen Diagramm mit Projektionen

$$\begin{array}{ccc} k[Y_1,...,Y_m] & \xrightarrow{\Phi} & k[X_1,...,X_n] \\ \downarrow & & \downarrow \\ k[Y] & \xrightarrow{\varphi_g} & k[X] \end{array}$$

Umgekehrt induziert ein k-Morphismus zwischen den Koordinatenringen

$$\varphi : k[Y] \longrightarrow k[X]$$

ein kommutatives Diagramm

$$\begin{array}{ccc} k[Y_1,...,Y_m] & \xrightarrow{\Phi} & k[X_1,...,X_n] \\ \downarrow & & \downarrow \\ k[Y] & \xrightarrow{\varphi} & k[X] \end{array},$$

wenn man jeweils zur Definition von $\Phi(Y_i) \in k[X_1,...,X_n]$ ein Polynom $g_i \in k[X_1,...,X_n]$ wählt mit

$$\varphi(Y_i \bmod Id(Y)) = g_i \bmod Id(X)$$

und setzt

$$\Phi(Y_i) := g_i \in k[X_1,..., X_n].$$

Die gewählten Polynome $g_i \in k[X_1,..., X_n]$ definieren dann durch

$$G := (g_1,..., g_m)$$

folgendes kommutative Diagramm

$$\begin{array}{ccc} \boldsymbol{A}^n(K) & \xrightarrow{G} & \boldsymbol{A}^m(K) \\ \uparrow\subset & & \uparrow\subset \\ X & \xrightarrow{g_\varphi} & Y \end{array}$$

und damit eine reguläre Abbildung

$$g_\varphi : X \longrightarrow Y .$$

Die kontravarianten Zuordnungen $g \mapsto \varphi_g$ und $\varphi \mapsto g_\varphi$ sind funktoriell, d.h. sie sind verträglich mit der Komposition von Abbildungen und respektieren die Identität.

Aus Bemerkung 2.7 ergibt sich als Konsequenz:

2.8 Satz (Affine Varietät und affine Algebra)

Zwei affine k-Varietäten $X \subset \boldsymbol{A}^n(K)$ und $Y \subset \boldsymbol{A}^m(K)$ sind genau dann k-isomorph, wenn ihre Koordinatenringe $k[X]$ und $k[Y]$ als k-Algebren isomorph sind.

Affine k-Varietäten und ihre Morphismen können also gleichwertig auf zwei Arten dargestellt werden:

- Entweder geometrisch als Nullstellengebilde von Polynomen und als polynomiale Abbildungen mit Definitionskörper k
- oder algebraisch als affine k-Algebren und als k-lineare Abbildungen zwischen diesen Algebren.

Dabei ist die Beschreibung mit affinen Algebren und ihren Morphismen unabhängig von einer gewählten Einbettung, also eine *instrinsische* Darstellung.

Das folgende Lemma zeigt, wie man aus dem Koordinatenring die Varietät zurückgewinnen kann ohne sie in einen konkreten affinen Raum einzubetten.

2.9 Lemma (Punkte und Auswertungsmorphismen)

Es sei $X \subset \boldsymbol{A}^n(K)$ eine affine k - Varietät und $k[X]$ ihr Koordinatenring. Dann definiert die Auswertung auf den Koordinatenfunktionen eine bijektive Abbildung

$$\varepsilon : Hom_k(k[X], K) \xrightarrow{\cong} X, \varphi \mapsto \left(\varphi(\overline{T_1}),..., \varphi(\overline{T_n})\right).$$

Beweis. Die Abbildung ist wohldefiniert, denn für jedes $g \in Id(X)$ gilt

$$g\left(\varphi\left(\overline{T_1}\right),...,\varphi\left(\overline{T_n}\right)\right)=\varphi\left(\overline{g}\right)=\varphi(0)=0\ .$$

Surjektivität: Für einen gegebenen Punkt $x\in X$ sei

$$\varphi : k[X]\longrightarrow K\ ,\ g\mapsto g(x),$$

die Auswertung an dieser Stelle. Es gilt

$$\varepsilon(\varphi)=x\ .$$

Injektivität: Da die Restklassen der Koordinatenfunktionen den Ring $k[X]$ erzeugen, müssen sich zwei verschiedene Morphismen im Bild mindestens einer Koordinatenfunktion unterscheiden, q.e.d.

An keiner Stelle im Beweis von Lemma 2.9 wurde benutzt, daß der Koordinatenkörper algebraisch-abgeschlossen ist. Daher läßt sich die Aussage des Lemmas auch folgendermaßen interpretieren: Jede affine k - Algebra

$$A=k[T_1,...,T_n]/I$$

definiert einen kontravarianten Funktor von der Kategorie der k - Algebren in die Menge

$$Hom_k(A\ ,-):\underline{k-Alg}\longrightarrow\underline{Set}\ .$$

Für einen beliebigen Erweiterungkörper $L\supset k$ - er muß nicht algebraisch-abgeschlossen sein - ist das Bild

$$X(L):=\varepsilon(\ Hom_k(A\ ,L)\ )\subset \boldsymbol{A}^n(L)$$

die Nullstellenmenge des Ideals

$$I\subset k[T_1,...,T_n]$$

mit Koordinaten im Körper L :

$$X(L)=\left\{x\in \boldsymbol{A}^n(L):\ f(x)=0\ \textit{für alle}\ f\in I\ \right\}.$$

Man nennt $X(L)$ die Menge der L -wertigen Punkte der affinen k - Algebra A . In dieser Sicht ist ein L -wertiger Punkt also ein Morphismus auf dem Koordinatenring und eine affine k - Algebra definiert nicht nur eine einzige Nullstellenmenge

$$X\subset \boldsymbol{A}^n(K),$$

sondern eine ganze Familie von Nullstellmengen $X(L)$ mit beliebigen Koordinatenkörpern

$$L\supset k\ .$$

Toolbeispiel 2.10 betrachtet die Fasern einer regulären Abbildung zwischen affinen Varietäten. Die Fasern sind wieder Varietäten, allerdings sind sie i.a. nicht über dem Definitionskörper der Ausgangsvarietäten definiert, sondern erst über einem Erweiterungskörper.

2.10 Beispiel *(Familie quadratischer Kurven)*

ad Toolbeispiel 1.2, Familie von quadratischen Kurven.

Das Beispiel der Familie von Kurven 2. Grades läßt sich beschreiben als reguläre Abbildung. Man definiert die Fläche

$$Z := \{ (x, y, z) \in \boldsymbol{A}^2 : x^2 + z \cdot y^2 - 1 = 0 \}.$$

Die Einschränkung der 3. Projektion

$$pr_3 : \boldsymbol{A}^3 \longrightarrow \boldsymbol{A}^1, (x, y, z) \mapsto z$$

definiert eine surjektive reguläre Abbildung

$$g : Z \longrightarrow \boldsymbol{A}^1.$$

Der zugehörige Morphismus von k-Algebren lautet

$$k[T] \longrightarrow k[X, Y, Z] \big/ \langle X^2 + Z \cdot Y^2 - 1 \rangle, T \mapsto Z \bmod \langle X^2 + Z \cdot Y^2 - 1 \rangle.$$

Die Fasern außerhalb des Nullpunktes, d.h. für $0 \neq z_0 \in \boldsymbol{A}^1(K)$,

$$g^{-1}(z_0) = \{ (x, y, z) \in \boldsymbol{A}^2 : x^2 + z \cdot y^2 = 1 \text{ und } z = z_0 \} = Var\left(\langle X^2 + Z \cdot Y^2 - 1, Z - z_0 \rangle \right) \subset \boldsymbol{A}^3,$$

sind wiederum affine Varietäten, allerdings $k(z_0)$-Varietäten. Als $k(z_0)$-Varietäten sind sie isomorph zu quadratischen Kurven wie Hyperbel oder Ellipse:

$$g^{-1}(z_0) \cong \{ (x, y) \in \boldsymbol{A}^2 : x^2 + z_0 \cdot y^2 \}.$$

Die Faser über dem Nullpunkt ist eine k-Varietät und als k-Varietät isomorph zur Doppelgeraden

$$g^{-1}(0) \cong \{ (x, y) \in \boldsymbol{A}^2 : x^2 = 1 \}.$$

Durch Komposition mit der Inklusion der Faser entsteht eine $k(z_0)$-reguläre Abbildung von affinen $k(z_0)$-Varietäten

$$j = [g^{-1}(z) \xrightarrow{\subset} Z \longrightarrow \boldsymbol{A}^1].$$

Für den zugehörigen Morphismus von $k(z_0)$-Algebren

$$\varphi_j = [A \longrightarrow B \longrightarrow B_{z_0}]$$

mit

$$A = k(z_0)[T], B = k(z_0)[X, Y, Z] \big/ \langle X^2 + Z \cdot Y^2 - 1 \rangle$$

und

$$B_{z_0} = B / \langle Z - z_0 \rangle \cong k(z_0)[X, Y, Z] \big/ \langle X^2 + Z \cdot Y^2 - 1, Z - z_0 \rangle \cong k(z_0)[X, Y] \big/ \langle X^2 + z_0 \cdot Y^2 - 1 \rangle$$

gilt

$$\varphi_j : A \longrightarrow B_{z_0}, T \mapsto z_0.$$

2.11 Beispiel (Hyperebenenschnitte)

i) ad Toolbeispiel 1.6, Familie von Hyperbeln.

Die Darstellung von Hyperbeln als Hyperebenenschnitte läßt sich als reguläre Abbildung folgendermaßen beschreiben: Man definiert die Fläche

$$Z := \{ (x, y, z) \in \boldsymbol{A}^3 : x \cdot y \cdot z - 2 = 0 \}.$$

Schränkt man die Projektion

$$pr_3 : \boldsymbol{A}^3 \longrightarrow \boldsymbol{A}^1, (x, y, z) \mapsto z ,$$

auf diese Fläche ein, so erhält man eine reguläre Abbildung

$$g : Z \longrightarrow \boldsymbol{A}^1 ,$$

welche die Fläche als eine Familie ebener quadratischer Kurven fasert: Die Faser über einem Punkt $z \in \boldsymbol{A}^1 - 0$ ist die Hyperbel

$$g^{-1}(z) \cong \left\{ (x, y) \in \boldsymbol{A}^2 : x \cdot y = \frac{2}{z} \right\},$$

die Faser über dem Nullpunkt ist leer

$$g^{-1}(0) = \varnothing .$$

Bei Variation des Basispunktes $z \in \boldsymbol{A}^1$ durchlaufen die Fasern eine Familie quadratischer Kurven, die sich bei Annäherung des Basispunktes an das Achsenkreuz annähern.

ii) ad Toolbeispiel 1.6, Familie von Kurven 3. Grades.

Analog läßt sich das Beispiel von Kurven 3. Grades als Hyperebenenschnitten als reguläre Abbildung folgendermaßen darstellen: Es sei

$$Z := \left\{ ((x, y), z) \in \boldsymbol{A}^2 \times \boldsymbol{A}^1 : y^2 - x^2(x - z) = 0 \right\}$$

und

$$g : Z \longrightarrow \boldsymbol{A}^1$$

die Einschränkung der Projektion

$$pr_3 : \boldsymbol{A}^3 \longrightarrow \boldsymbol{A}^1, (x, y, z) \mapsto z .$$

Jede Faser

$$g^{-1}(z) \cong \left\{ (x, y) \in \boldsymbol{A}^2 : y^2 - x^2(x - z) = 0 \right\}$$

ist eine kubische Kurve.

Zariski Topologie

2.12 Bemerkung (Affine Varietäten und Ideale)

Im folgenden studieren wir die in Bemerkung 2.2 eingeführten beiden Operationen

$$I \mapsto Var(I) \text{ und } X \mapsto Id(X).$$

Sie setzen affine k-Varietäten als Punktmengen eines affinen Raumes über dem Koordinatenkörper und reduzierte Ideale in Polynomringen über dem Definitionskörper zueinander in Beziehung.

i) Tabelle 1 zeigt, in welchem Maße beide Zuordnungen strukturtreue Abbildungen auf einem geeigneten Definitionsbereich sind. Beide Abbildungen liefern eine erste Übersetzung zwischen geometrischen und algebraischen Objekten der Algebraischen Geometrie, zwischen Punktmengen in affinen Räumen und Idealen in Polynomringen.

Geometrie	Übersetzung	Algebra
Affine k-Varietät in $\boldsymbol{A}^n(K)$	$X \mapsto Id(X)$ $Var(I) \leftarrow\mid I$	Reduziertes Ideal in $k[T_1,...,T_n]$
$X_1 \subset X_2$	$X_i \mapsto Id(X_i)$	$Id(X_1) \supset Id(X_2)$
$Var(I_1) \supset Var(I_2)$	$Var(I_i) \leftarrow\mid I_i$	$I_1 \subset I_2$
$X = Var(\ Id(\ X\ )\ )$		Hilbertscher Nullstellensatz: $I = Id(\ Var(\ I\ )\ )$
Durchschnitt von Varietäten		Summe von Idealen
	$Var(I_1 + I_2) = Var(I_1) \cap Var(I_2) \leftarrow\mid I_1 + I_2$	
	$X_1 \cap X_2 \mapsto Id(X_1 \cap X_2) = \sqrt{Id(X_1) + Id(X_2)}$	
Vereinigung von Varietäten		Durchschnitt von Idealen
	$X_1 \cup X_2 \mapsto Id(X_1 \cup X_2) = Id(X_1) \cap Id(X_2)$	
	$Var(I_1 \cap I_2) = Var(I_1) \cup Var(I_2) \leftarrow\mid I_1 \cap I_2$	

Tabelle 1: Korrespondenz von Geometrie und Algebra

Tabelle 1 enthält den Hilbertschen Nullstellensatz: Bei algebraisch-abgeschlossenem Koordinatenkörper K gilt für ein beliebiges, d.h. nicht notwendig reduziertes, Ideal

$$I \subset k[X_1,..., X_n]$$

die Gleichung

$$Id(Var(I)) = \sqrt{I}\ .$$

Zum Beweis siehe ([CLO1997] Chap. 4, §1). Insbesondere hat jedes echte Ideal

$$I \neq k[T_1,...,T_n]$$

eine nicht-leere Nullstellenmenge

$$Var(I) \neq \varnothing;$$

denn anderfalls wäre

$$Var(I) \neq \varnothing$$

Die Summe zweier reduzierter Ideale ist i.a. nicht wieder reduziert: Beide Ideale

$$I_1 = \langle Y - X^2 \rangle,\ I_2 = \langle Y \rangle \subset k[X,Y]$$

sind reduziert, aber für ihre Summe gilt

$$I_1 + I_2 = \langle X^2, Y \rangle \subsetneq \sqrt{I_1 + I_2} = \langle X, Y \rangle.$$

Für zwei, nicht notwendig reduzierte Ideale

$$I_1, I_2 \subset k[X_1,..., X_n]$$

gilt

$$I_1 \cdot I_2 \subset I_1 \cap I_2 \subset \sqrt{I_1 \cdot I_2}$$

und damit

$$Var(I_1 \cdot I_2) \supset Var(I_1 \cap I_2) \supset Var\left(\sqrt{I_1 \cdot I_2}\right).$$

Da die beiden äußeren Varietäten übereinstimmen, gilt auch

$$Var(I_1 \cdot I_2) = Var(I_1 \cap I_2).$$

ii) Der Zusammenhang aus Tabelle 1 überträgt sich auf den Durchschnitt beliebig vieler affiner Varietäten und auf die endliche Vereinigung:

- Beliebiger Durchschnitt

$$\bigcap_{j \in J} X_j = Var\left(\sqrt{\sum_{j \in J} Id(X_j)}\right)$$

- Endliche Vereinigung

$$\bigcup_{j \in J} X_j = Var\left(\bigcap_{j \in J} Id(X_j)\right),\ J\ endlich$$

- Leere Varietät, gesamter affiner Raum

$$\varnothing = Var(\langle 1 \rangle),\ \mathbf{A}^n = Var(\langle 0 \rangle)$$

Hinweis. Die beliebige Vereinigung affiner Varietäten ist i.a. keine affine Varietät: Die Teilmenge

$$\boldsymbol{Q} \subset \boldsymbol{A}^1(\boldsymbol{C})$$

ist keine Varietät, da sie sich nicht als Nullstellmenge endlich vieler Polynome darstellen läßt.

Damit erfüllen affine k-Varietäten in einem festen affinen Raum $\mathbf{A}^n(K)$ bezüglich der Bildung von beliebigen Durchschnitten und endlichen Vereinigungen genau die Eigenschaften, welche man von den abgeschlossenen Mengen eines topologischen Raumes fordert. Die Definition einer Topologie verwendet – komplementär dazu - die offenen Mengen:

2.13 Definition *(Topologie)*

Eine *Topologie* auf einer Menge X ist eine Familie $\mathcal{T}$ von Teilmengen von X mit folgenden Eigenschaften:

- $\mathcal{T}$ enthält die leere Menge $\varnothing$ und die gesamte Menge X
- $\mathcal{T}$ enthält mit je zwei Mengen U_1 und U_2 auch deren Durchschnitt $U_1 \cap U_2$
- $\mathcal{T}$ enthält mit einer beliebigen Familie von Mengen U_j, $j \in J$, auch deren Vereinigung $\bigcup_{j \in J} U_j$

Das Paar $(X, \mathcal{T})$ heißt *topologischer Raum*, die Mengen aus $\mathcal{T}$ heißen *offene* Mengen, ihre Komplemente

$$A := X - U, U \in \mathcal{T},$$

heißen *abgeschlossene* Mengen. Für eine Teilmenge $Y \subset X$ ist die *abgeschlossene Hülle*

$$\overline{Y} := \bigcap_{A \supset Y,\ A \text{ abgeschlossen}} A$$

die kleinste abgeschlossene Menge, welche Y umfasst. Eine Teilmenge von X heißt *dicht*, wenn

$$\overline{Y} = X .$$

2.14 Definition *(Zariski Topologie)*

Der affine Raum $\boldsymbol{A}^n(K)$ trägt als als k-Varietät eine kanonische Topologie, die *Zariski Topologie* oder genauer *k-Topologie*. Sie ist die eindeutig bestimmte Topologie mit den affinen k-Varietäten als abgeschlossenen Mengen, d.h. den Komplementen affiner k-Varietäten als offenen Mengen.

Für eine affine k-Varietät $X \subset \mathbf{A}^n(K)$ definiert man die *Zariski Topologie* von X als die Unterraumtopologie bzgl. des affinen Raumes, d.h. eine Teilmenge $Z \subset X$ ist genau dann abgeschlossen, wenn es eine affine k-Varietät $Y \subset \mathbf{A}^n(K)$ gibt mit

$$Z = Y \cap X .$$

2.15 Bemerkung *(Zariski Topologie)*

i) Nach Definition der Unterraumtopologie ist eine abgeschlossene Teilmenge eines abgeschlossenen Unterraumes auch abgeschlossen im gesamten Raum. Daher sind abgeschlossene Teilmenge einer affinen k-Varietät auch selbst affine k-Varietäten. Eine abgeschlossene Teilmenge Y einer affinen k-Varietät X ist die Nullstellenmenge eines Ideals

$$I \subset k[X],$$

nämlich

$$Y = Var_X(I) := \{ x \in X : f(x) = 0 \text{ für alle } f \in I \} = Var\left(\pi^{-1}(I)\right) \subset \boldsymbol{A}^n(K)$$

bzgl. der kanonischen Projektion

$$\pi : k[T_1,...,T_n] \longrightarrow k[X].$$

ii) k -reguläre Abbildungen zwischen affinen Varietäten sind stetig bzgl. der Zariski Topologie. Dabei heißt eine Abbildung

$$g : (X, \mathcal{T}_X) \longrightarrow (Y, \mathcal{T}_Y)$$

zwischen topologischen Räumen *stetig*, wenn das Urbild jeder offenen Menge wieder offen ist. Eine äquivalente Bedingung lautet: Das Urbild jeder abgeschlossenen Menge ist wieder abgeschlossen.

Die Stetigkeit einer k -regulären Abbildung

$$g : X \longrightarrow Y \text{ mit } \varphi_g : k[Y] \longrightarrow k[X]$$

folgt daraus, daß das Urbild einer affinen Varietät wieder eine affine Varietät ist: Wenn

$$Z = Var(I) \subset Y ,$$

so

$$g^{-1}(Z) = Var\left(\left\langle \varphi_g(I) \right\rangle_{k[X]}\right) \subset X .$$

Die Umkehrung gilt nicht: Die Abbildung der Neil Parabel

$$h : Z \longrightarrow \boldsymbol{A}^1,\ h(x,y) = \begin{cases} \dfrac{y}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

aus Beispiel 2.4 ist stetig: Alle affine k -Varietäten von $\boldsymbol{A}^1(K)$, welche von $\boldsymbol{A}^1(K)$ verschieden sind, sind endliche Punktmengen. Ihre Urbilder sind wiederum endliche Punktmengen. Die Abbildung ist jedoch nicht regulär.

iii) Im Falle k = $\boldsymbol{R}$ oder k = $\boldsymbol{C}$ sind Polynome stetige Funktionen bzgl. der Euklidischen Topologie des Zahlenraumes $\boldsymbol{A}^n(\boldsymbol{C})$. Abgeschlossene Mengen in der Zariski Topologie sind also auch abgeschlossen in der Euklidischen Topologie.

I.a. ist die Zariski Topologie echt gröber als die Euklidische Topologie: Im Falle k = $\boldsymbol{C}$ ist die Teilmenge der ganzen Zahlen

$$\boldsymbol{Z} \subset \boldsymbol{C}$$

abgeschlossen in der Euklidischen Topologie, aber nicht in der Zariski Topologie von $\boldsymbol{A}^1_{\boldsymbol{C}}$.

Insbesondere ist die Zariski Topologie i.a. keine Hausdorff Topologie, d.h. zwei unterschiedliche Punkte lassen sich nicht durch disjunkte, Zariski-offene Umgebungen trennen. Trotzdem ist die Zariski Topologie für große Teile der Algebraischen Geometrie die geeignete Topologie und hat hier dieselbe Bedeutung wie die Euklidische Topologie in der Analysis.

iii) Erst für zahlentheoretische Fragen braucht man eine Topologie, die feiner ist als die Zariski Topologie. Sie wurde von Grothendieck unter dem Namen ètale-Topologie entwickelt. Mit Hilfe der ètale-Topologie gelang Deligne nach Vorarbeiten von Grothendieck der Beweis der Weil-Vermutungen (1976).

Im Zusammenhang mit affinen Varietäten beziehen sich im folgenden topologische Begriffe immer auf die Zariski Topologie.

Für eine reguläre Abbildung

$$g : X \longrightarrow Y$$

zwischen zwei affinen Varietäten $X \subset \boldsymbol{A}^n$, $Y \subset \boldsymbol{A}^m$ ist das Bild

$$g(X) \subset Y$$

i.a. keine affine Varietät, siehe Beispiel 2.4, ii). Die kleinste affine Varietät $Z \subset \boldsymbol{A}^m$, welche das Bild $g(X)$ enthält, ist der Abschluß bzgl. der Zariski Topologie

$$Z := \overline{g(X)} \subset Y .$$

Durch welches Ideal von $k[Y_1,...,Y_m]$ läßt sich $Z \subset \boldsymbol{A}^m$ definieren? Die Antwort ergibt sich aus der Betrachtung des induzierten Morphismus der Koordinatenringe

$$\varphi_g : k[Y] \longrightarrow k[X].$$

2.16 Satz *(Reguläre Abbildung und Morphismus der Koordinatenringe)*

Es sei

$$g : X \longrightarrow Y$$

eine reguläre Abbildung zwischen zwei affinen Varietäten $X \subset \boldsymbol{A}^n$, $Y \subset \boldsymbol{A}^m$ und

$$\varphi_g : k[Y] \longrightarrow k[X]$$

der induzierte Morphismus der Koordinatenringe. Dann gilt:

- $\overline{g(X)} = Var_Y(\ker \varphi_g)$. Insbesondere ist φ_g genau dann injektiv, wenn $g(X) \subset Y$ dicht ist.
- Es ist φ_g genau dann surjektiv, wenn $g(X) \subset Y$ abgeschlossen und die Einschränkung

  $$g : X \longrightarrow g(X)$$

  ein Isomorphismus von Varietäten ist.

Beweis. i) Nach Definition von φ_g gilt die Äquivalenz

$$f \in \varphi_g \Leftrightarrow f \circ g = 0 .$$

Es folgt

$$f(g(X)) = 0 \text{ für alle } f \in \varphi_g ,$$

und das bedeutet

$$g(X) \subset Var_Y(\ker \varphi_g).$$

Da der Zariski Abschluß die kleinste abgeschlossene Menge ist, folgt die Inklusion

$$\overline{g(X)} \subset Var_Y(\ker \varphi_g).$$

Zum Beweis der Umkehrung: Zunächst gilt

$$\ker \varphi_g \supset Id_{k[Y]}(\, g(X)\,).$$

Es folgt

$$Var_Y\left(Id_{k[Y]}(\, g(X)\,)\right) = Var_Y\left(Id_{k[Y]}\left(\,\overline{g(X)}\,\right)\right) = \overline{g(X)} \supset Var_Y\left(\ker \varphi_g\right)$$

unter Verwendung der für eine beliebige Teilmenge $Z \subset Y$ gültigen Gleichheit

$$Var(\, Id(Z)\,) = Var\left(\, Id\left(\,\overline{Z}\,\right)\right), \text{ q.e.d.}$$

ii) Es sei

$$Z := \overline{g(X)} \subset Y$$

der Abschluß des Bildes von g. Aus der in Teil i) bewiesenen Gleichung

$$Z = Var_Y\left(\,\ker \varphi_g\,\right)$$

folgen mit dem Hilbertschen Nullstellensatz das Verschwindungideal

$$Id_{k[Y]}(\, Z\,) = Id_{k[Y]}(\, Var_Y(\,\ker \varphi\,)\,) = \sqrt{\ker \varphi} = \ker \varphi$$

und der Koordinatenring

$$k[Z] = k[Y]\,/\,Id_{k[Y]}(Z) = k[Y]\,/\,\ker \varphi_g\ .$$

Die Injektivität der Abbildung

$$\varphi_g : k[Y] \longrightarrow k[X]$$

ist äquivalent mit

$$\ker \varphi_g = 0$$

also mit

$$Id_{k[Y]}(\, Z\,) = 0\,.$$

Und diese Gleichung ist äquivalent mit

$$Z = Y\ .$$

Die Surjektivität der Abbildung

$$\varphi_g : k[Y] \longrightarrow k[X]$$

ist äquivalent mit dem Isomorphismus

$$\varphi : k[Z] = k[Y]\,/\,\ker \varphi_g \xrightarrow{\cong} k[X].$$

Diese Isomorphie auf dem Niveau der Koordinatenringe ist nach Satz 2.8 äquivalent mit der Isomorphie

$$g : X \longrightarrow Z\ ,\ \text{q.e.d.}$$

Die Anwendung von Satz 2.16 auf Toolbeispiel 2.4 bestätigt: Die Projektion der Neil Parabel auf die x-Achse

$$g_1 : Z \longrightarrow \boldsymbol{A}^1(K)$$

hat ein dichtes Bild, weil der zugeordnete Morphismus

$$\varphi_1 : k[T] \longrightarrow k[U^2, U^3], T \mapsto U^2,$$

injektiv ist. Die Abbildung g_1 ist sogar surjektiv. Sie ist jedoch kein Isomorphismus, weil φ_1 nicht surjektiv ist. Auch die bijektive Parametrisierung

$$g_2 : \boldsymbol{A}^1(K) \longrightarrow Z, t \mapsto (t^2, t^3),$$

ist kein Isomorphismus, weil die die Inklusion

$$\varphi_2 : k[U^2, U^3] \xrightarrow{\subset} k[U]$$

nicht surjektiv ist.

Das folgende Toolbeispiel 2.17 stellt das Blow-up als ein Geradenbündel über der exzeptionellen Menge dar.

2.17 Toolbeispiel (Blow-up)

ad Toolbeispiel 1.6, Blow-up.

Die Projektion des affinen Raumes auf die ersten beiden Koordinaten

$$pr : \boldsymbol{A}^3 \longrightarrow \boldsymbol{A}^2, (x, y, z) \mapsto (x, y)$$

induziert für das affine *Blow-up* von $\boldsymbol{A}^2$ im Nullpunkt

$$Z := \{ (x, y, z) \in \boldsymbol{A}^3 : y - z \cdot x = 0 \}$$

eine reguläre Abbildung

$$g : Z \longrightarrow \boldsymbol{A}^2 .$$

Ihr Bild läßt die punktierte y-Achse aus:

$$g(Z) = \boldsymbol{A}^2 - \{ (0, y) : y \neq 0 \}$$

Der Ursprung von $\boldsymbol{A}^2$ hat als Urbild die gesamte z-Achse:

$$E := g^{-1}(0,0) = \{ (0, 0, z) : z \in \boldsymbol{A}^1 \}.$$

Die Punkte der *exzeptionellen Geraden* E entsprechen bijektiv den Geraden der affinen Ebene durch den Nullpunkt - mit Ausnahme der y-Achse: Dem Punkt $(0,0, z_0) \in E$ wird die Gerade

$$\{ (x, y) \in \boldsymbol{A}^2 : y = z \cdot x \}$$

mit der Steigung z_0 zugeordnet. Jeder vom Nullpunkt verschiedene Punkt des Bildes

$$p = (x, y) \in g(Z) - (0, 0)$$

hat genau ein Urbild, den Punkt

$$g^{-1}(p) = \left(x, y, \frac{y}{x} \right) \in \boldsymbol{A}^3 .$$

Das Urbild eines solchen Punktes p hat als dritte Koordinate die Steigung der Geraden durch den Punkt p und den Nullpunkt. Die gesamte Fläche $Z \subset \boldsymbol{A}^3$ ist die disjunkte Vereinigung aller Geraden der affinen Ebene $\boldsymbol{A}^2$ durch den Nullpunkt – mit Ausnahme der y-Achse -,

parametrisiert durch die Punkte der exzeptionellen Geraden E. Daher nennt man die reguläre Abbildung

$$g : Z \longrightarrow \boldsymbol{A}^2$$

das Blow-up der affinen Ebene $\boldsymbol{A}^2$ im Nullpunkt: „Aufgeblasen“ wird der Nullpunkt, indem man ihn durch die Menge aller Geraden durch den Nullpunkt ersetzt – mit Ausnahme der y-Achse. Der zugehörige Morphismus von k-Algebren heißt

$$\varphi : k[X,Y] \to k[X,Y,Z]/I,\ X \mapsto X \bmod I, Y \mapsto Y \bmod I \text{ mit } I = \langle Y - Z \cdot X \rangle .$$

Diese Abbildung ist injektiv, nicht surjektiv und nicht endlich.

siehe Toolbeispiel Singular-Script

- RegularMap/BlowUp

Eine zweite reguläre Abbildung

$$h : Z \longrightarrow \boldsymbol{A}^1 \cong E$$

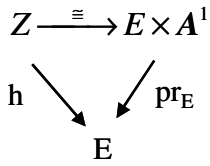
ist die Einschränkung der Projektion

$$pr : \boldsymbol{A}^3 \longrightarrow \boldsymbol{A}^1 \cong E, (x, y, z) \mapsto z .$$

Sie fasert die affine Varietät als eine Familie von Geraden: Die Faser $h^{-1}(z)$ eines Punktes $z \in E$ ist die Gerade mit der Steigung z. Man nennt

$$h : Z \longrightarrow E$$

daher ein Geradenbündel über E. In diesem Fall ist das Geradenbündel trivial, d.h. es gibt einen regulären Isomorphismus über E auf ein Produkt:



Der gesuchte Isomorphismus ist die Projektion

$$Z \longrightarrow E \times \boldsymbol{A}^1, (x, y, z) \mapsto (z, x)$$

mit regulärer Umkehrung

$$E \times \boldsymbol{A}^1 \longrightarrow Z, (u, v) \mapsto (\ v, u \cdot v, u\ ).$$

Frage: Wie muß man das Beispiel erweitern, um alle Geraden durch den Nullpunkt, einschließlich der y-Achse, zu parametrisieren?

3 Ergebnisse der kommutativen Algebra

In diesem Kapitel geht es um einige grundlegende Begriffe der kommutativen Algebra: Die Endlichkeit eines Moduls und die Primärzerlegung von Idealen. Ziel ist es, die Bedeutung beider Begriffe für die Geometrie von Varietäten und regulären Abbildungen darzustellen.

Der Beweis der grundlegenden Sätze verwendet Resultantensystemen.

Resultantensysteme

Nach dem Fundamentalsatz der Algebra hat jedes nicht-konstante Polynom in einer Veränderlichen mindestens eine Nullstelle in einem algebraisch-abgeschlossenen Körper. Resultantensysteme sind das klassische Hilfsmittel, um zu entscheiden, ob zwei oder mehrere Polynome einer Veränderlicher eine gemeinsame Nullstelle in einem algebraisch-abgeschlossenen Körper haben.

Im folgenden bezeichnet R einen kommutativen Ring mit 1 und k den Spezialfall eines Körpers.

3.1 Definition (Resultante zweier Polynome)

Es seien $f, g \in R[X]$ zwei Polynome der Gestalt

$$f(X) = a_0 \cdot X^n + a_1 \cdot X^{n-1} + ... + a_{n-1} \cdot X + a_n$$

$$g(X) = b_0 \cdot X^m + b_1 \cdot X^{m-1} + ... + b_{m-1} \cdot X + b_m .$$

Die *Resultante* der beiden Polynome ist definiert als die Determinante

$$Res(f,g) := \det \begin{pmatrix} a_0 & a_1 & ... & a_n & & & & & \\ & a_0 & a_1 & ... & a_n & & & & \\ & & ... & & & & & & \\ & & & a_0 & a_1 & ... & a_n & & \\ b_0 & b_1 & ... & ... & b_m & & & & \\ & b_0 & b_1 & ... & ... & b_m & & & \\ & & ... & & & & & & \\ & & & ... & & & & & \\ & & & & b_0 & b_1 & ... & ... & b_m \end{pmatrix} \in R$$

mit m Zeilen im oberen Teil und n Zeilen im unteren Teil der Matrix.

Mit der Resultante läßt sich entscheiden, ob zwei Polynome einen gemeinsamen Faktor haben, ohne die Polynome zuvor in Linearfaktoren zerlegen zu müssen.

3.2 Satz (Resultante)

i) Die Resultante zweier Polynome

$$f, g \in R[X]$$

liegt in dem Ideal, das von beiden Polynomen aufgespannt wird: Es gibt Polynome

$$a, b \in R[X] \text{ mit } \deg a < \deg g, \deg b < \deg f$$

mit

$$Res(f, g) = a \cdot f + b \cdot g \in R .$$

ii) Im Falle eines Körpers k und $\deg f \geq 1$ gilt die Äquivalenz:

- Beide Polynome haben einen gemeinsamen Faktor in $k[X]$ vom Grad ≥ 1
- $Res(f, g) = 0 \in k$.

Beweis. ad i) siehe [CLO1997], Chap. 3, §5 Prop. 9. Der Satz wird dort nur für den Fall eines Körpers bewiesen. In unserem Fall betrachte man den Quotientenkörper des Ringes der von den Koeffizienten beider Polynome über $\boldsymbol{Z}$ erzeugt wird.

ad ii) Nach Teil i) gibt es eine Darstellung

$$Res(f, g) = a \cdot f + b \cdot g .$$

Falls beide Polynome einen gemeinsamen Faktor $h \in k[X]$ vom Grad ≥ 1 haben, ist die Resultante ein Vielfaches des Polynoms h. Als Element des Grundkörpers folgt dann

$$Res(f, g) = 0 .$$

Zum Beweis der Umkehrung: Im Hauptidealring $k[X]$ gibt es ein Polynom

$$0 \neq d \in k[X]$$

mit

$$\langle d \rangle = \langle f, g \rangle \subset k[X].$$

Das Polynom d ist insbesondere ein gemeinsamer Faktor von f und g in $k[X]$. Wir zeigen, daß d einen Grad ≥ 1 hat, indem wir die Existenz einer Nullstelle von d im algebraischen Abschluß $K = \overline{k}$ nachweisen.

Das Polynom f zerfällt über K vollständig in Linearfaktoren:

$$f(X) = r_0 \cdot (X - \xi_1) \cdot \ldots \cdot (X - \xi_n) \in K[X].$$

Aus

$$0 = Res(f, g) = a \cdot f + b \cdot g$$

folgt

$$a(X) \cdot r_0 \cdot (X - \xi_1) \cdot \ldots \cdot (X - \xi_n) = -b(X) \cdot g(X) \in K[X].$$

Wegen

$$\deg b < \deg f = n$$

muß mindestens einer der Faktoren

$$(X - \xi_i) \in K[X]$$

auch ein Faktor von

$$g(X) \in K[X]$$

sein. Damit haben f und g eine gemeinsame Nullstelle in K, und diese Nullstelle ist auch eine Nullstelle von d, q. e. d.

3.3 Bemerkung (Resultante und Diskriminante)

Die *Diskriminante* eines Polynoms $f \in R[X]$ ist die Resultante des Polynoms und seiner Ableitung

$$disc(f) := Res(f, f').$$

3.4 Definition (Resultantensystem)

Es sei $F = (f_0, f_1, ..., f_m)$ eine Familie von Polynomen $f_i \in k[X]$, das erste von der Gestalt

$$f_0(X) = a_0 \cdot X^N + a_1 \cdot X^{N-1} + ... + a_{N-1} \cdot X + a_N,\ a_0 \neq 0 \in k\ .$$

Das *Resultantensystem* von F ist die Familie

$$Res\ F = (\ Res_\alpha(F)\ )_{|\alpha|=N},$$

deren Elemente $Res_\alpha(F)$ die Koeffizienten sind in der Darstellung

$$Res\left(f_0, \sum_{i=1}^{m} T_i \cdot f_i\right) = \sum_{|\alpha|=N} T^\alpha \cdot Res_\alpha(F) \in k[T_1, ..., T_m],\ T^\alpha := T_1^{\alpha_1} \cdot ... \cdot T_m^{\alpha_m},$$

mit den beiden Polynomen

$$f_0 \text{ und } \sum_{i=1}^{m} T_i \cdot f_i \in R[X],\ R := k[T_1, ..., T_m].$$

3.5 Satz (Resultantensystem)

Eine Familie $F = (f_0, f_1, ..., f_m)$ von Polynomen $f_i \in k[X]$ mit

$$f_0(X) = a_0 \cdot X^N + a_1 \cdot X^{N-1} + ... + a_{N-1} \cdot X + a_N,\ a_0 \neq 0 \in k$$

hat genau dann eine gemeinsame Nullstelle im algebraischen Abschluß $K = \bar{k}$, wenn ihr Resultantensystem verschwindet, d.h.

$$Res_\alpha(F) = 0 \in k \text{ für alle } \alpha = (\alpha_1, ..., \alpha_m)\ mit\ |\ \alpha\ | = N\ .$$

Beweis. Wir setzen

$$R := k[T_1, ..., T_m].$$

i) Wenn alle Polynome von $F = (f_0, f_1, ..., f_m)$ eine gemeinsame Nullstelle in K haben, so haben sie auch einen gemeinsamen Faktor in $k[X]$ vom Grad ≥ 1. Dann haben auch die beiden Polynome

$$f_0 \text{ und } \sum_{i=1}^{m} T_i \cdot f_i$$

einen gemeinsamen Faktor aus $R[X]$ vom Grad ≥ 1. Es sei

$$r := res\left(f_0, \sum_{i=1}^{m} T_i \cdot f_i \right) \in R$$

die Resultante beider Polynome. Für jeden festen Wert

$$t := (t_1,...,t_m) \in k$$

gilt nach Satz 3.2, Teil ii)

$$r(t) = 0 \in k .$$

Es folgt, daß r das Nullpolynom ist.

ii) Es sei

$$Res\left(f_0, \sum_{i=1}^{m} T_i \cdot f_i \right) = 0 \in R .$$

Wir bezeichnen den Quotientenkörper von R mit

$$L := Q(R) := k(T_1,...,T_m) .$$

Nach Satz 3.2, Teil ii) haben beide Polynome

$$f_0 \text{ und } \sum_{i=1}^{m} T_i \cdot f_i$$

einen gemeinsamen Faktor $h \in L[X]$ vom Grad ≥ 1, d.h.

$$f_0 = h \cdot g_0 \text{ und } \sum_{i=1}^{m} T_i \cdot f_i = h \cdot g$$

mit Polynomen

$$g_0, g \in L[X].$$

Ohne Einschänkung kann man annehmen, daß die Polynome

$$f_0, h \text{ und } g_0$$

normiert sind. Der Ring R ist faktoriell, daher gilt die Gleichung

$$f_0 = h \cdot g_0$$

bereits in $R[X]$. Wir betrachten nun die drei Elemente f_0, h und g_0 als Polynome mehrerer Veränderlicher mit Koeffizienten aus dem Körper $k(X)$, d.h.

$$f_0, h, g_0 \in k(X)[T_1,...,T_m].$$

Dann haben f_0 und damit auch h und g_0 den Grad 0. Also gilt die Gleichung

$$f_0 = h \cdot g_0$$

bereits in $k(X)$ und damit auch in $k[X]$. Aus der Darstellung

$$g = \sum_{i=1}^{m} T_i \cdot g_i,\ g_i \in k[X]$$

folgen durch Koeffizientenvergleich bzgl. der Unbestimmten T_i die Gleichungen

$$f_i = h \cdot g_i, i = 1,...,m .$$

Also haben alle Polynome aus $F = (f_0, f_1,..., f_m)$ den gemeinsamen Faktor

$$h \in k[X] \text{ vom Grad } \geq 1$$

und damit eine gemeinsame Nullstelle in K, q.e.d.

Endlichkeit

Ein Morphismus zwischen zwei Ringen

$$\varphi : R \longrightarrow S$$

erlaubt es, auf dem Ring S eine Skalarmultiplikation mit Elementen von R zu definieren:

$$r * s := \varphi(r) \cdot s \in S \text{ für } r \in R,\ s \in S .$$

Hierdurch kann man den Ring S als R-Modul und sogar als R-Algebra auffassen.

3.6 Definition (Endliche Abbildungen)

i) Ein Morphismus zwischen zwei Ringen

$$\varphi : R \longrightarrow S$$

heißt

- *endlich*, wenn S ein endlich erzeugter R-Modul ist,
- von *endlichem Typ*, wenn S eine endlich erzeugte R-Algebra ist, d.h. wenn es endlich viele Elemente $s_1,...,s_k \in S$ gibt mit

$$S = \varphi(R)[s_1,...,s_k]$$

- *ganz*, wenn jedes Element von S ganz über R ist.

  Dabei heißt ein Element $s \in S$ *ganz über* R, wenn es eine normierte Gleichung mit Koeffizienten aus R erfüllt:

$$s^n + r_1 * s^{n-1} + ... + r_{n-1} * s + r_n = 0 \text{ mit } r_i \in R, i = 1,...,n$$

  Die Menge der über R ganzen Elemente von S heißt der *ganze Abschluß* von R bzgl. φ. Falls er mit $\varphi(R)$ übereinstimmt heißt R *ganz-abgeschlossen* bzgl. φ.

ii) Eine reguläre Abbildung zwischen zwei affinen k-Algebren

$$g : X \longrightarrow Y$$

heißt *endlich* (bzw. *von endlichem Typ* bzw. *ganz*), wenn der induzierte Morphismus der Koordinatenringe

$$\varphi_g : k[Y] \longrightarrow k[X]$$

endlich (bzw. von endlichem Typ bzw. ganz) ist.

Für einen Morphismus ist die Eigenschaft, von endlichem Typ zu sein, wesentlich schwächer als die Eigenschaft, endlich zu sein. Beispielsweise ist die Inklusion eines Körpers k in seinen Polynomring einer Veränderlichen

$$k \xrightarrow{\subset} k[X]$$

von endlichem Typ, aber nicht endlich.

Die von einer regulären Abbildung zwischen algebraischen Varietäten induzierten Ringmorphismen zwischen den Koordinatenringen sind stets von endlichem Typ. Denn Koordinatenringe sind als affine Algebren bereits von endlichem Typ über dem Grundkörper.

Im Falle einer Körpererweiterung

$$R \xrightarrow{\subset} S$$

fallen die Begriffe „ganz“ und „algebraisch“ zusammen.

3.7 Satz (Ganzheit und Endlichkeit)

Es seien $R \subset S$ zwei Ringe. Dann sind für ein Element $s \in S$ die folgenden Aussagen äquivalent:

i) Es ist s ganz über R

ii) Es ist $R[s]$ ein endlich erzeugter R-Modul

iii) Es gibt einen Ring R' mit $R[s] \subset R' \subset S$, welcher ein endlich erzeugter R-Modul ist.

Beweis. i) => ii) Wenn s eine ganze Gleichung n-ten Grades erfüllt, so bilden die Elemente

$$1 = s^0, s^1, s^2, ..., s^{n-1}$$

ein Erzeugendsystem des R-Moduls $R[s]$.

ii) => iii) Setze $R' := R[s]$.

iii) => i) Der R-Modul R' werde von den Elementen

$$b_1, ..., b_n \in R'$$

erzeugt. Wir betrachten die R-lineare Multiplikation

$$R' \longrightarrow R', \; b \mapsto s \cdot b .$$

Die Bilder der erzeugenden Elemente lassen sich darstellen als

$$s \cdot b_i = \sum_{j=1}^{n} r_{ij} \cdot b_j, \; i = 1, ..., n \text{ mit Koeffizienten } r_{ij} \in R .$$

Hieraus erhält man die Matrixgleichung

$$0 = C \cdot b$$

mit der Matrix

$$C = \left(s \cdot \delta_{ij} - r_{ij} \right) \in M(n \times n, R)$$

und dem Spaltenvektor

$$b = \left(b_i \right) \in M(n \times 1, R').$$

Wir bezeichnen mit

$$\tilde{C} \in M(n \times n, R)$$

die Matrix der algebraischen Komplemente von C. Aus der Gleichung

$$\det C \cdot b = \left(\tilde{C} \cdot C \right) \cdot b = \tilde{C} \cdot (C \cdot b) = 0$$

folgt

$$\det C = 0,$$

und dies stellt eine ganze Gleichung für $s \in S$ bzgl. R dar, q.e.d.

3.8 Lemma (Endlichkeit und Ganzheit)

Die Komposition endlicher (bzw. ganzer) Abbildungen ist wieder endlich (bzw. ganz). Für einen Morphismus von Ringen

$$\varphi : R \longrightarrow S$$

gilt:

- Aus der Endlichkeit von φ folgt seine Ganzheit.
- Ist φ von endlichem Typ, so folgt aus der Ganzheit von φ auch seine Endlichkeit.
- Die ganzen Elemente bzgl. φ bilden einen Unterrring von S.

Beweis. ad i) Es seien

$$\varphi : R \longrightarrow S \text{ und } \psi : S \longrightarrow T$$

zwei Ringmorphismen. Im Falle endlicher Abbildungen erhält man aus einem Erzeugendensystem von T bzgl. ψ und einem Erzeugendensystem von S bzgl. φ durch Produktbildung ein Erzeugendensystem von T bzgl. $\psi \circ \varphi$.

Im Falle ganzer Abbildungen sei $t \in T$ ganz bzgl. ψ. Dann gibt es eine ganze Gleichung

$$t^n + s_1 * t^{n-1} + ... + s_{n-1} * t + s_n = 0$$

mit Elementen

$$s_i \in S, i = 1,...,n .$$

Also ist insbesondere die Abbildung

$$R[s_1,...,s_n] \longrightarrow R[s_1,...,s_n][t].$$

ganz.

Außerdem ist die Abbildung

$$R \longrightarrow R[s_1,...,s_n]$$

endlich: Beweis durch Induktion über n. Im Fall $n = 0$ ist nicht zu zeigen. Im Induktionsschritt verwenden wir die Ganzheit von $s_n \in S$ über R und a posteriori über

$$R[s_1,...,s_{n-1}] .$$

Dann ist nach Satz 3.7 die Inklusion

$$R[s_1,...,s_{n-1}] \xrightarrow{\subseteq} R[s_1,...,s_n] = R[s_1,...,s_{n-1}][s_n]$$

endlich. Nach Induktionsvoraussetzung ist die Inklusion

$$R \xrightarrow{\subset} R[s_1,...,s_{n-1}]$$

endlich. Aus der Transitivitiät der Endlichkeit folgt die Endlichkeit von

$$R \xrightarrow{\subset} R[s_1,...,s_n],$$

womit der Induktionsschritt bewiesen ist.

Die Komposition der endlichen Abbildung

$$R \xrightarrow{\subset} R[s_1,...,s_n]$$

und der ganzen Abbildung

$$R[s_1,...,s_n] \xrightarrow{\subset} R[s_1,...,s_n][t]$$

ist wegen der Transitivität der Endlichkeit wieder endlich. Damit ist $t \in T$ in dem endlich erzeugten R-Modul

$$R[s_1,...,s_n][t]$$

enthalten, und ist nach Satz 3.7 ganz über R.

ad ii) Die erste Aussage ist Inhalt von Satz 3.7. Zum Beweis der zweiten Aussage sei

$$S = R[s_1,...,s_n].$$

Der Beweis der Endlichkeit von

$$\varphi : R \longrightarrow S$$

folgt durch Induktion über n unter Benutzung von Satz 3.7 und dem bereits bewiesenen Teil über die Transitivität der Endlichkeit.

Zum Beweis der dritten Aussage. Sind zwei Elemente $x, y \in S$ ganz über R, so ist $R[x, y]$ endlich über R, und nach dem gerdae bewiesenen Teil auch ganz über R, q.e.d.

Die Bedeutung der Ganzheit von Ringerweiterungen liegt in folgendem Fortsetzungssatz.

3.9 Satz (Fortsetzungssatz für ganze Ringerweiterungen)

Es sei

$$R \xrightarrow{\subset} S$$

ein injektiver, ganzer Morphismus von Ringen und K ein algebraisch-abgeschlossener Körper. Dann läßt sich jeder Ringmorphismus

$$\varphi : R \longrightarrow K$$

auf S fortsetzen, d.h. es gibt einen Ringmorphismu

$$\Phi : S \longrightarrow K$$

mit

$$\Phi \mid R = \varphi .$$

Beweis. i) Wir beweisen zunächst den Spezialfall, daß die R-Algebra S von einem einzigen Element erzeugt wird:

$$S = R[s].$$

Es gibt eine exakte Sequenz

$$0 \longrightarrow I \longrightarrow R[X] \longrightarrow R[s] \longrightarrow 0 .$$

Da das Element s eine ganze Gleichung über R erfüllt, enthält das Ideal

$$I \subset R[X]$$

ein normiertes Polynom

$$f_0(X) = X^n + r_1 \cdot X^{n-1} + ... + r_{n-1} \cdot X + r_n .$$

Der gegebene Ringmorphismus

$$\varphi : R \longrightarrow K$$

läßt sich fortsetzen zu einem Ringmorphismus

$$\varphi_X : R[X] \longrightarrow K[X],\ r \mapsto \varphi(r),\ X \mapsto X .$$

Wir bezeichnen mit $I_X \subset K[X]$ das von den Bildern

$$\varphi_X(I) \subset K[X]$$

erzeugte Ideal. Die gesuchte Fortsetzung läßt sich auf dem Quotienten

$$R[s] = R[X]/I$$

wohl-definieren als

$$\Phi : R[s] \longrightarrow K,\ \sum_\nu r_\nu \cdot s^\nu \mapsto \sum_\nu \varphi(r_\nu) \cdot \xi^\nu ,$$

sobald ein Element $\xi \in K$ gefunden ist mit

$$\varphi_X(f)(\xi) = 0 \in K \text{ für alle } f \in I .$$

Denn in diesem Fall folgt für jedes Polynom

$$f = \sum_\nu a_\nu \cdot s^\nu \in I$$

daß

$$\varphi_X(f)(\xi) = \sum_\nu \varphi(a_\nu) \cdot \xi^\nu = 0 \in K .$$

Die Polynome

$$f_0, f_1, ..., f_m \in R[X]$$

seien ein Erzeugendensystem des Ideals $I \subset R[X]$. Dann sind die Polynome

$$\varphi_X(f_0), \varphi_X(f_1), ..., \varphi_X(f_m) \in K[X]$$

ein Erzeugendensystem des Ideals $\varphi_X(I) \subset K[X]$, und es bleibt zu zeigen, daß alle Polynome

$$\varphi_X(f_\nu) \in K[X],\ \nu = 0, 1, ..., m$$

eine gemeinsame Nullstelle haben.

Das Polynom

$$\varphi_X(f_0)(X) = X^n + c_1 \cdot X^{n-1} + ... + c_{n-1} \cdot X + c_n$$

ist normiert. Nach Satz 3.5 ist zu zeigen, daß alle Elemente des Resultantensystems

$$Res_\alpha(\ \varphi_X(f_0); \varphi_X(f_1), ..., \varphi_X(f_m)\ ) \in K,\ |\alpha| = n ,$$

verschwinden. Wegen

$$R \cap I = \langle 0 \rangle$$

gilt bereits

$$Res_\alpha(\ f_0\ ;\ f_1,...,f_m\ ) = 0 \in R \cap I,\ |\alpha| = n\ .$$

Es folgt

$$Res_\alpha(\ \varphi_X(f_0)\ ;\ \varphi_X(f_1),...,\varphi_X(f_m)\ ) = \varphi(Res_\alpha(\ f_0\ ;\ f_1,...,f_m\ )) = 0 \in K,\ |\alpha| = n\ .$$

ii) Falls der Ring S endlich erzeug ist über R, so folgt die Behauptung durch Induktion über die Anzahl der Erzeugendenzahlen aus der in Teil i) bewiesenen Aussage.

iii) Im allgemeinen Fall folgt die Aussage durch transfinite Induktion als Anwendung des Zornschen Lemmas, q.e.d.

Der wichtigste Satz über endliche reguläre Abbildungen ist der Projektionssatz. Er heißt in der Sprache der Zariski Topologie:

3.10 Korollar (Projektionssatz für endliche Abbildungen)

Jede k-reguläre endliche Abbildung zwischen affinen k-Varietäten

$$g : X \longrightarrow Y$$

ist abgeschlossen, d.h. sie bildet abgeschlossenen Teilmenge von X auf abgeschlossene Teilmengen von Y ab.

Beweis. Es genügt den Fall zu betrachten, daß die Abbildung dichtes Bild hat, d.h. man kann annehmen

$$\overline{g(X)} = Y\ .$$

Nach Satz 2.16 ist dann die induzierte Abbildung der Koordinatenringe

$$\varphi_g : k[Y] \xrightarrow{\ \subset\ } k[X]$$

injektiv. Nach Voraussetzgung ist sie endlich, nach Lemma 3.7 also ganz. Damit liegt die Situation von Satz 3.9 vor. Es sei $y \in Y$ ein vorgegebener Punkt und

$$\alpha : k[Y] \longrightarrow K,\ f \mapsto f(y),$$

der zugehörige Auswertungshomomorphismus. Es gibt daher eine Fortsetzung

$$\tilde{\alpha} : k[X] \longrightarrow K\ .$$

Nach Lemma 2.9 ist dieser $k-$Algebra-Morphismus die Auswertung an einer Stelle $x \in X$. Man rechnet nach:

$$g(x) = y\ ,\ \text{q.e.d.}$$

3.11 Beispiel (Projektionssatz)

i) Die Projektion der Hyperbel auf die x-Achse ist keine endliche Abbildung, siehe Toolbeispiel 2.5. Der Morphismus der Koordinatenringe

$$\varphi : k[T] \xrightarrow{\ \subset\ } k\left[T, \frac{1}{T}\right]$$

ist nicht endlich. Das Bild der Projektion ist die gelochte affine Gerade, welche keine affine -Varietät ist.

ii) Die Projektion der Neil Parabel auf die -Achse ist eine endliche Abbildung, siehe Toolbeispiel 2.4. Das Bild ist die affine Gerade. Der Morphismus der Koordinatenringe

$$\varphi : k[T] \longrightarrow k[U^2, U^3],\ T \mapsto U^2,$$

ist endlich.

3.12 Definition *(Normalisierung)*

Die *Normalisierung* eines Integritätsbereiches R ist der ganze Abschluß von R bezüglich der Einbettung

$$R \xrightarrow{\subset} Q(R)$$

in seinen Quotientenkörper $Q(R)$. Der Integritätsbereich R heißt *normal*, wenn er ganz-abgeschlossen ist in seinem Quotientenkörper, d.h. wenn er mit seiner Normalisierung übereinstimmt.

3.13 Bemerkung *(Normalität)*

Jeder faktorielle Ring ist normal, insbesondere jeder Polynomring $k[T_1,...,T_n]$.

Beweis. Sei R ein faktorieller Ring und

$$\frac{f}{g} \in Q(R)$$

ein ganzes Element aus dem Quotientenkörper $Q(R)$. Da R faktoriell ist, können wir o.E. annehmen, daß die beiden Elemente $f, g \in R$ teilerfremd sind. Aus dem Bestehen einer ganzen Gleichung

$$\left(\frac{f}{g}\right)^m + r_1 \cdot \left(\frac{f}{g}\right)^{m-1} + ... + r_{m-1} \cdot \left(\frac{f}{g}\right) + r_m = 0 \text{ mit } r_i \in R,\ i = 1,...,m,$$

folgt nach Multiplikation mit g^m

$$-f^m = g \cdot \left(r_1 \cdot f^{m-1} + ... + r_{m-1} \cdot f^{m-2} + r_m \cdot g^{m-1} \right)$$

Also teilt g die Potenz f^m im Widerspruch zur vorausgesetzen Teilerfreiheit.

Die Faktorialität des Polynomrings ist der Satz von Gauss: Der Polynomring in einer Veränderlichen über einem Ring ist genau dann faktoriell, wenn der Ring selbst faktoriell ist, q.e.d.

3.14 Toolbeispiel *(Normalisierung)*

Die Normalisierung einer Kurve ist immer die affine Gerade bzw. der Polynomring in einer Veränderlichen. Die zugehörige reguläre Abbildung ist dann eine Parameterdarstellung eines dichten Teils der Kurve. In manchen Fällen ist auch die Normalisierung einer Fläche ein Polynomring, bzw. die affine Ebene. In diesen Fällen erhält man eine Parameterdarstellung eines dichten Teils der Fläche. Mit Hilfe von Singular berechnet man die Normalisierung.

- MyExamples/Normalization/Examples

i) Die Neil Parabel Z, siehe Beispiel 2.4, Teil i) und die affine Gerade sind nicht regulär isomorph: Sowohl der Koordinatenring der Neil Parabel $k[T^2, T^3]$ als auch der Koordinatenring $k[T]$ der affinen Geraden sind Integritätsbereiche und haben denselben Quotientenkörper $k(T)$. Der Ring $k[T^2, T^3]$ ist jedoch nicht normal: Das Element

$$T \in k(T^2, T^3)$$

ist ganz ist über $k[T^2, T^3]$, denn es erfüllt die ganze Gleichung

$$T^2 - r = 0 \quad \text{mit } r = T^2 \in k[T^2, T^3].$$

Es gehört aber nicht zum Koordinatenring der Neil Parabel. Die Normalisierung der *Neil-Parabel* ist die Abbildung

$$g : \boldsymbol{A}^1 \longrightarrow Z \subset \boldsymbol{A}^2, t \mapsto (t^2, t^3)$$

bzw. auf dem Niveau der Koordinatenringe die Inklusion

$$k[Z] \xrightarrow{\subset} k[T].$$

ii) Die Normalisierung des *Whitney-Umbrella*

$$W = \{ (x, y, z) \in \boldsymbol{A}^3 : y^2 - z \cdot x^2 = 0 \}$$

ist auf dem Niveau der Koordinatenringe die Inklusion

$$k[W] = k[X, Y, Z] \big/ \langle Y^2 - Z \cdot X^2 \rangle \xrightarrow{\subset} k[U, V],\ X \mapsto U, Y \mapsto U \cdot V, Z \mapsto V^2.$$

Der Whitney-Umbrella hat also den Koordinatenring

$$k[U, U \cdot V, V^2].$$

Auf dem Niveau der Varietäten ist die Normalisierung die reguläre Abbildung

$$g : \boldsymbol{A}^2 \longrightarrow W \subset \boldsymbol{A}^3, (u, v) \mapsto (u, u \cdot v, v^2).$$

Sie hat dichtes Bild, siehe Satz 2.16, es fehlt im Bild nur die z-Achse:

$$g(\boldsymbol{A}^2) = W - \{ (x, y, z) \in W : x = y = 0 \}$$

iii) Die Normalisierung der *5-nodalen Kurve*

$$Z = \{ (x, y) \in \boldsymbol{A}^2 : 32x^2 - 2097152y^{11} + 1441792y^9 - 360448y^7 + 39424y^5 - 1760y^3 + 22y - 1 = 0 \}$$

ist die reguläre Abbildung

$$g : \boldsymbol{A} \longrightarrow Z \subset \boldsymbol{A}^2,$$

$$g(t) = \left(\frac{1}{33554432} t^{11} - \frac{11}{2097152} t^9 + \frac{11}{32768} t^7 - \frac{77}{8192} t^5 + \frac{55}{512} t^3 - \frac{11}{32} t, \frac{1}{64} t^2 - \frac{1}{2} \right)$$

3.15 Satz *(Noethersche Normalisierung)*

Es sei

$$A = k[T_1, \ldots, T_n] \,/\, I$$

eine affine k-Algebra. Dann existiert ein k-Automorphismus

$$\varphi : k[T_1,...,T_n] \xrightarrow{\cong} k[T_1,...,T_n]$$

und eine Zahl $d \le n$, so daß die von der Inklusion induzierte Abbildung

$$k[T_1,...,T_d] \longrightarrow k[T_1,...,T_n]/\varphi(I) \cong A$$

injektiv und endlich ist (*Noether Normalisierung*).

Beweis. siehe [GP2002], Theor. 3.4.1.

Satz 3.15 besagt in geometrischer Formulierung, daß sich jede affine Varietät als verzweigte Überlagerung über einem wohlbestimmten affinen Raum darstellen läßt: Zu jeder affinen Varietät $X \subset \boldsymbol{A}^n(K)$ gibt es eine Zahl $d \le n$, so daß sich X - eventuell nach einer Koordinatentransformation des affinen Raumes $\boldsymbol{A}^n(K)$ - unter der regulären Abbildung

$$\boldsymbol{A}^n(K) \longrightarrow \boldsymbol{A}^d(K), (x_1,...,x_n) \mapsto (x_1,...,x_d)$$

surjektiv und endlich auf den affinen Raum $\boldsymbol{A}^d(K)$ projiziert.

3.16 Toolbeispiel (Noethersche Normalisierung)

Mit Hilfe von Singular berechnet man die Noethersche Normalisierung.

- MyExamples/NoetherNormalization/Examples

Affine Ebene mit transversaler affiner Geraden

$$Var(\langle X \rangle \cap \langle Y, Z \rangle) = Var(\langle X \cdot Y, X \cdot Z \rangle) \subset \boldsymbol{A}^3(K)$$

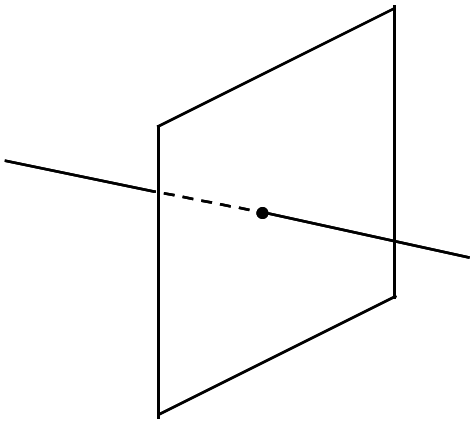


Abbildung 1: Y/Z-Ebene vereinigt mit X-Achse

Primärzerlegung

Ein weiterer wichtiger Bezug zwischen dem Koordinatenring einer affinen Varietät und ihren geometrischen Eigenschaften wird bei der Zerlegung einer affinen Varietät in irreduzible Komponenten deutlich. Hier entsprechen sich

- die Zerlegung des Verschwindungsideals in einen Durchschnitt von Primidealen
- und die Zerlegung der Varietät in eine Vereinigung irreduzibler Untervarietäten.

3.17 Definition (Primideale und Spektrum)

i) Ein echtes Ideal $I \underset{\neq}{\subset} R$ eines Ringes R heißt

- *Primideal*, wenn es mit einem Produkt von Elementen auch mindestens einen Faktor enthält, d.h.

$$f \cdot g \in I \Rightarrow f \in I \text{ oder } g \in I ,$$

- *Primärideal*, wenn gilt:

$$f \cdot g \in I \Rightarrow f \in I \text{ oder } g^k \in I \text{ für ein geeignetes } k \in \mathbf{N} .$$

- *maximal*, wenn das einzige echt größere Ideal nur der Ring R selbst ist:

$$I \underset{\neq}{\subset} J \Rightarrow J = R .$$

ii) Die Menge aller Primdideale

$$Spec\ R := \{\, p \subset R : p \text{ Primideal} \,\}$$

heißt das *Spektrum* von R, die Teilmenge aller maximalen Ideale

$$Specm\ R := \{\, m \in Spec\ R : m \text{ maximal} \,\}$$

heißt das *Maximalspektrum* von R.

Das Radikal eines Primärideals ist immer ein Primideal:

$$\sqrt{Primärideal} = Primideal .$$

3.18 Satz (Primärzerlegung)

In einem Noetherschen Ring R besitzt jedes Ideal $I \subset R$ eine endliche Zerlegung

$$I = \bigcap_{j \in J} q_j , \# J < \infty$$

mit Primäridealen q_j, die in folgendem Sinne unverkürzbar ist:

$$\bigcap_{i \neq j} q_i \not\subset q_j \text{ für alle } j \in J \text{ und } \sqrt{q_i} \neq \sqrt{q_j} \text{ für } i \neq j .$$

i) Eindeutig bestimmt sind die zugehörigen Primideale

$$p_j := \sqrt{q_j} , j \in J$$

und ebenso die Primärideale q_j zu minimalen Primidealen

$$p_j \in \{\, p_i : i \in J \,\}.$$

ii) Für ein reduziertes Ideal I sind alle Primärideale q_j bereits Primideale.

Beweis. Siehe [CLO1997], Chap. 4, §7.

3.19 Toolbeispiel (Primärzerlegung)

Mit Hilfe von Singular berechnet man die Primärzerlegung von Idealen:

- MyExamples/PrimaryDecomposition/Examples

Das Ideal

$$I := \langle X^2, X \cdot Y \rangle \subset k[X,Y]$$

ist nicht reduziert

$$\sqrt{I} = \langle X \rangle \subset k[X,Y].$$

Es hat die beiden verschiedenen, unverkürzbaren Zerlegungen

$$I = \langle X \rangle \cap \langle X^2, Y \rangle = \langle X \rangle \cap \langle X^2, X \cdot Y, Y^2 \rangle.$$

Mit den Primäridealen

$$q_1 := \langle X \rangle, q_2 := \langle X^2, Y \rangle$$

gilt

$$I = q_1 \cap q_2 .$$

Und mit den Primäridealen

$$q_1' := \langle X \rangle, q_2' := \langle X^2, X \cdot Y, Y^2 \rangle$$

gilt ebenfalls

$$I = q_1' \cap q_2' .$$

Die zugehörigen Primideale

$$p_1 := q_1 = q_1' = \langle X \rangle$$

und

$$p_2 := \sqrt{q_2} = \sqrt{q_2'} = \langle X, Y \rangle$$

stimmen überein. Das Primideal p_2 ist nicht minimal in der Menge $\{\, p_1, p_2 \,\}$, es gilt

$$q_2 = \langle X^2, Y \rangle \neq q_2' = \langle X^2, X \cdot Y, Y^2 \rangle .$$

Geometrisch definieren die beiden Ideale I und $\sqrt{I}$ dieselbe Varietät

$$Var(I) = Var(\sqrt{I}) = y - Achse .$$

Um beide Ideale auch geometrisch unterscheiden zu können, muß man die Kategorie der affinen Varietäten zur Kategorie der affinen Schemata erweitern. Auf der Seite der Algebra handelt es sich dann nicht mehr um affine k-Algebren, sondern in einer ersten Verallgemeinerung um endlich erzeugte, aber nicht reduzierte k-Algebren wie

$$k[X,Y]\Big/\langle X^2, X\cdot Y, Y^2\rangle \cong k \oplus k\cdot X \oplus k\cdot Y\,.$$

Dann kann man dem nicht-reduzierten Ideal I als affines Schema die y-Achse mit einem eingebetteten Doppelpunkt zuordnen. Die Theorie der Schemata wird z.B. in [EH2000] behandelt.

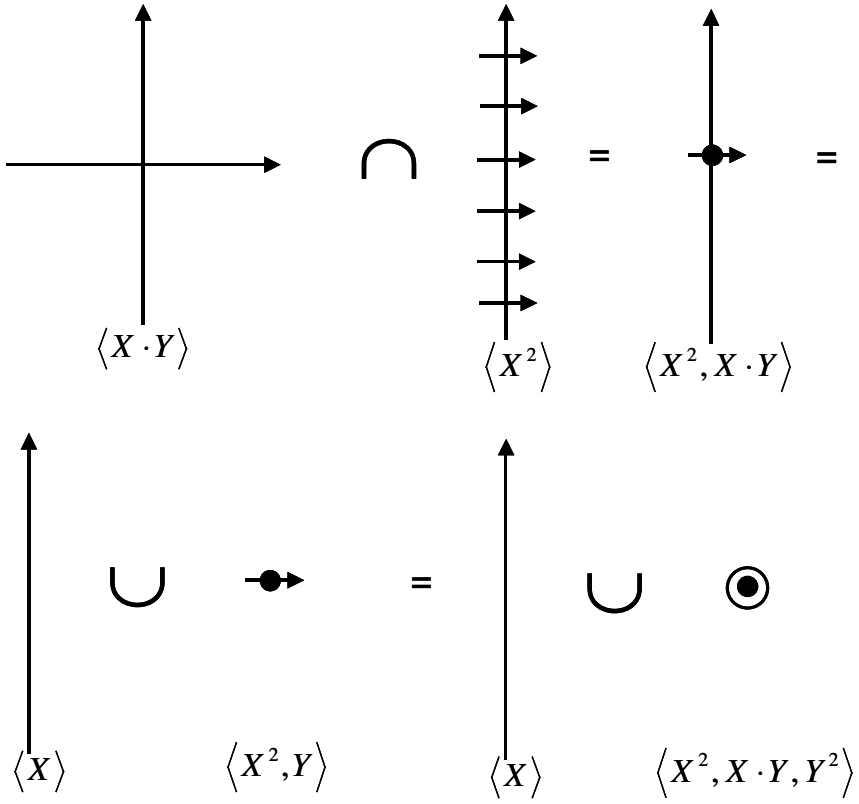


Abbildung 2: Eingebetteter Doppelpunkt

Wie bei jedem topologischen Raum kann man auch bzgl. der Zariski Topologie einer affinen k-Varietät von irreduziblen Mengen sprechen.

3.20 Definition *(Irreduzible Varietät)*

Eine nicht-leere k-affine Varietät

$$\varnothing \neq X \subset \boldsymbol{A}^n(K)$$

heißt *irreduzibel*, wenn sie sich nicht darstellen läßt in der Form

$$X = X_1 \cup X_2$$

mit zwei nichtleeren, voneinander verschiedenen, k-Varietäten

$$X_i \subset \boldsymbol{A}^n(K), i = 1, 2 .$$

Andernfalls heißt sie *reduzibel*. Die leere Menge heißt reduzibel.

3.21 Satz *(Irreduzible Varietät und Primideal)*

Für eine affine k-Varietät $X \subset \boldsymbol{A}^n(K)$ sind äquivalent:

- Es ist $X \subset \boldsymbol{A}^n(K)$ irreduzibel
- Das Verschwindungsideal $Id(X) \subset k[T_1,...,T_n]$ ist ein Primideal.
- Der Koordinatenring $k[X]$ ist ein Integritätsbereich.

Beweis. Die Äquivalenz der beiden letzten Aussagen folgt aus der Darstellung als Quotient

$$k[X] = k[T_1,...,T_n] / Id(X) .$$

Zur Äquivalenz der beiden ersten Aussagen:

i) Es sei $X \subset \boldsymbol{A}^n(K)$ irreduzibel. Zu zeigen ist, daß

$$Id(X) \subset k[T_1,...,T_n]$$

ein Primideal ist. Dazu seien zwei Elemente $f, g \in k[T_1,...,T_n]$ vorgegeben mit

$$f \cdot g \in Id(X).$$

Mit

$$Var(f) \cup Var(g) = Var(f \cdot g) \supset Var(Id(X)) = X$$

erhält man die Zerlegung

$$X = X \cap Var(f \cdot g) = [X \cap Var(f)] \cup [X \cap Var(g)].$$

Wegen der Irreduzibilität gilt o.E.

$$X \cap Var(f) = X .$$

Es folgt

$$X \subset Var(f) \text{ oder } f \in Id(X).$$

ii) Es sei $Id(X)$ ein Primideal. Zu zeigen ist die Irreduzibilität von X. Annahme: Es gibt eine Zerlegung

$$X = X_1 \cup X_2$$

mit zwei nichtleeren, abgeschlossenen echten Teilmengen $X_i \underset{\neq}{\subset} X$. Dann gilt

$$Id(X) = Id(X_1 \cup X_2) = Id(X_1) \cap Id(X_2)$$

und

$$Id(X_i) \underset{\neq}{\supset} Id(X).$$

Es gibt also Elemente

$$f_i \in Id(X_i) - Id(X)$$

mit

$$f_1 \cdot f_2 \in Id(X_1) \cap Id(X_2) = Id(X)$$

im Widerspruch zur Primalität von $Id(X)$, q.e.d.

3.22 Definition (Rationaler Funktionenkörper)

Der Körper $k(X)$ der *rationalen Funktionen* einer irreduziblen affinen k-Varietät X ist der Quotientenkörper ihres Koordinatenringes

$$k(X) := Q(k[X]).$$

3.23 Bemerkung (Rationale Funktionen)

i) Eine nicht-leere offene Teilmenge einer irreduziblen affinen Varietät ist dicht.

Zum Beweis sei

$$\emptyset \neq U \underset{\neq}{\subset} X$$

eine offene Teilmenge der irreduziblen Varietät X. Mit

$$X_1 := X - U \ , \ X_2 := \overline{U}$$

erhält man eine Zerlegung

$$X := X_1 \cup X_2$$

in abgeschlossene Teilmengen. Aus der Irreduzibilität folgt

$$X = X_2 = \overline{U} \ .$$

ii) Es sei X eine irreduzible k-Varietät und $g \in k[X]$ eine von Null verschiedene reguläre Funktion auf X. Nach Teil i) ist die Menge

$$D(g) := X - Var_X(\langle g \rangle) \subset X$$

eine dichte, offene Teilmenge. Insbesondere hat jede rationale Funktion

$$\frac{f}{g} \in k(X)$$

auf der offenen dichten Menge

$$D(g) \subset X$$

einen wohldefinierten Funktionswert.

3.24 Korollar (Zerlegung in irreduzible Komponenten)

Es sei $X \subset \boldsymbol{A}^n(K)$ eine nicht-leere affine k-Varietät. Dann entsprechen die irreduziblen Untervarietäten von X bijektiv den Primidealen des Koordinatenringes unter den Abbildungen

$$\{ Y \subset X : Y \text{ irreduzibel} \} \underset{Var_X}{\overset{Id_{k[X]}}{\rightleftarrows}} Spec\, k[X].$$

Die Primzerlegung

$$Id(X) = \bigcap_{j \in J} p_j$$

liefert eine Zerlegung

$$X = \bigcup_{j \in J} Var(p_j)$$

in irreduzible Untervarieäten, sie heißen *irreduzible Komponenten* von X .

Für einen algebraisch-abgeschlossenen Koordinatenkörper $k = \bar{k} = K$ gilt:

3.25 Korollar *(Punkte und maximale Ideale)*

Es sei $X \subset \boldsymbol{A}^n(K)$ eine nicht-leere, affine K -Varietät mit algebraisch-abgeschlossenem Definitionskörper. Unter den Zuordnungen von Korollar 3.21 entsprechen die maximalen Ideale des Koordinatenringes bijektiv den Punkten von X

$$Id_{K[X]} : X \xrightarrow{\cong} Specm\ K[X].$$

Beweis. Für jeden Punkt

$$x = (x_1, ..., x_n) \in X$$

ist die 1-punktige Teilmenge

$$\{ x \} \subset X$$

abgeschlossen in der K -Topologie und irreduzibel, denn

$$\{ x \} = Var_X(\langle T_i - x_i : i = 1, ..., n \rangle) \text{ mit } T_i - x_i \in K[T_1, ..., T_n].$$

An dieser Stelle brauchen wir, daß der Definitionskörper den Koordinatenkörper enthält, daß also Definitions- und Koordinatenkörper übereinstimmen.

Das Bild der Einschränkung

$$Id_{K[X]} \mid X \xrightarrow{\cong} Spec\ K[X]$$

auf die 1-punktigen irreduziblen Teilmengen liegt sogar schon in $Specm\ K[X]$: Sei

$$m_x := Id_{K[X]} \subset K[X]$$

das Verschwindungsideal eines Punktes $x \in X$. Zum Nachweis der Maximalität des Ideals m_x ist für jedes $h \notin m_x$ zu zeigen:

$$\langle h \rangle + m_x = \langle 1 \rangle .$$

Wegen $h(x) \neq 0$ gilt

$$\frac{1}{h(x)} \in K ,$$

so daß durch

$$g := 1 - \frac{h}{h(x)}$$

eine reguläre Funktion $g \in K[X]$ definiert wird. Es gilt sogar $g \in m_x$, und es folgt

$$\frac{h}{h(x)} + g = 1 .$$

Als Einschränkung einer injektiven Abbildung, siehe Korollar 3.24, ist die Abbildung selbst injektiv. Die Abbildung ist auch surjektiv: Für ein vorgegebenes maximales Ideal

$$m \subset K[X]$$

gilt nach dem Hilbertschen Nullstellensatz, siehe Bemerkung 2.12,

$$m = Id_{K[X]}(Var_X(m)).$$

An dieser Stelle benötigen wir die algebraische Abgeschlossenheit des Koordinatenkörpers. Insbesondere gibt es einen Punkt $x \in Var(m)$. Aus der Inklusion der beiden maximalen Ideale

$$m_x \supset Id_{K[X]}(Var_X(m)) = m$$

folgt ihre Gleichheit, q.e.d.

In Korollar 3.25 ist die Voraussetzung wesentlich, daß auch der Definitionskörper der affinen k-Varietät algebraisch abgeschlossen ist. Andernfalls brauchen 1-punktigen Mengen in $X \subset \boldsymbol{A}^n(K)$ keinesfalls abgeschlossen zu sein. Gegenbeispiel: Im Falle $k = \boldsymbol{Q}$ ist die kleinste abgeschlossene Menge der k-Varietät

$$X := Var\left(\left\langle T^2 + 1 \right\rangle \right) \subset A^1(\boldsymbol{C}),$$

welche den Punkt $i \in X$ enthält, die 2-punktige Menge

$$\{ i, -i \} = X$$

4 Gröbner Basics

Die Gröbner Theorie stellt die entscheidenden Algorithmen zum expliziten Rechnen mit Idealen in Polynomringen zur Verfügung. Als wichtigste Frage läßt sich damit algorithmisch klären: Gehört ein Polynom zu einem Ideal oder nicht?

Das Prinzip aller Algorithmen zum Rechnen mit Polynomen und Idealen in Polynomringen lautet:

Reduktion auf Monome

Jedes Ideal in einem Polynomring hat ein endliches Erzeugendensystem. Aber nicht alle Erzeugendensysteme sind in gleicher Weise geeignet für die Implementierung von Algorithmen. Die ausgezeichneten Erzeugendensysteme heißen Gröbner Basen, ihre Elemente erfüllen auch noch eine Bedingung an die führenden Monome.

Divisions Algorithmus

Der Divisionsalgorithmus verallgemeinert den bekannte Divisionsalgorithmus mit Rest auf den Fall von Polynomen mehrerer Veränderlicher. Mit Hilfe des Divisionsalgorithmus läßt sich für den Polynomring in einer einzigen Veränderlichen entscheiden, ob ein Polynom zu einem gegebenen Ideal gehört oder nicht: Das Ideal ist ein Hauptideal. Man dividiert durch ein erzeugendes Polynom des Hauptideals und betrachtet den Rest. Genau dann wenn der Rest verschwindet, gehört das Polynom zu dem gegebenen Ideal.

Im Falle mehrerer Veränderlichen führt die analoge Fragestellung auf ein endliches Erzeugendensystem des Ideals. Man braucht daher als erstes einen Algorithmus, welcher den Rest der simultanen Division eines Polynoms mit den Polynomen eines Erzeugendensystems als Divisoren berechnet.

Der Divisionsalgorithmus hat wie im Falle einer Veränderlichen zwei Schritte:

- Probedivision durch das führende Monom eines Divisors
- und Reduktion des Dividenden durch Subtraktion des Produktes.

Die Auszeichung des führenden Monoms eines Polynoms setzt eine Ordnung auf den Monomen voraus. Bei Polynomen einer Veränderlichen wird sie durch den Grad der Monome gegeben. Bei Polynomen mehrerer Veränderlichen gibt es keine ausgezeichnete Anordnung ihrer Monome. Es lassen sich vielmehr verschiedene Monomordnungen definieren.

4.1 Definition (Monome und Monomordnung)

i) Die *Monome* eines Polynomringes

$$R = k[T_1,...,T_n]$$

sind die Produkte der Form

$$T_1^{\alpha_1} \cdot T_2^{\alpha_2} \cdot ... \cdot T_n^{\alpha_n}, \alpha_1, \alpha_2, ..., \alpha_n \in \mathbf{N} .$$

Der *Grad* eines Monoms ist definiert als die Summe der Exponenten

$$\deg\left(T_1^{\alpha_1} \cdot T_2^{\alpha_2} \cdot ... \cdot T_n^{\alpha_n}\right) := \sum_{j=1}^{n} \alpha_j .$$

Durch Multiplikation eines Monoms mit einem Element des Grundkörpers entsteht ein *Term*.

ii) Die Monome des Polynomringes $k[T_1,...,T_n]$ entsprechen bijektiv den Elementen

$$\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in \boldsymbol{N}^n .$$

Eine Ordnung ">" auf der Menge $\boldsymbol{N}^n$ heißt *Monomordnung*, wenn gilt:

- Für alle $\alpha, \beta \in \boldsymbol{N}^n$ gilt entweder $\alpha = \beta$ oder $\alpha > \beta$ oder $\beta > \alpha$ (Totalität)
- Für alle $\alpha \in \boldsymbol{N}^n$ gilt $\alpha \geq 0$, d.h. entweder $\alpha > 0$ oder $\alpha = 0$ (Beschränktheit nach unten)
- Wenn $\alpha > \beta$, so gilt für alle $\gamma \in \boldsymbol{N}^n$ auch $\alpha + \gamma > \beta + \gamma$ (Verträglichkeit mit der Monoidstruktur von $(\boldsymbol{N}^n, +)$)

Eine Monomordnung heißt *graduiert*, wenn gilt:

$$\deg(\alpha) > \deg(\beta) \Rightarrow a > \beta .$$

Hinweis. Die Bezeichnung ist nicht einheitlich in der Literatur. In manchen Büchern, z.B. [BW1998], werden die Bezeichungen „Term“ und „Monom“ in genau umgekehrter Bedeutung gebraucht.

Bei der Gleichsetzung der Monome des Polynomringes $k[T_1,...,T_n]$ mit den Elementen aus $\boldsymbol{N}^n$ als ihren Exponenten geht die Multiplikation von Monomen über in die Addition der Exponenten. Das von den Monomen bzgl. der Multiplikation gebildete Monom ist also isomorph zum freien Abelschen Monoid $(\boldsymbol{N}^n, +)$ mit n Erzeugenden.

Da wir uns über einem Körper k befinden, spielt hier die Unterscheidung von Monomen und Termen keine große Rolle. Jedes Polynom f hat eine eindeutige Darstellung als Summe nicht-verschwindender Terme und bestimmt eine zugehörige Menge $Mon(f)$ von Monomen.

*4.2 **Definition** (Monomiales Ideal, Koordinatenunterraum)*

Ein *monomiales Ideal*

$$I \subset k[T_1,...,T_n]$$

ist ein Ideal, das ein Erzeugendensystem aus Monomen besitzt. Eine durch ein monomiales Ideal I definierte Varietät

$$Var(I) \subset \boldsymbol{A}^n(K)$$

heißt *monomiale Varietät*. Ein *Koordinatenunterrraum* von $\boldsymbol{A}^n(K)$ ist eine monomiale Varietät

$$Var\left(\left\langle T_{i_1},...,T_{i_d}\right\rangle\right),$$

die durch Koordinatenfunktionen definiert wird.

Ein Polynom gehört genau dann zu einem monomialen Ideal, wenn alle Monome des Polynoms dazugehören. Wenn ein Monom zu einem monomialen Ideal gehört, dann ist es bereits Vielfaches eines der monomialen Erzeuger des Ideals. Das Radikal eines monomialen Ideals ist wieder monomial.

4.3 Lemma (Koordinatenunterraum)

Jede monomiale Varietät

$$X = Var(\langle f_1,...,f_m \rangle)$$

ist endliche Vereinigung von Koordinatenunterräumen. Die Koordinatenunterrräume E_i, die bei einer unverkürzbaren Darstellung

$$X = \bigcup_{i \in I} E_i\ ,\ E_i \not\subset E_j \text{ für } i \neq j\ ,$$

auftreten, sind die irreduziblen Komponenten von X.

Beweis. Zunächst ist die durch ein Monom definierte Hyperfläche

$$f = T_{i_1}^{\alpha_1} \cdot ... \cdot T_{i_r}^{\alpha_r}, \alpha_1,...,\alpha_r \in \mathbf{N} - 0$$

Vereinigung von Koordinaten-Hyperflächen

$$Var(f) = Var(\ T_{i_1}^{\alpha_1} ... \cdot T_{i_r}^{\alpha_r}) = Var(T_{i_1}^{\alpha_1}) \cup ... \cup Var(T_{i_r}^{\alpha_r}) = Var(T_{i_1}) \cup ... \cup Var(T_{i_r}).$$

Die gegebene monomiale Varietät X ist Durchschnitt von monomialen Hyperflächen

$$X = \bigcap_{i=1}^{m} Var(f_i),$$

und jede Varietät $Var(f_i)$ ist Vereinigung von Koordinaten-Hyperflächen. Unter Verwendung des Distributivgesetzes erhält man für X eine Darstellung als Vereinigung von Durchschnitten von Koordinatenhyperflächen. Ein Durchschnitt von Koordinatenhyperflächen ist aber ein Koordinatenunterraum, q.e.d.

Aus der Darstellung in Lemma 4.3 leitet sich die Forderung ab, die Dimension einer affinen Varietät so zu definieren, daß sich für eine monomiale Varietät das Maximum der Vektorraumdimensionen der auftretenden Koordinatenunterräume ergibt.

4.4 Beispiel (Monomordnung)

Die wichtigsten Monomordnungen des Polynomringes $k[T_1,...,T_n]$ sind:

Monomordnung	$\alpha > \beta$	**Singular**	**Macaulay**
Lexikographisch	Der am weitesten links stehende, von Null verschiedene Eintrag von $\gamma = (\gamma_1, \gamma_2,..., \gamma_n) := \alpha - \beta$ ist positiv	lp	Lex

Monomordnung	$\alpha > \beta$	**Singular**	**Macaulay**
Graduiert lexikographisch	• Entweder $\deg(\alpha) > \deg(\beta)$ • oder $\deg(\alpha) = \deg(\beta)$ und $\alpha >_{Lex} \beta$	Dp	GLex
Rückwärts lexikographisch	Der am weitesten rechts stehende, von Null verschiedene Eintrag von $\gamma = (\gamma_1, \gamma_2, ..., \gamma_n) := \alpha - \beta$ ist negativ	rp	RevLex
Graduiert rückwärts lexikographisch	• Entweder $\deg(\alpha) > \deg(\beta)$ • oder $\deg(\alpha) = \deg(\beta)$ und $\alpha >_{RevLex} \beta$	dp, default	GRevLex, default
r-te Eliminationsordnung, $r \in \{1,...,n\}$	• Entweder $\sum_{i=1}^{r} \alpha_i > \sum_{i=1}^{r} \beta_i$ • oder $\sum_{i=1}^{r} \alpha_i = \sum_{i=1}^{r} \beta_i$ und $\alpha >_{GRevLex} \beta$	(dp(r), dp(n-r))	Eliminate r

Die lexikographische Anordnung entspricht der alphabetischen Anordnung von Wörtern mit fester Länge n, wobei die großen Wörter am Anfang stehen:

$$a > b > c > ... > y > z.$$

Im Polynomring $k[X,Y]$ gilt z.B.

$$X^2 >_{Lex} X \cdot Y >_{Lex} X >_{Lex} Y .$$

Im Polynomring $k[X,Y,Z]$ gilt z.B.

$$X^2 \cdot Y \cdot Z^2 >_{Lex} X \cdot Y^3 \cdot Z \text{, aber } X \cdot Y^3 \cdot Z >_{RevLex} X^2 \cdot Y \cdot Z^2 .$$

Die r-te Eliminationsordnung hat die Eigenschaft, daß ein Monom mit einer der Variablen

$$T_1, ..., T_r$$

größer ist als jedes Momon, das nur die Variablen

$$T_{r+1}, ..., T_n$$

enthält. Diese Eigenschaft besitzt die Lex-Ordnung für jedes $r \in \{1,...,n\}$.

*4.5 **Definition** (Führendes Monom, führendes Ideal)*

In einem Polynomring mit einer festen Monomordnung

$$R = (k[T_1, ..., T_n], <)$$

lassen sich die Monome eines Polynoms $f \in R$ eindeutig nach absteigender Größe anordnen.

i) Für ein von Null verschiedenes Polynom $0 \neq f \in R$ heißt

- das größte seiner Monome das *führende Monom* $lm(f)$,

- der zugehörige Term der *führende Term* $lt(f)$
- und sein Koeffizient der *führende Koeffizient* $lc(f)$:

$$lt(f) = lc(f) \cdot lm(f).$$

ii) Das *führende Ideal* eines Ideal

$$0 \neq I \subset R$$

ist das monomiale Ideal

$$lt(I) := \langle lt(f) : f \in I, f \neq 0 \rangle,$$

welches von den führenden Termen der nicht-verschwindenden Elemente aus I erzeugt wird.

Eine gegebene Monomordnung definiert auf dem gesamten Polynomring eine partielle Ordnung.

4.6 Definition (Induzierte Ordnung im Polynomring)

Es sei $(M, >)$ die Menge aller Monome im Polynomring $k[T_1,...,T_n]$ versehen mit einer beliebigen, aber festen Monomordung.

i) Es bezeichne $P_{fin}(M)$ die Menge aller endlichen Teilmengen von M. Jedes nicht-leere Element $A \in P_{fin}(M)$ hat ein eindeutig bestimmtes Maximum

$$\max A \in M.$$

Für zwei Elemente $A, B \in P_{fin}(M)$ definieren wir die *Ordnung* $A \leq B$ durch Induktion über die Anzahl der Elemente von A:

- Für $A = \varnothing$ gilt $A \leq B$ für beliebiges B.
- Für $A \neq \varnothing$ gilt $A \leq B$ genau dann, wenn $B \neq \varnothing$ und

$$\max A < \max B \text{ oder } (\max A = \max B \text{ und } \max(A - \max A) \leq \max(B - \max B))$$

ii) Für zwei Polynome $f, g \in k[T_1,...,T_n]$ definieren wir die *partielle Ordnung* $f \leq g$ durch die Vorschrift:

$$f \leq g :\Leftrightarrow Mon(f) \leq Mon(g).$$

Die Ordnung $(k[T_1,...,T_n], \leq)$ ist *Noethersch*, ebenso wie die vorgegebene Monomordnung, d.h. jede absteigende Folge von Elementen wird nach endlich vielen Schritten stationär.

Im Polynomring einer Veränderlichen ist jedes Ideal ein Hauptideal

$$I = \langle g \rangle \subset k[T].$$

Die Frage der Zugehörigkeit eines Polynoms zu einem gegebenen Ideal reduziert sich damit auf die Frage nach der Teilbarkeit zweier Polynome: Für

$$f \in k[T]$$

gilt

$$f \in I \Leftrightarrow g \text{ teilt } f .$$

Um die Teilbarkeit zu prüfen, reduziert man den Dividenden f modulo des Divisors g vermöge sukzessiver Probedivision durch den Leitterm von g nach dem aus der Schule bekannten Algorithmus „Division mit Rest“. Man erhält:

$$f = a \cdot g + r \text{ mit } a, r \in k[X] \text{ und } r = 0 \text{ oder } \deg(r) < \deg(g).$$

Der Rest r über die Zugehörigkeit zum Ideal:

$$f \in I \Leftrightarrow r = 0 .$$

Der Polynomring in mehr als einer Veränderlichen ist kein Hauptidealring. Ideale in $k[T_1,...,T_n]$ sind zwar weiterhin endlich erzeugt, aber benötigen i.a. ein Erzeugendensystem aus mehr als einem Element

$$I = \langle g_1,..., g_k \rangle \subset k[T_1,...,T_n].$$

Um die Zugehörigkeit eines Polynoms

$$f \in k[T_1,...,T_n]$$

zu I zu klären, wird eine Reduktion von f nach der Menge $\{ g_1,..., g_k \}$ gesucht, d.h. eine Darstellung

$$f = \sum_{i=1}^{k} a_i \cdot g_i + r \text{ mit } a_i, r \in k[T_1,...,T_n],$$

so daß man wieder allein durch Betrachtung des Restes r die Frage der Zugehörigkeit entscheiden kann.

Man kann zunächst den Divisionsalgorithmus

$$f : g \text{ mit zwei Polynomen } f, g \in k[T] \text{ einer Veränderlichen}$$

erweitern zu einem Divisionsalgorithmus

$$f : \{ g_1,..., g_k \} \text{ mit Polynomen } f, g_i \in k[T_1,...,T_n] \text{ mehrerer Veränderlicher.}$$

*4.7 **Beispiel** (Division mit Rest)*

Als Beispiel soll im Polynomring $(k[X,Y], >_{Lex})$ das Polynom

$$f = X \cdot Y^2 - X \in k[X, Y]$$

durch die Divisoren

$$\{ g_1 = X \cdot Y + 1,\ g_2 = Y^2 - 1 \}$$

geteilt werden. Bzgl. der lexikographischen Ordnung gilt

$$lt(f) = X \cdot Y^2 >_{Lex} lt(g_1) = X \cdot Y >_{Lex} lt(g_2) = Y^2 .$$

Probedivision durch den Leitterm von g_1 liefert

$$lt(f) = Y \cdot lt(g_1)$$

also

$$f : g_1 = Y \; Rest - X - Y$$

Im nächsten Schritt gilt

$$lt(-X - Y) = -X \; ,$$

so daß ist keine weitere Division durch $lt(g_1)$ oder $lt(g_2)$ möglich ist. Der Divisionsalgorithmus terminiert mit einem von Null verschiedenen Rest:

$$f = Y \cdot g_1 + r \text{ mit } r = -X - Y \; .$$

Beginnt man dagegen mit der Probedivision durch den Leitterm von g_2, so erhält man

$$lt(f) = X \cdot lt(g_2)$$

also

$$f = X \cdot g_2$$

mit verschwindendem Rest

$$r = 0 \; .$$

Also gehört f zum Ideal I, obwohl bei einer ungünstigen Reihenfolge von Divisionen der Algorithmus mit einem von Null verschiedenen Rest terminiert. Das Verschwinden des Restes ist zwar eine hinreichende, aber keine notwendige Bedingung für die Zugehörigkeit zum Ideal I. Es wird sich jedoch herausstellen, daß bei Verwendung einer Gröbner Basis das Verschwinden des Restes auch notwendig ist.

4.8 Algorithmus *(Division mit Rest)*

Vorgegeben: Polynomring mit Monomordnung $(k[T_1,...,T_n], <)$

Input:

- Dividend: Polynom f
- Divisoren: Endliche Menge von Null verschiedener Polynomen $G = \{ g_1,..., g_k \}$

Output: Polynom r, Menge von Polynomen $\{ a_1,..., a_k \}$ mit folgenden Eigenschaften:

- $f = \sum_{i=1}^{k} a_i \cdot g_i + r$
- Für jedes i = 1,...,k mit $a_i \neq 0$ gilt $lt(f) \geq lt(a_i \cdot g_i)$
- Im Falle $r \neq 0$ ist kein Term von r durch einen der Leitterme $lt(g_1),...,lt(g_k)$ teilbar

$r = 0,\ a_1 = ... = a_k = 0$	
$p = f$	
while $p \neq 0$	
	$i = 1$
	divisionOccured = false
	while $i \leq k$ and divisionOccured = = false
	if $lt(g_i)$ divides $lt(p)$ $a_i = a_i + \frac{lt(p)}{lt(g_i)},\ p = p - \frac{lt(p)}{lt(g_i)} g_i$, divisionOccured = true else $i = i + 1$
	if divisionOccured = = false $r = r + lt(p),\ p = p - lt(p)$

Tabelle 2: Divisionsalgorithmus

Der Divisionsschritt ist genau dann möglich, wenn der Leitterm des Polynoms p einen Term enthält, der durch den Leitterm eines der Divisoren $g_1,...,g_k$ teilbar ist. Die anschließende Multiplikation und Subtraktion eliminiert den Leitterm von p (Top Reduktion) und addiert ggf. kleinere Terme:

$$p > p - \frac{lt(p)}{lt(g_i)} \cdot g_i$$

Der Algorithmus terminiert, da die Teilordnung auf den Polynomen Noethersch ist.

4.9 **Toolbeispiel** *(Divisionsalgorithmus)*

Für die Implementierung des Divisionsalgorithmus 4.8 mit Hilfe des Tools Macaulay2 siehe

- MyExamples/DivisionAlgorithm/Examples

4.10 **Definition** *(Normalform bzgl. einer Divisorenmenge)*

Im Polynomring mit einer festen Monomordnung

$$R = (k[T_1,...,T_n], <)$$

seien

$$G = \{ g_1,...,g_s \}$$

eine endliche Menge nicht verschwindender Elemente und

$$\langle G \rangle := \langle g_1,...,g \rangle \subset R$$

das von ihnen erzeugte Ideal.

i) Eine *Standardarddarstellung bezüglich* G eines nicht verschwindenden Elementes $f \in \langle G \rangle$ ist eine Summendarstellung

$$f = \sum_{i=1}^{s} a_i \cdot g_i \text{ , } a_i \in R \text{ , } i = 1,...,s \text{ ,}$$

in der sich keine führenden Terme einzelner Summanden herausheben:

$$lt(\ f\ ) \geq lt(\ a_i \cdot g_i\ ) \textit{ für alle i mit } a_i \neq 0 \text{ .}$$

ii) Eine *Normalform bezüglich* G eines Elementes $f \in R$ ist ein Element

$$NF(f \mid G) \in R$$

mit folgenden Eigenschaften:

- Falls $NF(f \mid G) \neq 0$, so ist $NF(f \mid G)$ durch die Elemente von G nicht weiter top-reduzierbar:

$$lt(\ NF(f \mid G)\ ) \notin lt(\langle G \rangle).$$

- Für die Differenz gilt

$$f - NF(f \mid G) \in \langle G \rangle$$

Falls sogar kein einziger Term von $NF(f \mid G)$ in $lt(\langle G \rangle)$ liegt, heißt die Normalform *reduziert*.

Algorithmus 4.8 liefert für das Polynom $f \in R$ bzgl. der endlichen Menge G mit dem Rest der Division eine reduzierte Normalform bezüglich G

$$NF(f \mid G) = r$$

und eine zugehörige Standarddarstellung bezüglich G für die Differenz

$$f - N(f \mid G) = \sum_{i=1}^{k} a_i \cdot g_i \text{ .}$$

Offensichtlich kann man die Mitgliedschaft von f im Ideal $\langle G \rangle$ auch an einer Normalform $NF(f \mid G) \in R$ entscheiden. Welche Bedingung muß die Familie G erfüllen, damit gilt:

$$f \in \langle G \rangle \Leftrightarrow NF(f \mid G) = 0 \text{ ?}$$

Während die Implikation

$$NF(f \mid G) = 0 \Rightarrow f \in \langle G \rangle$$

für jede Familie G gilt, wird Satz 4.16 für eine Gröbner Basis G die Umkehrung liefern und zeigen, daß eine Gröbner Basis durch diese Eigenschaft sogar charakterisiert ist.

In Beispiel 4.7 terminierte der Divisionsalgorithmus mit den Divisoren

$$\{\, g_1 = X \cdot Y + 1,\ g_2 = Y^2 - 1 \,\}$$

in der Darstellung

$$f = Y \cdot g_1 + r \text{ mit } r = -X - Y$$

mit einem nicht-verschwindenden Rest. Trotzdem gilt

$$f \in \langle g_1, g_2 \rangle,$$

denn

$$r = -Y - X = -Y \cdot g_1 + X \cdot g_2 \in \langle g_1, g_2 \rangle.$$

Allerdings heben sich in dieser Darstellung die Leitterme von g_1 und g_2 gegeneinander heraus, so daß

$$lt(r) < lt(g_1) \text{ und } lt(r) < lt(g_2):$$

Der Leitterm $lt(r)$ liegt nicht in dem Ideal, das durch die Leitterme von g_1 und g_2 erzeugt wird:

$$lt(r) = -X \notin \langle\, lt(g_1), lt(g_2) \,\rangle = \langle\, X \cdot Y, Y^2 \,\rangle.$$

Gröbner Basen

Der Algorithmus aus 4.8 liefert keinen eindeutigen Rest, aus dem sich die Mitgliedschaft des Dividenden in dem von den Divisoren erzeugten Ideal ablesen ließe. Jedoch läßt sich die Brauchbarkeit des Divisionsalgorithmus retten, wenn man sich bei den Divisoren auf eine bestimmte Art von Erzeugendensystemen des von den Divisoren erzeugten Ideals, sogenannte *Gröbner Basen*, beschränkt: Eine Gröbner Basis erzeugt nicht nur das Ideal, sondern ihre Leitterme erzeugen auch das Ideal aller Leitterme. Mit einer Gröbner Basis als Divisorenmenge ist der Rest eindeutig bestimmt und entscheidet – genauso wie im Falle einer einzigen Veränderlichen - über die Mitgliedschaft des Dividenden in dem gegebenen Ideal.

Alle in diesem Abschnitt auftretenden Polynomringe seien mit einer Monomordnung versehen.

4.11 Definition (Gröbner Basis)

Eine endliche Menge

$$G = \{ g_1,...,g_s \}$$

von Null verschiedener Elemente eines Ideals

$$I \subset k[T_1,...,T_n]$$

heißt *Gröbner Basis* von I, wenn gilt:

$$lt(I) = \langle lt(g) : g \in G \rangle,$$

d.h. wenn das monomiale Ideal der Leitterme aller nicht-verschwindenden Elemente aus I erzeugt wird von den Leittermen der Elemente aus G.

Aus dem Divisionsalgorithmus 4.8 folgt, daß jede Gröbner Basis eines Ideals auch das Ideal erzeugt:

4.12 Lemma (Gröbner Basis)

Jede Gröbner Basis eines Ideals ist auch Erzeugendensystem des Ideals, d.h. für jede endliche Teilmenge

$$G = \{ g_1,...,g_s \}$$

von Elementen eines Ideals

$$I \subset k[T_1,...,T_n]$$

gilt:

$$lt(I) = \langle lt(g) : g \in G \rangle \text{ impliziert } I = \langle g : g \in G \rangle.$$

Beweis. Für ein vorgegebenes Element $f \in I$ terminiert der Divisionsalgorithmus 4.8 zur Berechnung von

$$f : G$$

mit einem Rest

$$r = f - \sum_{i=1}^{s} a_i \cdot g_i \in I.$$

Im Falle $r \neq 0$ wäre kein Term von r durch einen Leitterm $lt(g_i)$ teilbar. Nach Definition der Gröbner Basis gilt

$$lt(r) \in \langle\, lt(g_1),...,lt(g_s)\,\rangle .$$

Dieses Ideal ist monomial, so daß bereits einer seiner Erzeuger $lt(g_i)$ den Leitterm $lt(r)$ teilt, ein Widerspruch, q.e.d.

Die Division eines Polynoms durch eine endliche Familie von Dividenden gemäß Algorithmus 4.8 ist ein Beispiel einer Reduktionsrelation, wie sie auch in anderen Teilen der Mathematik auftritt. Beispielsweise bei der Reduktion von Worten einer Gruppe im Rahmen des Wort-Problems oder bei der Reduktion von Formeln einer formalen Sprache anhand einer Grammatik.

4.13 Definition (Reduktion)

Eine endliche Menge

$$G \subset k[T_1,...,T_n]$$

nicht-verschwindender Polynome definiert auf der Menge $k[T_1,...,T_n]$ aller Polynome die folgende Relation der *Reduktion modulo G*:

i) Das Polynom f läßt sich vermöge eines Elementes $g \in G$ zum Polynom r reduzieren, geschrieben

$$f \xrightarrow[g]{} r ,$$

wenn ein Term t von f durch den Leitterm $lt(g)$ von g teilbar ist und

$$r = f - \frac{t}{lt(g)}\, g .$$

ii) Das Polynom f läßt sich modulo G zum Polynom r reduzieren, geschrieben

$$f \xrightarrow[G]{} r ,$$

wenn ein $g \in G$ existiert mit

$$f \xrightarrow[g]{} r .$$

iii) Der transitive Abschluß der Relation $\xrightarrow[G]{}$ wird mit $\xrightarrow[G]{*}$ bezeichnet, die erzeugte Äquivalenzrelation mit $\xleftrightarrow[G]{*}$.

iv) Ein Polynom, das nicht modulo G reduzierbar ist, heißt in *Normalform* bzgl. der Reduktion modulo G.

Algorithmus 4.8 führt eine spezielle Art der Reduktion (Top-Reduktion) durch. Er prüft, ob eine Elimination des Leittermes des Dividenden möglich ist.

Die Reduktion modulo G ist eine strikt antisymmetrische, Noethersche Relation, d.h.

- Wenn $f \xrightarrow[G]{*} r$, dann nicht $r \xrightarrow[G]{*} f$ (Strikt antisymmetrisch)

- Jede Folge von Reduktionen eines gegebenen Elementes endet nach endlich vielen Schritten mit einer Normalform (Noethersch)

Beide Aussagen folgen aus der Tatsache, daß eine Reduktion

$$f \xrightarrow[G]{} r$$

die Größe verringert $r < f$.

Die Reduktion einer Differenz läßt sich als Differenz geeigneter Reduktionen beider Summanden darstellen.

4.14 Lemma (Translationslemma)

Es sei G eine endliche Menge nicht-verschwindender Polynome aus $k[T_1,...,T_n]$. Für zwei Polynome $f_1,\ f_2 \in k[T_1,...,T_n]$ gebe es eine Reduktion ihrer Differenz:

$$f_1 - f_2 \xrightarrow[G]{*} r \text{ für ein Polynom } r \in k[T_1,...,T_n].$$

Dann gibt es zwei Polynome

$$r_i \in k[T_1,...,T_n], i = 1, 2 \text{, mit } r_1 - r_2 = r$$

und zugehörige Reduktionen

$$f_i \xrightarrow[G]{*} r_i,\ i = 1, 2 .$$

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl k der Reduktionsschritte der Reduktion

$$f_1 - f_2 \xrightarrow[G]{*} r .$$

Im Falle $k = 0$ gilt $r = f_1 - f_2$ und wir können $r_i := f_i, i = 1, 2$ setzen. Im Induktionsschritt zerlegen wir eine gegebene Reduktion

$$f_1 - f_2 \xrightarrow[G]{*} r$$

mit $k + 1$ Schritten in eine Reduktion mit k Schritten

$$f_1 - f_2 \xrightarrow[G]{*} r'$$

und in eine Reduktion mit einem Schritt

$$r' \xrightarrow[g]{} r .$$

Bei dieser Reduktion werde der Term t von r' eliminiert. Sein Monom heiße m :

$$r = r' - \frac{t}{LT(g)} \cdot g = r' - \frac{c}{b} \cdot u \cdot g$$

mit

$$\text{Term } t = c \cdot m \text{, Koeffizient } c = LC(t) \text{, Monom } u := \frac{m}{LM(g)} \text{ und Koeffizient } b := LC(g).$$

Nach Induktionsvoraussetzung über die Reduktion

$$f_1 - f_2 \xrightarrow[G]{*} r'$$

gibt es zwei Polynome r_i', $i = 1, 2$, mit

$$r' = r_1' - r_2'$$

und zugehörigen Reduktionen

$$f_i \xrightarrow[G]{*} r_i' .$$

Mit den Definitionen

$$r_i := r_i' - \frac{c_i}{b} \cdot u \cdot g$$

$$c_1 := \begin{cases} Koeffizient\ des\ Monoms\ m\ bzgl.\ r_2' & falls\ Koeffizient \neq 0 \\ 0 & sonst \end{cases}$$

und analog c_2. Unabhängig von der Fallunterscheidung gilt

$$c_1 - c_2 = c \text{ und } r_1 - r_2 = r .$$

Außerdem gilt

$$r_i' \xrightarrow[G]{\circ} r_i \text{ für } i = 1, 2 ,$$

da entweder

$$r_i' = r_i \text{ oder } r_i' \xrightarrow[g]{} r_i , \text{ q.e.d.}$$

Wenn zwei Polynome kongruent sind bezüglich eines Ideals, so lassen sie sich durch eine endliche, aber möglicherweise ungerichtete Folge von Reduktionen modulo eines beliebigen Erzeugendensystems verbinden.

4.15 Lemma *(Reduktion und Kongruenz)*

Es sei G ein endliches Erzeugendensystem eines Ideals $I \subset k[X_1,..., X_n]$. Dann gilt

$$f_1 \xleftrightarrow[G]{*} f_2 \text{ genau dann, wenn } f_1 - f_2 \in I .$$

Beweis. i) Für jeden Reduktionsschritt modulo G, bei dem ein Term t eines Polynoms $f \in k[X_1,..., X_n]$ eliminiert wird

$$f \xrightarrow[g]{} r := f - \frac{t}{LT(g)} \cdot g ,$$

gilt für die Differenz

$$f - r = \frac{t}{LT(g)} \cdot g \in I .$$

ii) Die Differenz $f_1 - f_2 \in I$ hat eine Darstellung

$$f_1 - f_2 = \sum_{i=1}^{k} a_i \cdot g_i \text{ mit Elementen } a_i \in k[X_1,..., X_n] \text{ und } g_i \in G,\ i = 1,..., k .$$

Wir beweisen die Behauptung $f_1 \xleftarrow[G]{*} f_2$ durch Induktion über k. Im Induktionsanfang $k = 0$ gilt $f_1 = f_2$. Im Induktionsschritt sei

$$f_1 - f_2 = \sum_{i=1}^{k+1} a_i \cdot g_i = \sum_{i=1}^{k} a_i \cdot g_i + a_{k+1} \cdot g_{k+1}.$$

Wir wenden die Induktionsvoraussetzung an auf die beiden Polynome

$$f_1 \text{ und } f_2 + a_{k+1} \cdot g_{k+1}$$

und erhalten

$$f_1 \xleftarrow[G]{*} f_2 + a_{k+1} \cdot g_{k+1}.$$

Es bleibt zu zeigen

$$f_2 + a_{k+1} \cdot g_{k+1} \xleftarrow[G]{*} f_2.$$

Hierfür zeigen wir im ersten Schritt: Für jedes feste Element $g \in G$ und für alle Polynome $a \in k[X_1,..., X_n]$ gilt

$$a \cdot g \xrightarrow[G]{*} 0$$

Beweis hierfür durch Widerspruch. Annahme: Es gibt ein Polynom a, für das die Aussage falsch ist. Dann sei a mit dieser Eigenschaft minimal gewählt bzgl. der Teilordnung auf $k[X_1,..., X_n]$. Für die Leitterme gilt

$$LT(a \cdot g) = LT(a) \cdot LT(g)$$

Also ist eine Top-Reduktion möglich

$$a \cdot g \xrightarrow[G]{} a \cdot g - \frac{LT(a \cdot g)}{LT(g)} \cdot g = (\, a - LT(a)\,) \cdot g$$

Da

$$a - LT(a) < a$$

läßt sich dieses Polynom wegen der Minimalität von a weiter reduzieren

$$(a - LT(a)) \cdot g \xrightarrow[G]{*} 0\,.$$

Mit der vorgeschalteten Top-Reduktion erhält man

$$a \cdot g \xrightarrow[G]{*} 0\,,$$

einen Widerspruch.

Im zweiten Schritt wenden wir das Translationslemma an auf die Differenz

$$(f_2 + a_{k+1} \cdot g_{k+1}) - f_2 = a_{k+1} \cdot g_{k+1}.$$

Wie gerade bewiesen gilt

$$a_{k+1} \cdot g_{k+1} \xrightarrow[G]{*} 0\,.$$

Daher gibt es nach Lemma 4.14 zwei Reduktionen

$$f_2 + a_{k+1} \cdot g_{k+1} \xrightarrow[G]{*} r$$

und

$$f_2 \xrightarrow[G]{*} r'$$

mit

$$r - r' = 0 \text{, d.h. } r = r' .$$

Insbesondere gilt also

$$f_2 + a_{k+1} \cdot g_{k+1} \xleftrightarrow[G]{*} f_2 \text{, q.e.d.}$$

Lemma 4.15 läßt sich für den Fall einer Gröbner Basis wesentlich verschärfen zur Church-Rosser Eigenschaft der Reduktion. Zugleich zeigt der folgende Satz, daß der Divisionsalgorithmus 4.8 bei der Division durch eine Gröbner Basis eines Ideals einen eindeutig bestimmten Rest liefert. Genau dann, wenn dieser Rest verschwindet, ist der Dividend Element des Ideals.

4.16 Satz *(Reduktion modulo einer Gröbner Basis)*

Für eine endliche Menge G nicht-verschwindender Polynome aus $k[T_1,...,T_n]$ sind folgende Eigenschaften äquivalent:

i) Die Menge G ist eine *Gröbner Basis*.

ii) Es gilt

$$f \xrightarrow[G]{*} 0$$

für jedes Polynom $f \in \langle G \rangle$ aus dem von G erzeugten Ideal.

iii) Die Reduktion ist *lokal-konfluent*: Wenn sich ein Polynom durch zwei verschiedene Divisionen reduzieren läßt, so gibt es eine gemeinsame Reduktion der Reste:

$$f \xrightarrow[G]{} r_i, i = 1, 2 \text{, impliziert } r_i \xrightarrow[G]{*} r, i = 1, 2 \text{ für ein geeignetes Polynom } r$$

iv) Die Reduktion ist *konfluent*: Wenn sich ein Polynom auf zwei Arten reduzieren läßt, so gibt es eine gemeinsame Reduktion beider Reste

$$f \xrightarrow[G]{*} r_i, i = 1, 2 \text{, impliziert } r_i \xrightarrow[G]{*} r, i = 1, 2 \text{ für ein geeignetes Polynom } r$$

v) Die Reduktion liefert *eindeutige* Normalformen:

$$f \xrightarrow[G]{*} r_i, i = 1, 2 \text{ mit Normalformen } r_i \text{ impliziert } r_1 = r_2$$

vi) Die Reduktion hat die *Church-Rosser* Eigenschaft:

$$f_1 \xleftrightarrow[G]{*} f_2 \text{ impliziert } f_i \xrightarrow[G]{*} r, i = 1, 2 \text{, für ein geeignetes Polynom } r$$

Beweis. i) => vi) Es seien zwei Polynome gegeben mit

$$f_1 \xleftrightarrow[G]{*} f_2 .$$

Nach Lemma 4.15 gilt

$$f_1 - f_2 \in \langle G \rangle .$$

Wir reduzieren jedes Polynom f_i zu einer Normalform r_i

$$f_i \xrightarrow[G]{*} r_i, i = 1, 2 .$$

Auch für die Normalformen gilt

$$r_1 - r_2 \in \langle G \rangle .$$

Annahme: $r_1 \neq r_2$. Da G eine Gröbner Basis ist, gilt

$$LT(r_1 - r_2) \in LT\langle G \rangle .$$

Also gibt es mindestens einen Term t von r_1 oder von r_2 mit

$$t \in LT\langle G \rangle ,$$

o.E. sei t ein Term von r_1 . Dann gibt es eine Reduktion

$$r_1 \xrightarrow[G]{} r_1'$$

im Widerspruch dazu, daß r_1 eine Normalform ist.

vi) => ii) Für jedes Polynom $f \in \langle G \rangle$ gilt $f \equiv 0 \bmod \langle G \rangle$, also

$$f \xleftrightarrow[G]{*} 0$$

nach Lemma 4.15. Mit der Church-Rosser Eigenschaft folgt hieraus

$$f \xrightarrow[G]{*} 0 .$$

ii) => i) Nach Voraussetzung ist für jedes Polynom

$$0 \neq f \in \langle G \rangle$$

mindestens eine Reduktion möglich. Annahme: Es gibt ein $0 \neq f \in \langle G \rangle$, für das keine Top-Reduktion möglich ist. Sei f mit dieser Eigenschaft minimal gewählt bzgl. der Teilordnung auf $k[X_1,...,X_n]$. Dann gibt es eine Reduktion

$$f \xrightarrow[G]{} r .$$

Da die Reduktion keine Top-Reduktion ist, gilt

$$LT(f) = LT(r).$$

Wegen

$$r < f \text{ und } 0 \neq r \in \langle G \rangle$$

ist für r eine Top-Reduktion möglich, d.h.

$$LT(f) = LT(r) \in LT\langle G \rangle ,$$

im Widerspruch zur Annahme.

Die Äquivalenz der Eigenschaften iii) bis vi) gilt bei jeder Noetherschen Reduktionsrelation, siehe Newman's Lemma in [BW1993], Theor. 4.73, q.e.d.

Die folgende Abbildung 3 veranschaulicht die charakteristische Eigenschaft der Division durch eine Gröbner Basis: In welcher Reihenfolge man auch die einzelnen Divisionen ausführt, stets erhält man im Falle einer Gröbner Basis denselben Rest

$$r = r_1 = r_2 .$$

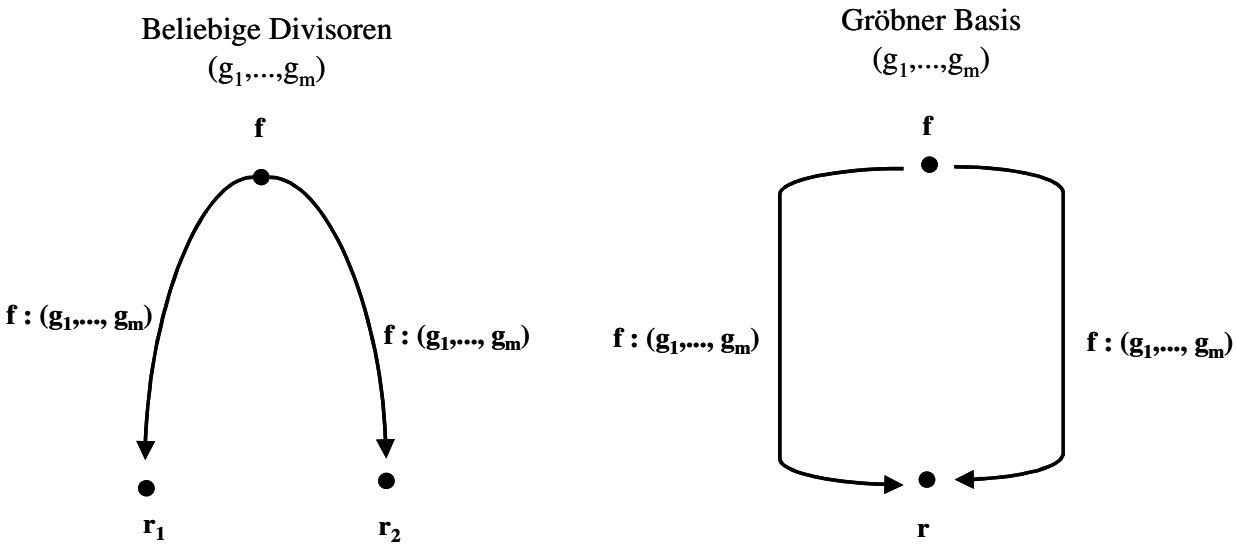


Abbildung 3: Unabhängigkeit des Restes bei Division durch Elemente einer Gröbner Basis

Beispiel 4.9 zeigt, wie bei dem Divisionsalgorithmus die Eindeutigkeit des Restes verloren gehen kann, wenn sich die Leitterme zweier Divisoren herausheben. Die resultierende Differenz heißt S-Polynom.

4.17 Definition (S-Polynom)

Das *S-Polynom* zweier von Null verschiedener Polynome

$$0 \neq g_1, g_2 \in k[X_1,..., X_n]$$

ist das Polynom

$$S(g_1, g_2) := LC(g_2) \cdot \frac{m}{LM(g_1)} g_1 - LC(g_1) \cdot \frac{m}{LM(g_2)} g_2 \in k[X_1,..., X_n]$$

wobei

$$m := lcm(LM(g_1), LM(g_2)) \in k[X_1,..., X_n]$$

das kleinste gemeinsame Vielfache der beiden Leitmonome $LM(g_1)$ und $LM(g_2)$ ist.

S-Polynome dienen als Test, ob ein Erzeugendensystem eine Gröbner Basis ist. Zur Vorbereitung des Buchberger Kriteriums in Satz 4.19 beweisen wir einen Hilfssatz.

4.18 Hilfssatz *(Gröbner Basis)*

Eine endliche Menge G von Null verschiedener Polynome aus $k[X_1,...,X_n]$ ist eine Gröbner Basis, wenn sie folgende Eigenschaft hat: Für jedes Paar

$$g_1 \neq g_2 \in G$$

und jedes Paar von Termen

$$t_1, t_2 \in k[X_1,...,X_n]$$

gilt:

$$LT(t_1 \cdot g_1) = LT(t_2 \cdot g_2) \text{ impliziert } t_1 \cdot g_1 - t_2 \cdot g_2 \xrightarrow[G]{*} 0.$$

Beweis. Nach Satz 4.16 genügt es zu zeigen, daß die Reduktion modulo G lokal-konfluent ist. Es sei $f \in k[X_1,...,X_n]$ ein vorgegebenes Polynom mit zwei Reduktionen

$$f \xrightarrow[g_i]{} f - t_i \cdot g_i \text{ und Termen } t_i, i = 1, 2.$$

Wenn beide Reduktionen denselben Term von f eliminieren, so gilt

$$LT(t_1 \cdot g_1) = LT(t_2 \cdot g_2)$$

und nach Voraussetzung

$$t_1 \cdot g_1 - t_2 \cdot g_2 \xrightarrow[G]{*} 0.$$

Wenn beide Reduktionen dagegen unterschiedliche Terme von f eliminieren, so gilt o.E.

$$LT(t_1 \cdot g_1) > LT(t_2 \cdot g_2).$$

Mit zwei Reduktionen modulo g_1 bzw. g_2 erhält man ebenfalls

$$t_1 \cdot g_1 - t_2 \cdot g_2 \xrightarrow[G]{} -t_2 \cdot g_2 \xrightarrow[G]{} 0.$$

In beiden Fällen gilt für die Polynome

$$f_i := f - t_i \cdot g_i, i = 1, 2$$

die Reduktion

$$f_1 - f_2 \xrightarrow[G]{*} 0.$$

Nach dem Translationslemma 4.14 folgt die Existenz zweier Reduktionen

$$f_i \xrightarrow[G]{*} r_i, i = 1, 2$$

mit einem eindeutig bestimmten Polynom

$$r_1 = r_2 \in k[X_1,...,X_n], \text{ q.e.d.}$$

4.19 Satz *(Buchberger Kriterium)*

Es sei G eine endliche Menge von Null verschiedener Polynomen aus $k[X_1,...,X_n]$ und

$$I := \langle\, g : g \in G \,\rangle \subset k[X_1,...,X_n]$$

das von ihnen erzeugte Ideal. Dann sind äquivalent:

- G ist eine Gröbner Basis von I
- Für alle Paare $g_1 \neq g_2 \in G$ gilt $S(g_1, g_2) \xrightarrow[G]{*} 0$.

Beweis. i) Aus der Eigenschaft, Gröbner Basis zu sein, folgt die behauptete Aussage über die S−Polynome nach Satz 4.16.

ii) Zum Beweis der Umkehrung wenden wir Lemma 4.18 an: Wir gehen aus von zwei Elementen $g_1 \neq g_2 \in G$ und zwei Termen $t_1, t_2 \in k[X_1,..., X_n]$ mit

$$LT(t_1 \cdot g_1) = LT(t_2 \cdot g_2).$$

Wir wollen die Differenz

$$t_1 \cdot g_1 - t_2 \cdot g_2$$

in eine Aussage über das S-Polynom $S(g_1, g_2)$ umformulieren. Dazu betrachten wir für $i = 1, 2$ die Leitmonome und Leitkoeffzienten

$$m_i := LM(g_i),\ a_i := LC(g_i) \text{ sowie } u_i := LM(t_i),\ b_i := LC(t_i).$$

Nach Voraussetzung gilt

$$a_1 \cdot b_1 \cdot m_1 \cdot u_1 = a_2 \cdot b_2 \cdot m_2 \cdot u_2.$$

Insbesondere stimmen auf beiden Seiten die Koeffizienten überein:

$$a_1 \cdot b_1 = a_2 \cdot b_2, \text{ also } \frac{b_1}{a_2} = \frac{b_2}{a_1} \in k.$$

Und ebenso stimmen auf beiden Seiten die Monome überein:

$$m_1 \cdot u_1 = m_2 \cdot u_2.$$

Dieses Monom ist ein gemeinsames Vielfaches von m_1 und von m_2. Also gibt es ein Monom v mit

$$m_1 \cdot u_1 = m_2 \cdot u_2 = v \cdot lcm(m_1, m_2).$$

Es gibt Monome $s_1, s_2 \in k[X_1,..., X_n]$, so daß

$$lcm(m_1, m_2) = s_1 \cdot m_1 = s_2 \cdot m_2.$$

Es folgt für $i = 1, 2$ die Gleichheit der Monome

$$m_i \cdot u_i = v \cdot s_i \cdot m_i, \text{ also } u_i = v \cdot s_i.$$

Für die Differenz folgt

$$t_1 \cdot g_1 - t_2 \cdot g_2 =$$

$$= b_1 \cdot u_1 \cdot g_1 - b_2 \cdot u_2 \cdot g_2 = b_1 \cdot v \cdot s_1 \cdot g_1 - b_2 \cdot v \cdot s_2 \cdot g_2 =$$

$$= \frac{b_1}{a_2} \cdot v \cdot (a_2 \cdot s_1 \cdot g_1 - a_1 \cdot s_2 \cdot g_2) = \frac{b_1}{a_2} \cdot v \cdot S(g_1, g_2).$$

Nach Voraussetzung gilt

$$S(g_1, g_2) \xrightarrow[G]{*} 0 .$$

Hieruas folgt mit dem Term

$$h := \frac{b_1}{a_2} \cdot v$$

für das Produkt

$$h \cdot S(g_1, g_2) \xrightarrow[G]{*} 0 .$$

Denn allgemein gilt für die Reduktion eines Polynoms $f \in k[X_1,..., X_n]$:

$$f \xrightarrow[G]{} r \text{ impliziert } s \cdot f \xrightarrow[G]{} s \cdot r \text{ für einen beliebigen Term } s .$$

Beweis hierfür: Ist t ein Term von f, der durch den Leitterm $LT(g)$ eines Elementes $g \in G$ teilbar ist, so gilt

$$f \xrightarrow[G]{} r = f - \frac{t}{LT(g)} g .$$

Dann ist $s \cdot t$ ein Term von $s \cdot f$, und dieser Term ist ebenfalls durch $LT(g)$ teilbar. Also

$$s \cdot f \xrightarrow[G]{} s \cdot f - \frac{s \cdot t}{LT(g)} g = s \cdot \left(f - \frac{t}{LT(g)} g \right) = s \cdot r .$$

Damit sind alle Voraussetzungen von Hilfssatz 4.18 erfüllt. Es folgt, daß die Menge G eine Gröbner Basis ist, q.e.d.

Gröbner Basen wurden mehrfach in der Mathematik unter verschiedenem Namen entdeckt. Ihre heutige Bedeutung geht zurück auf Buchberger (1964). Er entdeckte das Buchberger Kriterium und entwickelte darauf aufbauend einen Algorithmus, der jedes endliche Erzeugendensystem eines Ideals $I \subset k[X_1,..., X_n]$ zu einer Gröbner Basis erweitert. Der Buchberger Algorithmus prüft sukzessive zu je zwei Elementen g_1 und g_2 eines Erzeugendensystems von I den Rest ihres S-Polynoms bei Division bzgl. des Erzeugendenystems und nimmt ihn ggf. als weiteren Erzeuger hinzu. Der Algorithmus terminiert, denn die monomialen Ideale, die in jedem Schritt von den Leitmonomen des aktuellen Erzeugendensystems erzeugt werden, bilden eine aufsteigende Folge. Diese wird stationär im Noetherschen Ring $k[X_1,..., X_n]$.

4.20 Algorithmus (Buchberger)

Vorgegeben ein Polynomring mit Monomordnung.

Input: Endliche Menge $\{ g_1,...,g_s \}$ von Elementen $0 \neq g_i \in k[T_1,..., T_n]$

Output: Gröbner Basis $G = \{ g_1,..., g_s, g_{s+1},...,g_m \}$ des Ideals $\langle g_1,...,g_s \rangle \subset k[T_1,..., T_n]$

$G = \{ g_1,...,g_s \}$		
	$G' = G$	
	for every pair $g_1 \neq g_2 \in G'$	
		determine a rest r of division $S(g_1, g_2) : G'$
		if $r \neq 0$ then $G = G \cup \{ r \}$
until $G' = G$		

Tabelle 3: Buchberger Algorithmus

Beweis. [CLO1997], Chap.2 , §7.

4.21 Toolbeispiel (Gröbner Basis)

i) Algorithmus 4.20 berechnet für das Ideal

$$I := \langle g_1 = X \cdot Y + 1,\ g_2 = Y^2 - 1 \rangle \subset k[X, Y]$$

aus Beispiel 4.9 bzgl. der Lex-Ordnung die Gröbner Basis

$$G = \{ g_1,\ g_2,\ X + Y \}.$$

In Beispiel 4.9 führte das Polynom, das aus der Subtraktion der führenden Terme

$$-Y - X = -Y \cdot g_1 + X \cdot g_2 \in \langle g_1,\ g_2 \rangle$$

entsteht, zu einem vorzeitigen Terminieren. Es wird jetzt für die Gröbner Basis als weiteres Erzeugendes hinzugenommen.

ii) Allerdings sind weder Gröbner Basen noch ihre Kardinalitäten eindeutig bestimmt. Computer Tools rechnen i.a. mit einer „reduzierten“ Gröbner Basis G :

- Alle Elemente $g \in G$ haben den Leitkoeffizienten $LC(g) = 1$
- Jedes $g \in G$ ist in Normalform bzgl. Reduktion modulo $G - \{ g \}$.

Eine reduzierte Gröbner Basis ist bei gegebener Monomordnung eindeutig bestimmt.

Die reduzierte Gröbner Basis von I lautet

$$G' = \{ g_2,\ X + Y \}.$$

iii) Computer Tools zur Kommutativen Algebra verfügen über einen Befehl zur Berechnung der Gröbner Basis eines Ideals. Das Ergebnis hängt stark von der gewählten Monomordnung des Polynomrings ab.

Macaulay2 Script:

- „MyExamples/GroebnerBase/Examples“

Das Rechnen mit Idealen

In Computertools der kommutativen Algebra beruht die Kalkulation mit Idealen in Polynomringen auf folgenden Schritten:

- Zurückführung von Operationen mit Idealen auf die Frage der Zugehörigkeit zu einem geeigneten Ideal.
- Berechnung einer Gröbner Basis G für das erhaltene Ideal nach dem Buchberger Algorithmus 4.20.
- Entscheidung der Zugehörigkeit eines Elementes zu dem erhaltenen Ideal durch eine Reduktion modulo G mit Hilfe des Divisionsalgorithmus 4.8.

In diesem Abschnitt bezeichne K den algebraischen Abschluß des Körpers k.

Die Zugehörigkeit zu einem Radikal läßt sich nach dem sogenannten „Trick von Rabinovitsch“ auf die Zugehörigkeit der Eins zu einem geeigneten erweiterten Ideal zurückführen.

4.22 Lemma (Zugehörigkeit zu einem Radikal)

Sei $I \subset k[T_1,...,T_n]$ ein Ideal. Dann gilt für ein Polynom $f \in k[T_1,...,T_n]$:

$$f \in \sqrt{I} \;\Leftrightarrow\; 1 \in I^e + \langle\, 1 - T \cdot f \,\rangle \subset k[T_1,...,T_n,T].$$

Dabei bedeutet

$$I^e := k[T_1,...,T_n,T] \cdot I \subset k[T_1,...,T_n,T]$$

das erweiterte Ideal.

Beweis. Bekanntlich gilt in einer Veränderlichen Y

$$Y^m - 1 = \left(Y^{m-1} + Y^{m-2} + ... + Y + 1 \right) \cdot \left(Y - 1 \right)$$

also

$$1 = Y^m + \left(Y^{m-1} + Y^{m-2} + ... + Y + 1 \right) \cdot \left(1 - Y \right).$$

i) Sei $f \in \sqrt{I}$, also $f^m \in I$. Mit

$$Y := T \cdot f$$

folgt

$$1 \in I^e + \langle\, 1 - T \cdot f \,\rangle \subset k[T_1,...,T_n,T].$$

ii) Ohne Einschränkung sei $f \neq 0$. Dann existiert das Inverse

$$\frac{1}{f} \in k(T_1,...,T_n)\ .$$

Sei

$$I = \langle g_1,..., g_k \rangle \subset k[T_1,...,T_n].$$

Nach Voraussetzung existiert eine Darstellung

$$1 = \sum_{i=1}^{k} a_i(T) \cdot g_i + a_0(T) \cdot (1 - T \cdot f) \in k[T_1,...,T_n,T]$$

mit Elementen

$$a_i(T) \in k[T_1,...,T_n][T], i = 0, 1,..., k .$$

Unter der kanonischen Abbildung

$$k[T_1,...,T_n][T] \longrightarrow k(T_1,...,T_n), T \mapsto \frac{1}{f}$$

geht obige Darstellung über in die Gleichung

$$1 = \sum_{i=1}^{k} a_i\left(\frac{1}{f}\right) \cdot g_i + a_0\left(\frac{1}{f}\right) \cdot \left(1 - \frac{1}{f} \cdot f\right) \in k(T_1,...,T_n),$$

d.h.

$$1 = \sum_{i=1}^{k} a_i\left(\frac{1}{f}\right) \cdot g_i \in k(T_1,...,T_n).$$

Nach Multiplikation mit einer genügend hohen Potenz f^m lassen sich alle Nenner eliminieren, so daß die Gleichung im Quotientenkörper

$$f^m = \sum_{i=1}^{k} \left(f^m \cdot a_i\left(\frac{1}{f}\right)\right) \cdot g_i \in k(T_1,...,T_n)$$

sogar schon eine Gleichung im Polynomring $k[T_1,...,T_n]$ ist, q.e.d.

4.23 Definition *(Eliminationsideal)*

Es sei $I \subset k[T_1,...,T_n]$ ein Ideal. Für eine Zahl $1 \le r < n$ heißt das Ideal

$$I_r := I \cap k[T_{r+1},...,T_n] \subset k[T_{r+1},...,T_n]$$

das *r-te Eliminationsideal* von I .

Das r-te Eliminationsideal enthält alle Elemente des Ideals, die nicht von den ersten r Variablen abhängen. Aus Sicht der Geometrie entspricht der Elimination von Variablen die Projektion längs dieser Variablen.

4.24 Lemma *(Projektion und Elimination)*

Es sei

$$X = Var(I) \subset \boldsymbol{A}^n(K)$$

die affine Varietät eines Ideals $I \subset k[T_1,...,T_n]$. Mit $1 \le r < n$ gilt für die Projektion

$$pr : \boldsymbol{A}^n(K) \longrightarrow \boldsymbol{A}^{n-r}(K), (x_1,..., x_n) \mapsto (x_{r+1},..., x_n)$$

längs der ersten r Koordinaten die Gleichung

$$\overline{pr(X)} = Var(I_r) \subset \boldsymbol{A}^{n-r}(K).$$

Beweis. Die Einschränkung der Projektion ist eine reguläre Abbildung

$$g : X \longrightarrow \boldsymbol{A}^{n-r}(K).$$

Für sie gilt nach Satz 2.16

$$\overline{g(X)} = Var(\ker \varphi_g) \subset \boldsymbol{A}_K^{n-r}$$

mit der induzierten Abbildung der Koordinatenringe

$$\varphi_g : k[T_{r+1},...,T_n] \longrightarrow k[X] = k[T_1,...,T_n]/I$$

die von der Inklusion

$$k[T_{r+1},...,T_n] \xrightarrow{\subset} k[T_1,...,T_n]$$

stammt. Offensichtlich gilt

$$\ker \varphi_g = k[T_{r+1},...,T_n] \cap I = I_r, \text{ q.e.d.}$$

Auch der Kern beliebiger Morphismen in affine Algebren ist ein Eliminationsideal.

4.25 Satz (Kern von Algebra-Morphismen)

Gegeben sei eine affine k-Algebra

$$A = k[X_1,..., X_n]/I$$

und ein Morphismus

$$\varphi : k[Y_1,...,Y_m] \longrightarrow A.$$

Dann gilt

$$\ker \varphi = J_n \subset k[Y_1,...,Y_m]$$

mit dem n-ten Eliminationsideal J_n eines Ideals

$$J \subset k[X_1,..., X_n, Y_1,...,Y_m],$$

das wie folgt entsteht: Nach Wahl eines Morphismus

$$\Phi : k[Y_1,...,Y_m] \longrightarrow k[X_1,..., X_n],\ Y_j \mapsto \Phi_j,\ j = 1,...,m,$$

mit

$$\pi(\Phi_j) = \varphi(Y_i),\ j = 1,...,m,$$

bezüglich der kanonischen Restklassenabbildung

$$\pi : k[X_1,..., X_n] \longrightarrow A$$

sei definiert

$$J := I^e + \langle\, Y_j - \Phi_j : j = 1,...,m \,\rangle \subset k[X_1,..., X_n, Y_1,...,Y_m].$$

Beweis. Der Morphismus

$$\varphi : k[Y_1,...,Y_m] \longrightarrow A$$

ist die folgende Komposition von Morphismen

$$k[Y_1,...,Y_m] \xrightarrow{\subset} k[X_1,...,X_n,Y_1,...,Y_m] \xrightarrow{\Phi^e} k[X_1,...,X_n] \xrightarrow{\pi} A = k[X_1,...,X_n]/I$$

mit

$$\Phi^e(X_i) := X_i,\ i = 1,...,n \text{, und } \Phi^e(Y_j) := \Phi(Y_j) = \Phi_j \in k[X_1,...,X_n],\ j = 1,...,m.$$

Wir setzen

$$I_\Gamma := \langle\ Y_j - \Phi_j : j = 1,...,m\ \rangle \subset k[X_1,...,X_n,Y_1,...,Y_m].$$

Der Morphismus Φ^e bedeutet die Beibehaltung der Variablen X_i und die Ersetzung der Variablen Y_j durch das Polynom

$$\Phi_j \in k[X_1,...,X_n].$$

Bei dieser Ersetzung gehen Elemente des Ideals I_Γ in Null über. Daher gilt

$$\Phi^e(I_\Gamma) = 0.$$

Wir zeigen umgekehrt

$$\ker \Phi^e \subset I_\Gamma:$$

Im Ring $k[X_1,...,X_n,Y_1,...,Y_m]$ gilt

$$Y_j = \Phi_j + (\ Y_j - \Phi_j\ ),\ j = 1,...,m.$$

Daher läßt sich jedes Polynom

$$f \in k[X_1,...,X_n,Y_1,...,Y_m]$$

zerlegen in der Form

$$f = f(X_1,...,X_n,Y_1,...,Y_m) = f(X_1,...,X_n,\Phi_1,...,\Phi_m) + F$$

mit einem Polynom

$$F = F(X_1,...,X_n,Y_1,...,Y_m) \in I_\Gamma.$$

Im Falle

$$f \in \ker \Phi^e$$

folgt aus

$$0 = \Phi^e(f) = f(X_1,...,X_n,\Phi_1,...,\Phi_m) + \Phi^e(F)$$

wegen

$$F \in I_\Gamma \subset \ker \Phi^e, \text{ d.h. } \Phi^e(F) = 0,$$

die Gleichung

$$f(X_1,...,X_n,\Phi_1,...,\Phi_m) = 0$$

und damit die Gleichheit

$$f = F \in I_\Gamma .$$

Mit

$$\ker \Phi^e = I_\Gamma$$

folgt für die Kompositionen

$$\ker \left[\pi \circ \Phi^e\right] = I^e + I_\Gamma$$

und schließlich

$$\ker \varphi = \left(I^e + I_\Gamma\right) \cap k[Y_1,...,Y_m], \text{ q.e.d.}$$

Hinweis. Dem im Beweis betrachteten Ideal I_Γ entspricht geometrisch der Graph

$$\Gamma \subset \boldsymbol{A}^{n+m}(K)$$

der zu Φ gehörigen regulären Abbildung

$$\boldsymbol{A}^n(K) \longrightarrow \boldsymbol{A}^m(K),$$

dem Morphismus Φ^e entspricht die Einbettung

$$\boldsymbol{A}^n(K) \xrightarrow{\cong} \Gamma \subset \boldsymbol{A}^{n+m}(K)$$

auf den Graphen.

Aus der Gröbner Basis eines Ideals ergeben sich sofort Gröbner Basen seiner Eliminationsideale. Damit lassen sich Eliminationsideale algorithmisch berechnen. Als Monomordnung kann die Lex-Ordnung oder - besser - eine zu den eliminierten Variablen passende Eliminationsordnung verwendet werden:

4.26 Satz (Gröbner Basis des Eliminationsideals)

Es sei $I \subset k[T_1,...,T_n]$ ein Ideal und $1 \le r < n$. Es sei G eine Gröbner Basis von I bzgl. der Lex-Ordnung oder der r-ten Eliminationsordnung. Dann ist die Menge

$$G_r := G \cap k[T_{r+1},...,T_n]$$

eine Gröbner Basis des r-ten Eliminationsideals I_r von I.

Beweis. Nach Definition gehören alle Elemente der Menge G_r zu I_r. Zu zeigen ist also:

$$lt(I_r) = \left\langle\, lt(g) : g \in G_r \,\right\rangle .$$

i) Wegen $G_r \subset I_r$ gilt

$$lt(I_r) \supset \left\langle\, lt(g) : g \in G_r \,\right\rangle .$$

ii) Zum Beweis der Umkehrung

$$ltT(I_r) \subset \left\langle\, lt(g) : g \in G_r \,\right\rangle$$

sei ein Polynom $f \in I_r$ vorgegeben. Da G eine Gröbner Basis von $I \supset I_r$ ist, gilt

$$lt(f) \in \left\langle\, lt(g) : g \in G \,\right\rangle .$$

Bei einem monomialen Ideal gilt dann

$$lt(f) \in \langle\, lt(g) \,\rangle$$

für ein geeignetes $g \in G$. Da $f \in I_r$ keine der Variablen

$$T_1,...,T_r$$

enthält, gilt dasselbe auch für $lt(f)$ und damit auch für $lt(g)$. Es bleibt zu zeigen, daß kein Monom von g eine der Variablen

$$T_1,...,T_r$$

enthält: Wenn ein Monom von g eine dieser Variablen enhielte, wäre dieses Monom bzgl. der Lex-Ordnung oder der r-ten Eliminationsordnung größer als jedes Monom aus $k[T_{r+1},...,T_n]$, insbesondere größer als das Leitmonom $lt(g)$, ein Widerspruch. Daher gilt

$$g \in k[T_{r+1},...,T_n], \text{ d.h. } g \in G_r, \text{ q.e.d.}$$

4.27 Toolbeispiel (Zariski Abschluß des Bildes)

Macaulay2

- MyExamples/GroebnerBase/TwistedCubicCurve

Die kubische Kurve im 3-dimensionalen affinen Raum wird gegeben durch die Parameterdarstellung

$$f : \mathbf{A}^1(K) \longrightarrow \mathbf{A}^3(K),\ f(t) = (t, t^2, t^3) \in \mathbf{A}^3(K).$$

Durch welches Ideal wird die Varietät

$$\overline{f(\mathbf{A}^1(K))} \subset \mathbf{A}^3(K)$$

beschrieben?

Der zugehörige kontravariante Morphismus zwischen den Koordinatenringen lautet

$$\varphi := \varphi_f : k[X,Y,Z] \longrightarrow k[T],\ \varphi(X) := T, \varphi(Y) := T^2, \varphi(Z) := T^3 \in k[T].$$

Diese Abbildung ist surjektiv. Nach Satz 2.16 ist daher das Bild

$$Z := f(\mathbf{A}^1(K)) \subset \mathbf{A}^3(K)$$

abgeschlossen und die Einschränkung

$$f : \mathbf{A}^1(K) \longrightarrow Z \subset \mathbf{A}^3(K)$$

ein regulärer Isomorphismus. Das Bild

$$Z \subset \mathbf{A}^3(K)$$

ist die affine Varietät zum Ideal

$$\ker \varphi = \langle X^2 - Y,\ X \cdot Y - Z,\ Y^2 - X \cdot Z \,\rangle \subset k[X,Y,Z].$$

Dieses Ideal wird überdies auch schon von 2 Elementen erzeugt:

$$\ker \varphi = \langle X^3 - Z,\ X^2 - Y \rangle \subset k[X,Y,Z]$$

Der Durchschnitt zweier Ideale ist ein geeignetes Eliminationsideal:

4.28 Lemma *(Durchschnitt zweier Ideale)*

Der Durchschnitt zweier Ideale $I_1, I_2 \subset k[T_1,...,T_n]$ ist das 1-Eliminationsideal

$$I_1 \cap I_2 = J_1 \subset k[T_1,...,T_n]$$

des Ideals

$$J := \langle T \cdot I_1 \rangle + \langle\ (1-T) \cdot I_2\ \rangle \subset k[T,T_1,...,T_n].$$

Beweis. i) Die Inklusion

$$I_1 \cap I_2 \subset J_1$$

folgt aus der für beliebiges $f \in k[T_1,...,T_n]$ gültigen Darstellung

$$f = T \cdot f + (1-T) \cdot f \in k[T,T_1,...,T_n]$$

ii) Die Umkehrung

$$I_1 \cap I_2 \supset J_1$$

folgt, indem man in einer Darstellung

$$f(T_1,...,T_n) = a_1(T,T_1,...,T_n) \cdot T \cdot g_1(T_1,...,T_n) + a_2(T,T_1,...,T_n) \cdot (1-T) \cdot g_2(T_1,...,T_n),$$

$$g_i \in I_i \subset k[T_1,...,T_n],\ i = 1, 2,$$

sukzessive $T = 0$ bzw. $T = 1$ setzt, q.e.d.

Dem Durchschnitt zweier Ideale entspricht geometrisch die Vereinigung der zugehörigen Varietäten (siehe Bemerkung 2.12):

$$Var(I_1 \cap I_2) = Var(I_1) \cup Var(I_2).$$

4.29 Definition *(Quotient zweier Ideale)*

Für zwei Ideale $I, J \subset R$ in einem Ring R definiert man ihren *Quotienten* als

$$I : J := \{\ r \in R : r \cdot J \subset I\ \}.$$

Der Quotient zweier Ideale läßt sich auf den Durchschnitt geeigneter Ideale zurückführen. Das folgende Lemma 4.30 gilt insbesondere für den Fall eines Polynomringes R.

4.30 Lemma *(Quotient zweier Ideale)*

Es seien $I, J \subset R$ zwei Ideale in einem Noetherschen Integritätsbereich R.

i) Mit einer Darstellung

$$J = \langle\ g_1,...,g_m\ \rangle$$

gilt

$$I : J = \bigcap_{i=1}^{m} I : \langle g_i \rangle$$

ii) Für ein Hauptideal $\langle g \rangle \subset R$ folgt aus einer Darstellung

$$I \cap \langle g \rangle = \langle\ f_1 \cdot g, ..., f_k \cdot g\ \rangle$$

die Darstellung des Quotienten als

$$I : \langle g \rangle = \langle f_1, ..., f_k \rangle .$$

Beweis. Die einzige nicht-triviale Aussage

$$I : \langle g \rangle \subset \langle f_1, ..., f_k \rangle$$

folgt aus der Nullteilerfreiheit des Ringes, q.e.d.

4.31 Lemma (Komplement einer affinen Varietät)

Für die Varietäten zweier Ideale

$$I, J \subset k[T_1, ..., T_n],\ I = \sqrt{I}\ \text{ reduziert,}$$

gilt

$$Var(I : J) = \overline{Var(I) - Var(J)}.$$

Beweis. Für eine beliebige Teilmenge $X \subset \boldsymbol{A}_{\boldsymbol{K}}^{\boldsymbol{n}}$ gilt

$$Var(\ Id\ (X)\ ) = \overline{X}\ .$$

Wir setzen

$$X := Var(\ I\ ) - Var(J).$$

Dann ist folgende Aussage über Ideale zu zeigen:

$$I : J = Id(\ Var(I) - Var(J)\ ).$$

i) Beweis der Inklusion

$$I : J \subset Id(\ Var(I) - Var(J)\ ).$$

Sei

$$f \in I : J\text{, d.h. } f \cdot J \subset I\ .$$

Für einen beliebigen Punkt

$$x \in Var(I) - Var(J)$$

gilt:

$$(f \cdot g)(x) = 0 \text{ für alle } g \in J$$

und es existiert ein Element $g_0 \in J$ mit $g_0(x) \neq 0$. Aus

$$(f \cdot g_0)(x) = 0\text{, aber } g_0(x) \neq 0,$$

folgt $f(x) = 0$. Also gilt

$$f \in Id\big(\, Var(I) - Var(J)\,\big).$$

ii) Beweis der umgekehrten Inklusion

$$Id\big(\, Var(I) - Var(J)\,\big) \subset I : J\ .$$

Sei

$$f \in Id\big(\, Var(I) - Var(J)\,\big).$$

Dann gilt

$$f(x) = 0 \text{ für alle } x \in Var(I) - Var(J).$$

Für jedes Element $g \in J$ gilt

$$g(x) = 0 \text{ für alle } x \in Var(J)$$

also

$$(f \cdot g)(x) = 0 \text{ für alle } x \in Var(I)$$

oder

$$f \cdot g \in Id\big(\, Var(I)\,\big).$$

Nach dem Hilbertschen Nullstellensatz (siehe Bemerkung 2.12) und der Voraussetzung über I gilt

$$Id\big(\, Var(I)\,\big) = \sqrt{I} = I$$

und daher

$$f \cdot g \in I\ .$$

Es folgt

$$f \cdot J \subset I \text{, d.h. } f \in I : J \text{, q.e.d.}$$

4.32 Toolbeispiel (Komplement einer affinen Varietät)

Macaulay2:

- MyExamples/IdealOperations/Examples

Aus der Varietät von Beispiel 3.16 entsteht durch Herausnahme der x-Achse die y/z-Ebene:

$$\overline{Var\big(\,\langle X \cdot Y, X \cdot Z\rangle\,\big)} - Var\big(\,\langle X, Y\rangle\,\big) = Var\big(\,\langle X\rangle\,\big).$$

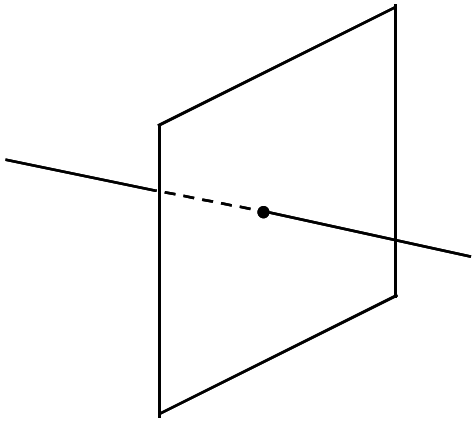


Abbildung 4: Y/Z-Ebene vereinigt mit X-Achse

5 Hilbert Polynom und Dimension

Die Theorie der Hilbert Polynome setzt graduierte Ringe und Moduln voraus. Daher behandeln wir als nächstes graduierte Objekte. Danach definieren als Anwendung der Graduierung in Definition 5.10 die Dimension einer affinen Varietät mit Hilfe des Hilbert Polynoms ihres Koordinatenringes.

Die Poincaré Reihe graduierter Algebren

5.1 Definition (Graduierte Objekte)

Ein *graduierter Ring* ist ein Ring A zusammen mit einer *Graduierung*, d.h. einer Familie

$$(A_s)_{s\in N}$$

von Untergruppen der additiven Gruppe $(A,+)$ mit der Eigenschaft:

$$A = \oplus_{s\in N} A_s$$

und Multiplikationsverhalten

$$A_r \cdot A_s \subset A_{r+s}\,.$$

Ein *Morphismus graduierter Ringe*

$$f : (A,(A_s)_{s\in N}) \longrightarrow (B,(B_s)_{s\in N})$$

ist eine Abbildung von Ringen

$$f : A \longrightarrow B \text{ mit } f(A_s) \subset B_s, s \in \boldsymbol{N}\,.$$

Ist A ein graduierter Ring, so ist ein *graduierter A-Modul* ein A-Modul M zusammen mit einer *Graduierung*, d.h. einer Familie

$$(M_s)_{s\in N}$$

von Untergruppen der additiven Gruppe $(M,+)$ mit der Eigenschaft:

$$M = \oplus_{s\in N} M_s \text{ und } A_r \cdot M_s \subset M_{r+s}\,.$$

Ein *Morphismus graduierter A-Moduln*

$$f : (M,(M_s)_{s\in N}) \longrightarrow (N,(N_s)_{s\in N})$$

ist eine Abbildung von Moduln

$$f : M \longrightarrow N \text{ mit } f(M_s) \subset N_s, s \in \boldsymbol{N}\,.$$

Im Falle einer Graduierung $(A_s)_{s\in N}$ oder $(M_s)_{s\in N}$ heißen die Elemente

$$a \in A_s \text{ bzw. } m \in M_s$$

homogen vom Grad $s \in \boldsymbol{N}$.

Bei einem graduierten Ring A ist die Komponente A_0 wegen der Bedingung

$$A_0 \cdot A_0 \subset A_0$$

ein Ring und man nennt A daher auch eine graduierte A_0-Algebra. Wir werden uns vor allem mit dem Fall eines Körpers

$$A_0 = k$$

befassen. Die Teilmenge

$$A_+ := \oplus_{s\geq 1} A_s \subset A$$

ist ein Ideal von A.

Die Graduierung eines Ringes bzw. Moduls zerlegt den Ring oder Modul also als eine direkte Summe additiver Untergruppen, die in vorgeschriebener Weise mit der Ringmultiplikation verträglich sind. Ziel ist es dann, das gesamte Objekt mit Hilfe seiner Komponenten zu studieren. Die Komponenten einer graduierten k-Algebra sind k-Vektorräume. Sie sind endlich dimensional, wenn die graduierte k-Algebra ein Noetherscher Ring ist. Ebenso sind die Komponenten eines endlich erzeugten Moduls über einer Noetherschen k-Algebra A endlich dimensionale k-Vektorräume. Die wichtigste Eigenschaft dieser Komponenten sind ihre Vektorraumdimensionen. Man studiert daher als erstes die Dimension

$$\dim_k M_s$$

als Funktion von $s \in \boldsymbol{N}$. Die Funktion heißt die Hilbert Funktion von M.

*5.2 **Beispiel** (Graduierte Algebra)*

i) Das Musterbeispiel einer graduierten k-Algebra ist der Polynomring

$$R = k[T_1,...,T_n]$$

mit der Graduierung durch die homogenen Polynome fester Grade:

$$R_s := \{ f \in R : f \text{ homogen und } \deg(f) = s\},\ s \in \boldsymbol{N}.$$

Dabei heißt ein Polynom

$$f \in k[T_1,...,T_n]$$

homogen vom Grad s, wenn alle seine Monome denselben Grad s haben. Ein Ideal

$$I \subset k[T_1,...,T_n]$$

heißt homogen, wenn es ein Erzeugendensystem aus homogenen Polynomen hat; ihre Grade können verschieden sein.

Aus der graduierten k-Algebra des Polynomrings entspringen sofort weitere Beispiele. Für ein homogenes Ideal $I \subset R$ überträgt sich die Graduierung von R auf den Quotienten

$$A = k[T_1,...,T_n] \,/\, I :$$

Wir setzen

$$I_s := I \cap R_s$$

und definieren eine Graduierung von A als

$$A_s := R_s / I_s,\ s \in \boldsymbol{N}.$$

Dabei ist zu beachten, daß wir das Ideal I als homogenes Ideal voraussetzen müssen, um eine direkte Summenzerlegung

$$A = \oplus_{s\in N} A_s$$

zu erhalten. Diese Art von graduierten Ringen spielt in der projektiven algebraischen Geometrie die zentrale Rolle. Wir werden sie in Kapitel ??? behandeln.

ii) Eine zweite Art von graduierten Ringen und Moduln leitet sich aus einem Paar (A, I) mit einem beliebigen Ring A und einem ausgezeichneten Ideal $I \subset A$ ab: Die Quotienten

$$I^s / I^{s+1}\ ,\ s \in \mathbf{N}\ ,$$

sind additive Gruppen bzgl. der von $(I, +)$ induzierten Addition. Die Abelsche Gruppe

$$\oplus_{s\in N}\ I^s / I^{s+1}$$

wird durch die Multiplikation

$$\left(x + I^{r+1}\right)\cdot\left(y + I^{s+1}\right) := x \cdot y + I^{r+s+1}$$

zu einem graduierten Ring

$$Gr(A, I)$$

mit der Graduierung

$$\left(I^s / I^{s+1}\right)_{s\in N}\ .$$

Analog definiert jeder A-Modul M einen graduierter $Gr(A, I)$-Modul $Gr(M, I)$: Setzt man

$$M_s := I^s \cdot M\ ,\ s \in \mathbf{N}\ ,$$

und

$$Gr(M, I) := \oplus_{s\in N}\ M_s / M_{s+1}\ , s \in \mathbf{N}\ ,$$

so ist die Familie

$$\left(M_s / M_{s+1}\right)_{s\in N}$$

eine Graduierung von $Gr(M, I)$.

Zur Vorbereitung der Hilbert Funktion beweisen wir ein Kriterium, unter welchen Voraussetzungen sich die Noether Eigenschaft der Ausgangsringe und Moduln auf die graduierten Objekte überträgt.

5.3 Lemma (Noether Eigenschaft graduierter Ringe und graduierter Moduln)

i) Ein graduierter Ring A mit Graduierung $\left(A_s\right)_{s\in N}$ ist genau dann Noethersch, wenn der Ring A_0 Noethersch und A eine endlich erzeugte A_0-Algebra ist.

ii) Für ein Paar (A, I) mit einem Noetherschen Ring A und einem Ideal $I \subset A$ ist auch der graduierte Ring $Gr(A, I)$ Noethersch.

iii) Es sei A ein Noetherscher Ring und M ein endlich erzeugter A-Modul. Dann ist $Gr(M, I)$ ein endlich erzeugter $Gr(A, I)$-Modul.

Beweis. ad i) Ist A_0 Noethersch und A eine endlich erzeugte A_0-Algebra, so ist A als Quotient eines Polynomringes $A_0[T_1,...,T_n]$ ebenfalls Noethersch nach dem Hilbertschen Basisatz.

Beweis der Umkehrung: Die Teilmenge

$$A_+ := \oplus_{s\geq 1} A_s \subset A$$

ist ein Ideal. Als Quotient eines Noetherschen Ringes ist $A_0 = A/A_+$ selbst Noethersch. Außerdem wird das Ideal A_+ von endlich vielen Elementen $a_1,...,a_n$ erzeugt, die wir als homogene Elemente mit positiven Graden $d_1,...,d_n$ annehmen dürfen. Wir behaupten

$$A = A_0[a_1,...,a_n].$$

Dazu zeigen wir $A_s \subset A_0[a_1,...,a_n]$ durch Induktion über $s \in \boldsymbol{N}$. Für $s = 0$ ist die Aussage wahr. Ein beliebiges homogenes Element $y \in A_s$ hat als Mitglied des Ideals A_+ die Gestalt

$$y = \sum_{i=1}^{n} b_i \cdot a_i$$

mit homogenen Koeffizienten $b_i \in A_{s-d_i}$. Sie liegen nach Induktionsvoraussetzung alle in $A_0[a_1,...,a_n]$, also gilt das auch für y.

ad ii) Zunächst ist $A_0 := A/I$ Noethersch. Es sei

$$a_1,...,a_n \in I$$

ein endliches Erzeugendensystem des Ideals $I \subset A$ und es seien

$$\overline{a_1},...,\overline{a_n} \in I/I^2$$

die Restklassen. Dann gilt

$$Gr(A,I) = A_0\left[\overline{a_1},...,\overline{a_n}\right].$$

Nach dem bereits bewiesenen Teil i) ist $Gr(A,I)$ Noethersch.

ad iii) Wir setzen

$$G_s(M) := I^s \cdot M / I^{s+1} \cdot M .$$

Ist $m_1,...,m_n$ ein Erzeugendensystem des A-Moduls M, so bilden die Restklassen

$$\overline{m_1},...,\overline{m_n} \in G_0(M)$$

ein Erzeugendensystem des A_0-Moduls

$$G_0(M).$$

Nun gilt

$$G_s(M) = I^s \cdot G_0(M)$$

und nach Teil ii)

$$Gr(A,I) = A_0\left[\overline{a_1},...,\overline{a_n}\right] \text{ mit } \overline{a_1},...,\overline{a_n} \in I/I^2 .$$

Hieraus folgt, daß

$$Gr(M, I) = \oplus_{s \in \mathbf{N}} G_s(M)$$

über dem Ring $Gr(A, I)$ von den Elementen

$$\overline{m_1}, \ldots, \overline{m_n} \in G_0(M)$$

erzeugt wird, q.e.d.

*5.4 **Definition** (Hilbert Funktion und Poincaré Reihe)*

Es sei k ein Körper, A eine graduierte k-Algebra von endlichem Typ und M ein graduierter, endlich erzeugter A-Modul mit Graduierung $(M_s)_{s \in \mathbf{N}}$. Die *Hilbert Funktion von* M ist die Funktion

$$Hilb_M : \mathbf{N} \longrightarrow \mathbf{N},\ s \mapsto \dim_k M_s,$$

ihre erzeugende formale Potenzreihe

$$Poinc_M(T) := \sum_{s=0}^{\infty} Hilb_M(s) \cdot T^s \in \mathbf{Z}[[T]]$$

heißt *Poincaré Reihe von* M.

Weil M als A-Modul endlich erzeugt ist, sind auch alle k-Vektorräume M_s endlich-dimensional, und die Hilbert Funktion ist wohldefiniert.

Die Poincaré Reihe wurde als formale Potenzreihe eingeführt. Ihre wichtigste Eigenschaft ist die Rationalität: Die Poincaré Reihe ist eine rationale Funktion. Hieraus folgt in wichtigen Fällen, daß die Hilbert Funktion sich für großes Argument wie ein Polynom verhält.

*5.5 **Satz** (Rationalität der Poincaré Reihe)*

Es sei k ein Körper, A eine graduierte Noethersche k-Algebra und M ein endlich erzeugter, graduierter A-Modul.

i) Die Poincaré Reihe von M ist eine rationale Funktion der Gestalt

$$Poinc_M(T) = \frac{f(T)}{\prod_{i=1}^{n} \left(1 - T^{m_i}\right)}$$

mit einem Polynom $f(T) \in \mathbf{Z}[T]$. Dabei sind die im Nenner auftretenden Exponenten

$$m_i := \deg a_i \in \mathbf{N}$$

die Grade der homogenen Elementen

$$a_i \in A,\ i = 1, \ldots, n,$$

eines Erzeugendensystems der k-Algebra

$$A = k[a_1, \ldots, a_n].$$

ii) Falls alle Erzeugenden denselben Grad $m_i = 1$ haben, existieren ein eindeutig bestimmtes Polynom, das *Hilbert Polynom von* M,

$$HP_M(T) \in \boldsymbol{Q}[T]$$

und eine Konstante $t_0 \in \boldsymbol{N}$ mit

$$Hilb_M(t) = HP_M(t) \text{ für alle } t \geq t_0 .$$

Das Hilbert Polynom hat die Gestalt

$$HP_M(T) = \frac{e}{m!} \cdot T^m + \text{Terme niedrigeren Grades in } T .$$

Sein Grad $m \in \boldsymbol{N}$ berechnet sich als

$$m = d - 1$$

aus der Ordnung $d \in \boldsymbol{N}$ der Polstelle der Poincaré Reihe im Punkt $t = 1$. Der Zähler

$$e \in \boldsymbol{N}$$

seines Leitkoeffizienten ist der niedrigste, von Null verschiedene Koeffizient in der Laurententwicklung der Poincaré Reihe um den Punkt $t = 1$. Das Nullpolynom erhält den Grad

$$m = -1 .$$

Beweis. i) Wir beweisen die Aussage über die Rationalität der Poincaré Reihe durch Induktion über die Anzahl n der Algebra-Erzeugenden von

$$A = A_0[a_1, ..., a_n].$$

Im Falle $n = 0$ ist

$$A = A_0 = k$$

ein Körper und M ein endlich dimensionaler k-Vektorraum. Es gibt ein $s_0 \in \boldsymbol{N}$ mit

$$M_s = 0 \text{ für } s \geq s_0 .$$

Die Poincaré Reihe ist sogar ein Polynom aus $\boldsymbol{Z}[T]$.

Für den Induktionsschritt sei $n > 0$ vorgegeben. Für jedes $s \in \boldsymbol{N}$ liefert die Multiplikation mit dem homogenen Element $a_n \in A$ vom Grad $m = m_n$ eine kanonische exakte Sequenz von A-Moduln

$$0 \longrightarrow K_s \longrightarrow M_s \xrightarrow{a_n} M_{s+m} \longrightarrow Q_{s+m} \longrightarrow 0 .$$

Die durch den Kern bzw. den Cokern definierten graduierten A-Moduln

$$K := \oplus_{s \in \boldsymbol{N}} K_s \text{ und } Q := \oplus_{s \in \boldsymbol{N}} Q_s \text{ mit } M_s / (a_n \cdot M_{s-m})$$

werden von a_n annuliert, sind also schon Moduln über dem Ring $A_0[a_1, ..., a_{n-1}]$. Als k-Vektorräume sind alle auftretenden Moduln endlich dimensional. Aus der Additivität der Dimension folgt

$$\dim_k K_s - \dim_k M_s + \dim_k M_{s+m} - \dim_k Q_{s+m} = 0$$

Multiplikation mit T^{s+m} liefert

$$T^m \cdot \dim_k K_s \cdot T^s - T^m \cdot \dim_k M_s \cdot T^s + \dim_k M_{s+m} \cdot T^{s+m} - \dim_k Q_{s+m} \cdot T^{s+m} = 0$$

und die formale Summation über s mit $s \geq -m$ ergibt

$$T^m \cdot Poinc_K(T) - T^m \cdot Poinc_M(T) + Poinc_M(T) - Poinc_Q(T) = 0 .$$

Auf die rechte Seite der Gleichung

$$Poinc_M(T) \cdot (1 - T^m) = Poinc_Q(T) - T^m \cdot Poinc_K(T)$$

wenden wir die Induktionsvoraussetzung an und erhalten

$$Poinc_M(T) = \frac{Poinc_Q(T) - T^m \cdot Poinc_K(T)}{1 - T^m} = \frac{1}{1 - T^m} \cdot \frac{f_Q(T) - T^m \cdot f_K(T)}{\prod_{i=1}^{n-1} (1 - T^{m_i})}$$

mit Polynomen

$$f_Q(T),\ f_K(T) \in \boldsymbol{Z}[T].$$

Wir erhalten die gewünschte Darstellung

$$Poinc_M(T) = \frac{f(T)}{\prod_{i=1}^{n} (1 - T^{m_i})}$$

wenn wir definieren

$$f(T) := f_Q(T) - T^m \cdot f_K(T) \in \boldsymbol{Z}[T].$$

ii) Nach Teil i) ist die Poincaré Reihe nicht nur eine formale Reihe, sondern sogar eine rationale Funktion mit einem Pol höchstens an der Stelle $t = 1$. Es sei

$$d := ord_\infty(Poinc_M(T),\ t = 1) \geq 0$$

die zugehörige Polordnung.

Im Falle $d = 0$ ist die Poincaré Reihe ein Polynom, so daß die Hilbert Funktion für große Argumente verschwindet. Das Hilbert Polynom ist daher das Nullpolynom.

Wir betrachten nun den Fall $d \geq 1$. Nach eventuellem Kürzen können wir annehmen, daß in der Darstellung

$$Poinc_M(T) = \frac{f(T)}{(1 - T)^d}$$

Zähler und Nenner teilerfremd sind, also

$$0 \neq f(1) \in \boldsymbol{Z} .$$

Der Funktionswert $Hilb_M(s)$ ist der Koeffizient des Monoms T^s in der formalen Potenzreihe des Quotienten

$$\frac{f(T)}{(1 - T)^d} .$$

Wir müssen daher die formale Potenzreihendarstellung dieses Quotienten finden. Der Zähler ist ein Polynom eines Grades N der Form

$$f(T)=\sum_{i=0}^{N} b_i \cdot T^i \text{ mit Koeffizienten } b_i \in \boldsymbol{Z}\,.$$

Durch $d-1$-maliges Differenzieren der geometrischen Reihe

$$\frac{1}{1-T}=\sum_{i=0}^{\infty} T^i$$

erhalten wir

$$\frac{(d-1)!}{(1-T)^d}=\sum_{i=0}^{\infty} i\cdot(i-1)\cdot\ldots\cdot(i-(d-1)+1)\cdot T^{i-(d-1)}=\sum_{j=0}^{\infty}(j+d-1)\cdot(j+d-2)\cdot\ldots\cdot(j+1)\cdot T^j\,,$$

also für den Nenner

$$\frac{1}{(1-T)^d}=\sum_{j=0}^{\infty}\binom{j+d-1}{d-1}\cdot T^j$$

Nach der Formel für die Koeffizienten des Produktes

$$Poinc_M(T)=\frac{f(T)}{(1-T)^d}=\left[\sum_{i=0}^{N} b_i\cdot T^i\right]\cdot\left[\sum_{j=0}^{\infty}\binom{j+d-1}{d-1}\cdot T^j\right]$$

berechnen wir den Koeffizienten des Monoms T^s in $Poinc_M(T)$ als Summe der Produkte der Ordnung s zu

$$Hilb_M(s)=\sum_{i=0}^{\min(N,s)} b_i\cdot\binom{s-i+d-1}{d-1}.$$

Als Funktion von s ist jeder Binomialkoeffizient

$$\binom{s-i+d-1}{d-1}$$

ein Polynom vom Grad $d-1$ mit rationalen Koeffizienten und Leitkoeffizient

$$\frac{1}{(d-1)!}.$$

Wir definieren das Polynom

$$HP_M(T):=\sum_{i=0}^{N} b_i\cdot\binom{T-i+d-1}{d-1}\in\boldsymbol{Q}[T].$$

Es hat den Leitkoeffizienten

$$\frac{\sum_{i=0}^{N} b_i}{(d-1)!}=\frac{f(1)}{(d-1)!}\neq 0\,,$$

den Grad $d-1$, und für alle $s\geq s_0:=N$ gilt

$$Hilb_M(s)=HP_M(s).$$

Durch die letzte Gleichung ist das Polynom eindeutig bestimmt. Mit

$$Hilb_M(s)\geq 0 \text{ für alle } s\in\boldsymbol{N}$$

folgt, daß der Leitkoeffizient des Hilbert Polynoms $HP_M(T)$ positiv ist, also $e \in \boldsymbol{N}^*$, q.e.d.

In der Darstellung der Poicaré Reihe eines graduierten A-Moduls M gemäß Satz 5.5 hängt der Nenner nicht von M, sondern allein von A ab. Der Beweis von Satz 5.5 zeigt, daß die Polordnung unter den Voraussetzungen von Teil ii) nach oben beschränkt ist durch die Anzahl der Erzeugenden der k-Algebra

$$A = k[a_1,...,a_n].$$

5.6 **Beispiel** *(Hilbert Polynom des Polynomringes)*

i) Der Polynomring $k[T_1,...,T_n]$ mit seiner Graduierung durch die homogenen Polynome stimmt überein mit der graduierten k-Algebra

$$A = Gr(k[T_1,...,T_n], m_T)$$

bzgl. des maximalen Ideals

$$m_T := \langle T_1,...,T_n \rangle \subset k[T_1,...,T_n].$$

Wir fassen A als graduierten Modul über sich selbst auf und berechnen seine Hilbert Funktion, seine Poincaré Reihe und sein Hilbert Polynom: Es ist

$$\dim_k A_s = \binom{s+n-1}{s-1} = \binom{s+n-1}{n-1}.$$

Die Poincaré Reihe ergibt sich mit der im Beweis von Satz 5.5 gezeigten Formel für die Ableitung der geometrischen Reihe als

$$Poinc_A(T) = \sum_{s=0}^{\infty} \binom{s+n-1}{n-1} \cdot T^s = \frac{1}{(1-T)^n}.$$

Sie ist eine rationale Funktion mit einem einzigen Pol an der Stelle $T = 1$. Er hat die Ordnung n, der zugehörige Koeffizient der Laurent Entwicklung hat den Wert 1. Das Hilbert Polynom hat die Gestalt

$$HP_A(T) = \frac{1}{(n-1)!} T^{n-1} + \textit{Terme niedrigeren Grades in } T\ .$$

Es stellt die Hilbert Funktion für alle Argumente $t \geq 0$ dar. Für spätere Zwecke halten wir noch fest: Für

$$A_{\leq s} := \oplus_{i \leq s} A_i$$

gilt

$$\dim_k A_{\leq s} = \sum_{i=0}^{s} \dim_k A_i = \binom{s+n}{n}.$$

ii) Ein Koordinatenunterraum des $\boldsymbol{A}^n(K)$

$$X = Var(\langle T_{i_1},...,T_{i_r} \rangle)$$

mit r verschiedenen Variablenindizes

$$J = \{ i_1,...,i_r \}$$

hat als Koordinatenring

$$k[X] = k[T_i : i \notin J] \cong k[T_1, ..., T_{n-r}]$$

den Polynomring in $n - r$ Variablen.

Dimension einer affinen Varietät

In Beispiel 5.6 deutete sich bereits der gesuchte Zusammenhang an zwischen der Dimension einer affinen Varietät und dem Hilbert-Polynom ihres Koordinatenringes. Der Polynomring

$$k[T_1,...,T_n]$$

soll als Koordinatenring der affinen Varietät $\boldsymbol{A}^n(K)$ die Dimension n erhalten. Seine Poincaré Reihe hat eine Polstelle der Ordnung n, ihr Hilbert Polynom daher den Grad $n-1$.

Zuvor müssen wir aber noch folgende Schwierigkeit überwinden. Der Koordinatenring einer algemeinen affinen Varietät ist kein graduierter Ring. Daher läßt sich das Konzept der Hilbert Funktion nicht direkt anwenden. Wir zeigen aber, daß man dem Koordinatenring einen graduierten Ring zuordnen kann, und daß der Grad seines Hilbert Polynoms eine geeignete Definition der Dimension ist. Der Übergang vom Koordinatenring zu einem graduierten Ring ist das Verfahren der Homogenisierung.

5.7 Definition (Homogenisierung und Dehomogenisierung)

Ein Polynom $f \in k[T_0,T_1,...,T_n]$ heißt *homogen* vom Grad $d \in \boldsymbol{N}$, wenn $Mon(f)$, die Menge seiner Monome, nur Monome vom Grad $d \in \boldsymbol{N}$ enthält.

i) Die *Homogenisierung eines Polynoms*

$$f \in k[T_1,...,T_n]$$

vom Grad $d \in \boldsymbol{N}$ in n Veränderlichen bzgl. einer zusätzlichen Veränderlichen T_0 ist das homogene Polynom

$$f^{\text{hom}} \in k[T_0,T_1,...,T_n]$$

in $n+1$ Veränderlichen:

$$f^{\text{hom}}(T_0,T_1,...,T_n) := T_0^{\,d} \cdot f\left(\frac{T_1}{T_0},...,\frac{T_n}{T_0}\right) \in k[T_0,T_1,...,T_n].$$

Die Homogenisierung ist ein homogenes Polynom desselben Grades wie das Ausgangspolynom. Die *Homogenisierung eines Ideals*

$$I \subset k[T_1,...,T_n]$$

ist das homogene Ideal

$$I^{\text{hom}} := \left\langle f^{\text{hom}} : f \in I \right\rangle \subset k[T_0,T_1,...,T_n].$$

ii) Die *Dehomogenisierung eines homogenen Polynoms*

$$f \in k[T_0,T_1,...,T_n] \text{ in } n+1$$

Veränderlichen bzgl. der Veränderlichen T_0 ist das Polynom

$$f^{dehom} \in k[T_1,...,T_n]$$

in n Veränderlichen mit

$$f^{dehom}(T_1,...,T_n) := f(1,T_1,...,T_n).$$

Die *Dehomogenisierung eines homogenen Ideals*

$$I \subset k[T_0, T_1, ..., T_n]$$

ist das Ideal

$$I^{dehom} := \left\langle f^{dehom} : f \in I \right\rangle \subset k[T_1, ..., T_n].$$

Dabei ist zu beachten, daß nicht aus jedem Erzeugendensystem eines Ideals durch Homogenisierung ein Erzeugendensystem des homogenisierten Ideals entsteht: Es sei

$$I := \left\langle X^3 + Z^2, X^3 + Y^2 \right\rangle \subset k[X, Y, Z].$$

Bzgl. der homogenisierenden Koordinate T gilt dann

$$\left\langle X^3 + T \cdot Z^2,\ X^3 + T \cdot Y^2 \right\rangle \underset{\neq}{\subset} I^{\text{hom}} \subset k[T, X, Y, Z],$$

weil

$$Z^2 - Y^2 = \left(\left(X^3 + Z^2 \right) - \left(X^3 + Y^2 \right) \right)^{\text{hom}} \notin \left\langle X^3 + T \cdot Z^2,\ X^3 + T \cdot Y^2 \right\rangle.$$

Anders im Falle einer Gröbnerbasis, hier gilt:

5.8 Lemma (Homogenisierung und Dehomogenisierung)

Es sei

$$I \subset k[T_1, ..., T_n]$$

ein Ideal und

$$I^{\text{hom}} \subset k[T_0, T_1, ..., T_n]$$

seine Homogenisierung.

i) Ist G eine Gröbnerbasis von I bzgl. einer graduierten Monomordnung, so ist

$$G^{\text{hom}} := \left\{ g^{\text{hom}} : g \in G \right\}$$

eine Gröbnerbasis von I^{hom} bzgl. einer graduierten Fortsetzung der Monomordnung. Insbesondere ist G^{hom} also ein Erzeugendensystem von I^{hom}.

ii) Ist G ein Erzeugendensystem von I^{hom}, so ist die Familie

$$G^{dehom} := \left\{ g^{dehom} : g \in G \right\}$$

ein Erzeugendensystem von I.

Beweis. ad i) Für jedes Polynom

$$h \in k[T_1, ..., T_n] \text{ vom Grad } d = \deg h$$

gilt bei einer graduierten Monomordnung

$$lt(h) = lt(h_d)$$

und bzgl. der graduierten Fortsetzung

$$lt\left(h^{\text{hom}}\right) = lt(h_d) = lt(h).$$

Weil G eine Gröbnerbasis von I ist, existiert für jedes Element $f \in I$ ein $g \in G$ und ein Monom a mit

$$lt(f) = a \cdot lt(g).$$

Es folgt

$$lt(f^{\text{hom}}) = lt(f) = a \cdot lt(g) = a \cdot lt(g^{\text{hom}}),$$

also

$$lt(f^{\text{hom}}) \in \langle\, lt(g) : g \in G^{\text{hom}} \,\rangle.$$

ad ii) Die Familie G^{dehom} ist ein Erzeugendensystem von I : Für ein Element

$$f \in k[T_1,...,T_n]$$

rechnet man sofort nach

$$\left(f^{\text{hom}}\right)^{dehom} = f\ .$$

Für $f \in I$ folgt aus einer Darstellung seiner Homogenisierung

$$f^{\text{hom}} = \sum_{g \in G} a_g \cdot g\ ,\ a_g \in k[T_0,T_1,...,T_n],\ g \in G\ ,$$

die Darstellung

$$f = \left(f^{\text{hom}}\right)^{dehom} = \sum_{g \in G} a_g{}^{dehom} \cdot g^{dehom}\ ,$$

also

$$f \in \langle\, g^{dehom} : g \in G \,\rangle.$$

Andererseits hat jedes $g \in G$ als Element von I^{hom} eine Darstellung

$$g = \sum_{i=1}^{s} a_i \cdot f_i^{\text{hom}} \ \text{ mit } a_i \in k[T_0,T_1,...,T_n] \text{ und } f_i \in I\ ,$$

so daß

$$g^{dehom} = \sum_{i=1}^{s} a_i{}^{dehom} \cdot \left(f_i^{\text{hom}}\right)^{dehom} = \sum_{i=1}^{s} a_i{}^{dehom} \cdot f \in I\ ,\ \text{q.e.d.}$$

Wir beginnen mit der Dimension des Koordinatenringes einer affinen Varietät und betrachten dazu etwas allgemeiner eine endliche erzeugte k -Algebra der Gestalt

$$A = k[T_1,...,T_n] \,/\, I$$

mit einem nicht notwendig reduzierten Ideal $I \subset k[T_1,...,T_n]$. Weil das Ideal nicht notwendig homogen ist, induziert die Graduierung von

$$R := k[T_1,...,T_n]$$

i.a. keine Graduierung des Quotienten A . Daher gehen wir zur Homogenisierung bzgl. einer neuen Variablen T_0 über. Wir fassen

$$A^{\hom} := k[T_0, T_1, ..., T_n] / I^{\hom}$$

als graduierte k-Algebra gemäß Beispiel 5.2 auf. Um sie mit der Ausgangsalgebra A zu vergleichen, setzen wir

$$R_{\leq s} := \{ f \in R : f \text{ homogen und } \deg(f) \leq s \} = \oplus_{i \leq s} R_i,$$

$$I_{\leq s} := I \cap R_{\leq s} \text{ und } A_{\leq s} := R_{\leq s} / I_{\leq s}, s \in \boldsymbol{N}.$$

Die Mengen $I_{\leq s}$ sind endlich dimensionale k-Vektorräume und ebenso die Quotienten $A_{\leq s}$. Für jedes $s \in \boldsymbol{N}$ ist die k-lineare Abbildung

$$k[T_1, ..., T_n]_{\leq s} \longrightarrow k[T_0, T_1, ..., T_n]_s, \; f \mapsto T_0^{\,s - \deg f} \cdot f^{\hom},$$

ein Isomorphismus mit Umkehrabbildung

$$k[T_0, T_1, ..., T_n]_s \longrightarrow k[T_1, ..., T_n]_{\leq s}, \; f \mapsto f^{dehom}$$

Daher sind die beiden k-Algebren

$$A_{\leq s} \text{ und } A^{\hom}{}_s$$

für jedes $s \in \boldsymbol{N}$ isomorph.

*5.9 **Definition** (Affine Hilbert Funktion)*

Die *affine Hilbert Funktion* $Hilb_A^{aff} \in Q[T]$ einer endlich-erzeugten k-Algebra

$$A = k[T_1, ..., T_n] / I$$

ist die Hilbert Funktion der zugehörigen graduierten k-Algebra

$$A^{\hom} := k[T_0, T_1, ..., T_n] / I^{\hom},$$

d.h.

$$Hilb_A^{aff} = Hilb_{A^{\hom}}.$$

Es gilt also

$$Hilb_A^{aff}(s) = \dim_k A_{\leq s} \text{ für } s \in \boldsymbol{N}.$$

Nach Satz 5.5 verhält sich die Hilbert Funktion $Hilb_{A^{\hom}}$ für großes Argument wie ein Polynom. Also gibt es ein Polynom, das *affine Hilbert Polynom* von A,

$$HP_A^{aff}(T) \in \boldsymbol{Q}[T]$$

und eine Konstante s_0, so daß

$$Hilb_A^{aff}(s) = HP_A^{aff}(s) \text{ für alle } s \geq s_0.$$

*5.10 **Definition** (Dimension einer affinen Varietät)*

Die *Dimension einer endlich erzeugten k-Algebra* ist der Grad ihres affinen Hilbert Polynoms, die *Dimension einer affinen k-Varietät* ist die Dimension ihres Koordinatenringes.

Aufgrund der Berechnung des affinen Hilbert Polynoms in Beispiel 5.6 erhält der affine Raum $\boldsymbol{A}^n(K)$ gemäß Definition 5.10 die Dimension n. Sie stimmt mit der Vektorraumdimension des k-Vektorraumes

$$\boldsymbol{A}^n(K) = K^n$$

überein. Da Koordinatenunterräume ebenfalls affine Räume sind, stimmen auch für einen Koordinatenunterraum Dimension und Vektorraumdimension überein.

5.11 Toolbeispiel (Affines Hilbert Polynom)

Singular berechnet das affine Hilbert Polynom:

- MyExamples/HilbertPolynomial/Examples.

Um die Dimension einer affinen Varietät zu berechnen, muß man das definierende Ideal homogenisieren und den Grad des Hilbert Polynoms der resultierenden graduierten Algebra bestimmen. Hierbei kann man sich sogar auf monomiale Ideale beschränken, siehe Satz 5.13.

Definition 5.10 ist jedoch nur sinnvoll, wenn sie eine Eigenschaft der Isomorphieklasse der Varietät beschreibt, also nicht von der Wahl eines repräsentierenden Ideals abhängt. Wir werden die Unabhängigkeit der Dimension von der Wahl des repräsentierenden Ideals in Satz 5.17 beweisen. Das Resultat ist keinesfalls selbstverständlich, weil das affine Hilbert Polynom als ganzes sehr wohl von der Einbettung abhängt: Die affine Gerade

$$X = \boldsymbol{A}_k^1$$

hat das affine Hilbert Polynom

$$HP_X^{aff}(T) = 1 + T\ ,$$

die zu X isomorphe Parabel Y mit Ideal

$$I = \left\langle T_2 - T_1^2 \right\rangle \subset k[T_1, T_2]$$

hat dagegen das affine Hilbert Polynom

$$HP_Y^{aff}(T) = 1 + 2 \cdot T\ .$$

Im nächsten Schritt zeigen wir, daß für monomiale Varietäten der Dimensionsbegriff auf die Dimension eines Koordinatenunterraumes, und damit auf den linearen Fall einer Vektorraumdimension zurückgeführt werden kann: Die Dimension einer monomialen Varietät ist die Vektorraumdimension eines Koordinatenunterraumes maximaler Dimension.

5.12 Lemma (Dimension einer monomialen Varietät)

Es sei

$$I = \langle m_1, ..., m_r \rangle \underset{\neq}{\subset} k[T_1, ..., T_n]$$

ein monomiales Ideal, das nicht notwendig reduziert ist, und

$$A := k[T_1, ..., T_n] / I\ .$$

Die affine Hilbert Funktion von A an der Stelle $s \in \mathbf{N}$ zählt die Monome vom Grad $\leq s$, die nicht in I liegen:

$$Hilb_A^{aff}(s) = card\ \{ m \in k[T_1,...,T_n]_{\leq s} : m\ Monom\ und\ m \notin I \}.$$

Die Dimension von A ist die maximale Dimension eines in der Varietät

$$X := Var(I) \subset \mathbf{A}^n(K)$$

enthaltenen Koordinatenunterraumes. Insbesondere stimmen die Dimensionen von A und seiner Reduktion

$$A_{red} = k[T_1,...,T_n] / \sqrt{I}$$

überein.

Beweis. Nach Definition gilt

$$Hilb_A^{aff}(s) = \dim_k \left(k[T_1,...,T_n]_{\leq s} / I_{\leq s} \right) = \dim_k k[T_1,...,T_n]_{\leq s} - \dim_k I_{\leq s}.$$

Die Monome des k-Vektorraums $I_{\leq s}$ bilden eine Basis von $I_{\leq s}$, weil ein Polynom genau dann zu einem monomialen Ideal gehört, wenn jedes seiner Monome dazugehört.

Damit ist die Berechnung der Hilbert Funktion einer monomialen Varietät zurückgeführt auf die Abzählung von Monomen

$$m \in k[T_1,...,T_n],$$

und das geschieht am besten durch Abzählung der zugehörigen Exponenten

$$\alpha(m) \in \mathbf{N}^n.$$

Sei

$$C(I) := \mathbf{N}^n - \bigcup_{i=1,...,r} \left(a(m_i) + \mathbf{N}^n \right)$$

das Komplement aller Exponenten, die nicht zu Monomen aus I gehören, sowie

$$C(I)_{\leq s} \subset C(I)$$

die Teilmenge der Exponenten vom Grad $\leq s$. Bezeichnen wir mit

$$e_i \in \mathbf{N}^n,\ i = 1,...,n,$$

die kanonischen Einheitsvektoren, so ist die Menge $C(I)$ eine endliche Vereinigung

$$C(I) = \bigcup_{j \in I} T_j$$

von affinen Teilmengen

$$T_j = \alpha_j + span_{\mathbf{N}} \left\langle e_{i_1},...,e_{i_j} \right\rangle,\ \alpha_j \in \mathbf{N}^n,$$

die von

$$d_j := card\{ i_1,...,i_j \}$$

Einheitsvektoren aufgespannt werden. Die Abzählung der Elemente in

$$span_{\mathbf{N}} \left\langle e_{i_1},...,e_{i_j} \right\rangle$$

folgt Beispiel 5.6 für einen Polynomring mit d_j Variablen. Nach Translation um α_j ergibt sich

$$card\ T_{j,\le s} = \binom{d_j + s - |\alpha_j|}{s - |\alpha_j|} = \binom{d_j + s - |\alpha_j|}{d_j} \text{ für } s \ge |\alpha_j|.$$

Also ist die Kardinalität von $T_{j,\le s}$ für großes s ein Polynom vom Grad d_j mit führendem Koeffizienten $\frac{1}{d_j!}$. Die Vereinigung der T_j ist nicht notwendig disjunkt, daher dürfen bei der Berechnung der Kardinalität von $C(I)_{\le s}$ die Exponenten in den mehrfachen Durchschnitten nur einfach gezählt werden. Man zeigt, daß für großes s jedoch die Beiträge der T_j mit maximalem

$$d := \max\{d_j : j \in I\}$$

überwiegen. Für eine gegebene Familie von Variablenindizes

$$J = \{i_1,...,i_j\} \subset \{1,...,n\}$$

liegt der von den komplentären Variablen definierte Koordinatenunterraum E mit Ideal

$$I_E := \langle T_i : i \notin J \rangle \subset k[T_1,...,T_n]$$

genau dann in X, wenn

$$I_E \supset I,$$

d.h. wenn die Monome, die nicht in I_E liegen, zu $C(I)$ gehören. Die Monome, die nicht in I_E liegen, werden von keinem der Monome

$$T_i, i \notin J,$$

geteilt. Ihre Exponenten bilden die Menge

$$span_N\langle e_i : i \in J\rangle.$$

Äquivalent sind also:

- $E = Var(\langle T_i : i \notin J \rangle) \subset X = Var(I)$
- $span_N\langle e_i : i \in J\rangle \subset C(I)$
- $\alpha + span_N\langle e_i : i \in J\rangle \subset C(I)$ *für jedes* $\alpha \in \mathbf{N}^n$

Die Koordinatenunterräume maximaler Dimension, die in X enthalten sind, gehören also zu Teilmengen J mit maximaler Kardinalität. Die in obiger Darstellung

$$C(I) = \bigcup_{j \in I} T_j$$

auftretenden linearen Teilmengen T_j mit maximalem d_j gehören also zu in X enthaltenen Koordinatenunterräumen maximaler Dimension d. Die führenden Koeffizienten $\frac{1}{d!}$ ihrer Polynome sind positiv und können sich daher nicht annullieren. Daher verhält sich die affine Hilbert Funktion

$$Hilb_{k[X]}^{aff} : \boldsymbol{N} \longrightarrow \boldsymbol{N},\ s \mapsto card\ C(I)_{\leq s},$$

für großes Argument wie ein Polynom vom Grad d, q.e.d.

Der folgende Satz von Macaulay zeigt die Bedeutung des führenden Ideals für die Berechnung der Dimension: Ein homogenes Ideal und sein bezüglich einer beliebigen Monomordung gebildetes führendes Ideal haben dieselbe Hilbert Funktion. Damit ist der Dimensionbegriff einer beliebigen Varietät zurückgeführt auf die Dimension einer monomialen Varietät.

5.13 Satz *(Hilbert Funktion und führendes Ideal)*

Für ein homogenes Ideal

$$I \subset k[T_1,...,T_n]$$

hat die Quotientenalgebra

$$k[T_1,...,T_n]/I$$

dieselbe Hilbert Funktion wie die bzgl. einer beliebigen monomialen Ordnung gebildete Quotientenalgebra

$$k[T_1,...,T_n]/lt(I).$$

Beweis. Wir beweisen, daß für jedes feste $s \in \boldsymbol{N}$ die Restklassen der Monome aus der Menge

$$S := \{ m \in k[T_1,...,T_n]_s : m \notin lt(I) \}$$

in den jeweiligen k-Vektorräumen

$$k[T_1,...,T_n]_s/I_s \text{ bzw. } k[T_1,...,T_n]_s/lt(I)_s$$

eine Basis sind. Dazu zeigen wir, daß die beiden von der Inklusion induzierten Abbildungen

$$span_k S \longrightarrow k[T_1,...,T_n]_s/I_s \text{ und } span_k S \longrightarrow k[T_1,...,T_n]_s/lt(I)_s$$

Isomorphismen von k-Vektorräumen sind. Die Injektivität der ersten Abbildungen folgt sofort aus der Definition von S, bei der Injektivität der zweiten ist zu beachten, daß das Ideal $lt(I)$ monomial ist, also mit jedem Polynom auch alle seine Monome enthält. Für die Surjektivität beider Abbildungen, zeigen wir, daß jede Restklasse der Quotienten

$$k[T_1,...,T_n]_s/I_s \text{ und } k[T_1,...,T_n]_s/lt(I)_s$$

ein Element aus $span_k S$ enthält. Das gesuchte Element kann als die Normalform eines beliebigen Elementes der Restklasse gewählt werden: Dazu wählen wir eine Standardbasis G von I bzgl. der gegebenen monomialen Ordnung. Ein homogenes Element

$$f \in k[T_1,...,T_n]_s$$

hat auch homogene Normalformen

$$NF(f \mid G) \in k[T_1,...,T_n]_s \text{ bzw. } NF(f \mid lt(G)) \in k[T_1,...,T_n]_s,$$

und diese definieren in

$$k[T_1,...,T_n]_s/I_s \text{ bzw. } k[T_1,...,T_n]_s/lt(I)_s$$

jeweils dieselbe Restklasse wie f. Nach Definition der Normalform gehört der führende Terme von $NF(f \mid G)$ nicht zu $lt(G)$. Weil G eine Standardbasis ist, gilt

$$lt(G) = lt(I),$$

und damit gehört der führende Term von $NF(f \mid G)$ auch nicht zu $lt(I)$, sondern nach Definition zu S. Der führende Term von

$$NF(\ f \mid lt(G)\ )$$

gehört nicht zu

$$lt(lt(G)) = lt(G) = lt(I),$$

und gehört damit ebenfalls zu S. Wir iterieren die Berechnung der Normalformen für die Elemente

$$tail(\ NF(\ f \mid G)\ ) \text{ und } tail(\ NF(\ f \mid lt(G))\ )$$

und erhalten nach endlich vielen Schritten Darstellungen

$$NF(f \mid G) \in span_k S \text{ und } NF(f \mid lt(G)\ ) \in span_k S \text{ , q.e.d.}$$

Um die Hilbert Funktion des Quotienten

$$k[T_1,...,T_n]\ /lt(I)$$

zu berechnen, zählt man nach Lemma 5.12 die Monome eines gegebenen Grades, welche nicht in dem monomialen Ideal $lt(I)$ liegen.

Ein Ideal und sein bezüglich einer graduierten Monomordung gebildetes führendes Ideal haben dieselbe affine Hilbert-Funktion.

5.14 Korollar (Affine Hilbert Funktion und führendes Ideal)

Für ein Ideal

$$I \subset k[T_1,...,T_n]$$

hat die Quotientenalgebra

$$k[T_1,...,T_n]\ /I$$

dieselbe affine Hilbert Funktion wie die bzgl. einer graduierten monomialen Ordnung gebildete Quotientenalgebra

$$k[T_1,...,T_n]\ /lt(I).$$

Beweis. Bei der Homogenisierung

$$\text{von } I \subset k[T_1,...,T_n] \text{ zu } I^{\text{hom}} \subset k[T_0,T_1,...,T_n]$$

setzen wir die auf $k[T_1,...,T_n]$ gegebene graduierte Ordnung zu einer graduierten Ordnung ">" auf $k[T_0,T_1,...,T_n]$ fort mit

$$T_i > T_0,\ i = 1,...,n\ .$$

Die gegebene monomiale Ordnung ist graduiert. Daher hat der führenden Term eines Elementes

$$f \in k[T_1,...,T_n]$$

dieselbe Ordnung wie f, und nach Wahl der Fortsetzung hat die Homogenisierung

$$f^{\text{hom}} \in k[T_0,T_1,...,T_n]$$

denselben führenden Term

$$lt(f) = lt\left(f^{\text{hom}}\right) \in k[T_1,...,T_n] \subset k[T_0,T_1,...,T_n].$$

Es gilt also

$$lt\left(I^{\text{hom}}\right) = \langle\ lt(I)\ \rangle = lt(I)^{\text{hom}} \subset k[T_0,T_1,...,T_n],$$

weil die Homogenisierung ein Monom nicht ändert. Wir erhalten

$$k[T_0,T_1,...,T_n]\ /lt\left(I^{\text{hom}}\right) = k[T_0,T_1,...,T_n]\ /lt(I)^{\text{hom}}$$

Nach Satz 5.13 haben

$$k[T_0,T_1,...,T_n]\ /lt\left(I^{\text{hom}}\right) \text{ und } k[T_0,T_1,...,T_n]\ /I^{\text{hom}}$$

dieselbe Hilbert Funktion. Daher haben auch die beiden Quotientenalgebren

$$k[T_1,...,T_n]\ /I \text{ und } k[T_1,...,T_n]\ /lt(I)$$

dieselbe affine Hilbert Funktion, q. e. d.

5.15 Korollar *(Ideal und Radikal)*

Für ein Ideal

$$I \subset k[T_1,...,T_n]$$

haben die beiden Quotientenalgebren

$$k[T_1,...,T_n]\ /I \text{ und } k[T_1,...,T_n]\ /\sqrt{I}$$

dieselbe Dimension.

Beweis. Im Falle eines monomialen Ideals

$$I \subset k[T_1,...,T_n]$$

liefert Lemma 5.12 die Behauptung. Im Falle eines beliebigen Ideals wählen wir eine graduierte Monomordung von $k[T_1,...,T_n]$ und gehen aus von den Inklusionen

$$lt(I) \subset lt\left(\sqrt{I}\right) \subset \sqrt{lt(I)}\,.$$

Die linke Inklusion ergibt sich aus

$$I \subset \sqrt{I}$$

die rechte Inklusion aus der Implikation

$$h = lt(f)\ mit\ f^r \in I \Rightarrow h^r = lt\left(f^r\right).$$

Nach der für monomiale Ideale bereits bewiesenen Aussage haben die beiden Quotientenalgebren

$$k[T_1,...,T_n] / lt(I) \text{ und } k[T_1,...,T_n] / \sqrt{lt(I)}$$

dieselbe Dimension.

Für zwei beliebige Ideale

$$I_1 \subset I_2 \subset k[T_1,...,T_n]$$

gilt

$$(I_1)_{\leq s} < (I_2)_{\leq s},\ s \in \boldsymbol{N},$$

und hieraus folgt für die affinen Hilbert Funktionen der beiden Quotienten

$$A_i := k[T_1,...,T_n] / I_i,\ i = 1, 2,$$

die Abschätzung

$$Hilb_{A_1}^{aff}(s) \leq Hilb_{A_2}^{aff}(s),\ s \in \boldsymbol{N}.$$

Insbesondere hat das affine Hilbert Polynom von A_2 mindestens den Grad des affinen Hilbert Polynoms von A_1, d.h.

$$\dim A_1 \leq \dim A_2.$$

Wenden wir diese Überlegung auf die Ausgangskette von Inklusionen an, so erhalten wir die Dimensionsgleichheit der drei Quotientenalgebren

$$k[T_1,...,T_n] / lt(I),\ k[T_1,...,T_n] / \sqrt{lt(I)} \text{ und } k[T_1,...,T_n] / lt\left(\sqrt{I}\right).$$

Mit Satz 5.13 folgen daraus die Gleichheiten

$$\dim k[T_1,...,T_n] / I = \dim k[T_1,...,T_n] / lt(I) =$$

$$= \dim k[T_1,...,T_n] / lt\left(\sqrt{I}\right) = \dim k[T_1,...,T_n] / \sqrt{I},\ \text{q.e.d.}$$

5.16 Korollar (Dimension einer Vereinigung)

Die Dimension der Vereinigung zweier affiner k-Varietäten

$$X_1, X_2 \subset \boldsymbol{A}^n(K)$$

ist das Maximum der Dimensionen beider Komponenten:

$$\dim X_1 \cup X_2 = \max\{\dim X_1, \dim X_2\}.$$

Die Dimension einer affinen k-Varietät ist das Maxium der Dimensionen ihrer irreduziblen Komponenten.

Beweis. i) Mit

$$I_j := Id(X_j) \subset k[T_1,...,T_n],\ j = 1, 2,$$

gilt für das Verschwindungsideal der Vereinigung

$$Id(X_1 \cup X_2) = I_1 \cap I_2.$$

Die Inklusion

$$I_1 \cdot I_2 \subset I_1 \cap I_2 \subset \sqrt{I_1 \cdot I_2}$$

liefert eine Abschätzung der Grade der jeweiligen affinen Hilbert Polynome und damit die Abschätzung der Dimensionen

$$\dim k[T_1,...,T_n]/I_1 \cdot I_2 \geq \dim k[T_1,...,T_n]/I_1 \cap I_2 \geq \dim k[T_1,...,T_n]/\sqrt{I_1 \cdot I_2}$$

Weil nach Korollar 5.15 die beiden äußeren Dimensionen übereinstimmen, gilt insbesondere

$$\dim k[T_1,...,T_n]/I_1 \cdot I_2 = \dim k[T_1,...,T_n]/I_1 \cap I_2 .$$

Die Dimension der Vereinigung

$$\dim X_1 \cup X_2$$

ist demnach der Grad des affinen Hilbert Polynoms des Quotienten

$$k[T_1,...,T_n]/I_1 \cdot I_2 .$$

bzw. nach Korollar 5.14 des Quotienten

$$k[T_1,...,T_n]/lt(I_1 \cdot I_2)$$

bzgl. einer graduierten monomialen Ordnung. Nun gilt für jede monomiale Ordnung

$$lt(I_1) \cdot lt(I_2) \subset lt(I_1 \cdot I_2):$$

Denn nach Wahl zweier Gröbner Basen

$$G_j \text{ von } I_j,\ j = 1, 2$$

ist die Familie

$$G_1 \cdot G_2 := \{ g_1 \cdot g_2 : g_j \in G_j,\ j = 1, 2 \}$$

ein Erzeugendensystem von

$$I_1 \cdot I_2$$

und die Familie

$$\{ lt(g_1) \cdot lt(g_2) : g_j \in G_j,\ j = 1, 2 \}$$

ein Erzeugendensystem von

$$lt(I_1) \cdot lt(I_2).$$

Für jedes dieser Elemente gilt

$$lt(g_1) \cdot lt(g_2) = lt(g_1 \cdot g_2),$$

es folgt

$$lt(I_1) \cdot lt(I_2) \subset lt(I_1 \cdot I_2).$$

Für die zugehörigen Varietäten erhalten wir die Inklusion

$$Var(lt(I_1)) \cup Var(lt(I_2)) \supset Var(lt(I_1 \cdot I_2))$$

Sei nun

$$E \subset Var(lt(I_1 \cdot I_2))$$

ein Koordinatenunterraum maximaler Vektorraumdimension. Als irreduzible algebraische Varietät liegt E als Teilmenge der Vereinigung

$$Var(\, lt(\, I_1\,)\,) \cup Var(\, lt(\, I_2\,)\,)$$

schon in einer der beiden Komponenten. Mit Hilfe von Lemma 5.11 folgt

$$\dim_K E = \dim Var(\, lt(I_1 \cdot I_2)\,) = \dim X_1 \cup X_2 \le \max\{\dim X_1, \dim X_2\}.$$

Die umgekehrte Inklusion

$$\dim X_1 \cup X_2 \ge \max\{\dim X_1, \dim X_2\}$$

folgt aus den Inklusionen

$$I_1 \cap I_2 \subset I_1 \text{ und } I_1 \cap I_2 \subset I_2$$

und der Monotonie der affinen Hilbert Funktion.

ii) Der Zusammenhang zwischen der Dimension einer affinen Varietät und der Dimension ihrer irreduziblen Komponenten ergibt sich sofort aus Teil i) und der Tatsache, daß eine Varietät nur endlich viele irreduzible Komponenten hat, q.e.d.

5.17 Satz *(Dimension und Transzendenzgrad)*

Die Dimension einer irreduziblen affinen k-Varietät X stimmt mit dem Transzendenzgrad ihres rationalen Funktionenkörpers überein:

$$trdeg_k k(X) = \dim X\,.$$

Beweis. Wir zeigen die folgende Kette von Abschätzungen:

$$\dim X \le trdeg_k\, k(X) \le \dim X$$

ad i) Wir beweisen die Abschätzung

$$\dim X \le trdeg_k\, k(X)\,.$$

Nach Korollar 5.14 stimmt die Dimension von X überein mit der Dimension der monomialen Varietät

$$Y := Var(\, lt(I)\,) \subset \boldsymbol{A}^n(K).$$

Diese enthält nach Satz 5.12 einen Koordinatenunterraum

$$E \subset Y$$

der Vektorraumdimension

$$d := \dim Y = \dim X\,,$$

also o. E.

$$E = span_K \langle e_1, ..., e_d \rangle \subset K^n,\ e_i \in K^n \text{ kanonischer Basisvektor.}$$

Wir betrachten den Punkt

$$y := \sum_{i=1}^{d} e_i = (\,1, ..., 1, 0, ..., 0) \in E \subset Y\,.$$

Nach Definition von Y verschwindet jedes Monom aus $lt(I)$ an der Stelle $y \in Y$, enthält also zumindest eine der Variablen

$$T_r \text{ mit } d+1 \le r \le n\,.$$

Daher gilt

$$lt(I) \cap k[T_1,...,T_d] = 0$$

also auch

$$I \cap k[T_1,...,T_d] = 0 .$$

Die Koordinatenfunktionen

$$T_1,...,T_d \in k[T_1,...,T_n]$$

definieren reguläre Funktionen

$$f_1,..., f_d \in k[X],$$

also insbesondere rationale Funktionen aus $k(X)$.

Annahme: Diese Funktionen sind algebraisch abhängig. Dann gibt es ein nicht verschwindendes Polynom

$$0 \neq P \in k[U_1,...,U_d]$$

mit

$$P(f_1,...,f_d) = 0 \in k[X], \text{ d.h. } P(T_1,...,T_d) \in I .$$

Nach der gerade bewiesenen Aussage

$$I \cap k[T_1,...,T_d] = 0$$

folgt hieraus

$$P(T_1,...,T_d) = 0 , \text{ d.h. } P = 0 .$$

Also sind die Funktionen

$$f_1,..., f_d \in k[X] \subset k(X)$$

algebraisch unabhängig, und wir haben gezeigt

$$d \leq trdeg_k\, k(X).$$

ad ii) Wir zeigen $trdeg_k\, k(X) \leq \dim X$. Es sei

$$f_1,..., f_r \in k(X)$$

eine vorgegebene Familie algebraisch unabhängiger Funktionen. Nach Einführung eines Hauptnenners haben sie die Gestalt

$$f_i = \frac{g_i}{h},\ i = 1,..., r ,$$

mit regulären Funktionen

$$h,\ g_1,..., g_r \in k[X].$$

Eine Auswahl zugehöriger Repräsentanten in $k[T_1,...,T_n]$ seien

$$H, G_1,..., G_r \in k[T_1,...,T_n],\ F_i := \frac{G_i}{H} \in k(T_1,...,T_n) .$$

Es sei N das Maximum der Grade der Polynome

$$H, G_1,...,G_r \in k[T_1,...,T_n].$$

Es sei

$$I := Id(X) \subset k[T_1,...,T_r]$$

das Verschwindungsideal von X. Für jedes $s \in \boldsymbol{N}$ definieren wir eine k-lineare Abbildung

$$\alpha_s : k[U_1,...,U_r]_{\leq s} \longrightarrow k[T_1,...,T_r]_{\leq N\cdot s}/I_{\leq N\cdot s}, P \mapsto H^s \cdot P(F_1,...,F_r) + I_{\leq N\cdot s}.$$

Die Abbildung ist wohldefiniert, weil der Grad von

$$H^s \cdot P(F_1,...,F_r)$$

nach Wahl von N durch $N \cdot s$ beschränkt ist. Zum Beweis der Injektivität sei

$$\left[H^s \cdot P(F_1,...,F_r)\right] = 0 \in k[T_1,...,T_r]_{\leq N\cdot s}/I_{\leq N\cdot s}.$$

Vermöge der kanonischen injektiven Abbildungen

$$k[T_1,...,T_r]_{\leq N\cdot s}/I_{\leq N\cdot s} \longrightarrow k[T_1,...,T_r]/I \xrightarrow{\subset} k(X)$$

folgt

$$\left[H^s \cdot P(F_1,...,F_r)\right] = h^s \cdot P(f_1,...,f_r) = 0 \in k(X).$$

Im Körper $k(X)$ folgt hieraus das Verschwinden von

$$P(f_1,...,f_r) \in k(X)$$

und wegen der algebraischen Unabhängigkeit der rationalen Funktionen

$$f_1,...,f_r \in k(X)$$

das Verschwinden des Polynoms

$$P \in k[U_1,...,U_r].$$

Aus der Injektivität aller Abbildungen

$$\alpha_s, s \in \boldsymbol{N},$$

folgt die Abschätzung für die affinen Hilbert Funktionen

$$Hilb^{aff}_{k[U_1,...,U_r]}(s) \leq Hilb^{aff}_{k[X]}(N \cdot s) \text{ für alle } s \in \boldsymbol{N}$$

und für die affinen Hilbert Polynome

$$HP^{aff}_{k[U_1,...,U_r]}(s) \leq HP^{aff}_{k[X]}(N \cdot s) \text{ für alle } s \geq s_0.$$

Somit hat das affine Hilbert Polynom von $k[X]$ mindestens den Grad des affinen Hilbert Polynoms des Polynomringes $k[U_1,...,U_r]$, d.h.

$$r \leq dim\ X, \text{ q.e.d.}$$

Singularitäten einer affinen Varietät

Eine Singularität ist eine lokale Eigenschaft einer Varietät. Man spricht von singulären und von glatten Punkten einer Varietät. Aus Sicht der Geometrie heißt eine Kurve glatt in einem Punkt, wenn sie dort eine eindeutig bestimmte Tangente hat. Analog heißt eine Fläche glatt in einem Punkt, wenn alle Tangenten im ausgezeichneten Punkt eine Ebene bilden.

Wir setzen ab jetzt voraus, daß der Definitionskörper ebenfalls algebraisch abgeschlossen ist und mit dem Koordinatenkörper übereinstimmt

$$k = \bar{k} = K$$

und betrachten affine K-Varietäten. Für eine affine K-Varietät $X \subset \boldsymbol{A}^n(K)$ entsprechen dann nach Korollar ??? die Punkte von X bijektiv den maximalen Idealen des Koordinatenringes $K[X]$. Einem Punkt $x \in X$ ist dabei sein Verschwindungsideal

$$m_x = \langle T_1 - x_1, ..., T_n - x_n \rangle \subset K[X]$$

zugeordnet und es gilt

$$K \cong K[X] / m_x .$$

5.18 **Definition** *(Cotangential- und Tangentialraum)*

Es sei $X \subset \boldsymbol{A}^n(K)$ eine affine K-Varietät. Der *Cotangentialraum* in einem Punkt

$$x \in X$$

mit Verschwindungsideal

$$m_x \subset K[X]$$

ist der K-Vektorraum

$$\Omega_{X,x} := m_x / m_x^{\,2} ,$$

der *Tangentialraum* im Punkt $x \in X$ ist der duale K-Vektorraum

$$TX_x := \left(m_x / m_x^{\,2}\right)^* .$$

Die Dimension beider Vektorräume heißt *Einbettungsdimension*

$$eibdim(X, x)$$

der affinen Varietät X im Punkt $x \in X$.

5.19 **Definition** *(Glattheit und Singularität)*

Eine irreduzible affine K-Varietät $X \subset \boldsymbol{A}^n(K)$ heißt *glatt* in einem Punkt $x \in X$, wenn dort die Einbettungsdimension mit der Dimension übereinstimmen:

$$dim\ X = eibdim(X, x).$$

Andernfalls heißt $x \in X$ ein *singulärer* Punkt oder eine *Singularität* von X.

Der Tangentialraum hat auch eine geometrische Bedeutung, er stellt die Tangentialebene an die Varietät dar.

5.20 Lemma *(Tangentialraum und geometrische Tangentialebene)*

Es sei $X \subset \boldsymbol{A}^n(K)$ eine affine K-Varietät. Die durch den Kern der Jacobi Matrix in einem Punkt $a \in X$

$$Jac(X, a) := \begin{pmatrix} \frac{\partial f_1}{\partial T_1}(a) & \ldots & \frac{\partial f_1}{\partial T_n}(a) \\ \ldots & & \ldots \\ \frac{\partial f_r}{\partial T_1}(a) & \ldots & \frac{\partial f_r}{\partial T_n}(a) \end{pmatrix}, \langle f_1, \ldots, f_r \rangle = Id(X) \subset K[T_1, \ldots, T_n]$$

definierte geometrische Tangentialebene

$$\{ x \in K^n : Jac(X, a) \cdot (x - a) = 0 \}$$

ist isomorph zum Tangentialraum TX_a.

Beweis. Wir geben eine Abbildung von TX_a in die geometrische Tangentialebene an: Es sei ein Element

$$\lambda : m_a / m_a^2 \longrightarrow K$$

des Tangentialraumes vorgegeben. Für jedes Polynom $f \in Id(X)$ gilt

$$f(T_1, \ldots, T_n) - f(a) = \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(a) \cdot (T_i - a_i) + m_a^2 \in Id(X)$$

und daher

$$0 = \lambda(f(T_1, \ldots, T_n) - f(a)) = \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(a) \cdot \lambda(T_i - a_i).$$

Also liegt der Vektor

$$(\lambda(T_1 - a_1), \ldots, \lambda(T_n - a_n)) \in K^n$$

in der geometrischen Tangentialebene.

5.21 Satz *(Jacobi Kriterium)*

Eine irreduzible affine K-Varietät $X \subset \boldsymbol{A}^n(K)$ ist genau dann glatt in einem Punkt $a \in X$, wenn für die Jacobi Matrix an dieser Stelle gilt

$$n - rang\ Jac(X, a) = dim\ X.$$

Eine Hyperfläche

$$X = Var(f) \subset \boldsymbol{A}^n(K)$$

ist genau dann glatt in einem Punkt $a \in X$, wenn dort mindestens eine der partiellen Ableitungen nicht verschwindet

$$\frac{\partial f}{\partial T_i}(a) \neq 0$$

für mindestens ein $i = 1, \ldots, n$.